



Implementierungshandbuch

Cloud Migration Factory auf AWS



Cloud Migration Factory auf AWS: Implementierungshandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Übersicht über die Lösung	1
Features und Vorteile	2
Anwendungsfälle	3
Konzepte und Definitionen	3
Übersicht über die Architektur	5
Architekturdiagramm	5
Optionaler Migrationstracker	6
AWSÜberlegungen zu Well-Architected Design	8
Operational Excellence	8
Sicherheit	8
Zuverlässigkeit	8
Leistungseffizienz	9
Kostensoptimierung	9
Nachhaltigkeit	9
Einzelheiten zur Architektur	10
Server zur Migrationsautomatisierung	10
Migrationsdienste, Rest-APIs	11
Dienste einloggen	11
Admin-Dienste	11
Dienste für Benutzer	12
Tools und Dienste	12
Migration Factory-Weboberfläche	13
AWS-Dienste in dieser Lösung	13
Planen Sie Ihren Einsatz	18
Kosten	18
(Optional/empfohlen) Stellen Sie eine Amazon Elastic Compute Cloud-Instanz bereit, um die Ausführung von Automatisierungsskripten zu unterstützen	20
Sicherheit	21
IAM-Rollen	21
Amazon Cognito	21
Amazonas CloudFront	21
Amazon AWS WAF — Firewall für Webanwendungen	22
Unterstützte AWS Regionen	22
Kontingente	23

Kontingente für AWS Dienste in dieser Lösung	24
AWS CloudFormation-Kontingente	24
Bereitstellen der Lösung	25
Voraussetzungen	25
Berechtigungen des Quellservers	25
AWS Application Migration Service (AWS MGN)	25
Private Bereitstellung	25
AWS CloudFormation-Vorlagen	25
Übersicht über den Bereitstellungsprozess	26
Schritt 1: Wählen Sie Ihre Bereitstellungsoption	27
Schritt 2: Starten des Stacks	28
Schritt 3: Starten des Zielkonto-Stacks im AWS Zielkonto	37
Schritt 4: Erstellen des ersten Benutzers	38
Erstellen Sie den ersten Benutzer und melden Sie sich bei der Lösung an	38
Hinzufügen eines Benutzers zur Admin-Gruppe	40
Identifizieren der CloudFront URL	40
Schritt 5: (Optional) Bereitstellen statischer Inhalte der privaten Webkonsole	41
Schritt 6: Aktualisieren des Factory-Schemas	42
Aktualisieren der aws_accountid für AWS MGN	42
Schritt 7: Konfigurieren eines Migrationsautomatisierungsservers	43
Erstellen eines Windows Server 2016 oder höher-Servers	43
Installieren der erforderlichen Software zur Unterstützung der Automatisierungen	44
Konfigurieren von AWS Berechtigungen für den Migrationsautomatisierungsserver und Installieren von AWS Systems Manager Agent (SSM Agent)	45
Schritt 8: Testen der Lösung mit den Automatisierungsskripten	51
Importieren von Migrationsmetadaten in die Factory	51
Zugriff auf die Domains	56
Durchführen eines Testlaufs der Migrationsautomatisierung	56
Schritt 9: (Optional) Erstellen eines Migrations-Tracker-Dashboards	57
Festlegen der QuickSight Berechtigung und der Verbindungen	57
Erstellen eines Dashboards	66
Schritt 10: (Optional) Konfigurieren zusätzlicher Identitätsanbieter in Amazon Cognito	76
Überwachung der Lösung mit Service Catalog AppRegistry	79
Aktivieren Sie CloudWatch Application Insights	80
Aktiviere AWS Cost Explorer	82
Aktivieren Sie die mit der Lösung verknüpften Kostenzuweisungs-Tags	83

Bestätigen Sie die mit der Lösung verknüpften Kostenschilder	83
Aktualisieren Sie die Lösung	85
Deinstalliere die Lösung	87
Leeren Amazon S3 SBUckets	87
Verwenden vonAWS Management Console, um den Stapel zu löschen	87
Wird verwendetAWS Command Line Interface, um den Stapel zu löschen	88
Benutzerhandbuch	89
Verwaltung von Metadaten	89
Daten anzeigen	89
Einen Datensatz hinzufügen oder bearbeiten	90
Löschen eines Datensatzes	91
Daten exportieren	91
Importieren von -Daten	92
Verwaltung von Anmeldedaten	95
Fügen Sie ein Geheimnis hinzu	96
Bearbeiten Sie ein Geheimnis	97
Löschen eines Secrets	97
Führen Sie die Automatisierung von der Konsole aus aus	97
Führen Sie Automatisierungen von der Befehlszeile aus	100
Manuelles Ausführen eines Automatisierungspakets	100
Erstellung der Datei .json FactoryEndpoints	101
Starten Sie AWS MGN-Jobs von Cloud Migration Factory	102
Erforderliche Aktivitäten	103
Ursprüngliche Definition	103
Einen Job initiieren	105
Umstellung auf EC2	106
Voraussetzungen	106
Anfängliche Konfiguration	107
Bereitstellungsmaßnahmen	110
Verwaltung von Skripten	111
Laden Sie ein neues Skriptpaket hoch	112
Laden Sie Skriptpakete herunter	112
Neue Version eines Skriptpakets hinzufügen	113
Löschen von Skriptpaketen und Versionen	113
Ein neues Skriptpaket zusammenstellen	113
Schemaverwaltung	118

Ein Attribut hinzufügen/bearbeiten	118
Verwaltung von Berechtigungen	129
Richtlinien	131
Rollen	132
Entwicklerhandbuch	133
Quellcode	133
Zusätzliche Themen	134
Liste der automatisierten Migrationsaktivitäten mithilfe der Factory-Webkonsole	134
Prüfen Sie die Voraussetzungen	134
Installieren Sie die Replikationsagenten	135
Veröffentlichen Sie die Post-Launch-Skripte	136
Überprüfen Sie den Replikationsstatus	137
Überprüfen Sie die Startvorlage	138
Starten Sie Instances zum Testen	139
Überprüfen Sie den Status der Zielinstanz	140
Als bereit für die Umstellung markieren	141
Fahren Sie die Quellserver im Geltungsbereich herunter	142
Starten Sie Instanzen für Cutover	143
Liste der automatisierten Migrationsaktivitäten mithilfe der Befehlszeile	143
Prüfen Sie die Voraussetzungen	144
Installieren Sie die Replikationsagenten	146
Veröffentlichen Sie die Post-Launch-Skripte	148
Überprüfen Sie den Replikationsstatus	150
Überprüfen Sie den Status der Zielinstanz	151
Fahren Sie die Quellserver im Geltungsbereich herunter	152
Rufen Sie die Zielinstanz-IP ab	153
Überprüfen Sie die Verbindungen zum Zielservers	154
Referenz	156
Anonymisierte Datenerfassung	156
Zugehörige Ressourcen	157
Mitwirkende	158
Revisionen	159
Hinweise	162
.....	clxiii

Koordinieren und Automatisieren von groß angelegten Migrationen zur AWS Cloud mithilfe der Lösung Cloud Migration Factory in AWS

Veröffentlichungsdatum: Juni 2020 ([letzte Aktualisierung](#): Januar 2024)

Die Cloud Migration Factory in-AWS-Lösung wurde entwickelt, um manuelle Prozesse für groß angelegte Migrationen mit einer großen Anzahl von Servern zu koordinieren und zu automatisieren. Diese Lösung hilft Unternehmen bei der Verbesserung der Leistung und verhindert lange Cutover-Fenster, indem sie eine Orchestrierungsplattform für die Migration von Workloads in AWS großem Umfang bereitstellt. [AWS Professional Services](#), [AWS -Partner](#) und andere Unternehmen haben diese Lösung bereits verwendet, um Kunden bei der Migration von Tausenden von Servern zur zu unterstützen AWS Cloud.

Diese Lösung unterstützt Sie bei Folgendem:

- Integrieren Sie die vielen verschiedenen Arten von Tools, die die Migration unterstützen, z. B. Erkennungstools, Migrationstools und Tools für die Konfigurationsmanagementdatenbank (CMDB).
- Automatisieren Sie Migrationen, die viele kleine, manuelle Aufgaben beinhalten, die einige Zeit in Anspruch nehmen und langsam und schwer zu skalieren sind.

Ein end-to-end vollständiges Bereitstellungshandbuch für diese Lösung finden Sie unter [Automatisieren von groß angelegten Servermigrationen mit Cloud Migration Factory](#) im AWS Cloud Migration Factory Guide für Prescriptive Guidance.

In diesem Leitfaden zur Implementierung werden Überlegungen zur Architektur und zu den Konfigurationsschritten für die Bereitstellung der Cloud Migration Factory in-AWS-Lösung in der Amazon Web Services (AWS) Cloud erörtert. Es enthält Links zu [AWS CloudFormation](#) Vorlagen, die die für die Bereitstellung dieser Lösung erforderlichen AWS Services mithilfe AWS bewährter Methoden für Sicherheit und Verfügbarkeit starten und konfigurieren.

Der Leitfaden richtet sich an IT-Infrastrukturarchitekten, Administratoren und DevOps Experten, die über praktische Erfahrungen beim Entwerfen in der verfügen AWS Cloud.

Verwenden Sie diese Navigationstabelle, um schnell Antworten auf diese Fragen zu finden:

Wenn Sie . . .	Lesen Sie . . .
<p>Machen Sie sich mit den Kosten für die Ausführung dieser Lösung vertraut.</p> <p>Die geschätzten Kosten für den Betrieb dieser Lösung in der us-east-1 Region betragen 14,31 USD pro Monat für -AWSRessourcen.</p>	Kosten
Machen Sie sich mit den Sicherheitsüberlegungen für diese Lösung vertraut.	Sicherheit
Erfahren Sie, wie Sie Kontingente für diese Lösung planen.	Kontingente
Erfahren Sie, welche diese Lösung AWS-Regionen unterstützen.	Unterstützte AWS-Regionen
Zeigen Sie die in dieser Lösung enthaltenen AWS CloudFormation Vorlagen an oder laden Sie sie herunter, um die Infrastrukturressourcen (den „Stack“) für diese Lösung automatisch bereitzustellen.	AWS CloudFormation-Vorlagen

Features und Vorteile

Die Lösung bietet die folgenden Funktionen:

Verwalten, verfolgen und initiieren Sie Ihre Workload-Migration zu AWS von einer einzigen Weboberfläche aus, die mehrere Ziele AWS-Konten und Regionen unterstützt.

Wird mit statischem Amazon S3-Website-Hosting oder in privater Bereitstellung von einer Amazon EC2-Instance bereitgestellt, auf der ein Webserver ausgeführt wird. Alle von der Lösung durchgeführten Aktivitäten werden von mit einer einzigen Weboberfläche initiiert, die von der Lösung bereitgestellt wird. Einzelheiten finden Sie unter Migration Factory-Webschnittstelle.

Vorgefertigte Automatisierungsaufgaben zur Ausführung vieler Aufgaben, die für die vollständige Migration von Workloads zu AWS mit AWS Application Migration Service erforderlich sind.

Die Lösung bietet alle Automatisierungsaufgaben, die erforderlich sind, um Tausende von Workloads zu migrieren, AWS ohne dass Skripts erforderlich sind und mit begrenztem Wissen, das für den Einstieg erforderlich ist. Alle Automatisierungen können von der Webschnittstelle aus initiiert werden und hinter den Szenen verwenden AWS System Manager, um die Automatisierungsaufträge auf dem/ den bereitgestellten Automatisierungsserver(n) zu initiieren und auszuführen.

Passen Sie die Lösung mit Automatisierungspaketen und Attributschemaerweiterungen an

Die meisten Migrationen erfordern die Ausführung benutzerdefinierter Automatisierungsaufgaben für Anwendungen und andere umfeldspezifische Gründe. Cloud Migration Factory in AWS unterstützt die Benutzeranpassung der bereitgestellten Skripte sowie die Möglichkeit, benutzerdefinierte Skripte in die Lösung zu laden. Die Lösung ermöglicht auch, dass der Migrationsmetadatenpeicher innerhalb von Sekunden erweitert wird, sodass Administratoren dem Schema Attribute hinzufügen und entfernen können, die während der Migration verfolgt oder verwendet werden müssen.

Integration mit Service Catalog AppRegistry und AWS Systems Manager Application Manager

Diese Lösung enthält eine Service-Catalog- AppRegistry Ressource, um die CloudFormation Vorlage der Lösung und die zugrunde liegenden Ressourcen als Anwendung sowohl in [Service Catalog AppRegistry](#) als auch in [AWS Systems Manager Application Manager](#) zu registrieren.

Mit dieser Integration können Sie die Ressourcen der Lösung zentral verwalten und Aktionen zur Anwendungssuche, -berichterstattung und -verwaltung aktivieren.

Anwendungsfälle

Migrieren und Verwalten von groß angelegten Migrationen von Workloads zu AWS

Aktivieren Sie einen einzigen Bereich der Glasansicht von groß angelegten Workload-Migrationen zu AWS. Bereitstellung von vorgefertigtem Automatisierungs-, Berichts- und rollenbasiertem Zugriff über eine einzige Weboberfläche, die speziell für Migrationen entwickelt wurde.

Konzepte und Definitionen

In diesem Abschnitt werden die wichtigsten Konzepte beschrieben und eine für diese Lösung spezifische Terminologie definiert:

Anwendung

Eine Gruppe von Ressourcen, aus denen ein einzelner Geschäftsservice oder eine einzelne Anwendung besteht.

Welle

Eine Gruppe von Anwendungen, die im selben Ereignis migriert werden. Dies könnte auf der Affinität untereinander oder einem anderen Grund basieren.

server

Quellserver, der migriert werden soll.

Datenbank

Quelldatenbank, die migriert werden soll.

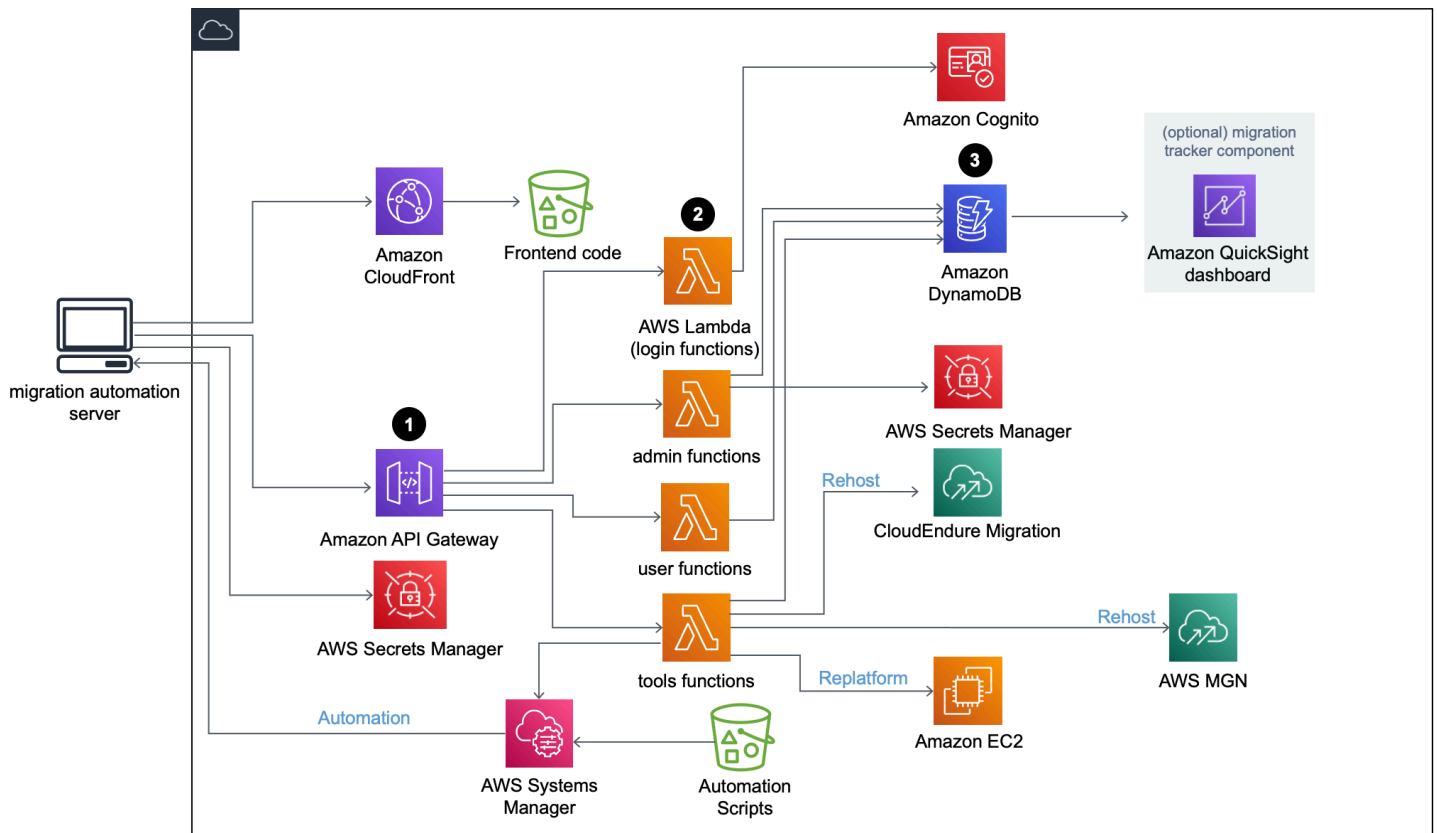
Eine allgemeine Referenz zu AWS Begriffen finden Sie im [AWS -Glossar](#) in der AWS Allgemeinen Referenz zu .

Übersicht über die Architektur

Dieser Abschnitt enthält ein Referenzdiagramm zur Implementierungsarchitektur für die mit dieser Lösung bereitgestellten Komponenten.

Architekturdiagramm

Durch die Bereitstellung der Standardlösung wird die folgende serverlose Umgebung in der AWS Cloud erstellt.



Cloud Migration Factory im AWS Architekturdiagramm

Mit der AWS CloudFormation Vorlage der Lösung werden die AWS Dienste gestartet, die Unternehmen bei der Migration ihrer Server benötigen.

Note

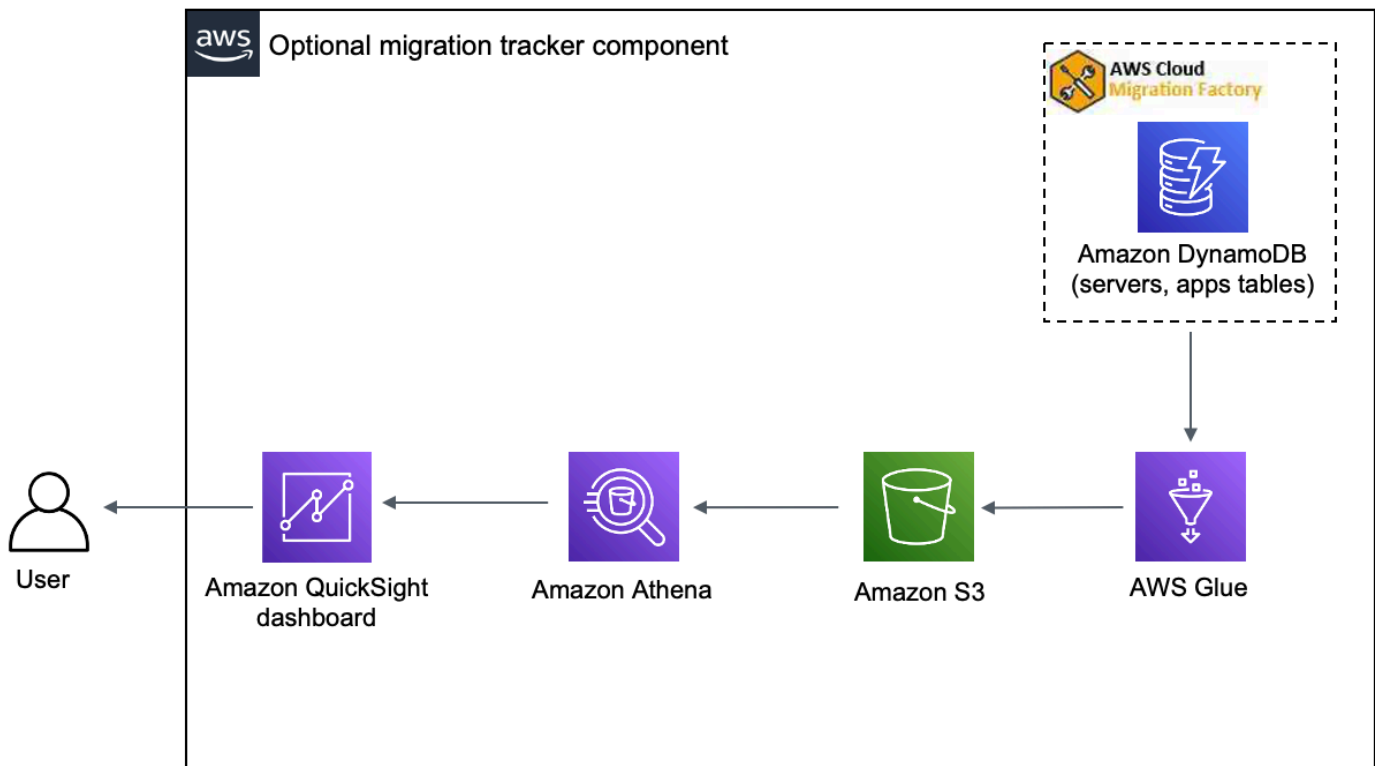
Die Cloud Migration Factory AWS on-Lösung verwendet einen Server zur Migrationsautomatisierung, der nicht Teil der AWS CloudFormation Bereitstellung ist. Weitere

Informationen zur manuellen Erstellung des Servers finden Sie unter [Einen Server für die Migrationsautomatisierung erstellen](#).

1. [Amazon API Gateway](#) empfängt Migrationsanfragen vom Migrationsautomatisierungsserver über RestAPIs.
2. [AWS Lambda](#) Funktionen bieten die erforderlichen Dienste, mit denen Sie sich an der Weboberfläche anmelden, die erforderlichen Verwaltungsfunktionen zur Verwaltung der Migration ausführen und eine Verbindung zu APIs von Drittanbietern herstellen können, um den Migrationsprozess zu automatisieren.
 - Die `user` Lambda-Funktion nimmt die Migrationsmetadaten in eine [Amazon DynamoDB-Tabelle](#) auf. Standard-HTTP-Statuscodes werden Ihnen über die RestAPI vom API Gateway zurückgegeben. Ein [Amazon Cognito Cognito-Benutzerpool](#) wird für die Benutzerauthentifizierung an der Weboberfläche und den Rest-APIs verwendet. Sie können ihn optional so konfigurieren, dass er sich bei externen SAML-Identitätsanbietern (Security Assertion Markup Language) authentifiziert.
 - Die `tools` Lambda-Funktionen verarbeiten externe Rest-APIs und rufen den [CloudEndure Migration](#) and [AWS Application Migration Service \(AWSMGN\)](#) zur AWS Migration auf. Die `tools` Lambda-Funktion ruft auch [Amazon EC2 zum Starten von EC2-Instances](#) auf und ruft [AWSSystems Manager](#) auf, um Automatisierungsskripts auf dem Migration Automation Server auszuführen.
3. Die in Amazon DynamoDB gespeicherten Migrationsmetadaten werden an die AWS MGN-API weitergeleitet, um Rehost-Migrationsaufträge zu initiieren und Server zu starten. Wenn Ihr Migrationsmuster Replatform to EC2 lautet, startet die `tools` Lambda-Funktion CloudFormation Startvorlagen im AWS-Zielkonto, um Amazon EC2 EC2-Instances zu starten.

Optionaler Migrationstracker

Diese Lösung stellt auch eine optionale Migrationstracker-Komponente bereit, die den Fortschritt Ihrer Migration verfolgt.



Optionale Komponente für den Migrations-Tracker

Die CloudFormation Vorlage wird bereitgestellt, [AWS Glue](#) um die Migrationsmetadaten aus der Cloud Migration Factory DynamoDB-Tabelle abzurufen, und exportiert die Metadaten zweimal täglich (um 5:00 Uhr und 13:00 Uhr UTC) nach [Amazon Simple Storage Service](#) (Amazon S3). Nach Abschluss des AWS Glue Jobs wird eine Amazon Athena Athena-Speicherabfrage initiiert, und Sie können Amazon so einrichten, QuickSight dass die Daten aus den Athena-Abfrageergebnissen abgerufen werden. Anschließend können Sie die Visualisierungen erstellen und ein Dashboard erstellen, das Ihren Geschäftsanforderungen entspricht. Anleitungen zum Erstellen von Grafiken und zum Erstellen eines Dashboards finden Sie unter [Erstellen eines Migrations-Tracker-Dashboards](#).

Diese optionale Komponente wird durch den Tracker-Parameter in der CloudFormation Vorlage verwaltet. Standardmäßig ist diese Option aktiviert, Sie können diese Option jedoch deaktivieren, indem Sie den Tracker-Parameter auf `ändernfalse` ändern.

AWSÜberlegungen zu Well-Architected Design

Diese Lösung nutzt die Best Practices des [AWSWell-Architected Framework](#), das Kunden dabei unterstützt, zuverlässige, sichere, effiziente und kostengünstige Workloads in der Cloud zu entwerfen und zu betreiben.

In diesem Abschnitt wird beschrieben, wie die Entwurfsprinzipien und Best Practices des Well-Architected Framework dieser Lösung zugute kommen.

Operational Excellence

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers [Operational Excellence](#) konzipiert haben.

- Ressourcen, die als IaC definiert sind und verwenden. CloudFormation
- Alle Aktionen und Auditprotokolle werden an Amazon gesendet CloudWatch, sodass automatisierte Antworten bereitgestellt werden können.

Sicherheit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der [Sicherheitssäule](#) konzipiert haben.

- IAM wird für die Authentifizierung und Autorisierung verwendet.
- Der Umfang der Rollenberechtigungen sollte so eng wie möglich sein. In vielen Fällen erfordert diese Lösung jedoch Platzhalterberechtigungen, um auf beliebige Ressourcen zugreifen zu können.
- Optionaler Einsatz von WAF zur weiteren Sicherung der Lösung.
- Amazon Coginto und optionale Möglichkeit, sich mit externen IdPs zu verbinden.

Zuverlässigkeit

[In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der Säule Zuverlässigkeit konzipiert haben.](#)

- Serverlose Dienste ermöglichen es der Lösung, eine fehlertolerante Architektur bereitzustellen.

Leistungseffizienz

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers [Leistungseffizienz](#) konzipiert haben.

- Serverlose Dienste ermöglichen eine bedarfsgerechte Skalierung der Lösung.

Kostenoptimierung

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Methoden des Pfeilers [Kostenoptimierung](#) konzipiert haben.

- Serverlose Dienste ermöglichen es Ihnen, nur für das zu bezahlen, was Sie tatsächlich nutzen.

Nachhaltigkeit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der [Säule Nachhaltigkeit](#) konzipiert haben.

- Serverlose Dienste ermöglichen es Ihnen, nach Bedarf nach oben oder unten zu skalieren.

Einzelheiten zur Architektur

Server zur Migrationsautomatisierung

Diese Lösung nutzt einen Server zur Migrationsautomatisierung, um Migrationen mithilfe von Rest-APIs durchzuführen. Dieser Server wird nicht automatisch mit der Lösung bereitgestellt und muss manuell erstellt werden. Weitere Informationen finden Sie unter [Erstellen eines Migrationsautomatisierungsservers](#). Es wird empfohlen, den Server in Ihrer AWS Umgebung zu erstellen. Sie können den Server jedoch auch lokal in Ihrer Netzwerkumgebung einrichten. Der Server muss die folgenden Anforderungen erfüllen:

- Windows Server 2016 oder spätere Versionen
- Mindestens 4 CPUs mit 8 GB RAM
- Wird als neue virtuelle Maschine bereitgestellt, ohne dass zusätzliche Anwendungen installiert sind
- (Falls eingebautAWS) In derselben Region AWS-Konto und in derselben Region wie Cloud Migration Factory

Nach der Installation benötigt der Server Internetzugang und eine uneingeschränkte interne Netzwerkkonnektivität zu den Quellservern im Geltungsbereich (Server, auf die migriert werden soll).
AWS

Wenn eine Portbeschränkung vom Migrationsautomatisierungsserver zu den Quellservern erforderlich ist, müssen die folgenden Ports vom Migrationsautomatisierungsserver zu den Quellservern geöffnet sein:

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

Es wird empfohlen, dass sich der Server für die Migrationsautomatisierung in derselben Active Directory-Domäne wie die Quellserver befindet. Wenn sich die Quellserver in mehreren Domänen befinden, bestimmt die Sicherheitskonfiguration für die Domänenvertrauensstellung in jeder Domäne, ob Sie mehr als einen Server für die Migrationsautomatisierung benötigen.

- Wenn Domänenvertrauen in allen Domänen mit Quellservern besteht, kann ein einziger Server für die Migrationsautomatisierung eine Verbindung zu allen Domänen herstellen und Automatisierungsskripts für diese ausführen.
- Wenn nicht in allen Domänen eine Domänenvertrauensstellung besteht, müssen Sie für jede nicht vertrauenswürdige Domäne einen zusätzlichen Migrationsautomatisierungsserver erstellen. Andernfalls müssen für jede Aktion, die auf dem Automatisierungsserver ausgeführt werden soll, alternative Anmeldeinformationen mit den entsprechenden Berechtigungen auf den Quellservern bereitgestellt werden.

Migrationsdienste, Rest-APIs

Die Cloud Migration Factory AWS on-Lösung automatisiert den Migrationsprozess mithilfe von Rest-APIs, die über AWS Lambda Funktionen, ein Amazon API Gateway AWS Managed Services, AWS Application Migration Service (AWS MGN) und CloudEndure Migration verarbeitet werden. Wenn Sie eine Anfrage stellen oder eine Transaktion initiieren, z. B. einen Server hinzufügen oder eine Liste von Servern oder Anwendungen anzeigen, werden Rest-API-Aufrufe an Amazon API Gateway gesendet, wodurch eine AWS Lambda Funktion zur Ausführung der Anfrage initiiert wird. In den folgenden Services werden die Komponenten für den automatisierten Migrationsprozess detailliert beschrieben.

Dienste einloggen

Zu den Anmeldediensten gehören die `login` Lambda-Funktionen und Amazon Cognito. Sobald Sie sich mit der `login` API über das API Gateway bei der Lösung angemeldet haben, validiert die Funktion die Anmeldeinformationen, ruft ein Authentifizierungstoken von Amazon Cognito ab und gibt die Token-Details an Sie zurück. Sie können dieses Authentifizierungstoken verwenden, um eine Verbindung zu den anderen Diensten in dieser Lösung herzustellen.

Admin-Dienste

Zu den Admin-Services gehören das Amazon API Gateway, `admin` Lambda-Funktionen und Amazon DynamoDB. Administratoren der Lösung können die `admin` Lambda-Funktion verwenden, um das Migrationsmetadatenchema zu definieren, bei dem es sich um die Anwendungs- und Serverattribute handelt. Die Admin-Services-API stellt die Schemadefinition für die DynamoDB-Tabelle bereit. Benutzerdaten, einschließlich Anwendungs- und Serverattributen, müssen dieser Schemadefinition entsprechen. Zu den typischen Attributen gehören die Felder `app_name` `wave_id` `server_name`,, und andere Felder, die unter [Migrationsmetadaten in die Factory importieren](#) beschrieben sind.

Standardmäßig stellt die AWS CloudFormation Vorlage automatisch ein gemeinsames Schema bereit, das jedoch nach der Bereitstellung angepasst werden kann.

Administratoren können auch Admin-Services verwenden, um Migrationsrollen für die Mitglieder ihres Migrationsteams zu definieren. Der Administrator hat eine detaillierte Kontrolle, um bestimmte Benutzerrollen bestimmten Attributen und Migrationsphasen zuzuordnen. Eine Migrationsphase ist ein Zeitraum, in dem bestimmte Migrationsaufgaben ausgeführt werden, z. B. eine Erstellungsphase, eine Testphase und eine Umstellungsphase.

Dienste für Benutzer

Zu den Benutzerdiensten gehören das Amazon API Gateway, user Lambda-Funktionen und Amazon DynamoDB. Benutzer können die Migrationsmetadaten verwalten, sodass sie die Wellen-, Anwendungs- und Serverdaten in der Migrationsmetadaten-Pipeline lesen, erstellen, aktualisieren und löschen können.

Hinweis

Eine Migrationswelle ist ein Konzept der Gruppierung von Anwendungen mit einem Start- und einem Ende- oder Umstellungsdatum. Zu den Wave-Daten gehören die Bewerbungen von Migrationskandidaten und die für eine bestimmte Migrationswelle geplanten Antragsgruppen.

Benutzerdienste bieten eine API für das Migrationsteam zur Bearbeitung der Daten in der Lösung: Erstellen, Aktualisieren und Löschen der Daten mithilfe des Python-Skripts und der CSV-Quelldateien. Ausführliche Schritte finden Sie unter Automatisierte Migrationsaktivitäten mit der Migration Factory-Webkonsole und Automatisierte Migrationsaktivitäten mit der Befehlszeile.

Tools und Dienste

Zu den Tool-Services gehören Amazon API Gateway, tools Lambda-Funktionen, Amazon DynamoDBAWS Managed Services, AWS Application Migration Service und Migration. CloudEndure Sie können diese Dienste verwenden, um eine Verbindung zu APIs von Drittanbietern herzustellen und den Migrationsprozess zu automatisieren. Mithilfe des Service für CloudEndure Migration und AWS Anwendungsmigration kann das Migrationsteam den Serverstartprozess mit einem einzigen Tastendruck orchestrieren, um alle Server in derselben Welle zu starten, die aus einer Gruppe von Anwendungen und Servern mit demselben Umstellungsdatum besteht. Mithilfe AWS Managed Services der Cloud Migration Factory AWS on-Lösung wird der RFC-Prozess zur Workload-Erfassung automatisiert und der manuelle Aufwand während des Migrationsprozesses reduziert.

Migration Factory-Weboberfläche

Die Lösung umfasst eine Migration Factory-Weboberfläche, die standardmäßig in einem Amazon S3 S3-Bucket oder auf einem bereitgestellten Webserver (nicht Teil der Lösungsbereitstellung) gehostet werden kann, sodass Sie die folgenden Aufgaben mit einem Webbrowser ausführen können:

- Aktualisieren Sie Wellen-, Anwendungs- und Server-Metadaten über Ihren Webbrowser
- Verwalten Sie Anwendungs- und Serverschemadefinitionen
- Führen Sie Automatisierungsskripten aus, um Migrationsaktivitäten zu automatisieren, z. B. die Voraussetzungen zu überprüfen und MGN-Agenten zu installieren
- Erstellen Sie Anmeldeinformationen für die Migration, um eine Verbindung zu den Quellservern herzustellen
- Connect zu Diensten von Drittanbietern wie AWS Application Migration Service und CloudEndure Migration her und automatisieren AWS Managed Services Sie den Migrationsprozess

AWS Dienste in dieser Lösung

AWS-Service	Beschreibung	
Amazon API Gateway	Kern. Stellt REST-APIs für die gesamte Lösung bereit, die für den Zugriff auf Backend-Daten und die Initiierung und Verwaltung von Automatisierungsaufgaben bei der Migration verwendet werden.	
AWS Lambda	Kern. Stellen Sie die erforderlichen Dienste bereit, damit Sie sich bei der Weboberfläche anmelden, die erforderlichen Verwaltungsfunktionen zur Verwaltung der Migration ausführen und eine Verbindung zu APIs von Drittanbietern herstellen können, um	

AWS-Service	Beschreibung	
	den Migrationsprozess zu automatisieren.	
Amazon DynamoDB	Kern. Metadatenpeicher für alle benutzer- und systemverwalteten Daten, auf die über Amazon API Gateways und Lambda-Funktionen zugegriffen wird.	
Amazon Cognito	Kern. Benutzerautorisierung und Authentifizierung sowie ein optionaler Verbund mit anderen IdPs werden ebenfalls über Amazon Cognito erreicht.	
AWS Systems Manager	Unterstützend. Unterstützt die Ausführung von Cloud Migration Factory auf AWS Automatisierungspaketen auf dem vom Kunden bereitgestellten Automation-Server.	
Amazon EC2	Unterstützend. Automatisierungsserver, auf dem AWS Systems Manager Manager-Agenten ausgeführt werden, um die Ausführung von Automatisierungspaketen zu ermöglichen.	

AWS-Service	Beschreibung	
Amazon S3	Unterstützend. Wird in mehreren Bereichen der Lösung verwendet, 1/ verwendet die statische Webhosting-Funktion von Amazon S3 und bedient die Haupt-Weboberfläche (über Amazon CloudFront), 2/ Protokolle und andere Automatisierungsausgaben werden von der Lösung in Amazon S3 gespeichert.	
AWS Secrets Manager	Unterstützend. Wird bei der Nutzung der Automatisierungsfunktionen der Lösung zum sicheren Speichern der Anmeldeinformationen verwendet, AWS Secrets Manager die für den Zugriff auf Migrationsressourcen verwendet werden, um Aufgaben und Aktionen zur Erleichterung und Migration von Workloads auszuführen.	

AWS-Service	Beschreibung	
Amazon CloudFront	Optional. Für Standardbereitstellungen stellt Amazon die Verteilung der Webinterface-Inhalte von Amazon S3 bereit, wodurch sie weltweit hochverfügbar sind und von überall aus sicheren TLS-Zugriff auf die Webinterface-Inhalte ermöglicht werden.	
AWS-Service zur Anwendungsmigration (AWSMGN)	Optional. Bei der Durchführung von Rehost-Migrationen von Windows- oder Linux-Workloads AWS verwendet Cloud Migration Factory on AWS MGN, um die Systemmigration zu Amazon EC2 zu erleichtern.	
Amazon QuickSight	Optional. Ermöglicht die Erstellung anpassbarer Migrations-Dashboards auf der Grundlage der Daten, die im Migrations-Metastore in Amazon DynamoDB gespeichert sind, sodass Teams die Daten erhalten, die sie benötigen, um ihre Migrationen zu verfolgen und darüber zu berichten.	

AWS-Service	Beschreibung	
AWS Glue	Optional. Extrahiert regelmäßig in Amazon DynamoDB gespeicherte Daten nach Amazon S3 und stellt Berichtsdaten zur Verwendung in Amazon Athena und Amazon-Dashboards bereit. QuickSight	
Amazon Athena	Optional. Bietet Zugriff auf Berichtsdaten, die von AWS Glue aus den Migration smetadaten extrahiert wurden, sodass Dashboards mit Amazon erstellt werden können. QuickSight	
AWSFirewall für Webanwendungen	Optional. Wenden Sie zusätzliche Sicherheitsmaßnahmen auf den Endpunkten für Amazon API Gateway und Amazon CloudFront an, um den Zugriff auf bestimmte Geräte auf der Grundlage der Quell-IP-Adresse oder anderer Zugriffskriterien einzuschränken.	

Planen Sie Ihren Einsatz

Dieser Abschnitt hilft Ihnen bei der Planung Ihrer Kosten, Sicherheit, AWS-Regionen und Bereitstellungstypen für die Cloud Migration Factory on AWS-Lösung.

Kosten

Sie sind für die Kosten der AWS Dienste verantwortlich, die Sie beim Betrieb dieser Lösung in Anspruch nehmen. Zum jetzigen Zeitpunkt belaufen sich die geschätzten Kosten für den Betrieb dieser Lösung mit Standardeinstellungen in der Region USA Ost (Nord-Virginia) und unter der Annahme, dass Sie mit dieser Lösung 200 Server pro Monat migrieren, auf etwa 14,31\$ pro Monat. Die Kosten für den Betrieb dieser Lösung hängen von der Menge der Daten ab, die geladen, angefordert, gespeichert, verarbeitet und dargestellt werden, wie in der folgenden Tabelle dargestellt.

AWS-Service	Faktoren	Kosten/Monat [USD]
Kerndienste		
Amazon API Gateway	10.000 Anfragen/Monat x (3,50 USD/Million)	0,035\$
AWS Lambda	10.000 Aufrufe/Monat (durchschnittliche Dauer 3.000 ms und 128 MB Speicher)	0,065 US-Dollar
Amazon DynamoDB	20.000 Schreibenanforderungen/ Monat x (1,25\$ pro Million \$) 40.000 Leseanforderungen/ Monat x (0,25 USD/Million \$) Datenspeicher: 1 GB x 0,25\$	0,035\$
Amazon S3	Speicherplatz (10 MB) und 50.000 Abrufanfragen/Monat	0,25\$
Amazonas CloudFront	Regionaler Datentransfer ins Internet: die ersten 10 TB	0,92\$

AWS-Service	Faktoren	Kosten/Monat [USD]
	Regionaler Datentransfer zum Ursprung: gesamte Datenübertragung HTTPS-Anfragen: 50.000 Anfragen/Monat X (0,01/10.000 Anfragen)	
AWS Systems Manager	10.000 Schritte/Monat	0,00\$
AWS Secrets Manager	5 Geheimnisse x Dauer von 30 Tagen	2,00\$
Amazon Cognito (direkte Anmeldung)	Bis zu 50.000 aktive Benutzer (MAUs) pro Monat, abgedeckt durch das kostenlose AWS-Kontingent	0,00\$
Amazon Athena	10 MB täglich x 5,00 USD pro TB gescannter Daten	0,0015\$
Optionale Dienstleistungen		
AWS Glue(optionaler Migrationstracker)	2 Minuten täglich x Standard 10 DPU x 0,44\$ pro DPU-Stunde	4,40\$
AWS WAF	2 Web ACLs 5,00\$ pro Monat (anteilig stündlich berechnet) 2 Regeln 1,00\$ pro Monat (anteilig stündlich) 10.000 Anfragen x (0,60\$ pro 1 Million Anfragen)	6,60\$

AWS-Service	Faktoren	Kosten/Monat [USD]
Amazon Cognito (SAML-Anmeldung)	Bis zu 50 MAUs im Rahmen des kostenlosen AWS-Kontingents Über 50 MAUs, 0,015 USD/MAU	0,00\$
Insgesamt:		~14,31 \$/Monat

(Empfohlen) Stellen Sie eine Amazon Elastic Compute Cloud-Instanz bereit, um die Ausführung von Automatisierungsskripten zu unterstützen

Wir empfehlen die Bereitstellung einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um die Verbindung zu den APIs und AWS Boto3-APIs der Lösung mit IAM-Rollen zu automatisieren. Bei der folgenden Kostenschätzung wird davon ausgegangen, dass sich die Amazon EC2 EC2-Instance in der us-east-1 Region befindet und acht Stunden am Tag, fünf Tage die Woche läuft.

AWS-Service	Faktoren	Kosten/Monat [USD]
Amazon EC2	176 Stunden pro Monat x 0,1108 USD/Stunde () t3.large	19,50\$
Amazon Elastic Block Store (Amazon EBS)	30 GB x 0,08 USD/GB-Monat (gp3) x (176 Stunden/720 Stunden)	0,59\$
Insgesamt:		~20,09 \$

Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite für jeden AWS Service, den Sie in dieser Lösung verwenden werden.

Sicherheit

Wenn Sie Systeme auf der AWS Infrastruktur aufbauen, teilen Sie sich die Sicherheitsverantwortung zwischen Ihnen und AWS. Dieses [gemeinsame Modell](#) kann Ihren betrieblichen Aufwand reduzieren, da AWS die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen die Services ausgeführt werden, betrieben, verwaltet und kontrolliert werden. Weitere Informationen zur Sicherheit finden Sie AWS unter [AWS Cloud Security](#).

IAM-Rollen

AWS Identity and Access Management (IAM-) Rollen können Sie Diensten und Benutzern in der Cloud detaillierte Zugriffsrichtlinien und -berechtigungen zuweisen. AWS Diese Lösung erstellt IAM-Rollen, die der AWS Lambda Funktion Zugriff auf die anderen in dieser Lösung verwendeten AWS Dienste gewähren.

Amazon Cognito

Der mit dieser Lösung erstellte Amazon Cognito Cognito-Benutzer ist ein lokaler Benutzer mit Berechtigungen, nur auf die RestAPIs für diese Lösung zuzugreifen. Dieser Benutzer hat keine Berechtigungen, auf andere Dienste in Ihrem AWS Konto zuzugreifen. Weitere Informationen finden Sie unter [Amazon Cognito User Pools](#) im Amazon Cognito Developer Guide.

Die Lösung unterstützt optional die externe SAML-Anmeldung über die Konfiguration von Federated Identity Providers und die gehostete UI-Funktionalität von Amazon Cognito.

Amazon CloudFront

Diese Standardlösung stellt eine Webkonsole bereit, die in einem Amazon S3 S3-Bucket [gehostet wird](#). Um die Latenz zu reduzieren und die Sicherheit zu verbessern, umfasst diese Lösung eine [CloudFront Amazon-Distribution](#) mit einer Ursprungszugriffsidentität. Dabei handelt es sich um einen speziellen CloudFront Benutzer, der den öffentlichen Zugriff auf die Inhalte des Website-Buckets der Lösung ermöglicht. Weitere Informationen finden Sie unter [Beschränken des Zugriffs auf Amazon S3 S3-Inhalte mithilfe einer Origin-Zugriffsidentität](#) im Amazon CloudFront Developer Guide.

Wenn bei der Stack-Bereitstellung ein privater Bereitstellungstyp ausgewählt wird, wird keine CloudFront Distribution bereitgestellt und erfordert, dass ein anderer Webhosting-Dienst zum Hosten der Webkonsole verwendet wird.

AWS WAF — Firewall für Webanwendungen

Wenn der Bereitstellungstyp im Stack Öffentlich mit [AWS WAF](#) ausgewählt ist, CloudFormation werden die erforderlichen AWS WAF Web-ACLs und Regeln bereitgestellt CloudFront, die zum Schutz von API Gateway- und Cognito-Endpunkten konfiguriert sind, die von der CMF-Lösung erstellt wurden. Diese Endpunkte werden so eingeschränkt, dass nur bestimmte Quell-IP-Adressen auf diese Endpunkte zugreifen können. Während der Stack-Bereitstellung müssen zwei CIDR-Bereiche bereitgestellt werden, sodass nach der Bereitstellung über die Konsole zusätzliche Regeln hinzugefügt werden können. AWS WAF

Unterstützte AWS Regionen

Diese Lösung verwendet Amazon Cognito und Amazon QuickSight, die derzeit nur in bestimmten AWS Regionen verfügbar sind. Daher müssen Sie diese Lösung in einer Region starten, in der diese Dienste verfügbar sind. Die aktuelle Verfügbarkeit von Diensten nach Regionen finden Sie in der [Liste der AWS regionalen Dienste](#).

Note

Die Datenübertragung während des Migrationsprozesses wird durch regionale Bereitstellungen nicht beeinträchtigt.

Cloud Migration Factory auf AWS ist in den folgenden AWS-Regionen verfügbar:

Namen der Regionen	
USA Ost (Ohio)	Asien-Pazifik (Tokio)
USA Ost (Nord-Virginia)	Kanada (Zentral)
USA West (Nordkalifornien)	Europa (Frankfurt)
USA West (Oregon)	Europa (Irland)
*Afrika (Kapstadt)	Europa (London)
*Asien-Pazifik (Hongkong)	*Europa (Mailand)

Namen der Regionen	
*Asien-Pazifik (Hyderabad)	*Europa (Spanien)
*Asien-Pazifik (Jakarta)	Europa (Paris)
*Asien-Pazifik (Melbourne)	Europa (Stockholm)
Asien-Pazifik (Mumbai)	*Europa (Zürich)
Asien-Pazifik (Osaka)	*Naher Osten (Bahrain)
Asien-Pazifik (Seoul)	*Naher Osten (VAE)
Asien-Pazifik (Singapur)	Israel (Tel Aviv)
Asien-Pazifik (Sydney)	Südamerika (São Paulo)

Important

*Aufgrund der CloudFront Amazon-Zugriffsprotokollierung nur für private Bereitstellungen verfügbar. Aktuelle Informationen finden Sie unter [Konfiguration und Verwendung von Standardprotokollen \(Zugriffsprotokollen\)](#) im Amazon CloudFront Developer Guide.

Cloud Migration Factory auf AWS ist in den folgenden AWS-Regionen nicht verfügbar:

Name der Region	Nicht verfügbare (n) Dienst (e) oder Serviceoption
AWS GovCloud (USA-Ost)	Amazon Cognito
AWS GovCloud (USA West)	Amazon Cognito

Kontingente

Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto.

Kontingente für AWS Services in dieser Lösung

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der [in dieser Lösung implementierten Dienste](#) verfügen. Weitere Informationen finden Sie unter [AWSDienstkontingente](#).

Wählen Sie einen der folgenden Links, um zur Seite für diesen Dienst zu gelangen. Um die Servicekontingente für alle AWS-Services in der Dokumentation anzuzeigen, ohne die Seiten wechseln zu müssen, zeigen Sie die Informationen der Seite [Service-Endpunkte und -kontingente](#) stattdessen in der PDF-Datei an.

AWS CloudFormation-Kontingente

Ihr System AWS-Konto verfügt über CloudFormation Kontingente, die Sie beachten sollten, wenn Sie den Stack für diese Lösung starten. Wenn Sie diese Kontingente verstehen, können Sie Limitationsfehler vermeiden, die Sie daran hindern würden, diese Lösung erfolgreich einzusetzen. Weitere Informationen finden Sie unter [AWS CloudFormationKontingente](#) im AWS CloudFormationBenutzerhandbuch.

Bereitstellen der Lösung

Diese Lösung verwendet [AWS CloudFormation Vorlagen und Stacks](#), um ihre Bereitstellung zu automatisieren. Die CloudFormation Vorlage(n) gibt(y) die in dieser Lösung enthaltenen AWS Ressourcen und ihre Eigenschaften an. Der CloudFormation Stack stellt die Ressourcen bereit, die in der/den Vorlage(n) beschrieben sind.

Voraussetzungen

Berechtigungen des Quellserver

Für Windows- und Linux-Server (sudo permissions) ist ein Domain-Benutzer mit lokalen Administratorberechtigungen für die Quellserver erforderlich, die für die Migration bestimmt sind. Wenn sich Quellserver nicht in einer Domain befinden, können andere Benutzer verwendet werden, einschließlich eines LDAP-Benutzers mit Sudo/Administratorberechtigungen oder eines lokalen Sudo/Administrator-Benutzers. Bevor Sie diese Lösung starten, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen oder sich mit der entsprechenden Person in Ihrer Organisation mit -Berechtigungen abgestimmt haben.

AWS Application Migration Service (AWS MGN)

Wenn Sie AWS MGN für diese Lösung verwenden, müssen Sie zuerst den AWS MGN-Service in jedem Zielkonto und jeder Region initialisieren, bevor Sie den Zielkonto-Stack starten. Weitere Informationen finden Sie unter [Initialisieren des Application Migration Service](#) im Benutzerhandbuch für Application Migration Service.

Private Bereitstellung

Wenn Sie sich für die Bereitstellung einer privaten Instance von CMF entschieden haben, stellen Sie einen Webserver in Ihrer Umgebung bereit, bevor Sie mit der Bereitstellung der CMF-Lösung fortfahren.

AWS CloudFormation-Vorlagen

Diese Lösung verwendet AWS CloudFormation, um die Bereitstellung der Cloud Migration Factory in-AWS-Lösung in der AWS Cloud zu automatisieren. Sie enthält die folgende AWS CloudFormation Vorlage, die Sie vor der Bereitstellung herunterladen können.

View template

aws-

cloud-migration-factory-solution.template – Verwenden Sie diese Vorlage, um die Cloud Migration Factory auf -AWSLösung und alle zugehörigen Komponenten zu starten. Die Standardkonfiguration stellt AWS Lambda Funktionen, Amazon-DynamoDB-Tabellen, ein Amazon API Gateway , Amazon CloudFront, Amazon S3-Buckets, einen Amazon Cognito-Benutzerpool, AWS Systems Manager Automation Document und [AWS Secrets Manager](#) Secrets bereit. Sie können die Vorlage jedoch auch an Ihre spezifischen Anforderungen anpassen.

View template

aws-

cloud-migration-factory-solution-target-account.template – Verwenden Sie diese Vorlage, um das/ die Zielkonto(s) der Cloud Migration Factory in AWS-Lösung zu starten. Die Standardkonfiguration stellt IAM-Rollen und einen Benutzer bereit, aber Sie können die Vorlage auch an Ihre spezifischen Anforderungen anpassen.

Übersicht über den Bereitstellungsprozess

Bevor Sie die automatisierte Bereitstellung starten, lesen Sie sich die Architektur, Komponenten und andere in diesem Leitfaden beschriebene Überlegungen durch. Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Cloud Migration Factory in-AWSLösung in Ihrem Konto zu konfigurieren und bereitzustellen.

Zeit für die Bereitstellung: ungefähr 20 Minuten

Note

Wenn Sie diese Lösung in anderen AWS-Regionen als USA Ost (Nord-Virginia) bereitstellen, kann es länger dauern, bis die Migration Factory- CloudFront URL verfügbar ist. Während dieser Zeit erhalten Sie beim Zugriff auf die Weboberfläche die Meldung Zugriffsverweigerung.

[Schritt 1: Wählen Sie Ihre Bereitstellungsoption](#)

[Schritt 2: Starten des Stacks](#)

[Schritt 3: Starten des Zielkonto-Stacks im Ziel-AWS-Konto](#)

[Schritt 4: Erstellen des ersten Benutzers](#)

[Schritt 5: \(Optional\) Bereitstellen statischer Inhalte der privaten Webkonsole](#)

[Schritt 6: Aktualisieren des Factory-Schemas](#)

[Schritt 7: Erstellen eines Migrationsautomatisierungsservers](#)

[Schritt 8: Testen der Lösung mit den Automatisierungsskripten](#)

[Schritt 9: \(Optional\) Erstellen eines Migrations-Tracker-Dashboards](#)

[Schritt 10: \(Optional\) Konfigurieren zusätzlicher Identitätsanbieter in Amazon Cognito](#)

Important

Diese Lösung umfasst die Option, anonymisierte Betriebsmetriken an zu senden AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und zugehörige Services und Produkte verwenden. AWS besitzt die im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der [AWS Datenschutzrichtlinie](#). Um sich von dieser Funktion abzumelden, laden Sie die Vorlage herunter, ändern Sie den AWS CloudFormation Zuweisungsabschnitt und verwenden Sie dann die AWS CloudFormation Konsole, um Ihre aktualisierte Vorlage hochzuladen und die Lösung bereitzustellen. Weitere Informationen finden Sie im Abschnitt [Anonymisierte Datenerfassung](#) dieses Handbuchs.

Schritt 1: Wählen Sie Ihre Bereitstellungsoption

Es gibt drei Optionen für die Bereitstellung des anfänglichen Stacks und die Auswahl der richtigen hängt von den Sicherheitsrichtlinien für die Zielumgebung ab.

Diese Optionen sind:

- Öffentlich (Standard): Alle Cloud Migration Factory auf -AWS-Endpunkten sind mit der Benutzerauthentifizierung öffentlich adressierbar. Diese Option stellt die folgenden Einstiegspunkte bereit: CloudFront Öffentliche API-Gateway-Endpunkte und Cognito.

- Öffentlich mit AWS WAF: Der Zugriff auf Cloud Migration Factory-Endpunkte ist auf anpassbare CIDR-Bereiche beschränkt. Diese Option stellt die folgenden Einstiegspunkte bereit: CloudFrontÖffentliche API-Gateway-Endpunkte, Cognito und AWS WAF Einschränken des Zugriffs auf bestimmte CIDR-Bereiche.
- Privat: Alle Cloud Migration Factory-Endpunkte sind nur von Ihren VPC-Netzwerken aus zugänglich und die Cloud Migration Factory auf der AWS Webkonsole muss auf einem privaten Webserver gehostet werden, der separat bereitgestellt wird. Diese Option stellt die folgenden Einstiegspunkte bereit: [Private API Gateway-Endpunkte](#) (nur innerhalb einer VPC zugänglich) und Cognito.

Schritt 2: Starten des Stacks

Important

Diese Lösung beinhaltet die Option, anonymisierte Betriebsmetriken an AWS zu senden. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und zugehörige Services und Produkte verwenden. AWS besitzt die im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der [AWS-Datenschutzrichtlinie](#) . Um sich von dieser Funktion abzumelden, laden Sie die Vorlage herunter, ändern Sie den AWS CloudFormation Zuweisungsabschnitt und verwenden Sie dann die AWS CloudFormation Konsole, um Ihre Vorlage hochzuladen und die Lösung bereitzustellen. Weitere Informationen finden Sie im [Anonymisierte Datenerfassung](#) Abschnitt dieses Handbuchs.

Diese automatisierte AWS CloudFormation Vorlage stellt die Lösung Cloud Migration Factory in AWS in der AWS Cloud bereit.

Note

Sie sind für die Kosten der AWS Services verantwortlich, die bei der Ausführung dieser Lösung verwendet werden. Weitere Informationen finden Sie im [Kosten](#) Abschnitt . Ausführliche Informationen finden Sie auf der Webseite mit den Preisen für jeden AWS Service, den Sie in dieser Lösung verwenden werden.

1. Melden Sie sich bei der an AWS Management Console und wählen Sie die Schaltfläche aus, um die `cloud-migration-factory-solution` AWS CloudFormation Vorlage zu starten.



Sie können auch [die Vorlage herunterladen](#) als Ausgangspunkt für eine eigene Implementierung verwenden.

- Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der Konsole.


Note


Diese Lösung verwendet Amazon Cognito und Amazon QuickSight, die derzeit nur in bestimmten AWS Regionen verfügbar sind. Daher müssen Sie diese Lösung in einer -AWSRegion starten, in der diese Services verfügbar sind. Die aktuellste Verfügbarkeit nach Regionen finden Sie in der [AWS Liste der regionalen Services](#).

Bei der Bereitstellung in Public und Public mit WAF-Bereitstellungstypen verwendet die Lösung auch die Amazon- CloudFront Protokollierung in Amazon S3. Heute ist die Protokollzustellung von Amazon CloudFront an Amazon S3 nur in bestimmten -Regionen verfügbar. Weitere Informationen finden Sie unter [Auswählen eines Amazon S3-Buckets für Ihre Standardprotokolle](#), um zu überprüfen, ob Ihre Region unterstützt wird.

- Überprüfen Sie auf der Seite Stack erstellen, ob die richtige Vorlagen-URL im Textfeld Amazon S3-URL angezeigt wird, und wählen Sie Weiter aus.
- Weisen Sie Ihrem Lösungs-Stack auf der Seite Stack-Details angeben einen Namen zu.
- Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
Anwendungsname	migration-factory	Geben Sie ein Präfix für die AWS CloudFormation physische ID ein, das die von dieser Lösung bereitgestellte AWS Services identifiziert.


Parameter	Standard	Beschreibung
		<p> Note</p> <p>Der Anwendung sname wird als Präfix verwendet, um die bereitgestellten AWS Ressourcen zu identifizieren:</p> <p><i><application-name> -<environment-name> -<aws-resource></i> . Wenn Sie den Standardnamen ändern, empfehlen wir, die kombinierten Präfixbezeichnungen auf 40 Zeichen oder weniger zu belassen, um sicherzustellen, dass Sie die Zeichenbeschränkungen nicht überschreiten.</p>

Parameter	Standard	Beschreibung
Umgebungsname	test	<p>Geben Sie einen Namen ein, um die Netzwerkumgebung zu identifizieren, in der die Lösung bereitgestellt wird. Wir empfehlen einen beschreibenden Namen wie test, dev oder prod.</p> <div data-bbox="1089 590 1507 1766" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Der Umgebungsname wird als Präfix verwendet, um die bereitgestellten AWS Ressourcen zu identifizieren: <i><application-name> -<environment-name> -<aws-resource></i>. Wenn Sie den Standardnamen ändern, empfehlen wir, die kombinierten Präfixbezeichnungen auf 40 Zeichen oder weniger zu belassen, um sicherzustellen, dass Sie die Zeichenbeschränkungen nicht überschreiten.</p></div>

Parameter	Standard	Beschreibung
Migration Tracker	<code>true</code>	Standardmäßig ist das optionale Migrations-Tracker-Dashboard aktiviert, aber Sie können es deaktivieren, indem Sie diesen Parameter in <code>ändernfalse</code> .
Plattformwechsel EC2	<code>true</code>	Standardmäßig ist die Funktion Plattform-EC2 ersetzen aktiviert, aber Sie können sie deaktivieren, indem Sie diesen Parameter in <code>ändernfalse</code> .
ServiceAccountEmail	<code>serviceaccount@yourdomain.com</code>	Standard-E-Mail-Adresse des Servicekontos, die Automatisierungsskripte der Migrationsfabrik verwenden dieses Konto, um eine Verbindung mit der Factory-API herzustellen.
Zulassen, dass ein zusätzlicher Identitätsanbieter in Cognito konfiguriert wird	<code>false</code>	Standardmäßig verwendet die Lösung Amazon Cognito, um den Zugriff zu erstellen und zu verwalten. Wenn Sie diesen Parameter in <code>änderttrue</code> , wird die Lösung so konfiguriert, dass externe SAML-Identitätsanbieter zu Amazon Cognito hinzugefügt und für die Anmeldung verwendet werden können.

Parameter	Standard	Beschreibung
Bereitstellungstyp	Public	<p>Standardmäßig ist der Bereitstellungstyp Public und alle Cloud Migration Factory-Endpunkte sind mit der Benutzerauthentifizierung öffentlich zugänglich.</p> <p>Öffentlich mit AWS WAF: Der Zugriff auf CMF-Endpunkte ist auf anpassbare CIDR-Bereiche beschränkt.</p> <p>Private : Alle Cloud Migration Factory-Endpunkte sind nur von Ihren VPC-Netzwerken aus zugänglich und die Cloud Migration Factory Web UI muss auf einem privaten Webserver gehostet werden, der separat bereitgestellt wird.</p>

(Optional) Nur privater Bereitstellungstyp

Parameter	Standard	Beschreibung
Vollständige URL für den Zugriff auf die Web-Benutzeroberfläche	[not set]	<p>Erforderlich, wenn der Bereitstellungstyp auf Privat festgelegt ist. Geben Sie die URL der Webschnittstelle der Migrationsfabrik an, die den statischen Webinhalt bereitstellt. Beispiel https://cmf.yourdomain.local.</p> <div data-bbox="1086 636 1510 1745" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><ul style="list-style-type: none">• Fügen Sie der URL keinen abschließenden Schrägstrich hinzu. Dies führt dazu, dass die Weboberfläche beim Laden fehlschlägt.• In privaten Bereitstellungen ist ein Webserver erforderlich, um den statischen Inhalt zu hosten, und muss vor der Bereitstellung der CloudFormation Vorlage bereitgestellt werden.</div>

Parameter	Standard	Beschreibung
VPC-ID zum Hosten von API Gateway-Endpunkten	[not set]	Erforderlich, wenn der Bereitstellungstyp auf Privat festgelegt ist. Geben Sie eine einzelne VPC-ID an, in der die privaten API Gateway-Endpunkte erstellt werden.
Subnetze zum Hosten von API Gateway-Schnittstellenendpunkten	[not set]	Erforderlich, wenn der Bereitstellungstyp auf Privat festgelegt ist. Geben Sie zwei Subnetz-IDs an, in denen die privaten API Gateway-Endpunkte erstellt werden. Die angegebenen Subnetz-IDs müssen sich innerhalb der oben angegebenen VPC befinden.

(Optional) Öffentlich nur mit AWS WAF Bereitstellungstyp

Parameter	Standard	Beschreibung
Zulässiges CIDR	[not set]	Erforderlich, wenn der Bereitstellungstyp mit auf Öffentlich AWS WAFgesetz ist. Geben Sie zwei CIDR-Bereiche an, aus denen die Benutzer und der Automatisierungsserver auf die Endpunkte zugreifen.

 **Important**

- Sie müssen 2 CIDR-Bereiche angeben.
- Nach der Bereitstellung ist es möglich, den AWS WAF Regeln bei Bedarf zusätzliche Bereiche und Einschränkungen hinzuzufügen.

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
8. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Aktivieren Sie die Kontrollkästchen, in denen bestätigt wird, dass die Vorlage [AWS Identity and Access Management](#) (IAM)-Ressourcen erstellt und dass sie möglicherweise die Funktion CAPABILITY_AUTO_EXPAND erfordert.
9. Wählen Sie Absenden, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 20 Minuten den Status CREATE_COMPLETE erhalten.

⚠ Important

Wenn Sie AWS MGN verwenden, müssen Sie die Voraussetzungen für AWS MGN erfüllen, bevor Sie mit Schritt 3 fortfahren.

Schritt 3: Starten des Zielkonto-Stacks im AWS Zielkonto

Diese automatisierte AWS CloudFormation Vorlage stellt IAM-Rollen im AWS Zielkonto bereit, damit das Factory-Konto Rollen übernehmen und MGN-Aktionen im Zielkonto ausführen kann. Wiederholen Sie diesen Schritt für jedes Zielkonto. Wenn der Factory-Stack im vorherigen Schritt ein Zielkonto ist, muss dieser Ziel-Stack darin bereitgestellt werden.


📘 Note

Das Zielkonto muss für AWS Application Migration Service initialisiert werden, bevor dieser Stack gestartet wird. Weitere Informationen finden Sie unter [Initialisieren des Application Migration Service](#) im Benutzerhandbuch für Application Migration Service.

Der Zielkonto-Stack muss in derselben Region wie der Factory-Stack im vorherigen Schritt gestartet werden, unabhängig davon, welche Region als Migrationszielregion verwendet wird. Dieser Stack ist nur für kontoübergreifende Berechtigungen vorgesehen.

1. Melden Sie sich an der [AWS CloudFormation-Konsole](#) an. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen aus, um die Bereitstellung der Vorlage zu starten. Sie können auch [die Vorlage herunterladen](#) als Ausgangspunkt für eine eigene Implementierung verwenden.
2. Weisen Sie Ihrem Lösungs-Stack auf der Seite Stack-Details angeben einen Namen zu.
3. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
FabrikAWSAccountld	111122223333	Geben Sie eine -Konto-ID ein, in der die Migration Factory bereitgestellt wurde.

Parameter	Standard	Beschreibung
		<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Starten Sie diesen Stack in derselben AWS-Region wie der Migration Factory-Stack.</p> </div>
Wechsel der Plattform	Yes	Aktivieren Sie diese Option, wenn Sie das EC2-Modul „Replatform“ dieser Lösung verwenden möchten
RehostMGN	Yes	Aktivieren Sie diese Option, wenn Sie das Rehost-MGN-Modul dieser Lösung verwenden möchten

4. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
6. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass die Vorlage [AWS Identity and Access Management \(IAM\)](#)-Ressourcen erstellt.
7. Wählen Sie Absenden, um den Stack bereitzustellen.


Sie können den Status des Stacks in der AWS CloudFormation-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 5 Minuten den Status CREATE_COMPLETE erhalten.

Schritt 4: Erstellen des ersten Benutzers

Erstellen Sie den ersten Benutzer und melden Sie sich bei der Lösung an


Gehen Sie wie folgt vor, um den ursprünglichen Benutzer zu erstellen.

1. Navigieren Sie zur [Amazon-Cognito-Konsole](#).
2. Wählen Sie im Navigationsbereich Benutzerpools aus.
3. Wählen Sie auf der Seite Benutzerpools den Benutzerpool aus, der mit dem migration-factory Präfix beginnt.
4. Wählen Sie die Registerkarte Benutzer und dann Benutzer erstellen aus.
5. Gehen Sie auf dem Bildschirm Benutzer erstellen im Abschnitt Benutzerinformationen wie folgt vor:
 1. Stellen Sie sicher, dass die Option Einladung senden ausgewählt ist.
 2. Geben Sie eine E-Mail-Adresse ein.

 **Important**


Diese E-Mail-Adresse muss sich von der Adresse unterscheiden, die Sie im -ServiceAccountEmailParameter verwendet haben, den die Lösung bei der Bereitstellung der primären CloudFormation Vorlage verwendet.

3. Wählen Sie Passwort festlegen aus.
4. Geben Sie im Feld Passwort ein Passwort ein.

 **Note**

Das Passwort muss mindestens acht Zeichen lang sein, einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

6. Wählen Sie Create user (Benutzer erstellen) aus.

 **Note**

Sie erhalten eine E-Mail mit dem temporären Passwort. Bis Sie das temporäre Passwort ändern, wird der Kontostatus für diesen Benutzer als Passwortänderung erzwingen angezeigt. Sie können das Passwort später in der Bereitstellung aktualisieren.

Hinzufügen eines Benutzers zur Admin-Gruppe

Gehen Sie in der Amazon Cognito-Konsole wie folgt vor, um der Standard-Admin-Gruppe einen Benutzer hinzuzufügen.

1. Navigieren Sie zur Amazon-Cognito-Konsole.
2. Wählen Sie im Navigationsmenü Benutzerpools aus.
3. Wählen Sie auf der Seite Benutzerpools den Benutzerpool aus, der mit dem `migration-factory` Präfix beginnt.
4. Wählen Sie die Registerkarte Gruppen und öffnen Sie die Gruppe mit dem Namen Admin, indem Sie den Namen auswählen.
5. Wählen Sie Benutzer zur Gruppe hinzufügen und dann den hinzuzufügenden Benutzernamen aus.
6. Wählen Sie Hinzufügen aus.

Der ausgewählte Benutzer wird nun der Mitgliederliste der Gruppe hinzugefügt. Diese Standard-Administratorgruppe autorisiert den Benutzer, alle Aspekte der Lösung zu verwalten.

Note

Nachdem Sie die ersten Benutzer erstellt haben, können Sie die Gruppenmitgliedschaft in der Lösungsbenutzeroberfläche verwalten, indem Sie Administration, dann Berechtigungen und dann Gruppen auswählen.

Identifizieren der CloudFront URL (öffentlich und öffentlich nur mit AWS WAF Bereitstellungen)

Gehen Sie wie folgt vor, um die Amazon- CloudFront URL der Lösung zu identifizieren. Auf diese Weise können Sie sich anmelden und das Passwort ändern.

1. Navigieren Sie zur [-AWS CloudFormationKonsole](#) und wählen Sie den Stack der Lösung aus.
2. Wählen Sie auf der Seite Stacks die Registerkarte Outputs und dann den Wert für die MigrationFactoryURL aus.

Note

Wenn Sie die Lösung in einer anderen -AWSRegion als USA Ost (Nord-Virginia) gestartet haben, CloudFront kann die Bereitstellung länger dauern und die MigrationFactoryURL ist möglicherweise nicht sofort zugänglich (Sie erhalten die Fehlermeldung „Zugriff verweigert“). Es kann bis zu vier Stunden dauern, bis die URL verfügbar ist. Die URL enthält `cloudfront.net` als Teil der Zeichenfolge.

3. Melden Sie sich mit Ihrem Benutzernamen und Ihrem temporären Passwort an, erstellen Sie dann ein neues Passwort und wählen Sie Passwort ändern aus.

Note

Das Passwort muss mindestens acht Zeichen lang sein, einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Schritt 5: (Optional) Bereitstellen statischer Inhalte der privaten Webkonsole

Wenn Sie während der Stack-Bereitstellung den Bereitstellungstyp Privat ausgewählt haben, müssen Sie den Code der CMF-Webkonsole manuell auf dem von Ihnen erstellten Webserver bereitstellen und dann unter Vollständige URL für den Zugriff auf den Webbenutzeroberflächenparameter des Stacks angeben. Überspringen Sie diesen Schritt für alle anderen Bereitstellungstypen.

Einrichtungs- und Konfigurationsanweisungen für jeden Webserver unterscheiden sich, daher enthält dieses Handbuch nur allgemeine Anweisungen dazu, von wo aus der Inhalt kopiert werden soll. Sie sollten den Webserver entsprechend Ihren eigenen Anforderungen konfigurieren, bevor Sie den Inhalt aktualisieren.

1. Stellen Sie sicher, dass der Webserver Zugriff auf S3 hat und die AWS CLI installiert und konfiguriert ist. Alternativ können Sie den Inhalt des Frontend-Buckets herunterladen und ihn mit einem anderen Gerät auf den Webserver kopieren.
2. Führen Sie mit der AWS CLI den folgenden Befehl aus und ersetzen Sie dabei den Umgebungsnamen durch den Namen, der während der Stack-Bereitstellung angegeben wurde, die AWS-Konto-ID durch die ID des AWS-Kontos, in dem der Stack bereitgestellt wurde, und

das Zielverzeichnis durch den des Standardstammverzeichnisses des Webserver. Dadurch wird der statische Cloud Migration Factory-Webkonsolencode zusammen mit der spezifischen Konfiguration kopiert, die für diese Cloud Migration Factory-Lösungsbereitstellung erforderlich ist:

Windows-Beispiel:

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

Linux-Beispiel:

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

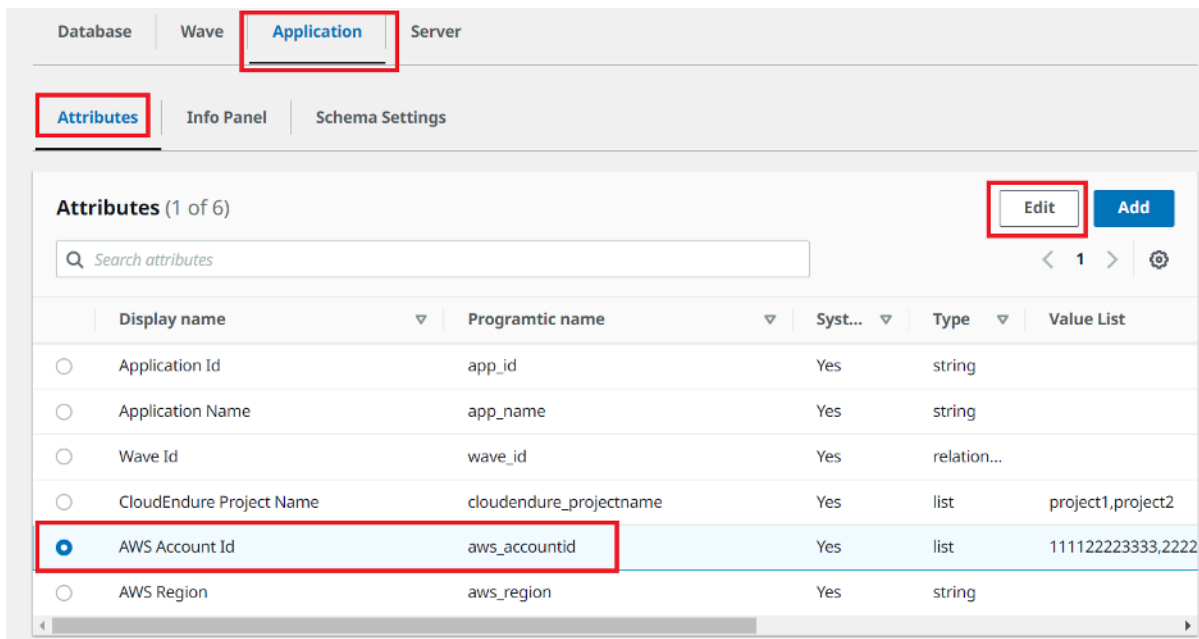
Note

Wenn eine Aktualisierung der Stack-Parameter vorgenommen wird, müssen die Dateien auf dem Webserver vom Frontend-Bucket aus ersetzt werden, um sicherzustellen, dass alle Konfigurationsänderungen für die Webkonsole verfügbar sind.

Schritt 6: Aktualisieren des Factory-Schemas

Aktualisieren der AWS-Konto-ID für AWS MGN-Migrationen

1. Wählen Sie auf der Webschnittstelle Migration Factory die Option Administration und dann Attribute aus.
2. Wählen Sie auf der Seite Attributkonfiguration die Option Anwendung und dann Attribute aus.
3. Wählen Sie AWS-Konto-ID und dann Bearbeiten aus.



- Aktualisieren Sie auf der Seite Attribut ändern die Liste Wert mit Ihren AWS-Zielkonto-IDs und wählen Sie Speichern aus.

Note

Wenn Sie mehr als eine AWS Konto-ID haben, trennen Sie die ID durch Kommas.

Schritt 7: Konfigurieren eines Migrationsautomatisierungsservers

Der Migrationsautomatisierungsserver wird verwendet, um die Migrationsautomatisierung auszuführen.

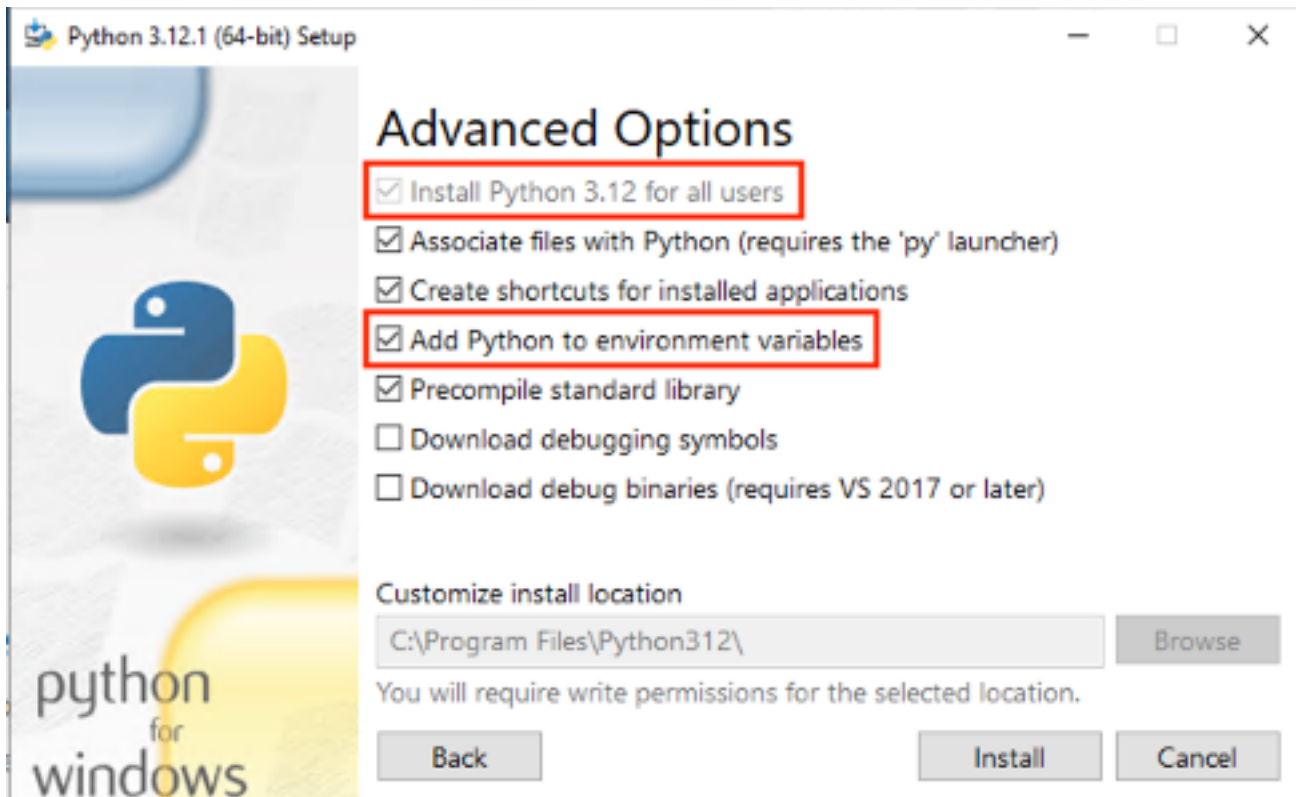
Erstellen eines Windows Server 2016 oder höher-Servers

Wir empfehlen, den Server in Ihrem AWS-Konto zu erstellen, kann aber auch in Ihrer On-Premises-Umgebung erstellt werden. Wenn es in ein AWS-Konto integriert ist, muss es sich im selben AWS-Konto und in derselben Region wie Cloud Migration Factory befinden. Informationen zum Überprüfen der Serveranforderungen finden Sie unter [Migrationsautomatisierungsserver](#).

Unabhängig davon, wo Sie die Windows-Instance bereitstellen, sollte sie als Standardinstallation für Windows 2016 oder höher bereitgestellt werden, die Ihren Sicherheits- und Betriebsanforderungen entspricht.

Installieren der erforderlichen Software zur Unterstützung der Automatisierungen

1. Laden Sie [Python v3.12.1](#) herunter.
2. Melden Sie sich als Administrator an, installieren Sie Python v3.12.1 und wählen Sie Installation anpassen aus.
3. Wählen Sie Weiter und für alle Benutzer Installieren und Python zu Umgebungsvariablen hinzufügen aus. Wählen Sie Installieren aus.



4. Stellen Sie sicher, dass Sie über Administratorrechte verfügen, öffnen Sie und führen Sie die folgenden Befehle auscmd . exe, um die Python-Pakete einzeln zu installieren:

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

Wenn einer dieser Befehle fehlschlägt, führen Sie ein Upgrade von pip durch, indem Sie den folgenden Befehl ausführen:

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

5. Installieren Sie [AWS CLI \(Befehlszeilenschnittstelle\)](#).
6. Installieren Sie mit dem [PowerShell für das AWS-Modul](#) . Stellen Sie sicher, dass Sie den Parameter `-Scope AllUsers` im Befehl enthalten haben.

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

7. Öffnen Sie PowerShell Script Execution, indem Sie die PowerShell CLI als Administrator öffnen und den folgenden Befehl ausführen:

```
Set-ExecutionPolicy RemoteSigned
```

Konfigurieren von AWS Berechtigungen für den Migrationsautomatisierungsserver und Installieren von AWS Systems Manager Agent (SSM Agent)

Je nachdem, wo Sie den Migrationsausführungsserver bereitstellen, wählen Sie eine der folgenden Optionen aus, um AWS Berechtigungen für den Migrationsautomatisierungsserver zu konfigurieren. Die IAM-Rolle oder -Richtlinie gewährt dem Automatisierungsserver die Berechtigung und dem Zugriff auf AWS Secrets Manager, Installationsschlüssel eines Kundendienstmitarbeiters und Anmeldeinformationen für das Factory-Servicekonto abzurufen. Sie können den Migrationsautomatisierungsserver entweder AWS in als EC2-Instance oder On-Premises bereitstellen.

Option 1: Gehen Sie wie folgt vor, um die Berechtigungen für den Migrationsautomatisierungsserver in Amazon EC2 und in demselben AWS-Konto und derselben Region wie die Fabrik zu konfigurieren.

1. Navigieren Sie zur [AWS CloudFormation -Konsole](#) und wählen Sie den Stack der Lösung aus.
2. Wählen Sie die Registerkarte Outputs in der Spalte Key den Wert aus, `AutomationServerIAMRole` der später in der Bereitstellung verwendet werden soll.

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. Navigieren Sie zur [Amazon Elastic Compute Cloud](#)-Konsole.
4. Wählen Sie im linken Navigationsbereich Instances aus.
5. Verwenden Sie auf der Seite Instances das Feld Instances filtern und geben Sie den Namen des Migrationsausführungsservers ein, um die Instance zu finden.
6. Wählen Sie die Instance und dann Aktionen im Menü aus.
7. Wählen Sie in der Dropdown-Liste Sicherheit und dann IAM-Rolle ändern aus.

The screenshot shows the AWS Management Console interface for an EC2 instance. The 'Actions' menu is open, and the 'Security' option is highlighted with a red box. Below the 'Security' option, the 'Modify IAM role' option is also highlighted with a red box. The 'Launch instances' button is visible in the top right corner.

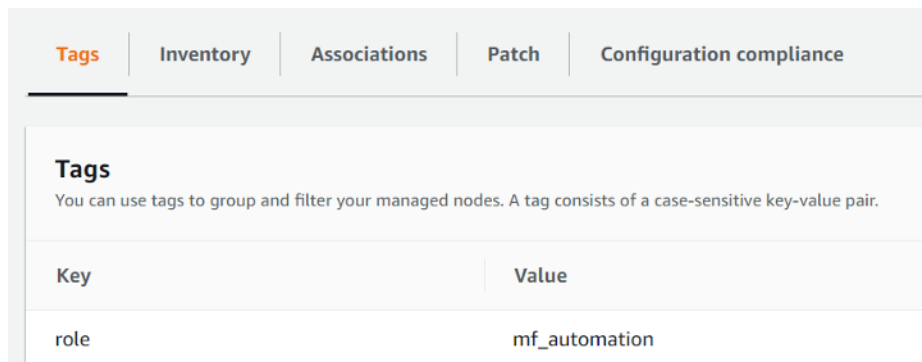
8. Suchen Sie in der Liste der IAM-Rollen die IAM-Rolle, die den Wert für `AutomationServerIAMRole`, den Sie in Schritt 2 aufgezeichnet haben, und wählen Sie Speichern aus.
9. Verwenden Sie Ihr Remote Desktop Protocol (RDP), um sich beim Migrationsautomatisierungsserver anzumelden.

10. Laden Sie den [SSM Agent](#) herunter und installieren Sie ihn auf dem Migrationsautomatisierungsserver.

Note

Standardmäßig ist der AWS Systems Manager-Agent auf Amazon Machine Images des Windows Server 2016 vorinstalliert. Führen Sie diesen Schritt nur aus, wenn der SSM-Agent nicht installiert ist.

11. Fügen Sie der EC2-Instance des Migrationsautomatisierungsservers das folgende Tag hinzu: Schlüssel = `role` und Wert = `mf_automation`.

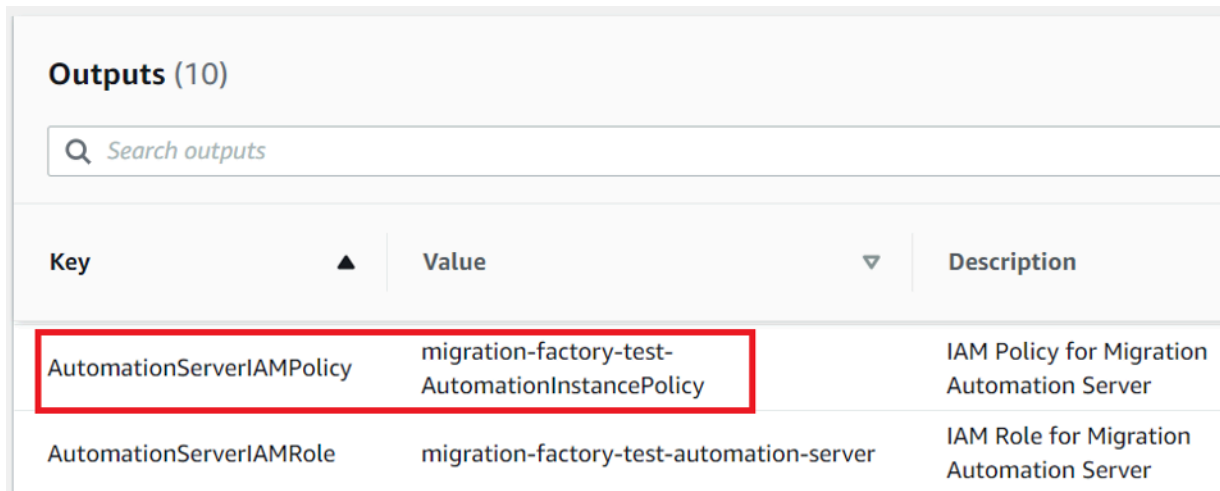


Key	Value
role	mf_automation

12. Öffnen Sie die AWS Systems Manager-Konsole und wählen Sie Fleet Manager aus. Überprüfen Sie den Status des Automatisierungsservers und stellen Sie sicher, dass der Ping-Status des SSM-Agenten online ist.

Option 2: Gehen Sie wie folgt vor, um die Berechtigungen für den On-Premises-Migrationsautomatisierungsserver zu konfigurieren.

1. Navigieren Sie zur [AWS CloudFormation -Konsole](#) und wählen Sie den Stack der Lösung aus.
2. Wählen Sie die Registerkarte Outputs in der Spalte Key den Wert aus, `AutomationServerIAMPolicy` der später in der Bereitstellung verwendet werden soll.



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. Gehen Sie zur [Identity and Access Management-Konsole](#).
4. Wählen Sie im linken Navigationsbereich Benutzer und dann Benutzer hinzufügen aus.
5. Erstellen Sie im Feld Benutzername einen neuen Benutzer.
6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Berechtigungen festlegen unter Berechtigungsoptionen die Option Richtlinien direkt anfügen aus. Eine Liste von Richtlinien wird angezeigt.
8. Suchen Sie in der Liste der Richtlinien die Richtlinie, die den Wert für `AutomationServerIAMPolicy`, den Sie in [Schritt 2](#) aufgezeichnet haben, und wählen Sie sie aus.
9. Wählen Sie Next und überprüfen Sie dann, ob die richtige Richtlinie ausgewählt ist.
10. Wählen Sie Create user (Benutzer erstellen) aus.
11. Nachdem Sie zur Seite Benutzer weitergeleitet wurden, wählen Sie den Benutzer aus, den Sie im vorherigen Schritt erstellt haben, und wählen Sie dann die Registerkarte Sicherheitsanmeldeinformationen.
12. Wählen Sie im Abschnitt Access keys (Zugriffsschlüssel) Create access key (Zugriffsschlüssel erstellen).


Note

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Diese werden zum Signieren der von Ihnen ausgeführten programmgesteuerten Anforderungen an AWS verwendet. Wenn Sie noch keine Zugriffsschlüssel besitzen, können Sie diese über die AWS-Managementkonsole erstellen. Als bewährte Methode verwenden Sie nicht die

Stammbenutzerzugriffsschlüssel des -Kontos für die Aufgaben, für die dies nicht erforderlich ist. [Erstellen Sie stattdessen einen neuen Administrator-IAM-Benutzer](#) mit Zugriffsschlüsseln für sich selbst.

Sie können den geheimen Zugriffsschlüssel nur beim Erstellen anzeigen oder herunterladen. Später kann er nicht mehr wiederhergestellt werden. Sie können jedoch jederzeit neue Zugriffsschlüssel anlegen. Sie müssen auch über Berechtigungen zum Ausführen der erforderlichen IAM-Aktionen verfügen. Weitere Informationen finden Sie unter [Erforderliche Berechtigungen für den Zugriff auf IAM-Ressourcen](#) im IAM-Benutzerhandbuch.

13. Wählen Sie zum Anzeigen des neuen Zugriffsschlüsselpaars Show (Anzeigen) aus. Sie haben keinen Zugriff auf den geheimen Zugriffsschlüssel mehr, nachdem das Dialogfeld geschlossen wird. Ihre Anmeldeinformationen sehen etwa folgendermaßen aus:
 - Access key ID: AKIAIOSFODNN7EXAMPLE
 - Secret access key: wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
14. Wählen Sie zum Herunterladen des Schlüsselpaars Download .csv file aus. Speichern Sie die Schlüssel an einem sicheren Ort. Sie haben keinen Zugriff auf den geheimen Zugriffsschlüssel mehr, nachdem das Dialogfeld geschlossen wird.

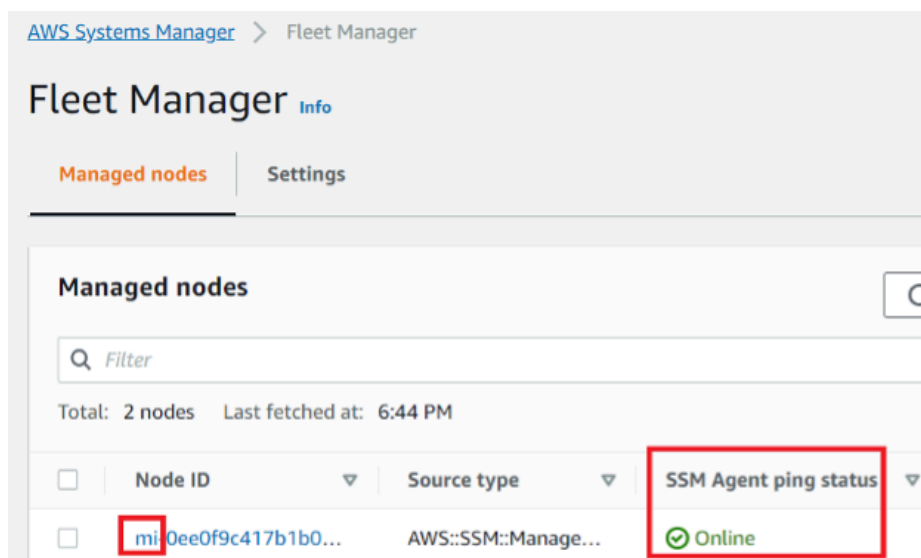
 **Important**

Halten Sie die Schlüssel vertraulich, um Ihr AWS-Konto zu schützen, und senden Sie sie niemals per E-Mail. Geben Sie sie nicht außerhalb Ihrer Organisation weiter, selbst wenn eine Anfrage von AWS oder Amazon.com zu kommen scheint. Niemand, der Amazon legitim vertritt, wird Sie nach dem geheimen Schlüssel fragen.

15. Nachdem Sie die .csv-Datei heruntergeladen haben, klicken Sie auf Close (Schließen) Wenn Sie einen Zugriffsschlüssel erstellen, ist das Schlüsselpaar standardmäßig aktiv, und Sie können es sofort verwenden.
16. Verwenden Sie Ihr Remote Desktop Protocol (RDP), um sich beim Migrationsausführungsserver anzumelden.
17. Öffnen Sie als Administrator angemeldet eine Eingabeaufforderung (CMD . exe).
18. Führen Sie den folgenden Befehl aus, um die AWS Anmeldeinformationen auf dem Server zu konfigurieren. Ersetzen Sie *<your_access_key_id>*, *<your_secret_access_key>* und *<your_region>* durch Ihre Werte:

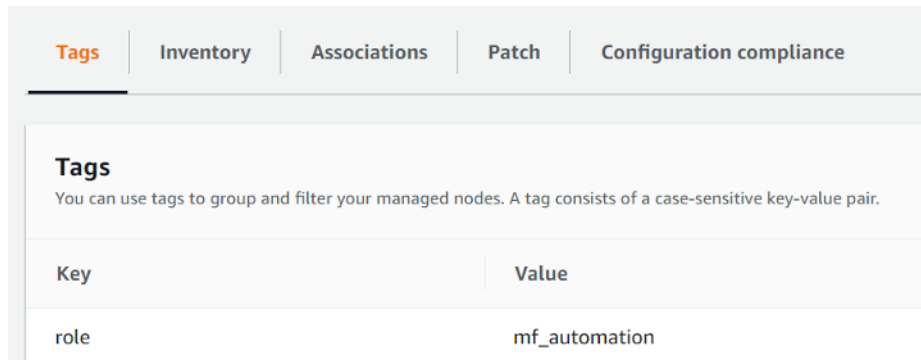
```
SETX /m AWS_ACCESS_KEY_ID <your_access_key_id>
SETX /m AWS_SECRET_ACCESS_KEY <your_secret_access_key>
SETX /m AWS_DEFAULT_REGION <your_region>
```

19. Starten Sie den Automatisierungsserver neu.
20. Installieren Sie den AWS Systems Manager-Agenten im Hybridmodus (On-Premises-Server).
 - a. Erstellen Sie eine Hybrid-Aktivierung; siehe [Erstellen einer Aktivierung \(Konsole\)](#) im AWS Systems Manager-Benutzerhandbuch. Wenn Sie während dieses Prozesses aufgefordert werden, eine IAM-Rolle anzugeben, wählen Sie eine vorhandene IAM-Rolle aus und wählen Sie die Rolle mit dem Suffix -automation-server aus, der automatisch bei der Bereitstellung des Cloud Migration Factory-Stacks erstellt wurde.
 - b. Melden Sie sich beim Migrationsautomatisierungsserver als Administrator an.
 - c. Installieren Sie AWS Systems Manager Agent (SSM Agent). Weitere Informationen finden Sie unter [Installieren des SSM Agent für eine Hybrid- und Multi-Cloud-Umgebung](#) im AWS Systems Manager-Benutzerhandbuch. Verwenden Sie die Hybrid-Aktivierung, die in Schritt 20.a erstellt wurde.
 - d. Sobald der Agent erfolgreich installiert wurde, wählen Sie in der AWS Systems Manager-Konsole Fleet Manager aus. Identifizieren Sie die Knoten-ID mit dem Präfix mi- mit dem Online-Status.



- e. Wählen Sie die Knoten-ID aus und stellen Sie sicher, dass die IAM-Rolle diejenige ist, die Sie mit dem Automatisierungsserver-Suffix ausgewählt haben.

- f. Fügen Sie das folgende Tag für diesen Hybrid-Knoten hinzu: Schlüssel = `role` und Wert = `mf_automation`. Kleinbuchstaben.



Schritt 8: Testen der Lösung mit den Automatisierungsskripten

Importieren von Migrationsmetadaten in die Factory

Um den Migrationsprozess zu starten, laden Sie die [server-list.csv](#) Datei aus dem GitHubRepository herunter. Die `server-list.csv` Datei ist ein Beispiel für ein AWS MGN Service-Migrationsaufnahmeformular zum Importieren der Attribute für die Quellserver im Umfang.


Note

Die CSV-Datei und die Beispiel-Automatisierungsskripts waren Teil des -Pakets aus demselben GitHub Repository.

Sie können das Formular für Ihre Migration anpassen, indem Sie die Beispieldaten durch Ihre spezifischen Server- und Anwendungsdaten ersetzen. In der folgenden Tabelle sind die zu ersetzenden Daten aufgeführt, um diese Lösung an Ihre Migrationsanforderungen anzupassen.

Feldname	Erforderlich?	Beschreibung
Wave_Name	Ja	Der Wave-Name basiert auf Prioritäts- und Anwendungsserverabhängigkeiten. Rufen Sie diese Kennung aus Ihrem Migrationsplan ab.

Feldname	Erforderlich?	Beschreibung
app_name	Ja	Die Namen der Anwendungen, die in den Umfang der Migration fallen. Vergewissern Sie sich, dass Ihre Anwendungsgruppierung alle Anwendungen enthält, die dieselben Server nutzen.
aws_accountid	Ja	Eine 12-stellige Kennung für Ihr , die AWS-Konto sich in Ihrem Kontoprofil befindet. Um auf zuzugreifen, wählen Sie Ihr Kontoprofil in der oberen rechten Ecke der AWS Management Console und dann Mein Konto aus dem Dropdown-Menü aus.
aws_region	Ja	AWS-Region Code. Beispiel: us-east-1 Die vollständige Liste der Regionscodes finden Sie .
server_name	Ja	Der Name der On-Premises-Server, die in den Umfang der Migration fallen.
server_os_family	Ja	Das Betriebssystem (OS), das auf den Quellservern im Umfang ausgeführt wird. Verwenden Sie entweder Windows oder Linux, da diese Lösung nur diese Betriebssysteme unterstützt.

Feldname	Erforderlich?	Beschreibung
server_os_version	Ja	<p>Die Version des Betriebssystems, das auf den Quellservern im Umfang ausgeführt wird.</p> <div data-bbox="1068 445 1510 1045" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Verwenden Sie die Betriebssystemversion, nicht die Kernel-Version, z. B. RHEL 7.1, Window Server 2012 R2 oder CentOS 7.5, 7.6. Verwenden Sie nicht Linux 3.xx, 4.xx oder Windows 8.1.x.</p></div>
server_fqdn	Ja	<p>Der vollqualifizierte Domänenname des Quellserver, bei dem es sich um den Servernamen gefolgt vom Domännennamen handelt. Zum Beispiel server123.company.com.</p>

Feldname	Erforderlich?	Beschreibung
server_tier	Ja	Eine Bezeichnung, um zu identifizieren, ob der Quellserver ein Web-, ein App- oder ein Datenbankserver ist. Wir empfehlen, den Quellserver als App zu kennzeichnen, wenn der Server als mehr als eine Stufe funktioniert, z. B. wenn der Server Web-, App- und Datenbankebenen zusammen ausführt.
server_environment	Ja	Ein Label zur Identifizierung der Umgebung des Servers. Zum Beispiel dev , test , prod , QA oder pre-prod .
r_type	Ja	Ein Label zur Identifizierung der Migrationsstrategie. Zum Beispiel Außerbetriebnahme, Beibehalten, Verschieben, Hostwechsel, Neukauf, Plattformwechsel, Rearchitekt, TBC.
subnet_IDs	Ja	Die Subnetz-ID für die Amazon EC2-Ziel-Instance für die Migration nach dem Cutover.
Sicherheitsgruppen-IDs	Ja	Die Sicherheitsgruppen-ID für die Amazon EC2-Ziel-Instance für die Migration nach dem Cutover.

Feldname	Erforderlich?	Beschreibung
subnet_IDs _test	Ja	Die Ziel-Subnetz-ID für den Quellserver, der getestet wird.
Sicherheitsgruppe_IDs _test	Ja	Die Zielsicherheitsgruppen-ID für den Quellserver, der getestet wird.
instanceType	Ja	Der Amazon EC2-Instance-Typ, der in den Ermittlungs- und Planungsbemühungen identifiziert wurde. Weitere Informationen zu EC2-Instance-Typen finden Sie unter Amazon EC2-Instance-Typen .
tenancy	Ja	Der Tenancy-Typ, der bei den Ermittlungs- und Planungsbemühungen identifiziert wird. Verwenden Sie einen der folgenden Werte, um die Tenancy zu identifizieren: Shared , Dedicated oder Dedicated Host . Sie können Freigegeben als Standardwert verwenden, es sei denn, die Lizenz einer Anwendung erfordert einen bestimmten Typ.
Tags	Nein	Die Tags für die Serverressourcen, z. B. CostCenter=123;BU=IT;Location=US

Feldname	Erforderlich?	Beschreibung
private_ip	Nein	Die private IP für die Ziel-Instance. Falls nicht enthalten, erhält die Instance eine IP von DHCP.
iamRole	Nein	IAM-Rolle für die Ziel-Instance. Falls nicht enthalten, wird der Ziel-Instance keine IAM-Rolle zugeordnet.

1. Melden Sie sich bei der Cloud Migration Factory-Webkonsole an.
2. Wählen Sie unter Migrationsmanagement die Option Import und wählen Sie Datei auswählen aus. Wählen Sie das Aufnahmeformular aus, das Sie zuvor ausgefüllt haben, und wählen Sie Weiter aus.
3. Überprüfen Sie die Änderungen und stellen Sie sicher, dass keine Fehler angezeigt werden (Informationmeldung ist normal), und wählen Sie Weiter.
4. Wählen Sie Upload, um Server hochzuladen.

Zugriff auf die Domains

Die in dieser Lösung enthaltenen Beispiel-Automatisierungsskripts stellen eine Verbindung zu den Quellservern im Umfang her, um Migrationsaufgaben zu automatisieren, z. B. die Installation des Replikationsagenten und das Herunterfahren der Quellserver. Um einen Testlauf der Lösung durchzuführen, ist für Windows- und Linux-Server (sudo permissions) ein Domänenbenutzer mit lokalen Administratorberechtigungen für die Quellserver erforderlich. Wenn Linux nicht in der Domain enthalten ist, können andere Benutzer wie LDAP-Benutzer mit Sudo-Berechtigungen oder ein lokaler Sudo-Benutzer verwendet werden. Weitere Informationen zu automatisierten Migrationsaufgaben finden Sie unter [Automatisierte Migrationsaktivitäten mithilfe der Migration Factory-Webkonsole und Automatisierte Migrationsaktivitäten mithilfe der Eingabeaufforderung](#) .

Durchführen eines Testlaufs der Migrationsautomatisierung

Mit dieser Lösung können Sie einen Testlauf der Migrationsautomatisierung durchführen. Mithilfe von Automatisierungsskripten importiert der Migrationsprozess die Daten aus der CSV-Migrationsdatei

in die Lösung. Für die Quellserver werden die erforderlichen Prüfungen durchgeführt, der Replikationsagent wird an die Quellserver übertragen, der Replikationsstatus wird überprüft und der Zielserver wird über die Webschnittstelle von Migration Factory gestartet. step-by-step Anweisungen zum Ausführen eines Tests finden Sie unter [Automatisierte Migrationsaktivitäten mithilfe der Migration Factory-Webkonsole](#) und [Automatisierte Migrationsaktivitäten mithilfe der Eingabeaufforderung](#).

Schritt 9: (Optional) Erstellen eines Migrations-Tracker-Dashboards

Wenn Sie die optionale Migrations-Tracker-Komponente bereitgestellt haben, können Sie ein QuickSight Dashboard einrichten, das die in der Amazon-DynamoDB-Tabelle gespeicherten Migrationsmetadaten visualisiert.

Führen Sie die folgenden Schritte aus, um ...

1. [Festlegen der QuickSight Berechtigungen und Verbindungen](#)
2. [Erstellen eines Dashboards](#)

Note

Wenn die Migration Factory leer ist und keine Wave-, Anwendungs- und Serverdaten vorhanden sind, gibt es keine Daten zum Erstellen eines QuickSight Dashboards.

Festlegen der QuickSight Berechtigung und der Verbindungen

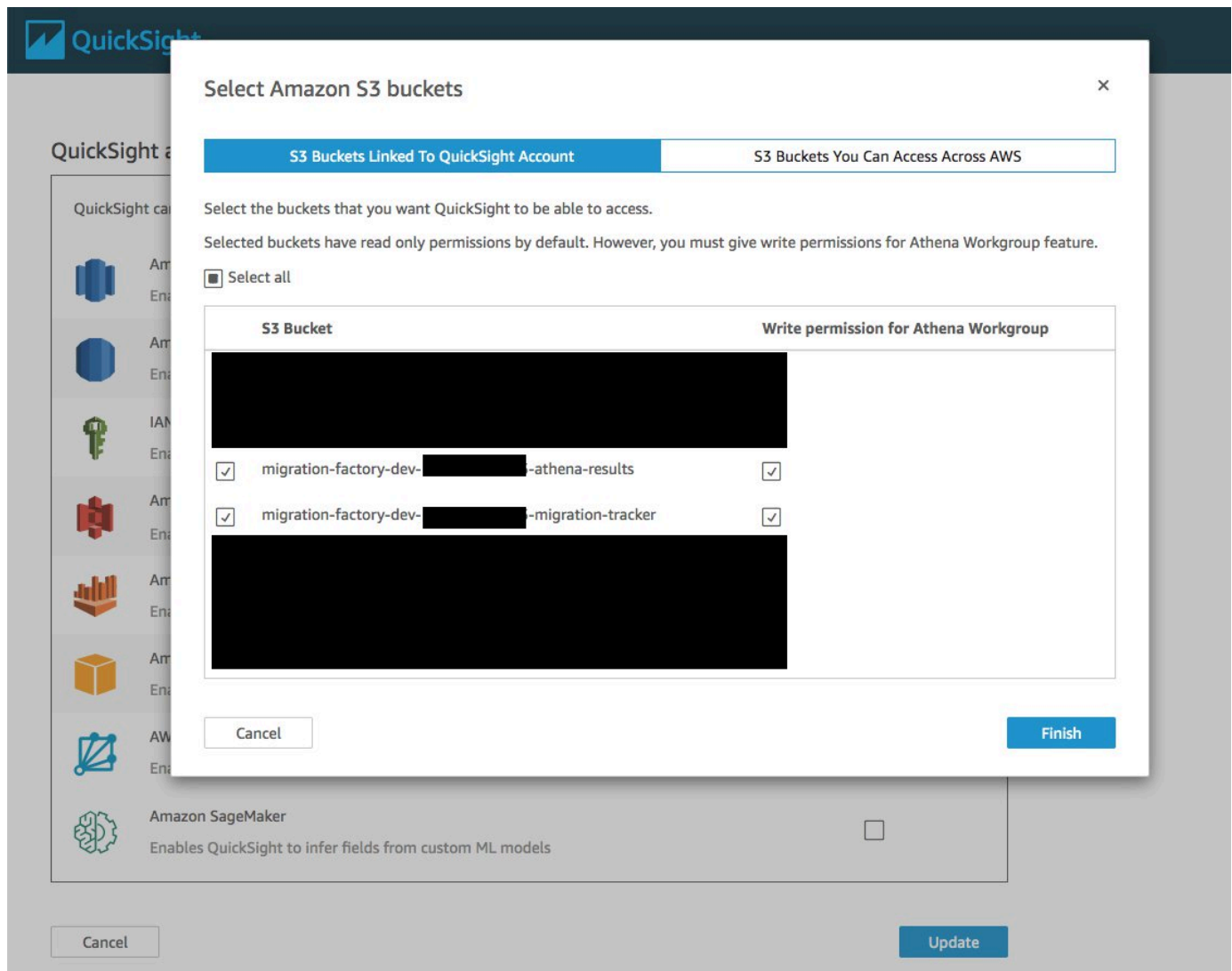
Wenn Sie Amazon nicht QuickSight in Ihrem AWS-Konto eingerichtet haben, finden Sie weitere Informationen unter [Einrichten von für Amazon QuickSight](#) im Amazon- QuickSight Benutzerhandbuch. Nachdem Sie ein QuickSight Abonnement eingerichtet haben, gehen Sie wie folgt vor, um die Berechtigungen und Verbindungen zwischen QuickSight und dieser Lösung festzulegen.

Note

Diese Lösung verwendet die Amazon QuickSight -Unternehmenslizenz. Wenn Sie jedoch nicht möchten, dass die E-Mail-Berichte, Einblicke und die stündliche Datenaktualisierung erfolgen, können Sie sich für eine Standardlizenz entscheiden, die auch mit dem Migrations-Tracker verwendet werden kann.

Stellen Sie zunächst eine Verbindung QuickSight mit dem Amazon S3-Bucket her:

1. Navigieren Sie zur [QuickSight-Konsole](#).
2. Wählen Sie auf der QuickSight Seite das Symbol aus, das eine Person in der oberen rechten Ecke und Verwalten QuickSight anzeigt.
3. Wählen Sie auf der Seite Kontoname im linken Menübereich Sicherheit und Berechtigungen aus.
4. Wählen Sie auf der Seite Sicherheit und Berechtigungen im Abschnitt QuickSight Zugriff auf AWS-Services die Option Verwalten aus.
5. Aktivieren Sie auf der Seite QuickSight Zugriff auf AWS-Services das Kontrollkästchen für Amazon S3.
6. Vergewissern Sie sich im Dialogfeld Amazon S3-Buckets auswählen, dass Sie sich auf der Registerkarte S3-Buckets, die mit QuickSight dem Konto verknüpft sind, befinden, und aktivieren Sie sowohl die rechten als auch die linken Kontrollkästchen für die S3-Buckets athena-results und migration-tracker.



i Note

Wenn Sie bereits QuickSight für andere S3-Datenanalysen verwenden, deaktivieren Sie die Option Amazon S3 und wiederholen Sie sie, um das Dialogfeld für die Bucket-Auswahl anzuzeigen.

7. Wählen Sie Finish (Abschließen).

Richten Sie als Nächstes Berechtigungen für Amazon Athena ein:

1. Aktivieren Sie auf der Seite QuickSight Zugriff auf AWS-Services das Kontrollkästchen für Amazon Athena .
2. Wählen Sie im Dialogfeld Amazon Athena-Berechtigungen die Option Weiter aus.

3. Vergewissern Sie sich im Dialogfeld Amazon Athena-Ressourcen, dass Sie sich auf der Registerkarte S3-Buckets, die mit QuickSight dem Konto verknüpft sind, befinden, und überprüfen Sie, ob dieselben S3-Buckets überprüft sind – athena-results und migration-tracker .

Select Amazon S3 buckets ×

S3 Buckets Linked To QuickSight Account | S3 Buckets You Can Access Across AWS

Select the buckets that you want QuickSight to be able to access.
Selected buckets have read only permissions by default. However, you must give write permissions for Athena Workgroup feature.

Select all

S3 Bucket	Write permission for Athena Workgroup
[Redacted]	<input type="checkbox"/>
<input checked="" type="checkbox"/> migration-factory [Redacted]-athena-results	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> migration-factory [Redacted]-migration-tracker	<input checked="" type="checkbox"/>
[Redacted]	<input type="checkbox"/>
[Redacted]	<input type="checkbox"/>
[Redacted]	<input type="checkbox"/>

Cancel Finish

4. Wählen Sie Finish (Abschließen).
5. Wählen Sie auf der Seite QuickSight Zugriff auf AWS-Services die Option Speichern aus.

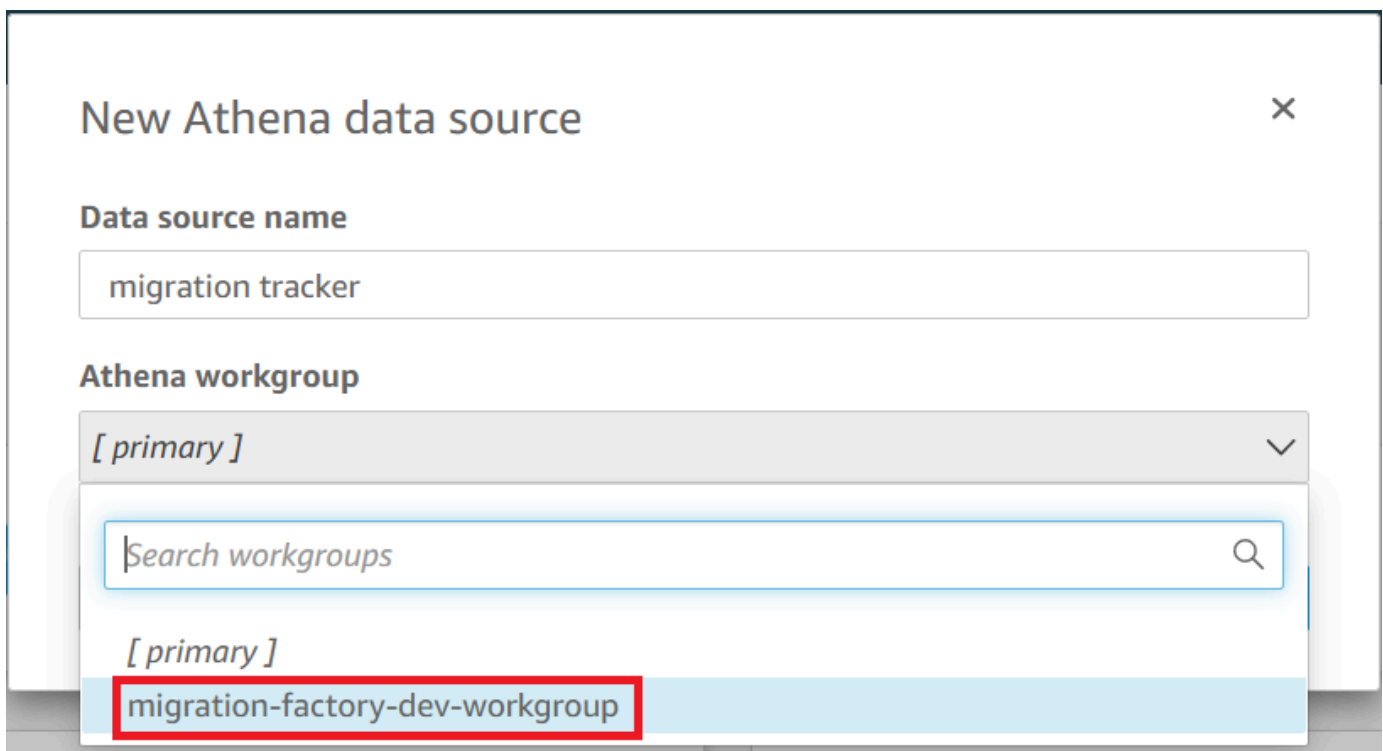
Richten Sie als Nächstes eine neue Analyse ein:

1. Wählen Sie das QuickSight Logo aus, um zur QuickSight Homepage zurückzukehren.
2. Wählen Sie auf der Seite Analyse die Option Neue Analyse aus.
3. Wählen Sie Neuer Datensatz.
4. Wählen Sie auf der Seite Datensatz erstellen die Option Athena aus.
5. Führen Sie im Dialogfeld Neue Athena-Datenquelle die folgenden Aktionen aus:

- a. Geben Sie im Feld Datenquellenname einen Namen für die Datenquelle ein.
- b. Wählen Sie im Feld Athena-Arbeitsgruppe die entsprechende *<migration-factory>*-workgroup aus.

Note

Wenn Sie diese Lösung mehrmals bereitgestellt haben, gibt es mehr als eine Arbeitsgruppe. Wählen Sie diejenige aus, die für Ihre aktuelle Bereitstellung erstellt wurde.



The screenshot shows a dialog box titled "New Athena data source" with a close button (X) in the top right corner. Below the title, there are two main sections: "Data source name" and "Athena workgroup". The "Data source name" field contains the text "migration tracker". The "Athena workgroup" section shows a dropdown menu with "[primary]" selected. Below the dropdown, there is a search bar with the placeholder text "Search workgroups" and a magnifying glass icon. Below the search bar, a list of workgroups is displayed, with "[primary]" and "migration-factory-dev-workgroup" visible. The "migration-factory-dev-workgroup" option is highlighted with a red rectangular box.

6. Wählen Sie Verbindung validieren, um sicherzustellen, dass mit Athena kommunizieren QuickSight kann.
7. Nachdem die Verbindung validiert wurde, wählen Sie Datenquelle erstellen aus.
8. Führen Sie im nächsten Dialogfeld Wählen Sie Ihre Tabelle aus die folgenden Aktionen aus:
 - a. Wählen Sie in der Liste Katalog die Option ausAwsDataCatalog.
 - b. Wählen Sie in der Liste Datenbank die Option *<Athena-table>*-tracker aus.
 - c. Wählen Sie in der Liste Tabellen die Option *<tracker-name>*-general-view aus.

d. Wählen Sie Select (Auswählen).

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.

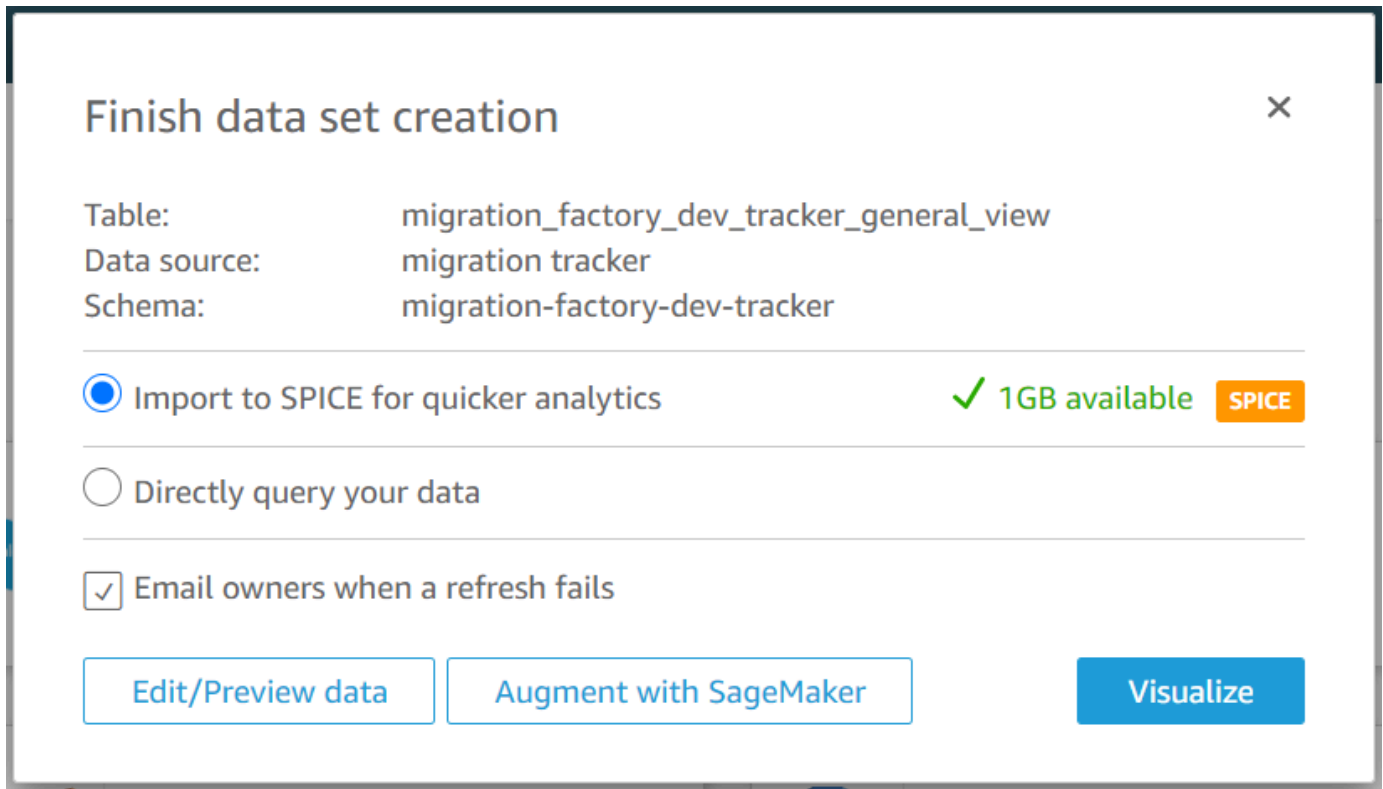
migration_factory_dev_apps

migration_factory_dev_servers

migration_factory_dev_tracker_general_view

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

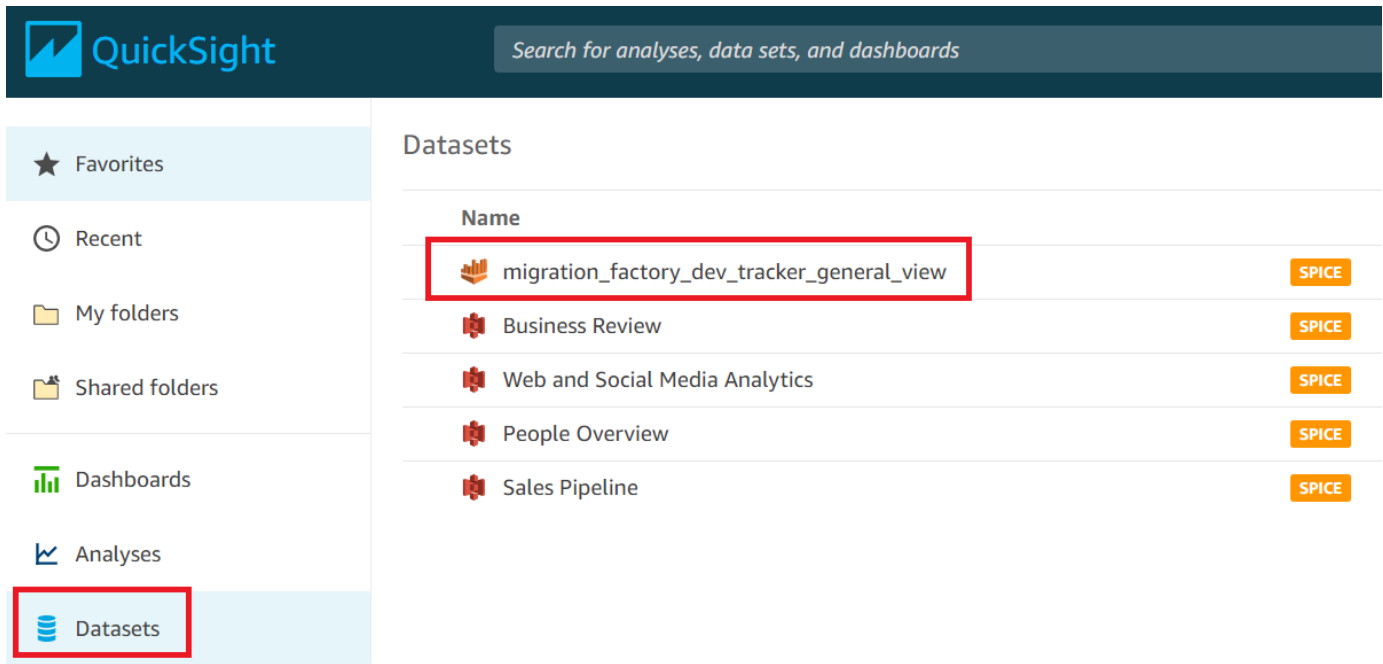
9. Wählen Sie im nächsten Dialogfeld Datensatzerstellung beenden die Option Visualisieren aus.



10. Wählen Sie unter Neues Blatt die Option Interaktives Blatt und dann Erstellen aus.

Nachdem die Daten importiert wurden, werden Sie zur Seite Analyse weitergeleitet. Bevor Sie jedoch Ihre Visualisierungen erstellen, richten Sie einen Zeitplan ein, um Ihren Datensatz zu aktualisieren.

1. Navigieren Sie zur - QuickSight Homepage.
2. Wählen Sie im Navigationsbereich Datensätze aus.
3. Wählen Sie auf der Seite Datensätze den Datensatz *<migration-factory>-general-view* aus.



QuickSight

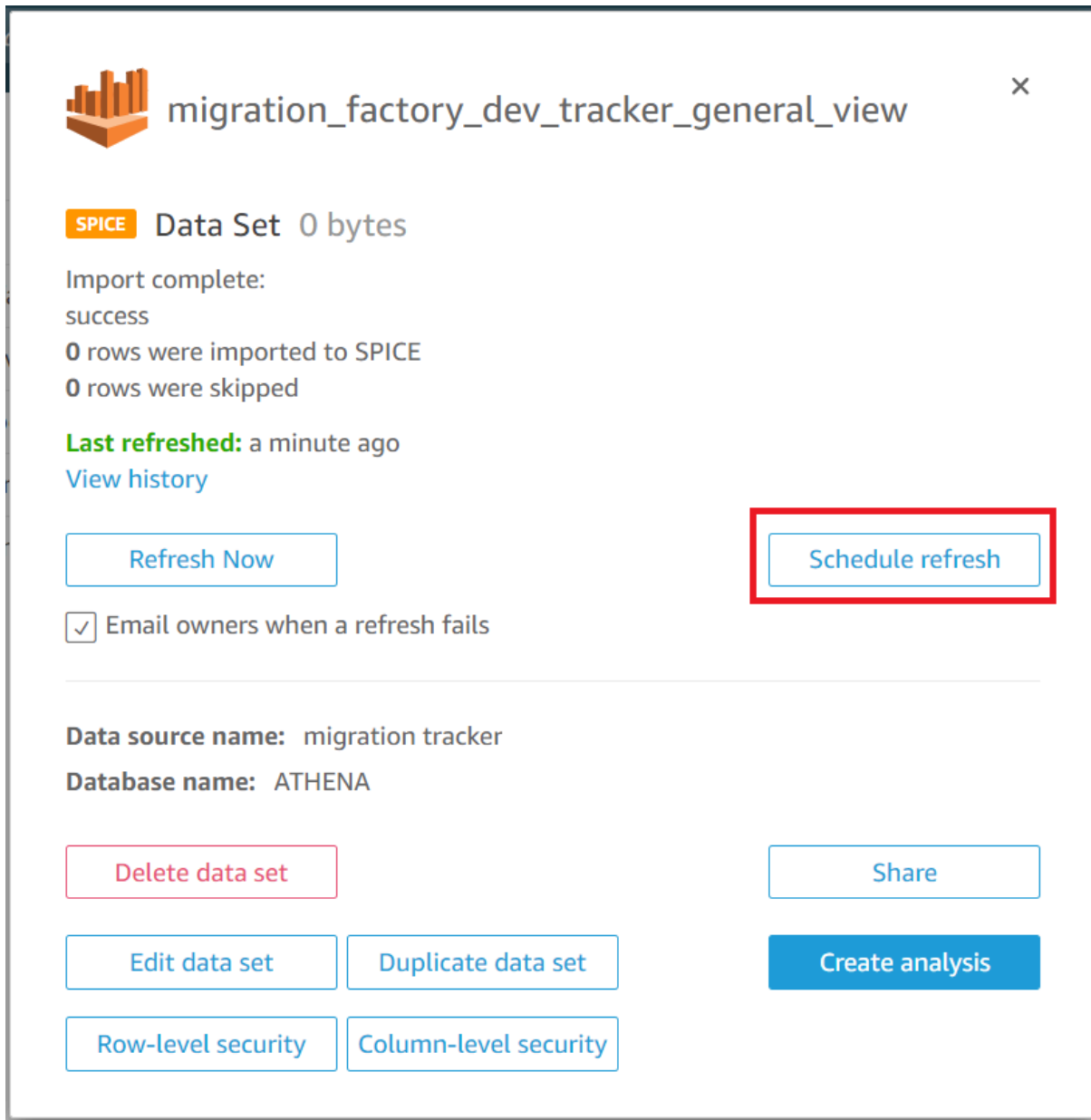
Search for analyses, data sets, and dashboards

- ★ 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. Wählen Sie auf der Seite *<migration-factory>-general-view* Datasets die Registerkarte Aktualisieren aus.



The screenshot displays a web interface for a data set named "migration_factory_dev_tracker_general_view". At the top left is a bar chart icon. The title "migration_factory_dev_tracker_general_view" is at the top right with a close button (X). Below the title, a "SPICE" badge is followed by "Data Set 0 bytes". The status "Import complete: success" is shown, along with "0 rows were imported to SPICE" and "0 rows were skipped". A green message "Last refreshed: a minute ago" is present, with a "View history" link below it. Two buttons are visible: "Refresh Now" and "Schedule refresh", with the latter highlighted by a red rectangular box. A checkbox "Email owners when a refresh fails" is checked. Below a horizontal separator, the "Data source name" is "migration tracker" and the "Database name" is "ATHENA". At the bottom, there are several buttons: "Delete data set" (red border), "Share", "Edit data set", "Duplicate data set", "Create analysis" (blue), "Row-level security", and "Column-level security".

5. Wählen Sie Neuen Zeitplan hinzufügen aus.
6. Wählen Sie auf der Seite Zeitplan für die Aktualisierung erstellen die Option Vollständige Aktualisierung aus, wählen Sie die entsprechende Zeitzone aus, geben Sie eine Startzeit ein und wählen Sie die Häufigkeit aus.
7. Wählen Sie Speichern.

Create a schedule ×

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

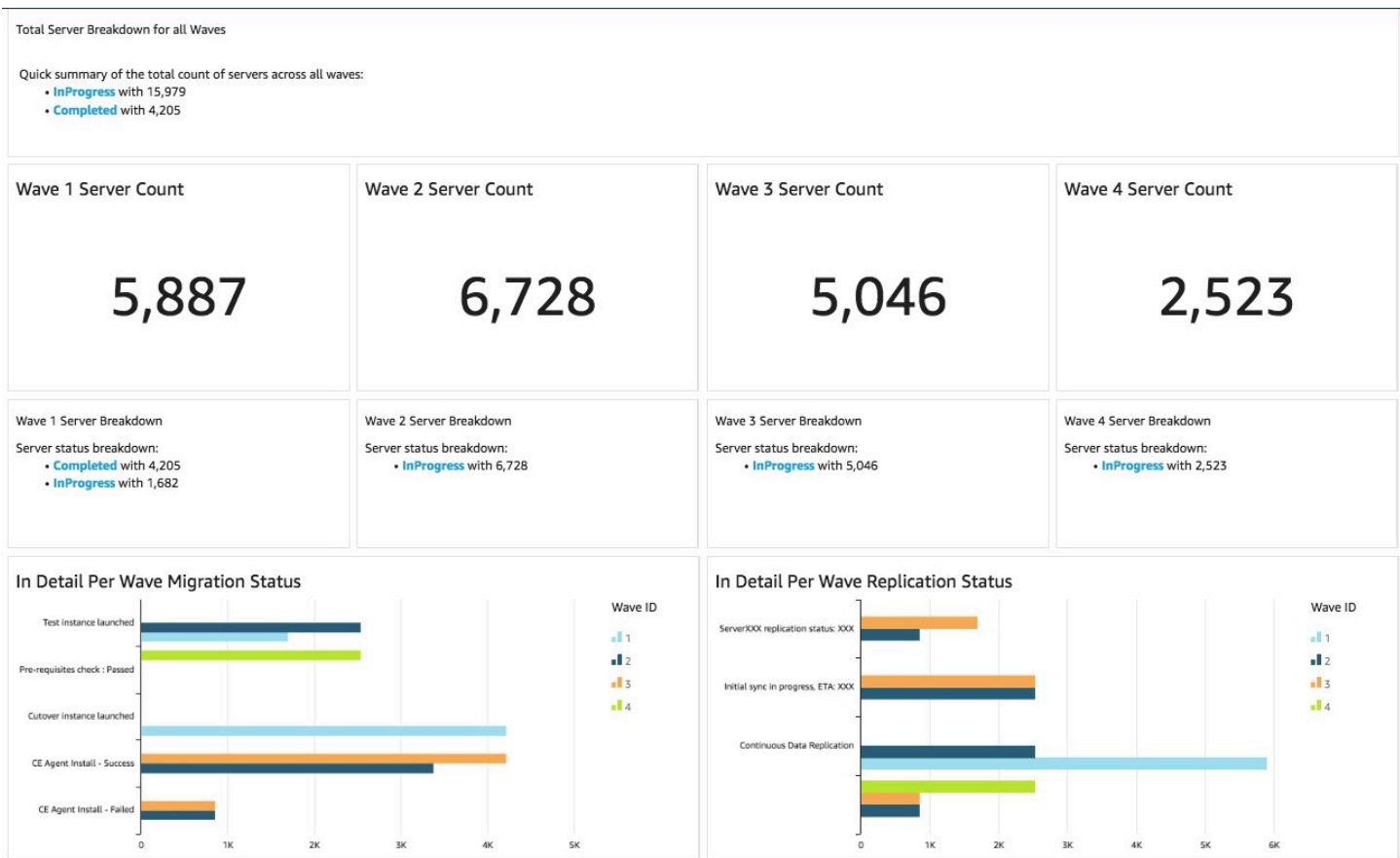
Time zone

Repeats ▾

Starting

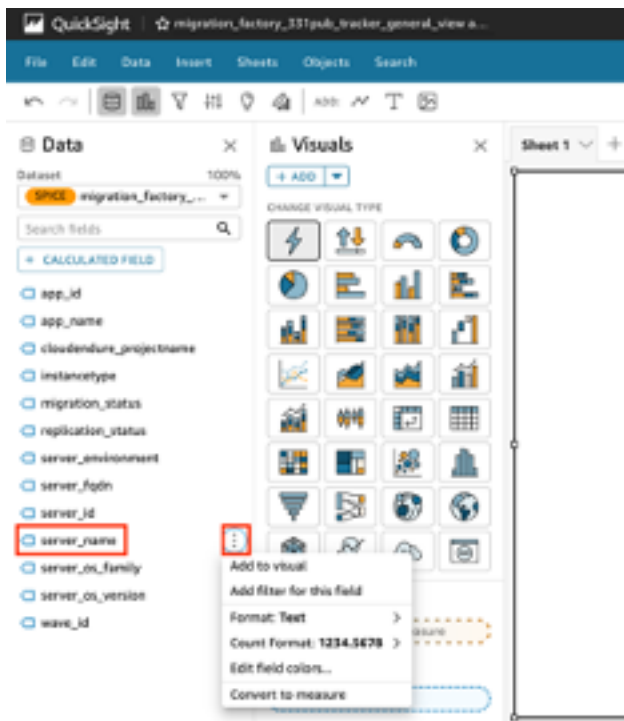
Erstellen eines Dashboards

Amazon QuickSight bietet die Flexibilität, ein benutzerdefiniertes Dashboard zu erstellen, das Ihnen hilft, Ihre Migrationsmetadaten zu visualisieren. Im folgenden Tutorial wird ein Dashboard mit einer Visualisierung zur Zählung erstellt, die die Serveranzahl nach Wellen und Balkendiagramme mit dem Migrationsstatus anzeigt. Sie können dieses Dashboard an Ihre Geschäftsanforderungen anpassen.

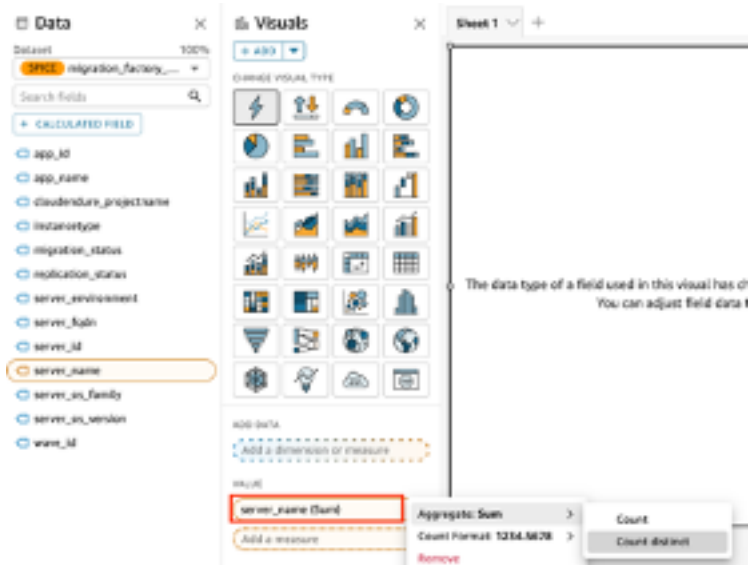


Führen Sie die folgenden Schritte aus, um eine Zählübersicht nach Migrationswellen zu erstellen. Diese Ansicht zählt alle Server im Datensatz, die pro Welle gruppiert sind, und bietet eine detaillierte Ansicht der Gesamtzahl der Server in einer Welle. Um diese Ansicht zu erstellen, konvertieren Sie `server_name` in eine Kennzahl, mit der Sie unterschiedliche Servernamen zählen können. Anschließend erstellen Sie einen Wave by Wave-Filter.

1. Navigieren Sie zur - QuickSight Homepage.
2. Wählen Sie im Navigationsbereich Analysen aus.
3. Wählen Sie *<migration-factory>*-general-view aus.
4. Bewegen Sie auf der Seite Visualisieren den Mauszeiger über `server_name` und wählen Sie die Ellipse rechts aus.



5. Wählen Sie Zu Maß umwandeln aus, um den Datensatz von einer Dimension in ein Maß zu konvertieren. Der Text `server_name` wird grün, um anzuzeigen, dass der Datensatz in ein Maß konvertiert wurde.
6. Wählen Sie `server_name` aus, um das Bild zu visualisieren. Die Visualisierung enthält eine Fehlermeldung, die darauf hinweist, dass die Felddatentypen aktualisiert werden müssen.
7. Wählen Sie im Bereich Visualisierungen den `server_name` (Summe) aus, wählen Sie unter Wert die Option Aggregieren: Summe und dann Verschiedene zählen aus.



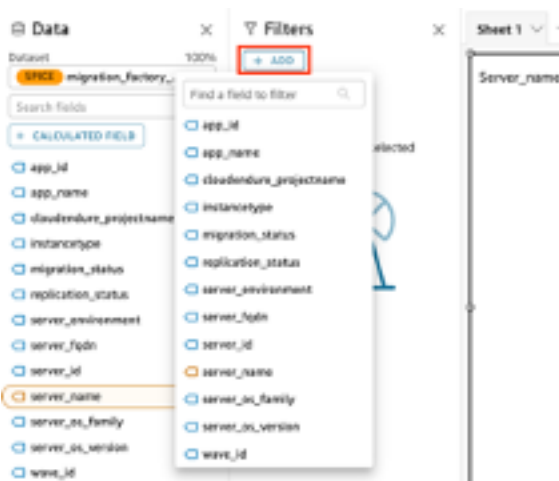
Es wird eine Anzahl der eindeutigen Servernamen angezeigt, die Sie in Ihrem Datensatz haben. Sie können die Größe der Visualisierung nach Bedarf ändern, um sicherzustellen, dass die Informationen auf Ihrem Monitor klar angezeigt werden.

Note

Möglicherweise müssen Sie Ihren Datensatz wieder in die Dimension konvertieren, wenn Sie eine weitere Visualisierung erstellen.

Fügen Sie als Nächstes Filter zur Visualisierung hinzu, um die Serveranzahl für jede Migrationskurve zu ermitteln. Mit den folgenden Schritten wird ein `wave_id`-Filter auf Ihre Visualisierung angewendet.

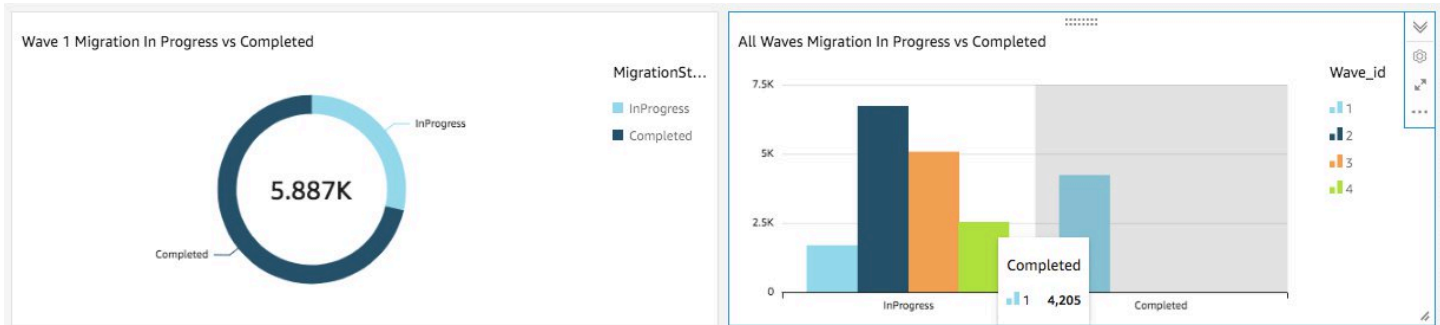
1. Stellen Sie sicher, dass die Visualisierung ausgewählt ist. Wählen Sie im oberen Navigationsbereich Filter aus.
2. Wählen Sie im linken Bereich Filter die Option HINZUFÜGEN und dann Wave_ID aus der Liste aus.



3. Wählen Sie `wave_id` aus der Filterliste aus.
4. Aktivieren Sie im Bereich Filter unter Suchwerte das Kontrollkästchen neben dem Wert 1.
5. Wählen Sie Apply (Anwenden) aus.
6. Ändern Sie in der Visualisierung den Titel in Wave 1 Server Count, indem Sie doppelt auf den aktuellen Titel klicken.

Wiederholen Sie diese Schritte für die anderen Wellen, die in Ihrem Dashboard visualisiert werden. Filterbereich bearbeiten

Die nächste Visualisierung, die wir im Dashboard hinzufügen werden, ist ein Donut-Diagramm mit Servern, die gerade migriert werden, im Vergleich zu Servern, die die Migration abgeschlossen haben. Dieses Diagramm verwendet superschnelle, parallele In-Memory-Berechnungs-Engine (SPICE)-Abfragen, indem eine neue Spalte im Datensatz erstellt wird, die bestimmt, dass ein unvollständiger Status als in Bearbeitung identifiziert wird. Alle Werte im Datensatz, die nicht abgeschlossen sind, werden kombiniert und als in Bearbeitung kategorisiert.



Note

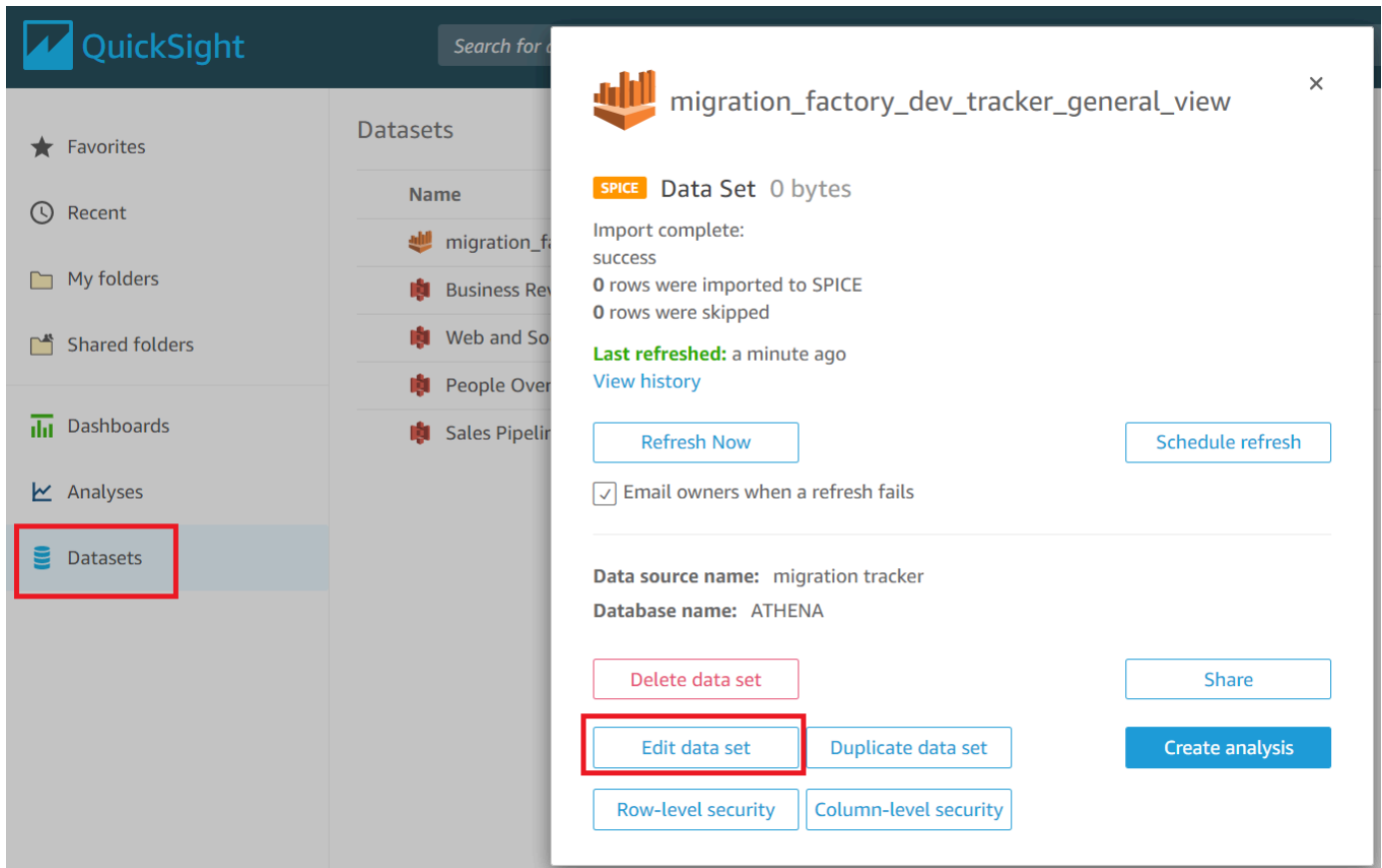
Wenn keine benutzerdefinierte Abfrage auf den Datensatz angewendet wird, können standardmäßig bis zu fünf Migrations-/Replikationsstatus angezeigt werden. Für diese Lösung wird eine MigrationStatusSummary Abfrage in einer neuen Spalte erstellt:

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

Diese Abfrage kombiniert die Werte der Status, um eine Spalte zu erstellen, die für die Visualisierung verwendet wird. Weitere Informationen zum Erstellen einer Abfrage finden Sie unter [Verwenden des Abfrage-Editors](#) im Amazon- QuickSight Benutzerhandbuch.

Gehen Sie wie folgt vor, um die MigrationStatusSummary Spalte zu erstellen:

1. Navigieren Sie zur - QuickSight Homepage.
2. Wählen Sie im Navigationsbereich Datensätze aus.
3. Wählen Sie auf der Seite Datensätze den *<migration-factory>*-general-view Datensatz aus.
4. Wählen Sie auf der Datensatzseite Datensatz bearbeiten aus.



5. Wählen Sie im Bereich Felder die Option + und dann Berechnetes Feld hinzufügen aus.
6. Geben Sie auf der Seite Berechnetes Feld hinzufügen einen Namen für Ihre SQL-Abfrage ein, z. B. MigrationStatusSummary.
7. Geben Sie die folgende SQL-Abfrage in den SQL-Editor ein:

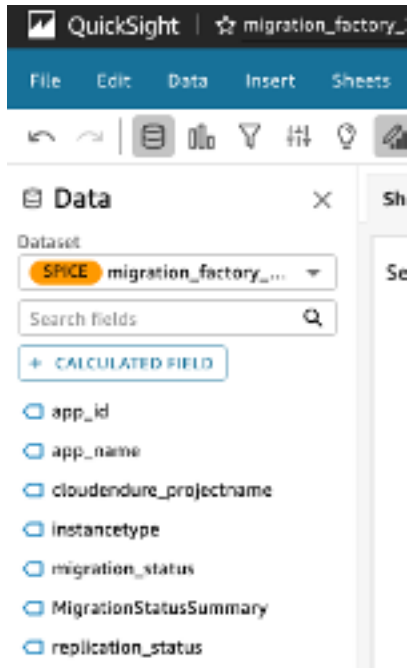
```
ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')
```

8. Wählen Sie Speichern.



9. Wählen Sie auf der Seite Datensatz die Option Speichern und veröffentlichen aus.

Ihre neu hinzugefügte Abfrage wird in der Liste Datensatzfelder aufgeführt.



Erstellen Sie als Nächstes das Dashboard.

1. Navigieren Sie zur - QuickSight Homepage.
2. Wählen Sie Analysen und dann die zuvor erstellten migration_factory-Analysen aus.
3. Stellen Sie sicher, dass in Blatt 1 keine Diagramme ausgewählt sind.
4. Bewegen Sie im Bereich Datensatz den Mauszeiger über die MigrationStatusSummary und wählen Sie die Ellipse auf der rechten Seite aus.
5. Wählen Sie Zur Visualisierung hinzufügen aus.
6. Wählen Sie dann Wave_ID aus.
7. Wählen Sie im Bereich Visualisierungen die Dimension X-Achse aus und verschieben Sie MigrationStatusSummary sie in die Dimension X-Achse und wählen Sie Wave_name als GROUP/COLOR aus.

Wenn Sie über eine Unternehmenslizenz für Amazon verfügen QuickSight, werden Erkenntnisse generiert, nachdem die benutzerdefinierten Spalten erstellt wurden. Sie können Ihre Beschreibungen für jeden Einblick anpassen. Beispielsweise:



Sie können die Daten auch anpassen, indem Sie die Metadaten in Wellen aufteilen. Beispielsweise:



(Optional) Anzeigen von Insights im QuickSight Dashboard

Note

Sie können das folgende Verfahren verwenden, wenn Sie über eine Unternehmenslizenz für Amazon verfügen QuickSight.

Führen Sie die folgenden Schritte aus, um Ihrem Dashboard einen Einblick hinzuzufügen, der eine Aufschlüsselung der abgeschlossenen und laufenden Migrationen zeigt.

1. Wählen Sie im oberen Navigationsbereich Insights aus.
2. Bewegen Sie auf der Seite Insights im Abschnitt Anzahl der Datensätze BY MIGRATIONSTATUSSUMMARY den Mauszeiger über das Element Top 2 MigrationSummarys und wählen Sie + aus, um der Visualisierung einen Einblick hinzuzufügen.

Filter

TOP 3 SERVER_IDS

Top 3 server_ids for total count of records are:

- 2 with 1
- 4 with 1
- 5 with 1

Parameters

TOP 3 REPLICATION_STATUS

Top 3 replication_status for total count of records are:

- Continuous Data Replication with 2
- Initial sync in progress, ETA: 24 Minutes with 1
- Initial sync in progress, ETA: 14 Minutes with 1

Actions

COUNT OF RECORDS BY MIGRATIONSTATUSSUMMARY

TOP 2 MIGRATIONSTATUSSUMMARY

Top 2 MigrationStatusSummaries for total count of records are:

- Completed with 2
- InProgress with 1

Themes

Settings

3. Passen Sie die Erkenntnis für Ihre Analyse an, indem Sie in der Visualisierung die Option Customizerative auswählen.

Top ranked

Top 2 MigrationStatusSummary for total count of server_name are:

- InProgress with 15,979
- Completed with 4,205

Total Server Breakdown for all Waves

Insert code Paragraph B i U S Abc Abc

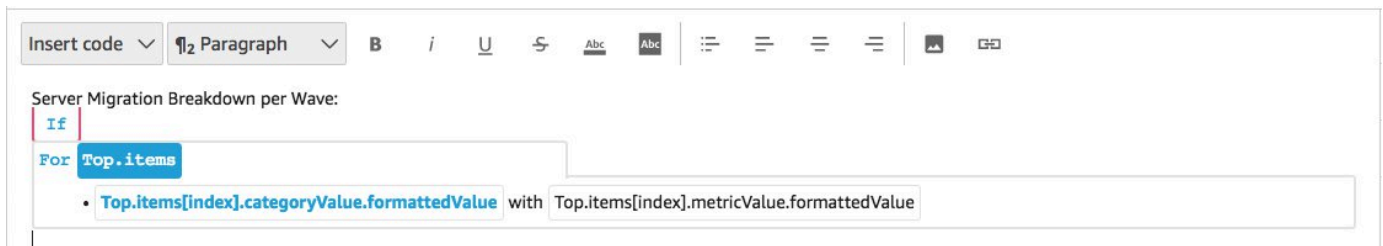
Top If Top.itemsCount > 1 Top.itemsCount Top.categoryField.name for total count of Top.metricField.name If Top.itemsCount > 1 are: I

f Top.itemsCount < 2 is:

For Top.items

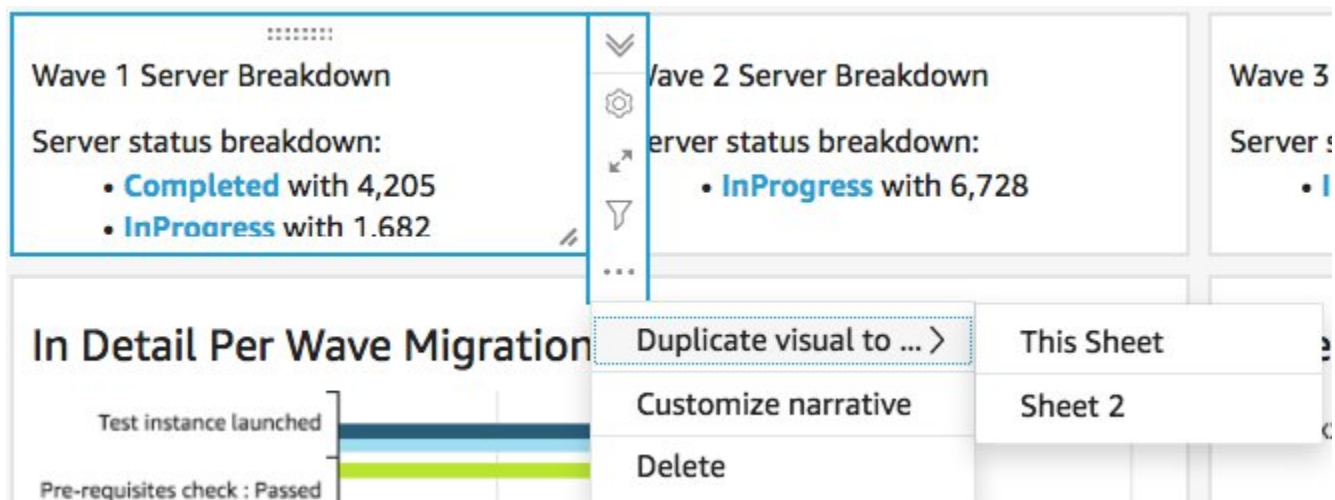
- Top.items[index].categoryValue.formattedValue with Top.items[index].metricValue.formattedValue

4. Bearbeiten Sie die Beschreibung entsprechend Ihrem Anwendungsfall und wählen Sie Speichern aus. Beispielsweise:



Kehren Sie zum Dashboard zurück und filtern Sie es, um jede Welle anzuzeigen:

5. Wählen Sie im linken Menübereich Filter aus.
6. Wählen Sie die Schaltfläche + und dann Wave_ID aus.
7. Wählen Sie eine zu visualisierende Welle aus und wählen Sie Anwenden aus.
8. Um alle Migrationswellen zu visualisieren, duplizieren Sie die Visualisierungen, indem Sie die Ellipse auf der linken Seite der Visualisierung auswählen und dann Visualisierung duplizieren auswählen.



9. Ändern Sie den Filter für jede Visualisierung, um eine Aufschlüsselung für jede Migrationskurve anzuzeigen.

Diese Erkenntnis wird angepasst, um die Gesamtzahl der Server in allen Wellen zusammenzufassen. Weitere Informationen und Anleitungen zum Anpassen von Erkenntnissen finden Sie unter [Arbeiten mit Insights](#) im QuickSight -Benutzerhandbuch. Sie können von jedem Gerät aus auf dieses QuickSight Dashboard zugreifen und es nahtlos in Ihre Anwendungen, Portale und Websites einbetten. Weitere Informationen zu QuickSight Dashboards finden Sie unter [Arbeiten mit Dashboards](#) im Amazon- QuickSight Benutzerhandbuch.

Schritt 10: (Optional) Konfigurieren zusätzlicher Identitätsanbieter in Amazon Cognito

Wenn Sie `true` für die optionale Konfiguration des zusätzlichen Identitätsanbieters im Cognito-Parameter beim Starten des Stacks ausgewählt haben, können Sie zusätzliche IdPs in Amazon Cognito einrichten, um die Anmeldung mit dem vorhandenen SAML-IdP zu ermöglichen. Der Prozess zum Einrichten des externen IdP variiert je nach Anbieter. In diesem Abschnitt werden die Amazon Cognito-Konfiguration und generische Schritte zur Konfiguration des externen IdP beschrieben.

Führen Sie die folgenden Schritte aus, um Informationen von Amazon Cognito zu sammeln, die dem externen IdP zur Verfügung gestellt werden:

1. Navigieren Sie zur [AWS- CloudFormation Konsole](#) und wählen Sie den Stack Cloud Migration Factory in AWS aus.
2. Wählen Sie die Registerkarte Ausgaben aus.
3. Suchen UserPoolId und notieren Sie in der Spalte Schlüssel den Wert, der später während der Einrichtung verwendet werden soll.
4. Navigieren Sie zur [Amazon-Cognito-Konsole](#).
5. Wählen Sie den Benutzerpool aus der Lösungs-Stack-Ausgabe aus, der der Benutzerpool-ID entspricht.
6. Wählen Sie die Registerkarte App-Integration und notieren Sie sich die Cognito-Domäne, die Sie später während der Einrichtung verwenden möchten.

Führen Sie die folgenden Schritte innerhalb der Verwaltungsschnittstelle Ihres vorhandenen IdP:

Note

Diese Anweisungen sind generisch und unterscheiden sich zwischen den Anbietern. Ausführliche Informationen zur Einrichtung von SAML-Anwendungen finden Sie IdP.

1. Navigieren Sie zur Verwaltungsschnittstelle Ihres IdP.
2. Wählen Sie die Option zum Hinzufügen von Anwendungen oder zum Einrichten der SAML-Authentifizierung für eine Anwendung aus und erstellen oder fügen Sie eine neue Anwendung hinzu.

3. Bei der Einrichtung dieser SAML-Anwendung werden Sie nach den folgenden Werten gefragt:

a. ID (Entitäts-ID) oder ähnliches. Geben Sie den folgenden Wert an:

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

b. Antwort-URL (Assertion Consumer Service URL) oder ähnliches. Geben Sie den folgenden Wert an:

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


c. Attribute und Ansprüche oder ähnliches. Stellen Sie mindestens sicher, dass eine eindeutige Kennung oder ein eindeutiger Betreff zusammen mit einem Attribut konfiguriert ist, das die E-Mail-Adresse des Benutzers angibt.

4. Es gibt entweder eine Metadaten-URL oder die Möglichkeit, eine Metadaten-XML-Datei herunterzuladen. Laden Sie eine Kopie der Datei herunter oder notieren Sie sich die URL, die später während der Einrichtung verwendet werden soll.
5. Konfigurieren Sie innerhalb der Einrichtung die Zugriffsliste der Benutzer vom IdP, die sich bei der CMF-Anwendung anmelden dürfen. Allen Benutzern, die Zugriff auf die Anwendung im IdP erhalten, wird automatisch schreibgeschützter Zugriff auf die CMF-Konsole gewährt.

Führen Sie die folgenden Schritte aus, um den neuen IdP zum Amazon Cognito-Benutzerpool hinzuzufügen, der während der Stack-Bereitstellung erstellt wurde:

1. Navigieren Sie zur [Amazon-Cognito-Konsole](#).
2. Wählen Sie den Benutzerpool aus der Lösungs-Stack-Ausgabe aus, der der Benutzerpool-ID entspricht.
3. Wählen Sie die Registerkarte Sign-in experience (Anmeldeerlebnis) aus.
4. Wählen Sie Identitätsanbieter hinzufügen und dann SAML als Drittanbieter aus.
5. Geben Sie einen Namen für den Anbieter an. Dieser wird dem Benutzer auf dem CMF-Anmeldebildschirm angezeigt.
6. Geben Sie im Abschnitt Metadatendokumentquelle entweder die Metadaten-URL an, die von der IDP-SAML-Einrichtung erfasst wurde, oder laden Sie die Metadaten-XML-Datei hoch.
7. Wählen Sie im Abschnitt Attribute zuordnen die Option Weiteres Attribut hinzufügen aus.
8. Wählen Sie E-Mail für den Wert des Benutzerpool-Attributs aus. Geben Sie für das SAML-Attribut den Namen des Attributs ein, für das Ihr externer IdP die E-Mail-Adresse bereitstellen wird.

9. Wählen Sie Identitätsanbieter hinzufügen, um diese Konfiguration zu speichern.
10. Wählen Sie die Registerkarte App integration (Anwendungsintegration) aus.
11. Wählen Sie im Abschnitt App-Clientliste den Migrationsfazilanwendungsclient aus (es sollte nur ein Client aufgeführt sein), indem Sie auf den Namen klicken.
12. Wählen Sie im Abschnitt Gehostete Benutzeroberfläche die Option Bearbeiten aus.
13. Aktualisieren Sie die ausgewählten Identitätsanbieter, indem Sie den neuen IdP auswählen, den Sie in Schritt 5 hinzugefügt haben, und die Auswahl des Cognito-Benutzerpools aufheben.

 Note

Cognito-Benutzerpool ist nicht erforderlich, da er in den CMF-Anmeldebildschirm integriert ist. Wenn er ausgewählt ist, wird er zweimal angezeigt.

14. Wählen Sie Änderungen speichern aus.

Die Konfiguration ist jetzt abgeschlossen. Auf der CMF-Anmeldeseite sehen Sie die Schaltfläche Mit Ihrer Unternehmens-ID anmelden. Wenn Sie diese Option wählen, wird der Anbieter angezeigt, den Sie zuvor konfiguriert haben. Benutzer, die diese Option wählen, werden angewiesen, sich anzumelden und dann zur CMF-Konsole zurückzukehren, sobald sie sich erfolgreich angemeldet haben.

Überwachung der Lösung mit Service Catalog AppRegistry

Diese Lösung umfasst eine Service AppRegistry Catalog-Ressource, mit der die CloudFormation Vorlage und die zugrunde liegenden Ressourcen als Anwendung sowohl in [Service Catalog AppRegistry](#) als auch im [AWSSystems Manager Application Manager](#) registriert werden können.

Application Manager bietet Ihnen einen Überblick über diese Lösung und ihre Ressourcen auf Anwendungsebene, sodass Sie:

- Überwachen Sie die Ressourcen, die Kosten für die bereitgestellten Ressourcen über Stacks und AWS-Konten die mit dieser Lösung verknüpften Protokolle von einem zentralen Standort aus.
- Zeigen Sie Betriebsdaten für die AWS Ressourcen der Lösung (z. B. Bereitstellungsstatus, [CloudWatch Amazon-Alarme](#), Ressourcenkonfigurationen und Betriebsprobleme) im Kontext einer Anwendung an.

Die folgende Abbildung zeigt ein Beispiel für die Anwendungsansicht für den Cloud Migration Factory One AWS-Stack in Application Manager.

The screenshot displays the AWS Systems Manager Application Manager interface. On the left, a 'Components (7)' sidebar lists various resources like 'cmf32-Replatform...', 'cmf32', and 'cmf32-AppMigSer...'. The main area shows the application 'migration-factory-cmf32-us-east-...' with a 'Start runbook' button. Below this, the 'Application information' section includes details like 'Application type: AWS-AppRegistry', 'Name: migration-factory-cmf32-us-east-...', and 'Application monitoring: Not enabled'. A navigation bar offers tabs for Overview, Resources, Instances, Compliance, Monitoring, OpsItems, Logs, and Runbooks. The 'Insights and Alarms' section features a donut chart showing 27 units (58%) as 'OK' and 45 units (63%) as 'Insufficient'. The 'Cost' section shows a line graph for 'Cost (USD)' over time, with a table below indicating zero total cost for October, November, and December 2022.

Application	Oct 2022	Nov 2022	Dec 2022
migration-factory-cmf32-us-east-...	0	0	0
Total cost (USD)	0	0	0

Note

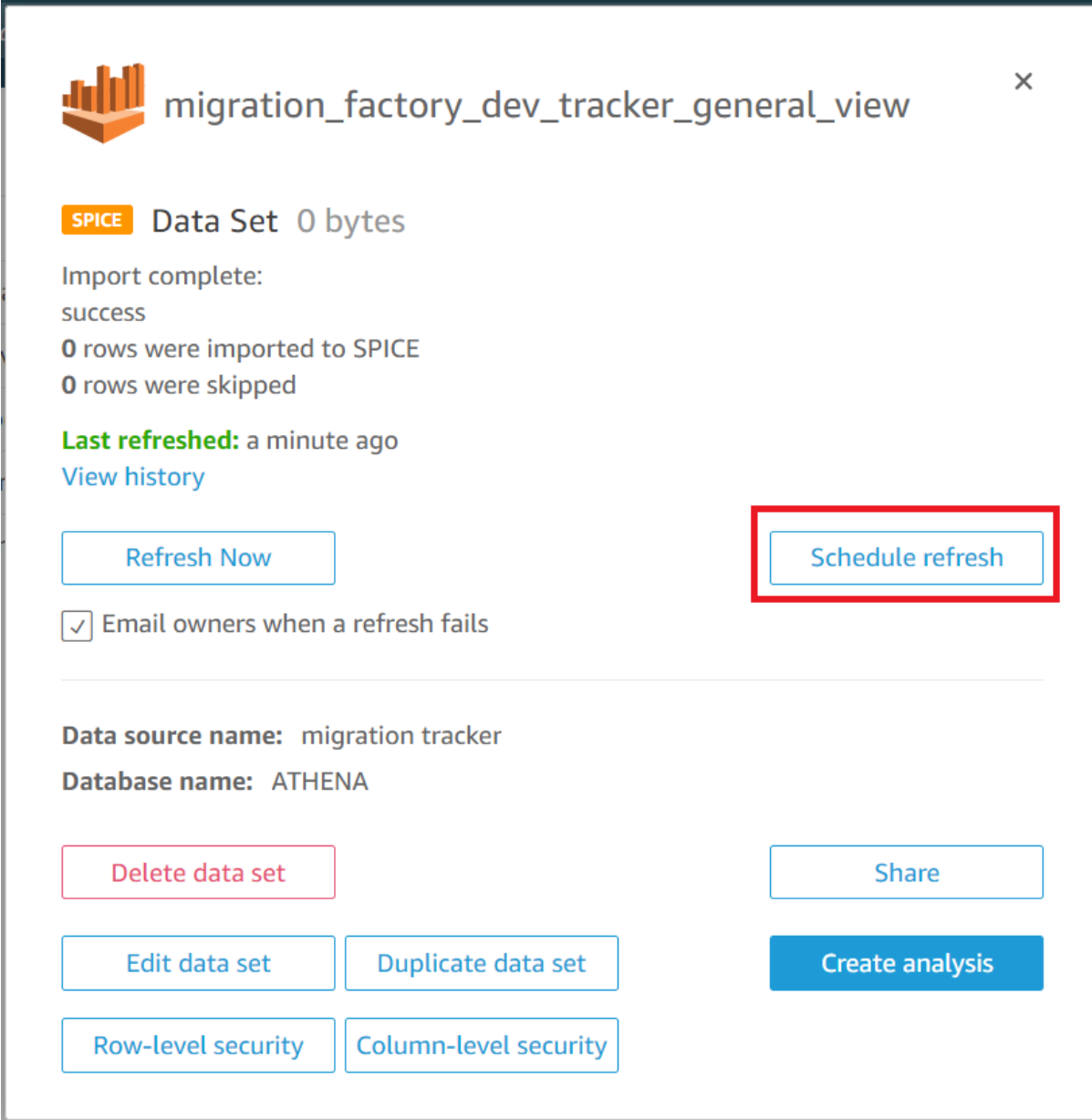
Sie müssen die mit dieser Lösung AWS Cost Explorer verknüpften Tags CloudWatch Application Insights und Cost Allocation aktivieren. Sie sind standardmäßig nicht aktiviert.

Aktivieren Sie CloudWatch Application Insights

1. Melden Sie sich bei der [Systems Manager Manager-Konsole](#) an.
2. Wählen Sie im Navigationsbereich Application Manager aus.
3. Wählen Sie unter Anwendungen die Option AppRegistry Anwendungen aus.
4. Suchen Sie in AppRegistryAnwendungen nach dem Anwendungsnamen für diese Lösung und wählen Sie ihn aus.

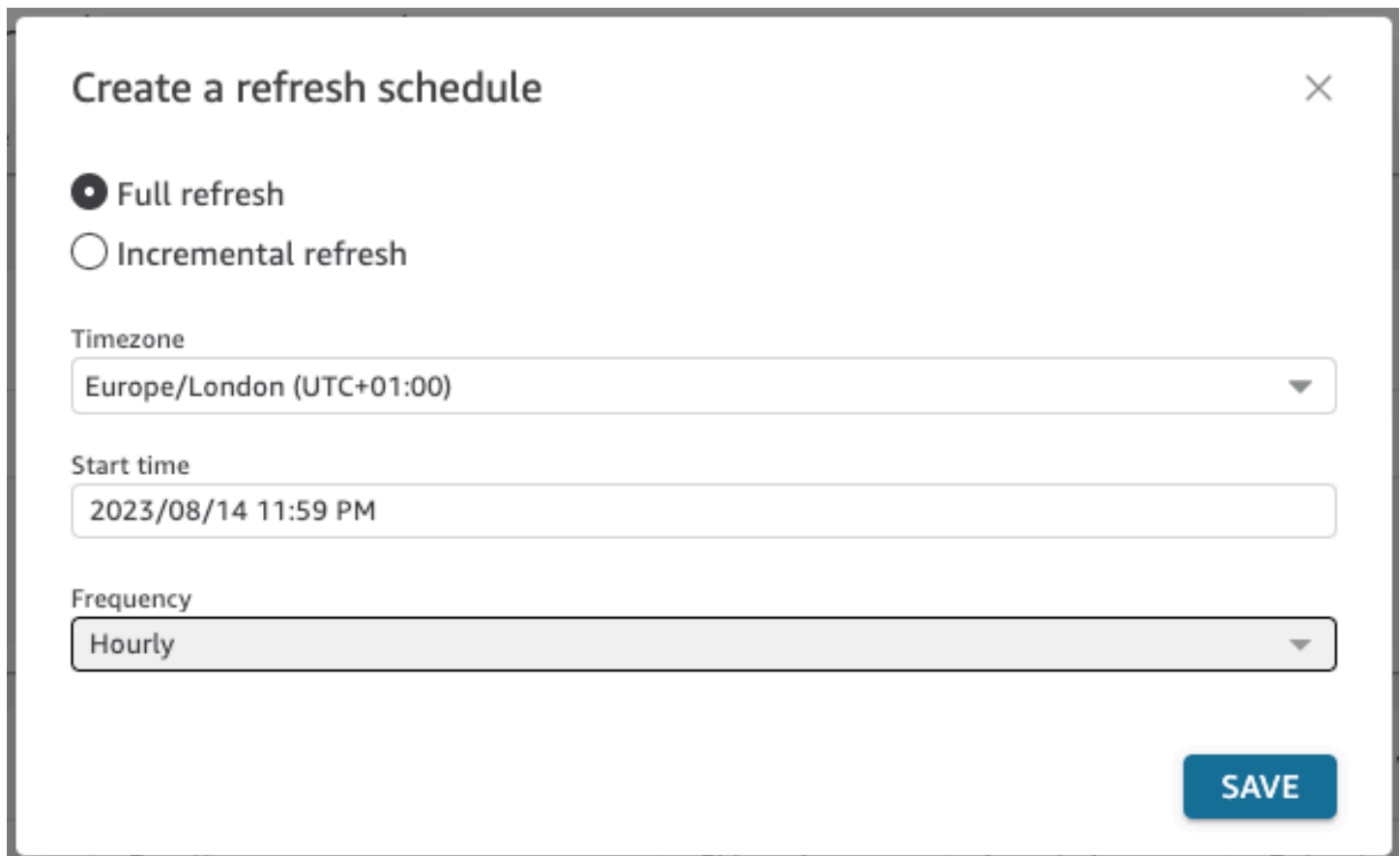
Wenn Sie den Anwendungsmanager das nächste Mal öffnen, finden Sie die neue Anwendung für Ihre Lösung in der AppRegistry Anwendungskategorie.

5. Wählen Sie in der Komponentenstruktur den Anwendungsstapel aus, den Sie aktivieren möchten.
6. Wählen Sie auf der Registerkarte Überwachung in Application Insights die Option Anwendungsüberwachung automatisch konfigurieren aus.



The screenshot displays a web interface for a data set named "migration_factory_dev_tracker_general_view". At the top left is a bar chart icon. The title "migration_factory_dev_tracker_general_view" is at the top right with a close button (X). Below the title, a yellow "SPICE" tag is followed by "Data Set 0 bytes". The status "Import complete: success" is shown, along with "0 rows were imported to SPICE" and "0 rows were skipped". A green "Last refreshed: a minute ago" message is present, with a blue "View history" link. A "Refresh Now" button is on the left, and a "Schedule refresh" button is on the right, highlighted with a red border. Below these is a checked checkbox for "Email owners when a refresh fails". A horizontal separator line follows. The "Data source name: migration tracker" and "Database name: ATHENA" are listed. At the bottom, there are buttons for "Delete data set" (red border), "Share", "Edit data set", "Duplicate data set", "Create analysis" (blue), "Row-level security", and "Column-level security".

7. Die Überwachung Ihrer Anwendungen ist jetzt aktiviert und das folgende Statusfeld wird angezeigt:



Create a refresh schedule ✕

Full refresh
 Incremental refresh

Timezone
Europe/London (UTC+01:00) ▼

Start time
2023/08/14 11:59 PM

Frequency
Hourly ▼

SAVE

Aktivieren AWS Cost Explorer

Eine Übersicht der mit der Anwendung und den Anwendungskomponenten verbundenen Kosten finden Sie in der Application Manager-Konsole. Die Integration AWS Cost Explorer muss zuerst aktiviert werden. Der Cost Explorer hilft Ihnen bei der Kostenverwaltung, indem er Ihnen einen Überblick über Ihre AWS Ressourcenkosten und -nutzung im Laufe der Zeit bietet. So aktivieren Sie den Cost Explorer für die Lösung:

1. Melden Sie sich bei der [AWSCost Management Console](#) an.
2. Wählen Sie im linken Navigationsmenü Cost Explorer aus.
3. Wählen Sie auf der Seite Welcome to Cost Explorer (Willkommen bei Cost Explorer) die Option Launch Cost Explorer (Cost Explorer starten).

Es kann bis zu 24 Stunden dauern, bis der Aktivierungsvorgang abgeschlossen ist. Nach der Aktivierung können Sie die Cost Explorer Explorer-Benutzeroberfläche öffnen, um die Kostendaten für die Lösung weiter zu analysieren.

Aktivieren Sie die mit der Lösung verknüpften Kostenzuweisungs-Tags

Nachdem Sie den Cost Explorer aktiviert haben, müssen Sie die mit dieser Lösung verknüpften Kostenzuordnungs-Tags aktivieren, um die Kosten für diese Lösung zu sehen. Die Kostenzuweisungs-Tags können nur über das Verwaltungskonto der Organisation aktiviert werden. So aktivieren Sie Tags für die Kostenzuweisung:

1. Melden Sie sich bei der [AWS Billing and Cost Management und Cost Management Console](#) an und wählen Sie im linken Navigationsmenü die Option Cost Allocation Tags aus.
2. Filtern Sie auf der Seite mit den Tags für die Kostenzuweisung `AppManagerCFNStackKey` nach dem Tag und wählen Sie dann das Tag aus den angezeigten Ergebnissen aus.
3. Wählen Sie Activate.

Es kann bis zu 24 Stunden dauern, bis der Aktivierungsvorgang abgeschlossen ist und die Tag-Daten angezeigt werden.

Bestätigen Sie die mit der Lösung verknüpften Kostenschilder


Nachdem Sie die mit der Lösung verknüpften Kostenzuordnungs-Tags aktiviert haben, müssen Sie die Kostenzuordnungs-Tags bestätigen, um die Kosten für diese Lösung zu sehen. So bestätigen Sie die Tags für die Kostenzuweisung:

1. Melden Sie sich bei der [Systems Manager Manager-Konsole](#) an.
2. Wählen Sie im Navigationsbereich Application Manager aus.
3. Wählen Sie unter Anwendungen den Anwendungsnamen für diese Lösung und wählen Sie ihn aus.
4. Wählen Sie auf der Registerkarte Übersicht unter Kosten die Option Benutzertag hinzufügen aus.

Cost

View resource costs per application using AWS Cost Explorer.

[View all](#)



To enable cost tracking, add the "AppManagerCFNStackKey" user tag to your CloudFormation stack.

Adding the user tag will require redeployment of the stack.

[Add user tag](#)

5. Geben Sie auf der Seite Benutzertag hinzufügen den Text ein `confirm` und wählen Sie dann Benutzertag hinzufügen aus.

Es kann bis zu 24 Stunden dauern, bis der Aktivierungsvorgang abgeschlossen ist und die Tag-Daten angezeigt werden.

Aktualisieren Sie die Lösung

Wenn Sie die Lösung bereits bereitgestellt haben, gehen Sie wie folgt vor, um den Cloud Migration Factory on CloudFormation AWS-Lösungsstapel zu aktualisieren und die neueste Version des Lösungsframeworks zu erhalten.

1. Melden Sie sich bei der [AWS CloudFormationKonsole](#) an, wählen Sie Ihre bestehende Cloud Migration Factory im AWS CloudFormation Lösungsstapel aus und wählen Sie Aktualisieren aus.
2. Wählen Sie Aktuelle Vorlage ersetzen aus.
3. Gehen Sie unter Vorlage angeben wie folgt vor:
 - a. Wählen Sie Amazon S3 S3-URL aus.
 - b. Kopieren Sie den Link für die [neueste Vorlage](#).
 - c. Fügen Sie den Link in das Amazon S3 S3-URL-Feld ein.
 - d. Vergewissern Sie sich, dass die richtige Vorlagen-URL im Textfeld Amazon S3 S3-URL angezeigt wird, und wählen Sie Weiter. Wählen Sie erneut Next (Weiter).
4. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Weitere Informationen finden Sie in [Schritt 2. Starten Sie den Stack](#) für Details zu den Parametern.
5. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
7. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Achten Sie darauf, das Kästchen anzukreuzen, das bestätigt, dass die Vorlage möglicherweise AWS Identity and Access Management (IAM-) Ressourcen erstellt.
8. Wählen Sie Änderungssatz anzeigen und überprüfen Sie die Änderungen.
9. Wählen Sie Stack aktualisieren, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 10 Minuten den Status UPDATE_COMPLETE erhalten.

Nach der Aktualisierung des Stacks müssen Sie die API Gateway Gateway-APIs erneut bereitstellen: admin, login, tools und user. Dadurch wird sichergestellt, dass alle Änderungen an der Konfiguration für alle APIs verfügbar sind.

1. Melden Sie sich bei der [Amazon API Gateway Gateway-Konsole](#) an, wählen Sie im linken Navigationsbereich APIs und dann die CMF-API aus.
2. Wählen Sie in den API-Ressourcen Aktionen und anschließend API bereitstellen aus.
3. Wählen Sie Deployment Stage of prod und anschließend Deploy aus.
4. Wiederholen Sie die Schritte 1—3 für jede der CMF-APIs.

Deinstalliere die Lösung

Sie können die Cloud Migration Factory on AWS-Lösung über den AWS Management Console oder deinstallieren, indem Sie den verwenden AWS Command Line Interface. Sie müssen alle Amazon Simple Storage Service (Amazon S3) -Buckets, die mit dieser Lösung AWS Lösungsimplementierungen löschen S3-Buckets nicht automatisch, falls Sie Daten zur Aufbewahrung gespeichert haben.

Leeren Amazon S3 SBuckets

Wenn Sie sich entscheiden, den AWS CloudFormation Stack zu löschen, ist diese Lösung so konfiguriert, dass der erstellte Amazon S3 S3-Bucket (für die Bereitstellung in einer Opt-In-Region) beibehalten wird, um versehentlichen Datenverlust zu verhindern. Sie müssen alle S3-Buckets manuell leeren, bevor Sie den Stapel vollständig löschen. Follow these steps to empty the Amazon S3 bucket.

1. Melden Sie sich bei der [Amazon S3-Konsole](#) an.
2. Klicken Sie auf Buckets.
3. Suchen Sie die <stack-name>S3-Buckets.
4. Wählen Sie den S3-Bucket aus und wählen Sie Empty.

AWS

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

Verwenden von AWS Management Console, um den Stapel zu löschen

1. Melden Sie sich an der [AWS CloudFormation-Konsole](#) an.
2. Wählen Sie auf der Seite Stacks den Installationsstack dieser Lösung aus.
3. Wählen Sie Löschen.

Wird verwendetAWS Command Line Interface, um den Stapel zu löschen

Ermitteln Sie, ob dieAWS Command Line Interface (AWS CLI) in Ihrer Umgebung verfügbar ist. Installationsanweisungen finden Sie unter [Was ist dasAWS Command Line Interface](#) im AWS CLI-Benutzerhandbuch. AWS

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

Benutzerhandbuch

Die folgenden Abschnitte enthalten Anleitungen zur Nutzung der verschiedenen Funktionen, die in einer bereitgestellten Cloud Migration Factory on AWS-Instanz bei einer groß angelegten Migration zu AWS verfügbar sind.

Verwaltung von Metadaten

Die Cloud Migration Factory AWS on-Lösung bietet einen erweiterbaren Datenspeicher, mit dem Datensätze von der Benutzeroberfläche aus hinzugefügt, bearbeitet und gelöscht werden können. Alle Aktualisierungen der im Datenspeicher gespeicherten Daten werden mit Prüfstempeln auf Datensatzebene geprüft, die Zeitstempel für die Erstellung und Aktualisierung zusammen mit Benutzerdetails enthalten. Der gesamte Aktualisierungszugriff auf Datensätze wird durch die Gruppen und die zugehörigen Richtlinien gesteuert, die dem angemeldeten Benutzer zugewiesen wurden. Weitere Informationen zur Gewährung von Benutzerberechtigungen finden Sie unter [Berechtigungsverwaltung](#).

Daten anzeigen

Über den Navigationsbereich der Migrationsverwaltung können Sie die Datensatztypen (Anwendung, Welle, Datenbank, Server) auswählen, die im Datenspeicher gespeichert sind. Nachdem Sie eine Ansicht ausgewählt haben, wird eine Tabelle mit den vorhandenen Datensätzen für den ausgewählten Datensatztyp angezeigt. Die Tabelle jedes Datensatztyps enthält einen Standardsatz von Spalten, der vom Benutzer geändert werden kann. Änderungen bleiben zwischen den Sitzungen bestehen und werden im Browser und auf dem Computer gespeichert, auf dem die Änderungen vorgenommen wurden.

Ändern der in Tabellen angezeigten Standardspalten

Um die Standardspalten zu ändern, wählen Sie das Einstellungssymbol in der oberen rechten Ecke einer beliebigen Datentabelle und dann die anzuzeigenden Spalten aus. Von diesem Bildschirm aus können Sie auch die Standardanzahl der anzuzeigenden Zeilen ändern und den Zeilenumbruch für Spalten mit großen Datenmengen aktivieren.

Einen Datensatz anzeigen

Um einen bestimmten Datensatz in einer Tabelle anzuzeigen, können Sie auf eine beliebige Stelle in der Zeile klicken oder das Kontrollkästchen neben der Zeile aktivieren. Wenn Sie mehrere Zeilen

auswählen, wird kein Datensatz angezeigt. Dadurch wird der Datensatz dann im schreibgeschützten Modus unter der Datentabelle am unteren Bildschirmrand angezeigt. Für den angezeigten Datensatz stehen die folgenden Standardtabellen zur Verfügung.

Details — Dies ist eine zusammenfassende Ansicht der erforderlichen Attribute und Werte für den Datensatztyp.

Alle Attribute — Hier wird eine vollständige Liste aller Attribute und ihrer Werte angezeigt.

Je nach ausgewähltem Datensatztyp können weitere Registerkarten vorhanden sein, die zugehörige Daten und Informationen enthalten. Anwendungsdatensätze verfügen beispielsweise über die Registerkarte **Server**, auf der eine Tabelle mit den Servern angezeigt wird, die zu der ausgewählten Anwendung gehören.

Einen Datensatz hinzufügen oder bearbeiten

Die Vorgänge werden je nach Datensatztyp über Benutzerberechtigungen gesteuert. Wenn ein Benutzer nicht über die erforderlichen Rechte verfügt, um einen bestimmten Datensatztyp hinzuzufügen oder zu bearbeiten, sind die Schaltflächen **Hinzufügen** und/oder **Bearbeiten** ausgegraut und deaktiviert.

Um einen neuen Datensatz hinzuzufügen:

1. Wählen Sie in der oberen rechten Ecke der Tabelle die Option **Hinzufügen** für den Datensatztyp, den Sie erstellen möchten.

Standardmäßig werden auf dem Bildschirm „Anwendung hinzufügen“ die Abschnitte **Details** und **Audit** angezeigt. Je nach Typ und etwaigen Anpassungen des Schemas können jedoch auch andere Abschnitte angezeigt werden.

2. Wenn Sie das Formular ausgefüllt und alle Fehler behoben haben, wählen Sie **Speichern**.

Um einen vorhandenen Datensatz zu bearbeiten:

1. Wählen Sie einen Datensatz aus der Tabelle aus, den Sie bearbeiten möchten, und wählen Sie dann **Bearbeiten**.
2. Bearbeiten Sie den Datensatz und stellen Sie sicher, dass keine Validierungsfehler vorliegen, und wählen Sie dann **Speichern**.

Einen Datensatz löschen

Wenn ein Benutzer nicht berechtigt ist, einen bestimmten Datensatztyp zu löschen, ist die Schaltfläche Löschen ausgegraut und deaktiviert.

Important

Aus dem Datenspeicher gelöschte Datensätze können nicht wiederhergestellt werden. Wir empfehlen, regelmäßige Backups der DynamoDB-Tabelle zu erstellen oder die Daten zu exportieren, um sicherzustellen, dass es im Falle eines Problems einen Wiederherstellungspunkt gibt.

Um einen oder mehrere Datensätze zu löschen:

1. Wählen Sie einen oder mehrere Datensätze aus der Tabelle aus.
2. Wählen Sie Delete (Löschen) und bestätigen Sie die Aktion.

Daten exportieren

Der Großteil der in der Cloud Migration AWS Factory-Lösung gespeicherten Daten kann in Excel-Dateien (.xlsx) exportiert werden. Sie können Daten auf Datensatztypenebene oder als vollständige Ausgabe aller Daten und Typen exportieren.

Um einen bestimmten Datensatztyp zu exportieren:

1. Gehen Sie zu der Tabelle, die Sie exportieren möchten.
2. Optional: Wählen Sie die Datensätze aus, die in eine Excel-Tabelle exportiert werden sollen. Wenn keine ausgewählt sind, werden alle Datensätze exportiert.
3. Wählen Sie das Exportsymbol in der oberen rechten Ecke des Datentabellenbildschirms.

Eine Excel-Datei mit dem Namen des Datensatztyps (z. B. `servers.xlsx`) wird in den Standard-Download-Speicherort des Browsers heruntergeladen.

Um alle Daten zu exportieren:

1. Gehen Sie zu Migration Management und wählen Sie Exportieren aus.
2. Markieren Sie Alle Daten herunterladen.

Eine Excel-Datei mit dem Namen `all-data.xlsx` wird in den Standard-Download-Speicherort des Browsers heruntergeladen. Diese Excel-Datei enthält eine Registerkarte pro Datensatztyp, und alle Datensätze für jeden Typ werden exportiert.

Importieren von -Daten

Die Cloud Migration Factory AWS on-Lösung bietet eine Datenimportfunktion, mit der einfache Datensatzstrukturen, z. B. eine Serverliste, in den Datenspeicher importiert werden können. Sie kann auch komplexere relationale Daten importieren, zum Beispiel könnte sie einen neuen Anwendungsdatensatz und mehrere Server in derselben Datei erstellen und sie in einer einzigen Importaufgabe miteinander verknüpfen. Auf diese Weise kann ein einziger Importvorgang für jeden Datentyp verwendet werden, der importiert werden muss. Beim Importvorgang werden die Daten anhand derselben Validierungsregeln validiert, die verwendet werden, wenn der Benutzer Daten auf der Benutzeroberfläche bearbeitet.

Eine Vorlage wird heruntergeladen

Um Vorlagen-Aufnahmeformulare vom Importbildschirm herunterzuladen, wählen Sie die gewünschte Vorlage aus der Aktionsliste aus. Die folgenden zwei Standardvorlagen sind verfügbar.

Vorlage mit nur erforderlichen Attributen — Diese enthält nur die als erforderlich markierten Attribute. Sie bietet den Mindestsatz an Attributen, der zum Importieren von Daten für alle Datensatztypen erforderlich ist.

Vorlage mit allen Attributen — Diese enthält alle Attribute im Schema. Diese Vorlage enthält zusätzliche Schema-Helfer-Informationen für jedes Attribut, um das Schema zu identifizieren, in dem es gefunden wurde. Diese Hilfspräfixe für die Spaltenüberschriften können bei Bedarf entfernt werden. Wenn sie während eines Imports beibehalten werden, werden die Werte in der Spalte nur in den jeweiligen Datensatztyp geladen und nicht für relationale Werte verwendet. Weitere Informationen finden Sie unter Helfer zum Importieren von Header-Schemas.

Eine Datei importieren

Importdateien können entweder im XLSX- oder CSV-Format erstellt werden. Für CSV muss es mit UTF8-Kodierung gespeichert werden, da die Datei sonst leer erscheint, wenn die Validierungstabelle vor dem Upload angezeigt wird.

Um eine Datei zu importieren:

1. Gehen Sie zu Migration Management und wählen Sie Import aus.

2. Wählen Sie Datei auswählen. Standardmäßig können Sie nur Dateien mit den .xlsx Erweiterungen .csv oder auswählen. Wenn die Datei erfolgreich gelesen wurde, werden der Dateiname und die Größe der Datei angezeigt.
3. Wählen Sie Weiter aus.
4. Der Bildschirm zur Überprüfung vor dem Upload zeigt das Ergebnis der Zuordnung der Header innerhalb der Datei zu Attributen innerhalb des Schemas und der Validierung der angegebenen Werte.
 - Die Zuordnungen der Spaltenüberschriften der Datei werden in den Spaltennamen der Tabelle auf dem Bildschirm angezeigt. Um zu überprüfen, welche Dateispaltenüberschrift zugeordnet wurde, wählen Sie den erweiterbaren Namen in der Kopfzeile aus, um weitere Informationen zur Zuordnung zu erhalten, einschließlich der ursprünglichen Dateiüberschrift und des Schemanamens, dem sie zugeordnet wurde. In der Spalte Validierung wird eine Warnung für alle Dateiüberschriften angezeigt, die nicht zugeordnet wurden oder wenn in mehreren Schemas doppelte Namen vorhanden sind.
 - Alle Header validieren die Werte für jede Zeile der Datei anhand der Anforderungen für das zugeordnete Attribut. Alle Warnungen oder Fehler im Dateiinhalte werden in der Spalte Validierung angezeigt.
5. Sobald keine Validierungsfehler mehr vorliegen, wählen Sie Weiter.
6. Der Schritt Daten hochladen zeigt eine Übersicht über die Änderungen, die nach dem Hochladen dieser Datei vorgenommen werden. Für jedes Element, bei dem beim Hochladen eine Änderung vorgenommen wird, können Sie unter dem jeweiligen Aktualisierungstyp die Option Details auswählen, um die Änderungen anzuzeigen, die vorgenommen werden.
7. Sobald die Überprüfung abgeschlossen ist, wählen Sie Hochladen aus, um diese Änderungen in die Live-Daten zu übernehmen.

Wenn der Upload erfolgreich war, wird oben im Formular eine Meldung angezeigt. Alle Fehler, die während des Uploads auftreten, werden unter Upload-Übersicht angezeigt.

Helfer zum Importieren von Header-Schemas

Standardmäßig sollten die Spaltenüberschriften in der Eingabedatei auf den Namen eines Attributs aus einem beliebigen Schema gesetzt sein. Der Importvorgang durchsucht alle Schemas und versucht, den Header-Namen einem Attribut zuzuordnen. Wenn ein Attribut in mehreren Schemas gefunden wird, wird eine Warnung angezeigt, insbesondere bei Beziehungsattributen, die in den meisten Fällen ignoriert werden können. Wenn Sie jedoch beabsichtigen, eine bestimmte Spalte einem bestimmten Schemaattribut zuzuordnen, können Sie dieses Verhalten außer Kraft setzen,

indem Sie der Spaltenüberschrift ein Schema-Helfer-Präfix voranstellen. Dieses Präfix hat das Format `[{schema name}]{attribute name}`, wobei `{schema name}` der Name des Schemas auf seinem Systemnamen (Wave, Anwendung, Server, Datenbank) basiert und der Systemname des Attributs im Schema `{attribute name}` ist. Wenn dieses Präfix vorhanden ist, werden alle Werte nur in Datensätze für dieses spezifische Schema eingetragen, auch wenn der Attributname in anderen Schemas vorhanden ist.

Wie in der folgenden Abbildung dargestellt, wurde der Überschrift in Spalte C ein Präfix vorangestellt `[database]`, sodass das Attribut dem `database_type` Attribut im Datenbankschema zugeordnet werden muss.

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

Header-Schema-Helfer importieren

Importformat für Attribute

Die folgende Tabelle enthält eine Anleitung zur Formatierung der Werte in einer Importdatei, um sie korrekt in die Cloud Migration Factory-Attribute zu importieren.

Typ	Unterstütztes Importformat	Beispiel
Zeichenfolge	Akzeptiert alphanumerische Zeichen und Sonderzeichen.	123456AbCd.!
Mehrwertige Zeichenfolge	Eine Liste vom Typ Zeichenfolge, getrennt durch ein Semikolon.	Item1;Item2;Item3
Passwort	Akzeptiert alphanumerische Zeichen und Sonderzeichen.	123456AbCd.!
Datum	MM/TT/JJJJ HH:mm	01/30/2023 10:00
Checkbox	Boolescher Wert in Form einer Zeichenfolge für ausgewählt und für nicht ausgewählt. TRUE FALSE	TRUE oder FALSE

Typ	Unterstütztes Importformat	Beispiel
Textbereich	Zeichenfolgentyp mit Unterstützung für Zeilenvorschübe und Zeilenumbrüche.	Test line1 oder Testline 2
Tag	Tags müssen so formatiert sein, dass key=value ; mehrere Tags durch ein Semikolon getrennt werden müssen.	TagKey1=Tagvalue1; TagKey2=tagvalue2;
Auflisten	Wenn Sie ein einzelnes Wertelistenattribut festlegen , verwenden Sie dieselbe Formatierung wie beim Typ „Zeichenfolge“, bei einer Mehrfachauswahlliste dann die Formatierung gemäß dem Typ „Zeichenfolge mit mehreren Werten“.	Selection1;Selecti on2;
Beziehung	Akzeptiert alphanumerische Zeichen und Sonderzeichen, die mit einem Wert übereinstimmen müssen, der auf dem in der Attributdefinition definierten Schlüssel basiert.	Application1

Verwaltung von Anmeldedaten

Die Cloud Migration Factory AWS on-Lösung verfügt über einen Credentials Manager, der in AWS Secrets Manager innerhalb des Kontos integriert ist, in dem die Instanz bereitgestellt wird. Mit dieser Funktion können Administratoren Systemanmeldedaten in AWS Secrets Manager speichern, um sie in Automatisierungsskripten zu verwenden, ohne Benutzern Zugriff zum direkten Abrufen der Anmeldeinformationen zu gewähren oder Benutzern Zugriff auf AWS Secrets Manager gewähren zu müssen. Benutzer können gespeicherte Anmeldeinformationen anhand ihres Namens und

ihrer Beschreibung auswählen, wenn sie sie für einen Automatisierungsjob bereitstellen. Der Automatisierungsjob ruft dann nur die Anmeldeinformationen ab, die bei der Ausführung auf dem Automatisierungsserver angefordert wurden. Zu diesem Zeitpunkt wird die der EC2-Instance zugewiesene IAM-Rolle für den Zugriff auf die erforderlichen Geheimnisse verwendet.

Der Credentials Manager-Administrationsbereich ist nur für Benutzer sichtbar, die Mitglieder der Administratorgruppe in Amazon Cognito sind. Benutzer ohne Administratorrechte können die Namen und Beschreibungen ihrer Anmeldeinformationen nur einsehen, wenn sie über eine Automatisierung oder eine andere Datensatzbeziehung referenziert werden.

Die folgenden drei Geheimtypen können in AWS Secrets Manager über Credentials Manager gespeichert werden.

Betriebssystemanmeldedaten — In der Form von, `username` und `password`.

Geheimer Schlüssel/Wert — In der Form eines `key` und `value`

Klartext — In Form einer einzigen Klartext-Zeichenfolge.

Füge ein Geheimnis hinzu

1. Wählen Sie in der Liste Credential Manager Secrets die Option Hinzufügen aus.
2. Wählen Sie den Geheimtyp aus, den Sie hinzufügen möchten.
3. Geben Sie einen geheimen Namen ein. Dies ist derselbe Name, der im AWS Secrets Manager für den geheimen Namen angezeigt wird.
4. Geben Sie eine geheime Beschreibung ein. Dies ist dieselbe Beschreibung, die im AWS Secrets Manager für die geheime Beschreibung angezeigt wird.
5. Geben Sie die Anmeldeinformationen für den Geheimtyp ein.

Note

Für den geheimen Typ OS Credentials gibt es eine Option zur Auswahl des Betriebssystemtyps, auf den in benutzerdefinierten Skripten verwiesen werden kann.

Bearbeiten Sie ein Geheimnis

Mit Ausnahme des Geheimnamens und -typs können Sie alle Eigenschaften des Geheimnisses über die Credentials Manager-Benutzeroberfläche bearbeiten.

Löschen eines Secrets

Wählen Sie in der Credentials Manager-Ansicht das Geheimnis aus, das Sie löschen möchten, und klicken Sie auf Löschen. Die Löschung des Secrets wird in AWS Secrets Manager geplant, was einige Minuten dauern kann. Jeder Versuch, während dieser Zeit ein neues Geheimnis mit demselben Namen hinzuzufügen, schlägt fehl.

Führen Sie die Automatisierung von der Konsole aus aus

Die Cloud Migration Factory AWS on-Lösung bietet eine Automatisierungs-Engine, mit der Benutzer Jobs in Form von Skripten anhand des Inventars im Datenspeicher ausführen können. Mit dieser Funktion können Sie alle Automatisierungen verwalten, anpassen und bereitstellen, die für den Abschluss der end-to-end Migrationsaktivitäten erforderlich sind.


Von AWS CMF initiierte Jobs werden auf Automatisierungsservern ausgeführt, die vor Ort AWS Cloud oder vor Ort gehostet werden können. Auf diesen Servern muss Windows mit installiertem AWS SSM-Agent sowie Python und Microsoft PowerShell ausgeführt werden. Sie können auch andere Frameworks installieren, falls dies für benutzerdefinierte Automatisierungen erforderlich ist. Weitere Informationen finden Sie in [Schritt 6. Einzelheiten zum Build des Automatisierungsservers](#) [finden Sie beim Erstellen eines Migrationsautomatisierungsservers](#). Für die Ausführung von Jobs über die AWS CMF-Konsole ist mindestens ein Automatisierungsserver erforderlich.

Bei der Bereitstellung können Sie Skripts für die häufigsten Aufgaben verwenden, die zum Rehosten von Workloads mithilfe von MGN erforderlich sind. AWS Laden Sie die Skripts von der Weboberfläche herunter und verwenden Sie sie als Ausgangspunkt für benutzerdefinierte Skripts. Einzelheiten zur Erstellung von benutzerdefinierten Automatisierungsskripten finden Sie unter [Verwaltung von Skripten](#).

Um einen Job von der Konsole aus zu initiieren, wählen Sie eine Welle aus, für die die Automatisierung ausgeführt werden soll, wählen Sie dann Aktionen und dann Automatisierung ausführen aus. Sie können auch einen Job auswählen, für den die Automatisierung ausgeführt werden soll, dann Aktionen und dann Automatisierung ausführen auswählen.


Aus der Option „Automatisierung ausführen“:

1. Geben Sie den Jobnamen ein. Dies wird verwendet, um den Job im Protokoll zu identifizieren.

 Note

Jobnamen müssen nicht eindeutig sein, da allen Jobs auch eine eindeutige ID und Zeitstempel zugewiesen werden, um sie weiter zu identifizieren.

2. Wählen Sie den Skriptnamen aus der Liste aus. Dies ist eine Liste aller Skripten, die in die AWS CMF-Instanz geladen wurden. Wenn der Job gesendet wird, wird die Standardversion des ausgewählten Skripts ausgeführt. Um die Details des Skripts, einschließlich der aktuellen Standardversion, zu überprüfen, wählen Sie unter dem Skriptnamen die Option Verwandte Details aus. Einzelheiten zur Aktualisierung der Standardversion von Skripten finden Sie unter Standardversion des Skriptpakets ändern. Wenn Sie das auszuführende Skript auswählen, werden die erforderlichen Parameter unter Skriptargumente angezeigt.
3. Wählen Sie aus der Instanz-ID den Automatisierungsserver für den Job aus der Liste aus.

 Note

In der Liste werden nur Instanzen angezeigt, auf denen der SSM-Agent installiert ist und bei denen entweder die EC2-Instance oder bei nicht auf EC2 gehosteten Automatisierungsservern das Managed Instance-Tag von `role` gesetzt ist. `mf_automation`

4. Geben Sie im Feld Skriptargumente die erforderlichen Eingabeargumente für das Skript ein.
5. Nachdem Sie alle erforderlichen Parameter eingegeben und überprüft haben, wählen Sie Automationsjob einreichen.

Wenn Sie den Automatisierungsjob einreichen, wird der folgende Prozess eingeleitet:

1. In der AWS Cloud Migration Factory-Ansicht „Jobs“ wird ein Auftragsdatensatz erstellt, der die Details des Jobs und den aktuellen Status enthält.
2. Ein AWS Systems Manager Manager-Automatisierungsjob wird erstellt und beginnt mit der Ausführung des SSM-Automatisierungsdokuments von AWS Cloud Migration

Factory auf dem Automatisierungsserver, der über die Instanz-ID bereitgestellt wird. Das Automatisierungsdokument:

- a. Lädt die aktuelle Standardversion des Skriptpakets aus dem AWS Cloud Migration Factory S3-Bucket auf den Automatisierungsserver in das `C:\migration\scripts` Verzeichnis herunter.
 - b. Entpackt und verifiziert das Paket.
 - c. Startet das Python-Skript für die Masterdatei, das in der ZIP-Datei `package-structure.yml` enthalten ist.
3. Sobald das Python-Skript für die Masterdatei gestartet wurde, wird jede Ausgabe des Skripts vom SSM-Agenten erfasst und in dieses CloudWatch eingespeist. Es wird dann regelmäßig erfasst und zusammen mit dem ursprünglichen Auftragsdatensatz im AWS Cloud Migration Factory-Datenspeicher gespeichert, sodass eine vollständige Prüfung des ausgeführten Jobs möglich ist.
- a. Wenn das Skript Anmeldeinformationen für AWS Cloud Migration Factory benötigt, kontaktiert das Skript AWS Secrets Manager, um die Anmeldeinformationen für das Dienstkonto zu erhalten. Wenn die Anmeldeinformationen falsch oder nicht vorhanden sind, gibt das Skript einen Fehler zurück.
 - b. Wenn das Skript auf andere Secrets zugreifen muss, die mit der AWS Cloud Migration Factory Credentials Manager-Funktion gespeichert wurden, kontaktiert es AWS Secrets Manager, um auf diese Anmeldeinformationen zuzugreifen. Wenn dies nicht möglich ist, gibt das Skript einen Fehler zurück.
4. Sobald das Python-Skript der Masterdatei beendet ist, bestimmt das Ergebnis dieses Skripts den Status, der dem AWS Cloud Migration Factory-Jobdatensatz zugewiesen wird. Ein Rückgabewert ungleich Null wird auf `gesetztJob Status. Failed`

Note

Wenn bei der ersten Ausführung des AWS SSM-Dokuments ein Fehler auftritt, wird dieser derzeit nicht in der Weboberfläche angezeigt. Fehler werden erst protokolliert, wenn die Masterdatei Python gestartet wird.

Bei allen Jobs, die von der Konsole aus initiiert wurden, wird nach 12 Stunden ein Timeout erreicht, wenn sie nicht den Status „Erfolg“ oder „Fehler“ zurückgegeben haben.

Führen Sie Automatisierungen von der Befehlszeile aus

Wir empfehlen zwar, Automatisierungsjobs über die Weboberfläche auszuführen, Sie können Automatisierungsskripts jedoch manuell über eine Befehlszeile auf dem Automatisierungsserver ausführen. Dies bietet zusätzliche Optionen, wenn Unternehmen die Kombination aus AWS CMF Credentials Manager, AWS Secrets Manager und AWS Systems Manager nicht in der Umgebung verwenden können oder wollen oder wenn AWS Benutzer von Cloud Migration Factory on einmalige Zugangscodes für die Multi-Faktor-Authentifizierung (MFA) bereitstellen müssen, um sich bei Cloud Migration Factory anzumelden. AWS

Wenn Skripts über die Befehlszeile ausgeführt werden, sind der Jobverlauf und die Protokolle in der Job-Ansicht der Weboberfläche nicht verfügbar. Die Protokollausgabe wird nur an die Befehlszeilenausgabe weitergeleitet. Die Skripts können weiterhin über AWS APIs auf die Cloud Migration Factory zugreifen, um Datensätze zu lesen und zu aktualisieren, sowie auf andere Funktionen, die über die APIs verfügbar sind.

Wir empfehlen, Skripts in der Skriptbibliothek oder an einem anderen zentralen Ort zu speichern, um sicherzustellen, dass Sie auf die neueste Version des Skripts zugreifen und diese verwenden, oder die Version, deren Verwendung derzeit genehmigt ist.

Manuelles Ausführen eines Automatisierungspakets

In diesem Abschnitt werden die Schritte beschrieben, um ein Paket von Cloud Migration Factory herunterzuladen AWS und es manuell auf dem Automatisierungsserver auszuführen. Sie können den Vorgang auch für andere Skriptquellenspeicherorte verfolgen, indem Sie die Schritte 1 und 2 durch die quellenspezifischen Download-Schritte ersetzen.

1. Wenn Skripts in Cloud Migration Factory on gespeichert sind AWS, folgen Sie den Schritten unter [Skriptpakete herunterladen](#), um die ZIP-Datei für das Automatisierungspaket zu erhalten.
2. Kopieren Sie die ZIP-Datei an einen Speicherort auf dem Automatisierungsserver, z. B. c : \migrations\scripts, und entpacken Sie den Inhalt.
3. Kopieren Sie die `FactoryEndpoints.json` Datei in jeden der entpackten Skriptordner. Konfigurieren Sie die Datei mit den spezifischen API-Endpunkten für die Cloud Migration Factory-Instanz, die die Server oder andere Datensätze enthält, auf die dieser Automatisierungsjob verweist. Weitere Informationen zur [Erstellung dieser Datei finden Sie unter Erstellung der FactoryEndpoints.json-Datei](#).
4. Stellen Sie in der Befehlszeile sicher, dass Sie sich im Stammverzeichnis des entpackten Pakets befinden, und führen Sie den folgenden Befehl aus:

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

Paket-Master-Skriptdatei — diese finden Sie `Package-Structure.yml` unter dem `MasterFileName` Schlüssel.

Skriptargumente — Informationen zu den Argumenten finden Sie `Package-Structure.yml` unter dem `Arguments` Schlüssel.

5. Die Skripts fordern Anmeldeinformationen an, die für Cloud Migration Factory auf AWS APIs und dem Remoteserver erforderlich sind. Alle manuell eingegebenen Anmeldeinformationen werden für die Dauer dieses Vorgangs im Speicher zwischengespeichert, um zu vermeiden, dass dieselben Anmeldeinformationen erneut eingegeben werden. Wenn Sie Skriptargumente eingeben, um auf Secrets zuzugreifen, die mit der Credentials Manager-Funktion gespeichert wurden, ist Zugriff auf AWS Secrets Manager und die zugehörigen Secrets erforderlich. Wenn das Abrufen von Geheimnissen aus irgendeinem Grund fehlschlägt, fordert das Skript zur Eingabe von Benutzeranmeldedaten auf.

Erstellung der Datei `.json FactoryEndpoints`

Wir empfehlen, diese Datei einmal bei der Bereitstellung der Cloud Migration Factory auf der AWS-Lösung zu erstellen, da sich der Inhalt nach der ersten Bereitstellung nicht ändert und an einem zentralen Ort auf dem Automatisierungsserver gespeichert wird. Diese Datei enthält die Automatisierungsskripte mit der Cloud Migration Factory auf AWS-API-Endpunkten und anderen wichtigen Parametern. Ein Beispiel für den Standardinhalt der Datei finden Sie hier:

```
{
  "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

Die meisten Informationen, die zum Erstellen dieser Datei für eine bereitgestellte AWS Cloud Migration Factory-Instanz erforderlich sind, sind auf der Registerkarte AWS CloudFormation Outputs des bereitgestellten Stacks verfügbar, mit Ausnahme von `UserPoolClientId`. Ermitteln Sie diesen Wert, indem Sie die folgenden Schritte ausführen:

1. Navigieren Sie zur Amazon-Cognito-Konsole.
2. Öffnen Sie die Benutzerpool-Konfiguration.
3. Wählen Sie App-Integration aus, um die App-Client-Konfiguration bereitzustellen.

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

Ersetzen Sie `< LoginApi -value>`, `< UserApi -value>`, und `< UserPoolId -value>` `<Region-value>` durch die entsprechenden Werte, die Sie aus der Outputs-Konsole abgerufen haben. AWS CloudFormation Fügen Sie am Ende der URLs keinen Schrägstrich (/) hinzu.

Die Datei hat einen optionalen `DefaultUser` Schlüssel. Sie können den Wert für diesen Schlüssel auf die Standardbenutzer-ID festlegen, die für den Zugriff auf die Cloud Migration Factory verwendet wird, AWS um zu vermeiden, dass Sie ihn jedes Mal eingeben müssen. Wenn Sie zur Eingabe der Cloud Migration Factory-Benutzer-ID aufgefordert werden, können Sie entweder eine Benutzer-ID eingeben oder den Standardwert verwenden, indem Sie die Eingabetaste drücken. Dies ist nur möglich, wenn die Skripts manuell ausgeführt werden.

Starten Sie AWS MGN-Jobs von Cloud Migration Factory aus

Die Cloud Migration Factory AWS on-Lösung verfügt über eine integrierte Automatisierung zur Initiierung und Verwaltung der Rehost-Migration mithilfe von AWS MGN. Diese Automatisierungen ermöglichen es Migrationsteams, alle Aspekte ihrer Migration von einer einzigen Benutzeroberfläche aus zu verwalten. Dabei werden die wichtigsten Aktionen, die in der AWS MGN-Servicekonsole

verfügbar sind, mit der AWS Cloud Migration Factory-Automatisierungsbibliothek kombiniert, die die Funktionalität um vorgefertigte Skripte für Massenmigrationen erweitert, was dazu beiträgt, die Geschwindigkeit der Migrationsaktivitäten zu erhöhen. Eine vollständige Liste der verfügbaren MGN-Automatisierungsjobs finden Sie in der Liste der automatisierten Migrationsaktivitäten für den AWS Application Migration Service (AWSMGN). Die Verwendung von AWS Cloud Migration Factory ermöglicht auch nahtlose Migrationen mehrerer Konten mithilfe von AWS MGN, da die Cloud Migration Factory automatisch Rollen in verschiedenen Zielkonten übernehmen kann, basierend auf den zu migrierenden Cloud Migration Factory-Anwendungs- und Serverdefinitionen.

Erforderliche Aktivitäten

1. Für jedes Zielkonto wurde AWS CMF für jedes Zielkonto CloudFormation bereitgestellt. Weitere Informationen finden Sie im Abschnitt [AWS CloudFormationVorlagen](#) in diesem Dokument.
2. [AWSMGN wird in jedem Zielkonto initialisiert.](#)

Ursprüngliche Definition

Die Definition des lokalen Inventars erfolgt durch die Erstellung von Wellen-, Anwendungs- und Serverelementen entweder über die Benutzeroberfläche oder durch den Import eines CSV-Eingabeformulars. Diese Definitionen werden verwendet, um die Serveridentitäten vor Ort sowie die EC2-Zielparameter sowie andere für die Verwaltung der Migrationsaktivität erforderliche Daten bereitzustellen.

Definition der Benutzeroberfläche

Um die AWS MGN-Funktionalität nutzen zu können, müssen Sie einen Wave-Record mit zugehörigen Anwendungsdatensätzen und schließlich einen oder mehrere Serverdatensätze erstellen, die den Anwendungen zugeordnet sind. Der Wave-Record wird zur Gruppierung der Anwendungen verwendet und stellt keine Parameter für die Automatisierung bereit, wohingegen der Anwendungsdatensatz die AWS-Konto Ziel-ID definiert und zu der AWS-Region die Anwendung migriert wird. Die Serverdatensätze enthalten die Automatisierungsaktionen und die AWS MGN-Integration die Zielparameter für die EC2-Instances, wie Instance-Typ, Subnetze, Sicherheitsgruppen usw.

Bei der Definition eines Servers im AWS CMF-Datenspeicher für die Verwendung mit der AWS MGN-Funktionalität muss der Server mit der Migrationsstrategie Rehost konfiguriert werden. Sobald Rehost ausgewählt ist, werden die zusätzlichen Attribute, die für diese Funktionalität erforderlich sind, auf

dem Bildschirm angezeigt. Die folgenden Attribute müssen ausgefüllt werden, um einen AWS MGN-Migrationsauftrag erfolgreich zu initiieren:

Erforderlich

Server-Betriebssystemfamilie — Je nach Betriebssystemfamilie entweder auf Linux oder Windows eingestellt.

Serverbetriebssystemversion — Wählen Sie die detaillierte Betriebssystemversion aus, die auf dem Server ausgeführt wird.

Instanztyp — Der zu verwendende EC2-Instance-Typ.

Tenancy — Shared Hosting, dedizierter Host.

Sicherheitsgruppen-IDs — Liste der Sicherheitsgruppen, die der Instance zugewiesen werden, wenn die endgültige Umstellung eingeleitet wird.

Sicherheitsgruppen-IDs — Test — Liste der Sicherheitsgruppen, die der Instance zugewiesen werden, wenn der Test gestartet wird.

Bedingt

Subnetz-Ids — Subnetz-ID, der diese EC2-Instance zugewiesen werden soll, wenn die endgültige Umstellung eingeleitet wird. (gilt nicht, wenn die Netzwerkschnittstellen-ID angegeben wurde)

Subnetzkennungen — Test — Subnetz-ID, der diese EC2-Instance zugewiesen werden soll, wenn der Test gestartet wird. (Gilt nicht, wenn Netzwerkschnittstellen-ID-Test angegeben ist)

Netzwerkschnittstellen-ID — ENI-ID, die verwendet werden soll, wenn die endgültige Umstellung eingeleitet wird.

Netzwerkschnittstellen-ID — Test — ENI-ID, die verwendet werden soll, wenn der Test eingeleitet wird.

Dedizierte Host-ID — Dedizierte Host-ID, auf der die Instance gestartet wird. (gilt nur, wenn Tenancy auf Dedicated Host gesetzt ist).

Optional

Tags — EC2-Instance-Tags, die auf die Instance angewendet werden sollen.

Alle anderen hier nicht aufgeführten Attribute haben keinen Einfluss auf die AWS MGN-Jobs, die von der AWS CMF-Lösung aus initiiert wurden.

Definition des Aufnahmeformulars

Eingabeformulare können die Details zum Erstellen oder Aktualisieren mehrerer Arten von Datensätzen mit dem Datenspeicher in einer einzigen Zeile der CSV-Datei enthalten. Dadurch wird der Import verwandter Daten ermöglicht. Im folgenden Beispiel werden die Wave-, Anwendungs- und Serverdatensätze während des Imports automatisch erstellt und miteinander verknüpft.

Um das Aufnahmeformular zu importieren, gehen Sie genauso vor wie bei anderen Datenimporten in die Cloud Migration Factory. Die AWS Lösung wird unter [Daten importieren beschrieben](#).

Einen Job initiieren

Das Initiieren eines AWS MGN-Jobs von AWS CMF aus erfolgt anhand einer Welle. Wählen Sie in der Wave-Listenansicht die Welle aus, und wählen Sie dann unter Aktionen Rehost > MGN aus.

In diesem Bildschirm muss der Benutzer die folgenden Optionen treffen, bevor er den Job einreichen kann.

1. Wählen Sie die AWS MGN-Aktion aus, die für die Anwendungen und Server in der Welle ausgeführt werden soll. Diese Aktionen entsprechen größtenteils denen, die in der AWS MGN-Servicekonsole und der API verfügbar sind, mit Ausnahme von Validate Launch Template (Einzelheiten zu dieser Aktion finden Sie weiter unten). Einzelheiten zu den Auswirkungen der einzelnen Aktionen finden Sie im AWS MGN-Benutzerhandbuch.
2. Wählen Sie die Welle aus, gegen die die Aktion ausgeführt werden soll.
3. Wählen Sie die Anwendungen aus der Welle aus, für die die Aktion ausgeführt werden soll. In dieser Liste werden nur Anwendungen angezeigt, die mit der ausgewählten Welle verknüpft sind.
4. Sobald alle Optionen korrekt sind, wählen Sie Senden aus.

Die Automatisierung initiiert nun die ausgewählte Aktion für das Ziel jeder ausgewählten Anwendung AWS-Konto, wie im Anwendungsdatensatz angegeben. Die Ergebnisse der Aktion werden in der Benachrichtigung angezeigt, einschließlich aller Fehler.

Überprüfen Sie die Startvorlage

Diese Aktion wird verwendet, um zu überprüfen, ob die in CMF für jeden Server gespeicherten Konfigurationsdaten gültig sind, bevor eine Übernahme versucht wird. Um diese Aktion ausführen zu können, müssen Sie die AWS MGN-Agenten erfolgreich auf dem Quellserver bereitgestellt haben.

Die für jeden Server durchgeführten Validierungen sind:

- Stellen Sie sicher, dass der Instanztyp gültig ist.
- Stellen Sie sicher, dass das IAM-Instanzprofil existiert.
- Sicherheitsgruppen existieren sowohl für Test- als auch für Live-Anwendungen.
- Subnetze existieren sowohl für Test- als auch für Live-Übertragungen (sofern ENI nicht angegeben ist).
- Ein dedizierter Host ist vorhanden (falls angegeben).
 - Wenn ein dedizierter Host angegeben ist, werden die folgenden Prüfungen durchgeführt:
 - Unterstützt der dedizierte Host den angegebenen Instance-Typ?
 - Verfügt der dedizierte Host über freie Kapazität für alle Anforderungen dieser Welle, basierend auf den erforderlichen Instance-Typen?
- ENI ist vorhanden (falls angegeben).

Die Ergebnisse der Aktion werden in der Benachrichtigung angezeigt, einschließlich aller Fehler.

Umstellung auf EC2

Die Cloud Migration Factory AWS On-Lösung ermöglicht den automatischen Start von Gruppen von EC2-Instances anhand von Konfigurationen, die im Datenspeicher definiert sind. Dabei werden EC2-Instances mit angeschlossenen EBS-Volumes bereitgestellt. Dies bietet die Möglichkeit, neue EC2-Instances bereitzustellen, sodass über AWS CloudFormation eine einzige CMF-Benutzeroberfläche lokale Server mit MGN auf Replatform und Rehost umgestellt werden können. AWS Bevor Sie diese Funktion verwenden können, muss der Datenspeicher die Definition der Server enthalten. Sobald dies behoben ist, sollten die Server mit einer Welle verbunden werden. Wenn die Entscheidung getroffen wurde, die EC2-Instances zu starten, kann der Benutzer die folgenden Aktionen gegen die Welle einleiten:

- Validierung der EC2-Eingabe
- EC2 Generieren Sie eine CF-Vorlage
- EC2-Bereitstellung

Voraussetzungen

Berechtigungen zum Hinzufügen des Replatform-Attributzugriffs.

Anfängliche Konfiguration

Die Konfiguration der neuen EC2-Instances erfolgt durch die Erstellung neuer Serverelemente entweder über die Benutzeroberfläche oder durch den Import eines CSV-Eingabefelds, das die Serverelemente enthält. Diese Definitionen werden in AWS Cloud Formation-Vorlagen konvertiert, die in einem S3-Bucket gespeichert werden, in dem AWS-Konto die AWS CMF-Instanz bereitgestellt wird.

Definition der Benutzeroberfläche

Bei der Definition eines Servers im AWS Cloud Migration Factory-Datenspeicher zur Verwendung mit der Replatform to EC2-Funktionalität muss der Server mit der Migrationsstrategie Replatform konfiguriert werden. Sobald Replatform ausgewählt ist, werden die zusätzlichen Attribute, die für diese Funktion erforderlich sind, auf dem Bildschirm angezeigt. Die folgenden Attribute müssen ausgefüllt werden, damit die Funktionalität funktioniert:

Erforderliche Attribute

AMI-ID — ID des Amazon Machine Image, das zum Starten der EC2-Instance verwendet wurde.

Availability Zone — AZ, in der die EC2-Instance bereitgestellt wird.

Größe des Root-Volumes — Größe des Root-Volumes für die Instance in GB.

Instance-Typ — Der zu verwendende EC2-Instance-Typ.

Sicherheitsgruppen-IDs — Liste der Sicherheitsgruppen, die der Instance zugewiesen sind.

Subnetz-Ids — Subnetz-ID, der diese EC2-Instance zugewiesen werden soll.

Tenancy — Derzeit ist Shared die einzige unterstützte Option für die Integration von Replatform to EC2. Jede andere Option wird bei der Generierung der Vorlage durch Shared ersetzt.

Optionale Attribute

Detaillierte Überwachung aktivieren — Aktivieren Sie diese Option, um die detaillierte Überwachung zu aktivieren.

Zusätzliche Datenträgernamen — Liste zusätzlicher EBS-Volumennamen. Jedes Element in der Liste muss derselben Zeile zugeordnet werden wie die Listen Größe und Typ.

Zusätzliche Volumengrößen — Liste zusätzlicher EBS-Volumengrößen. Jedes Element in der Liste muss derselben Zeile zugeordnet werden wie die Listen „Namen“ und „Typ“.

Zusätzliche Volume-Typen — Liste zusätzlicher EBS-Volume-Typen. Jedes Element in der Liste muss derselben Zeile wie die Namen - und Größenlisten zugeordnet sein. Wenn nichts angegeben ist, wird standardmäßig gp2 für alle Volumes verwendet.

EBS KMS-Schlüssel-ID für Volumenverschlüsselung — Wenn EBS-Volumes verschlüsselt werden sollen, geben Sie die Schlüssel-ID, den Schlüssel-ARN, den Schlüsselalias oder den Alias-ARN an.

EBS-optimiert aktivieren — Wählen Sie diese Option, um EBS Optimized zu aktivieren.

Name des Root-Volumes — Wählen Sie eine der verfügbaren Optionen aus. Falls nicht angegeben, wird die ID verwendet.

Root-Volume-Typ — Geben Sie den EBS-Typ des zu erstellenden Volumes an. Falls nicht angegeben, wird standardmäßig gp2 verwendet.

Definition des Aufnahmeformulars

Eingabeformulare können die Details zum Erstellen oder Aktualisieren mehrerer Arten von Datensätzen mit dem Datenspeicher in einer einzigen Zeile der CSV-Datei enthalten. Dadurch wird der Import verwandter Daten ermöglicht. Im folgenden Beispiel werden die Wave-, Anwendungs- und Serverdatensätze während des Imports automatisch erstellt und miteinander verknüpft.

Beispiel: Aufnahmeformular

Spaltenname	Beispieldaten	Erforderlich	Hinweise
wave_name	Welle1	Ja	
app_name	App 1	Ja	
aws_Konto-ID	1234567890	Ja	
Servername	Server1	Ja	
Server_FQDN	Server 1	Ja	
Server_Betriebssystemfamilie	linux	Ja	
Server_Betriebssystemversion	Amazon	Ja	

Spaltenname	Beispieldaten	Erforderlich	Hinweise
Serverebene	Web	Nein	
Serverumgebung	Entwickler	Nein	
Subnetz-IDs	subnetz-xxxxxxx	Ja	
Sicherheitsgruppen-IDs	sg-yyyyyyyyyyyyy	Ja	
instanceType	m5.large	Ja	
Ich bin Role	benutzerdefinierte ec2-Rolle	Nein	
tenancy	Freigegeben	Ja	
r_typ	Wechsel der Plattform	Ja	
root_vol_size	50	Ja	
ami_id	ami-zzzzzzzzzz	Ja	
Verfügbarkeitszone	us-west-2a	Ja	
root_vol_type	gp2	Nein	
add_vols_size	40:100	Nein	
vols_type hinzufügen	gp2: gp3	Nein	
ebs_optimized	false	Nein	
ebs_kms-Schlüssel-ID	1111-1111-1111-1111	Nein	
detaillierte_Überwachung	true	Nein	
Name der Stammdatei	Server1_Root-Volume	Nein	

Spaltenname	Beispieldaten	Erforderlich	Hinweise
vols_name hinzufügen	server1_root_volume A: server1_root_volum e B	Nein	

Um das Aufnahmeformular zu importieren, gehen Sie genauso vor wie bei allen anderen Datenimporten in die Cloud Migration Factory auf Lösung. AWS

Maßnahmen zur Bereitstellung

Validierung der EC2-Eingabe

Nachdem Sie die Instanzparameter definiert haben, müssen Sie zuerst die Wave-Aktion ausführen: Replatform > EC2 > EC2-Eingabevalidierung. Diese Aktion überprüft, ob alle richtigen Parameter für jeden Server angegeben wurden, um eine gültige Vorlage zu erstellen. CloudFormation

Note

Bei dieser Überprüfung wird derzeit nicht überprüft, ob die Eingabeparameter gültig sind, sondern nur, ob sie in jeder Serverdefinition vorhanden sind. Sie müssen die korrekten Werte überprüfen, bevor Sie die Vorlage erstellen. Andernfalls schlägt die Bereitstellung der Vorlage fehl.

EC2: Vorlage generieren CloudFormation

Sobald die Definitionen für alle in einer Welle enthaltenen Server überprüft wurden, kann die CloudFormation Vorlage generiert werden. Führen Sie dazu die folgende Wave-Aktion aus: Replatform > EC2 > EC2 Generate CF Template. Diese Aktion erstellt eine CloudFormation Vorlage für jede Anwendung in der Welle, wobei die Server in der Anwendung die Migrationsstrategie Replatform verwenden. Server, für die andere Migrationsstrategien definiert wurden, werden nicht in die Vorlage aufgenommen.

Nach der Ausführung werden die Vorlagen für jede Anwendung im S3-Bucket gespeichert: [instanzspezifisches Präfix] -gfbuild-cftemplates, der bei der Bereitstellung der Cloud Migration Factory On-Lösung automatisch erstellt wurde. AWS Die Ordnerstruktur dieses Buckets sieht wie folgt aus:

- [AWSZielkonto-ID]
 - [Wellenname]
 - CFN_Template_ [Anwendungs-ID] _ [Anwendungsname] .yaml

Jedes Mal, wenn die Generierungsaktion ausgeführt wird, wird eine neue Version der Vorlage im S3-Bucket gespeichert. Die S3-URIs für die Vorlagen werden in der Benachrichtigung bereitgestellt. Diese Vorlagen können vor der Bereitstellung nach Bedarf überprüft oder bearbeitet werden.

Die CloudFormation Vorlagen generieren derzeit die folgenden CloudFormation Ressourcentypen:

- AWS: :EC2: :Instanz
- AWS: :EC2: :Volumen
- AWS: :EC2:: VolumeAttachment

Bereitstellung von EC2

Sobald Sie bereit sind, die neuen EC2-Instances bereitzustellen, können Sie die EC2-Bereitstellungsaktion initiieren, die über die Wellenaktion Replatform > EC2 > EC2 Deployment initiiert werden kann. Diese Aktion verwendet die neueste Version der CloudFormation Vorlage für jede Anwendung in der Welle und stellt diese Vorlagen in den ausgewählten Zielkonten über bereit. AWS CloudFormation

Verwaltung von Skripten

Die Cloud Migration Factory AWS on-Lösung ermöglicht es Benutzern, die Bibliothek mit Automatisierungsskripten oder Paketen innerhalb der Benutzeroberfläche vollständig zu verwalten. Sie können neue benutzerdefinierte Skripts sowie neue Versionen des Skripts über die Skriptverwaltungsoberfläche hochladen. Wenn mehrere Versionen verfügbar sind, kann ein Administrator zwischen diesen Versionen wechseln und so Updates testen, bevor sie als Standard festgelegt werden. Über die Skriptverwaltungsoberfläche können Administratoren auch Skriptpakete herunterladen, um den Inhalt zu aktualisieren oder zu überprüfen.

Ein unterstütztes Skriptpaket ist ein komprimiertes ZIP-Archiv, das die folgenden obligatorischen Dateien im Stammverzeichnis enthält:

- `Package-structure.yml` — Wird verwendet, um die Argumente des Skripts und andere Metadaten wie Beschreibung und Standardname zu definieren. Weitere Informationen finden Sie unter [Ein neues Skriptpaket erstellen](#).
- `[benutzerdefiniertes Python-Skript] .py` — Dies ist das erste Skript, das ausgeführt wird, wenn ein Job eingereicht wird. Dieses Skript kann andere Skripte und Module aufrufen, und wenn ja, sollten diese im Archiv enthalten sein. Der Name dieses Skripts muss mit dem Wert übereinstimmen, der im `MasterFileName` Schlüssel in der angegeben ist `Package-Structure.yml`.

Laden Sie ein neues Skriptpaket hoch

Note

Ein Skriptpaket muss dem unterstützten Format entsprechen. Weitere Informationen finden Sie unter [Ein neues Skriptpaket erstellen](#).

1. Wählen Sie in der Tabelle Automatisierungsskripten die Option Hinzufügen aus.
2. Wählen Sie die Paket-Archivdatei aus, die Sie hochladen möchten.
3. Geben Sie einen eindeutigen Namen für das Skript ein. Benutzer referenzieren das Skript mit diesem Namen, um Jobs zu initiieren.

Laden Sie Skriptpakete herunter

Sie können Skriptpakete von der Konsole herunterladen, um Updates und die Inhaltsüberprüfung zu aktivieren.

1. Wählen Sie Automatisierung und dann Skripte aus.
2. Wählen Sie das Skript, das Sie herunterladen möchten, aus der Tabelle aus, wählen Sie dann Aktionen aus und wählen Sie Standardversion herunterladen oder Neueste Version herunterladen aus.

Sie können bestimmte Versionen eines Skripts herunterladen. Wählen Sie dazu das Skript, dann Aktionen und dann Standardversion ändern aus. Wählen Sie in der Liste „Standardversion des Skripts“ die Option Ausgewählte Version herunterladen aus.

Neue Version eines Skriptpakets hinzufügen

Updates für AWS Cloud Migration Factory-Skriptpakete können im Abschnitt Automatisierung > Skripts hochgeladen werden, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie Automatisierung und dann Skripte aus.
2. Wählen Sie das vorhandene Skript aus, um eine neue Version hinzuzufügen, wählen Sie dann Aktionen und dann Neue Version hinzufügen aus.
3. Wählen Sie die aktualisierte Paket-Archivdatei aus, die Sie hochladen möchten, und klicken Sie auf Weiter. Die neue Skriptversion behält standardmäßig den vorhandenen Namen bei. Geben Sie einen eindeutigen Skriptnamen ein. Jede Namensänderung wird nur auf diese Version des Skripts angewendet.
4. Sie können die neue Version des Skripts zur Standardversion machen, indem Sie Als Standardversion festlegen auswählen.
5. Klicken Sie auf Hochladen.

Löschen von Skriptpaketen und Versionen

Sie können Skripts oder Versionen eines Skripts nicht zu Prüfungszwecken löschen. Auf diese Weise können Sie genau das Skript überprüfen, das zu einem bestimmten Zeitpunkt auf einem System ausgeführt wurde. Jede Skriptversion hat beim Hochladen eine eindeutige Signatur und ID, die anhand des Auftragsverlaufs aufgezeichnet wird, in dem das Skript und die Version verwendet wurden.

Ein neues Skriptpaket zusammenstellen

Cloud Migration Factory auf AWS Skriptpaketen unterstützt Python als primäre Skriptsprache. Sie können andere Shell-Skriptsprachen nach Bedarf aus einem Python-Hauptprogramm oder einem Python-Wrapper heraus initiieren. Um schnell ein neues Skriptpaket zu erstellen, empfehlen wir, eine Kopie eines der vorgefertigten Skripts herunterzuladen und es zu aktualisieren, um die erforderliche Aufgabe auszuführen. Sie müssen zuerst ein Master-Python-Skript erstellen, das die Kernfunktionen des Skripts ausführt. Erstellen Sie dann eine `Package-Structure.yml` Datei, um die Argumente und andere Metadaten zu definieren, die das Skript benötigt. Weitere Informationen finden Sie unter `Package-Structure.yml` Optionen.

Python-Python-Skript

Dies ist das erste Hauptskript, das ausgeführt wird, wenn ein Job initiiert wird. Sobald die Ausführung des Skripts abgeschlossen ist, ist die Aufgabe abgeschlossen und der endgültige Rückgabecode bestimmt den Status des Jobs. Die gesamte Ausgabe dieses Skripts wird erfasst, wenn es remote ausgeführt wird, und als Referenz in das Ausgabeüberwachungsprotokoll des Auftrags übergeben. Dieses Protokoll wird auch in Amazon gespeichert CloudWatch.

Zugriff auf Cloud Migration Factory mit AWS Daten und APIs über ein Skript

Um den Zugriff auf die Cloud Migration Factory über AWS APIs und Daten zu ermöglichen, können Sie das mitgelieferte Python-Hilfsmodul verwenden. Das Modul bietet die folgenden allgemeinen Funktionen:

Anmeldung ab Werk

Gibt ein Zugriffstoken zurück, mit dem Cloud Migration Factory auf AWS APIs aufgerufen werden kann. Diese Funktion versucht, sich mit einer Reihe von Anmeldeversuchen bei CMF anzumelden:

1. Durch den Versuch, auf das Standardgeheimnis zuzugreifen, das die Benutzer-ID und das Passwort des Dienstkontos enthält, falls es existiert und der Zugriff erlaubt ist. Dieser geheime Name MF ServiceAccount - [**Benutzerpool-ID**] wird überprüft.
2. Wenn Schritt 1 nicht erfolgreich ist und der Benutzer das Skript von der Befehlszeile aus ausführt, wird der Benutzer aufgefordert, eine Benutzer-ID und ein Passwort für die AWS Cloud Migration Factory-Version einzugeben. Wenn die Ausführung von einem Remote-Automatisierungsauftrag aus erfolgt, schlägt der Job fehl.

getServerCredentials

Gibt die Anmeldeinformationen für einen Server zurück, der in AWS Cloud Migration Factory entweder im Credentials Manager oder durch Benutzereingabe gespeichert ist. Diese Funktion überprüft eine Reihe verschiedener Quellen, um die Anmeldeinformationen für einen bestimmten Server zu ermitteln. Die Reihenfolge der Quellen ist:

1. Wenn `local_username` und `local_password` gesetzt und gültig sind, werden diese zurückgegeben.
2. Wenn `secret_override` gesetzt ist, wird dies verwendet, um das angegebene AWS Geheimnis von Secret Manager abzurufen. Andernfalls wird geprüft, ob der Servereintrag den Schlüssel `secret_name` enthält und dieser nicht leer ist, dann wird dieser geheime Name verwendet.

3. Wenn die angegebenen Geheimnisse nicht gefunden oder darauf zugegriffen werden können, fordert die Funktion den Benutzer zur Eingabe der Anmeldeinformationen auf, jedoch nur, wenn `no_user_prompts` auf `False` gesetzt ist, andernfalls gibt sie einen Fehler zurück.

Parameter

`local_username` — Wenn übergeben, wird es zurückgegeben.

`local_password` — Wenn es übergeben wurde, wird es zurückgegeben.

`server` — Servername, wie er im `server_name`-Attribut in AWS Cloud Migration Factory gespeichert ist.

`secret_overIDE` — Wird übergeben, wird der geheime Name festgelegt, der vom Secrets Manager für diesen Server abgerufen werden soll.

`no_user_prompts` — Weist die Funktion an, einen Benutzer nicht zur Eingabe einer Benutzer-ID und eines Passworts aufzufordern, wenn sie nicht gespeichert sind. Dies sollte für jedes Remote-Automatisierungsskript `True` sein.

GetCredentials

Ruft die mit AWS Cloud Migration Factory Credentials Manager gespeicherten Anmeldeinformationen von Secrets Manager ab.

Parameter

`secret_name` — Name des abzurufenden Geheimnisses.

`get_factory_servers`

Gibt ein Array von Servern aus dem AWS Cloud Migration Factory-Datenspeicher zurück, basierend auf der angegebenen `Waveid`.

Parameter

`Waveid` — Wave-Record-ID der Server, die zurückgegeben werden.

`Token` — Authentifizierungstoken, das von der `FactoryLogin` Lambda-Funktion abgerufen wurde.

`UserHost` — URL des AWS Cloud Migration Factory-Benutzer-API-Endpunkts.

`osSplit` — Wenn auf `gesetztttrue`, werden zwei Listen zurückgegeben, eine für Linux- und eine für Windows-Server. Wenn `False`, wird eine einzelne kombinierte Liste zurückgegeben.

Endgültige Zusammenfassung der Nachricht

Es wird empfohlen, eine zusammenfassende Meldung mit dem Ergebnis des Skripts als endgültige Ausgabe auf dem Bildschirm oder Sysout bereitzustellen. Dies wird auf der Konsole in der Eigenschaft `Letzte Nachricht` angezeigt, die einen schnellen Status des Skriptergebnisses bietet, ohne dass der Benutzer das vollständige Ausgabeprotokoll lesen muss.

Rückgabecode

Das Haupt-Python-Skript sollte beim Beenden einen Rückgabecode ungleich Null zurückgeben, wenn die Funktion des Skripts nicht vollständig erfolgreich war. Beim Empfang eines Rückgabecodes ungleich Null wird der Auftragsstatus im Auftragsprotokoll als Fehlgeschlagen angezeigt, was dem Benutzer bedeutet, dass er das Ausgabeprotokoll auf Einzelheiten des Fehlers überprüfen sollte.

YAML Package-structure.yml-Optionen

Beispiel für eine YAML-Datei

```
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"

```

Beschreibungen der YAML-Schlüssel

Erforderlich

Name — Standardname, den das Skript beim Import verwendet.

Beschreibung — Beschreibung der Verwendung des Skripts.

MasterFileName— Dies ist der Ausgangspunkt für die Ausführung des Skripts. Es muss sich um einen Python-Dateinamen handeln, der im Skriptpaketarchiv enthalten ist.

Argumente — Eine Liste von Argumenten, die das MasterFileName Python-Skript akzeptiert. Jedes Argument, das angegeben werden muss, hat das AWS Cloud Migration Factory-Attributdefinitionsformat. Erforderliche Eigenschaften für jedes Argument sind Name und Typ, alle anderen Eigenschaften sind optional.

Optional

UpdateUrl— Geben Sie eine URL an, unter der die Quelle des Skriptpakets für die Bereitstellung von Updates verfügbar ist. Derzeit dient dies nur als Referenz.

SchemaExtensions— Eine Liste von Attributen, die das Python-Skript im Schema enthalten muss, um Ausgaben zu speichern oder zusätzliche Daten abzurufen. Jedes Attribut muss im AWS CMF-Attributdefinitionsformat angegeben werden. Erforderliche Eigenschaften für jedes Attribut sind Schema, Name, Beschreibung und Typ. Alle anderen Eigenschaften sind optional. Alle neuen Attribute werden dem Schema automatisch hinzugefügt, wenn das Skript zum ersten Mal geladen wird, und Änderungen SchemaExtensions daran werden für neue Versionen des Skripts nicht verarbeitet. Wenn dies für das Hinzufügen eines neuen Skripts erforderlich ist, müssen manuelle Aktualisierungen des Schemas vorgenommen werden.

Schemaverwaltung

Die Cloud Migration Factory AWS on-Lösung bietet ein vollständig erweiterbares Metadaten-Repository, sodass Daten für die Automatisierung, Prüfung und Statusverfolgung in einem einzigen Tool gespeichert werden können. Das Repository bietet zum Zeitpunkt der Bereitstellung einen Standardsatz von Entitäten (Waves, Anwendungen, Server und Datenbanken) und Attributen, damit Sie mit der Erfassung und Verwendung der am häufigsten verwendeten Daten beginnen können. Von hier aus können Sie das Schema nach Bedarf anpassen.

Nur Benutzer der Cognito-Administratorgruppe haben die Rechte, das Schema zu verwalten. Informationen dazu, wie Sie einen Benutzer zum Mitglied des Administrators oder anderer Gruppen machen, finden Sie unter [Benutzerverwaltung](#).

Gehen Sie zu Administration und wählen Sie Attribute für die Standard-Entitätsregisterkarten aus. Die folgenden Registerkarten stehen zur Unterstützung der Verwaltung der Entität zur Verfügung.

Attribute — Ermöglicht das Hinzufügen, Bearbeiten und Löschen von Attributen.

Informationsbereich — Ermöglicht die Bearbeitung des Hilfeinhalts des Informationsfensters. Dieser wird auf der rechten Seite des Entitätsbildschirms im Abschnitt Migrationsverwaltung angezeigt.

Schemaeinstellungen — Derzeit bietet diese Registerkarte nur die Möglichkeit, den Anzeigenamen der Entität zu ändern. Dies ist der Name, der auf der Benutzeroberfläche angezeigt wird. Wenn nicht definiert, verwendet die Benutzeroberfläche den programmatischen Namen der Entität.

Ein Attribut hinzufügen/bearbeiten

Attribute können dynamisch über den Bereich Attributverwaltung der Cloud Migration Factory on AWS-Lösung geändert werden. Wenn Attribute hinzugefügt, bearbeitet oder gelöscht werden, werden die Aktualisierungen in Echtzeit übernommen, sodass der Administrator die Änderung

vornimmt. Die Sitzung jedes anderen Benutzers, der derzeit bei derselben Instanz angemeldet ist, wird innerhalb einer Minute, nachdem die Änderungen vom Administrator gespeichert wurden, automatisch aktualisiert.

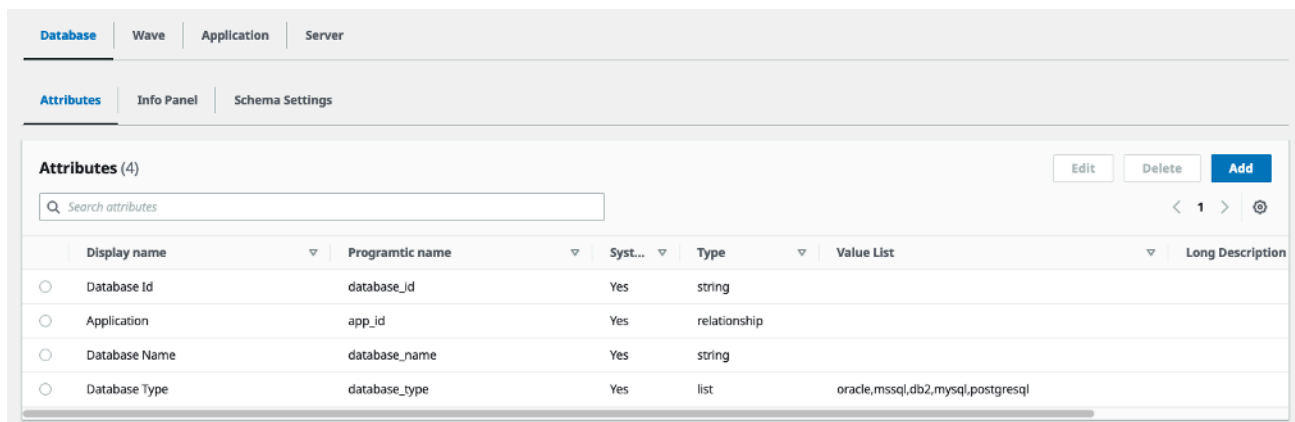
Einige Attribute sind als Systemattribute definiert, was bedeutet, dass das Attribut der Schlüssel zur Kernfunktionalität von Cloud Migration Factory auf AWS ist und daher nur einige Eigenschaften für Administratoren zur Änderung verfügbar sind. Jedes Attribut, bei dem es sich um ein Systemattribut handelt, wird mit einer Warnung oben auf dem Bildschirm „Attribut ändern“ angezeigt.

Bei systemdefinierten Attributen kann nur Folgendes bearbeitet werden:

- Informationsfenster
- Erweiterte Optionen
 - Gruppierung und Positionierung von Attributen
 - Überprüfung der Eingabe

Alle anderen Eigenschaften des vom System definierten Attributs sind schreibgeschützt.

Hinzufügen eines Attributs:



Sie können neue Attribute hinzufügen, indem Sie auf der Registerkarte Attribute der Entität, der Sie das Attribut hinzufügen möchten, auf die Schaltfläche Hinzufügen klicken. Im obigen Beispiel wird durch die Auswahl von Hinzufügen ein neues Attribut zur Datenbankentität hinzugefügt.


Im Dialogfeld „Attribut ändern“ müssen Sie die folgenden erforderlichen Eigenschaften angeben:

Programmatischer Name — Dies ist der Schlüssel, der verwendet wird, um Daten für das Attribut anhand von Elementen in der DynamoDB-Tabelle zu speichern. Er wird auch bei der Verwendung der Migration Factory-APIs und in Automatisierungsskripten referenziert.

Anzeigename — Dies ist die Bezeichnung, die auf der Weboberfläche neben dem Dateneingabefeld angezeigt wird.

Typ — Diese Dropdownauswahl definiert den Datentyp, den der Benutzer für das Attribut speichern darf. Verfügbar sind die nachfolgend aufgeführten Optionen:

Typ	Verwendung
Zeichenfolge	Benutzer können eine beliebige Textzeile eingeben. Zeilenumbrüche sind nicht zulässig.
Mehrwertige Zeichenfolge	Ähnlich wie bei einer Zeichenfolge besteht der einzige Unterschied darin, dass der Benutzer mehrere Werte in separate Zeilen innerhalb des Felds eingeben kann. Diese werden dann als Array/Liste gespeichert.
Passwort	Bietet dem Benutzer die Möglichkeit, Daten, die standardmäßig nicht auf dem Bildschirm angezeigt werden sollen, sicher einzugeben.

 **Note**

Daten werden bei Verwendung dieses Attributtyps nicht verschlüsselt gespeichert und werden bei der Anzeige in API-Payloads im Klartext angezeigt. Sie sollten daher nicht zum Speichern vertraulicher Daten verwendet werden. Alle Passwörter oder Geheimnisse sollten im Migration Factory Credential Manager (in diesem Dokument behandelt) gespeichert werden, der AWS Secrets Manager verwendet, um Anmeldeinformationen sicher zu speichern und Zugriff darauf zu gewähren.

Typ	Verwendung
Datum	Stellt ein Feld mit einer Datumsauswahl zur Verfügung, in der der Benutzer ein Datum auswählen kann, oder er kann das erforderliche Datum manuell eingeben.
Checkbox	Stellt ein Standard-Kontrollkästchen bereit. Wenn diese Option aktiviert ist, wird der Schlüsselwert „wahr“ gespeichert. Ist diese Option nicht aktiviert, ist er „falsch“ oder der Schlüssel ist nicht im Datensatz vorhanden.
TextArea	Im Gegensatz zum Typ String TextAreas bietet er die Möglichkeit, mehrzeiligen Text zu speichern, unterstützt er nur einfache Textzeichen.
Tag	Ermöglicht Benutzern das Speichern einer Liste von Schlüssel/Wert-Paaren.
Auflisten	Stellt dem Benutzer eine Liste vordefinierter Optionen zur Auswahl bereit. Diese Optionen sind in der Schemaattributdefinition in der Eigenschaft Werteliste des Attributs definiert.

Typ	Verwendung
Beziehung	<p>Dieser Attributtyp bietet die Möglichkeit, Beziehungen zwischen zwei beliebigen Entitäten oder Datensätzen zu speichern. Wenn Sie ein Beziehungsattribut definieren, wählen Sie die Entität aus, zu der die Beziehung bestehen soll, und dann den Schlüsselwert, der verwendet wird, um die Elemente miteinander in Beziehung zu setzen, und wählen das Attribut aus dem zugehörigen Element aus, das Sie dem Benutzer anzeigen möchten.</p> <p>Dem Benutzer wird eine Dropdownliste angezeigt, die auf der Entität und den für die Beziehung verfügbaren Werten basiert.</p> <p>Unter jedem Beziehungsfeld hat der Benutzer einen Quicklink, über den die Zusammenfassung des zugehörigen Elements angezeigt wird.</p>
JSON	<p>Stellt ein JSON-Editorfeld bereit, in dem JSON-Daten gespeichert und bearbeitet werden können. Dies könnte zum Speichern von Eingabe-/Ausgabeparametern von Skripten oder anderen Daten verwendet werden, die für die Automatisierung von Aufgaben oder für andere Zwecke benötigt werden.</p>

Wenn Sie ein neues Attribut hinzufügen, müssen Sie Benutzern über eine Richtlinie Zugriff auf das neue Attribut gewähren. Einzelheiten dazu, wie Sie Attributzugriff gewähren, finden Sie im Abschnitt [Berechtigungsverwaltung](#).

Bedienfeld „Informationen“

Bietet die Möglichkeit, kontextuelle Hilfe und Anleitungen für die Verwendung des Attributs anzugeben. Wenn diese Option angegeben ist, wird für die Bezeichnung des Attributs auf der Benutzeroberfläche auf der rechten Seite ein Link mit Informationen angezeigt. Wenn der Benutzer auf diesen Link klickt, werden die in diesem Abschnitt angegebenen Hilfeinhalte und Hilfelinks auf der rechten Seite des Bildschirms angezeigt.

Das Informationsfenster bietet zwei Ansichten der Daten: die Bearbeitungsansicht, in der Sie den Inhalt definieren können, und die Vorschauansicht, die eine schnelle Vorschau dessen bietet, was dem Benutzer angezeigt wird, wenn Aktualisierungen am Attribut gespeichert werden.

Der Hilfetitel unterstützt nur Klartextwerte. Der Inhalt der Hilfe unterstützt eine Teilmenge von HTML-Tags, die eine Textformatierung ermöglichen. Wenn Sie beispielsweise `Start- und` Endtags um den Text herum hinzufügen, wird der eingeschlossene Text fett formatiert (d. h. `Netzwerkschnittstellen-ID` würde zu Netzwerkschnittstellen-ID führen). Die unterstützten Tags lauten wie folgt:

Tag	Verwendung	Beispiel für die Benutzeroberfläche
<code><p></p></code>	Definiert einen Absatz.	<code><p>Mein erster Absatz</p></code> <code><p>Mein zweiter Absatz</p></code>
<code><a></code>	Definiert einen Hyperlink.	<code>Besuch! AWS</code>
<code><h3></code> , <code><h4></code> und <code><h5></code>	Definiert die Überschriften h3 bis h5	<code><h3>Meine Überschrift 3</h3></code>
<code></code>	Definiert einen Textabschnitt, sodass zusätzliche Formatierungen wie Textfarbe, Größe und Schriftart angewendet werden können.	<code>blau</code>

Tag	Verwendung	Beispiel für die Benutzerschnittfläche
<code><div></code>	Definiert einen Block des Dokuments, sodass zusätzliche Formatierungen wie Textfarbe, Größe und Schriftart angewendet werden können.	<pre> <div style="color:blue"> <h3>Dies ist eine blaue Überschrift</h3> <p>Das ist ein blauer Text in einem Div. </p> </div> </pre>
<code>+ </code>	Definiert eine ungeordnete Aufzählung.	<pre> Erneut hosten Plattform neu einrichten In Rente gehen </pre>
<code>, </code>	Definiert eine sortierte/ nummerierte Liste.	<pre> Erneut hosten Plattform neu einrichten In Rente gehen </pre>
<code><code></code>	Definiert einen Textblock oder Textabschnitt, der Code enthält.	<pre> <code>Hintergrundfarbe</code> </pre>

Tag	Verwendung	Beispiel für die Benutzerschnittfläche
<code><pre></code>	Definiert einen Block mit vorformatiertem Text, alle Zeilenumbrüche, Tabulatoren und Leerzeichen werden ausgegeben.	<pre><pre> Mein vorformatierter Text. Dieser Text wird in einer Schrift mit fester Breite angezeigt und wird wie eingegeben angezeigt. <<Diese Leerzeichen werden angezeigt. </pre></pre>
<code><dl>, <dt>und <dd></code>	Definiert eine Beschreibungsliste.	<pre><dl> <dt>Erneut hosten</dt> <dd>Migration per Lift & Shift</dd> <dt>In Rente gehen</dt> <dd>Nehmen Sie die Instanz oder den Dienst außer Betrieb</dd> </dl></pre>
<code><hr></code>	Definiert eine horizontale Linie auf der Seite, um einen Schalter in einem Thema oder Abschnitt anzuzeigen.	<code><hr></code>

Tag	Verwendung	Beispiel für die Benutzeroberfläche
<code>
</code>	Definiert einen Zeilenumbruch im Text. Diese werden unterstützt, sind aber nicht erforderlich, da alle Zeilenumbrüche im Editor <code>
</code> beim Speichern durch ersetzt werden.	<code>
</code>
<code><i></code> und <code></code>	Definierte den eingeschlossenen Text kursiv oder in einem anderen lokalisierten Format.	<code><i></code> Dies ist kursiv <code></i></code> oder <code></code> Das ist auch kursiv <code></code>
<code></code> und <code></code>	Definiert den eingeschlossenen Text in Fettschrift.	<code></code> Ich bin fett gedruckt <code></code> oder <code></code> Das ist anders <code></code>

Eine weitere verfügbare Option, um Hilfe bereitzustellen, sind Links zu externen Inhalten und Anleitungen. Um der kontextuellen Hilfe des Attributs einen externen Link hinzuzufügen, klicken Sie auf Neue URL hinzufügen und geben Sie eine Bezeichnung und eine URL an. Sie können nach Bedarf mehrere Links zu demselben Attributtyp hinzufügen.

Erweiterte Optionen

Gruppierung und Positionierung von Attributen

In diesem Abschnitt kann der Administrator festlegen, wo auf der Benutzeroberfläche zum Hinzufügen/Bearbeiten das Attribut positioniert werden soll. Außerdem können Attribute gruppiert werden, sodass der Benutzer auf einfache Weise verwandte Attribute finden kann.

UI-Gruppe ist ein Textwert, der den Namen der Gruppe definiert, in der das Attribut angezeigt werden soll. Alle Attribute mit demselben UI-Gruppenwert werden in derselben Gruppe platziert, jedes Attribut, für das keine UI-Gruppe angegeben wurde, wird in der Standardgruppe oben im Formular mit dem Titel Details platziert. Wenn die UI-Gruppe angegeben ist, zeigt die Benutzeroberfläche den hier angezeigten Text als Titel der Gruppe an.

Die zweite Eigenschaft in diesem Abschnitt ist Reihenfolge in der Gruppe. Sie kann auf eine beliebige positive oder negative Zahl gesetzt werden. Wenn diese Eigenschaft angegeben ist, werden die Attribute anhand dieses Werts vom niedrigsten zum höchsten Wert aufgelistet. Alle Attribute, für die keine Gruppenreihenfolge angegeben ist, haben eine niedrigere Priorität und werden alphabetisch sortiert.

Überprüfung der Eingabe

In diesem Abschnitt kann der Administrator Validierungskriterien definieren, die sicherstellen, dass der Benutzer gültige Daten eingegeben hat, bevor er ein Element speichern kann. Bei der Überprüfung wird ein regulärer Ausdruck oder eine Regex-Zeichenfolge verwendet, bei der es sich um eine Reihe von Zeichen handelt, die ein Suchmuster für einen Textwert angeben. Beispielsweise sucht das Muster `^(subnet- ([a-z0-9] {17}) *)$` nach dem Text `subnet-`, gefolgt von einer beliebigen Kombination der Zeichen `a` bis `z` (Kleinbuchstaben) und den Ziffern `0` bis `9` mit einer exakten Anzahl von Zeichen von `17`, wenn es etwas anderes findet, gibt es `false` zurück, was bedeutet, dass die Überprüfung fehlgeschlagen ist. In diesem Leitfaden können wir nicht alle verfügbaren Kombinationen und Muster behandeln, aber es gibt viele Ressourcen im Internet, die Ihnen helfen können, das perfekte für Ihren Anwendungsfall zu erstellen. Hier sind einige gängige Beispiele, um Ihnen den Einstieg zu erleichtern:

Regex-Muster	Verwendung
<code>^(?! \ s*\$) . +</code>	Stellt sicher, dass der Wert gesetzt ist.
<code>^(Subnetz- ([a-z0-9] {17}) *)\$</code>	Überprüft, ob der Wert eine gültige Subnetz-ID ist. [Beginnt mit dem Text <code>Subnetz</code> , gefolgt von <code>17</code> Zeichen, die nur aus Buchstaben und Zahlen bestehen]
<code>^(ami- ((([a-z0-9] {8,17}) +))\$)</code>	Stellen Sie sicher, dass der Wert eine gültige AMI-ID ist. [Beginnt mit dem Text <code>ami-</code> , gefolgt von <code>8</code> bis <code>17</code> Zeichen, die nur aus Buchstaben und Zahlen bestehen]

Regex-Muster	Verwendung
<code>^(sg- ([a-z0-9] {17}) *) \$</code>	Überprüft, ob der Wert ein gültiges Sicherheitsgruppen-ID-Format hat. [Beginnt mit dem Text sg-, gefolgt von 17 Zeichen, die nur aus Buchstaben und Zahlen bestehen]
<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>	Stellt sicher, dass Servernamen gültig sind und nur alphanumerische Zeichen, Bindestriche und Punkte enthalten.
<code>^([1-9] [1-9] [0-9] [1-9] [0-9] [0-9] [0-9] [1-9] [0-9] [0-9] [0-9] [1] [0-6] [0-3] [0-8] [0-4]) \$</code>	Stellt sicher, dass eine Zahl zwischen 1 und 1634 eingegeben wird.
<code>^(Standard io1 io2 gp2 gp3) \$</code>	Stellt sicher, dass die Zeichenfolge enter entweder mit Standard, io1, io2, gp2 oder gp3 übereinstimmt.

Nachdem Sie Ihr Regex-Suchmuster erstellt haben, können Sie die spezifische Fehlermeldung angeben, die dem Benutzer unter dem Feld angezeigt wird. Geben Sie diese in die Eigenschaft Validierungs-Hilfemeldung ein.

Sobald diese beiden Eigenschaften festgelegt sind, sehen Sie auf demselben Bildschirm unten einen Validierungssimulator. Hier können Sie testen, ob Ihr Suchmuster wie erwartet funktioniert und ob die Fehlermeldung korrekt angezeigt wird. Geben Sie einfach einen Testtext in das Feld Testvalidierung ein, um zu überprüfen, ob das Muster korrekt übereinstimmt.

Beispieldaten

Der Abschnitt mit den Beispieldaten bietet dem Administrator die Möglichkeit, dem Benutzer ein Beispiel für ein Datenformat zu zeigen, das für ein Attribut erforderlich ist. Dieses Format kann für das Datenformat angegeben werden, das bei einem Upload eines Aufnahmeformulars erforderlich ist, über die Benutzeroberfläche und/oder direkt über die API.

Beispieldaten, die in der Eigenschaft „Beispieldaten für das Aufnahmeformular“ angezeigt werden, werden in jeder Eingabevorlage ausgegeben, in der das Attribut enthalten ist, wenn Sie die Funktion

Herunterladen, eine Vorlage für das Aufnahmeformular, unter Migrationsmanagement > Import verwenden.

Beispieldaten für die Benutzeroberfläche und API-Beispieldaten werden im Attribut gespeichert, aber derzeit nicht in der Weboberfläche verfügbar gemacht. Diese können in Integrationen und Skripten verwendet werden.

Verwaltung von Berechtigungen

Die Cloud Migration Factory AWS on-Lösung bietet eine detaillierte, rollenbasierte Zugriffskontrolle auf die in der Lösung verfügbaren Daten und Automatisierungsfunktionen. Grundlage dafür ist Amazon Cognito, das das Benutzerverzeichnis und die Authentifizierungs-Engine bereitstellt.

Die folgende Tabelle zeigt die verschiedenen Elemente, aus denen sich das Framework für die Zugriffskontrolle innerhalb der Cloud Migration Factory on AWS-Lösung zusammensetzt, und zeigt, von wo aus jedes Element verwaltet wird.

Element zur Zugriffskontrolle	Verwaltungsschnittstelle	Beschreibung
Benutzer	Amazon Cognito und Cloud Migration Factory auf AWS	Benutzer werden in Amazon Cognito erstellt, gelöscht und aktualisiert, wo das Benutzerprofil eingerichtet und bei Bedarf eine Multi-Faktor-Authentifizierung (MFA) eingerichtet werden kann. In der AWS CMF-Benutzeroberfläche können Sie nur Benutzer zu Gruppen hinzufügen und daraus entfernen.
Gruppe	Cloud Migration Factory aktiviert AWS	Sie können Gruppen von der AWS CMF-Benutzeroberfläche aus erstellen oder löschen.
Rolle	Cloud Migration Factory aktiviert AWS	Eine Rolle ist einer oder mehreren Gruppen zugeordnet

Element zur Zugriffskontrolle	Verwaltungsschnittstelle	Beschreibung
		<p>t. Das Ändern der Gruppen, denen eine Rolle zugewiesen ist, erfolgt im AWS CMF-Administrationsbereich. Jedem Benutzer, der Mitglied einer Gruppe ist, die einer Rolle zugewiesen ist, werden alle Richtlinien zugewiesen, die der Rolle zugeordnet sind.</p> <p>Einer Rolle können eine oder mehrere Richtlinien zugewiesen werden.</p>
Richtlinie	Cloud Migration Factory aktiviert AWS	<p>Eine Richtlinie enthält die detaillierten Rechte, die jedem Benutzer zugewiesen werden, für den die Richtlinie gilt (über die Gruppenmitgliedschaft). Eine einzelne Richtlinie kann Datenzugriffsrechte für mehrere Entitäten oder eine einzelne Entität sowie Zugriffsrechte zur Ausführung von Automatisierungsjobs und anderen Aktionen innerhalb der AWS CMF-Benutzeroberfläche umfassen. Diese Richtlinien gelten auch, wenn ein Benutzer mit den AWS CMF-APIs interagiert.</p>

Richtlinien

Eine Richtlinie bietet die detailliertesten Berechtigungen, die in Cloud Migration Factory möglich sind. Sie enthält die Definition auf Aufgabenebene AWS, welche Rechte einem Benutzer gewährt werden. Innerhalb einer Richtlinie gibt es zwei Hauptberechtigungsstypen, die einer Benutzergruppe erteilt werden können: Metadatenberechtigungen und Automatisierungsaktionsberechtigungen. Mithilfe von Metadatenberechtigungen kann ein Administrator kontrollieren, welche Zugriffsebene eine Gruppe auf einzelne Schemas und deren Attribute hat. Dabei können Rechte zum Erstellen, Lesen, Aktualisieren und/oder Löschen nach Bedarf festgelegt werden. Berechtigungen für Automatisierungsaktionen gewähren Benutzern Zugriff auf die Ausführung bestimmter Automatisierungsaktionen, wie z. B. der AWS MGN-Integrationsaktion.

Berechtigungen für Metadaten

Für jedes Schema oder jede Entität innerhalb von AWS CMF kann ein Administrator eine Richtlinie definieren, die Benutzern den Zugriff auf bestimmte Attribute ermöglicht, und auch die Zugriffsebene definieren, die sie auf diese Attribute haben. Bei der Erstellung einer neuen Richtlinie sind die Standardrechte für alle Schemas kein Zugriff. Als Erstes sollte die Zugriffsebene festgelegt werden, die für diese Richtlinie auf Element-/Datensatzebene erforderlich ist. In der folgenden Tabelle werden die verfügbaren Zugriffsberechtigungen auf Datensatzebene beschrieben.

Zugriffsebene	Beschreibung
Erstellen	Wenn diese Option ausgewählt ist, kann ein Benutzer, für den diese Richtlinie gilt, neue Datensätze/Elemente dieses Typs zum Metadatenpeicher hinzufügen. Wenn „Erstelle n“ ausgewählt ist, aber keine anderen Rechte gewährt werden, kann der Benutzer unabhängig von den ausgewählten Attributen Datensätze erstellen und nur die erforderlichen Attribute auf einen Wert setzen.
Lesen	Noch nicht implementiert Wenn diese Option ausgewählt ist, hat ein Benutzer Leserechte für alle Datensätze/

Zugriffsebene	Beschreibung
	Elemente für diesen Entitätstyp. Wenn diese Option nicht ausgewählt ist, werden ihm die Datenelemente in der Benutzeroberfläche oder der API nicht angezeigt.
Aktualisierung	Wenn diese Option ausgewählt ist, kann ein Benutzer, für den diese Richtlinie gilt, Datensätze/Elemente dieses Typs im Metadatenpeicher aktualisieren, jedoch nur für die Attribute, die in der Zugriffsliste auf Attributebene angegeben sind. Wenn „Aktualisieren“ ausgewählt ist, muss mindestens ein Attribut ausgewählt werden, da andernfalls beim Speichern ein Fehler angezeigt wird.
Löschen	Wenn diese Option ausgewählt ist, kann ein Benutzer, für den diese Richtlinie gilt, Datensätze/Elemente dieses Typs aus dem Metadatenpeicher löschen.

Rollen

Mithilfe von Rollen können eine oder mehrere Richtlinien einer oder mehreren Gruppen zugewiesen werden. Die Kombination aller einer Rolle zugewiesenen Richtlinien bietet Zugriffsberechtigungen. Rollen können auf der Grundlage von Aufgabenrollen oder Funktionen innerhalb des Projekts oder der Organisation erstellt werden.

Entwicklerhandbuch

Quellcode

Sie können unser [GitHubRepository](#) besuchen, um die Vorlagen und Skripts für diese Lösung herunterzuladen und Ihre Anpassungen mit anderen zu teilen. Wenn Sie eine frühere Version der CloudFormation Vorlage benötigen oder ein technisches Problem melden möchten, können Sie dies auf der [GitHubProblemseite](#) tun. Melden Sie technische Probleme mit der Lösung auf der [Seite Probleme](#) des GitHub Repositorys.

Zusätzliche Themen

Liste der automatisierten Migrationsaktivitäten mithilfe der Migration Factory-Webkonsole

Die Cloud Migration Factory AWS on-Lösung stellt automatisierte Migrationsaktivitäten bereit, die Sie für Ihre Migrationsprojekte nutzen können. Sie können die unten aufgeführten Migrationsaktivitäten verfolgen und sie an Ihre Geschäftsanforderungen anpassen.

Bevor Sie mit einer der Aktivitäten beginnen, sollten Sie unbedingt das [Benutzerhandbuch — Automatisierung von der Konsole aus ausführen](#) lesen, um zu verstehen, wie das funktioniert. Außerdem müssen Sie [einen Automatisierungsserver erstellen](#) und [Windows- und Linux-Benutzer erstellen](#), um die Automatisierung von der Konsole aus auszuführen.

Verwenden Sie die folgenden Verfahren in derselben Reihenfolge, um einen vollständigen Testlauf der Lösung mithilfe des Beispiel-Automatisierungsskripts und der Aktivitäten durchzuführen.

Überprüfen Sie die Voraussetzungen

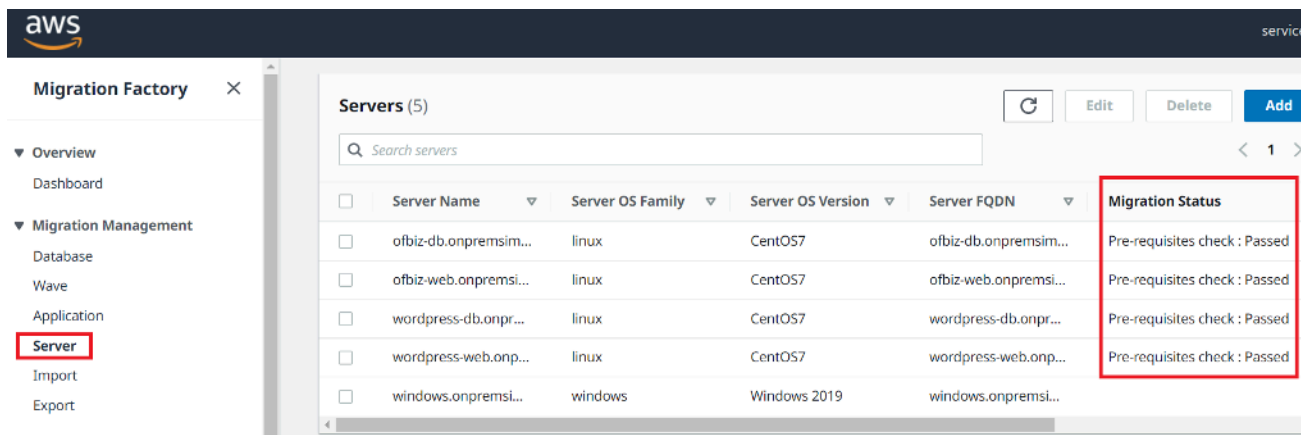
Connect zu den Quellservern im Geltungsbereich her, um die erforderlichen Voraussetzungen wie TCP 1500, TCP 443, freien Speicherplatz auf dem Root-Volume, .NET-Framework-Version und andere Parameter zu überprüfen. Diese Voraussetzungen sind für die Replikation erforderlich.

Bevor Sie die Prüfung der Voraussetzungen durchführen können, müssen Sie die erste Version manuell auf einem Quellserver installieren, damit ein Replikationsserver in EC2 erstellt wird. Wir stellen eine Verbindung zu diesem Server her, um den Port 1500 zu testen. Nach der Installation erstellt der AWS Application Migration Service (AWSMGN) den Replikationsserver in Amazon Elastic Compute Cloud (Amazon EC2). In dieser Aktivität müssen Sie den TCP-Port 1500 vom Quellserver zum Replikationsserver überprüfen. Informationen zur Installation des AWS MGN-Agenten auf Ihren Quellservern finden Sie in den [Installationsanweisungen](#) im AWS Application Migration Service-Benutzerhandbuch.

Gehen Sie wie folgt vor, während Sie bei der Migration Factory-Webkonsole angemeldet sind.

1. Wählen Sie in der Migration Factory-Konsole im Menü auf der linken Seite Jobs und dann auf der rechten Seite Aktionen und dann Run Automation aus.

2. Geben Sie den Jobnamen ein, wählen Sie das Skript 0-Check MGN Prerequisites und Ihren Automatisierungsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
3. Die Auswahl von Linux Secrets und/oder Windows Secrets hängt davon ab, welche Betriebssysteme Sie für diese Welle haben. Geben Sie die IP-Adresse des MGN-Replikationsservers ein, wählen Sie die Welle aus, auf der Sie die Automatisierung ausführen möchten, und klicken Sie auf Automatisierungsauftrag senden.
4. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte LAUTEN. Wählen Sie Aktualisieren, um den Status zu sehen. Nach ein paar Minuten sollte er zu Complete wechseln.
5. Das Skript aktualisiert auch den Migrationsstatus der Lösung in der Migration Factory-Weboberfläche, wie im folgenden Screenshot eines Beispielprojekts gezeigt.



Installieren Sie die Replikationsagenten

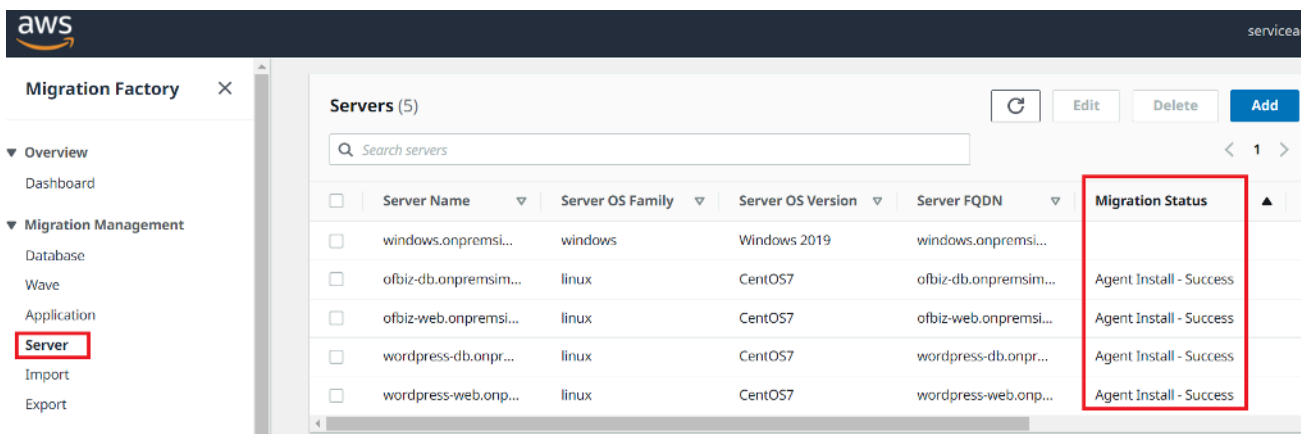
Note

Stellen Sie vor der Installation des Agenten sicher, dass [AWSMGN in jedem Zielkonto und jeder Region initialisiert ist](#).

Gehen Sie wie folgt vor, um die Replikationsagenten automatisch auf den Quellservern im Geltungsbereich zu installieren.

1. Wählen Sie in der Migration Factory-Konsole im Menü auf der linken Seite Jobs und dann auf der rechten Seite Aktionen und dann Run Automation aus.

2. Geben Sie den Jobnamen ein, wählen Sie 1-Install MGN Agents Script und Ihren Automationsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
3. Die Auswahl von Linux Secrets und/oder Windows Secrets hängt davon ab, welche Betriebssysteme Sie für diese Welle haben. Wählen Sie die Welle aus, für die Sie die Automatisierung ausführen möchten, und wählen Sie Automatisierungsjob einreichen.
4. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte laufen sein. Wählen Sie Aktualisieren, um den Status zu sehen. Nach ein paar Minuten sollte er zu Complete wechseln.
5. Das Skript stellt auch den Migrationsstatus in der Migration Factory-Weboberfläche bereit, wie im folgenden Beispiel-Screenshot gezeigt.



Übertragen Sie die Skripte nach dem Start

AWS Application Migration Service (MGN) unterstützt Skripte nach dem Start, um Sie bei der Automatisierung von Aktivitäten auf Betriebssystemebene zu unterstützen, z. B. bei der Installation/Deinstallation der Software nach dem Start von Ziel-Instances. Diese Aktivität überträgt die Skripte nach dem Start auf Windows- und/oder Linux-Computer, je nachdem, welche Server für die Migration identifiziert wurden.

Note

Bevor Sie die Skripte nach dem Start übertragen, müssen Sie die Dateien in einen Ordner auf dem Server für die Migrationsautomatisierung kopieren.

Gehen Sie wie folgt vor, um die Skripte nach dem Start auf Windows-Computer zu übertragen.

1. Wählen Sie in der Migration Factory-Konsole im Menü auf der linken Seite Jobs und dann auf der rechten Seite Aktionen und dann Run Automation aus.
2. Geben Sie den Jobnamen ein, wählen Sie 1-Copy Post Launch Scripts Script und Ihren Automatisierungsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
3. Die Auswahl von Linux Secrets und/oder Windows Secrets hängt davon ab, welche Betriebssysteme Sie für diese Welle haben. Geben Sie einen Linux-Quellpfad und/oder einen Windows-Quellpfad an.
4. Wählen Sie die Welle aus, für die Sie Automaton ausführen möchten, und wählen Sie Automatisierungsjob einreichen.
5. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte laufen sein und Sie können „Aktualisieren“ wählen, um den Status zu sehen. Nach ein paar Minuten sollte es zu Complete wechseln.

Überprüfen Sie den Replikationsstatus

Bei dieser Aktivität wird der Replikationsstatus für die Quellserver im Geltungsbereich automatisch überprüft. Das Skript wird alle fünf Minuten wiederholt, bis sich der Status aller Quellserver in der angegebenen Welle in den Status Fehlerfrei ändert.

Verwenden Sie das folgende Verfahren, um den Replikationsstatus zu überprüfen.

1. Wählen Sie in der Migration Factory-Konsole im Menü auf der linken Seite Jobs und dann auf der rechten Seite Aktionen und dann Run Automation aus.
2. Geben Sie den Jobnamen ein, wählen Sie 2-Verify Replication Status-Skript und Ihren Automatisierungsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
3. Wählen Sie die Welle aus, für die Sie Automaton ausführen möchten, und wählen Sie Automatisierungsjob einreichen.
4. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte laufen sein und Sie können auf die Schaltfläche „Aktualisieren“ klicken, um den Status zu sehen. Nach ein paar Minuten sollte es zu Complete wechseln.

The screenshot shows the AWS Application Migration Service console. The left sidebar contains navigation options like 'Source servers', 'Launch history', and 'Settings'. The main area displays a table of source servers. A red box highlights the 'Data replication status' column, which shows 'Healthy' for all four servers listed.

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

Die Replikation kann eine Weile dauern. Möglicherweise sehen Sie das Status-Update einige Minuten lang nicht von der Werkskonsole aus. Optional können Sie den Status auch im MGN-Dienst überprüfen.

Überprüfen Sie die Startvorlage

Diese Aktivität validiert die Server-Metadaten in der Migration Factory und stellt sicher, dass sie mit der EC2-Vorlage funktionieren und keine Tippfehler enthalten. Dabei werden sowohl Test- als auch Cutover-Metadaten validiert.

Verwenden Sie das folgende Verfahren, um die EC2-Startvorlage zu validieren.

1. Navigieren Sie zur Migration Factory-Konsole und wählen Sie im Menübereich Wave aus.
2. Wählen Sie die Zielwelle und dann Aktionen aus. Wählen Sie Rehost und dann MGN aus.
3. Wählen Sie für die Aktion „Startvorlage validieren“ und anschließend „Alle Anwendungen“ aus.
4. Wählen Sie Senden, um die Validierung zu starten.

Nach einiger Zeit wird die Validierung ein erfolgreiches Ergebnis zurückgeben.

Note

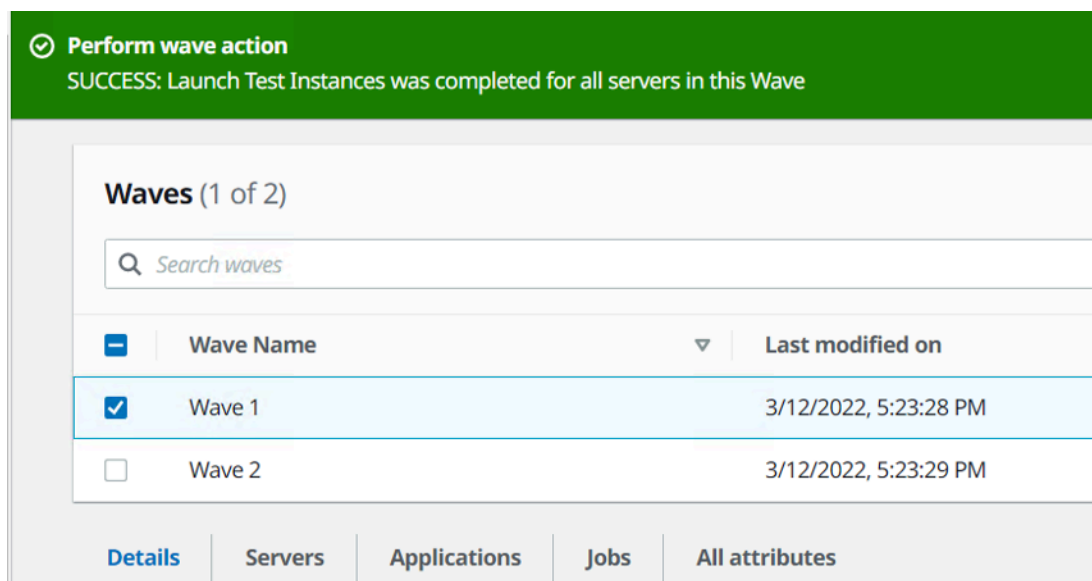
Wenn die Validierung nicht erfolgreich ist, erhalten Sie eine bestimmte Fehlermeldung: Die Fehler können auf ungültige Daten im Serverattribut zurückzuführen sein, z. B. auf ungültige Subnet_IDs, SecurityGroup_Ids oder InstanceType. Sie können von der Migration Factory-Weboberfläche zur Pipeline-Seite wechseln und den problematischen Server auswählen, um die Fehler zu beheben.

Starten Sie Instances zum Testen

Diese Aktivität startet alle Zielcomputer für eine bestimmte Welle in AWS Application Migration Service (MGN) im Testmodus.

Gehen Sie wie folgt vor, um Test-Instances zu starten.

1. Wählen Sie auf der Migration Factory-Konsole im Navigationsmenü Wave aus.
2. Wählen Sie Zielwelle und dann Aktionen aus. Wählen Sie Rehost und dann MGN aus.
3. Wählen Sie Aktion „Testinstanzen starten“ und anschließend „Alle Anwendungen“ aus.
4. Wählen Sie Senden, um Testinstanzen zu starten.
5. Nach einiger Zeit wird die Validierung ein erfolgreiches Ergebnis zurückgeben.



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

Durch diese Aktion wird auch der Migrationsstatus für den gestarteten Server aktualisiert.

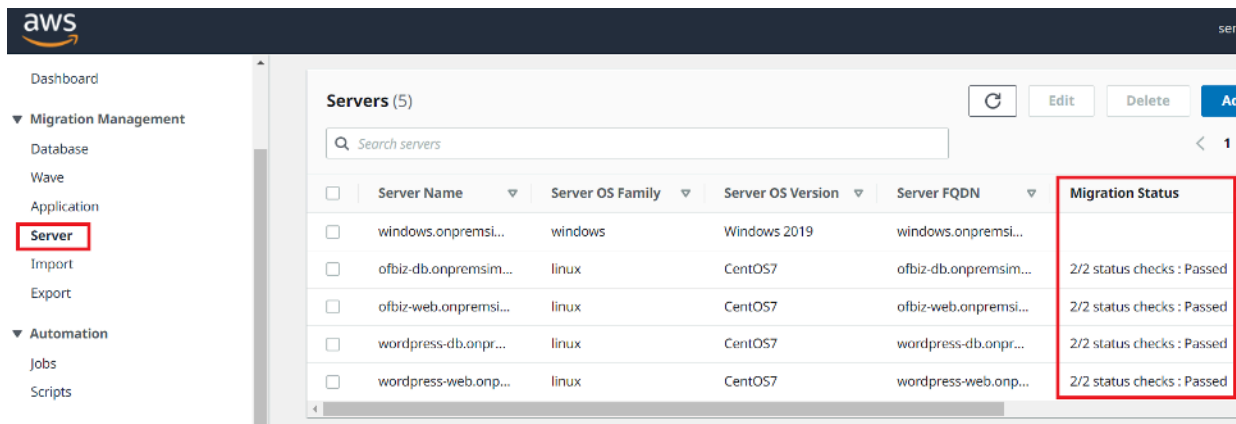
Überprüfen Sie den Status der Zielinstanz

Bei dieser Aktivität wird der Status der Zielinstanz überprüft, indem der Startvorgang für alle Quellserver im Geltungsbereich in derselben Welle überprüft wird. Es kann bis zu 30 Minuten dauern, bis die Ziel-Instances hochgefahren sind. Sie können den Status manuell überprüfen, indem Sie sich bei der Amazon EC2-Konsole anmelden, nach dem Namen des Quellservers suchen und den Status überprüfen. Sie erhalten eine Zustandsprüfungsnachricht, dass 2/2 Prüfungen bestanden wurden, was darauf hinweist, dass die Instance aus Sicht der Infrastruktur fehlerfrei ist.

Bei einer groß angelegten Migration ist es jedoch zeitaufwändig, den Status jeder Instanz zu überprüfen. Daher können Sie dieses automatisierte Skript ausführen, um zu überprüfen, ob der Status der 2/2 Prüfungen für alle Quellserver in einer bestimmten Welle bestanden wurde.

Verwenden Sie das folgende Verfahren, um den Status der Zielinstanz zu überprüfen.

1. Navigieren Sie zur Migration Factory-Konsole und wählen Sie im Menü auf der linken Seite Jobs aus.
2. Wählen Sie auf der rechten Seite Aktionen und dann Automatisierung ausführen aus.
3. Geben Sie den Jobnamen ein, wählen Sie 3-Verify Instance Status script und Ihren Automationsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
4. Wählen Sie die Welle aus, für die Sie Automaton ausführen möchten, und wählen Sie Automatisierungsjob einreichen.
5. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte laufen sein und Sie können „Aktualisieren“ wählen, um den Status zu sehen. Nach ein paar Minuten sollte es zu Complete wechseln.



Note

Der Start der Instanz kann eine Weile dauern, und es kann sein, dass Sie das Status-Update einige Minuten lang nicht von der Werkskonsole aus sehen. Migration Factory erhält außerdem ein Status-Update vom Skript. Aktualisieren Sie den Bildschirm bei Bedarf.

Note

Wenn Ihre Ziel-Instances die 2/2-Zustandsprüfungen beim ersten Mal nicht bestehen, kann das daran liegen, dass der Startvorgang länger dauert. Wir empfehlen, die Integritätsprüfungen etwa eine Stunde nach der ersten Integritätsprüfung ein zweites Mal durchzuführen. Dadurch wird sichergestellt, dass der Startvorgang abgeschlossen ist. Wenn die Integritätsprüfungen beim zweiten Mal fehlschlagen, wenden Sie sich an das [AWSSupport Center](#), um einen Supportfall zu protokollieren.

Als bereit für die Umstellung markieren

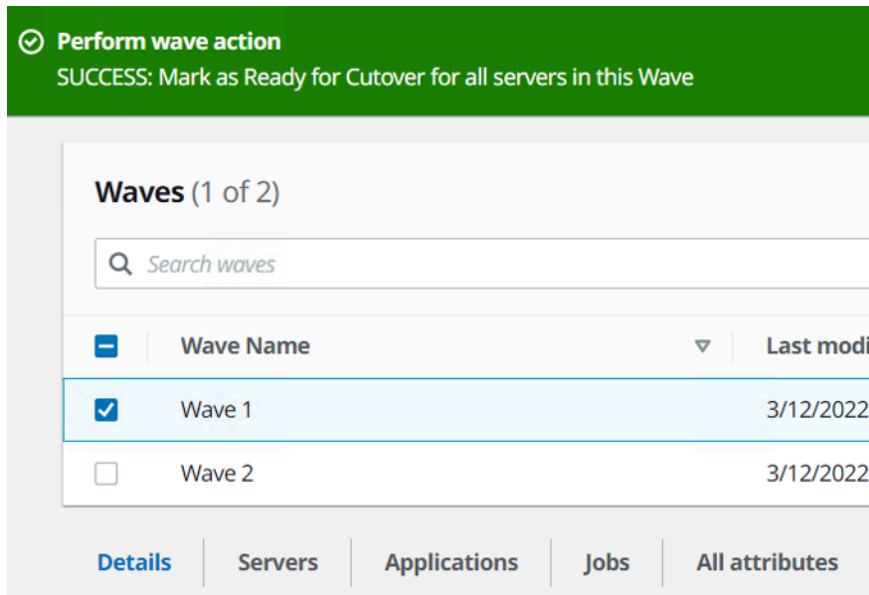
Sobald der Test abgeschlossen ist, ändert diese Aktivität den Status des Quellserver so, dass er als bereit für die Übernahme markiert wird, sodass der Benutzer eine Übernahmeinstanz starten kann.

Verwenden Sie das folgende Verfahren, um die EC2-Startvorlage zu validieren.

1. Wählen Sie auf der Migration Factory-Konsole auf der linken Seite Wave aus.
2. Wählen Sie die Zielwelle aus und klicken Sie auf die Schaltfläche Aktionen. Wählen Sie Rehost und dann MGN aus.
3. Wählen Sie Als „Bereit für die Übernahme“ markieren und anschließend Alle Anwendungen aus.

4. Wählen Sie Senden, um Live-Instanzen zu starten.

Nach einiger Zeit wird die Validierung zu einem erfolgreichen Ergebnis führen.



Fahren Sie die Quellserver im Geltungsbereich herunter

Durch diese Aktivität werden die Quellserver im Geltungsbereich heruntergefahren, die an der Migration beteiligt sind. Nachdem Sie den Replikationsstatus der Quellserver überprüft haben, können Sie die Quellserver herunterfahren, um Transaktionen von den Client-Anwendungen zu den Servern zu beenden. Sie können die Quellserver im Übernahmefenster herunterfahren. Das manuelle Herunterfahren der Quellserver kann fünf Minuten pro Server und bei großen Wellen insgesamt einige Stunden dauern. Stattdessen können Sie dieses Automatisierungsskript ausführen, um alle Ihre Server in der angegebenen Welle herunterzufahren.

Gehen Sie wie folgt vor, um alle an der Migration beteiligten Quellserver herunterzufahren.

1. Wählen Sie in der Migration Factory-Konsole im Menü auf der linken Seite Jobs und dann auf der rechten Seite Aktionen und dann Run Automation aus.
2. Geben Sie den Jobnamen ein, wählen Sie das 3-Shutdown All Server-Skript und Ihren Automatisierungsserver aus, um das Skript auszuführen. Wenn der Automatisierungsserver nicht existiert, stellen Sie sicher, dass Sie den Vorgang [Einen Migrationsautomatisierungsserver erstellen](#) abschließen.
3. Die Auswahl von Linux Secrets und/oder Windows Secrets hängt davon ab, welche Betriebssysteme Sie für diese Welle haben.

4. Wählen Sie die Welle aus, für die Sie Automaten ausführen möchten, und wählen Sie Automatisierungsjob einreichen.
5. Sie werden zur Seite mit der Jobliste weitergeleitet. Der Jobstatus sollte laufen sein und Sie können auf die Schaltfläche „Aktualisieren“ klicken, um den Status zu sehen. Nach ein paar Minuten sollte es zu Complete wechseln.

Starten Sie Instances für Cutover

Diese Aktivität startet alle Zielcomputer für eine bestimmte Welle in AWS Application Migration Service (MGN) im Cutover-Modus.

Gehen Sie wie folgt vor, um Test-Instances zu starten.

1. Wählen Sie auf der Migration Factory-Konsole auf der linken Seite Wave aus.
2. Wählen Sie Zielwelle und dann Aktionen aus. Wählen Sie Rehost und dann MGN aus.
3. Wählen Sie Aktion „Cutover-Instances starten“ und anschließend „Alle Anwendungen“ aus.
4. Wählen Sie Senden, um die Testinstanzen zu starten.

Nach einiger Zeit wird die Validierung ein erfolgreiches Ergebnis zurückgeben.

Note

Durch diese Aktion wird auch der Migrationsstatus für den gestarteten Server aktualisiert.

Liste der automatisierten Migrationsaktivitäten mithilfe der Befehlszeile


Note

Wir empfehlen, die Automatisierung über die Cloud Migration Factory auf der AWS-Konsole auszuführen. Sie können die folgenden Schritte verwenden, um Automatisierungsskripts auszuführen. Stellen Sie sicher, dass Sie die Automatisierungsskripts aus dem GitHub Repository herunterladen und den Automatisierungsserver anhand der Schritte [unter Automationen von der Befehlszeile ausführen](#) konfigurieren und den

Anweisungen zur Konfiguration von Berechtigungen unter [AWSBerechtigungen für den Migrationsautomatisierungsserver konfigurieren](#) folgen.

Die Cloud Migration Factory AWS on-Lösung stellt automatisierte Migrationsaktivitäten bereit, die Sie für Ihre Migrationsprojekte nutzen können. Sie können die unten aufgeführten Migrationsaktivitäten verfolgen und sie an Ihre Geschäftsanforderungen anpassen.

Bevor Sie mit einer der Aktivitäten beginnen, stellen Sie sicher, dass Sie an Ihrem Migrationsautomatisierungsserver als Domänenbenutzer mit lokalen Administratorrechten auf den Quellservern im Geltungsbereich angemeldet sind.

 **Important**

Sie müssen sich als Administratorbenutzer anmelden, um die in diesem Abschnitt aufgeführten Aktivitäten abzuschließen.

Verwenden Sie die folgenden Verfahren in derselben Reihenfolge, um einen vollständigen Testlauf der Lösung mithilfe des Beispiel-Automatisierungsskripts und der Aktivitäten durchzuführen.

Überprüfen Sie die Voraussetzungen

Connect zu den Quellservern im Geltungsbereich her, um die erforderlichen Voraussetzungen wie TCP 1500, TCP 443, freien Speicherplatz auf dem Root-Volume, .NET-Framework-Version und andere Parameter zu überprüfen. Diese Voraussetzungen sind für die Replikation erforderlich.

Bevor Sie die Prüfung der Voraussetzungen durchführen können, müssen Sie den ersten Agenten manuell auf einem Quellserver installieren, damit ein Replikationsserver in EC2 erstellt wird. Wir stellen eine Verbindung zu diesem Server her, um Port 1500 zu testen. Nach der Installation erstellt der AWS Application Migration Service (AWSMGN) den Replikationsserver in Amazon Elastic Compute Cloud (Amazon EC2). In dieser Aktivität müssen Sie den TCP-Port 1500 vom Quellserver zum Replikationsserver überprüfen. Informationen zur Installation des AWS MGN-Agenten auf Ihren Quellservern finden Sie in den [Installationsanweisungen](#) im Application Migration Service-Benutzerhandbuch.

Verwenden Sie das folgende Verfahren, während Sie beim Migrationsautomatisierungsserver angemeldet sind, um die Voraussetzungen zu überprüfen.

1. Wenn Sie als Administrator angemeldet sind, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_0-Prerequisites-checks` Ordner und führen Sie den folgenden Python-Befehl aus:

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

Ersetzen Sie `<wave-id>` und `< rep-server-ip >` durch die entsprechenden Werte:

- Das Waveid ist ein eindeutiger Ganzzahlwert zur Identifizierung Ihrer Migrationswellen.
 - Der ReplicationServerIP Wert identifiziert die IP-Adresse des Replikationsservers. Ändern Sie diesen Wert in die Amazon EC2 EC2-IP-Adresse. Um diese Adresse zu finden, melden Sie sich bei der anAWS Management Console, suchen Sie nach Replication, wählen Sie einen der Replikationsserver aus und kopieren Sie die private IP-Adresse. Wenn die Replikation über das öffentliche Internet erfolgt, verwenden Sie stattdessen die öffentliche IP-Adresse.
3. Das Skript ruft automatisch eine Serverliste für die angegebene Welle ab.

Das Skript überprüft dann die Voraussetzungen für Windows-Server und gibt `fail` für jede Prüfung den Status entweder `pass` oder zurück.

Note

Möglicherweise erhalten Sie eine Sicherheitswarnung wie die folgende, wenn das PowerShell Skript nicht vertrauenswürdig ist. Führen Sie den folgenden Befehl aus PowerShell , um das Problem zu beheben:

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

Als Nächstes überprüft das Skript die Linux-Server.

Sobald die Prüfungen abgeschlossen sind, gibt das Skript für jeden Server ein Endergebnis zurück.

```
*****  
**** 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
```

Wenn der Server eine oder mehrere Prüfungen der Voraussetzungen nicht bestanden hat, können Sie den fehlerhaften Server identifizieren, indem Sie entweder die ausführliche Fehlermeldung lesen, die Sie nach Abschluss der Prüfung erhalten haben, oder indem Sie durch die Protokolldetails blättern.

Das Skript aktualisiert auch den Migrationsstatus der Lösung in der Migration Factory-Weboberfläche, wie im folgenden Screenshot eines Beispielprojekts gezeigt.

Installieren Sie die Replikationsagenten

Note

Stellen Sie vor der Installation des Agenten sicher, dass [AWSMGN in jedem Zielkonto initialisiert ist](#).

Gehen Sie wie folgt vor, um die Replikationsagenten automatisch auf den Quellservern im Geltungsbereich zu installieren.

1. Öffnen Sie auf dem Server für die Migrationsautomatisierung, der als Administrator signiert ist, eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_1-AgentInstall` Ordner und führen Sie den folgenden Python-Befehl aus:


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

Ersetzen Sie < wave-id > durch den entsprechenden Wave-ID-Wert, um den Replication Agent auf allen Servern in der identifizierten Welle zu installieren. Das Skript installiert den Agenten nacheinander auf allen Quellservern in derselben Welle.

Note

Um den Agenten erneut zu installieren, können Sie `--force` ein Argument hinzufügen.

- Das Skript generiert eine Liste mit den Quellservern, die für die angegebene Welle enthalten sind. Darüber hinaus können auch Server bereitgestellt werden, die in mehreren Konten und für verschiedene Betriebssystemversionen identifiziert wurden.

Wenn in dieser Welle Linux-Computer enthalten sind, müssen Sie Ihre Linux-Sudo-Anmeldedaten eingeben, um sich bei diesen Quellservern anzumelden.

Die Installation beginnt unter Windows und geht dann für jeden unter Linux weiter. AWS-Konto

```
*****
*** 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

Möglicherweise erhalten Sie eine Sicherheitswarnung wie die folgende, wenn das PowerShell Skript nicht vertrauenswürdig ist. Führen Sie den folgenden Befehl aus PowerShell , um das Problem zu beheben:

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

Die Ergebnisse werden angezeigt, nachdem das Skript die Installation der Replikationsagenten abgeschlossen hat. Überprüfen Sie die Ergebnisse auf Fehlermeldungen, um Server zu identifizieren, die die Agents nicht installieren konnten. Sie müssen die Agents auf den ausgefallenen Servern manuell installieren. Wenn die manuelle Installation nicht erfolgreich ist, rufen Sie das [AWS Support Center](#) auf und melden Sie eine Support-Anfrage.

```
*****  
*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
```

Das Skript stellt auch den Migrationsstatus in der Migration Factory-Weboberfläche bereit, wie im folgenden Screenshot eines Beispielprojekts dargestellt.

Veröffentlichen Sie die Skripte nach dem Start

AWS Application Migration Service unterstützt Skripte nach dem Start, um Sie bei der Automatisierung von Aktivitäten auf Betriebssystemebene wie der Installation/Deinstallation von Software nach dem Start von Ziel-Instances zu unterstützen. Diese Aktivität überträgt die Skripts nach dem Start auf Windows- und/oder Linux-Computer, je nachdem, welche Server für die Migration identifiziert wurden.

Verwenden Sie das folgende Verfahren vom Server für die Migrationsautomatisierung, um die Skripts nach dem Start auf Windows-Computer zu übertragen.

1. Als Administrator angemeldet, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_1-FileCopy` Ordner und führen Sie den folgenden Python-Befehl aus:

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

<wave-id> Ersetzen Sie es durch den entsprechenden Wave-ID-Wert und <file-path> durch den vollständigen Dateipfad für Source, wo sich das Skript befindet. Zum Beispiel `c:\migrations\scripts\script_mgn_1-FileCopy`. Mit diesem Befehl werden alle Dateien aus dem Quellordner in den Zielordner kopiert.

Note

Mindestens eines dieser beiden Argumente muss angegeben werden: `WindowsSource`, `LinuxSource`. Wenn Sie `WindowsSource` den Pfad angeben, überträgt dieses Skript nur Dateien auf Windows-Server in dieser Welle, genau wie `LinuxSource`, das nur Dateien auf die Linux-Server in dieser Welle überträgt. Wenn Sie beide angeben, werden Dateien sowohl auf Windows- als auch auf Linux-Server übertragen.

3. Das Skript generiert eine Liste mit den Quellservern, die für die angegebene Welle enthalten sind. Darüber hinaus können auch Server bereitgestellt werden, die in mehreren Konten und für verschiedene Betriebssystemversionen identifiziert wurden.

Wenn in dieser Welle Linux-Computer enthalten sind, müssen Sie Ihre Linux-Sudo-Anmeldedaten eingeben, um sich bei diesen Quellservern anzumelden.

4. Das Skript kopiert die Dateien in den Zielordner. Wenn der Zielordner nicht existiert, erstellt die Lösung ein Verzeichnis und benachrichtigt Sie über diese Aktion.

Überprüfen Sie den Replikationsstatus

Bei dieser Aktivität wird der Replikationsstatus für die Quellserver im Geltungsbereich automatisch überprüft. Das Skript wird alle fünf Minuten wiederholt, bis sich der Status aller Quellserver in der angegebenen Welle in den Status Fehlerfrei ändert.

Verwenden Sie das folgende Verfahren vom Migrationsautomatisierungsserver aus, um den Replikationsstatus zu überprüfen.

1. Als Administrator angemeldet, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `\migrations\scripts\script_mgn_2-Verify-replication` Ordner und führen Sie den folgenden Python-Befehl aus:

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

<wave-id> Ersetzen Sie ihn durch den entsprechenden Wave-ID-Wert, um den Replikationsstatus zu überprüfen. Das Skript überprüft die Replikationsdetails für alle Server in der spezifischen Welle und aktualisiert das Replikationsstatusattribut für den in der Lösung identifizierten Quellserver.

3. Das Skript generiert eine Liste mit den Servern, die für die angegebene Welle enthalten sind.

Der erwartete Status für die Quellserver im Geltungsbereich, die startbereit sind, lautet Fehlerfrei. Wenn Sie einen anderen Status für einen Server erhalten, ist er noch nicht startbereit.

Der folgende Screenshot einer Beispielwelle zeigt, dass alle Server in der aktuellen Welle die Replikation abgeschlossen haben und bereit sind, getestet oder umgestellt zu werden.

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

#####
#### Replication Status for Account: 515833311223 , region: us-east-1 ####
#####
Server Server-T1 replication status: Healthy
Server Server1 replication status: Healthy

#####
#### Replication Status for Account: 114707200000 , region: us-east-2 ####
#####
Server MF-Ubuntu replication status: Healthy
Server Server-T15 replication status: Healthy
Server Server2 replication status: Healthy
```

Optional können Sie den Status in der Migration Factory-Weboberfläche überprüfen.

Überprüfen Sie den Status der Zielinstanz

Bei dieser Aktivität wird der Status der Zielinstanz überprüft, indem der Startvorgang für alle Quellserver im Geltungsbereich in derselben Welle überprüft wird. Es kann bis zu 30 Minuten dauern, bis die Ziel-Instances hochgefahren sind. Sie können den Status manuell überprüfen, indem Sie sich bei der Amazon EC2-Konsole anmelden, nach dem Namen des Quellservers suchen und den Status überprüfen. Sie erhalten eine Zustandsprüfungsnachricht, dass 2/2 Prüfungen bestanden wurden, was darauf hinweist, dass die Instance aus Sicht der Infrastruktur fehlerfrei ist.

Bei einer groß angelegten Migration ist es jedoch zeitaufwändig, den Status jeder Instanz zu überprüfen. Sie können also dieses automatisierte Skript ausführen, um den Status der 2/2 Prüfungen für alle Quellserver in einer bestimmten Welle zu überprüfen.

Verwenden Sie das folgende Verfahren vom Migrationsautomatisierungsserver aus, um den Status der Zielinstanz zu überprüfen.

1. Als Administrator angemeldet, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_3-Verify-instance-status` Ordner und führen Sie den folgenden Python-Befehl aus:

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

<wave-id> Ersetzen Sie ihn durch den entsprechenden Wave-ID-Wert, um den Instanzstatus zu überprüfen. Dieses Skript überprüft den Instanzstartvorgang für alle Quellserver in dieser Welle.

3. Das Skript gibt eine Liste der Serverliste und der Instanz-IDs für die angegebene Welle zurück.
4. Das Skript gibt dann eine Liste mit Zielinstanz-IDs zurück.

Note

Wenn Sie eine Fehlermeldung erhalten, dass die Zielinstanz-ID nicht existiert, wird der Startjob möglicherweise immer noch ausgeführt. Warten Sie einige Minuten, bevor Sie fortfahren.

5. Sie erhalten Instanzstatusprüfungen, aus denen hervorgeht, ob Ihre Ziel-Instances die 2/2-Zustandsprüfungen bestanden haben.

Note

Wenn Ihre Ziel-Instances die 2/2-Zustandsprüfungen beim ersten Mal nicht bestehen, kann das daran liegen, dass der Startvorgang länger dauert. Wir empfehlen, die Integritätsprüfungen etwa eine Stunde nach der ersten Integritätsprüfung ein zweites Mal durchzuführen. Dadurch wird sichergestellt, dass der Startvorgang abgeschlossen ist. Wenn die Integritätsprüfungen beim zweiten Mal fehlschlagen, wenden Sie sich an das [AWSSupport Center](#), um einen Supportfall zu protokollieren.

Fahren Sie die Quellserver im Geltungsbereich herunter

Durch diese Aktivität werden die Quellserver im Geltungsbereich heruntergefahren, die an der Migration beteiligt sind. Nachdem Sie den Replikationsstatus der Quellserver überprüft haben, können Sie die Quellserver herunterfahren, um Transaktionen von den Client-Anwendungen zu den Servern zu beenden. Sie können die Quellserver im Übernahmefenster herunterfahren. Das manuelle Herunterfahren der Quellserver kann fünf Minuten pro Server und bei großen Wellen insgesamt einige Stunden dauern. Stattdessen können Sie dieses Automatisierungsskript ausführen, um alle Ihre Server in der angegebenen Welle herunterzufahren.

Verwenden Sie das folgende Verfahren vom Migrationsautomatisierungsserver aus, um alle an der Migration beteiligten Quellserver herunterzufahren.

1. Melden Sie sich als Administrator an und öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_3-Shutdown-all-servers` Ordner und führen Sie den folgenden Python-Befehl aus:

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

3. <wave-id> Ersetzen Sie ihn durch den entsprechenden Wave-ID-Wert, um die Quellserver herunterzufahren.
3. Das Skript gibt eine Liste der Serverliste und der Instanz-IDs für die angegebene Welle zurück.
4. Das Skript fährt zuerst Windows-Server in der angegebenen Welle herunter. Nachdem die Windows-Server heruntergefahren wurden, wechselt das Skript zur Linux-Umgebung und fordert Sie zur Eingabe der Anmeldeinformationen auf. Nach erfolgreicher Anmeldung fährt das Skript die Linux-Server herunter.

Rufen Sie die Zielinstanz-IP ab

Diese Aktivität ruft die Zielinstanz-IP ab. Wenn das DNS-Update in Ihrer Umgebung ein manueller Prozess ist, müssten Sie die neuen IP-Adressen für alle Zielinstanzen abrufen. Sie können jedoch das Automatisierungsskript verwenden, um die neuen IP-Adressen für alle Instanzen in der angegebenen Welle in eine CSV-Datei zu exportieren.

Verwenden Sie das folgende Verfahren vom Migrationsautomatisierungsserver, um die IPs der Zielinstanz abzurufen.

1. Als Administrator angemeldet, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem `c:\migrations\scripts\script_mgn_4-Get-instance-IP` Ordner und führen Sie den folgenden Python-Befehl aus:

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

<wave-id> Ersetzen Sie ihn durch den entsprechenden Wave-ID-Wert, um die neuen IP-Adressen für die Zielinstanzen abzurufen.

3. Das Skript gibt eine Serverliste und die ID-Informationen der Zielinstanz zurück.
4. Das Skript gibt dann die Zielservers-IP zurück.

Das Skript exportiert den Servernamen und die IP-Adressen in eine CSV-Datei (<wave-id>- <project-name>-Ips.csv) und platziert sie im selben Verzeichnis wie Ihr Migrationsskript (c:\migrations\scripts\script_mgn_4-Get-instance-IP).

Die CSV-Datei enthält Details zu instance_name und instance_IPS. Wenn die Instanz mehr als eine Netzwerkkarte oder IP enthält, werden sie alle aufgelistet und durch Kommas getrennt.

Überprüfen Sie die Verbindungen zum Zielserver

Diese Aktivität überprüft die Verbindungen für den Zielserver. Nachdem Sie die DNS-Einträge aktualisiert haben, können Sie mit dem Hostnamen eine Verbindung zu den Zielinstanzen herstellen. In dieser Aktivität überprüfen Sie, ob Sie sich mithilfe des Remote Desktop Protocol (RDP) oder über Secure Shell (SSH) beim Betriebssystem anmelden können. Sie können sich manuell bei jedem Server einzeln anmelden, es ist jedoch effizienter, die Serververbindung mithilfe des Automatisierungsskripts zu testen.

Verwenden Sie das folgende Verfahren vom Migrationsautomatisierungsserver aus, um die Verbindungen für den Zielserver zu überprüfen.

1. Als Administrator angemeldet, öffnen Sie eine Befehlszeile (CMD.exe).
2. Navigieren Sie zu dem c:\migrations\scripts\script_mgn_4-Verify-server-connection Ordner und führen Sie den folgenden Python-Befehl aus:

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

<wave-id> Ersetzen Sie ihn durch den entsprechenden Wave-ID-Wert, um die neuen IP-Adressen für die Zielinstanzen abzurufen.

Note

Dieses Skript verwendet den Standard-RDP-Port 3389 und den SSH-Port 22. <rdp-port><ssh-port> Bei Bedarf können Sie die folgenden Argumente hinzufügen, um auf die Standardports zurückzusetzen: --rdpPort --sshPort.

3. Das Skript gibt eine Serverliste zurück.
4. Das Skript gibt die Testergebnisse sowohl für den RDP- als auch für den SSH-Zugriff zurück.

Referenz

Dieser Abschnitt enthält Verweise auf die Bereitstellung der Cloud Migration Factory in AWS-Lösung.

Anonymisierte Datenerfassung

Diese Lösung beinhaltet die Option, anonymisierte Betriebsmetriken an AWS zu senden. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. Wenn diese Option aktiviert ist, werden die folgenden Informationen erfasst und an AWS gesendet:

- Lösungs-ID: Die AWS-Lösungs-ID
- Unique ID (UUID): Zufällig generierte, eindeutige Kennung für jede Cloud Migration Factory bei der AWS Lösungsbereitstellung
- Zeitstempel: Zeitstempel der Datenerfassung
- Status: Der Status wird migriert, sobald ein Server mit dieser Lösung in AWS MGN gestartet wird
- Region: Die AWS Region, in der die Lösung bereitgestellt wird

Note

AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der [AWS-Datenschutzrichtlinie](#). Führen Sie die folgenden Schritte aus, bevor Sie die AWS CloudFormation Vorlage starten, um sich von dieser Funktion abzumelden.

1. Laden Sie die [AWS CloudFormation Vorlage](#) auf Ihre lokale Festplatte herunter.
2. Öffnen Sie die AWS CloudFormation Vorlage mit einem Texteditor.
3. Ändern Sie den AWS CloudFormation Vorlagenzuordnungsabschnitt von:

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

auf:

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

4. Melden Sie sich an der [AWS CloudFormation-Konsole](#) an.
5. Wählen Sie Stack erstellen aus.
6. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus.
7. Wählen Sie unter Vorlagendatei hochladen die Option Datei auswählen und wählen Sie die bearbeitete Vorlage von Ihrem lokalen Laufwerk aus.
8. Wählen Sie Weiter und folgen Sie den Schritten unter [Starten des Stacks](#) im Abschnitt Automatisierte Bereitstellung dieses Handbuchs.

Zugehörige Ressourcen

AWS-Schulung

- [Verwenden von AWS-Lösungen: Kurs zum Cloud Migration Factory Skill Builder](#) – Sie erfahren mehr über die Funktionen, Vorteile und die technische Implementierung der Lösung.
- [Nur für AWS-Partner: Erweiterte Migration zu AWS \(technisch, Unterrichtsraumbasiert\)](#) – Sie erfahren, wie Sie Workloads in großem Umfang migrieren und gängige Migrationsmuster behandeln, einschließlich eines praktischen Workshops für Cloud Migration Factory in AWS.

AWS-Services

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

AWS-Ressourcen

- [CloudEndure Migration-Factory-Leitfaden](#)

Mitwirkende

Die folgenden Personen haben zu diesem Dokument beigetragen:

- Aijun-Peng
- Vergissisch
- Entwicklungskar
- Dilshad Hussain
- Gnanasekaranlasam
- Jijo Bol
- Lakshmi Sudhakar Nekk anti
- Bolka Segura
- Phi Nguyen
- Shyam Kumar
- Bol Überschneidung
- Bolemo-Mechanismus
- Vijesh Vijayakumaran Nair
- Wally Lu

Revisionen

Datum	Änderung	
Juni 2020	Erstversion	
Februar 2021	Version v1.1.0: Optionale Migrations-Tracker-Komponente hinzugefügt. Weitere Informationen zu neuen Funktionen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Mai 2021	Version v1.1.1: AWS Lambda-Funktionen wurden aktualisiert, um Python v3.7 zu unterstützen. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
August 2021	Version v2.0.0: Neue Funktion zur Integration in AWS Application Migration Service (AWS MGN). Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
September 2021	Version v2.0.1: Fehlerbehebungen. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Oktober 2021	Version v2.0.2: Fehlerbehebungen. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Juni 2022	Version v3.0.0: Neue Web-Benutzeroberfläche und -Funktionalität zum Ausführen aller Automatisierungsaufgaben direkt über die Benutzeroberfläche mithilfe der neuen Remote-Automatisierungsfunktion. Diese Version entfernt die Anforderungen für den Wechsel zwischen den Befehlszeilen des Automatisierungsservers und der Web-Benutzeroberfläche und bietet eine einzelne Ansicht der Migrationsautomatisierung. Es wurde ein Plattformwechsel für EC2 eingeführt, mit dem die Migration Bereitstellungen neuer EC2-Instances basierend auf den Konfigurationen durchführen kann, die in den Cloud Migration Factory-Datenspeicher geladen sind, wodurch Migrationswellen die Möglichkeit haben, eine Mischung aus Migrationsstrategien zu haben, wobei Plattformwechsel auf EC2 und Hostwechsel	

Datum	Änderung	
	mit MGN über eine einzige Cloud-Migrationskonsole verwaltet werden. Weitere Informationen zu neuen Funktionen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Oktober 2022	Version v3.1.0: Unterstützung für die Bereitstellungstypen Public, Public mit und Private hinzugefügt AWS WAF, die während der CloudFormation Stack-Bereitstellung als Optionen verfügbar sind. Diese Version enthält auch kleinere Updates, die auf Feedback der Benutzer-Community basieren. Weitere Informationen zu neuen Funktionen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Dezember 2022	Version v3.2.0: Optionale Unterstützung für externe Identität sanbieter und die Verwaltung von Gruppen in der CMF-Konsole hinzugefügt. Weitere Informationen zu neuen Funktionen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Dezember 2022	Version v3.2.0: Optionale Unterstützung für externe Identität sanbieter und die Verwaltung von Gruppen in der CMF-Konsole hinzugefügt. Kleinere Updates für andere Comp-Onents. Weitere Informationen zu Aktualisierungen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Januar 2023	Version v3.2.1: Das Python-Anforderungspaket wurde auf 4.1.0 aktualisiert, um Sicherheitsempfehlungen für das Python-Paket abhängiger Zertifizierungen zu minimieren. Ausführliche Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
April 2023	Version v3.2.2: Abgeschwächte Auswirkungen, die durch neue Standardeinstellungen für S3 Object Ownership (ACLs deaktiviert) für alle neuen S3-Buckets verursacht werden. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	

Datum	Änderung	
Juni 2023	Version v3.3.0: Die Automatisierung der Workload-Erfassung von AWS Managed Services (AMS) wurde entfernt; erheblich es Quellcode-Refactoring zur Verbesserung der Wartungsbarkeit zur Unterstützung zukünftiger Versionen; sowie kleinere Updates und Fehlerbehebungen für andere Komponenten. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Oktober 2023	Version v3.3.1: Deutliches Quellcode-Refactoring zur Verbesserung der Wartungsbarkeit zur Unterstützung zukünftiger Versionen sowie kleinere Updates und Fehlerbehebungen für andere Komponenten. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
November 2023	Aktualisierung der Dokumentation: Bestätigen Sie die mit der Lösung verbundenen Kosten-Tags im AppRegistry Abschnitt Überwachung der Lösung mit AWS Service Catalog.	
Dezember 2023	Version v3.3.2: Deutliches Quellcode-Refactoring zur Verbesserung der Wartungsbarkeit zur Unterstützung zukünftiger Versionen sowie kleinere Updates und Fehlerbehebungen für andere Komponenten. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	
Januar 2024	Version v3.3.3: Kleinere Aktualisierungen der IAM-Berechtigungen in Zielkonten und andere Fehlerbehebungen sowie weiterer Quellcode-Refactoring zur Verbesserung der Wartungsbarkeit. Weitere Informationen finden Sie in der Datei CHANGELOG.md im GitHub Repository.	

Hinweise

Die Kunden sind dafür verantwortlich, die Informationen in diesem Dokument selbst unabhängig zu bewerten. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden, noch ändert es diese.

Die Cloud Migration Factory on AWS-Lösung ist gemäß den Bedingungen des [MIT No Attribution](#) lizenziert.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.