



Guida all'implementazione

Cloud Migration Factory su AWS



Cloud Migration Factory su AWS: Guida all'implementazione

Copyright © 2024 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 delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Panoramica della soluzione	1
Funzionalità e vantaggi	2
Casi d'uso	3
Concetti e definizioni	3
Panoramica dell'architettura	5
Diagramma architetturale	5
Tracker di migrazione opzionale	6
AWSConsiderazioni sulla progettazione Well-Architected	7
Eccellenza operativa	8
Sicurezza	8
Affidabilità	8
Efficienza delle prestazioni	8
Ottimizzazione dei costi	9
Sostenibilità	9
Dettagli architettonici	10
Server di automazione della migrazione	10
I servizi di migrazione RestAPIs	11
Servizi di accesso	11
Servizi di amministrazione	11
Servizi per gli utenti	12
Strumenti e servizi	12
Interfaccia web Migration Factory	13
AWSservizi inclusi in questa soluzione	13
Pianifica la tua implementazione	17
Costo	17
(Facoltativo/consigliato) Distribuisci un'istanza Amazon Elastic Compute Cloud per facilitare l'esecuzione di script di automazione	19
Sicurezza	20
Ruoli IAM	20
Amazon Cognito	20
Amazon CloudFront	20
Amazon AWS WAF - Firewall per applicazioni Web	21
Regioni AWS supportate	21
Quote	23

Quote per i AWS servizi di questa soluzione	23
Quote AWS CloudFormation	23
Implementa la soluzione	24
Prerequisiti	24
Autorizzazioni del server di origine	24
AWS Servizio di migrazione delle applicazioni (AWS MGN)	24
Implementazione privata	24
AWS CloudFormation modelli	24
Panoramica del processo di distribuzione	25
Fase 1: Scegli l'opzione di implementazione	26
Fase 2: Avvia lo stack	27
Passaggio 3: avvia lo stack di account di destinazione nell'account di destinazione AWS	36
Fase 4: Creare il primo utente	38
Crea l'utente iniziale e accedi alla soluzione	38
Aggiungi un utente al gruppo di amministratori	39
Identifica l'URL CloudFront	39
Fase 5: (Facoltativo) Implementazione del contenuto statico della console Web privata	40
Fase 6: Aggiornare lo schema di fabbrica	41
Aggiorna l'aws_accountid per MGN AWS	41
Fase 7: Configurazione di un server di automazione della migrazione	42
Crea un server Windows Server 2016 o versione successiva	42
Installazione del software richiesto per supportare le automazioni	43
Configura AWS le autorizzazioni per il server di automazione della migrazione e installa AWS Systems Manager Agent (SSM Agent)	44
Fase 8: Testare la soluzione utilizzando gli script di automazione	50
Importa i metadati di migrazione in fabbrica	50
Accedi ai domini	55
Esegui un test dell'automazione della migrazione	55
Fase 9: (Facoltativo) Creazione di un dashboard per il monitoraggio della migrazione	55
Imposta l' QuickSight autorizzazione e le connessioni	56
Creazione di un pannello di controllo	64
Passaggio 10: (Facoltativo) Configurazione di provider di identità aggiuntivi in Amazon Cognito	74
Monitora la soluzione con Service Catalog AppRegistry	77
Attiva CloudWatch Application Insights	77
Conferma i cartellini dei costi associati alla soluzione	79

Attiva i tag di allocazione dei costi associati alla soluzione	80
AWS Cost Explorer	81
Aggiornare la soluzione	82
Risoluzione dei problemi	84
Contatto AWS Support	84
Crea caso	84
Come possiamo aiutare?	84
Informazioni aggiuntive	84
Aiutaci a risolvere il tuo caso più rapidamente	85
Risolvi ora o contattaci	85
Dissoluzione soluzione soluzione soluzione soluzione	86
Svuota i bucket Amazon S3.	86
Utilizzo diAWS Management Console per eliminare lo stack	86
UtilizzoAWS Command Line Interface per eliminare lo stack	87
Guida per l'utente	88
Gestione dei metadati	88
Visualizzazione dei dati	88
Aggiungere o modificare un record	89
Eliminazione di un record	89
Esportazione dei dati	90
Importazione dei dati	91
Gestione delle credenziali	95
Aggiungi un segreto	95
Modifica un segreto	96
Eliminare un segreto	96
Esegui l'automazione dalla console	96
Esegui le automazioni dal prompt dei comandi	98
Esecuzione manuale di un pacchetto di automazione	99
Creazione del file.json FactoryEndpoints	100
Avvia i lavori AWS MGN da Cloud Migration Factory	101
Attività prerequisite	101
Definizione iniziale	102
Avvio di un lavoro	103
Ripiattaforma su EC2	105
Prerequisiti	105
Configurazione iniziale	105

Azioni di distribuzione	108
Gestione degli script	110
Carica un nuovo pacchetto di script	110
Scarica pacchetti di script	111
Aggiungi una nuova versione di un pacchetto di script	111
Eliminazione di pacchetti e versioni di script	111
Composizione di un nuovo pacchetto di script	112
Gestione dello schema	116
Aggiunta/modifica di un attributo	116
Gestione delle autorizzazioni	126
Policy	128
Roles	129
Guida per sviluppatori	130
Codice sorgente	130
Argomenti supplementari	131
Elenco delle attività di migrazione automatizzata tramite la console web di fabbrica	131
Verifica i prerequisiti	131
Installare gli agenti di replica	132
Invia gli script post-lancio	133
Verificare lo stato della replica	134
Convalida il modello di lancio	135
Avvia istanze per il test	136
Verifica lo stato dell'istanza di destinazione	137
Contrassegna come pronto per il taglio	138
Spegnerne i server di origine compresi nell'ambito	139
Avvia le istanze per Cutover	140
Elenco delle attività di migrazione automatizzata tramite il prompt dei comandi	140
Verifica i prerequisiti	141
Installare gli agenti di replica	143
Invia gli script post-lancio	145
Verificare lo stato della replica	146
Verifica lo stato dell'istanza di destinazione	148
Spegnerne i server di origine compresi nell'ambito	149
Recupera l'IP dell'istanza di destinazione	149
Verifica le connessioni al server di destinazione	150
Documentazione di riferimento	152

Raccolta di dati anonimizzata	152
Risorse correlate	153
Collaboratori	154
Revisioni	155
Note	159
.....	clx

Coordina e automatizza le migrazioni su larga scala verso il AWS cloud utilizzando la soluzione Cloud Migration Factory on AWS

Data di pubblicazione: giugno 2020 ([ultimo aggiornamento](#): aprile 2024)

La AWS soluzione Cloud Migration Factory on è progettata per coordinare e automatizzare i processi manuali per le migrazioni su larga scala che coinvolgono un numero considerevole di server. Questa soluzione aiuta le aziende a migliorare le prestazioni ed evita lunghe interruzioni fornendo una piattaforma di orchestrazione per la migrazione dei carichi di lavoro su larga scala. AWS [AWS Servizi professionali](#), [AWS partner](#) e altre aziende hanno già utilizzato questa soluzione per aiutare i clienti a migrare migliaia di server verso. Cloud AWS

Questa soluzione consente di:

- Integra i diversi tipi di strumenti che supportano la migrazione, come strumenti di rilevamento, strumenti di migrazione e strumenti per il database di gestione della configurazione (CMDB).
- Automatizza le migrazioni che comportano molte piccole attività manuali, che richiedono tempo per essere eseguite e sono lente e difficili da scalare.

Per una guida completa all' end-to-end implementazione con questa soluzione, consulta [Automazione delle migrazioni di server su larga scala con Cloud Migration Factory nella AWS Prescriptive Guidance Cloud Migration Factory](#) Guide.

Questa guida all'implementazione illustra le considerazioni sull'architettura e i passaggi di configurazione per l'implementazione di Cloud Migration Factory su AWS una soluzione nel cloud Amazon Web Services (AWS). Include collegamenti a [AWS CloudFormation](#) modelli che avviano e configurano i AWS servizi necessari per implementare questa soluzione utilizzando le AWS migliori pratiche per la sicurezza e la disponibilità.

La guida è destinata agli architetti, agli amministratori e DevOps ai professionisti dell'infrastruttura IT che hanno esperienza pratica nell'architettura in. Cloud AWS

Utilizza questa tabella di navigazione per trovare rapidamente le risposte a queste domande:

Se vuoi.	Leggi..
Conosci il costo di esecuzione di questa soluzione. Il costo stimato per l'esecuzione di questa soluzione nella us-east-1 regione è di 14,31 USD al mese per le AWS risorse.	Costo
Comprendi le considerazioni sulla sicurezza di questa soluzione.	Sicurezza
Scopri come pianificare le quote per questa soluzione.	Quote
Scopri quali Regioni AWS supporti questa soluzione.	Supportata Regioni AWS
Visualizza o scarica i AWS CloudFormation modelli inclusi in questa soluzione per distribuire automaticamente le risorse dell'infrastruttura (lo «stack») per questa soluzione.	AWS CloudFormation modelli

Funzionalità e vantaggi

La soluzione offre le seguenti funzionalità:

Gestisci, monitora e avvia la migrazione del carico di lavoro AWS da un'unica interfaccia web, supportando più destinazioni Account AWS e aree geografiche.

Fornito con hosting di siti Web statici Amazon S3 o in distribuzione privata da un'istanza Amazon EC2 che esegue un server Web. Tutte le attività eseguite dalla soluzione vengono avviate da un'unica interfaccia web, fornita dalla soluzione. Vedi l'interfaccia web di Migration Factory per i dettagli.

Attività di automazione preconfezionate per eseguire molte delle attività necessarie per migrare completamente i carichi di lavoro all' AWS utilizzo AWS di Application Migration Service.

La soluzione fornisce tutte le attività di automazione necessarie per migrare migliaia di carichi di lavoro AWS senza la necessità di script e con conoscenze limitate necessarie per iniziare. Tutte le automazioni possono essere avviate dall'interfaccia web e in ambito tecnico si utilizza AWS System Manager per avviare ed eseguire i processi di automazione sui server di automazione forniti.

Personalizza la soluzione con pacchetti di automazione ed estensioni dello schema degli attributi

La maggior parte delle migrazioni richiede l'esecuzione di attività di automazione personalizzate per applicazioni e altri motivi ambientali specifici. Cloud Migration Factory on AWS supporta la personalizzazione da parte dell'utente degli script forniti, nonché la possibilità di caricare script personalizzati nella soluzione. La soluzione consente inoltre di estendere l'archivio dei metadati di migrazione in pochi secondi, offrendo agli amministratori la possibilità di aggiungere e rimuovere attributi dallo schema che devono essere tracciati o utilizzati durante la migrazione.

Integrazione con Service Catalog AppRegistry e AWS Systems Manager Application Manager

Questa soluzione include una AppRegistry risorsa Service Catalog per registrare il CloudFormation modello della soluzione e le relative risorse sottostanti come applicazione sia in [Service Catalog AppRegistry](#) che in [AWS Systems Manager Application Manager](#). Con questa integrazione, è possibile gestire centralmente le risorse della soluzione e abilitare le azioni di ricerca, reportistica e gestione delle applicazioni.

Casi d'uso

Migra e gestisci migrazioni su larga scala dei carichi di lavoro verso AWS

Abilita una visualizzazione da un'unica schermata delle migrazioni dei carichi di lavoro su larga scala verso AWS. Fornisce automazione, reportistica e accesso basato sui ruoli predefiniti tramite un'unica interfaccia web progettata specificamente per le migrazioni.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questa soluzione:

applicazione

Un gruppo di risorse che costituiscono un singolo servizio o applicazione aziendale.

ondata

Un gruppo di applicazioni che verranno migrate nello stesso evento. Ciò potrebbe essere basato sull'affinità reciproca o su qualsiasi altro motivo.

server

Server di origine da migrare.

database

Database di origine da migrare.

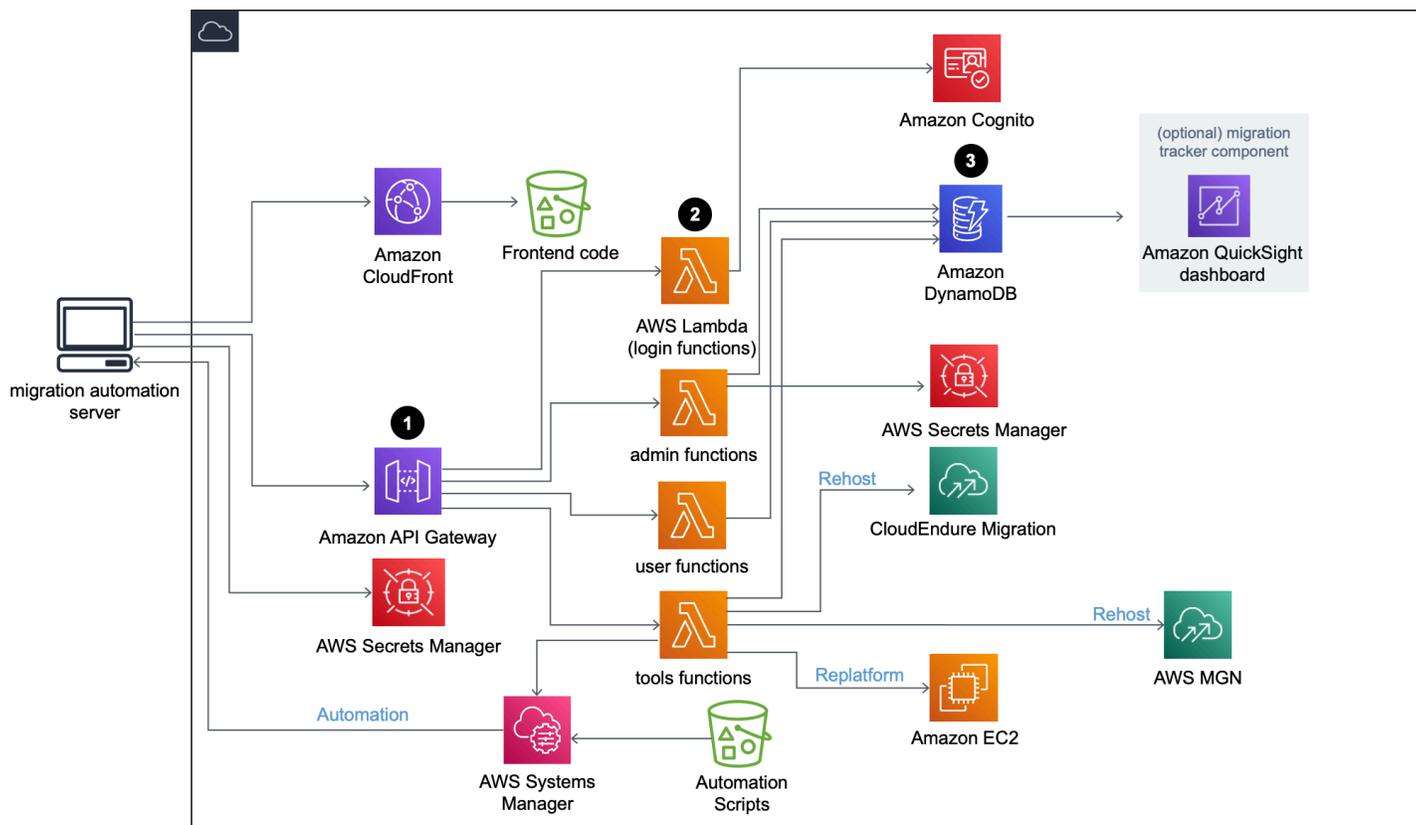
Per un riferimento generale dei AWS termini, consulta il [AWS glossario](#) nella Guida AWS generale.

Panoramica dell'architettura

Questa sezione fornisce un diagramma dell'architettura di implementazione di riferimento per i componenti distribuiti con questa soluzione.

Diagramma architetturale

L'implementazione della soluzione predefinita crea il seguente ambiente serverless nel cloud. AWS



Cloud Migration Factory sul diagramma AWS dell'architettura

Il AWS CloudFormation modello della soluzione lancia i AWS servizi necessari per aiutare le aziende a migrare i propri server.

Note

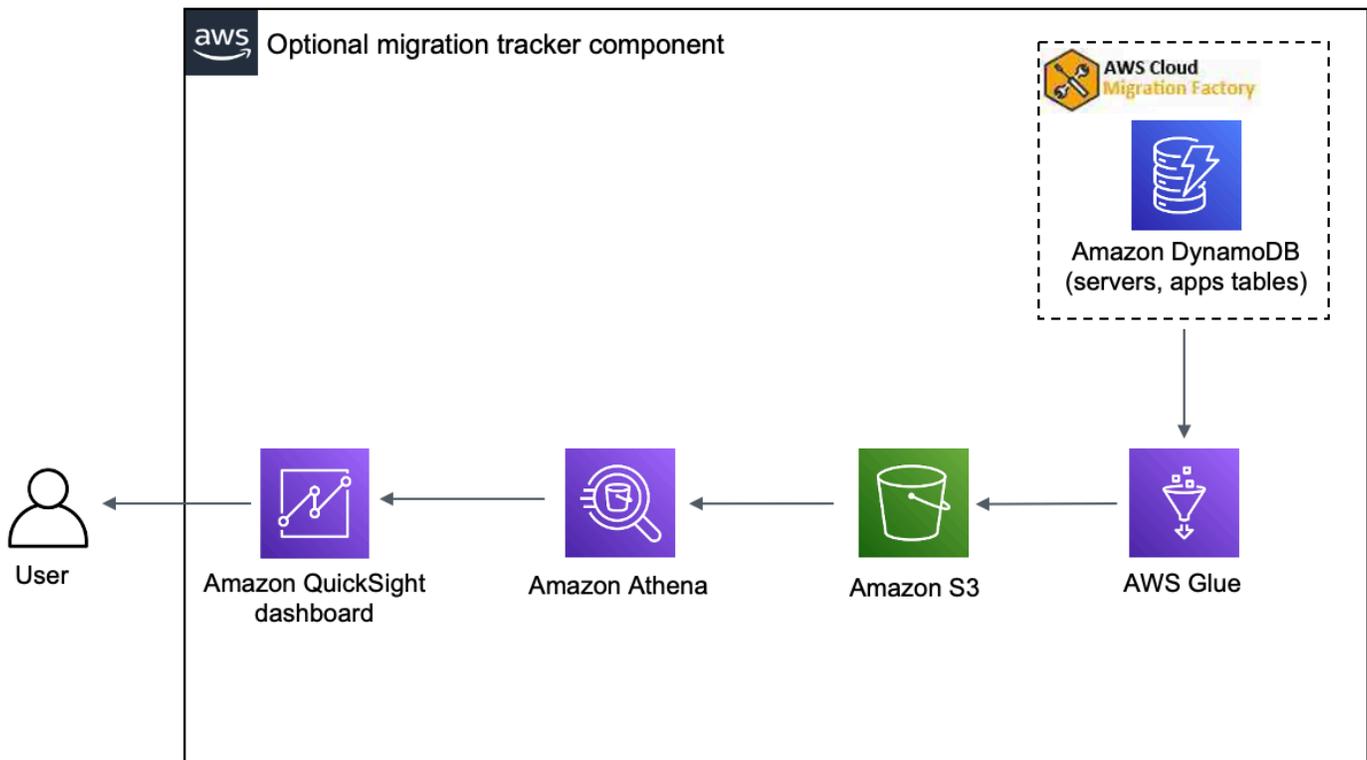
La AWS soluzione Cloud Migration Factory on utilizza un server di automazione della migrazione che non fa parte della AWS CloudFormation distribuzione. Per maggiori dettagli

sulla creazione manuale del server, consulta [Creare un server di automazione della migrazione](#).

1. [Amazon API Gateway](#) riceve le richieste di migrazione dal server di automazione della migrazione tramite RestAPI.
2. [AWS Lambda](#) le funzioni forniscono i servizi necessari per accedere all'interfaccia Web, eseguire le funzioni amministrative necessarie per gestire la migrazione e connettersi a API di terze parti per automatizzare il processo di migrazione.
 - [La funzione user Lambda inserisce i metadati di migrazione in una tabella Amazon DynamoDB](#). I codici di stato HTTP standard vengono restituiti all'utente tramite RestAPI dall'API Gateway. Un pool di utenti [Amazon Cognito](#) viene utilizzato per l'autenticazione degli utenti all'interfaccia Web e alle API Rest e, facoltativamente, puoi configurarlo per l'autenticazione con provider di identità SAML (Security Assertion Markup Language) esterni.
 - Le funzioni tools Lambda elaborano le API Rest esterne e richiamano il [CloudEndure Migration and AWS Application Migration Service \(AWSMGN\) per la migrazione](#). AWS La funzione tools Lambda richiama inoltre [Amazon EC2](#) per il lancio di istanze EC2 e chiama [AWSSystems Manager](#) per eseguire script di automazione sul Migration Automation Server.
3. I metadati di migrazione archiviati in Amazon DynamoDB vengono indirizzati all'API MGN AWS per avviare processi di migrazione Rehost e avviare i server. Se il modello di migrazione è Replatform to EC2, la funzione tools Lambda avvia i modelli di avvio CloudFormation nell'account AWS di destinazione per avviare le istanze Amazon EC2.

Tracker di migrazione opzionale

Questa soluzione implementa anche un componente opzionale di monitoraggio della migrazione che monitora l'avanzamento della migrazione.



Componente opzionale per il monitoraggio della migrazione

Il CloudFormation modello si [AWS Glue](#) implementa per ottenere i metadati di migrazione dalla tabella DynamoDB di Cloud Migration Factory ed esporta i metadati su Amazon Simple [Storage Service](#) ([Amazon S3](#)) due volte al giorno (alle 5:00 e alle 13:00 UTC). Al termine del AWS Glue processo, viene avviata una query di salvataggio di Amazon Athena e puoi configurare QuickSight Amazon per estrarre i dati dai risultati della query Athena. Puoi quindi creare le visualizzazioni e creare una dashboard che soddisfi le tue esigenze aziendali. Per indicazioni sulla creazione di immagini e sulla creazione di una dashboard, consulta [Creazione di una dashboard per il monitoraggio delle migrazioni](#).

Questo componente opzionale è gestito dal parametro Tracker nel modello CloudFormation. Per impostazione predefinita, questa opzione è attivata, ma è possibile disattivarla modificando il parametro Tracker in `false`.

AWS Considerazioni sulla progettazione Well-Architected

Questa soluzione utilizza le migliori pratiche del [AWS Well-Architected](#) Framework, che aiuta i clienti a progettare e gestire carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud.

Questa sezione descrive in che modo i principi di progettazione e le migliori pratiche di Well-Architected Framework favoriscono questa soluzione.

Eccellenza operativa

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'eccellenza [operativa](#).

- Risorse definite come IaC utilizzando CloudFormation
- Tutte le azioni e la registrazione degli audit vengono inviate ad Amazon CloudWatch, per consentire l'implementazione di risposte automatiche.

Sicurezza

[Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sicurezza.](#)

- IAM utilizzato per l'autenticazione e l'autorizzazione.
- L'ambito delle autorizzazioni di ruolo è stato progettato per essere il più ristretto possibile, sebbene in molti casi questa soluzione richieda autorizzazioni jolly per poter agire su qualsiasi risorsa.
- Uso opzionale di WAF per proteggere ulteriormente la soluzione.
- Amazon Cognito e possibilità opzionale di federarsi con IDP esterni.

Affidabilità

[Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità.](#)

- I servizi serverless consentono alla soluzione di fornire un'architettura con tolleranza agli errori.

Efficienza delle prestazioni

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'[efficienza delle prestazioni](#).

- I servizi serverless consentono alla soluzione di scalare in base alle esigenze.

Ottimizzazione dei costi

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'[ottimizzazione dei costi](#).

- I servizi serverless ti consentono di pagare solo ciò che utilizzi.

Sostenibilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del [pilastro della sostenibilità](#).

- I servizi serverless consentono la scalabilità verso l'alto o verso il basso in base alle esigenze.

Dettagli architetturici

Server di automazione della migrazione

Questa soluzione sfrutta un server di automazione della migrazione per eseguire le migrazioni utilizzando le API Rest. Questo server non viene distribuito automaticamente con la soluzione e deve essere creato manualmente. Per ulteriori informazioni, consulta [Build a Migration Automation Server](#). Ti consigliamo di creare il server nel tuo AWS ambiente, ma puoi anche crearlo localmente nel tuo ambiente di rete. Il server deve soddisfare i seguenti requisiti:

- Windows Server 2016 o versioni successive
- Almeno 4 CPU con 8 GB di RAM
- Implementato come nuova macchina virtuale senza applicazioni aggiuntive installate
- (Se integrato AWS) Nella stessa Account AWS regione di Cloud Migration Factory

Una volta installato, il server richiede l'accesso a Internet e una connettività di rete interna non restrittiva ai server di origine pertinenti (server verso cui migrare). AWS

Se è richiesta la limitazione delle porte dal server di automazione della migrazione ai server di origine, è necessario aprire le seguenti porte dal server di automazione della migrazione ai server di origine:

- Porta SMB (TCP 445)
- Porta SSH (TCP 22)
- Porta WinRM (TCP 5985, 5986)

È consigliabile che il server di automazione della migrazione si trovi nello stesso dominio Active Directory dei server di origine. Se i server di origine risiedono in più domini, la configurazione di sicurezza per il dominio di fiducia in ogni dominio determina se è necessario più di un server di automazione della migrazione.

- Se la fiducia del dominio esiste in tutti i domini con server di origine, un singolo server di automazione della migrazione sarà in grado di connettersi ed eseguire script di automazione per tutti i domini.

- Se non esiste un trust di dominio in tutti i domini, è necessario creare un server di automazione della migrazione aggiuntivo per ogni dominio non attendibile oppure per ogni azione da eseguire sul server di automazione sarà necessario fornire credenziali alternative con le autorizzazioni appropriate sui server di origine.

I servizi di migrazione RestAPIs

La AWS soluzione Cloud Migration Factory automatizza il processo di migrazione utilizzando API Rest elaborate tramite AWS Lambda funzioni, un Amazon API Gateway, AWS Managed Services AWS Application Migration Service (AWS MGN) e Migration. CloudEndure Quando effettui una richiesta o inizi una transazione, ad esempio l'aggiunta di un server o la visualizzazione di un elenco di server o applicazioni, vengono effettuate chiamate API Rest ad Amazon API Gateway che avvia una AWS Lambda funzione per eseguire la richiesta. I seguenti servizi descrivono in dettaglio i componenti per il processo di migrazione automatizzato.

Servizi di accesso

I servizi di accesso includono le funzioni login Lambda e Amazon Cognito. Una volta effettuato l'accesso alla soluzione utilizzando l'loginAPI tramite API Gateway, la funzione convalida le credenziali, recupera un token di autenticazione da Amazon Cognito e ti restituisce i dettagli del token. Puoi utilizzare questo token di autenticazione per connetterti agli altri servizi di questa soluzione.

Servizi di amministrazione

I servizi di amministrazione includono Amazon API Gateway, funzioni admin Lambda e Amazon DynamoDB. Gli amministratori della soluzione possono utilizzare la funzione admin Lambda per definire lo schema dei metadati di migrazione, che sono gli attributi dell'applicazione e del server. L'API dei servizi di amministrazione fornisce la definizione dello schema per la tabella DynamoDB. I dati utente, inclusi gli attributi dell'applicazione e del server, devono rispettare questa definizione dello schema. Gli attributi tipici includono `app_name`, `wave_idserver_name`, e altri campi identificati in [Importazione dei metadati di migrazione in fabbrica](#). Per impostazione predefinita, il AWS CloudFormation modello implementa automaticamente uno schema comune, ma questo può essere personalizzato dopo la distribuzione.

Gli amministratori possono anche utilizzare i servizi di amministrazione per definire i ruoli di migrazione per i membri del proprio team di migrazione. L'amministratore dispone di un controllo

granulare per mappare ruoli utente specifici a attributi e fasi di migrazione specifici. Una fase di migrazione è un periodo di tempo necessario per eseguire determinate attività di migrazione, ad esempio una fase di compilazione, una fase di test e una fase finale.

Servizi per gli utenti

I servizi utente includono Amazon API Gateway, funzioni user Lambda e Amazon DynamoDB. Gli utenti possono gestire i metadati di migrazione, permettendo loro di leggere, creare, aggiornare ed eliminare i dati di wave, applicazioni e server nella pipeline di metadati di migrazione.

Nota

Un'ondata di migrazione è un concetto di raggruppamento di applicazioni con una data di inizio e una data di fine o limite. I dati Wave includono le applicazioni candidate alla migrazione e i raggruppamenti di applicazioni pianificati per una particolare ondata di migrazione.

I servizi utente offrono un'API per il team di migrazione per manipolare i dati nella soluzione: creare, aggiornare ed eliminare i dati utilizzando lo script Python e i file CSV di origine. Per i passaggi dettagliati, consulta [Attività di migrazione automatizzate utilizzando la console web Migration Factory](#) e [Attività di migrazione automatizzate tramite il prompt dei comandi](#).

Strumenti e servizi

I servizi degli strumenti includono Amazon API Gateway, le funzioni tools Lambda, Amazon DynamoDB AWS Managed ServicesAWS, Application Migration Service e Migration. CloudEndure Puoi utilizzare questi servizi per connetterti a API di terze parti e automatizzare il processo di migrazione. Utilizzando CloudEndure Migration and AWS Application Migration Service, il team addetto alla migrazione può orchestrare il processo di avvio del server premendo un solo pulsante per avviare tutti i server nella stessa fase, costituita da un gruppo di applicazioni e server con la stessa data di scadenza. UtilizzandoAWS Managed Services, la AWS soluzione Cloud Migration Factory on automatizza il processo RFC di inserimento del carico di lavoro e riduce lo sforzo manuale necessario durante il processo di migrazione.

Interfaccia web Migration Factory

La soluzione include un'interfaccia web Migration Factory che può essere ospitata, per impostazione predefinita, in un bucket Amazon S3 o su un server Web fornito (non parte della distribuzione della soluzione) che consente di completare le seguenti attività utilizzando un browser Web:

- Aggiorna i metadati di wave, applicazioni e server dal tuo browser web
- Gestisci le definizioni degli schemi di applicazioni e server
- Esegui script di automazione per automatizzare le attività di migrazione, ad esempio la verifica dei prerequisiti, l'installazione degli agenti MGN
- Crea credenziali di migrazione per connetterti ai server di origine
- Connect a servizi di terze parti come AWS Application Migration Service, CloudEndure Migration e AWS Managed Services automatizza il processo di migrazione

AWSservizi inclusi in questa soluzione

Servizio AWS	Descrizione	
Gateway Amazon API	Nucleo. Fornisce API REST all'intera soluzione, utilizzat e per accedere ai dati di backend e avviare e gestire le attività di automazione della migrazione.	
AWS Lambda	Nucleo. Fornisci i servizi necessari per accedere all'interfaccia web, eseguire le funzioni amministrative necessarie per gestire la migrazione e connetterti alle API di terze parti per automatizzare il processo di migrazione.	

Servizio AWS	Descrizione	
Amazon DynamoDB	Nucleo. Archivio di metadati per tutti i dati gestiti da utenti e sistemi, a cui si accede tramite Amazon API Gateways e funzioni Lambda.	
Amazon Cognito	Nucleo. L'autorizzazione e l'autenticazione degli utenti, la federazione opzionale con altri IdP, viene ottenuta anche tramite Amazon Cognito.	
AWS Systems Manager	Supporto. Supporta l'esecuzione di Cloud Migration Factory su pacchetti di AWS automazione sul server di automazione fornito dal cliente.	
Amazon EC2	Supporto. Server di automazione che esegue agenti AWS Systems Manager per consentire l'esecuzione di pacchetti di automazione.	
Amazon S3	Supporto. Utilizzato in diverse aree della soluzione, 1/ utilizzando la funzionalità di hosting web statico di Amazon S3, serve l'interfaccia Web principale (tramite CloudFront Amazon), 2/ i log e altri output di automazione vengono archiviati in Amazon S3 dalla soluzione.	

Servizio AWS	Descrizione	
AWS Secrets Manager	Supporto. Quando si utilizzano le funzionalità di automazione della soluzione, AWS Secrets Manager viene utilizzato per archiviare in modo sicuro le credenziali utilizzate per accedere alle risorse di migrazione al fine di eseguire attività e azioni per facilitare e migrare i carichi di lavoro.	
Amazon CloudFront	Facoltativo. Per le implementazioni standard, Amazon CloudFront fornisce la distribuzione del contenuto dell'interfaccia Web da Amazon S3, rendendolo altamente disponibile a livello globale e fornendo un accesso TLS sicuro ai contenuti dell'interfaccia Web da qualsiasi luogo.	
AWS Servizio di migrazione delle applicazioni (MGN) AWS	Facoltativo. Quando si eseguono migrazioni di rehosting di carichi di lavoro Windows o Linux, Cloud Migration Factory on AWS utilizza AWS MGN per semplificare la migrazione del sistema ad Amazon EC2.	

Servizio AWS	Descrizione	
Amazon QuickSight	Facoltativo. Consente di creare dashboard di migrazioni e personalizzabili in base ai dati archiviati nel metastore di migrazione contenuto in Amazon DynamoDB, fornendo ai team i dati necessari per tracciare e generare report sulle loro migrazioni.	
AWS Glue	Facoltativo. Estrae regolarmente i dati contenuti in Amazon DynamoDB su Amazon S3, fornendo dati di reporting da utilizzare nelle dashboard di Amazon Athena e Amazon QuickSight	
Amazon Athena	Facoltativo. Fornisce l'accesso ai dati di reporting estratti da AWS Glue dai metadati di migrazione, consentendo la creazione di dashboard utilizzando Amazon QuickSight	
AWS Firewall per applicazioni Web	Facoltativo. Applica una sicurezza aggiuntiva sugli endpoint per Amazon API Gateway e Amazon CloudFront per limitare l'accesso a dispositivi specifici in base all'indirizzo IP di origine o ad altri criteri di accesso.	

Pianifica la tua implementazione

Questa sezione ti aiuta a pianificare costi, sicurezza, regioni AWS e tipi di distribuzione per la soluzione Cloud Migration Factory on AWS.

Costo

Sei responsabile del costo dei AWS servizi utilizzati durante l'esecuzione di questa soluzione. A partire da questa revisione, il costo stimato per l'esecuzione di questa soluzione con le impostazioni predefinite nella regione Stati Uniti orientali (Virginia settentrionale) e supponendo che si stia migrando 200 server al mese con questa soluzione è di circa 14,31 USD al mese. Il costo di esecuzione di questa soluzione dipende dalla quantità di dati caricati, richiesti, archiviati, elaborati e presentati, come illustrato nella tabella seguente.

Servizio AWS	Fattori	Costo/mese [USD]
Servizi principali		
Gateway Amazon API	10.000 richieste/mese x (3,50 USD/milione)	0,035 USD
AWS Lambda	10.000 invocazioni/mese (durata media di 3.000 ms e 128 MB di memoria)	0,065 USD
Amazon DynamoDB	20.000 richieste di scrittura al mese x (1,25 USD/milione) 40.000 richieste di lettura/mese x (0,25 USD/milione) Archiviazione dati: 1 GB x 0,25 USD	0,035\$
Amazon S3	Archiviazione (10 MB) e 50.000 richieste di ottenimento al mese	0,25 USD

Servizio AWS	Fattori	Costo/mese [USD]
Amazon CloudFront	<p>Trasferimento dati regionale verso Internet: primi 10 TB</p> <p>Trasferimento dati da una regione all'origine: trasferimento di tutti i dati</p> <p>Richieste HTTPS: 50.000 richieste/mese X (0,01/10.000 richieste)</p>	0,92 USD
AWS Systems Manager	10.000 passi al mese	\$0,00
AWS Secrets Manager	5 segreti x 30 giorni di durata	\$2,00
Amazon Cognito (accesso diretto)	Fino a 50.000 utenti attivi mensili (MAU) coperti dal piano gratuito di AWS	0,00 USD
Amazon Athena	10 MB al giorno x 5,00 USD per TB di dati scansionati	0,0015 USD
Servizi opzionali		
AWS Glue(tracker di migrazione opzionale)	2 minuti al giorno x 10 DPU predefiniti x 0,44 USD per DPU/ora	4,40\$

Servizio AWS	Fattori	Costo/mese [USD]
AWS WAF	<p>2 Web ACL 5,00 USD al mese (ripartite proporzionalmente ogni ora)</p> <p>2 regole 1,00 USD al mese (ripartite proporzionalmente su base oraria)</p> <p>10.000 richieste x (0,60 USD per 1 milione di richieste)</p>	6,60\$
Amazon Cognito (accesso SAML)	<p>Fino a 50 MAU coperte dal piano gratuito di AWS</p> <p>Oltre 50 MAU, 0,015 USD/MAU</p>	\$0,00
Totale:		~ 14,31 USD/mese

(Consigliato) Implementa un'istanza Amazon Elastic Compute Cloud per facilitare l'esecuzione di script di automazione

Consigliamo di implementare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per automatizzare la connessione alle API della soluzione e alle API Boto3 con ruoli IAM. AWS La seguente stima dei costi presuppone che l'istanza Amazon EC2 si trovi us-east-1 nella regione e funzioni otto ore al giorno, cinque giorni alla settimana.

Servizio AWS	Fattori	Costo/mese [USD]
Amazon EC2	176 ore al mese x 0,1108 USD/ora () t3.large	\$19,50
Amazon Elastic Block Store (Amazon EBS)	30 GB x 0,08 USD/GB al mese (gp3) x (176 ore/720 ore)	0,59 USD

Servizio AWS	Fattori	Costo/mese [USD]
	Totale:	~20,09 \$

I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi di ogni AWS servizio che utilizzerai in questa soluzione.

Sicurezza

Quando crei sistemi sull'AWS infrastruttura, le responsabilità in materia di sicurezza vengono condivise tra te e AWS. Questo [modello condiviso](#) può ridurre il carico operativo in quanto AWS gestisce, gestisce e controlla i componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla sicurezza su AWS, visita [AWS Cloud Security](#).

Ruoli IAM

AWS Identity and Access Management ruoli (IAM) consentono di assegnare policy e autorizzazioni di accesso granulari a servizi e utenti nel cloud. AWS Questa soluzione crea ruoli IAM che garantiscono alla AWS Lambda funzione l'accesso agli altri AWS servizi utilizzati in questa soluzione.

Amazon Cognito

L'utente Amazon Cognito creato da questa soluzione è un utente locale con autorizzazioni per accedere solo alle RESAPI per questa soluzione. Questo utente non dispone delle autorizzazioni per accedere ad altri servizi del tuo account. AWS Per ulteriori informazioni, consulta i [pool di utenti di Amazon Cognito](#) nella Amazon Cognito Developer Guide.

La soluzione supporta opzionalmente l'accesso SAML esterno tramite la configurazione di provider di identità federati e la funzionalità dell'interfaccia utente ospitata di Amazon Cognito.

Amazon CloudFront

Questa soluzione predefinita implementa una console Web [ospitata](#) in un bucket Amazon S3. Per contribuire a ridurre la latenza e migliorare la sicurezza, questa soluzione include una CloudFront distribuzione [Amazon](#) con un'identità di accesso all'origine, ovvero un CloudFront utente speciale che aiuta a fornire l'accesso pubblico ai contenuti del bucket del sito Web della soluzione. Per

ulteriori informazioni, consulta la sezione [Limitazione dell'accesso ai contenuti Amazon S3 utilizzando un'identità Origin Access](#) nella CloudFront Amazon Developer Guide.

Se durante la distribuzione stack viene selezionato un tipo di distribuzione privata, la CloudFront distribuzione non viene distribuita e richiede l'utilizzo di un altro servizio di web hosting per ospitare la console web.

AWS WAF - Firewall per applicazioni Web

Se il tipo di distribuzione selezionato nello stack è Public with, [AWS WAF](#) CloudFormation distribuirà gli ACL AWS WAF Web richiesti e le regole configurate per proteggere gli endpoint API CloudFront Gateway e Cognito creati dalla soluzione CMF. Questi endpoint saranno limitati per consentire solo agli indirizzi IP di origine specificati di accedere a questi endpoint. Durante la distribuzione in stack, è necessario fornire due intervalli CIDR con la possibilità di aggiungere regole aggiuntive dopo la distribuzione tramite la console. AWS WAF

Regioni AWS supportate

Questa soluzione utilizza Amazon Cognito e Amazon QuickSight, che al momento sono disponibili solo in AWS regioni specifiche. Pertanto, è necessario avviare questa soluzione in una regione in cui questi servizi sono disponibili. Per la disponibilità dei servizi più aggiornata per regione, consulta [l'Elenco dei servizi AWS regionali](#).

Note

Il trasferimento dei dati durante il processo di migrazione non è influenzato dalle distribuzioni regionali.

Cloud Migration Factory on AWS è disponibile nelle seguenti regioni AWS:

Nomi delle regioni	
Stati Uniti orientali (Ohio)	Asia Pacifico (Tokyo)
Stati Uniti orientali (Virginia settentrionale)	Canada (Centrale)
Stati Uniti occidentali (California settentrionale)	Europa (Francoforte)

Nomi delle regioni	
Stati Uniti occidentali (Oregon)	Europa (Irlanda)
*Africa (Città del Capo)	Europa (Londra)
*Asia Pacifico (Hong Kong)	*Europa (Milano)
*Asia Pacifico (Hyderabad)	*Europa (Spagna)
*Asia Pacifico (Giacarta)	Europa (Parigi)
*Asia Pacifico (Melbourne)	Europa (Stoccolma)
Asia Pacifico (Mumbai)	*Europa (Zurigo)
Asia Pacifico (Osaka-Locale)	*Medio Oriente (Bahrain)
Asia Pacific (Seul)	*Medio Oriente (Emirati Arabi Uniti)
Asia Pacifico (Singapore)	Israele (Tel Aviv)
Asia Pacifico (Sydney)	Sud America (San Paolo)

 Important

*Disponibile solo per il tipo di distribuzione privata grazie alla registrazione degli CloudFront accessi di Amazon, consulta [Configurazione e utilizzo dei log standard \(log di accesso\) nella Amazon Developer Guide per i dettagli](#) più recenti. CloudFront

Cloud Migration Factory on AWS non è disponibile nelle seguenti regioni AWS:

Nome Regione	Servizi o opzioni di servizio non disponibili
AWS GovCloud (Stati Uniti orientali)	Amazon Cognito
AWS GovCloud (Stati Uniti occidentali)	Amazon Cognito

Quote

Le service quotas (o quote di servizio), a cui si fa riferimento anche come limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'Account AWS.

Quote per i AWS servizi di questa soluzione

Assicurati di disporre di una quota sufficiente per ciascuno dei [servizi implementati in questa soluzione](#). Per ulteriori informazioni, consulta le [quote AWS di servizio](#).

Seleziona uno dei seguenti link per accedere alla pagina relativa al servizio. Per visualizzare le quote di servizio per tutti i servizi AWS nella documentazione senza cambiare pagina, consulta le informazioni riportate in [Endpoint e quote del servizio](#) nel PDF.

Quote AWS CloudFormation

Hai delle CloudFormation quote di cui dovresti essere a conoscenza quando avvii lo stack per questa soluzione. Account AWS Comprendendo queste quote, è possibile evitare errori di limitazione che impedirebbero di implementare correttamente questa soluzione. Per ulteriori informazioni, consulta le [AWS CloudFormationquote nella Guida](#) per l'AWS CloudFormationutente.

Implementa la soluzione

Questa soluzione utilizza [AWS CloudFormation modelli e stack](#) per automatizzarne l'implementazione. I CloudFormation modelli specificano (y) le AWS risorse incluse in questa soluzione e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nei modelli.

Prerequisiti

Autorizzazioni del server di origine

Per i server Windows e Linux (autorizzazioni sudo) è necessario un utente di dominio con autorizzazioni di amministratore locale per i server di origine interessati alla migrazione. Se i server di origine non fanno parte di un dominio, è possibile utilizzare altri utenti, incluso un utente LDAP con autorizzazioni sudo/administrator o un utente sudo/amministratore locale. Prima di avviare questa soluzione, verificate di disporre delle autorizzazioni necessarie o di esservi coordinati con la persona appropriata all'interno dell'organizzazione responsabile delle autorizzazioni.

AWS Servizio di migrazione delle applicazioni (MGN)AWS

Se utilizzi AWS MGN per questa soluzione, devi prima inizializzare il servizio AWS MGN in ogni account e regione di destinazione prima di avviare lo stack di account di destinazione. Per maggiori dettagli, consulta [Initializing Application Migration Service nella Application Migration Service User Guide](#).

Implementazione privata

Se avete scelto di implementare un'istanza privata di CMF, installate un server Web nel vostro ambiente prima di procedere con l'implementazione della soluzione CMF.

AWS CloudFormation modelli

Questa soluzione consente AWS CloudFormation di automatizzare l'implementazione di Cloud Migration Factory su AWS una soluzione nel AWS cloud. Include il seguente AWS CloudFormation modello, che è possibile scaricare prima della distribuzione.

View template

[aws-](#)

[cloud-migration-factory-solution.template](#): utilizza questo modello per avviare Cloud Migration Factory sulla AWS soluzione e tutti i componenti associati. La configurazione predefinita implementa AWS Lambda funzioni, tabelle Amazon DynamoDB, un Amazon API Gateway, Amazon, bucket Amazon S3 CloudFront, un pool di AWS Systems Manager utenti Amazon Cognito, Automation [AWS Secrets Manager](#) Document e Secrets, ma puoi anche personalizzare il modello in base alle tue esigenze specifiche.

View template

[aws-](#)

[cloud-migration-factory-solution-target-account.template](#): utilizza questo modello per avviare gli account target della soluzione Cloud Migration Factory on AWS. La configurazione predefinita implementa ruoli IAM e un utente, ma puoi anche personalizzare il modello in base alle tue esigenze specifiche.

Panoramica del processo di implementazione

Prima di avviare la distribuzione automatizzata, esamina l'architettura, i componenti e le altre considerazioni discusse in questa guida. Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la AWS soluzione Cloud Migration Factory on nel tuo account.

Tempo di implementazione: circa 20 minuti

Note

Se distribuisce questa soluzione in regioni AWS diverse dagli Stati Uniti orientali (Virginia settentrionale), l' CloudFront URL di Migration Factory potrebbe richiedere più tempo per diventare disponibile. Durante questo periodo, riceverai un messaggio di accesso negato quando accedi all'interfaccia web.

[Fase 1: Scegli l'opzione di implementazione](#)

[Fase 2: Avvia lo stack](#)

[Fase 3: Avvia lo stack di account di destinazione nell'account AWS di destinazione](#)

[Fase 4: Creare il primo utente](#)

[Fase 5: \(Facoltativo\) Implementazione del contenuto statico della console Web privata](#)

[Fase 6: Aggiornare lo schema di fabbrica](#)

[Fase 7: Creazione di un server di automazione della migrazione](#)

[Fase 8: Testare la soluzione utilizzando gli script di automazione](#)

[Fase 9: \(Facoltativo\) Creazione di un dashboard per il monitoraggio della migrazione](#)

[Passaggio 10: \(Facoltativo\) Configurazione di provider di identità aggiuntivi in Amazon Cognito](#)

Important

Questa soluzione include un'opzione per inviare metriche operative anonime a AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS possiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'[AWS Informativa sulla privacy](#).

Per disattivare questa funzionalità, scarica il modello, modifica la sezione di AWS CloudFormation mappatura, quindi utilizza la AWS CloudFormation console per caricare il modello aggiornato e distribuire la soluzione. Per ulteriori informazioni, consulta la sezione [Raccolta di dati anonimi](#) di questa guida.

Fase 1: Scegli l'opzione di implementazione

Esistono tre opzioni per l'implementazione dello stack iniziale e la scelta di quella corretta dipende dalle politiche di sicurezza per l'ambiente di destinazione.

Queste opzioni sono:

- **Pubblico (impostazione predefinita):** tutti i Cloud Migration Factory sugli AWS endpoint sono indirizzabili pubblicamente con l'autenticazione dell'utente. Questa opzione implementa i seguenti punti di ingresso: CloudFront, Public API Gateway, Endpoints e Cognito.
- **Pubblico con AWS WAF:** L'accesso agli endpoint di Cloud Migration Factory è limitato agli intervalli CIDR personalizzabili. Questa opzione implementa i seguenti punti di ingresso: CloudFront, Public API Gateway Endpoints, Cognito e AWS WAF limita l'accesso a intervalli CIDR specifici.

- Privato: tutti gli endpoint Cloud Migration Factory sono accessibili solo dalle tue reti VPC e Cloud Migration Factory AWS sulla console web deve essere ospitato su un server web privato distribuito separatamente. Questa opzione implementa i seguenti punti di ingresso: [Endpoint API Gateway privati \(accessibili solo all'interno di un VPC\)](#) e Cognito.

Fase 2: Avvia lo stack

Important

Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS possiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta alla [politica sulla privacy di AWS](#).

Per disattivare questa funzionalità, scarica il modello, modifica la sezione di AWS CloudFormation mappatura, quindi usa la AWS CloudFormation console per caricare il modello e distribuire la soluzione. Per ulteriori informazioni, consulta la [Raccolta di dati anonimizzata](#) sezione di questa guida.

Questo AWS CloudFormation modello automatizzato implementa la soluzione Cloud Migration Factory on AWS nel AWS cloud.

Note

Sei responsabile del costo dei AWS servizi utilizzati durante l'esecuzione di questa soluzione. Per ulteriori dettagli, consulta la [Costo](#) sezione. Per tutti i dettagli, consulta la pagina web dei prezzi di ogni AWS servizio che utilizzerai in questa soluzione.

1. Accedi a AWS Management Console e seleziona il pulsante per avviare il `cloud-migration-factory-solution` AWS CloudFormation modello.

**Launch
solution**

Puoi anche [scaricare il modello](#) come punto di partenza per un'implementazione personalizzata.

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra AWS regione, utilizza il selettore della regione nella barra di navigazione della console.

Note

Questa soluzione utilizza Amazon Cognito e Amazon QuickSight, che al momento sono disponibili solo in AWS regioni specifiche. Pertanto, è necessario avviare questa soluzione in una AWS regione in cui questi servizi sono disponibili. Per la disponibilità più aggiornata per regione, consulta [l'elenco dei servizi AWS regionali](#).

Se distribuita in modalità Public e Public con tipi di distribuzione WAF, la soluzione utilizza anche la CloudFront registrazione di Amazon su Amazon S3. Oggi, la consegna dei log da Amazon CloudFront ad Amazon S3 è disponibile solo in regioni specifiche. Consulta [Scelta di un bucket Amazon S3 per i log standard per verificare che la tua regione sia supportata](#).

3. Nella pagina Create stack, verifica che l'URL del modello corretto sia visualizzato nella casella di testo URL Amazon S3 e scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni.
5. In Parametri, esaminate i parametri per il modello e modificateli se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
Application name (Nome applicazione)	migration-factory	Immettete un prefisso per l'ID AWS CloudFormation fisico che identifica i AWS servizi distribuiti da questa soluzione.

 Note

<application-name><environment-name><aws-resource>Il nome dell'applicazione

Parametro	Predefinito	Descrizione
		<p>viene utilizzato come prefisso per identificare le AWS risorse distribuite: - -. Se si modifica il nome predefinito, si consiglia di mantenere le etichette dei prefissi combinate a un massimo di 40 caratteri per assicurarsi di non superare i limiti di caratteri.</p>

Parametro	Predefinito	Descrizione
Nome dell'ambiente	test	<p>Immettere un nome per identificare l'ambiente di rete in cui viene distribuita la soluzione. È consigliabile utilizzare un nome descrittivo come testdev, o. prod</p> <div data-bbox="1089 541 1510 1570"><p> Note</p><p><application-name> <environment-name> <aws-resource>Il nome dell'ambiente viene utilizzato o come prefisso per identificare le AWS risorse distribuite: - -. Se si modifica il nome predefinito, si consiglia di mantenere le etichette dei prefissi combinate a un massimo di 40 caratteri per assicurarsi di non superare i limiti di caratteri.</p></div>

Parametro	Predefinito	Descrizione
Migration Tracker	<code>true</code>	Per impostazione predefinita, la dashboard opzionale di Migration Tracker è attivata, ma è possibile disattivarla modificando questo parametro in <code>false</code>
Ripiattaforma EC2	<code>true</code>	Per impostazione predefinita, la funzionalità Replatform EC2 è attivata, ma è possibile disattivarla modificando questo parametro in <code>false</code>
ServiceAccountEmail	<code>serviceaccount@yourdomain.com</code>	Indirizzo e-mail predefinito dell'account di servizio, gli script di Migration Factory Automation utilizzano questo account per connettersi all'API di fabbrica.
Consenti la configurazione di un provider di identità aggiuntivo in Cognito	<code>false</code>	Per impostazione predefinita, la soluzione utilizza Amazon Cognito per creare e gestire l'accesso. La modifica di questo parametro <code>true</code> configurerà la soluzione per consentire l'aggiunta di provider di identità SAML esterni ad Amazon Cognito e l'utilizzo per l'accesso.

Parametro	Predefinito	Descrizione
Tipo di distribuzione	Public	<p>Per impostazione predefinita, il tipo di implementazione è Pubblico e tutti gli endpoint di Cloud Migration Factory sono accessibili pubblicamente con l'autenticazione dell'utente.</p> <p>Pubblico con AWS WAF: L'accesso agli endpoint CMF è limitato agli intervalli CIDR personalizzabili.</p> <p>Privato: tutti gli endpoint di Cloud Migration Factory sono accessibili solo dalle reti VPC e l'interfaccia utente Web di Cloud Migration Factory deve essere ospitata su un server Web privato distribuito separatamente.</p>

(Facoltativo) Solo tipo di implementazione privata

Parametro	Predefinito	Descrizione
URL completo utilizzato per accedere all'interfaccia utente Web	[not set]	<p>Richiesto quando Deployment Type è impostato su Privato. Specificate l'URL dell'interfaccia web di Migration Factory che servirà il contenuto web statico. Esempio https://cmf.yourdomain.local.</p> <div data-bbox="1089 684 1510 1604" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><ul style="list-style-type: none">• Non aggiungete una barra finale all'URL, altrimenti l'interfaccia web fallirà durante il caricamento.• Nelle distribuzioni private è necessario un server Web per ospitare il contenuto statico e deve essere distribuito prima della distribuzione del modello. CloudFormation</div>

Parametro	Predefinito	Descrizione
ID VPC per ospitare gli endpoint API Gateway	[not set]	Richiesto quando Deployment Type è impostato su Privato. Specificare un singolo ID VPC in cui verranno creati gli endpoint API Gateway privati.
Sottoreti per ospitare gli endpoint dell'interfaccia API Gateway	[not set]	Richiesto quando Deployment Type è impostato su Privato. Specificare due ID di sottorete in cui verranno creati gli endpoint API Gateway privati. Gli ID di sottorete specificati devono trovarsi all'interno del VPC specificato sopra.
(Facoltativo) Pubblico solo con tipo di distribuzione AWS WAF		

Parametro	Predefinito	Descrizione
CIDR consentito	[not set]	<p>Richiesto quando Deployment Type è impostato su Pubblico con AWS WAF. Specifica te due intervalli CIDR da cui gli utenti e il server di automazione accederanno agli endpoint.</p> <div data-bbox="1089 638 1510 1318" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <ul style="list-style-type: none"> • È necessario specificare 2 intervalli CIDR. • Una volta implementato, è possibile aggiungere intervalli e restrizioni aggiuntivi alle AWS WAF regole, se necessario. </div>

6. Seleziona Successivo.
7. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
8. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona le caselle riconoscendo che il modello creerà risorse [AWS Identity and Access Management](#)(IAM) e che potrebbe richiedere la funzionalità CAPABILITY_AUTO_EXPAND.
9. Scegli Invia per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere lo stato CREATE_COMPLETE in circa 20 minuti.

⚠ Important

Se si utilizza AWS MGN, è necessario completare i prerequisiti per AWS MGN prima di continuare con la Fase 3.

Passaggio 3: Avvia lo stack di account di destinazione nell'account di destinazione AWS

Questo AWS CloudFormation modello automatizzato distribuisce i ruoli IAM nell' AWS account di destinazione per consentire all'account di fabbrica di assumere ruoli ed eseguire azioni MGN nell'account di destinazione. Ripeti questo passaggio per ogni account di destinazione. Se lo stack di fabbrica del passaggio precedente è un account di destinazione, sarà necessario che questo stack di destinazione venga distribuito su di esso.

📘 Note

L'account di destinazione deve essere inizializzato per AWS Application Migration Service prima di avviare questo stack. Per maggiori dettagli, consulta [Initializing Application Migration Service nella Application Migration Service User Guide](#).

Lo stack di account di destinazione deve essere avviato nella stessa regione dello stack di fabbrica nel passaggio precedente, indipendentemente dalla regione che verrà utilizzata come regione di destinazione della migrazione. Questo stack è destinato solo alle autorizzazioni per più account.

1. Accedi alla [console AWS CloudFormation](#). Scegli Crea stack, quindi seleziona Con nuove risorse, per avviare la distribuzione del modello. Puoi anche [scaricare il modello](#) come punto di partenza per un'implementazione personalizzata.
2. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni.
3. In Parametri, esamina i parametri per il modello e modificateli se necessario. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
Fabbrica AWSAccountId	111122223333	Inserisci un ID account in cui è stato distribuito Migration Factory. <div data-bbox="1089 422 1510 737" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Avvia questo stack nella stessa regione AWS dello stack Migration Factory.</p> </div>
Conversione piattaforma	Yes	Attiva questa opzione se prevedi di utilizzare il modulo Replatform EC2 di questa soluzione
RehostMGN	Yes	Attiva questa opzione se prevedi di utilizzare il modulo Rehost MGN di questa soluzione

4. Seleziona Successivo.
5. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
6. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà risorse [AWS Identity and Access Management\(IAM\)](#).
7. Scegli Invia per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere lo stato CREATE_COMPLETE in circa 5 minuti.

Fase 4: Creare il primo utente

Crea l'utente iniziale e accedi alla soluzione

Utilizzare la procedura seguente per creare l'utente iniziale.

1. Passa alla [console di Amazon Cognito](#).
2. Dal riquadro di navigazione, scegli Pool di utenti.
3. Nella pagina Pool di utenti, scegli il pool di utenti che inizia con il migration-factory prefisso.
4. Seleziona la scheda Utenti e scegli Crea utente.
5. Nella schermata Crea utente, sezione Informazioni utente, procedi come segue:
 1. Verifica che l'opzione Invia un invito sia selezionata.
 2. Immetti un indirizzo e-mail

Important

Questo indirizzo e-mail deve essere diverso da quello utilizzato nel ServiceAccountEmail parametro, utilizzato dalla soluzione per la distribuzione del CloudFormation modello principale.

3. Seleziona Imposta una password.
4. Nel campo Password, inserisci una password.

Note

La password deve contenere almeno otto caratteri, tra cui lettere maiuscole e minuscole, numeri e caratteri speciali.

6. Selezionare Create user (Crea utente).

Note

Riceverai un'email con la password temporanea. Finché non modifichi la password temporanea, lo stato dell'account per questo utente verrà visualizzato come Modifica

forzata della password. È possibile aggiornare la password in un secondo momento della distribuzione.

Aggiungi un utente al gruppo di amministratori

Nella console Amazon Cognito, utilizza la seguente procedura per aggiungere un utente al gruppo di amministratori predefinito.

1. Passa alla console di Amazon Cognito.
2. Dal menu di navigazione, scegli Pool di utenti.
3. Nella pagina Pool di utenti, scegli il pool di utenti che inizia con il `migration-factory` prefisso.
4. Seleziona la scheda Gruppi e apri il gruppo denominato `admin` selezionando il nome.
5. Scegli Aggiungi utente al gruppo, quindi seleziona il nome utente da aggiungere.
6. Scegli Aggiungi.

L'utente scelto verrà ora aggiunto all'elenco dei membri del gruppo. Questo gruppo di amministratori predefinito autorizza l'utente a gestire tutti gli aspetti della soluzione.

Note

Dopo aver creato gli utenti iniziali, puoi gestire l'appartenenza ai gruppi nell'interfaccia utente della soluzione selezionando Amministrazione, quindi Autorizzazioni, quindi Gruppi.

Identifica l' CloudFront URL (pubblico e pubblico solo con AWS WAF distribuzioni)

Utilizza la seguente procedura per identificare l' CloudFront URL Amazon della soluzione. Ciò consente di accedere e modificare la password.

1. Vai alla [AWS CloudFormation console](#) e seleziona lo stack della soluzione.
2. Nella pagina Stacks, seleziona la scheda Output e seleziona il valore per l'URL. MigrationFactory

Note

Se hai avviato la soluzione in una AWS regione diversa dagli Stati Uniti orientali (Virginia settentrionale), l'implementazione CloudFront potrebbe richiedere più tempo e l'`MigrationFactoryURL` potrebbe non essere accessibile immediatamente (riceverai un errore di accesso negato). Possono essere necessarie fino a quattro ore prima che l'URL diventi disponibile. L'URL include `cloudfront.net` come parte della stringa.

3. Accedi con il tuo nome utente e la password temporanea, quindi crea una nuova password e scegli **Cambia password**.

Note

La password deve contenere almeno otto caratteri, incluse lettere maiuscole e minuscole, numeri e caratteri speciali.

Passaggio 5: (Facoltativo) Implementazione del contenuto statico della console Web privata

Se hai selezionato il tipo di distribuzione privata durante la distribuzione dello stack, devi distribuire manualmente il codice della console web CMF sul server Web che hai creato e quindi specificato nell'URL completo utilizzato per accedere al parametro dell'interfaccia utente Web dello stack. Per tutti gli altri tipi di distribuzione, saltate questo passaggio.

Le istruzioni di installazione e configurazione per ogni server Web sono diverse, pertanto questa guida fornirà solo istruzioni generiche su dove copiare il contenuto e, prima di aggiornare il contenuto, è consigliabile configurare il server Web in base alle proprie esigenze.

1. Assicurati che il server Web abbia accesso a S3 e che la CLI AWS sia installata e configurata. In alternativa, scarica il contenuto del bucket front-end e copialo sul server Web utilizzando un altro dispositivo.
2. Utilizzando l'AWS CLI, esegui il seguente comando, sostituendo il nome dell'ambiente con quello specificato durante la distribuzione dello stack, l'ID dell'account AWS con l'ID dell'account AWS in cui è stato distribuito lo stack e la directory di destinazione con quella della directory principale predefinita del server Web. Questo copierà il codice statico della console web di Cloud Migration

Factory insieme alla configurazione specifica necessaria per l'implementazione di questa soluzione Cloud Migration Factory:

Esempio di Windows:

```
aws s3 cp --recursive s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ C:\inetpub\wwwroot --recursive
```

Esempio di Linux:

```
aws s3 cp s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ /var/www/html --recursive
```

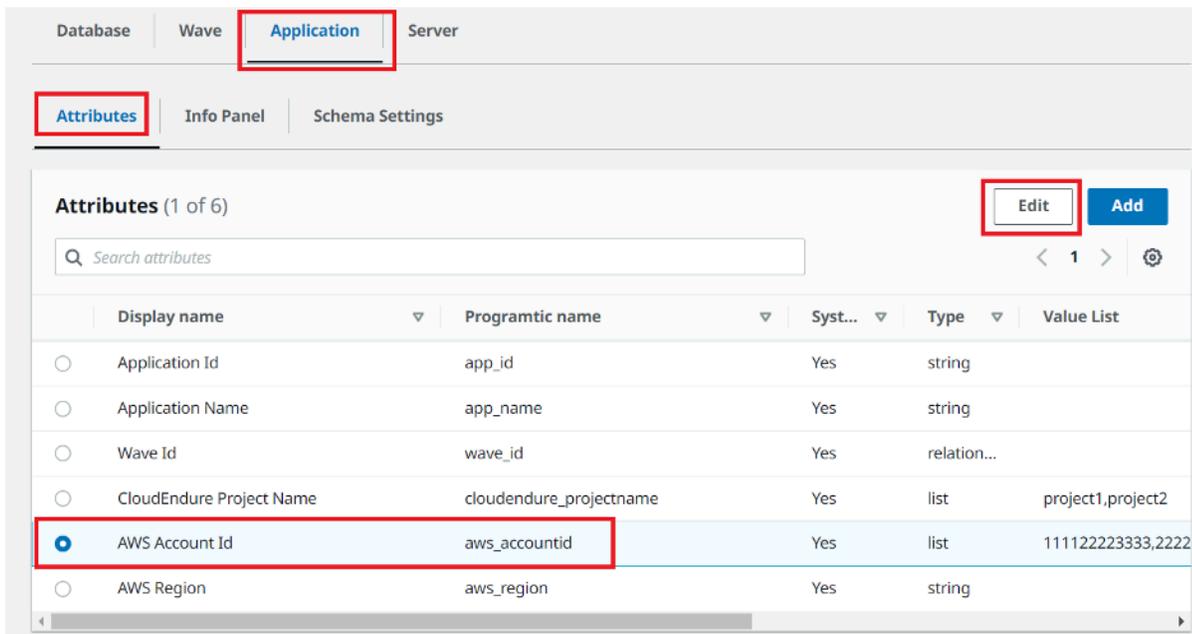
Note

Se viene effettuato un aggiornamento dei parametri dello stack, è necessario sostituire i file sul server Web dal bucket front-end per garantire che eventuali modifiche alla configurazione siano disponibili per la console Web.

Fase 6: Aggiornare lo schema di fabbrica

Aggiorna l'ID dell'account AWS di destinazione per le migrazioni AWS MGN

1. Nell'interfaccia web di Migration Factory, seleziona Amministrazione, quindi seleziona Attributi.
2. Nella pagina Configurazione degli attributi, selezionare Applicazione, quindi selezionare Attributi.
3. Seleziona ID account AWS, quindi scegli Modifica.



- Nella pagina Modifica attributo, aggiorna la lista valori con gli ID dell'account AWS di destinazione e scegli Salva.

Note

Se disponi di più di un ID AWS account, separalo con una virgola.

Fase 7: Configurazione di un server di automazione della migrazione

Il server di automazione della migrazione viene utilizzato per eseguire l'automazione della migrazione.

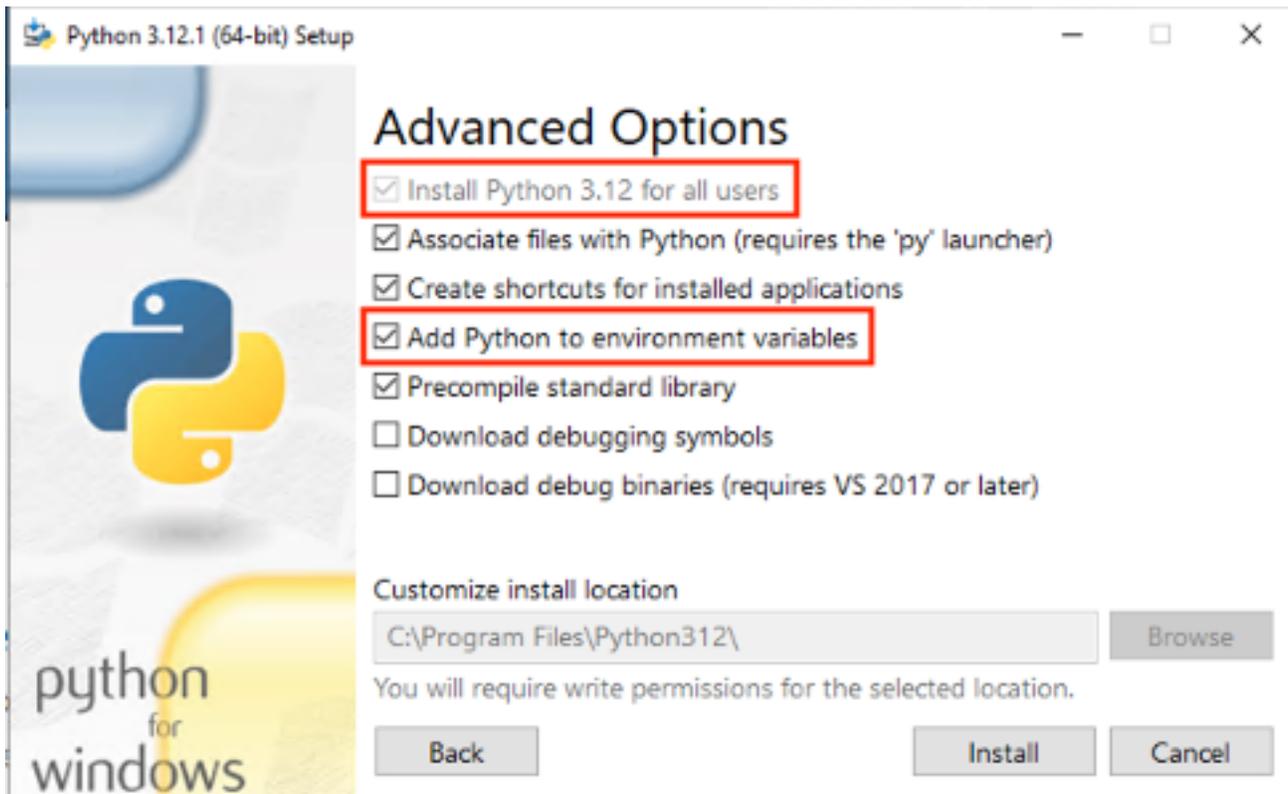
Crea un server Windows Server 2016 o versione successiva

Ti consigliamo di creare il server nel tuo account AWS, ma può anche essere creato nel tuo ambiente locale. Se creato in un account AWS, deve trovarsi nello stesso account AWS e nella stessa regione di Cloud Migration Factory. Per esaminare i requisiti del server, consulta [Migration automation server](#).

Ovunque venga distribuita l'istanza di Windows, questa deve essere distribuita come installazione standard di Windows 2016 o versione successiva che soddisfi i requisiti operativi e di sicurezza.

Installazione del software necessario per supportare le automazioni

1. Scarica [Python](#) v3.12.1.
2. Accedi come amministratore e installa Python v3.12.1, quindi scegli Personalizza installazione.
3. Scegli Avanti e seleziona Installa per tutti gli utenti e Aggiungi Python alle variabili di ambiente. Scegli Installa.



4. Verifica di avere i privilegi di amministratore e `cmd . exe`, apri ed esegui i seguenti comandi per installare i pacchetti Python uno alla volta:

```
python -m pip install requests
python -m pip install paramiko
python -m pip install boto3
```

Se uno di questi comandi fallisce, aggiorna pip eseguendo il seguente comando:

```
python -m pip install --upgrade pip
```

5. Installa [AWS CLI \(interfaccia a riga di comando\)](#).

6. Installa utilizzando il [modulo PowerShell for AWS](#), assicurandoti di avere il AllUsers parametro - Scope incluso nel comando.

```
Install-Module -Name AWSPowerShell -Scope AllUsers
```

7. Apri PowerShell Script Execution, aprendo la PowerShell CLI come amministratore ed esegui il seguente comando:

```
Set-ExecutionPolicy RemoteSigned
```

Configura AWS le autorizzazioni per il server di automazione della migrazione e installa AWS Systems Manager Agent (SSM Agent)

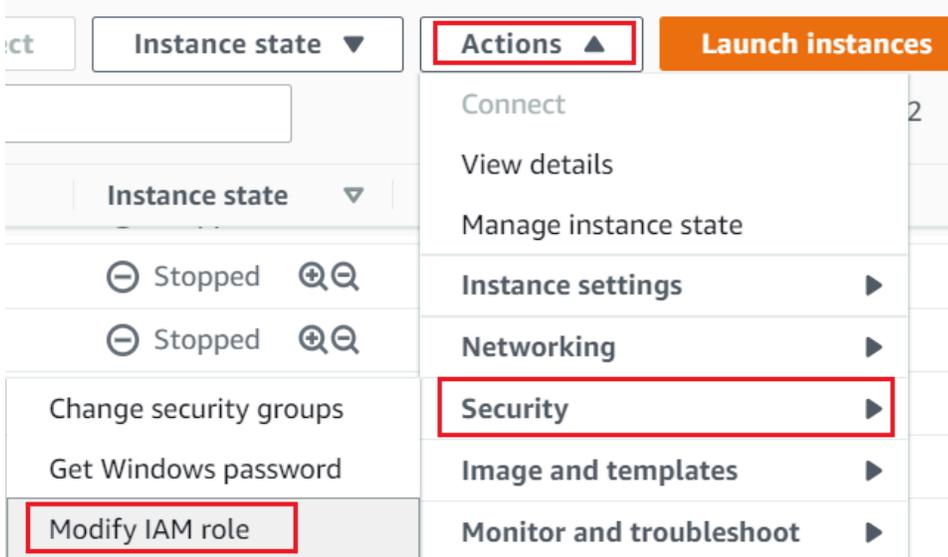
A seconda di dove distribuisce il server di esecuzione della migrazione, scegli una delle opzioni seguenti per configurare le AWS autorizzazioni per il server di automazione della migrazione. Il ruolo o la policy IAM fornisce l'autorizzazione al server di automazione e l'accesso a AWS Secrets Manager per ottenere le chiavi di installazione dell'agente e le credenziali dell'account del servizio di fabbrica. Puoi implementare il server di automazione della migrazione AWS come istanza EC2 o in locale.

Opzione 1: utilizza la seguente procedura per configurare le autorizzazioni per il server di automazione della migrazione in Amazon EC2 e nello stesso account e regione AWS della fabbrica.

1. Passa alla [AWS CloudFormation console](#) e seleziona lo stack della soluzione.
2. Seleziona la scheda Output, nella colonna Chiave, individua AutomationServerIAMRole e registra il valore da utilizzare successivamente nella distribuzione.

Outputs (10)		
<input type="text" value="Search outputs"/>		
Key ▲	Value ▼	Description
AutomationServerIAMPolicy	migration-factory-test-AutomationInstancePolicy	IAM Policy for Migration Automation Server
AutomationServerIAMRole	migration-factory-test-automation-server	IAM Role for Migration Automation Server

3. Passa alla console [Amazon Elastic Compute Cloud](#).
4. Dal riquadro di navigazione a sinistra, seleziona Istanze.
5. Nella pagina Istanze, utilizza il campo Filtra istanze e inserisci il nome del server di esecuzione della migrazione per trovare l'istanza.
6. Seleziona l'istanza e seleziona Azioni dal menu.
7. Seleziona Sicurezza dall'elenco a discesa, quindi seleziona Modifica ruolo IAM.

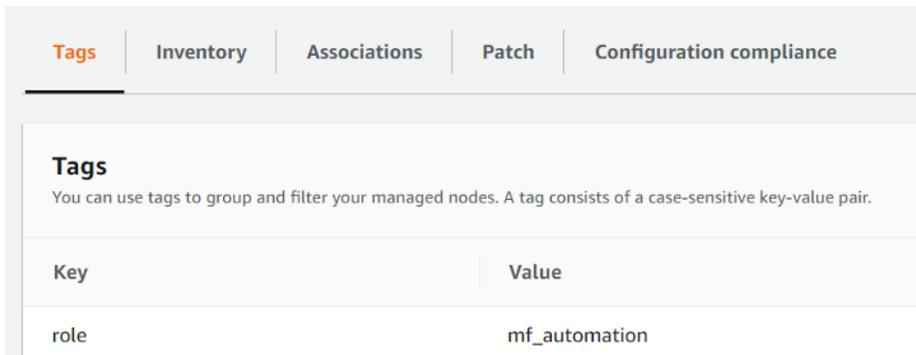


8. Dall'elenco dei ruoli IAM, individua e seleziona il ruolo IAM contenente il valore per `AutomationServerIAMRole` cui hai registrato nel passaggio 2 e scegli Salva.
9. Usa il tuo protocollo RDP (Remote Desktop Protocol) per accedere al server di automazione della migrazione.
10. Scarica e installa [SSM Agent](#) sul server di automazione della migrazione.

Note

Per impostazione predefinita, l'agente AWS Systems Manager è preinstallato su Amazon Machine Images di Windows Server 2016. Esegui questo passaggio solo se l'agente SSM non è installato.

11. Aggiungi il seguente tag all'istanza EC2 del server di automazione della migrazione: Key = `role` e Value = `mf_automation`

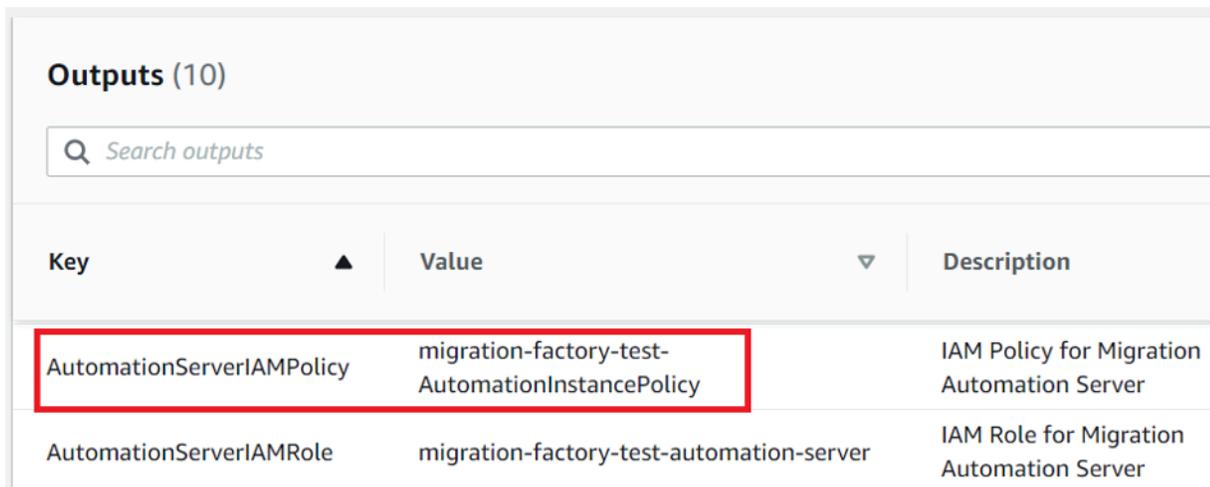


Key	Value
role	mf_automation

12. Apri la console AWS Systems Manager e scegli Fleet Manager. Controlla lo stato del server di automazione e assicurati che lo stato del ping dell'agente SSM sia online.

Opzione 2: utilizzare la seguente procedura per configurare le autorizzazioni per il server di automazione della migrazione in locale.

1. Vai alla [AWS CloudFormation console](#) e seleziona lo stack della soluzione.
2. Seleziona la scheda Output, nella colonna Chiave, individua `AutomationServerIAMPolicy` e registra il valore da utilizzare successivamente nella distribuzione.



Key	Value	Description
AutomationServerIAMPolicy	migration-factory-test-AutomationInstancePolicy	IAM Policy for Migration Automation Server
AutomationServerIAMRole	migration-factory-test-automation-server	IAM Role for Migration Automation Server

3. Accedere alla console [Identity and Access Management](#).
4. Dal riquadro di navigazione a sinistra, seleziona Utenti, quindi scegli Aggiungi utenti.
5. Nel campo Nome utente, crea un nuovo utente.
6. Seleziona Successivo.
7. Nella pagina Imposta autorizzazioni, in Opzioni di autorizzazione, seleziona Allega direttamente le politiche. Viene visualizzato un elenco di politiche.
8. Dall'elenco dei criteri, individua e seleziona il criterio AutomationServerIAMPolicy contenente il valore registrato nel [passaggio 2](#).
9. Scegli Avanti, quindi verifica che sia selezionata la politica corretta.
10. Selezionare Create user (Crea utente).
11. Dopo essere stato reindirizzato alla pagina Utenti, scegli l'utente creato nel passaggio precedente, quindi scegli la scheda Credenziali di sicurezza.
12. Nella sezione Chiavi di accesso, scegliere Crea chiave di accesso.

Note

Le chiavi di accesso sono composte da un ID chiave di accesso e una chiave di accesso segreta che sono utilizzati per firmare le richieste programmatiche eseguite verso AWS. In mancanza di chiavi di accesso, puoi crearle utilizzando la Console di gestione AWS. Come best practice, non utilizzare le chiavi di accesso dell'utente root per nessuna attività in cui non sia necessario. Invece, [crea un nuovo utente IAM amministratore](#) con le chiavi di accesso riservate a te.

L'unica volta che è possibile visualizzare o scaricare la chiave di accesso segreta è durante la creazione delle chiavi. Non è possibile recuperarle successivamente. Tuttavia,

è possibile creare nuove chiavi di accesso in qualsiasi momento. Occorre avere le autorizzazioni anche per effettuare le operazioni IAM richieste. Per ulteriori informazioni, consulta [Autorizzazioni necessarie per accedere alle risorse IAM](#) nella Guida per l'utente IAM.

- Per visualizzare la nuova chiave di accesso, seleziona Mostra. Non sarà possibile accedere nuovamente alla chiave di accesso segreta dopo la chiusura di questa finestra di dialogo. Le credenziali saranno simili a quanto segue:
 - Access key ID: AKIAIOSFODNN7EXAMPLE
 - Secret access key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
- Per fare il download della coppia di chiavi, scegliere Download .csv file. Conserva le chiavi in un posto sicuro. Non sarà possibile accedere nuovamente alla chiave di accesso segreta dopo la chiusura di questa finestra di dialogo.

 Important

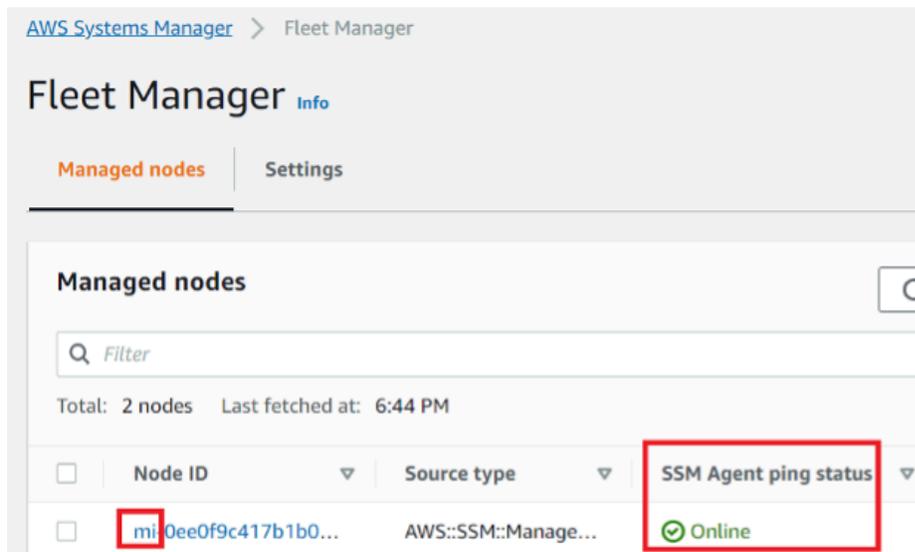
Mantieni riservate le chiavi per proteggere il tuo account AWS e non inviarle mai via e-mail. Non condividerli all'esterno della tua organizzazione, anche se sembra che una richiesta provenga da AWS o Amazon.com. Nessuno che rappresenta legittimamente Amazon richiederà mai la tua chiave segreta.

- Dopo aver scaricato il file .csv, seleziona Chiudi. Quando si crea una chiave di accesso, la coppia di chiavi è attiva di default e può essere utilizzata immediatamente.
- Usa il tuo protocollo RDP (Remote Desktop Protocol) per accedere al server di esecuzione della migrazione.
- Effettuato l'accesso come amministratore, apri il prompt dei comandi (CMD).exe.
- Esegui il comando seguente per configurare le AWS credenziali sul server. Sostituisci <your_access_key_id><your_secret_access_key>e <your_region>con i tuoi valori:

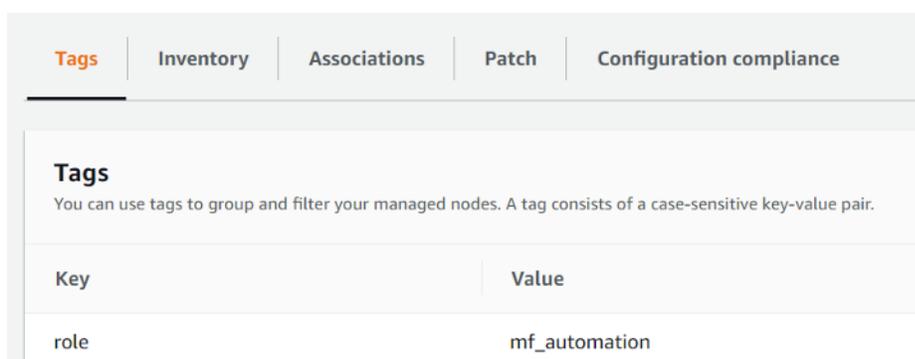
```
SETX /m AWS_ACCESS_KEY_ID <your_access_key_id>
SETX /m AWS_SECRET_ACCESS_KEY <your_secret_access_key>
SETX /m AWS_DEFAULT_REGION <your_region>
```

- Riavviare il server di automazione.
- Installa l'agente AWS Systems Manager utilizzando la modalità ibrida (server on-premise).

- a. Crea un'attivazione ibrida; consulta [Creare un'attivazione \(console\)](#) nella Guida per l'utente di AWS Systems Manager. Durante questo processo, quando ti viene chiesto di fornire un ruolo IAM, seleziona un ruolo IAM esistente e scegli il ruolo con il suffisso -automation-server che è stato creato automaticamente quando è stato distribuito lo stack Cloud Migration Factory.
- b. Accedi al server di automazione della migrazione come amministratore.
- c. Installa AWS Systems Manager Agent (SSM Agent); consulta [Installa l'agente SSM per un ambiente ibrido e multicloud](#) nella Guida per l'utente di AWS Systems Manager. Utilizza l'attivazione ibrida creata nella fase 20.a.
- d. Una volta installato correttamente l'agente, nella console AWS Systems Manager, scegli Fleet Manager. Identifica l'ID del nodo con il prefisso mi- con stato online.



- e. Seleziona l'ID del nodo e assicurati che il ruolo IAM sia quello selezionato con il suffisso automation-server.
- f. Aggiungi il seguente tag per questo nodo ibrido: Key = **role** e Value = **mf_automation**. Tutto in minuscolo.



Fase 8: testare la soluzione utilizzando gli script di automazione

Importa i metadati di migrazione in fabbrica

Per avviare il processo di migrazione, scaricate il [server-list.csv](#) file dal GitHub repository. Il `server-list.csv` file è un esempio di modulo di richiesta di migrazione al servizio AWS MGN per importare gli attributi per i server di origine pertinenti.

Note

Il file.csv e gli script di automazione di esempio facevano parte del pacchetto dello stesso repository. GitHub

È possibile personalizzare il modulo per la migrazione sostituendo i dati di esempio con i dati specifici del server e dell'applicazione. La tabella seguente descrive in dettaglio i dati da sostituire per personalizzare questa soluzione in base alle esigenze di migrazione.

Nome del campo	Obbligatorio?	Descrizione
wave_name	Sì	Il nome del wave si basa sulle dipendenze della priorità e del server delle applicazioni. Ottieni questo identificatore dal tuo piano di migrazione.
Nome_App	Sì	I nomi delle applicazioni che rientrano nell'ambito della migrazione. Verificate che il raggruppamento di applicazioni includa tutte le applicazioni che condividono gli stessi server.
aws_accountid	Sì	Un identificatore a 12 cifre che si trova nel profilo del tuo account. Account AWS Per accedere, seleziona il profilo

Nome del campo	Obbligatorio?	Descrizione
		del tuo account nell'angolo in alto a destra di AWS Management Console e seleziona Il mio account dal menu a discesa.
aws_region	Sì	Regione AWS codice. Ad esempio, us-east-1 . Consulta l' elenco completo dei codici regionali .
nome_server	Sì	Il nome dei server locali che rientrano nell'ambito della migrazione.
server_os_family	Sì	Il sistema operativo (OS) in esecuzione sui server di origine inclusi nell'ambito. Usa Windows o Linux poiché questa soluzione supporta solo questi sistemi operativi.

Nome del campo	Obbligatorio?	Descrizione
server_os_version	Sì	<p>La versione del sistema operativo in esecuzione sui server di origine inclusi nell'ambito.</p> <div data-bbox="1068 445 1507 999"><p> Note</p><p>Utilizza la versione del sistema operativo, non la versione del kernel, ad esempio usa RHEL 7.1, Window Server 2012 R2 o CentOS 7.5, 7.6. Non utilizzare Linux 3.xx, 4.xx o Windows 8.1.x.</p></div>
server_fqdn	Sì	<p>Il nome di dominio completo del server di origine, che è il nome del server seguito dal nome di dominio. Ad esempio, server123.company.com.</p>
server_tier	Sì	<p>Un'etichetta per identificare se il server di origine è un server Web, un'app o un database. Ti consigliamo di designare il server di origine come app se il server funziona come più di un livello, ad esempio se il server esegue insieme i livelli web, app e database.</p>

Nome del campo	Obbligatorio?	Descrizione
ambiente_server	Sì	Un'etichetta per identificare l'ambiente del server. Ad esempio, dev, test, prod, QA o pre-prod.
r_type	Sì	Un'etichetta per identificare la strategia di migrazione. Ad esempio, Retire, Retain, Relocate, Rehost, Repurchase, Replatform, Rearchitect, TBC.
ID_subnet	Sì	L'ID di sottorete per l'istanza Amazon EC2 di destinazione per la migrazione dopo il cutover.
SecurityGroup_IDS	Sì	L'ID del gruppo di sicurezza per l'istanza Amazon EC2 di destinazione per la migrazione dopo il cutover.
Subnet_IDS_Test	Sì	L'ID della sottorete di destinazione per il server di origine che verrà testato.
SecurityGroup_IDS_Test	Sì	L'ID del gruppo di sicurezza di destinazione per il server di origine che verrà testato.
instanceType	Sì	Il tipo di istanza Amazon EC2 identificato durante il processo di individuazione e pianificazione. Per informazioni sui tipi di istanze EC2, consulta i tipi di istanza di Amazon EC2 .

Nome del campo	Obbligatorio?	Descrizione
tenancy	Sì	Il tipo di locazione, che viene identificato durante le attività di scoperta e pianificazione. Utilizza uno dei seguenti valori per identificare la locazione: Shared, Dedicated o Dedicated Host. È possibile utilizzare Shared come valore predefinito, a meno che la licenza di un'applicazione non richieda un tipo specificato.
Tag	No	I tag per le risorse del server, ad esempio CostCenter =123; BU=IT; location=US
private_ip	No	L'IP privato per l'istanza di destinazione. Se non è incluso, l'istanza riceverà un IP da DHCP.
IAMRole	No	Ruolo IAM per l'istanza di destinazione. Se non incluso, nessun ruolo IAM verrà associato all'istanza di destinazione.

1. Accedi alla console web di Cloud Migration Factory.
2. In Gestione della migrazione, seleziona Importa e scegli Seleziona file. Seleziona il modulo di ammissione che hai completato in precedenza e scegli Avanti.
3. Controlla le modifiche e assicurati di non visualizzare errori (il messaggio informativo è normale), quindi scegli Avanti.
4. Scegli Carica per caricare i server.

Accedi ai domini

Gli script di automazione di esempio inclusi in questa soluzione si connettono ai server di origine interessati per automatizzare le attività di migrazione, come l'installazione dell'agente di replica e la chiusura dei server di origine. Per eseguire un test della soluzione, è necessario un utente di dominio con autorizzazioni di amministratore locale per i server di origine, per i server Windows e Linux (autorizzazioni sudo). Se Linux non è incluso nel dominio, è possibile utilizzare altri utenti come un utente LDAP con autorizzazioni sudo o un utente sudo locale. Per ulteriori informazioni sulle attività di migrazione automatizzata, consulta [Attività di migrazione automatizzata](#) utilizzando la console web Migration Factory e [Attività di migrazione automatizzata](#) tramite il prompt dei comandi.

Esegui un test dell'automazione della migrazione

Questa soluzione consente di eseguire un test dell'automazione della migrazione. Utilizzando gli script di automazione, il processo di migrazione importa i dati dal file CSV di migrazione nella soluzione. Vengono eseguiti controlli dei prerequisiti per i server di origine, l'agente di replica viene inviato ai server di origine, lo stato della replica viene verificato e il server di destinazione viene avviato dall'interfaccia web di Migration Factory. Per step-by-step istruzioni sull'esecuzione di un test, fare riferimento a [Attività di migrazione automatizzate](#) utilizzando la console web Migration Factory e [Attività di migrazione automatizzate](#) tramite il prompt dei comandi.

Fase 9: (Facoltativo) Creazione di un dashboard per il monitoraggio della migrazione

Se hai distribuito il componente opzionale di monitoraggio della migrazione, puoi configurare una QuickSight dashboard che visualizzerà i metadati di migrazione archiviati nella tabella Amazon DynamoDB.

Utilizza le seguenti procedure per:

1. [Impostare le QuickSight autorizzazioni e le connessioni](#)
2. [Crea una dashboard](#)

Note

Se la Migration Factory è vuota e non sono presenti dati relativi a wave, applicazioni e server, non ci saranno dati per creare una QuickSight dashboard.

Imposta l' QuickSight autorizzazione e le connessioni

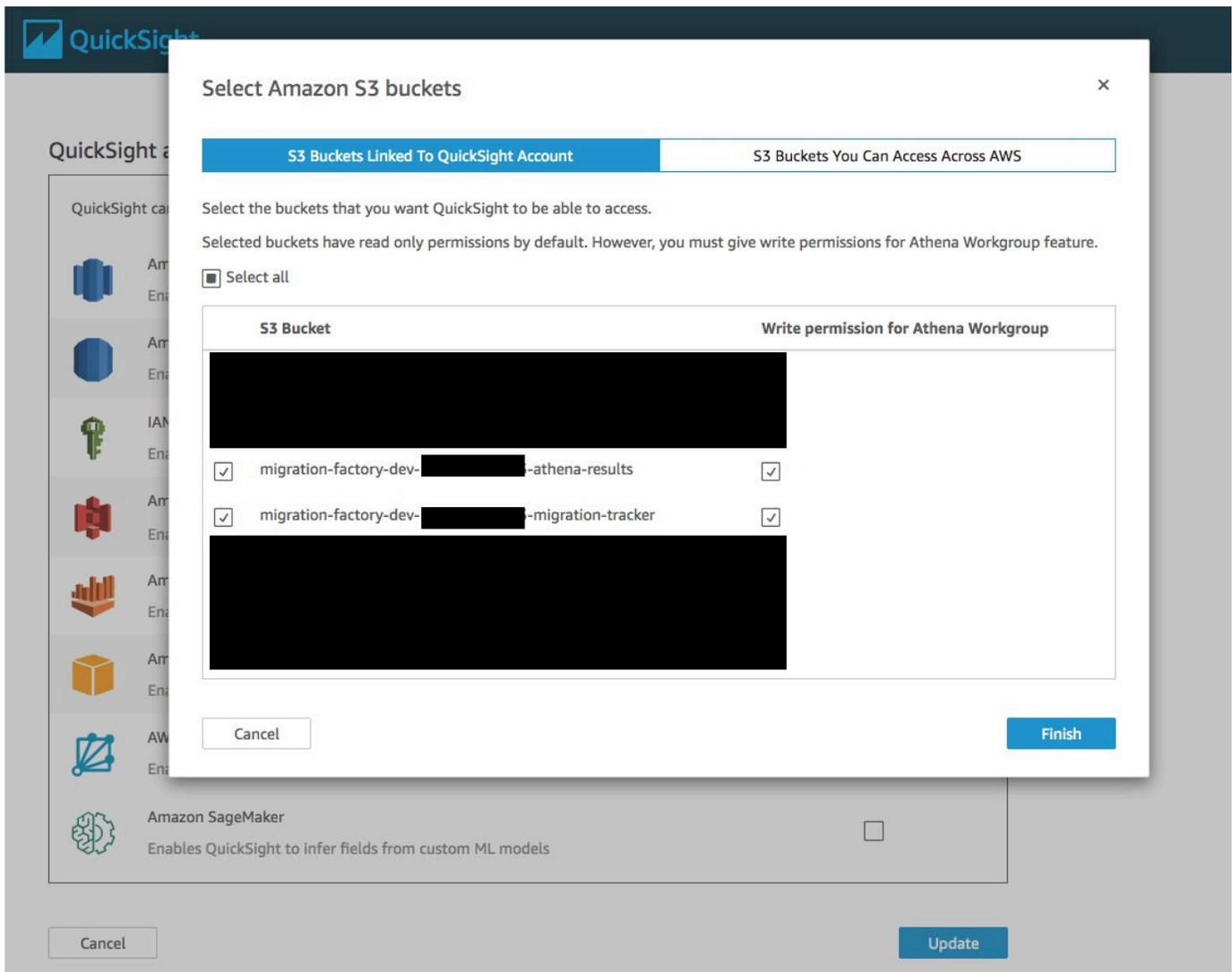
Se non hai configurato Amazon QuickSight nel tuo account AWS, consulta [Setting Up for Amazon QuickSight](#) nella Amazon QuickSight User Guide. Dopo aver configurato un QuickSight abbonamento, utilizza la seguente procedura per impostare le autorizzazioni e le connessioni tra QuickSight questa soluzione.

Note

Questa soluzione utilizza la licenza Amazon QuickSight Enterprise. Tuttavia, se non desideri che i report via e-mail, gli approfondimenti e l'aggiornamento orario dei dati vengano aggiornati, puoi optare per una licenza standard, che può essere utilizzata anche con Migration Tracker.

Innanzitutto, connettiti QuickSight con il bucket Amazon S3:

1. Passare alla [console QuickSight](#).
2. Nella QuickSight pagina, scegli l'icona che mostra una persona nell'angolo in alto a destra e scegli Gestisci. QuickSight
3. Nella pagina Nome account, dal riquadro del menu a sinistra, seleziona Sicurezza e autorizzazioni.
4. Nella pagina Sicurezza e autorizzazioni, nella sezione QuickSight Accesso ai servizi AWS, seleziona Gestisci.
5. Dalla pagina di QuickSight accesso ai servizi AWS, seleziona la casella di controllo per Amazon S3.
6. Nella finestra di dialogo Seleziona i bucket Amazon S3, verifica di essere nella scheda S3 Bucket collegati all' QuickSight account e seleziona le caselle di controllo destra e sinistra per i bucket S3 athena-results e migration-tracker.

**Note**

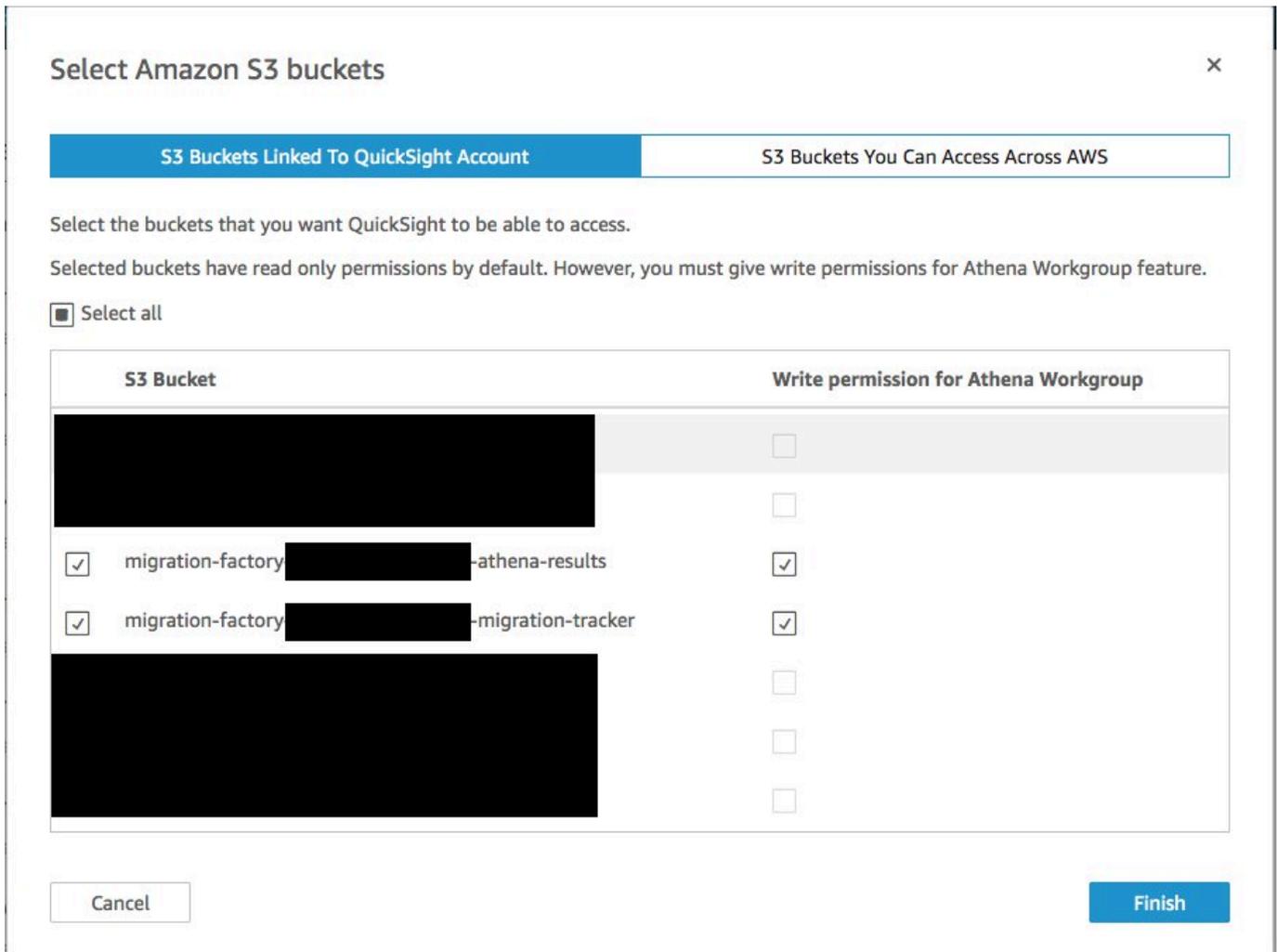
Se lo stai già utilizzando QuickSight per altre analisi dei dati S3, deseleziona e rizeleziona l'opzione Amazon S3 per visualizzare la finestra di dialogo di selezione del bucket.

7. Scegli Fine.

Successivamente, configura le autorizzazioni per Amazon Athena:

1. Nella pagina di QuickSight accesso ai servizi AWS, seleziona la casella di controllo per Amazon Athena.
2. Nella finestra di dialogo delle autorizzazioni di Amazon Athena, scegli Avanti.

3. Nella finestra di dialogo delle risorse di Amazon Athena, verifica di essere nella scheda S3 Bucket collegati all' QuickSightaccount e verifica che siano selezionati gli stessi bucket S3: athena-results e migration-tracker.



4. Scegli Fine.
5. Dalla pagina di QuickSight accesso ai servizi AWS, scegli Salva.

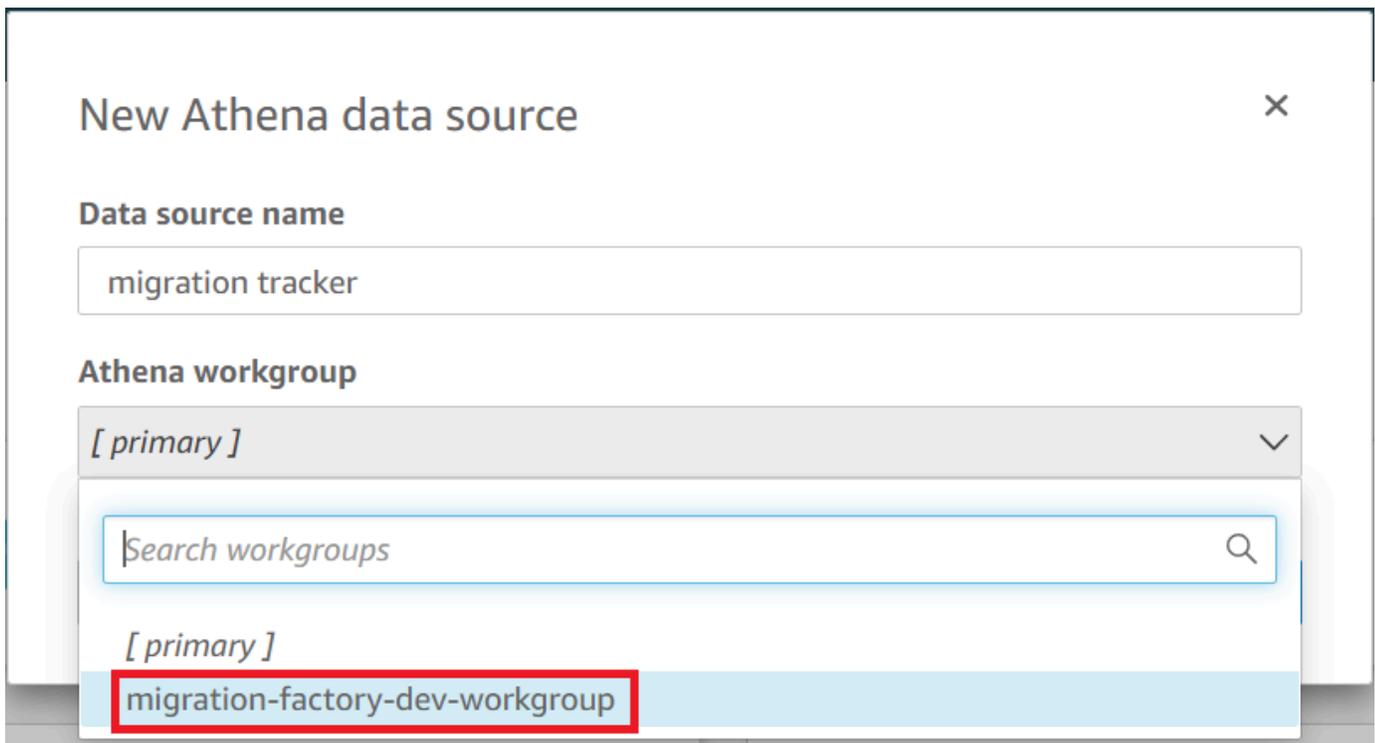
Quindi, configura una nuova analisi:

1. Seleziona il QuickSight logo per tornare alla QuickSight home page.
2. Nella pagina Analisi, scegli Nuova analisi.
3. Scegli Nuovo set di dati.
4. Nella pagina Crea un set di dati, scegli Athena.
5. Nella finestra di dialogo Nuova origine dati Athena, effettuate le seguenti azioni:

- a. Nel campo Nome origine dati, inserisci un nome per l'origine dati
- b. <migration-factory>Nel campo Athena workgroup, selezionare il -workgroup appropriato.

Note

Se hai distribuito questa soluzione più volte, ci sarà più di un gruppo di lavoro. Seleziona quello che è stato creato per la distribuzione corrente.



6. Scegli Convalida connessione per assicurarti che QuickSight possa comunicare con Athena.
7. Dopo la convalida della connessione, scegli Crea origine dati.
8. Nella finestra di dialogo successiva, Scegli la tua tabella, esegui le seguenti azioni:
 - a. Dall'elenco del catalogo, scegli AwsDataCatalog.
 - b. Dall'elenco Database, scegli <Athena-table>-tracker.
 - c. <tracker-name>Dall'elenco Tabelle, scegli -general-view.
 - d. Scegli Seleziona.

Choose your table ×

migration tracker

Catalog: contain sets of databases.

AwsDataCatalog ▾

Database: contain sets of tables.

migration-factory-dev-tracker ▾

Tables: contain the data you can visualize.

migration_factory_dev_apps

migration_factory_dev_servers

migration_factory_dev_tracker_general_view

[Edit/Preview data](#) [Use custom SQL](#) [Select](#)

9. Nella finestra di dialogo successiva, Termina la creazione del set di dati, scegli Visualizza.

Finish data set creation ✕

Table: migration_factory_dev_tracker_general_view
Data source: migration tracker
Schema: migration-factory-dev-tracker

Import to SPICE for quicker analytics ✓ 1GB available SPICE

Directly query your data

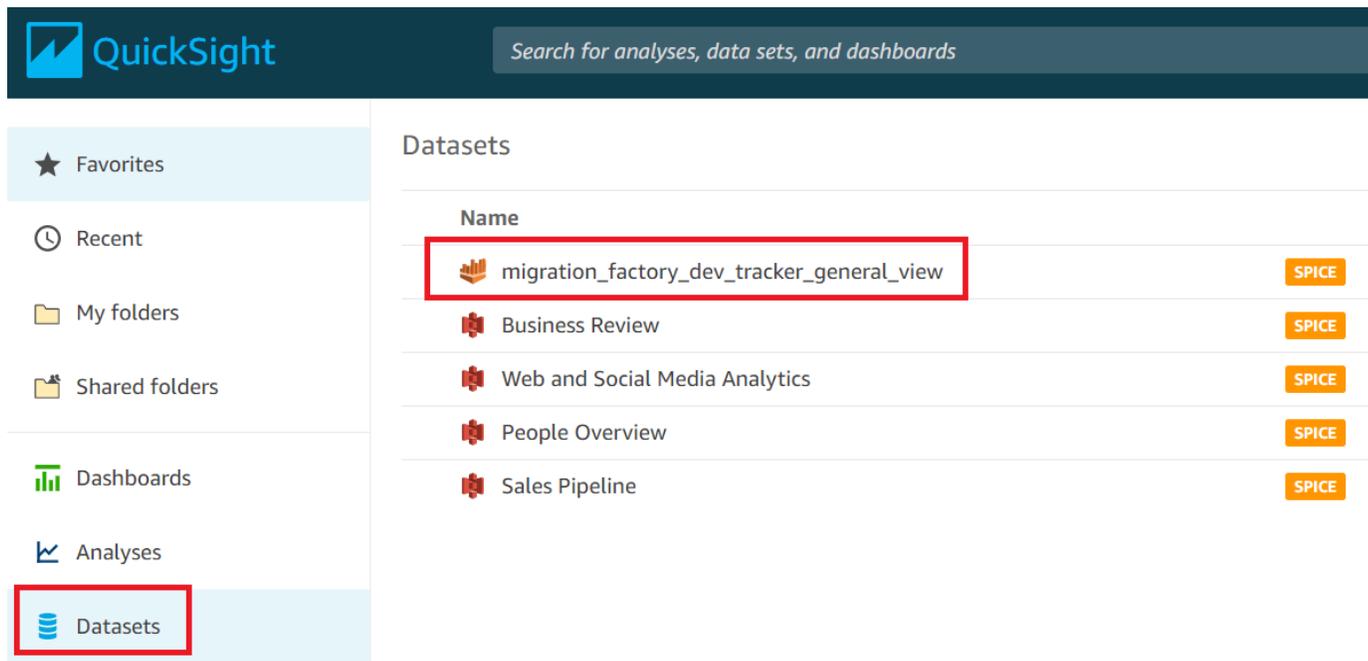
Email owners when a refresh fails

[Edit/Preview data](#) [Augment with SageMaker](#) [Visualize](#)

10. In Nuovo foglio, scegli Foglio interattivo, quindi scegli Crea.

Dopo l'importazione dei dati, verrai reindirizzato alla pagina Analisi. Tuttavia, prima di creare gli elementi visivi, imposta una pianificazione per aggiornare il set di dati.

1. Vai alla home page. QuickSight
2. Nel riquadro di navigazione, scegli Datasets.
3. Nella pagina Datasets, seleziona il dataset <migration-factory>-general-view.



QuickSight

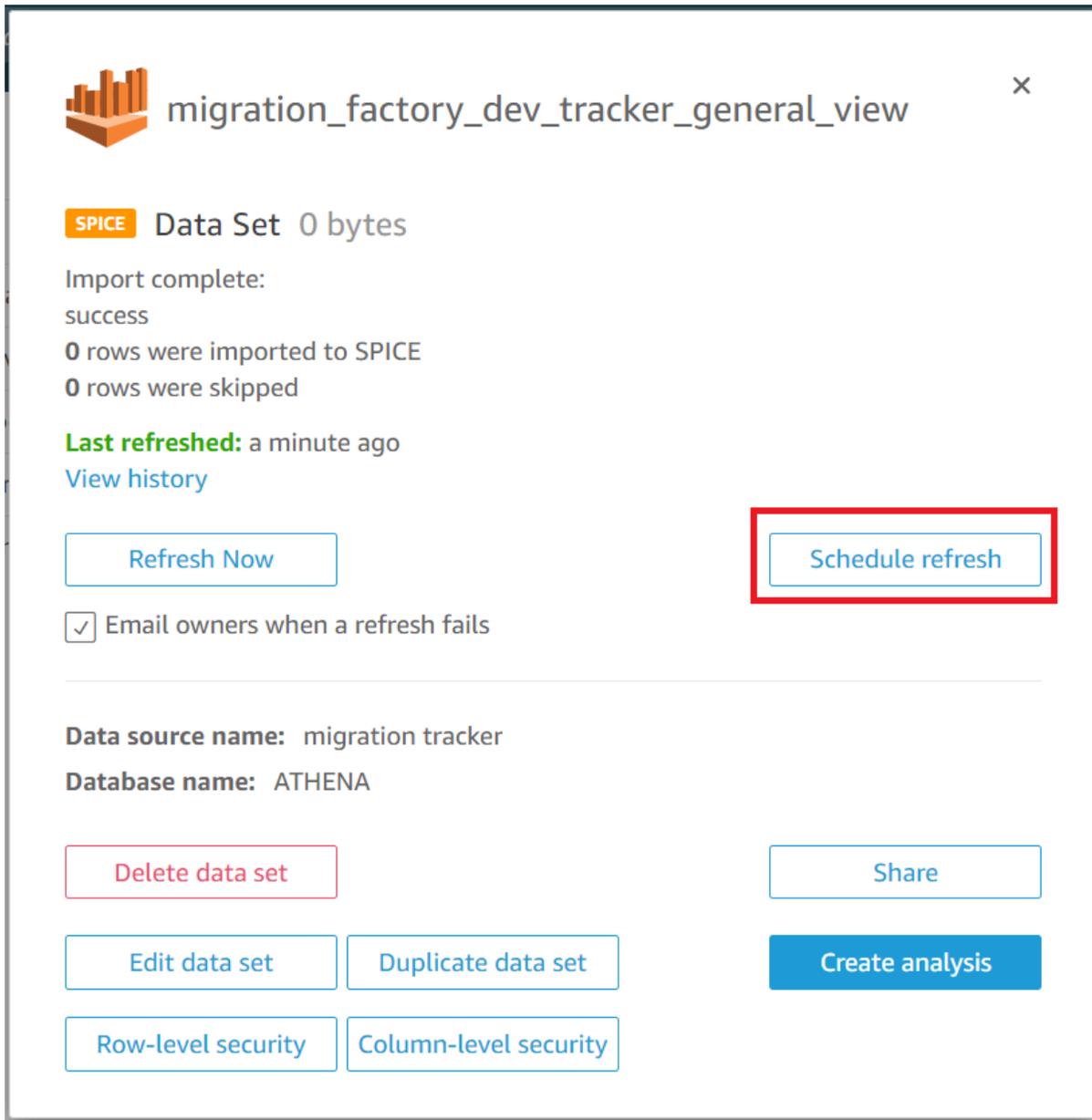
Search for analyses, data sets, and dashboards

- ★ Favorites
- 🕒 Recent
- 📁 My folders
- 📁 Shared folders
- 📊 Dashboards
- 📈 Analyses
- 📄 Datasets**

Datasets

Name	
migration_factory_dev_tracker_general_view	SPICE
Business Review	SPICE
Web and Social Media Analytics	SPICE
People Overview	SPICE
Sales Pipeline	SPICE

4. Nella pagina -general-view Datasets, scegli la scheda Aggiorna. <migration-factory>



migration_factory_dev_tracker_general_view ×

SPICE Data Set 0 bytes

Import complete:
success
0 rows were imported to SPICE
0 rows were skipped

Last refreshed: a minute ago
[View history](#)

[Refresh Now](#) [Schedule refresh](#)

Email owners when a refresh fails

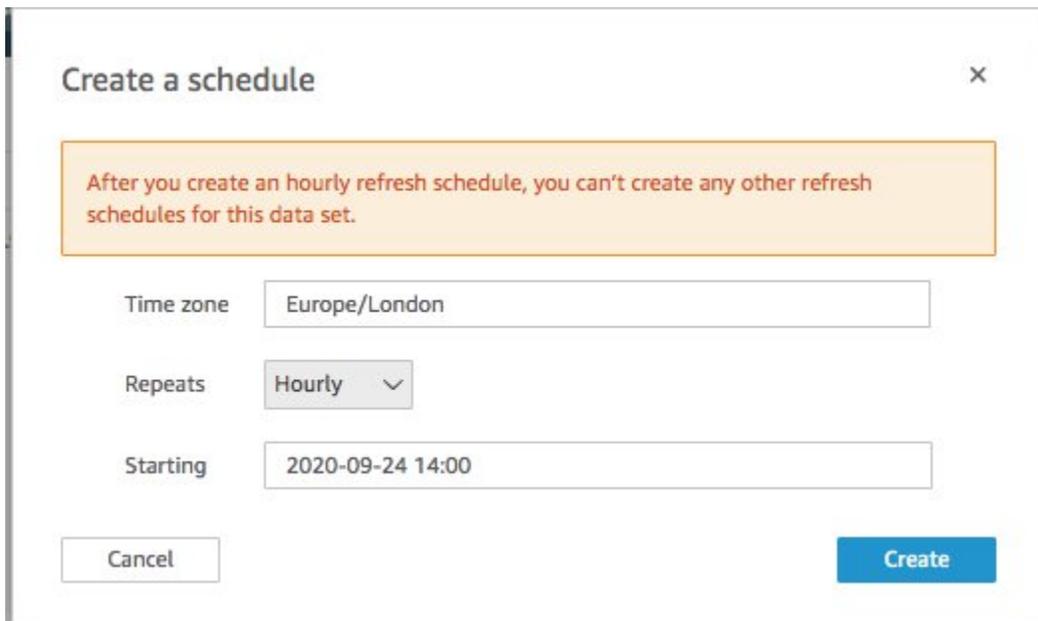
Data source name: migration tracker
Database name: ATHENA

[Delete data set](#) [Share](#)

[Edit data set](#) [Duplicate data set](#) [Create analysis](#)

[Row-level security](#) [Column-level security](#)

5. Scegli Aggiungi nuova pianificazione.
6. Nella pagina Crea una pianificazione di aggiornamento, seleziona Aggiornamento completo, seleziona il fuso orario appropriato, inserisci un'ora di inizio e seleziona la frequenza.
7. Selezionare Salva.



Create a schedule ×

After you create an hourly refresh schedule, you can't create any other refresh schedules for this data set.

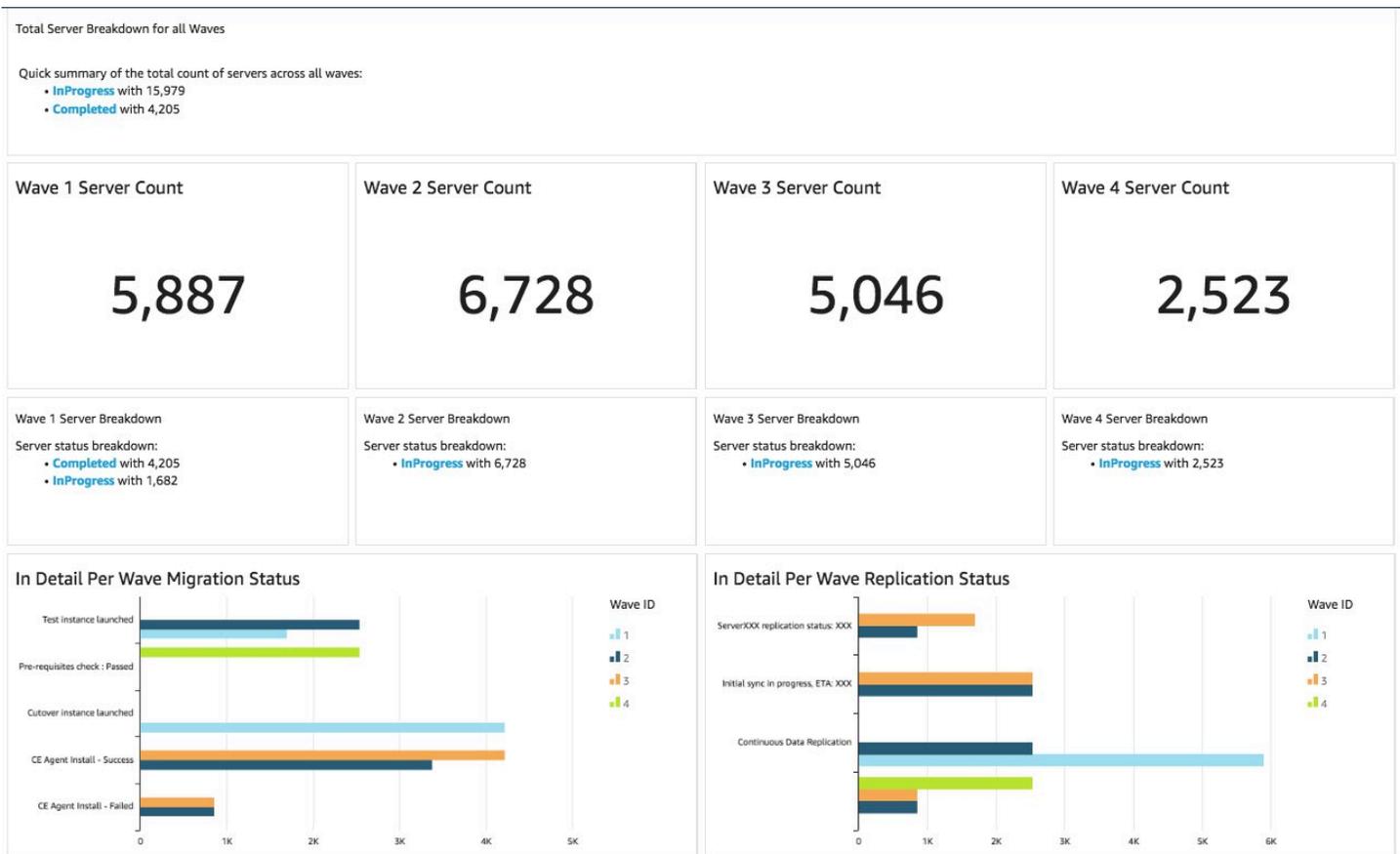
Time zone

Repeats

Starting

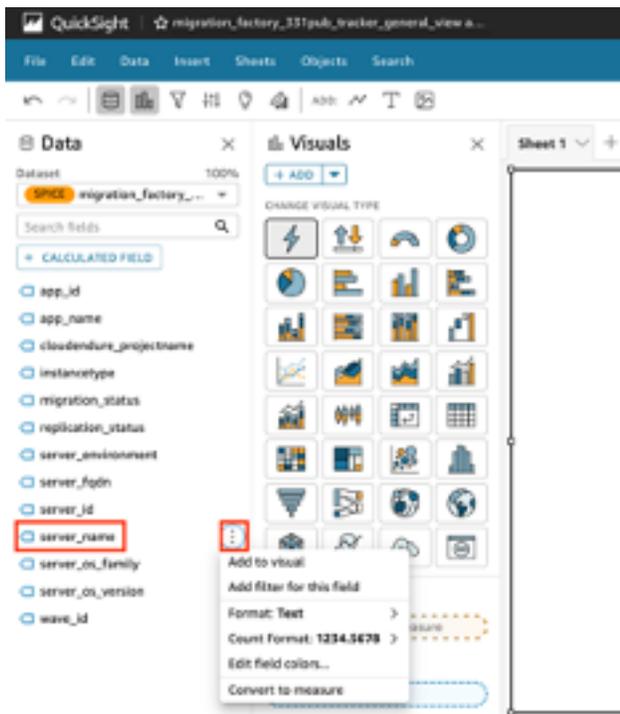
Creazione di un pannello di controllo

Amazon QuickSight offre la flessibilità necessaria per creare un pannello di controllo personalizzato che ti aiuti a visualizzare i metadati della migrazione. Il seguente tutorial crea una dashboard contenente una visualizzazione del conteggio che mostra il conteggio dei server per ondate e grafici a barre che mostrano lo stato della migrazione. Puoi personalizzare questa dashboard per soddisfare le tue esigenze aziendali.

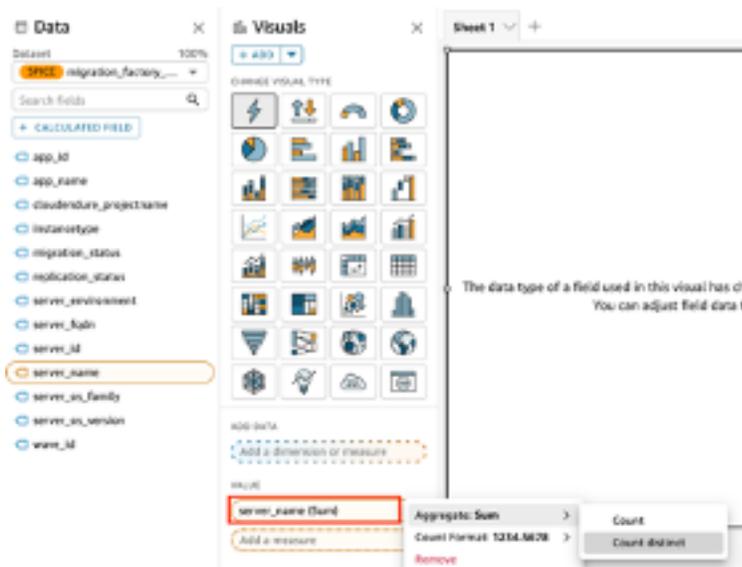


Utilizza i seguenti passaggi per creare una panoramica del conteggio in base alle ondate di migrazione. Questa visualizzazione conta tutti i server del set di dati raggruppati per ondata, fornendo una visione granulare del numero totale di server in un'ondata. Per creare questa vista, convertirte il server_name in una misura, che consente di contare nomi di server distinti. Quindi creerai un filtro onda per onda.

1. Vai alla QuickSight home page.
2. Nel riquadro di navigazione, scegli Analisi.
3. Seleziona <migration-factory>-general-view.
4. Nella pagina Visualize, passa il mouse sul server_name e scegli i puntini di sospensione a destra.



5. Seleziona Converti in misura per convertire il set di dati da una dimensione a una misura. Il testo `server_name` diventa verde per indicare che il set di dati è stato convertito in una misura.
6. Seleziona `server_name` per visualizzare l'immagine. L'immagine conterrà un messaggio di errore che indica che i tipi di dati del campo devono essere aggiornati.
7. Nel riquadro Immagini, seleziona `server_name (Sum)`, in Valore, seleziona Aggregate: Sum, quindi seleziona Count distinct.



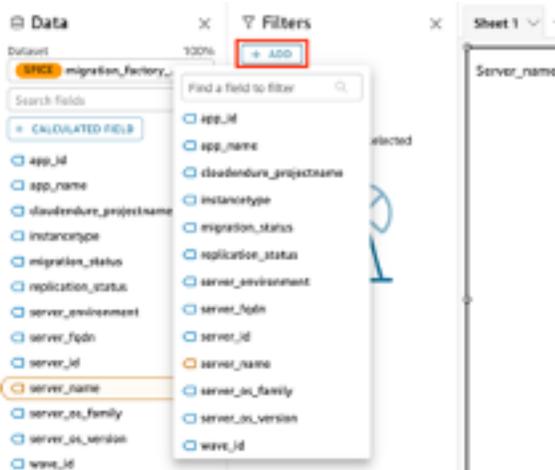
Viene visualizzato un conteggio del numero di nomi di server univoci presenti nel set di dati. È possibile ridimensionare la visualizzazione in base alle esigenze per garantire che mostri chiaramente le informazioni sul monitor.

Note

Potrebbe essere necessario riconvertire il set di dati in dimensioni quando si crea un'altra immagine.

Quindi, aggiungi filtri alla visualizzazione per identificare il numero di server per ogni ondata di migrazione. I passaggi seguenti applicheranno un filtro `wave_id` alla visualizzazione.

1. Verifica che la visualizzazione sia selezionata. Nel riquadro di navigazione superiore, seleziona **Filtro**.
2. Nel riquadro Filtri a sinistra, scegli **AGGIUNGI** e seleziona `wave_id` dall'elenco.

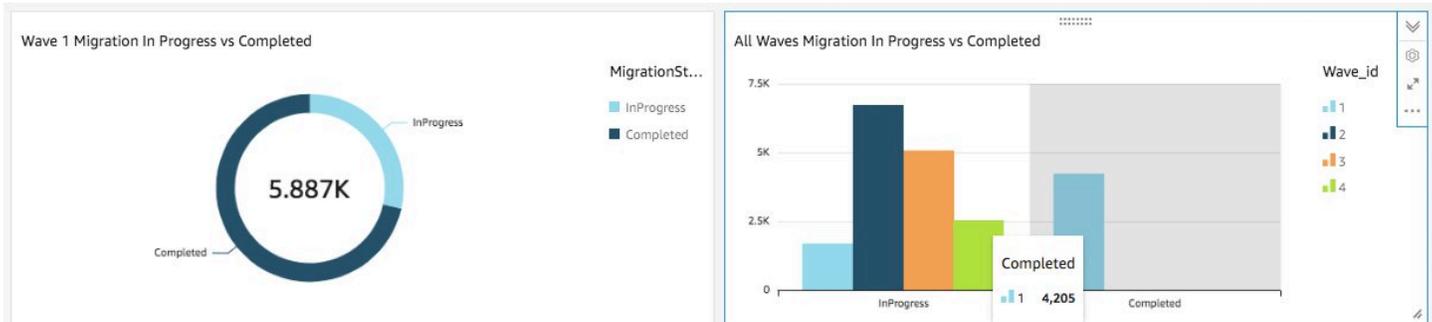


3. Scegli `wave_id` dall'elenco dei filtri.
4. Nel riquadro Filtro, in Valori di ricerca seleziona la casella di controllo accanto al valore 1.
5. Scegli **Applica**.
6. Nella visualizzazione, modifica il titolo in **Wave 1 Server Count** facendo doppio clic sul titolo corrente.

Ripeti questi passaggi per le altre ondate visualizzate nella dashboard.

Modifica riquadro del filtro

La prossima visualizzazione che aggiungeremo nella dashboard è un grafico ad anello che mostra i server in corso di migrazione rispetto a quelli che hanno completato la migrazione. Questo grafico utilizza le query SPICE (Super-Fast, Parallel, In-memory Calculation Engine) creando una nuova colonna nel set di dati che determina che uno stato incompleto verrà identificato come in corso. Tutti i valori del set di dati che non sono stati completati vengono combinati e classificati man mano che sono in corso.



Note

Per impostazione predefinita, quando non viene applicata alcuna query personalizzata al set di dati, è possibile visualizzare fino a cinque stati di migrazione/replica. Per questa soluzione, viene creata una MigrationStatusSummaryquery in una nuova colonna:

```
ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')
```

Questa query combina i valori degli stati per creare una colonna che viene utilizzata per la visualizzazione. Per informazioni sulla creazione di una query, consulta [Using the Query Editor](#) nella Amazon QuickSight User Guide.

Utilizza i seguenti passaggi per creare la MigrationStatusSummarycolonna:

1. Vai alla QuickSight home page.
2. Nel riquadro di navigazione, seleziona Datasets.
3. Nella pagina Dataset, seleziona il *<migration-factory>*-general-view set di dati.
4. Nella pagina del set di dati, scegli Modifica set di dati.

The screenshot shows the Amazon QuickSight interface. On the left, the 'Datasets' menu item is highlighted with a red box. The main panel displays the configuration for a dataset named 'migration_factory_dev_tracker_general_view'. The dataset is a SPICE Data Set with 0 bytes. It shows 'Import complete: success' with 0 rows imported and 0 rows skipped. The last refresh was 'a minute ago'. There are buttons for 'Refresh Now', 'Schedule refresh', 'Delete data set', 'Edit data set', 'Duplicate data set', 'Row-level security', 'Column-level security', 'Share', and 'Create analysis'. The 'Edit data set' button is also highlighted with a red box. The data source is 'migration tracker' and the database is 'ATHENA'.

5. Nel riquadro Campi, scegli +, quindi scegli Aggiungi campo calcolato.
6. Nella pagina Aggiungi campo calcolato, inserisci un nome per la tua query SQL, ad esempio MigrationStatusSummary.
7. Inserisci la seguente query SQL nell'editor SQL:

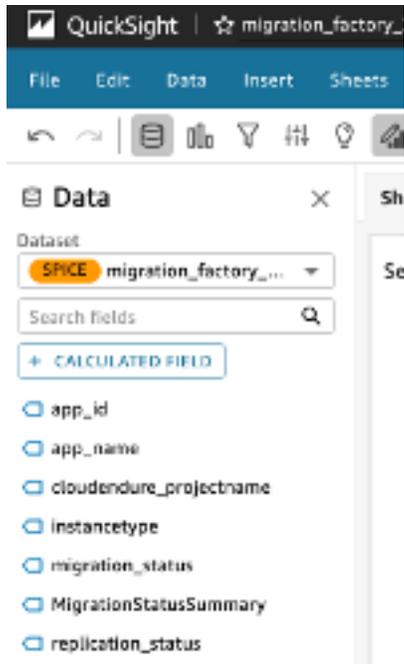
```
ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')
```

8. Selezionare Salva.

The screenshot shows the 'Add calculated field' dialog in Amazon QuickSight. The title is 'MigrationStatusSummary'. The SQL editor contains the query: `ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')`. The 'Save' button is highlighted.

9. Nella pagina Dataset, scegli Salva e pubblica.

La query appena aggiunta verrà elencata nell'elenco Campi del set di dati.



Quindi, crea la dashboard.

1. Vai alla QuickSight home page.
2. Scegli Analisi, quindi scegli le analisi migration_factory create in precedenza.
3. Assicuratevi che nessun grafico sia selezionato nel foglio 1.
4. Dal riquadro Set di dati, passa il mouse sopra MigrationStatusSummary e scegli i puntini di sospensione a destra.
5. Scegli Aggiungi alla visualizzazione.
6. Quindi, scegli wave_id.
7. Nel riquadro Immagini, selezionate e spostate la MigrationStatusSummary dimensione sull'asse x e selezionate wave_name come GROUP/COLOR.

Se disponi di una licenza aziendale per Amazon QuickSight, gli approfondimenti verranno generati dopo la creazione delle colonne personalizzate. Puoi personalizzare le tue narrazioni per ogni approfondimento. Per esempio:



Puoi anche personalizzare i dati suddividendo i metadati in ondate. Per esempio:



(Facoltativo) Visualizza Insights sulla dashboard QuickSight

Note

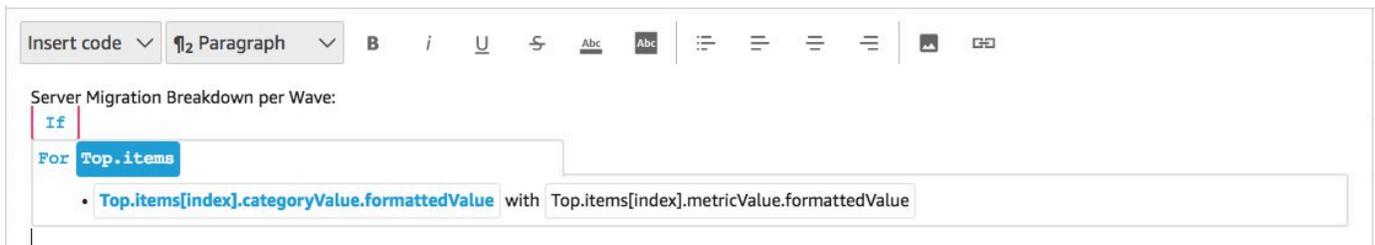
Puoi utilizzare la seguente procedura se disponi di una licenza aziendale per Amazon QuickSight.

Utilizza i seguenti passaggi per aggiungere una panoramica alla dashboard che mostri un'analisi dettagliata delle migrazioni completate e in corso.

1. Nel riquadro di navigazione in alto, scegli Insights.
2. Nella pagina Insights, nella sezione Count of Records BY MIGRATIONSTATUSSUMMARY, passa il mouse sull' MigrationSummaryselemento Top 2 e scegli il + per aggiungere un'idea all'immagine.

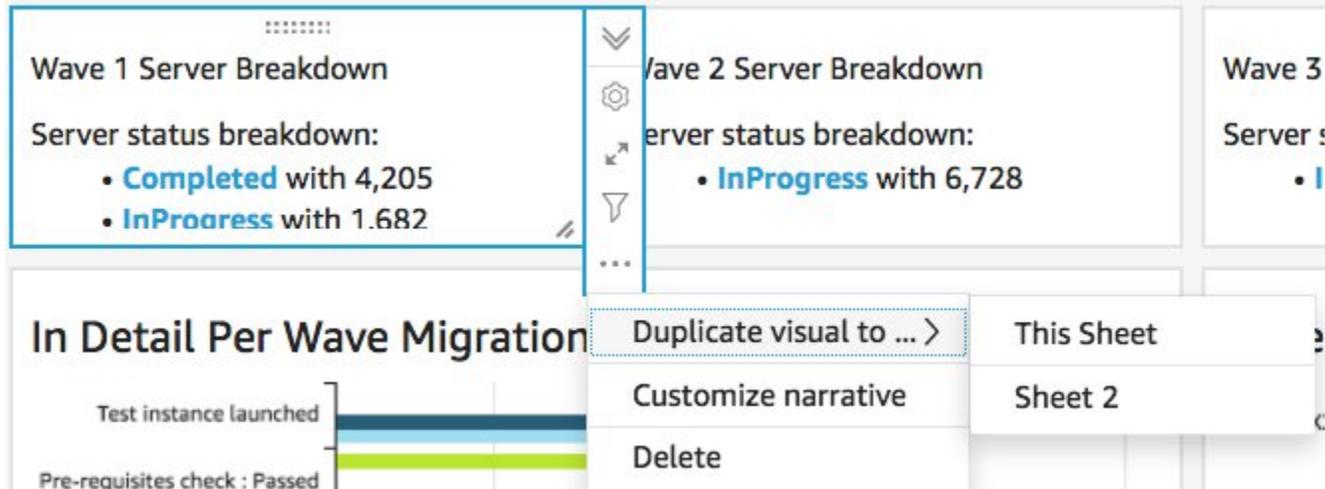
3. Personalizza le informazioni per la tua analisi scegliendo Personalizza narrazione nell'immagine.

4. Modifica la narrazione per adattarla al tuo caso d'uso e scegli Salva. Per esempio:



Torna alla dashboard e filtrala per mostrare ogni ondata:

5. Nel riquadro del menu a sinistra, scegli Filtro.
6. Scegli il pulsante + e seleziona wave_id.
7. Seleziona un'onda da visualizzare e scegli Applica.
8. Per visualizzare tutte le ondate di migrazione, duplica le immagini scegliendo i puntini di sospensione sul lato sinistro dell'immagine e selezionando Duplica immagine.



9. Modifica il filtro per ogni immagine per mostrare una suddivisione per ogni ondata di migrazione.

Queste informazioni sono personalizzate e riassumono il numero totale di server in tutte le ondate. Per ulteriori informazioni e guide su come personalizzare gli approfondimenti, consulta [Working with Insights](#) nella Guida per l'QuickSight utente. Puoi accedere a questa QuickSight dashboard da qualsiasi dispositivo e incorporarla senza problemi nelle tue applicazioni, portali e siti Web. Per ulteriori informazioni sui QuickSight pannelli di controllo, consulta [Working with Dashboards](#) nella Amazon QuickSight User Guide.

Passaggio 10: (Facoltativo) Configurazione di provider di identità aggiuntivi in Amazon Cognito

Se hai selezionato `true` il parametro opzionale `Consenti la configurazione del provider di identità aggiuntivo` in Cognito all'avvio dello stack, puoi impostarne altri in Amazon IdPs Cognito per consentire l'accesso utilizzando l'IdP SAML esistente. Il processo di configurazione dell'IdP esterno varia a seconda del provider. Questa sezione descrive la configurazione di Amazon Cognito e i passaggi generici per configurare l'IdP esterno.

Esegui i seguenti passaggi per raccogliere informazioni da Amazon Cognito da fornire all'IdP esterno:

1. Accedi alla [CloudFormation console AWS](#) e seleziona lo stack Cloud Migration Factory on AWS.
2. Selezionare la scheda Outputs (Output).
3. Nella colonna Chiave, individua `UserPoolId` registra il valore da utilizzare in seguito durante la configurazione.
4. Passa alla [console di Amazon Cognito](#).
5. Scegliete il pool di utenti che corrisponde all'ID del pool di utenti dall'output dello stack di soluzioni.
6. Scegli la scheda Integrazione app e registra il dominio Cognito da utilizzare in seguito durante la configurazione.

Esegui i seguenti passaggi all'interno dell'interfaccia di gestione del tuo IdP esistente:

Note

Queste istruzioni sono generiche e differiranno a seconda del provider. Consulta la documentazione del tuo IdP per tutti i dettagli sulla configurazione delle applicazioni SAML.

1. Accedi all'interfaccia di gestione del tuo IdP.
2. Scegli l'opzione per aggiungere applicazioni o configurare l'autenticazione SAML per un'applicazione e crea o aggiungi una nuova applicazione.
3. Durante la configurazione di questa applicazione SAML, ti verranno richiesti i seguenti valori:
 - a. Identifier (Entity ID) o qualcosa di simile. Fornisci il seguente valore:

```
urn:amazon:cognito:sp:<UserPoolId recorded earlier>
```

- b. URL di risposta (Assertion Consumer Service URL) o qualcosa di simile. Fornisci il seguente valore:

```
https://<Amazon Cognito domain recorded earlier>/saml2/idpresponse
```

- c. Attributi e rivendicazioni o qualcosa di simile. Come minimo, assicurati che un identificatore o oggetto univoco sia configurato insieme a un attributo che fornisce l'indirizzo e-mail dell'utente.
4. Sarà disponibile un URL di metadati o la possibilità di scaricare un file XML di metadati. Scarica una copia del file o registra l'URL fornito per utilizzarlo successivamente durante la configurazione.
5. All'interno della configurazione, configura l'elenco di accesso degli utenti dell'IdP a cui è consentito accedere all'applicazione CMF. A tutti gli utenti a cui è concesso l'accesso all'applicazione nell'IdP verrà automaticamente concesso l'accesso in sola lettura alla console CMF.

Esegui i seguenti passaggi per aggiungere il nuovo IdP al pool di utenti di Amazon Cognito creato durante la distribuzione dello stack:

1. Passa alla [console di Amazon Cognito](#).
2. Scegli il pool di utenti che corrisponde all'ID del pool di utenti dall'output dello stack di soluzioni.
3. Scegli la scheda Sign-in experience (Esperienza di accesso).
4. Scegli Aggiungi provider di identità, quindi scegli SAML come provider di terze parti.
5. Fornisci un nome per il provider; questo verrà visualizzato all'utente nella schermata di accesso CMF.
6. Nella sezione Origine del documento di metadati, fornisci l'URL dei metadati acquisito dalla configurazione IDP SAML o carica il file XML di metadati.
7. Nella sezione Attributi della mappa, scegli Aggiungi un altro attributo.
8. Scegli email per il valore dell'attributo User pool. Per l'attributo SAML, inserisci il nome dell'attributo a cui il tuo IdP esterno fornirà l'indirizzo email.
9. Scegli Aggiungi provider di identità per salvare questa configurazione.
10. Scegli la scheda App integration (Integrazione app).
11. Dalla sezione dell'elenco dei client dell'app, scegli il client dell'applicazione Migration Factory (dovrebbe essercene solo uno) facendo clic sul nome.
12. Dalla sezione Hosted UI, scegli Modifica.
13. Aggiorna i provider di identità selezionati selezionando il nuovo nome IdP aggiunto nel passaggio 5 e deselegando Cognito User Pool.

 Note

Il pool di utenti di Cognito non è necessario perché è integrato nella schermata di accesso CMF e, se selezionato, verrà visualizzato due volte.

14. Seleziona Salvataggio delle modifiche.

La configurazione è ora completa. Nella pagina di accesso a CMF, vedrai il pulsante Accedi con il tuo ID aziendale. Scegliendo questa opzione verrà visualizzato il provider che avete configurato in precedenza. Gli utenti che scelgono questa opzione verranno indirizzati ad accedere e quindi a tornare alla console CMF una volta effettuato correttamente l'accesso.

Monitora la soluzione con Service Catalog AppRegistry

Questa soluzione include una AppRegistry risorsa Service Catalog per registrare il CloudFormation modello e le risorse sottostanti come applicazione sia in [Service Catalog AppRegistry](#) che in [AWS Systems Manager Application Manager](#).

AWS Systems Manager Application Manager offre una visione a livello di applicazione di questa soluzione e delle relative risorse in modo da poter:

- Monitora le risorse, i costi delle risorse distribuite tra gli stack e Account AWS i log associati a questa soluzione da una posizione centrale.
- Visualizza i dati operativi relativi alle risorse di questa soluzione (come lo stato dell'implementazione, gli CloudWatch allarmi, le configurazioni delle risorse e i problemi operativi) nel contesto di un'applicazione.

La figura seguente mostra un esempio di visualizzazione delle applicazioni per lo stack di soluzioni in Application Manager.

The screenshot displays the AWS Systems Manager Application Manager console. On the left, a sidebar shows a tree view under 'Components (2)' with 'AWS-Systems-Manager-A' selected. The main content area is titled 'AWS-Systems-Manager-Application-Manager' and includes a 'Start runbook' button. Below the title is the 'Application information' section, which contains a 'View in AppRegistry' button and details for 'Application type' (AWS-AppRegistry), 'Name' (AWS-Systems-Manager-Application-Manager), and 'Application monitoring' (Not enabled). A description states: 'Service Catalog application to track and manage all your resources for the solution'. A navigation bar below this section includes tabs for Overview, Resources, Instances, Compliance, Monitoring, OpsItems, Logs, Runbooks, and Cost. At the bottom, there are two summary cards: 'Insights and Alarms' with a 'View all' button and 'Cost' with a 'View all' button. The cost card shows 'Cost (USD)'.

Stack di soluzioni in Application Manager

Attiva CloudWatch Application Insights

1. Accedere alla [console Systems Manager](#).

2. Nel riquadro di navigazione, scegli Application Manager.
3. In Applicazioni, cerca il nome dell'applicazione per questa soluzione e selezionalo.

Il nome dell'applicazione avrà il registro delle app nella colonna Origine dell'applicazione e avrà una combinazione del nome della soluzione, della regione, dell'ID dell'account o del nome dello stack.

4. Nell'albero dei componenti, scegliete lo stack di applicazioni che desiderate attivare.
5. Nella scheda Monitoraggio, in Application Insights, seleziona Configura automaticamente Application Insights.

Overview | Resources | Provisioning | Compliance | **Monitoring** | Opsitems | Logs | Runbooks | Cost

Application Insights (0) [Info](#) View Ignored Problems [Actions](#) [Add an application](#)

Problems detected by severity

[Last 7 days](#) < 1 >

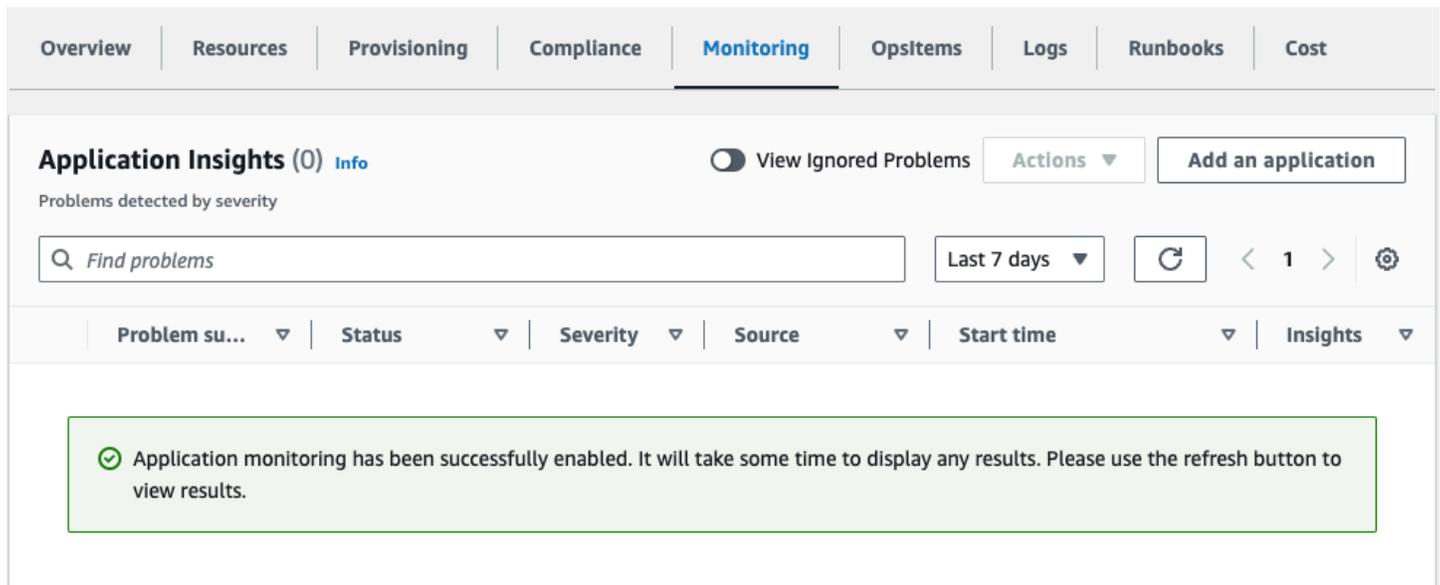
Problem su...	Status	Severity	Source	Start time	Insights
---------------	--------	----------	--------	------------	----------

Advanced monitoring is not enabled

When you onboard your first application, a service-linked role (SLR) is created in your account. The SLR is predefined by CloudWatch Application Insights and includes the permissions the service requires to monitor AWS services on your behalf.

[Auto-configure Application Insights](#)

Il monitoraggio delle applicazioni è ora attivato e viene visualizzata la seguente casella di stato:



Overview | Resources | Provisioning | Compliance | **Monitoring** | OpsItems | Logs | Runbooks | Cost

Application Insights (0) [info](#) View Ignored Problems Actions ▾ Add an application

Problems detected by severity

Last 7 days ▾ ↻ < 1 > ⚙️

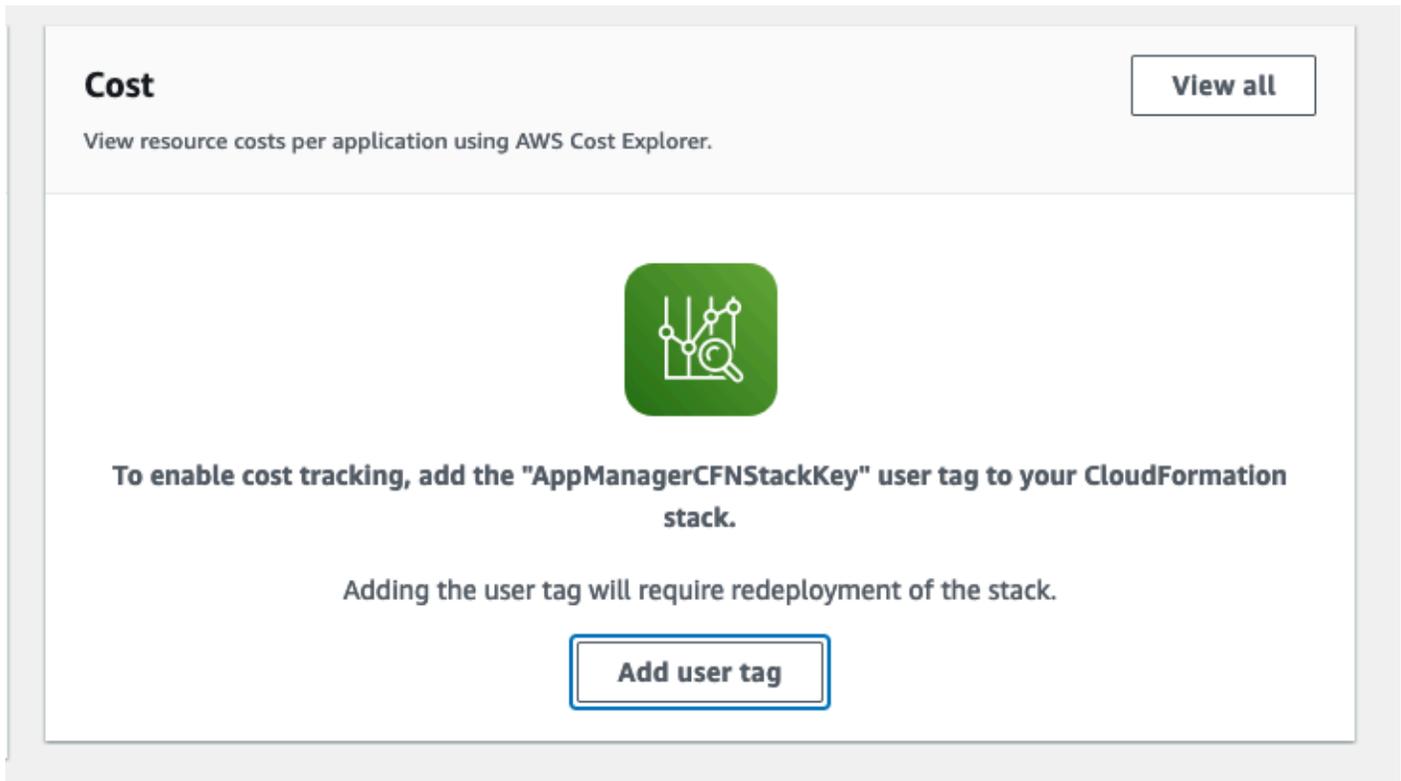
Problem su... ▾ | **Status** ▾ | **Severity** ▾ | **Source** ▾ | **Start time** ▾ | **Insights** ▾

✔️ Application monitoring has been successfully enabled. It will take some time to display any results. Please use the refresh button to view results.

Conferma i cartellini dei costi associati alla soluzione

Dopo aver attivato i tag di allocazione dei costi associati alla soluzione, è necessario confermare i tag di allocazione dei costi per visualizzare i costi di questa soluzione. Per confermare i tag di allocazione dei costi:

1. Accedere alla [console Systems Manager](#).
2. Nel riquadro di navigazione, scegli Application Manager.
3. In Applicazioni, scegli il nome dell'applicazione per questa soluzione e selezionala.
4. Nella scheda Panoramica, in Costo, seleziona Aggiungi tag utente.



5. Nella pagina Aggiungi tag utente, inserisci `confirm`, quindi seleziona Aggiungi tag utente.

Il completamento del processo di attivazione può richiedere fino a 24 ore e la visualizzazione dei dati del tag.

Attiva i tag di allocazione dei costi associati alla soluzione

Dopo aver confermato i tag dei costi associati a questa soluzione, è necessario attivare i tag di allocazione dei costi per visualizzare i costi di questa soluzione. I tag di allocazione dei costi possono essere attivati solo dall'account di gestione dell'organizzazione.

Per attivare i tag di allocazione dei costi:

1. Accedi alla [console AWS Billing and Cost Management and Cost Management](#).
2. Nel riquadro di navigazione, seleziona Tag di allocazione dei costi.
3. Nella pagina Tag di allocazione dei costi, filtra il `AppManagerCFNStackKey` tag, quindi seleziona il tag dai risultati visualizzati.
4. Seleziona **Attiva** (Attiva).

AWS Cost Explorer

È possibile visualizzare la panoramica dei costi associati all'applicazione e ai componenti dell'applicazione all'interno della console di Application Manager tramite l'integrazione con AWS Cost Explorer. Cost Explorer ti aiuta a gestire i costi fornendo una panoramica dei costi e dell'utilizzo delle risorse AWS nel tempo.

1. Accedi alla [console di gestione dei AWS costi](#).
2. Nel menu di navigazione, seleziona Cost Explorer per visualizzare i costi e l'utilizzo della soluzione nel tempo.

Aggiorna la soluzione

Se hai già distribuito la soluzione, segui questa procedura per aggiornare lo CloudFormation stack di soluzioni Cloud Migration Factory on AWS per ottenere la versione più recente del framework della soluzione.

1. Accedi alla [AWS CloudFormation console](#), seleziona la tua Cloud Migration Factory esistente nello CloudFormation stack di AWS soluzioni e seleziona **Aggiorna**.
2. Seleziona **Sostituisci modello corrente**.
3. In **Specificare il modello**:
 - a. Seleziona l'URL di Amazon S3.
 - b. Copia il link per il [modello più recente](#).
 - c. Incolla il link nella casella dell'URL di Amazon S3.
 - d. Verifica che l'URL del modello corretto sia visualizzato nella casella di testo URL di Amazon S3 e scegli **Avanti**. Scegliere **Next (Successivo)** di nuovo.
4. In **Parametri**, esamina i parametri del modello e modificali se necessario. Fate riferimento alla [Fase 2. Avvia lo Stack](#) per i dettagli sui parametri.
5. Seleziona **Successivo**.
6. Nella pagina **Configure stack options (Configura opzioni pila)**, scegliere **Next (Successivo)**.
7. Nella pagina **Rivedi**, verifica e conferma le impostazioni. Assicurati di selezionare la casella che conferma che il modello potrebbe creare risorse AWS Identity and Access Management (IAM).
8. Scegli **Visualizza set di modifiche e verifica le modifiche**.
9. Scegli **Aggiorna stack per distribuire lo stack**.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna **Stato**.

Dovresti ricevere lo stato `UPDATE_COMPLETE` entro circa 10 minuti.

Dopo aver aggiornato lo stack, è necessario ridistribuire le API API Gateway: admin, login, strumenti e utente. Ciò garantisce che tutte le modifiche alla configurazione siano disponibili per tutte le API.

1. Accedi alla [console Amazon API Gateway](#), seleziona API dalla barra di navigazione a sinistra, quindi seleziona l'API CMF.
2. Dalle risorse API, seleziona **Azioni** e seleziona **Deploy API**.
3. Seleziona **Deployment Stage of prod** e scegli **Deploy**.

4. Ripeti i passaggi 1-3 per ciascuna delle API di Cloud Migration Factory on AWS.

Note

L'aggiornamento della soluzione aggiunge le versioni correnti degli script inclusi allo stack distribuito, ma non imposta le versioni predefinite degli script sulla versione più recente. Il motivo è che non vogliamo sovrascrivere le personalizzazioni che potrebbero essere state applicate alla soluzione.

Per utilizzare le versioni più recenti degli script:

1. Passa alla Cloud Migration Factory sulla console AWS.
2. Nel menu di navigazione, seleziona Automation, quindi seleziona Scripts.
3. Nella pagina Script di automazione, per ogni script desideri che la versione più recente sia quella predefinita:
 - a. Seleziona lo script.
 - b. In Azioni, scegli Cambia versione predefinita.
 - c. Da Script Default Version, scegli il numero di versione più recente disponibile.
 - d. Selezionare Salva.

Risoluzione dei problemi

Se hai bisogno di assistenza con questa soluzione, contatta AWS Support per aprire una richiesta di supporto per questa soluzione.

Contatta AWS Support

Se disponi di [AWS Developer Support](#), [AWS Business Support](#) o [AWS Enterprise Support](#), puoi utilizzare il Support Center per ottenere l'assistenza di esperti su questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Accedi al [Support Center](#).
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Altre soluzioni.
4. Per Severità, seleziona l'opzione più adatta al tuo caso d'uso.
5. Quando si inseriscono i campi Servizio, Categoria e Severità, l'interfaccia compila i collegamenti alle domande più comuni per la risoluzione dei problemi. Se non riesci a risolvere la tua domanda con questi link, scegli Passaggio successivo: Informazioni aggiuntive.

Informazioni aggiuntive

1. In Oggetto, inserisci il testo che riassume la domanda o il problema.
2. Per Descrizione, descrivi il problema in dettaglio.
3. Scegli Allega file.
4. Allega le informazioni di cui AWS Support ha bisogno per elaborare la richiesta.

Aiutaci a risolvere il tuo caso più velocemente

1. Inserisci le informazioni richieste.
2. Scegli Passaggio successivo: risolvi ora o contattaci.

Risolvi subito o contattaci

1. Rivedi le soluzioni Solve now.
2. Se non riesci a risolvere il problema con queste soluzioni, scegli Contattaci, inserisci le informazioni richieste e scegli Invia.

Dissoluzione soluzione soluzione soluzione soluzione soluzione

Puoi disinstallare la soluzione Cloud Migration Factory on AWS da AWS Management Console o utilizzando il AWS Command Line Interface. È necessario svuotare manualmente tutti i bucket Amazon Simple Storage Service (Amazon S3). AWS Le implementazioni delle soluzioni non eliminano automaticamente i bucket S3 nel caso in cui siano presenti dati archiviati da conservare.

Svuota i bucket Amazon S3.

Se decidi di eliminare lo AWS CloudFormation stack, questa soluzione è configurata per conservare il bucket Amazon S3 creato (per l'implementazione in una regione opzionale) per evitare perdite accidentali di dati. È necessario svuotare manualmente tutti i bucket S3 prima di eliminare completamente lo stack. Per svuotare il bucket Amazon S3.

1. Accedere alla [console Amazon S3](#).
2. Scegli Bucket dal riquadro di navigazione a sinistra.
3. Individua i <stack-name>bucket S3.
4. Seleziona il bucket S3 e scegli Vuoto.

Per eliminare il bucket S3 utilizzando la AWS CLI, esegui il comando seguente:

```
aws s3 rm s3://<bucket-name> --recursive
```

Utilizzo di AWS Management Console per eliminare lo stack

1. Accedi alla [console AWS CloudFormation](#).
2. Nella pagina Stacks, seleziona lo stack di installazione di questa soluzione.
3. Scegli Delete (Elimina).

UtilizzoAWS Command Line Interface per eliminare lo stack

Determina seAWS Command Line Interface (AWS CLI) è disponibile nel tuo ambiente. Per le istruzioni di installazione, consulta [What Is theAWS Command Line Interface](#) in the AWS CLI User Guide. Dopo aver confermato che laAWS CLI è disponibile, esegui il comando seguente:

```
aws cloudformation delete-stack --stack-name <installation-stack-name>
```

Guida per l'utente

Le seguenti sezioni forniscono indicazioni su come utilizzare le varie funzionalità disponibili in un'istanza Cloud Migration Factory on AWS distribuita con una migrazione su larga scala verso AWS.

Gestione dei metadati

La AWS soluzione Cloud Migration Factory offre un datastore estensibile che consente di aggiungere, modificare ed eliminare i record dall'interno dell'interfaccia utente. Tutti gli aggiornamenti dei dati archiviati nel datastore vengono controllati con timbri di controllo di livello record, che forniscono timestamp di creazione e aggiornamento insieme ai dettagli dell'utente. Tutti gli accessi agli aggiornamenti ai record sono controllati dai gruppi e dalle politiche associate assegnati all'utente che ha effettuato l'accesso. [Per maggiori dettagli sulla concessione delle autorizzazioni agli utenti, consulta Gestione delle autorizzazioni.](#)

Visualizzazione dei dati

Tramite il riquadro di navigazione di Migration Management, è possibile selezionare i tipi di record (applicazione, wave, database, server) contenuti nel datastore. Dopo aver selezionato una vista, viene mostrata una tabella dei record esistenti per il tipo di record scelto. La tabella di ogni tipo di record mostra un set predefinito di colonne che possono essere modificate dall'utente. Le modifiche sono persistenti tra le sessioni e vengono memorizzate nel browser e nel computer utilizzati per apportare le modifiche.

Modifica delle colonne predefinite visualizzate nelle tabelle

Per modificare le colonne predefinite, seleziona l'icona delle impostazioni situata nell'angolo superiore destro di qualsiasi tabella di dati, quindi seleziona le colonne da visualizzare. Da questa schermata, puoi anche modificare il numero predefinito di righe da visualizzare e attivare la disposizione delle righe per le colonne con grandi quantità di dati.

Visualizzazione di un record

Per visualizzare un record specifico in una tabella, puoi fare clic in un punto qualsiasi della riga o selezionare la casella di controllo accanto alla riga. Se si selezionano più righe, non verrà visualizzato alcun record. Verrà quindi visualizzato il record in modalità di sola lettura nella tabella dei dati nella parte inferiore dello schermo. Il record visualizzato avrà le seguenti tabelle predefinite disponibili.

Dettagli: questa è una visualizzazione riepilogativa degli attributi e dei valori richiesti per il tipo di record.

Tutti gli attributi: visualizza un elenco completo di tutti gli attributi e dei relativi valori.

A seconda del tipo di record selezionato, possono essere presenti altre schede che forniscono dati e informazioni correlati. Ad esempio, i record dell'applicazione avranno una scheda Server che mostra una tabella dei server relativi all'applicazione selezionata.

Aggiungere o modificare un record

Le operazioni sono controllate in base al tipo di record tramite le autorizzazioni dell'utente. Se un utente non dispone dell'autorizzazione necessaria per aggiungere o modificare un tipo specifico di record, i pulsanti **Aggiungi** e/o **Modifica** sono disattivati e disattivati.

Per aggiungere un nuovo record:

1. Scegli **Aggiungi** nell'angolo superiore destro della tabella per il tipo di record che desideri creare.

Per impostazione predefinita, la schermata **Aggiungi** applicazione mostra le sezioni **Dettagli** e **Verifica**, ma a seconda del tipo e delle eventuali personalizzazioni dello schema, potrebbero essere visualizzate anche altre sezioni.

2. Dopo aver completato il modulo e risolto tutti gli errori, scegliete **Salva**.

Per modificare un record esistente:

1. Seleziona un record dalla tabella che desideri modificare, quindi scegli **Modifica**.
2. Modifica il record e assicurati che non esistano errori di convalida, quindi scegli **Salva**.

Eliminazione di un record

Se un utente non dispone dell'autorizzazione per eliminare un tipo specifico di record, il pulsante **Elimina** è disattivato e disattivato.

⚠ Important

I record eliminati dal datastore non sono recuperabili. Consigliamo di effettuare backup regolari della tabella DynamoDB o di esportare i dati per garantire che esista un punto di ripristino in caso di problemi.

Per eliminare uno o più record:

1. Seleziona uno o più record dalla tabella.
2. Scegliere Elimina e confermare l'operazione.

Esportazione dei dati

La maggior parte dei dati archiviati nella AWS soluzione Cloud Migration Factory on può essere esportata in file Excel (.xlsx). È possibile esportare i dati a livello di tipo di record o un output completo di tutti i dati e i tipi.

Per esportare un tipo di record specifico:

1. Vai alla tabella da esportare.
2. Facoltativo: seleziona i record da esportare in un foglio Excel. Se non ne viene selezionato nessuno, verranno esportati tutti i record.
3. Scegli l'icona Esporta nell'angolo in alto a destra della schermata della tabella dei dati.

Un file excel con il nome del tipo di record (ad esempio, `servers.xlsx`) verrà scaricato nella posizione di download predefinita del browser.

Per esportare tutti i dati:

1. Vai a Gestione della migrazione e seleziona Esporta.
2. Seleziona Scarica tutti i dati.

Un file excel con il nome `all-data.xlsx` verrà scaricato nella posizione di download predefinita del browser. Questo file excel contiene una scheda per tipo di record e tutti i record per ogni tipo verranno esportati.

Note

I file esportati potrebbero contenere nuove colonne poiché Excel ha un limite di testo nelle celle di 32767 caratteri. Pertanto, l'esportazione tronca il testo per tutti i campi che contengono più dati di quelli supportati da Excel. Per tutti i campi troncati, all'esportazione viene aggiunta una nuova colonna con il nome originale aggiunto al testo. [truncated - Excel max chars 32767] Inoltre, all'interno della cella troncata, vedrai anche il testo. [n characters truncated, first x provided] Il processo di troncamento protegge dallo scenario in cui un utente esporta e poi importa lo stesso Excel e, di conseguenza, sovrascrive i dati con i valori troncati.

Importazione dei dati

La AWS soluzione Cloud Migration Factory on offre una funzionalità di importazione dei dati in grado di importare semplici strutture di record nell'archivio dati, ad esempio un elenco di server. Può anche importare dati relazionali più complessi, ad esempio può creare un nuovo record di applicazioni e più server contenuti nello stesso file e metterli in relazione tra loro in un'unica attività di importazione. Ciò consente di utilizzare un unico processo di importazione per qualsiasi tipo di dati da importare. Il processo di importazione convalida i dati utilizzando le stesse regole di convalida utilizzate quando l'utente modifica i dati nell'interfaccia utente.

Scaricamento di un modello

Per scaricare i moduli di acquisizione dei modelli dalla schermata di importazione, selezionate il modello richiesto dall'elenco Azioni. Sono disponibili i due modelli predefiniti seguenti.

Modello con solo attributi obbligatori: contiene solo gli attributi contrassegnati come obbligatori. Fornisce il set minimo di attributi necessari per importare i dati per tutti i tipi di record.

Modello con tutti gli attributi: contiene tutti gli attributi dello schema. Questo modello contiene informazioni aggiuntive di supporto dello schema per ogni attributo per identificare lo schema in cui è stato trovato. Questi prefissi di supporto alle intestazioni delle colonne possono essere rimossi se necessario. Se lasciati invariati durante un'importazione, i valori all'interno della colonna verranno caricati solo nel tipo di record specifico e non utilizzati per i valori relazionali. Per maggiori dettagli, consulta Import Header Schema Helpers.

Importazione di un file

I file di importazione possono essere creati in formato.xlsx o.csv. Per il formato CSV, deve essere salvato utilizzando la codifica UTF8, altrimenti il file apparirà vuoto durante la visualizzazione della tabella di convalida pre-caricamento.

Per importare un file:

1. Vai a Gestione della migrazione e seleziona Importa.
2. Scegli Seleziona file. Per impostazione predefinita, puoi selezionare solo file con .xlsx estensione .csv o. Se il file viene letto correttamente, verranno visualizzati il nome e la dimensione del file.
3. Seleziona Successivo.
4. La schermata di convalida prima del caricamento mostra il risultato della mappatura delle intestazioni all'interno del file con gli attributi all'interno dello schema e della convalida dei valori forniti.
 - Le mappature delle intestazioni delle colonne dei file vengono visualizzate nei nomi delle colonne della tabella sullo schermo. Per verificare quale intestazione di colonna del file è stata mappata, seleziona il nome espandibile nell'intestazione per ulteriori informazioni sulla mappatura, inclusa l'intestazione del file originale e il nome dello schema su cui è stata mappata. Verrà visualizzato un avviso nella colonna Convalida per tutte le intestazioni di file non mappate o in caso di nomi duplicati in più schemi.
 - Tutte le intestazioni convalidano i valori di ogni riga del file rispetto ai requisiti per l'attributo mappato. Eventuali avvisi o errori nel contenuto del file vengono visualizzati nella colonna Convalida.
5. Quando non sono presenti errori di convalida, scegli Avanti.
6. La fase di caricamento dei dati mostra una panoramica delle modifiche che verranno apportate una volta caricato il file. Per qualsiasi elemento in cui verrà apportata una modifica al momento del caricamento, puoi selezionare Dettagli sotto il tipo di aggiornamento specifico per visualizzare le modifiche che verranno eseguite.
7. Una volta completata la revisione, scegli Carica per salvare le modifiche ai dati in tempo reale.

Se il caricamento ha esito positivo, nella parte superiore del modulo viene visualizzato un messaggio. Eventuali errori che si verificano durante il caricamento vengono visualizzati in Panoramica del caricamento.

Importa gli helper dello schema di intestazione

Per impostazione predefinita, le intestazioni delle colonne nel file di input devono essere impostate sul nome di un attributo di qualsiasi schema, il processo di importazione cerca tutti gli schemi e tenta di abbinare il nome dell'intestazione a un attributo. Se un attributo viene trovato in più schemi, verrà visualizzato un avviso, in particolare per gli attributi di relazione che possono essere ignorati nella maggior parte dei casi. Tuttavia, se l'intenzione è quella di mappare una colonna specifica a un attributo dello schema specifico, puoi sovrascrivere questo comportamento antepoendo all'intestazione della colonna un prefisso di supporto dello schema. Questo prefisso è nel formato `{schema name}{attribute name}`, dove `{schema name}` è il nome dello schema basato sul nome di sistema (wave, applicazione, server, database) e il nome di sistema dell'`{attribute name}` attributo nello schema. Se questo prefisso è presente, tutti i valori verranno inseriti solo nei record per questo schema specifico, anche se il nome dell'attributo è presente in altri schemi.

Come illustrato nella figura seguente, l'intestazione nella colonna C è stata preceduta da `[database]`, forzando la mappatura dell'attributo all'attributo nello schema del `database` database_type.

	B	C	D	E	F	G	H	I
1	database_name	[database]database_type	wave_name	aws_accountid	server_name	server_os_family	server_os_version	server_fqdn
2	importdb1	mssql	importwave1	123456789012	importserver1	linux	RH	importserver1

Helper per lo schema dell'intestazione di importazione

Formato di importazione degli attributi

La tabella seguente fornisce una guida alla formattazione dei valori in un file di importazione per importarli correttamente negli attributi di Cloud Migration Factory.

Type	Formato di importazione supportato	Esempio
Stringa	Accetta caratteri alfanumerici e speciali.	123456AbCd . !
Stringa multivalore	Un elenco di tipi di stringhe, delimitato da un punto e virgola.	Item1 ; Item2 ; Item3
Password	Accetta caratteri alfanumerici e speciali.	123456AbCd . !

Type	Formato di importazione supportato	Esempio
Data	MM/GG/AAAA HH:mm	01/30/2023 10:00
Checkbox	Valore booleano, sotto forma di stringa, per selezionato e per non selezionato. TRUE FALSE	TRUE o FALSE
Area di testo	Tipo di stringa con supporto per i feed di linea e i ritorni a carrello.	Test line1 o Testline 2
Tag	I tag devono essere formattati in quanto key=value; più tag devono essere delimitati da un punto e virgola.	TagKey1=Tagvalue1; TagKey2=tagvalue2;
Elenco	Se si imposta un singolo attributo della lista di valori, utilizzare la stessa formattazione del tipo String, se si imposta un elenco di selezione multipla, utilizzare la stessa formattazione del tipo String multivalore.	Selection1;Selection2;
Relazione	Accetta caratteri alfanumerici e speciali che devono corrispondere a un valore basato sulla chiave definita nella definizione dell'attributo.	Application1

Gestione delle credenziali

La AWS soluzione Cloud Migration Factory on include un Credentials Manager che si integra con AWS Secrets Manager all'interno dell'account in cui viene distribuita l'istanza. La funzionalità consente agli amministratori di salvare le credenziali di sistema in AWS Secrets Manager per utilizzarle negli script di automazione senza fornire agli utenti l'accesso per recuperare direttamente le credenziali o dover fornire l'accesso degli utenti a Secrets Manager. AWS Gli utenti possono selezionare le credenziali archiviate in base al nome e alla descrizione quando le forniscono a un processo di automazione. Il processo di automazione recupererà quindi solo le credenziali richieste durante l'esecuzione sul server di automazione e, a questo punto, il ruolo IAM allocato all'istanza EC2 verrà utilizzato per accedere ai segreti richiesti.

L'area di amministrazione di Credentials Manager è visibile solo agli utenti che sono membri del gruppo di amministratori all'interno di Amazon Cognito. Gli utenti non amministratori potranno visualizzare i nomi e le descrizioni delle credenziali solo se vi si fa riferimento tramite un'automazione o una relazione tra altri record.

I seguenti tre tipi di segreti possono essere archiviati in AWS Secrets Manager tramite Credentials Manager.

Credenziali del sistema operativo: sotto forma di `username` e `password`

Chiave/valore segreto: sotto forma di `e. key value`

Testo semplice: sotto forma di una singola stringa di testo semplice.

Aggiungi un segreto

1. Scegli Aggiungi dall'elenco dei segreti di Credential Manager.
2. Seleziona il tipo di segreto da aggiungere.
3. Inserisci un nome segreto. Sarà lo stesso nome che verrà visualizzato all'interno di AWS Secrets Manager per il nome segreto.
4. Inserisci una descrizione segreta. Questa sarà la stessa descrizione che verrà visualizzata all'interno di AWS Secrets Manager per la descrizione segreta.
5. Inserisci le informazioni sulle credenziali per il tipo segreto.

Note

Per il tipo segreto delle credenziali del sistema operativo, è disponibile un'opzione per selezionare il tipo di sistema operativo a cui è possibile fare riferimento negli script personalizzati.

Modifica un segreto

Ad eccezione del nome e del tipo del segreto, è possibile modificare tutte le proprietà del segreto utilizzando l'interfaccia utente di Credentials Manager.

Eliminare un segreto

Dalla vista di Credentials Manager, selezionate il segreto che desiderate eliminare e scegliete Elimina. L'eliminazione del segreto verrà pianificata in AWS Secrets Manager, operazione che potrebbe richiedere alcuni minuti. Qualsiasi tentativo di aggiungere un nuovo segreto con lo stesso nome durante questo periodo avrà esito negativo.

Esegui l'automazione dalla console

La AWS soluzione Cloud Migration Factory on fornisce un motore di automazione che consente agli utenti di eseguire lavori sotto forma di script sull'inventario all'interno del datastore. Con questa funzionalità, puoi gestire, personalizzare e implementare tutte le automazioni necessarie per completare le attività di migrazione. end-to-end

I lavori avviati da AWS CMF vengono eseguiti su server di automazione che possono essere ospitati in sede o in sede. Cloud AWS Questi server devono eseguire Windows con l'agente AWS SSM installato, oltre a Python e Microsoft. PowerShell Puoi anche installare altri framework, se necessario, per le automazioni personalizzate. [Fare riferimento alla Fase 6. Crea un server di automazione della migrazione](#) per i dettagli sulla build del server di automazione. È necessario almeno un server di automazione per eseguire i lavori dalla console AWS CMF.

Durante l'implementazione, è possibile utilizzare gli script per le attività più comuni necessarie per riospitare i carichi di lavoro utilizzando MGN. AWS Scaricate gli script dall'interfaccia web e usateli come punto di partenza per script personalizzati. Per i dettagli sulla creazione di script di automazione personalizzati, consulta Gestione [degli script](#).

Per avviare un processo dalla console, seleziona un'ondata su cui eseguire l'automazione, quindi seleziona Azioni e scegli Esegui automazione. In alternativa, puoi selezionare un lavoro su cui eseguire l'automazione, quindi selezionare Azioni e scegliere Esegui automazione.

Da Run Automation:

1. Inserisci il Job Name. Questo verrà utilizzato per identificare il lavoro nel registro.

 Note

I nomi dei lavori non devono essere necessariamente univoci, poiché a tutti i lavori vengono assegnati anche un ID univoco e timestamp per identificarli ulteriormente.

2. Seleziona il nome dello script dall'elenco. Questo è un elenco di tutti gli script che sono stati caricati nell'istanza AWS CMF. Quando il lavoro viene inviato, verrà eseguita la versione predefinita dello script selezionato. Per controllare i dettagli dello script, inclusa la versione predefinita corrente, scegli Dettagli correlati sotto il nome dello script. Fate riferimento a Modifica della versione predefinita del pacchetto di script per informazioni dettagliate sull'aggiornamento della versione predefinita degli script. Quando si seleziona lo script da eseguire, i parametri richiesti vengono visualizzati in Argomenti dello script.

3. Dall'ID dell'istanza, seleziona il server di automazione per il lavoro dall'elenco.

 Note

L'elenco mostrerà solo le istanze in cui è installato l'agente SSM e in cui l'istanza EC2, o per i server di automazione ospitati non EC2, è impostato su `role mf_automation`

4. In Script Arguments, inserisci gli argomenti di input richiesti per lo script.

5. Dopo aver inserito tutti i parametri richiesti e averli verificati, scegli Invia Automation Job.

Quando invii il lavoro di automazione, viene avviato il seguente processo:

1. Verrà creato un record di lavoro con la vista AWS Cloud Migration Factory Jobs contenente i dettagli del lavoro e lo stato corrente.

2. Verrà creato un processo di automazione AWS Systems Manager e inizierà a eseguire il documento di automazione SSM di AWS Cloud Migration Factory sul server di automazione fornito tramite l'ID istanza. Il documento di automazione:
 - a. Scarica la versione corrente predefinita del pacchetto di script dal bucket AWS Cloud Migration Factory S3 al server di automazione nella **C:\migration\scripts** directory.
 - b. Decomprime e verifica il pacchetto.
 - c. Avvia lo script python del file principale specificato nell'allegato allo zip. `package-structure.yml`
3. Una volta avviato lo script python del file master, qualsiasi output dello script viene acquisito dall'agente SSM e inserito. CloudWatch Viene quindi acquisito regolarmente e archiviato nel datastore di AWS Cloud Migration Factory con il record del lavoro originale, fornendo un controllo completo del lavoro eseguito.
 - a. Se lo script richiede credenziali per AWS Cloud Migration Factory, lo script contatterà AWS Secrets Manager per ottenere le credenziali dell'account del servizio. Se le credenziali sono errate o non sono presenti, lo script restituirà un errore.
 - b. Se lo script richiede di accedere ad altri segreti archiviati utilizzando la funzionalità AWS Cloud Migration Factory Credentials Manager, contatterà AWS Secrets Manager per accedere a tali credenziali. Se ciò non è possibile, lo script restituirà un errore.
4. Una volta terminato lo script python del file master, il risultato di questo script determinerà lo stato fornito al job record di AWS Cloud Migration Factory. Un ritorno diverso da zero verrà impostato su. `Job Status Failed`

Note

Attualmente, se si verifica un errore nell'esecuzione iniziale del documento AWS SSM, questo non viene visualizzato nell'interfaccia web. Gli errori vengono registrati solo dopo l'avvio del file master python.

Tutti i processi avviati dalla console scadranno dopo 12 ore se non hanno restituito lo stato di successo o di fallimento.

Esegui le automazioni dal prompt dei comandi

Sebbene sia consigliabile eseguire i lavori di automazione tramite l'interfaccia Web, è possibile eseguire gli script di automazione manualmente da una riga di comando sul server di automazione.

Ciò fornisce opzioni aggiuntive laddove le organizzazioni non possono o non vogliono utilizzare la combinazione di AWS CMF Credentials Manager, AWS Secrets Manager e AWS Systems Manager nell'ambiente, o se Cloud Migration Factory su AWS gli utenti devono fornire codici di accesso monouso per l'autenticazione a più fattori (MFA) per accedere a Cloud Migration Factory. AWS

Quando gli script vengono eseguiti dalla riga di comando, la cronologia e i log dei processi non sono disponibili nella vista Jobs dell'interfaccia web. L'output del registro verrà indirizzato solo all'output della riga di comando. Gli script possono comunque accedere a Cloud Migration Factory sulle AWS API per leggere e aggiornare i record e altre funzioni disponibili tramite le API.

Ti consigliamo di archiviare gli script nella libreria di script o in un'altra posizione centrale per assicurarti di accedere e utilizzare la versione più recente dello script o la versione attualmente approvata per l'uso.

Esecuzione manuale di un pacchetto di automazione

Questa sezione descrive i passaggi per scaricare un pacchetto da Cloud Migration Factory AWS ed eseguirlo manualmente sul server di automazione. Puoi anche seguire la procedura per altre posizioni di origine degli script sostituendo i passaggi 1 e 2 con i passaggi di download specifici della fonte.

1. Se gli script sono archiviati in Cloud Migration Factory on AWS, segui i passaggi descritti in [Scaricare i pacchetti di script](#) per ottenere il file zip del pacchetto di automazione.
2. Copia il file zip in una posizione sul server di automazione, ad esempio `c:\migrations\scripts`, e decomprimi il contenuto.
3. Copia il `FactoryEndpoints.json` file in ciascuna cartella di script decompressa. Configura il file con gli endpoint API specifici per l'istanza di Cloud Migration Factory che contiene i server o altri record a cui farà riferimento questo job di automazione. Per ulteriori informazioni su come [creare questo file, consulta Creazione del FactoryEndpoints file.json](#).
4. Dalla riga di comando, assicurati di trovarti nella directory principale del pacchetto decompresso ed esegui il comando seguente:

```
python [package master script file] [script arguments]
```

file di script principale del pacchetto: può essere ottenuto da `Package-Structure.yml` sotto la `MasterFileName` chiave.

argomenti dello script: le informazioni sugli argomenti sono fornite `Package-Structure.yml` sotto la `Arguments` chiave.

5. Gli script richiederanno le credenziali necessarie per Cloud Migration Factory sulle AWS API e sul server remoto. Tutte le credenziali inserite manualmente vengono memorizzate nella cache per tutta la durata di questo processo per evitare di reinserire le stesse credenziali. Se si immettono argomenti di script per accedere ai segreti archiviati utilizzando la funzionalità `Credentials Manager`, è necessario accedere a `AWS Secrets Manager` e ai segreti associati. Se il recupero dei segreti fallisce per qualsiasi motivo, lo script richiederà le credenziali dell'utente.

Creazione del file `json FactoryEndpoints`

Consigliamo di creare questo file una sola volta durante la distribuzione di Cloud Migration Factory sulla soluzione AWS, poiché il contenuto non cambia dopo la distribuzione iniziale e viene archiviato in una posizione centrale sul server di automazione. Questo file fornisce gli script di automazione con Cloud Migration Factory sugli endpoint delle API AWS e altri parametri chiave. Di seguito viene mostrato un esempio del contenuto predefinito del file:

```
{
  "UserApiUrl":
  "https://cmfuserapi.execute-api.us-east-1.amazonaws.com",
  "Region": "us-east-1",
  "UserPoolId": "us-east-1_AbCdEfG",
  "UserPoolClientId": "123456abcdef7890ghijk",
  "LoginApiUrl":
  "https://cmfloginapi.execute-api.us-east-1.amazonaws.com"
}
```

Note

La maggior parte delle informazioni necessarie per comporre questo file per un'istanza di AWS Cloud Migration Factory distribuita è disponibile nella scheda `AWS CloudFormation Output` dello stack distribuito, ad eccezione di `UserPoolClientId`. Ottieni questo valore completando i seguenti passaggi:

1. Passa alla console di Amazon Cognito.
2. Aprire la configurazione del pool di utenti.

3. Seleziona l'integrazione dell'app, che fornirà la configurazione del client dell'app.

```
{
  "UserApiUrl": <UserApi-value>,
  "Region": <Region-value>,
  "UserPoolId": <UserPoolId-value>,
  "UserPoolClientId": <Amazon-Cognito-user-pool-app-clients-console>,
  "LoginApiUrl": <LoginApi-value>
}
```

Sostituisci *< LoginApi -value>*, *< UserApi -value>* *<Region-value>*e *< UserPoolId -value>* con i valori corrispondenti recuperati dalla console Outputs. *AWS CloudFormation* Non aggiungete una barra (/) alla fine degli URL.

Il file ha una chiave opzionale `DefaultUser`. È possibile impostare il valore di questa chiave sull'ID utente predefinito da utilizzare per accedere a Cloud Migration Factory su AWS istanza per evitare di doverla inserire ogni volta. Quando viene richiesto l'ID utente di Cloud Migration Factory, è possibile inserire un ID utente o utilizzare il valore predefinito premendo il tasto invio. È possibile farlo solo quando gli script vengono eseguiti manualmente.

Avvia i lavori AWS MGN da Cloud Migration Factory

La AWS soluzione Cloud Migration Factory on ha integrato l'automazione per avviare e gestire la migrazione di Rehost utilizzando MGN. AWS Queste automazioni consentono ai team di migrazione di gestire tutti gli aspetti della migrazione da un'unica interfaccia utente, combinando le azioni chiave disponibili nella console di servizio AWS MGN, con la libreria di automazione AWS Cloud Migration Factory che estende la funzionalità con script predefiniti per le migrazioni di massa, che aiuta ad aumentare la velocità delle attività di migrazione. Consulta l'Elenco delle attività di migrazione automatizzate per AWS Application Migration Service (AWS MGN) per un elenco completo dei lavori di automazione MGN disponibili. AWS L'utilizzo di AWS Cloud Migration Factory offre anche migrazioni di più account senza interruzioni utilizzando AWS MGN, poiché Cloud Migration Factory ha la capacità di assumere automaticamente ruoli in diversi account di destinazione in base all'applicazione Cloud Migration Factory e alle definizioni del server da migrare.

Attività prerequisite

1. Account Target AWS CMF CloudFormation distribuito in ogni account di destinazione. Per ulteriori informazioni, consulta la sezione [AWS CloudFormation modelli di](#) questo documento.

2. [AWS MGN viene inizializzato in ogni account di destinazione.](#)

Definizione iniziale

La definizione dell'inventario locale viene eseguita tramite la creazione di elementi wave, applicativi e server utilizzando l'interfaccia utente o tramite l'importazione di un modulo di immissione CSV. Queste definizioni vengono utilizzate per fornire le identità dei server locali e anche i parametri EC2 di destinazione e altri dati necessari per gestire l'attività di migrazione.

Definizione dell'interfaccia utente

Per utilizzare la funzionalità AWS MGN, è necessario creare un record wave, con i record delle applicazioni associati e infine uno o più record del server associati alle applicazioni. Il record wave viene utilizzato per raggruppare le applicazioni e non fornisce parametri per l'automazione, mentre il record dell'applicazione definisce l' Account AWS ID di destinazione e verso il Regione AWS quale verrà migrata l'applicazione. I record del server forniscono alle azioni di automazione e all'integrazione con AWS MGN i parametri di destinazione per le istanze EC2, come il tipo di istanza, le sottoreti, i gruppi di sicurezza, ecc.

Quando si definisce un server nel datastore AWS CMF da utilizzare con la funzionalità AWS MGN, il server deve essere configurato con una strategia di migrazione di Rehost. Una volta selezionato Rehost, gli attributi aggiuntivi richiesti per questa funzionalità verranno visualizzati sullo schermo. È necessario compilare i seguenti attributi per avviare correttamente un processo di migrazione AWS MGN:

Richiesto

Famiglia di sistemi operativi server: imposta su linux o windows a seconda della famiglia di sistemi operativi.

Versione del sistema operativo del server: imposta la versione dettagliata del sistema operativo in esecuzione sul server.

Tipo di istanza: tipo di istanza EC2 da utilizzare.

Tenancy: hosting condiviso, host dedicato.

ID dei gruppi di sicurezza: elenco dei gruppi di sicurezza che verranno assegnati all'istanza quando verrà avviato il cutover finale.

ID dei gruppi di sicurezza - Test: elenco dei gruppi di sicurezza che verranno assegnati all'istanza all'avvio del test.

Condizionale

ID di sottorete: ID di sottorete a cui assegnare questa istanza EC2 quando viene avviato il cutover finale. (non applicabile quando è specificato l'ID dell'interfaccia di rete)

Subnet Ids - Test — ID di sottorete a cui assegnare questa istanza EC2 all'inizio del test. (non applicabile se è specificato Network Interface ID -Test)

Network Interface ID: ENI ID da utilizzare quando viene avviato il cutover finale.

Network Interface ID - Test - ENI ID da utilizzare all'inizio del test.

ID host dedicato: ID host dedicato su cui verrà avviata l'istanza. (applicabile solo quando Tenancy è impostata su Host dedicato).

Facoltativo

Tag: tag delle istanze EC2 da applicare all'istanza.

Tutti gli altri attributi non elencati qui non influiscono in alcun modo sui lavori AWS MGN avviati dall'interno della AWS soluzione CMF.

Definizione del modulo di assunzione

I moduli di immissione possono contenere i dettagli per creare o aggiornare più tipi di record con il datastore in un'unica riga del file csv, ciò consente l'importazione dei dati correlati. Nell'esempio seguente, i record wave, application e server verranno creati e messi in relazione tra loro automaticamente durante l'importazione.

Per importare il modulo di immissione, segui la stessa procedura utilizzata per le altre importazioni di dati in Cloud Migration Factory sulla AWS soluzione descritta in [Importazione di dati](#).

Avvio di un lavoro

L'avvio di un lavoro AWS MGN da AWS CMF viene eseguito in base a un'ondata, dalla visualizzazione dell'elenco delle ondate selezionate la ondata, quindi da Azioni selezionate Rehost > MGN.

Questa schermata richiede all'utente di effettuare le seguenti scelte prima di poter inviare il lavoro.

1. Seleziona l'azione AWS MGN da eseguire sulle applicazioni e sui server inclusi nell'ondata. Queste azioni replicano principalmente quelle disponibili nella console di servizio AWS MGN e nell'API, ad eccezione di Validate Launch Template (vedi sotto per i dettagli su questa azione). Per i dettagli sugli effetti di ciascuna azione, consulta la guida per l'utente di AWS MGN.
2. Seleziona l'onda contro cui eseguire l'azione.
3. Seleziona le applicazioni dall'ondata in cui verrà eseguita l'azione. Questo elenco mostrerà solo le applicazioni associate all'onda selezionata.
4. Una volta che tutte le opzioni sono corrette, scegli Invia.

L'automazione avvierà ora l'azione selezionata sulla destinazione di ciascuna applicazione selezionata Account AWS, come specificato nel record dell'applicazione. I risultati dell'azione verranno visualizzati nel messaggio di notifica, inclusi eventuali errori.

Convalida il modello di lancio

Questa azione viene utilizzata per verificare che i dati di configurazione memorizzati in CMF per ogni server siano validi prima di tentare le attività di cutover. Per eseguire questa azione, è necessario aver distribuito correttamente gli agenti AWS MGN sul server di origine.

Le convalide eseguite per ogni server sono:

- Verifica che il tipo di istanza sia valido.
- Verifica l'esistenza del profilo dell'istanza IAM.
- Esistono gruppi di sicurezza sia in fase di test che in modalità live.
- Le sottoreti esistono sia per test che per live (se ENI non è specificato).
- Esiste un host dedicato (se specificato).
 - Se viene specificato un host dedicato, vengono effettuati i seguenti controlli:
 - L'host dedicato supporta il tipo di istanza specificato?
 - L'host dedicato dispone di capacità libera per tutti i requisiti di questa ondata, in base ai tipi di istanze richiesti?
- L'ENI esiste (se specificato).

I risultati dell'azione verranno visualizzati nel messaggio di notifica, compresi gli eventuali errori.

Ripiattaforma su EC2

La AWS soluzione Cloud Migration Factory on consente di avviare automaticamente gruppi di istanze EC2 dalle configurazioni definite nel relativo datastore; implementando istanze EC2 con volumi EBS collegati. Ciò offre la possibilità di fornire nuove istanze EC2, permettendo a Replatform di utilizzare e riospitare server locali con MGN all'interno di un'unica AWS CloudFormation interfaccia utente CMF. AWS Prima di poter utilizzare questa funzionalità, il datastore deve contenere la definizione dei server. Una volta risolto questo problema, i server devono essere collegati a un'onda. Quando viene presa la decisione di avviare le istanze EC2, l'utente può avviare le seguenti azioni contro l'ondata:

- Convalida dell'input EC2
- EC2 Genera modello CF
- Implementazione EC2

Prerequisiti

Autorizzazioni per aggiungere l'accesso all'attributo Replatform.

Configurazione iniziale

La configurazione delle nuove istanze EC2 viene eseguita tramite la creazione di nuovi elementi del server utilizzando l'interfaccia utente o tramite l'importazione di un modulo di immissione CSV contenente gli elementi del server. Queste definizioni vengono convertite in modelli di Cloud AWS Formation archiviati in un bucket S3 all'interno dello stesso in Account AWS cui viene distribuita l'istanza CMF. AWS

Definizione dell'interfaccia utente

Quando si definisce un server nel datastore di AWS Cloud Migration Factory da utilizzare con la funzionalità Replatform to EC2, il server deve essere configurato con una strategia di migrazione di Replatform. Una volta selezionato Replatform, gli attributi aggiuntivi richiesti per questa funzionalità verranno visualizzati sullo schermo. Affinché la funzionalità funzioni, è necessario compilare i seguenti attributi:

Attributi obbligatori

ID AMI: ID dell'Amazon Machine Image utilizzato per avviare l'istanza EC2.

Zona di disponibilità: la zona in cui verrà distribuita l'istanza EC2.

Dimensione del volume principale: dimensione in GB del volume principale dell'istanza.

Tipo di istanza: tipo di istanza EC2 da utilizzare.

ID dei gruppi di sicurezza: elenco dei gruppi di sicurezza assegnati all'istanza.

Subnet Ids: ID di sottorete a cui assegnare questa istanza EC2.

Tenancy: attualmente l'unica opzione supportata per l'integrazione da Replatform a EC2 è Shared, mentre ogni altra opzione verrà sostituita da Shared al momento della generazione del modello.

Attributi facoltativi

Abilita monitoraggio dettagliato: seleziona questa opzione per abilitare il monitoraggio dettagliato.

Nomi di volume aggiuntivi: elenco di nomi di volume EBS aggiuntivi. Ogni elemento dell'elenco deve corrispondere alla stessa riga degli elenchi Dimensioni e Tipo.

Dimensioni di volume aggiuntive: elenco di dimensioni di volume EBS aggiuntive. Ogni elemento dell'elenco deve essere mappato sulla stessa riga degli elenchi Nomi e Tipi.

Tipi di volume aggiuntivi: elenco di tipi di volume EBS aggiuntivi. Ogni elemento dell'elenco deve corrispondere alla stessa riga degli elenchi Nomi e Dimensioni, se non viene specificato, il valore predefinito è gp2 per tutti i volumi.

ID chiave EBS KMS per la crittografia dei volumi: se i volumi EBS verranno crittografati, specifica l'ID chiave, l'ARN della chiave, l'alias della chiave o l'alias ARN.

Abilita EBS Optimized: seleziona per attivare EBS Optimized.

Nome del volume principale: seleziona una delle opzioni fornite, se non viene specificato, verrà utilizzato l'ID.

Tipo di volume principale: fornisce il tipo EBS del volume da creare, se non specificato, il valore predefinito è gp2.

Definizione del modulo di immissione

I moduli di immissione possono contenere i dettagli per creare o aggiornare più tipi di record con il datastore in un'unica riga del file csv, ciò consente l'importazione dei dati correlati. Nell'esempio

seguito, i record wave, application e server verranno creati e correlati tra loro automaticamente durante l'importazione.

Esempio: modulo di assunzione

Nome colonna	Dati di esempio	Richiesto	Note
wave_name	onda 1	Sì	
Nome_App	app 1	Sì	
aws_accountid	1234567890	Sì	
nome_server	Server 1	Sì	
server_fqdn	Server 1	Sì	
famiglia_server_os_	linux	Sì	
versione_os_server	Amazon	Sì	
livello_server	App	No	
ambiente_server	Sviluppatore	No	
ID_subnet	sottorete-xxxxxxx	Sì	
SecurityGroup_IDS	sg-yyyyyyyyyy	Sì	
instanceType	m5.large	Sì	
Sono Role	ruolo personalizzato ec2	No	
tenancy	Condiviso	Sì	
tipo_r	Conversione piattaforma	Sì	
root_vol_size	50	Sì	
ami_id	ami-zzzzzzzzzz	Sì	

Nome colonna	Dati di esempio	Richiesto	Note
zona di disponibilità	us-west-2a	Sì	
root_vol_type	gp2	No	
aggiunge_vols_size	40:100	No	
add_vols_type	gp2: gp3	No	
ebs_optimized	false	No	
ebs_kmskey_id	1111-1111-1111-1111	No	
monitoraggio_dettagliato	true	No	
root_vol_name	Server1_root_volume	No	
add_vols_name	server1_root_volumeA: Server1_root_volumeB	No	

Per importare il modulo di immissione, segui la stessa procedura di qualsiasi altra importazione di dati nella soluzione Cloud Migration Factory on. AWS

Azioni di distribuzione

Convalida dell'input EC2

Dopo aver definito i parametri dell'istanza, devi prima eseguire l'azione wave: Replatform > EC2 > EC2 Input Validation. Questa azione verifica che siano stati forniti tutti i parametri corretti per ciascun server al fine di creare un modello valido. CloudFormation

Note

Attualmente questa convalida non verifica che i parametri di input siano validi, ma solo che siano presenti in ogni definizione del server. È necessario verificare i valori corretti prima di creare il modello, altrimenti la distribuzione del modello avrà esito negativo.

EC2 genera un modello CloudFormation

Una volta verificate le definizioni per tutti i server inclusi in un'ondata, è possibile generare il CloudFormation modello. Per fare ciò, esegui l'azione wave: Replatform > EC2 > EC2 Genera CF Template. Questa azione crea un CloudFormation modello per ogni applicazione del wave, in cui i server dell'applicazione hanno una strategia di migrazione di Replatform; eventuali server con altre strategie di migrazione definite non verranno inclusi nel modello.

Una volta eseguiti, i modelli per ogni applicazione verranno archiviati nel bucket S3: [prefisso specifico dell'istanza]-gfbuid-cftemplates, che è stato creato automaticamente quando è stata distribuita la soluzione Cloud Migration Factory on. AWS La struttura delle cartelle di questo bucket è la seguente:

- [ID AWS account Target]
 - [Nome dell'onda]
 - CFN_Template_[ID applicazione]_[Nome applicazione].yaml

Ogni volta che viene eseguita l'azione di generazione, una nuova versione del modello viene archiviata nel bucket S3. Gli URI S3 per i modelli verranno forniti nella notifica; questi modelli possono essere esaminati o modificati secondo necessità prima della distribuzione.

Attualmente i CloudFormation modelli generano i seguenti tipi di risorse: CloudFormation

- AWS: :EC2: :Instance
- AWS: :EC2: :Volume
- AWS: :EC2:: VolumeAttachment

Implementazione EC2

Una volta che sei pronto per implementare le nuove istanze EC2, puoi avviare l'azione di implementazione EC2 tramite l'azione wave Replatform > EC2 > EC2 Deployment. Questa azione utilizzerà la versione più recente del CloudFormation modello per ogni applicazione inclusa nella ondata e distribuirà questi modelli negli account di destinazione selezionati, tramite. AWS CloudFormation

Gestione degli script

La AWS soluzione Cloud Migration Factory on consente agli utenti di gestire completamente la libreria di script o pacchetti di automazione all'interno dell'interfaccia utente. È possibile caricare nuovi script personalizzati e nuove versioni dello script utilizzando l'interfaccia di gestione degli script. Quando sono disponibili più versioni, un amministratore può passare da una versione all'altra, dando la possibilità di testare gli aggiornamenti prima di renderli predefiniti. L'interfaccia di gestione degli script consente inoltre agli amministratori di scaricare pacchetti di script per aggiornare o rivedere il contenuto.

Un pacchetto di script supportato è un archivio zip compresso contenente i seguenti file obbligatori nella directory principale:

- `Package-Structure.yml` — Utilizzato per definire gli argomenti dello script e altri metadati, come la descrizione e il nome predefinito. Per maggiori dettagli, consulta [Composizione di un nuovo pacchetto di script](#).
- `[script python personalizzato].py` — Questo è lo script iniziale che verrà eseguito quando viene inviato un lavoro. Questo script può richiamare altri script e moduli e, in tal caso, questi devono essere inclusi nell'archivio. Il nome di questo script deve corrispondere al valore specificato nella `MasterFileName` chiave in `Package-Structure.yml`

Carica un nuovo pacchetto di script

Note

Un pacchetto di script deve essere conforme al formato supportato. Per maggiori dettagli, [consulta Composizione di un nuovo pacchetto di script](#).

1. Scegli Aggiungi nella tabella Script di automazione.
2. Seleziona il file di archivio del pacchetto che desideri caricare.
3. Immettete un nome univoco per lo script. Gli utenti faranno riferimento allo script con questo nome per avviare i lavori.

Scarica i pacchetti di script

Puoi scaricare pacchetti di script dalla console per attivare gli aggiornamenti e la verifica dei contenuti.

1. Seleziona Automazione, quindi Script.
2. Seleziona lo script che desideri scaricare dalla tabella, quindi seleziona Azioni e scegli Scarica la versione predefinita o Scarica la versione più recente.

Puoi scaricare versioni specifiche di uno script. Per farlo, seleziona lo script, quindi Azioni e scegli Cambia versione predefinita. Dall'elenco Versione predefinita dello script, scegli Scarica la versione selezionata.

Aggiungi una nuova versione di un pacchetto di script

Gli aggiornamenti ai pacchetti di script di AWS Cloud Migration Factory possono essere caricati nella sezione Automazione > Script seguendo questi passaggi:

1. Seleziona Automazione, quindi Script.
2. Seleziona lo script esistente per aggiungere una nuova versione, quindi seleziona Azioni e scegli Aggiungi nuova versione.
3. Seleziona il file di archivio del pacchetto aggiornato che desideri caricare e scegli Avanti. La nuova versione dello script manterrà il nome esistente per impostazione predefinita. Immettete un nome di script univoco. Qualsiasi modifica del nome verrà applicata solo a questa versione dello script.
4. È possibile rendere la nuova versione dello script la versione predefinita selezionando Imposta versione predefinita.
5. Scegli Carica.

Eliminazione di pacchetti e versioni di script

Non è possibile eliminare script o versioni di uno script a scopo di controllo. Ciò consente di esaminare lo script esatto che è stato eseguito su un sistema in un determinato momento. Ogni versione dello script ha una firma e un ID univoci al momento del caricamento, che vengono registrati nella cronologia del lavoro in cui sono stati utilizzati lo script e la versione.

Composizione di un nuovo pacchetto di script

I pacchetti di AWS script di Cloud Migration Factory supportano Python come linguaggio di scripting principale. È possibile avviare altri linguaggi di shell scripting come richiesto dall'interno di un programma principale o wrapper Python. Per creare rapidamente un nuovo pacchetto di script, consigliamo di scaricare una copia di uno degli script preconfezionati e di aggiornarlo per eseguire l'operazione richiesta. È necessario innanzitutto creare uno script Python master che esegua le funzionalità principali dello script. Quindi, create un `Package-Structure.yml` file per definire gli argomenti e gli altri metadati richiesti dallo script. Fate riferimento alle `Package-Structure.yml` opzioni per maggiori dettagli.

Script principale in Python

Questo è lo script principale iniziale che viene eseguito quando viene avviato un processo. Una volta completata l'esecuzione dello script, l'attività è terminata e il codice restituito finale determina lo stato del lavoro. Tutto l'output di questo script viene acquisito quando viene eseguito in remoto e passato come riferimento nel registro di controllo dell'output del lavoro. Questo registro viene archiviato anche in Amazon CloudWatch.

Accesso a Cloud Migration Factory su AWS dati e API da uno script

Per fornire l'accesso a Cloud Migration Factory su AWS API e dati, puoi utilizzare il modulo di supporto python incluso. Il modulo fornisce le seguenti funzioni comuni:

Accesso in fabbrica

Restituisce un token di accesso che può essere utilizzato per chiamare Cloud Migration Factory sulle API. AWS Questa funzione tenterà di accedere a CMF utilizzando una serie di tentativi di credenziali:

1. Tentando di accedere al segreto predefinito contenente l'ID utente e la password dell'account di servizio, se esiste e l'accesso è consentito. Questo nome segreto MF ServiceAccount - **[*userpool id*]** verrà verificato.
2. Se il passaggio 1 non ha esito positivo e l'utente sta eseguendo lo script dalla riga di comando, all'utente verrà richiesto di fornire un ID utente e una password di AWS Cloud Migration Factory. Se eseguito da un processo di automazione remoto, il processo avrà esito negativo.

getServerCredentials

Restituisce le credenziali di accesso per un server archiviato in AWS Cloud Migration Factory in Credentials Manager o tramite l'input dell'utente. Questa funzione controllerà una serie di fonti diverse per determinare le credenziali per un server specifico, l'ordine delle fonti è:

1. Se `local_username` e `local_password` sono impostati e validi, verranno restituiti.
2. Se `secret_override` è impostato, questo verrà utilizzato per recuperare il segreto specificato da AWS Secret Manager, altrimenti, controlla se il record del server contiene la chiave `secret_name` e questa non è vuota, verrà utilizzato questo nome segreto.
3. Se si verifica un errore nell'individuazione o nell'accesso ai segreti specificati, la funzione tornerà a richiedere all'utente le credenziali, ma solo se `no_user_prompts` è impostato su `False`, altrimenti restituirà un errore.

Parametri

`local_username` — Se passato, verrà restituito.

`local_password` — Se passato, verrà restituito.

`server`: nome del server, come memorizzato nell'attributo `server_name` in Cloud Migration Factory.
AWS

`Secret_override` — Viene passato questo imposterà il nome segreto da recuperare da Secrets Manager per questo server.

`no_user_prompts` — Indica alla funzione di non richiedere all'utente un ID utente e una password se non sono memorizzati, questo dovrebbe essere vero per qualsiasi script di automazione remota.

getCredentials

Ottiene le credenziali archiviate utilizzando AWS Cloud Migration Factory Credentials Manager da Secrets Manager.

Parametri

`secret_name` — nome del segreto da recuperare.

get_factory_servers

Restituisce una serie di server dal datastore di AWS Cloud Migration Factory in base al `waveid` fornito.

Parametri

Waveid: ID del record Wave dei server che verranno restituiti.

Token: token di autenticazione ottenuto dalla funzione FactoryLogin Lambda.

UserHost: URL dell'endpoint dell'API utente di AWS Cloud Migration Factory.

OSSplit: se impostato su `true`, verranno restituiti due elenchi, uno per i server Linux e uno per Windows, se `False`, verrà restituito un unico elenco combinato.

Riepilogo finale del messaggio

Si consiglia di fornire un messaggio di riepilogo del risultato dello script come output finale sullo schermo o sul `sysout`. Questo verrà visualizzato sulla console nella proprietà Last Message, che fornisce uno stato rapido del risultato dello script senza che l'utente debba leggere l'intero registro di output.

Codice di ritorno

Lo script python principale dovrebbe restituire un codice di ritorno diverso da zero all'uscita se la funzione dello script non è stata completamente riuscita. Alla ricezione di un codice di ritorno diverso da zero, lo stato del processo verrà visualizzato come Failed nel log dei lavori, indicando all'utente che deve esaminare il log di output per i dettagli dell'errore.

Opzioni YAML Package-Structure.yml

File YAML di esempio

```
Name: "0-Check MGN Prerequisites"
Description: "This script will verify the source servers meet the basic requirements
  for AWS MGN agent installation."
MasterFileName: "0-Prerequisites-checks.py"
UpdateUrl: ""
Arguments:
-
  name: "ReplicationServerIP"
  description: "Replication Server IP."
  long_desc: "IP Address of an AWS MGN Replication EC2 Instance."
  type: "standard"
  required: true
-
  name: "SecretWindows"
  long_desc: "Windows Secret to use for credentials."
  description: "Windows Secret"
```

```

type: "relationship"
rel_display_attribute: "Name"
rel_entity: "secret"
rel_key: "Name"
-
name: "SecretLinux"
long_desc: "Linux Secret to use for credentials."
description: "Linux Secret"
type: "relationship"
rel_display_attribute: "Name"
rel_entity: "secret"
rel_key: "Name"
-
name: "Waveid"
description: "Wave Name"
type: "relationship"
rel_display_attribute: "wave_name"
rel_entity: "wave"
rel_key: "wave_id"
validation_regex: "^(?!\\s*$).+"
validation_regex_msg: "Wave must be provided."
required: true
SchemaExtensions:
-
schema: "server"
name: "server_pre_reqs_output"
description: "Pre-Req Output"
type: "string"

```

Descrizioni delle chiavi YAML

Richiesto

Nome: nome predefinito che lo script utilizzerà durante l'importazione.

Descrizione: descrizione dell'utilizzo dello script.

MasterFileName— Questo è il punto di partenza per l'esecuzione dello script, deve essere un nome di file Python incluso nell'archivio del pacchetto dello script.

Argomenti — Un elenco di argomenti accettati dallo script MasterFileName Python. Ogni argomento da specificare è nel formato di definizione degli attributi di AWS Cloud Migration Factory. Le proprietà obbligatorie per ogni argomento sono Name e Type, tutte le altre proprietà sono opzionali.

Facoltativo

UpdateUrl— Fornite un URL in cui è disponibile il codice sorgente del pacchetto di script per fornire gli aggiornamenti. Attualmente è solo di riferimento.

SchemaExtensions— Un elenco di attributi che lo script Python richiede che siano presenti nello schema per memorizzare l'output o recuperare dati aggiuntivi. Ogni attributo deve essere specificato nel formato di definizione degli attributi AWS CMF. Le proprietà richieste per ogni attributo sono Schema, Nome, Descrizione e Tipo. Tutte le altre proprietà sono facoltative. Tutti i nuovi attributi verranno aggiunti automaticamente allo schema al momento del caricamento iniziale dello script e le modifiche non SchemaExtensions verranno elaborate per le nuove versioni dello script. Se ciò è necessario per aggiungere un nuovo script, è necessario aggiornare manualmente lo schema.

Gestione dello schema

La AWS soluzione Cloud Migration Factory on fornisce un repository di metadati completamente estensibile, che consente di archiviare i dati per l'automazione, il controllo e il monitoraggio dello stato in un unico strumento. Il repository fornisce un set predefinito di entità (Waves, Applicazioni, Server e Database) e attributi al momento della distribuzione per consentirti di iniziare a catturare e utilizzare i dati utilizzati più di frequente e da qui puoi personalizzare lo schema secondo necessità.

Solo gli utenti del gruppo di amministratori di Cognito dispongono delle autorizzazioni per gestire lo schema. Per rendere un utente membro dell'amministratore o di altri gruppi, consulta [Gestione utenti](#).

Vai a Amministrazione e seleziona Attributi per le schede delle entità predefinite. Le seguenti schede sono disponibili per supportare la gestione dell'entità.

Attributi: consente di aggiungere, modificare ed eliminare attributi.

Pannello informazioni: consente di modificare il contenuto della guida del pannello Informazioni, visualizzato a destra della schermata delle entità nella sezione Gestione della migrazione.

Impostazioni dello schema: attualmente questa scheda offre solo la possibilità di modificare il nome descrittivo dell'entità, questo è il nome visualizzato nell'interfaccia utente. Se non è definita, l'interfaccia utente utilizza il nome programmatico dell'entità.

Aggiunta/modifica di un attributo

Gli attributi possono essere modificati dinamicamente tramite la sezione di amministrazione degli attributi della soluzione Cloud Migration Factory on AWS. Quando gli attributi vengono aggiunti, modificati o eliminati, gli aggiornamenti verranno applicati in tempo reale all'amministratore che

effettua la modifica. La sessione di tutti gli altri utenti attualmente connessi alla stessa istanza verrà aggiornata automaticamente entro un minuto dal salvataggio delle modifiche da parte dell'amministratore.

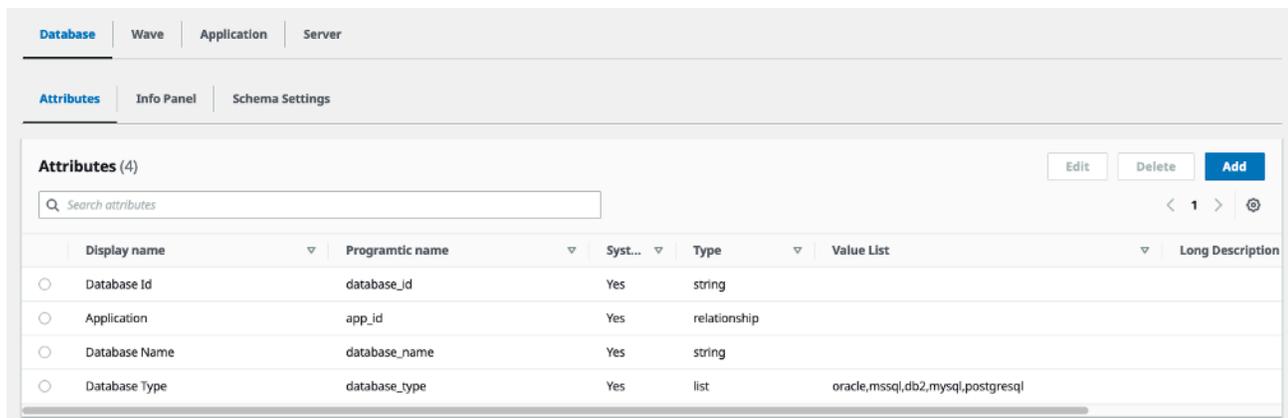
Alcuni attributi sono definiti come attributi di sistema, il che significa che l'attributo è fondamentale per le funzionalità di base di Cloud Migration Factory su AWS e quindi solo alcune proprietà possono essere modificate dagli amministratori. Qualsiasi attributo che sia un attributo di sistema verrà visualizzato con un avviso nella parte superiore della schermata di modifica degli attributi.

Per gli attributi definiti dal sistema è possibile modificare solo quanto segue:

- Pannello informativo
- Opzioni avanzate
 - Raggruppamento e posizionamento degli attributi
 - Convalida dell'input

Tutte le altre proprietà dell'attributo definito dal sistema sono di sola lettura.

Aggiungere un attributo:



Puoi aggiungere nuovi attributi scegliendo il pulsante Aggiungi nella scheda degli attributi dell'entità a cui desideri aggiungere l'attributo. Nell'esempio precedente, scegliendo Aggiungi si aggiungerà un nuovo attributo all'entità del database.

Nella finestra di dialogo Modifica attributo, è necessario fornire le seguenti proprietà obbligatorie:

Nome programmatico: questa è la chiave che verrà utilizzata per memorizzare i dati dell'attributo rispetto agli elementi della tabella DynamoDB. Viene inoltre utilizzato come riferimento quando si utilizzano le API Migration Factory e negli script di automazione.

Nome visualizzato: questa è l'etichetta che verrà visualizzata sull'interfaccia Web accanto al campo di immissione dei dati.

Tipo: questa selezione a discesa definisce il tipo di dati che l'utente potrà memorizzare in base all'attributo. Sono disponibili le seguenti opzioni:

Type	Utilizzo
Stringa	Gli utenti possono inserire una sola riga di testo. Non sono consentite restituzioni.
Stringa multivalore	Simile a una stringa, l'unica differenza è che l'utente può inserire più valori su righe separate all'interno del campo, questi vengono quindi memorizzati come matrice/elenco.
Password	Fornisce all'utente un modo per inserire in modo sicuro dati che non dovrebbero essere visualizzati sullo schermo per impostazione predefinita.

 **Note**

I dati non vengono archiviati in modo crittografato quando si utilizza questo tipo di attributo e vengono visualizzati in testo non crittografato quando vengono visualizzati nei payload delle API, pertanto non devono essere utilizzati per archiviare dati sensibili. Qualsiasi password o segreto deve essere archiviato nel Migration Factory Credential Manager (trattato in questo documento) che utilizza AWS Secrets Manager per archiviare e fornire l'accesso alle credenziali in modo sicuro.

Type	Utilizzo
Data	Fornisce un campo con un selettore di data che consente all'utente di selezionare una data, oppure può inserire manualmente la data richiesta.
Checkbox	Fornisce una casella di controllo standard, se selezionata, il valore della chiave memorizzerà «true», se non è selezionato, sarà «falso» o la chiave non esisterà nel record.
TextArea	A differenza del tipo String, TextAreasoffre la possibilità di memorizzare testo su più righe, supporta solo caratteri di testo di base.
Tag	Consente agli utenti di memorizzare un elenco di coppie chiave/valore.
Elenco	Fornisce all'utente un elenco di opzioni predefinite tra cui scegliere, queste opzioni sono definite nella definizione dell'attributo dello schema nella proprietà Value List dell'attributo.

Type	Utilizzo
Relazione	<p>Questo tipo di attributo offre la possibilità di memorizzare relazioni tra due entità o record qualsiasi. Quando si definisce un attributo di relazione, si seleziona l'entità con cui verrà stabilita la relazione, quindi il valore chiave utilizzato per correlare gli elementi e si seleziona l'attributo dall'elemento correlato che si desidera mostrare all'utente.</p> <p>All'utente viene presentato un elenco a discesa basato sull'entità e sui valori di visualizzazione disponibili per la relazione.</p> <p>In ogni campo di relazione l'utente dispone di un collegamento rapido per mostrare il riepilogo dell'elemento correlato.</p>
JSON	<p>Fornisce un campo editor JSON in cui i dati JSON possono essere archiviati e modificati. Questo può essere usato per memorizzare i parametri di input/output degli script o altri dati necessari per l'automazione delle attività o per qualsiasi altro uso.</p>

Quando si aggiunge un nuovo attributo, è necessario concedere agli utenti l'accesso al nuovo attributo tramite una politica. Consulta la sezione [Gestione delle autorizzazioni](#) per i dettagli su come concedere l'accesso agli attributi.

Pannello informativo

Fornisce la possibilità di specificare un aiuto e una guida contestuali per l'utilizzo dell'attributo. Quando specificato, l'etichetta dell'attributo nell'interfaccia utente avrà un link Info visualizzato a destra. Facendo clic su questo collegamento, all'utente vengono visualizzati il contenuto e i collegamenti di aiuto specificati in questa sezione a destra dello schermo.

La sezione del pannello Informazioni offre due viste dei dati, la vista Modifica in cui è possibile definire il contenuto e la vista Anteprima per fornire un'anteprima rapida di ciò che l'utente vedrà quando vengono salvati gli aggiornamenti all'attributo.

Il titolo della Guida supporta solo valori di testo semplice. Il contenuto della Guida supporta un sottoinsieme di tag html che consentono la formattazione del testo. Ad esempio, l'aggiunta di tag di `` inizio e `` fine attorno al testo renderà il testo racchiuso in grassetto (ad esempio, `Network Interface ID` risulterà in Network Interface ID). I tag supportati sono i seguenti:

Tag	Utilizzo	Esempio di interfaccia utente
<code><p></p></code>	Definisce un paragrafo.	<code><p>Il mio primo paragrafo</p></code> <code><p>Il mio secondo paragrafo</p></code>
<code><a></code>	Definisce un collegamento ipertestuale.	<code>Visita! AWS</code>
<code><h3></code> , <code><h4></code> e <code><h5></code>	Definisce i titoli da h3 a h5	<code><h3>La mia rubrica 3</h3></code>
<code></code>	Definisce una sezione di testo, che consente di applicare una formattazione aggiuntiva, come colore, dimensione e carattere del testo.	<code>blu</code>
<code><div></code>	Definisce un blocco del documento, che consente di applicare una formattazione aggiuntiva, come colore del testo, dimensione, carattere.	<code><div style="color:blue"></code> <code><h3>Questa è un'intestazione blu</h3></code> <code><p>Questo è del testo blu in un div. </p></code> <code></div></code>

Tag	Utilizzo	Esempio di interfaccia utente
<code>+ </code>	Definisce un elenco puntato non ordinato.	<pre> Riospitare Ripiattaforma Ritirarsi </pre>
<code>, </code>	Definisce un elenco ordinato/numerato.	<pre> Riospitare Ripiattaforma Ritirarsi </pre>
<code><code></code>	Definisce un blocco o una sezione di testo contenente codice.	<code><code>colore di sfondo</code></code>
<code><pre></code>	Definisce un blocco di testo preformattato, vengono emesse tutte le interruzioni di riga, le tabulazioni e gli spazi.	<pre><pre> Il mio testo preformattato. Viene visualizzato con un carattere a larghezza fissa e verrà visualizzato come digitato <<verranno visualizz ati questi spazi. </pre></pre>

Tag	Utilizzo	Esempio di interfaccia utente
<code><dl>, <dt>e <dd></code>	Definisce un elenco di descrizioni.	<pre> <dl> <dt>Riospitare</dt> <dd>Migrazione Lift and Shift</dd> <dt>Ritirarsi</dt> <dd>Disattivate l'istanza o il servizio</dd> </dl> </pre>
<code><hr></code>	Definisce una regola orizzontale sulla pagina per mostrare un cambiamento nell'argomento o nella sezione.	<code><hr></code>
<code>
</code>	Definisce un'interruzione di riga nel testo. Queste opzioni sono supportate ma non obbligatorie, in quanto tutte le restituzioni iniziali presenti nell'editor verranno sostituiti e da <code>
</code> quando verranno salvate.	<code>
</code>
<code><i>e </code>	Ha definito il testo racchiuso in corsivo o in un formato localizzato alternativo.	<code><i>È in corsivo o anche in corsivo</i></code>
<code>e </code>	Definisce il testo racchiuso in grassetto.	<code>Sono in grassetto o Questo è diverso</code>

Un'altra opzione disponibile per fornire assistenza sono i collegamenti a contenuti e linee guida esterni. Per aggiungere un link esterno alla guida contestuale dell'attributo, fai clic su **Aggiungi nuovo URL** e fornisci un'etichetta e un URL. Se necessario, puoi aggiungere più link allo stesso tipo di attributo.

Opzioni avanzate

Raggruppamento e posizionamento degli attributi

Questa sezione offre all'amministratore la possibilità di impostare la posizione dell'attributo nell'interfaccia utente **Aggiungi/Modifica** e consente inoltre di raggruppare gli attributi fornendo all'utente un modo semplice per individuare gli attributi correlati.

UI Group è un valore di testo che definisce il nome del gruppo in cui deve essere visualizzato l'attributo, tutti gli attributi con lo stesso valore di UI Group verranno inseriti nello stesso gruppo, qualsiasi attributo senza UI Group specificato verrà inserito nel gruppo predefinito nella parte superiore del modulo intitolato **Dettagli**. Quando viene specificato UI Group, l'interfaccia utente mostrerà il testo mostrato qui come titolo del gruppo.

La seconda proprietà in questa sezione è **Order in group**, può essere impostata su qualsiasi numero positivo o negativo e, quando specificato, gli attributi verranno elencati in base a un ordine dal più basso al più alto in base a questo valore. Tutti gli attributi per i quali non è specificato un ordine nel gruppo avranno una priorità inferiore e verranno ordinati alfabeticamente.

Convalida dell'input

Questa sezione consente all'amministratore di definire criteri di convalida che assicurino che l'utente abbia inserito dati validi prima di poter salvare un elemento. La convalida utilizza un'espressione regolare o una stringa regex, che è una serie di caratteri che specificano un modello di ricerca per un valore di testo. Ad esempio, il pattern `^(subnet- ([a-z0-9]{17}) *)$` cercherà la sottorete di testo seguita da qualsiasi combinazione dei caratteri dalla a alla z (minuscoli) e dalle cifre da 0 a 9 con un numero esatto di caratteri di 17, se trova qualcos'altro restituirà false indicando che la convalida è fallita. In questa guida non possiamo coprire tutte le possibili combinazioni e modelli disponibili, ma ci sono molte risorse su Internet che possono aiutarti a creare il perfetto per il tuo caso d'uso. Ecco alcuni esempi comuni per iniziare:

Modello regex	Utilizzo
<code>^(?! \s*\$) . +</code>	Assicura che il valore sia impostato.

Modello regex	Utilizzo
<code>^(sottorete-[a-z0-9]{17})*\$</code>	<p>Verifica che il valore sia un ID di sottorete valido.</p> <p>[Inizia con la sottorete di testo, seguita da 17 caratteri composti solo da lettere e numeri]</p>
<code>^(ami-([a-z0-9]{8,17})+)\$</code>	<p>Verifica che il valore sia un ID AMI valido.</p> <p>[Inizia con il testo ami- seguito da 8 a 17 caratteri composti solo da lettere e numeri]</p>
<code>^(sg-[a-z0-9]{17})*\$</code>	<p>Verifica che il valore sia in un formato ID del gruppo di sicurezza valido.</p> <p>[Inizia con il testo sg- seguito da 17 caratteri composti solo da lettere e numeri]</p>
<code>^(([a-zA-Z0-9] [a-za-Z0-9] [a-zA-Z0-9\ -] * [a-zA-Z0-9])\.)* ([a-zA-Z0-9] [a-zA-Z0-9] [a-zA-Z0-9\ -] * [a-zA-Z0-9])\$</code>	<p>Assicura che i nomi dei server siano validi e contengano solo caratteri alfanumerici, trattini e punti.</p>
<code>^([1-9] [1-9] [0-9] [1-9] [0-9] [0-9] [1-9] [0-9] [0-9] [0-9] [1] [0-6] [0-3] [0-8] [0-4])\$</code>	<p>Assicura che venga immesso un numero compreso tra 1 e 1634.</p>
<code>^(standard io1 io2 gp2 gp3)\$</code>	<p>Assicura che la stringa inserita corrisponda a standard, io1, io2, gp2 o gp3.</p>

Dopo aver creato il modello di ricerca regex, puoi specificare il messaggio di errore specifico che verrà mostrato all'utente sotto il campo, inseriscilo nella proprietà del messaggio di aiuto di convalida.

Una volta impostate queste due proprietà, nella stessa schermata vedrai sotto un simulatore di convalida, qui puoi verificare che il tuo modello di ricerca funzioni come previsto e che il messaggio di errore sia visualizzato correttamente. Basta digitare del testo di prova nel campo Test validation per verificare che il modello corrisponda correttamente.

Dati di esempio

La sezione dati di esempio offre all'amministratore la possibilità di mostrare all'utente un esempio di formato di dati richiesto per un attributo, che può essere specificato per il formato dei dati richiesto quando fornito nel caricamento di un modulo di inserimento, tramite l'interfaccia utente e/o direttamente tramite l'API.

I dati di esempio mostrati nella proprietà Intake form example data verranno generati in qualsiasi modello di input creato in cui l'attributo è incluso, quando si utilizza la funzione Download, una funzione del modulo di acquisizione del modello, in Gestione della migrazione > Importa.

I dati di esempio dell'interfaccia utente e i dati di esempio dell'API sono memorizzati nell'attributo, ma attualmente non sono esposti nell'interfaccia web. Questi possono essere utilizzati nelle integrazioni e negli script.

Gestione delle autorizzazioni

La AWS soluzione Cloud Migration Factory on fornisce un controllo granulare degli accessi basato sui ruoli ai dati e alle funzioni di automazione disponibili nella soluzione, alla base di ciò è Amazon Cognito, che fornisce la directory utente e il motore di autenticazione.

La tabella seguente mostra i vari elementi che compongono il framework di controllo degli accessi all'interno della soluzione Cloud Migration Factory on AWS e da dove viene gestito ogni elemento.

Elemento di controllo degli accessi	Interfaccia di gestione	Descrizione
Utente	Amazon Cognito e Cloud Migration Factory su AWS	Gli utenti vengono creati, eliminati e aggiornati in Amazon Cognito, dove è possibile stabilire il profilo degli utenti e, se necessario, l'autenticazione a più fattori (MFA). All'interno dell'interfaccia utente di AWS CMF, puoi aggiungere e rimuovere utenti solo dai gruppi.

Elemento di controllo degli accessi	Interfaccia di gestione	Descrizione
Group (Gruppo)	Cloud Migration Factory su AWS	Puoi creare o eliminare gruppi dall'interfaccia utente di AWS CMF.
Ruolo	Cloud Migration Factory su AWS	<p>Un ruolo è mappato su uno o più gruppi, la modifica dei gruppi a cui è assegnato un ruolo viene eseguita nella sezione di amministrazione AWS CMF. A qualsiasi utente membro di un gruppo assegnato a un ruolo verranno assegnate tutte le politiche mappate al ruolo.</p> <p>È possibile assegnare una o più politiche a un ruolo.</p>
Policy	Cloud Migration Factory su AWS	Una policy contiene i diritti dettagliati assegnati a qualsiasi utente a cui si applica la policy (tramite l'appartenenza al gruppo). Una singola policy può includere i diritti di accesso ai dati per più entità o per una singola entità, oltre ai diritti di accesso per eseguire lavori di automazione e altre azioni all'interno dell'interfaccia utente AWS CMF. Queste politiche si applicano anche quando un utente interagisce con le API AWS CMF.

Policy

Una policy fornisce le autorizzazioni più granulari possibili in Cloud Migration Factory on AWS, contiene la definizione a livello di attività dei diritti concessi a un utente. All'interno di una policy ci sono due tipi di autorizzazione principali che possono essere concessi a un gruppo di utenti, i permessi per i metadati e i permessi per le azioni di automazione. Le autorizzazioni per i metadati consentono a un amministratore di controllare il livello di accesso di un gruppo ai singoli schemi e ai relativi attributi, specificando i diritti di creazione, lettura, aggiornamento e/o eliminazione, se necessario. Le autorizzazioni di Automation Action concedono agli utenti l'accesso per eseguire azioni di automazione specifiche, come l'azione di integrazione MGN. AWS

Autorizzazioni per i metadati

Per ogni schema o entità all'interno di AWS CMF un amministratore può definire una politica che consente agli utenti di accedere a attributi specifici e definire anche il livello di accesso a tali attributi. Al momento della creazione di una nuova politica, i diritti di default per tutti gli schemi sono l'assenza di accesso, la prima cosa da impostare è il livello di accesso richiesto per questa politica a livello di articolo/record. Di seguito è riportata una tabella che descrive le autorizzazioni di accesso a livello di record disponibili.

Livello di accesso	Descrizione
Crea	Se selezionato, un utente a cui si applica questo criterio avrà la possibilità di aggiungere e nuovi record/elementi di questo tipo all'archivio di metadati. Quando è selezionata l'opzione di creazione ma non sono consentiti altri diritti, l'utente avrà la possibilità di creare record e impostare solo gli attributi obbligatori su un valore indipendentemente dagli attributi selezionati.
Lettura	Non ancora implementato Se selezionato, un utente avrà i diritti di lettura su tutti i record/elementi per questo tipo

Livello di accesso	Descrizione
	di entità, se non selezionato non vedrà gli elementi di dati nell'interfaccia utente o nell'API.
Aggiornamento	Se selezionato, un utente a cui si applica questo criterio avrà la possibilità di aggiornar e record/elementi di questo tipo nell'archivio di metadati, ma solo per gli attributi specificati nell'elenco di accesso a livello di attributo . Quando è selezionato l'aggiornamento, è necessario selezionare almeno un attributo o verrà visualizzato un errore durante il salvataggio.
Eliminazione	Se selezionato, un utente a cui si applica questo criterio avrà la possibilità di eliminare record/elementi di questo tipo dall'archivio dei metadati.

Roles

I ruoli consentono di assegnare una o più politiche a uno o più gruppi. La combinazione di tutte le politiche assegnate a un ruolo fornisce le autorizzazioni di accesso. I ruoli possono essere creati in base ai ruoli o alle funzioni professionali all'interno del progetto o dell'organizzazione.

Guida per sviluppatori

Codice sorgente

Puoi visitare il nostro [GitHub repository](#) per scaricare i modelli e gli script per questa soluzione e condividere le tue personalizzazioni con altri. Se hai bisogno di una versione precedente del CloudFormation modello o hai un problema tecnico da segnalare, puoi farlo dalla pagina [GitHub dei problemi](#). Segnala problemi tecnici relativi alla soluzione nella [pagina Problemi](#) del GitHub repository.

Argomenti supplementari

Elenco delle attività di migrazione automatizzate utilizzando la console web Migration Factory

La AWS soluzione Cloud Migration Factory on implementa attività di migrazione automatizzate che puoi sfruttare per i tuoi progetti di migrazione. Puoi seguire le attività di migrazione elencate di seguito e personalizzarle in base alle tue esigenze aziendali.

Prima di iniziare qualsiasi attività, assicurati di leggere la [Guida per l'utente — Run Automation from console](#) per capire come funziona. Inoltre, devi [creare un server di automazione](#) e [creare utenti Windows e Linux](#) per eseguire l'automazione dalla console.

Utilizzate le seguenti procedure nello stesso ordine per eseguire un test completo della soluzione utilizzando lo script e le attività di automazione di esempio.

Verifica i prerequisiti

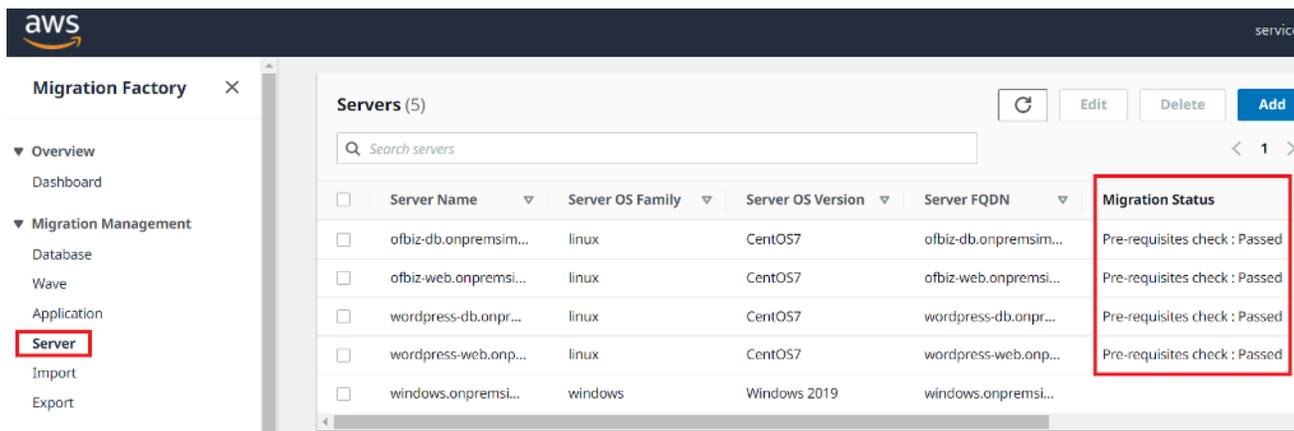
Connect con i server di origine inclusi nell'ambito per verificare i prerequisiti necessari come TCP 1500, TCP 443, spazio libero nel volume root, versione del framework.Net e altri parametri. Questi prerequisiti sono necessari per la replica.

Prima di poter effettuare il controllo dei prerequisiti, è necessario installare il primo manualmente su un server di origine, in modo da creare un server di replica in EC2. Ci collegheremo a questo server per il test della porta 1500. Dopo l'installazione, AWS Application Migration Service (AWSMGN) crea il server di replica in Amazon Elastic Compute Cloud (Amazon EC2). È necessario verificare la porta TCP 1500 dal server di origine al server di replica in questa attività. Per informazioni sull'installazione dell'agente AWS MGN sui tuoi server di origine, consulta [le istruzioni di installazione nella Guida per l'utente di AWS Application Migration Service](#).

Usa la seguente procedura dopo aver effettuato l'accesso alla console web di Migration Factory.

1. Nella console Migration Factory, seleziona Jobs nel menu a sinistra, seleziona Azioni, quindi Run Automation sul lato destro.
2. Immettere Job Name, selezionare lo script 0-Check MGN Prerequisites e il server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Crea un server di automazione della migrazione](#).

3. Seleziona Linux Secrets e/o Windows Secrets a seconda del sistema operativo di cui disponi per questa ondata. Immettete l'IP del server di replica MGN, scegliete l'onda su cui desiderate eseguire l'automazione e scegliete Submit Automation Job.
4. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere IN ESECUZIONE. Scegli Aggiorna per vedere lo stato. Dovrebbe passare a Completo dopo alcuni minuti.
5. Lo script aggiornerà anche lo stato della migrazione della soluzione nell'interfaccia web di Migration Factory, come mostrato nella seguente schermata di un progetto di esempio.



Installa gli agenti di replica

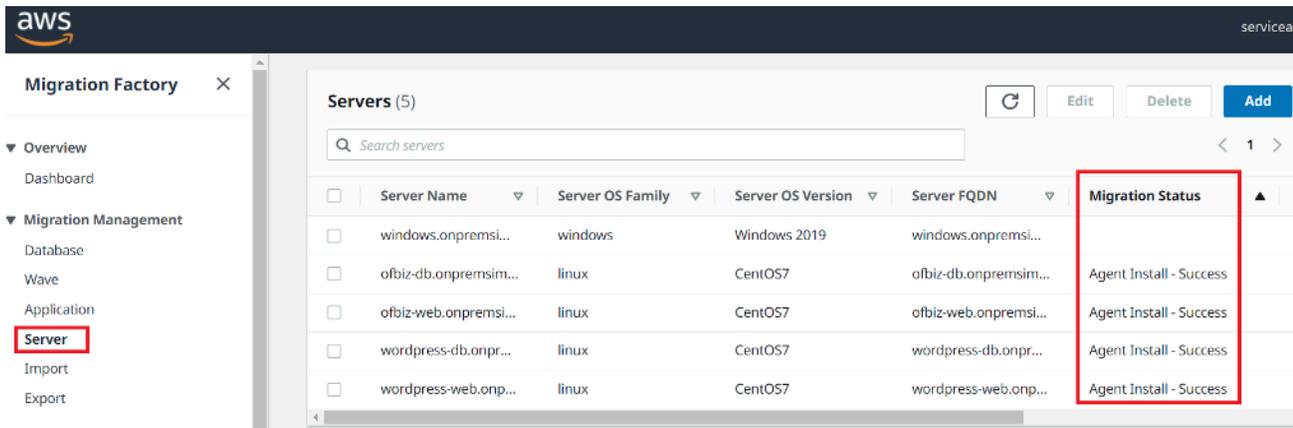
Note

Prima di installare l'agente, assicuratevi che [AWSMGN sia inizializzato in ogni account e regione di destinazione](#).

Utilizzate la seguente procedura per installare automaticamente gli agenti di replica nei server di origine pertinenti.

1. Nella console Migration Factory, seleziona Jobs nel menu a sinistra, seleziona Azioni, quindi Run Automation sul lato destro.
2. Immettere Job Name, selezionare lo script 1-Install MGN Agents e il server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Crea un server di automazione della migrazione](#).

3. Seleziona Linux Secrets e/o Windows Secrets a seconda del sistema operativo di cui disponi per questa ondata. Scegli l'ondata in cui desideri eseguire l'automazione e scegli Invia lavoro di automazione.
4. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere in corso. Scegli Aggiorna per vedere lo stato. Dovrebbe passare a Completo dopo alcuni minuti.
5. Lo script fornisce anche lo stato della migrazione nell'interfaccia web di Migration Factory, come mostrato nella seguente schermata di esempio.



Invia gli script post-lancio

AWS Application Migration Service (MGN) supporta script post-lancio per aiutarti ad automatizzare le attività a livello di sistema operativo, come l'installazione/disinstallazione del software dopo l'avvio delle istanze di destinazione. Questa attività invia gli script post-lancio a macchine Windows e/o Linux, a seconda dei server identificati per la migrazione.

Note

Prima di inviare gli script post-lancio, è necessario copiare i file in una cartella sul server di automazione della migrazione.

Utilizzare la procedura seguente per inviare gli script post-avvio ai computer Windows.

1. Nella console Migration Factory, seleziona Jobs nel menu a sinistra, seleziona Azioni, quindi Run Automation sul lato destro.

2. Inserisci Job Name, seleziona lo script 1-Copy Post Launch Scripts e il tuo server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Crea un server di automazione della migrazione](#).
3. Seleziona Linux Secrets e/o Windows Secrets a seconda del sistema operativo di cui disponi per questa ondata. Fornisci una posizione di origine Linux e/o una posizione di origine di Windows.
4. Scegli l'onda in cui vuoi eseguire automaton e scegli Invia Automation Job.
5. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere in esecuzione e potrai scegliere Aggiorna per visualizzare lo stato. Dovrebbe passare a Completato dopo alcuni minuti.

Verifica lo stato della replica

Questa attività verifica automaticamente lo stato di replica per i server di origine interessati. Lo script si ripete ogni cinque minuti fino a quando lo stato di tutti i server di origine nell'ondata data passa allo stato Integrato.

Utilizzare la procedura seguente per verificare lo stato della replica.

1. Nella console Migration Factory, seleziona Jobs nel menu a sinistra, quindi seleziona Azioni, quindi Run Automation sul lato destro.
2. Immettere Job Name, selezionare lo script 2-Verify Replication Status e il server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Crea un server di automazione della migrazione](#).
3. Scegli l'onda in cui vuoi eseguire automaton e scegli Invia Automation Job.
4. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere in esecuzione e potrai fare clic sul pulsante Aggiorna per visualizzare lo stato. Dovrebbe passare a Completato dopo alcuni minuti.

The screenshot shows the AWS Application Migration Service console. The left sidebar contains navigation options like 'Source servers', 'Launch history', and 'Settings'. The main content area displays a table titled 'Source servers (4)'. The table has columns for 'Source server name', 'Alerts', 'Replication type', 'Migration lifecycle', and 'Data replication status'. The 'Data replication status' column is highlighted with a red box, and all entries in this column are 'Healthy'.

Source server name	Alerts	Replication type	Migration lifecycle	Data replication status
ofbiz-db.onpremsim.env	-	Agent based	Ready for testing	Healthy
ofbiz-web.onpremsim.env	-	Agent based	Ready for testing	Healthy
wordpress-db.onpremsim.env	-	Agent based	Ready for testing	Healthy
wordpress-web.onpremsim.env	-	Agent based	Ready for testing	Healthy

Note

La replica può richiedere alcuni istanti. Potresti non visualizzare l'aggiornamento dello stato dalla console di fabbrica per alcuni minuti. Facoltativamente, puoi anche controllare lo stato nel servizio MGN.

Convalida il modello di lancio

Questa attività convalida i metadati del server nel Migration Factory e si assicura che funzionino con il modello EC2 e che non contengano errori di battitura. Convaliderà sia i metadati di test che quelli di cutover.

Utilizza la seguente procedura per convalidare il modello di lancio di EC2.

1. Vai alla console Migration Factory e seleziona Wave nel riquadro del menu.
2. Seleziona l'ondata di destinazione e scegli Azioni. Seleziona Rehost, quindi seleziona MGN.
3. Seleziona Convalida modello di avvio per l'azione, quindi seleziona Tutte le applicazioni.
4. Scegli Invia per avviare la convalida.

Dopo qualche tempo, la convalida restituirà un risultato positivo.

Note

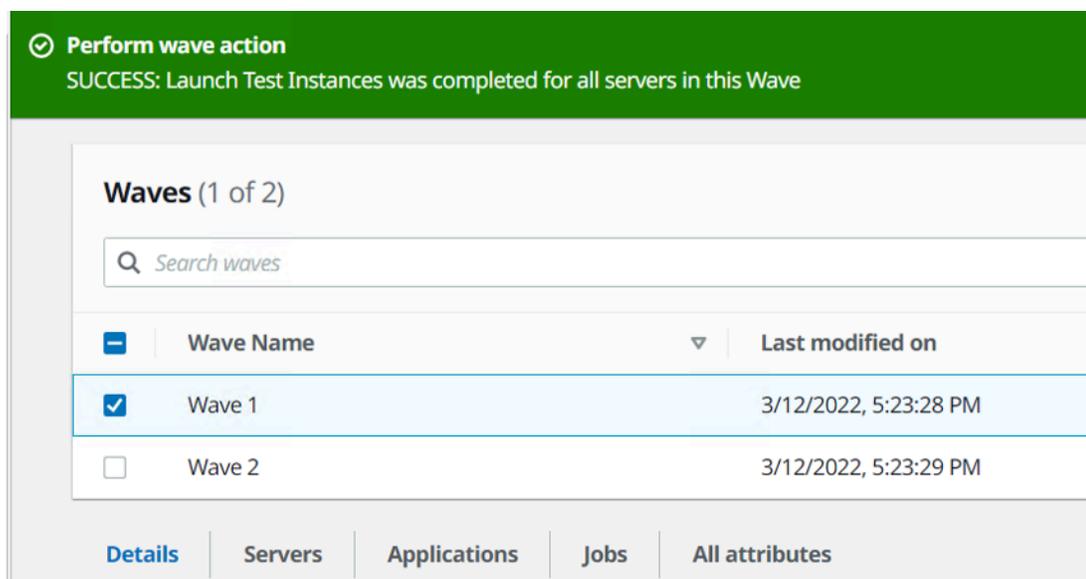
Se la convalida non ha esito positivo, riceverai un messaggio di errore specifico: Gli errori possono essere dovuti a dati non validi nell'attributo del server, ad esempio Subnet_IDS, SecurityGroup_IDS o InstanceType non validi. È possibile passare alla pagina Pipeline dall'interfaccia web di Migration Factory e selezionare il server problematico per correggere gli errori.

Avvia istanze per il test

Questa attività avvia tutte le macchine di destinazione per una determinata ondata in AWS Application Migration Service (MGN) in modalità test.

Utilizza la seguente procedura per avviare istanze di test.

1. Nella console Migration Factory, seleziona Wave nel menu di navigazione.
2. Seleziona target wave e scegli Azioni. Seleziona Rehost, quindi seleziona MGN.
3. Seleziona Launch Test Instances Action, seleziona Tutte le applicazioni.
4. Scegli Invia per avviare le istanze di test.
5. Dopo qualche tempo, la convalida restituirà un risultato positivo.



Perform wave action
SUCCESS: Launch Test Instances was completed for all servers in this Wave

Waves (1 of 2)

Search waves

<input type="checkbox"/>	Wave Name	Last modified on
<input checked="" type="checkbox"/>	Wave 1	3/12/2022, 5:23:28 PM
<input type="checkbox"/>	Wave 2	3/12/2022, 5:23:29 PM

Details Servers Applications Jobs All attributes

Note

Questa azione aggiornerà anche lo stato della migrazione per il server avviato.

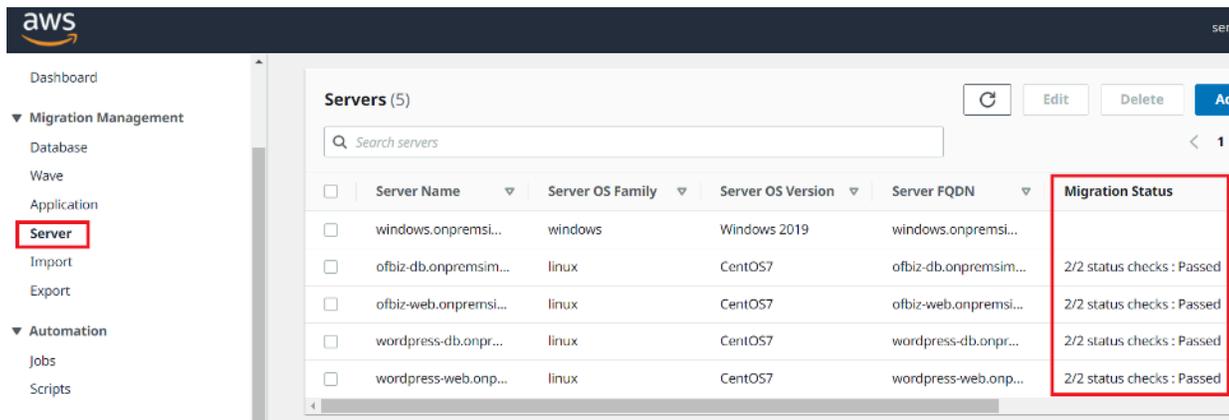
Verifica lo stato dell'istanza di destinazione

Questa attività verifica lo stato dell'istanza di destinazione controllando il processo di avvio di tutti i server di origine interessati nella stessa ondata. L'avvio delle istanze di destinazione può richiedere fino a 30 minuti. Puoi controllare lo stato manualmente accedendo alla console Amazon EC2, cercando il nome del server di origine e verificando lo stato. Riceverai un messaggio di controllo dello stato di salute indicante che due controlli sono stati superati, il che indica che l'istanza è integra dal punto di vista dell'infrastruttura.

Tuttavia, per una migrazione su larga scala, controllare lo stato di ogni istanza richiede molto tempo, quindi puoi eseguire questo script automatico per verificare che i 2/2 controlli abbiano superato lo stato per tutti i server di origine in una determinata ondata.

Utilizzate la procedura seguente per verificare lo stato dell'istanza di destinazione.

1. Vai alla console Migration Factory e seleziona Jobs nel menu a sinistra.
2. Seleziona Azioni, quindi Esegui automazione sul lato destro.
3. Immettere Job Name, selezionare lo script 3-Verify Instance Status e il server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Build a migration automation server](#).
4. Scegli l'ondata in cui desideri eseguire l'automazione e scegli Invia lavoro di automazione.
5. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere in esecuzione e potrai scegliere Aggiorna per visualizzare lo stato. Dovrebbe passare a Completato dopo alcuni minuti.



Note

L'avvio dell'istanza può richiedere del tempo e potresti non visualizzare l'aggiornamento dello stato dalla console di fabbrica per alcuni minuti. Migration Factory riceve anche un aggiornamento dello stato dallo script. Aggiorna lo schermo se necessario.

Note

Se le istanze target non superano i 2/2 controlli di integrità per la prima volta, è possibile che il processo di avvio richieda più tempo per essere completato. Ti consigliamo di eseguire i controlli sanitari una seconda volta circa un'ora dopo il primo controllo sanitario. Ciò garantisce il completamento del processo di avvio. Se i controlli sanitari falliscono questa seconda volta, vai al [centro di AWS supporto](#) per registrare una richiesta di assistenza.

Contrassegna come pronto per il cutover

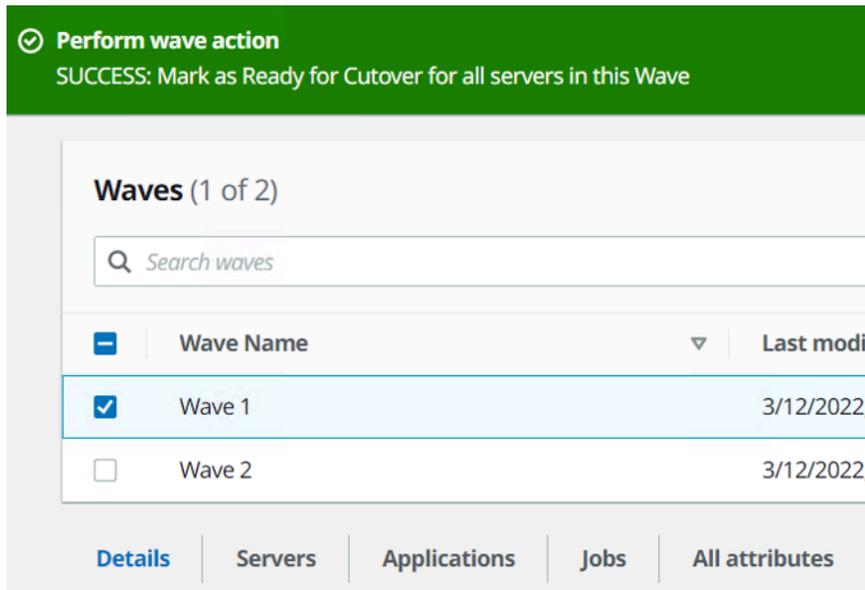
Una volta terminato il test, questa attività modifica lo stato del server di origine in modo che venga contrassegnato come pronto per il cutover, in modo che l'utente possa avviare un'istanza cutover.

Utilizza la seguente procedura per convalidare il modello di lancio di EC2.

1. Sulla console Migration Factory, seleziona Wave sul lato sinistro.
2. Seleziona l'onda di destinazione e fai clic sul pulsante Azioni. Seleziona Rehost, quindi seleziona MGN.
3. Seleziona Mark as Ready for Cutover Action, seleziona Tutte le applicazioni.

4. Scegli Invia per avviare istanze live.

Dopo qualche tempo, la convalida restituirà un risultato positivo.



Spegnete i server di origine compresi nell'ambito

Questa attività spegne i server di origine pertinenti coinvolti nella migrazione. Dopo aver verificato lo stato di replica dei server di origine, si è pronti a spegnere i server di origine per interrompere le transazioni dalle applicazioni client ai server. È possibile spegnere i server di origine nella finestra Cutover. Lo spegnimento manuale dei server di origine potrebbe richiedere cinque minuti per server e, per ondate di grandi dimensioni, alcune ore in totale. È invece possibile eseguire questo script di automazione per spegnere tutti i server in una determinata ondata.

Utilizzate la seguente procedura per spegnere tutti i server di origine coinvolti nella migrazione.

1. Nella console Migration Factory, seleziona Jobs nel menu a sinistra, seleziona Azioni, quindi Run Automation sul lato destro.
2. Immettere Job Name, selezionare lo script 3-Shutdown All Servers e il server di automazione per eseguire lo script. Se il server di automazione non esiste, assicurati di aver completato [Crea un server di automazione della migrazione](#).
3. Seleziona Linux Secrets e/o Windows Secrets a seconda del sistema operativo di cui disponi per questa ondata.
4. Scegli l'onda in cui vuoi eseguire automaton e scegli Invia Automation Job.

5. Verrai reindirizzato alla pagina dell'elenco dei lavori, lo stato del lavoro dovrebbe essere in esecuzione e potrai fare clic sul pulsante Aggiorna per visualizzare lo stato. Dovrebbe passare a Completato dopo alcuni minuti.

Avvia istanze per Cutover

Questa attività avvia tutte le macchine di destinazione per una determinata ondata in AWS Application Migration Service (MGN) in modalità Cutover.

Utilizza la seguente procedura per avviare istanze di test.

1. Nella console Migration Factory, seleziona Wave sul lato sinistro.
2. Seleziona target wave e scegli Azioni. Seleziona Rehost, quindi seleziona MGN.
3. Seleziona Launch Cutover Instances Action, seleziona Tutte le applicazioni.
4. Scegli Invia per avviare le istanze di test.

Dopo qualche tempo, la convalida restituirà un risultato positivo.

Note

Questa azione aggiornerà anche lo stato della migrazione per il server avviato.

Elenco delle attività di migrazione automatizzate tramite il prompt dei comandi

Note

Consigliamo di eseguire l'automazione dalla Cloud Migration Factory sulla console AWS. Puoi utilizzare i seguenti passaggi per eseguire script di automazione. Assicurati di scaricare gli script di automazione dal GitHub repository e di configurare il server di automazione seguendo i passaggi in [Esegui automazioni dal prompt](#) dei comandi e seguendo le istruzioni per configurare le autorizzazioni in Configurare le autorizzazioni per il server di automazione della [migrazione AWS](#).

La AWS soluzione Cloud Migration Factory on implementa attività di migrazione automatizzate che puoi sfruttare per i tuoi progetti di migrazione. Puoi seguire le attività di migrazione elencate di seguito e personalizzarle in base alle tue esigenze aziendali.

Prima di iniziare qualsiasi attività, verifica di aver effettuato l'accesso al server di automazione della migrazione come utente di dominio con autorizzazione di amministratore locale sui server di origine interessati.

Important

È necessario accedere come utente amministratore per completare le attività elencate in questa sezione.

Utilizzate le seguenti procedure nello stesso ordine per eseguire un test completo della soluzione utilizzando lo script e le attività di automazione di esempio.

Verifica i prerequisiti

Connect con i server di origine inclusi nell'ambito per verificare i prerequisiti necessari come TCP 1500, TCP 443, spazio libero nel volume root, versione del framework.Net e altri parametri. Questi prerequisiti sono necessari per la replica.

Prima di poter eseguire il controllo dei prerequisiti, è necessario installare il primo agente manualmente su un server di origine, in modo da creare un server di replica in EC2, ci collegheremo a questo server per il test della porta 1500. Dopo l'installazione, AWS Application Migration Service (AWSMGN) crea il server di replica in Amazon Elastic Compute Cloud (Amazon EC2). Per eseguire questa attività, dovrai verificare la porta TCP 1500 dal server di origine al server di replica. Per informazioni sull'installazione dell'agente AWS MGN sui server di origine, consultate [le istruzioni di installazione nella Guida per l'utente del servizio di migrazione delle applicazioni](#).

Utilizzate la seguente procedura dopo aver effettuato l'accesso al server di automazione della migrazione per verificare i prerequisiti.

1. Effettuato l'accesso come amministratore, aprite il prompt dei comandi (CMD).exe.
2. Vai alla `c:\migrations\scripts\script_mgn_0-Prerequisites-checks` cartella ed esegui il seguente comando Python:

```
python 0-Prerequisites-checks.py --Waveid <wave-id> --ReplicationServerIP <rep-server-ip>
```

Sostituisci <wave-id> e < rep-server-ip > con i valori appropriati:

- Waveid è un valore intero unico per identificare le ondate di migrazione.
- Il ReplicationServerIP valore identifica l'indirizzo IP del server di replica. Modifica questo valore nell'indirizzo IP di Amazon EC2. Per individuare questo indirizzo, accedi a AWS Management Console, cerca Replica, seleziona uno dei server di replica e copia l'indirizzo IP privato. Se la replica avviene sulla rete Internet pubblica, utilizza invece l'indirizzo IP pubblico.

3. Lo script recupera automaticamente un elenco di server per l'ondata specificata.

Lo script verifica quindi i prerequisiti per i server Windows e restituisce lo stato di uno pass o fail per ogni controllo.

Note

È possibile che venga visualizzato un avviso di sicurezza simile al seguente quando lo PowerShell script non è attendibile. Esegui il seguente comando PowerShell per risolvere il problema:

```
Unblock-File C:\migrations\scripts\script_mgn_0-Prerequisites-checks\0-Prerequisites-Windows.ps1
```

Successivamente, lo script controlla i server Linux.

Una volta completati i controlli, lo script restituirà un risultato finale per ogni server.

```
*****
**** Final results for all servers ****
*****

-----
-- Windows server passed all Pre-requisites checks --
-----

Server-T1.mydomain.local
server1.mydomain.local
Server-T15.mydomain.local
server2.mydomain.local

-----
-- Linux server passed all Pre-requisites checks --
-----

MF-RHEL.mydomain.local
MF-Ubuntu.mydomain.local
```

Se il server non supera uno o più controlli dei prerequisiti, è possibile identificare il server difettoso esaminando il messaggio di errore dettagliato fornito al termine del controllo o scorrendo i dettagli del registro.

Lo script aggiornerà anche lo stato di migrazione della soluzione nell'interfaccia web di Migration Factory, come mostrato nella seguente schermata di un progetto di esempio.

Installa gli agenti di replica

Note

Prima di installare l'agente, assicuratevi che [AWSMGN sia inizializzato in ogni](#) account di destinazione.

Utilizzate la procedura seguente per installare automaticamente gli agenti di replica nei server di origine pertinenti.

1. Nel server di automazione della migrazione, signed è un amministratore, aprete il prompt dei comandi (). CMD.exe
2. Vai alla c:\migrations\scripts\script_mgn_1-AgentInstall cartella ed esegui il seguente comando Python:

```
python 1-AgentInstall.py --Waveid <wave-id>
```

Sostituisci < wave-id > con il valore Wave ID appropriato per installare l'agente Replication su tutti i server nell'ondata identificata. Lo script installerà l'agente su tutti i server di origine nella stessa ondata uno per uno.

Note

Per reinstallare l'agente, puoi aggiungere un `--force` argomento.

3. Lo script genera un elenco che identifica i server di origine inclusi per l'ondata specificata. Inoltre, possono essere forniti anche server identificati in più account e per diverse versioni del sistema operativo.

Se in questa ondata sono incluse macchine Linux, è necessario inserire le credenziali di accesso Linux sudo per accedere a tali server di origine.

L'installazione inizia su Windows, quindi passa a Linux per ciascuno di essi. Account AWS

```
*****
*** Installing Agents ****
*****

#####
### In Account: 515800000000, region: us-east-1 ###
#####

-----
- Installing Application Migration Service Agent for: Server-T1.mydomain.local -
-----

** Successfully downloaded Agent installer for: Server-T1.mydomain.local **
Verifying that the source server has enough free disk space to install the AWS Replication Agent.
(a minimum of 2 GB of free disk space is required)
Identifying volumes for replication.
Disk to replicate identified: c:\0 of size 30 GiB
All volumes for replication were successfully identified.
Downloading the AWS Replication Agent onto the source server... Finished.
Installing the AWS Replication Agent onto the source server... Finished.
Syncing the source server with the Application Migration Service Console... Finished.
The following is the source server ID: s-3fe3e5342c624e6a0.
The AWS Replication Agent was successfully installed.
The installation of the AWS Replication Agent has started.

** Installation finished for : Server-T1.mydomain.local **
```

Note

È possibile che venga visualizzato un avviso di sicurezza simile al seguente quando lo PowerShell script non è attendibile. Esegui il seguente comando PowerShell per risolvere il problema:

```
Unblock-File C:\migrations\scripts\script_mgn_1-AgentInstall\1-Install-  
Windows.ps1
```

I risultati vengono visualizzati al termine dell'installazione degli agenti di replica da parte dello script. Esamina i risultati relativi ai messaggi di errore per identificare i server che non sono riusciti a installare gli agenti. Sarà necessario installare manualmente gli agenti sui server guasti. Se l'installazione manuale non riesce, vai al [centro di AWS supporto](#) e registra una richiesta di supporto.

```
*****  
*Checking Agent install results*  
*****  
  
-- SUCCESS: Agent installed on server: Server-T1.mydomain.local  
-- SUCCESS: Agent installed on server: server1.mydomain.local  
-- FAILED: Agent install failed on server: MF-RHEL.mydomain.local  
-- SUCCESS: Agent installed on server: Server-T15.mydomain.local  
-- SUCCESS: Agent installed on server: server2.mydomain.local  
-- SUCCESS: Agent installed on server: MF-Ubuntu.mydomain.local
```

Lo script fornisce anche lo stato della migrazione nell'interfaccia web di Migration Factory, come mostrato nella seguente schermata di un progetto di esempio.

Invia gli script post-lancio

AWS Application Migration Service supporta script post-lancio per aiutarti ad automatizzare attività a livello di sistema operativo come l'installazione/disinstallazione del software dopo l'avvio delle istanze di destinazione. Questa attività invia gli script post-lancio a macchine Windows e/o Linux, a seconda dei server identificati per la migrazione.

Utilizza la seguente procedura dal server di automazione della migrazione per inviare gli script post-avvio ai computer Windows.

1. Effettuato l'accesso come amministratore, apri il prompt dei comandi (`cmd.exe`)

2. Vai alla `c:\migrations\scripts\script_mgn_1-FileCopy` cartella ed esegui il seguente comando Python:

```
python 1-FileCopy.py --Waveid <wave-id> --WindowsSource <file-path> --  
LinuxSource <file-path>
```

Sostituisci `<wave-id>` con il valore Wave ID appropriato e `<file-path>` con il percorso completo del file Source, dove si trova lo script. Ad esempio, `c:\migrations\scripts\script_mgn_1-FileCopy`. Questo comando copia tutti i file dalla cartella di origine alla cartella di destinazione.

Note

È necessario fornire almeno uno di questi due argomenti: `WindowsSource`, `LinuxSource`. Se si fornisce `WindowsSource` path, questo script invierà i file solo ai server Windows in questa ondata, allo stesso `LinuxSource` modo in cui invia i file solo ai server Linux in questa ondata. Fornire `both` invierà i file a entrambi i server Windows e Linux.

3. Lo script genera un elenco che identifica i server di origine inclusi per l'ondata specificata. Inoltre, possono essere forniti anche server identificati in più account e per diverse versioni del sistema operativo.

Se in questa ondata sono incluse macchine Linux, è necessario inserire le credenziali di accesso Linux sudo per accedere a tali server di origine.

4. Lo script copia i file nella cartella di destinazione. Se la cartella di destinazione non esiste, la soluzione crea una directory e notifica all'utente questa azione.

Verifica lo stato della replica

Questa attività verifica automaticamente lo stato di replica per i server di origine interessati. Lo script si ripete ogni cinque minuti fino a quando lo stato di tutti i server di origine nell'ondata data passa allo stato Integrato.

Utilizzare la seguente procedura del server di automazione della migrazione per verificare lo stato della replica.

1. Effettuato l'accesso come amministratore, aprite il prompt dei comandi (CMD).exe.
2. Vai alla `\migrations\scripts\script_mgn_2-Verify-replication` cartella ed esegui il seguente comando Python:

```
python 2-Verify-replication.py --Waveid <wave-id>
```

Sostituisci `<wave-id>` con il valore Wave ID appropriato per verificare lo stato della replica. Lo script verifica i dettagli di replica per tutti i server della specifica ondata e aggiorna l'attributo dello stato di replica per il server di origine identificato nella soluzione.

3. Lo script genera un elenco che identifica i server inclusi per l'ondata specificata.

Lo stato previsto per i server di origine inclusi nell'ambito e pronti per l'avvio è Integro. Se ricevete uno stato diverso per un server, significa che non è ancora pronto per l'avvio.

La seguente schermata di un esempio mostra che tutti i server dell'ondata corrente hanno terminato la replica e sono pronti per il test o il cutover.

```
*****
* Verify replication status *
*****
Migration Factory : You have successfully logged in

#####
### Replication Status for Account: 515800000000 , region: us-east-1 ###
#####
Server Server-T1 replication status: Healthy
Server Server1 replication status: Healthy

#####
### Replication Status for Account: 114707000000 , region: us-east-2 ###
#####
Server MF-Ubuntu replication status: Healthy
Server Server-T15 replication status: Healthy
Server Server2 replication status: Healthy
```

Facoltativamente, è possibile verificare lo stato nell'interfaccia web di Migration Factory.

Verifica lo stato dell'istanza di destinazione

Questa attività verifica lo stato dell'istanza di destinazione controllando il processo di avvio di tutti i server di origine interessati nella stessa ondata. L'avvio delle istanze di destinazione può richiedere fino a 30 minuti. Puoi controllare lo stato manualmente accedendo alla console Amazon EC2, cercando il nome del server di origine e verificando lo stato. Riceverai un messaggio di controllo dello stato di salute indicante che due controlli sono stati superati, il che indica che l'istanza è integra dal punto di vista dell'infrastruttura.

Tuttavia, per una migrazione su larga scala, controllare lo stato di ogni istanza richiede molto tempo, quindi puoi eseguire questo script automatizzato per verificare che i 2/2 controlli abbiano superato lo stato per tutti i server di origine in una determinata ondata.

Utilizza la seguente procedura del server di automazione della migrazione per verificare lo stato dell'istanza di destinazione.

1. Effettuato l'accesso come amministratore, aprite un prompt dei comandi (CMD.exe).
2. Vai alla `c:\migrations\scripts\script_mgn_3-Verify-instance-status` cartella ed esegui il seguente comando Python:

```
python 3-Verify-instance-status.py --Waveid <wave-id>
```

Sostituisci `<wave-id>` con il valore Wave ID appropriato per verificare lo stato dell'istanza. Questo script verifica il processo di avvio dell'istanza per tutti i server di origine di questa ondata.

3. Lo script restituisce un elenco dell'elenco dei server e degli ID di istanza per l'ondata specificata.
4. Lo script restituirà quindi un elenco di ID di istanza di destinazione.

Note

Se viene visualizzato un messaggio di errore indicante che l'ID dell'istanza di destinazione non esiste, il processo di avvio potrebbe essere ancora in esecuzione. Attendi qualche minuto prima di continuare.

5. Riceverai controlli sullo stato delle istanze che indicano se le istanze di destinazione hanno superato i 2/2 controlli di integrità.

Note

Se le istanze target non superano i 2/2 controlli di integrità per la prima volta, è possibile che il processo di avvio richieda più tempo per essere completato. Ti consigliamo di eseguire i controlli sanitari una seconda volta circa un'ora dopo il primo controllo sanitario. Ciò garantisce il completamento del processo di avvio. Se i controlli sanitari falliscono questa seconda volta, vai al [centro di AWS supporto](#) per registrare una richiesta di assistenza.

Chiudi i server di origine inclusi nell'ambito

Questa attività spegne i server di origine pertinenti coinvolti nella migrazione. Dopo aver verificato lo stato di replica dei server di origine, si è pronti a spegnere i server di origine per interrompere le transazioni dalle applicazioni client ai server. È possibile spegnere i server di origine nella finestra Cutover. Lo spegnimento manuale dei server di origine potrebbe richiedere cinque minuti per server e, per ondate di grandi dimensioni, alcune ore in totale. È invece possibile eseguire questo script di automazione per spegnere tutti i server in una determinata ondata.

Utilizza la seguente procedura del server di automazione della migrazione per spegnere tutti i server di origine coinvolti nella migrazione.

1. Effettuato l'accesso come amministratore, apri il prompt dei comandi (CMD.exe).
2. Vai alla `c:\migrations\scripts\script_mgn_3-Shutdown-all-servers` cartella ed esegui il seguente comando Python:

```
Python 3-Shutdown-all-servers.py -Waveid <wave-id>
```

3. <wave-id> Sostituiscilo con il valore Wave ID appropriato per spegnere i server di origine.
3. Lo script restituisce un elenco dell'elenco dei server e degli ID di istanza per il wave specificato.
4. Lo script chiude innanzitutto i server Windows nell'ondata specificata. Dopo la chiusura dei server Windows, lo script passa all'ambiente Linux e richiede le credenziali di accesso. Dopo aver effettuato correttamente l'accesso, lo script chiude i server Linux.

Recupera l'IP dell'istanza di destinazione

Questa attività recupera l'IP dell'istanza di destinazione. Se l'aggiornamento DNS è un processo manuale nel tuo ambiente, dovrai ottenere i nuovi indirizzi IP per tutte le istanze di destinazione.

Tuttavia, puoi utilizzare lo script di automazione per esportare i nuovi indirizzi IP per tutte le istanze dell'ondata specificata in un file CSV.

Utilizza la seguente procedura dal server di automazione della migrazione per recuperare gli IP dell'istanza di destinazione.

1. Effettuato l'accesso come amministratore, apri il prompt dei comandi (CMD).exe.
2. Vai alla cartella `c:\migrations\scripts\script_mgn_4-Get-instance-IP` ed esegui il seguente comando Python:

```
Python 4-Get-instance-IP.py --Waveid <wave-id>
```

Sostituisci `<wave-id>` con il valore Wave ID appropriato per ottenere i nuovi indirizzi IP per le istanze di destinazione.

3. Lo script restituisce un elenco di server e le informazioni sull'ID dell'istanza di destinazione.
4. Lo script restituirà quindi l'IP del server di destinazione.

Lo script esporta le informazioni sul nome del server e sugli indirizzi IP in un file CSV (`<wave-id>-<project-name>-lps.csv`) e lo colloca nella stessa directory dello script di migrazione (`c:\migrations\scripts\script_mgn_4-Get-instance-IP`).

Il file CSV fornisce i dettagli di `instance_name` e `instance_IPS`. Se l'istanza contiene più di un NIC o IP, questi verranno tutti elencati e separati da virgole.

Verifica le connessioni al server di destinazione

Questa attività verifica le connessioni per il server di destinazione. Dopo aver aggiornato i record DNS, puoi connetterti alle istanze di destinazione con il nome host. In questa attività, si verifica se è possibile accedere al sistema operativo utilizzando Remote Desktop Protocol (RDP) o tramite l'accesso Secure Shell (SSH). È possibile accedere manualmente a ciascun server singolarmente, ma è più efficiente testare la connessione al server utilizzando lo script di automazione.

Utilizzare la seguente procedura del server di automazione della migrazione per verificare le connessioni per il server di destinazione.

1. Effettuato l'accesso come amministratore, aprite il prompt dei comandi (CMD).exe.
2. Vai alla `c:\migrations\scripts\script_mgn_4-Verify-server-connection` cartella ed esegui il seguente comando Python:

```
Python 4-Verify-server-connection.py --Waveid <wave-id>
```

Sostituisci <wave-id> con il valore Wave ID appropriato per ottenere i nuovi indirizzi IP per le istanze di destinazione.

Note

Questo script utilizza la porta RDP 3389 predefinita e la porta SSH 22. <rdp-port><ssh-port> Se necessario, è possibile aggiungere i seguenti argomenti per ripristinare le porte predefinite: `--rdpPort` `--SSHPort`.

3. Lo script restituisce un elenco di server.
4. Lo script restituisce i risultati del test per l'accesso RDP e SSH.

Riferimento

Questa sezione fornisce riferimenti per la distribuzione della soluzione Cloud Migration Factory on AWS.

Raccolta di dati anonimizzata

Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. Una volta attivata, le seguenti informazioni vengono raccolte e inviate ad AWS:

- ID della soluzione: l'identificatore della AWS soluzione
- ID univoco (UUID): identificatore univoco generato casualmente per ogni Cloud Migration Factory in fase di implementazione della soluzione AWS
- Timestamp: marcatura temporale di raccolta dati
- Stato: Status viene migrato una volta avviato un server in AWS MGN con questa soluzione
- Regione: la AWS regione in cui viene distribuita la soluzione

Note

AWS sarà proprietaria dei dati raccolti tramite questo sondaggio. La raccolta dei dati sarà soggetta alla [politica sulla privacy di AWS](#). Per disattivare questa funzionalità, completa i seguenti passaggi prima di avviare il AWS CloudFormation modello.

1. Scarica il [AWS CloudFormation modello](#) sul tuo disco rigido locale.
2. Apri il AWS CloudFormation modello con un editor di testo.
3. Modifica la sezione AWS CloudFormation di mappatura dei modelli da:

```
Send:  
  AnonymousUsage:  
    Data: 'Yes'
```

to:

```
Send:
  AnonymousUsage:
    Data: 'No'
```

4. Accedi alla [console AWS CloudFormation](#).
5. Seleziona Crea pila.
6. Nella pagina Crea stack, sezione Specificare il modello, seleziona Carica un file modello.
7. In Carica un file modello, scegli Scegli file e seleziona il modello modificato dall'unità locale.
8. Scegli Avanti e segui i passaggi descritti in [Avvia lo stack](#) nella sezione Distribuzione automatizzata di questa guida.

Risorse correlate

Formazione AWS

- [Utilizzando il corso AWS Solutions: Cloud Migration Factory Skill Builder](#): imparerai a conoscere le caratteristiche, i vantaggi e l'implementazione tecnica della soluzione.
- [Solo partner AWS: migrazione avanzata ad AWS \(tecnica, in aula\)](#): imparerai come migrare carichi di lavoro su larga scala e illustra i modelli di migrazione più comuni, incluso un workshop pratico per Cloud Migration Factory su AWS.

Servizi AWS

- [AWS CloudFormation](#)
- [AWS Lambda](#)
- [Gateway Amazon API](#)
- [Amazon CloudFront](#)
- [Amazon Cognito](#)
- [Amazon DynamoDB](#)
- [Amazon Simple Storage Service](#)
- [AWS Systems Manager](#)
- [AWS Secrets Manager](#)

Risorse AWS

- [CloudEndure Guida Migration Factory](#)

Collaboratori

Le seguenti persone hanno contribuito a questo documento:

- Aijun Peng
- Chris Baker
- Dev Kar
- Dilshad Hussain
- Gnanasekaran Kailasam
- Jijo James
- Lakshmi Sudhakar Nekkanti
- Lyka Segura
- Phi Nguyen
- Shyam Kumar
- Sapeksh Madan
- Simon Champion
- Thiemo Belmega
- Vijesh Vijayakumaran Nair
- Wally Lu

Revisioni

Data	Modifica
Giugno 2020	Rilascio iniziale
febbraio 2021	Versione v1.1.0: è stato aggiunto il componente opzionale di monitoraggio della migrazione; per ulteriori informazioni sulle nuove funzionalità, fare riferimento al file ChangeLog.md nel repository. GitHub
maggio 2021	Versione v1.1.1: funzioni AWS Lambda aggiornate per supportare Python v3.7; per ulteriori informazioni, consulta il file ChangeLog.md nel repository. GitHub
agosto 2021	Versione v2.0.0: nuova funzionalità da integrare con AWS Application Migration Service (AWS MGN); per ulteriori informazioni, fare riferimento al file ChangeLog.md nel repository . GitHub
settembre 2021	Versione v2.0.1: correzioni di bug; per ulteriori informazioni, fare riferimento al file ChangeLog.md nel repository. GitHub
ottobre 2021	Versione v2.0.2: correzioni di bug; per ulteriori informazioni, fare riferimento al file ChangeLog.md nel repository. GitHub
giugno 2022	Versione v3.0.0: nuova interfaccia utente Web e funzionalità per eseguire tutte le attività di automazione direttamente dall'interfaccia utente utilizzando la nuova funzionalità di automazione remota. Questa versione rimuove i requisiti per passare dalla riga di comando del server di automazione all'interfaccia utente Web, fornendo un'unica visualizzazione di automazione della migrazione. Abbiamo introdotto Replatform to EC2, che consente la migrazione per eseguire implementazioni di nuove istanze EC2 in base alle configurazioni caricate nel datastore di Cloud Migration Factory, offrendo a Migration Waves la possibilità di avere una combinazione di strategie di migrazione, con Replatform to EC2 e Rehost che utilizza MGN gestito tramite

Data	Modifica	
	un'unica console Cloud Migration. Per ulteriori informazioni sulle nuove funzionalità, consulta il file Changelog.md nel repository. GitHub	
ottobre 2022	Versione v3.1.0: Aggiunto il supporto per i tipi di distribuzione pubblica, pubblica con e privata disponibili come AWS WAF opzioni durante la distribuzione in stack. CloudFormation Questa versione include anche aggiornamenti minori basati sul feedback della comunità degli utenti. Per ulteriori informazioni sulle nuove funzionalità, fate riferimento al file ChangeLog.md nel repository. GitHub	
Dicembre 2022	Versione v3.2.0: Aggiunto il supporto opzionale per i provider di identità esterni e la gestione dei gruppi nella console CMF. Per ulteriori informazioni sulle nuove funzionalità, fate riferimento al file ChangeLog.md nel repository. GitHub	
Dicembre 2022	Versione v3.2.0: Aggiunto il supporto opzionale per i provider di identità esterni e la gestione dei gruppi nella console CMF. Aggiornamenti minori ad altri componenti aggiuntivi. Per ulteriori informazioni sugli aggiornamenti, fate riferimento al file ChangeLog.md nel repository. GitHub	
gennaio 2023	Versione v3.2.1: pacchetto di richieste python aggiornato alla 4.1.0 per mitigare l'avviso di sicurezza sul pacchetto certifi python dipendente, fai riferimento al file ChangeLog.md nel repository per tutti i dettagli. GitHub	
Aprile 2023	Versione v3.2.2: Impatto mitigato causato dalle nuove impostazioni predefinite per S3 Object Ownership (ACL disabilitate) per tutti i nuovi bucket S3. Per ulteriori informazioni, fate riferimento al file ChangeLog.md nel repository. GitHub	

Data	Modifica
Giugno 2023	Versione v3.3.0: l'automazione dell'inserimento del carico di lavoro di AWS Managed Services (AMS) è stata rimossa; un significativo refactoring del codice sorgente per migliorare la manutenibilità e supportare le versioni future; e aggiornamenti minori e correzioni di bug ad altri componenti. Per ulteriori informazioni, consulta il file Changelog.md nel repository. GitHub
Ottobre 2023	Versione v3.3.1: significativo refactoring del codice sorgente per migliorare la manutenibilità per supportare le versioni future; e aggiornamenti minori e correzioni di bug ad altri componenti. Per ulteriori informazioni, fate riferimento al file ChangeLog.md nel repository. GitHub
Novembre 2023	Aggiornamento della documentazione: sono stati aggiunti i tag di costo di conferma associati alla soluzione nella AppRegistry sezione Monitoraggio della soluzione con AWS Service Catalog.
Dicembre 2023	Versione v3.3.2: significativo refactoring del codice sorgente per migliorare la manutenibilità per supportare le versioni future; e aggiornamenti minori e correzioni di bug ad altri componenti. Per ulteriori informazioni, fate riferimento al file ChangeLog.md nel repository. GitHub
Gennaio 2024	Versione v3.3.3: aggiornamenti minori alle autorizzazioni IAM negli account di destinazione e altre correzioni di bug, oltre a un ulteriore refactoring del codice sorgente per migliorar e la manutenibilità. Per ulteriori informazioni, consulta il file Changelog.md nel repository. GitHub

Data	Modifica	
aprile 2024	<p>Versione v3.3.4: è stato corretto un bug che causava errori durante la visualizzazione degli attributi JSON nell'interfaccia utente; è stato inoltre risolto un errore durante l'esportazione in Excel quando i campi contengono grandi quantità di dati. Durante CloudFormation gli aggiornamenti, gli script di automazione vengono ora aggiornati. Inoltre, è stato completato un ulteriore refactoring del codice per migliorare la manutenibilità. Per ulteriori informazioni, fare riferimento al file ChangeLog.md nel repository. GitHub</p>	

Note

I clienti sono responsabili di effettuare una valutazione indipendente delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le offerte e le pratiche attuali dei AWS prodotti, che sono soggette a modifiche senza preavviso e (c) non crea alcun impegno o garanzia da parte AWS dei suoi affiliati, fornitori o licenziatari. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità nei confronti dei propri clienti sono regolate da accordi AWS e questo documento non fa parte né modifica alcun accordo tra i suoi clienti AWS e i suoi clienti.

La soluzione Cloud Migration Factory su AWS è concessa in licenza secondo i termini del [MIT No Attribution](#).

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.