



Guida per l'utente

AWS CloudFormation



Versione API 2010-05-15

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS CloudFormation: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è AWS CloudFormation?	1
Semplificazione della gestione dell'infrastruttura	1
Replicazione rapida dell'infrastruttura	1
Semplicità di controllo e rilevamento delle modifiche all'infrastruttura	2
Guida introduttiva con CloudFormation	2
Informazioni correlate	2
Nozioni di base	3
Come CloudFormation funziona	3
Concetti chiave	3
Come CloudFormation funziona	7
Modi per iniziare con CloudFormation	10
Iscrizione a un Account AWS	11
Registrati per un Account AWS	11
Crea un utente con accesso amministrativo	11
Creare il tuo primo stack	13
Prerequisiti	14
Crea uno CloudFormation stack con la console	14
Monitora la creazione dello stack	18
Prova il server web	19
Risoluzione dei problemi	19
Eliminazione	20
Passaggi successivi	21
Best practice	23
Abbreviare il ciclo di feedback per migliorare la velocità di consegna	24
Organizzare gli stack per ciclo di vita e proprietà	24
Utilizzare i riferimenti tra stack per l'esportazione di risorse condivise	25
Verificare le quote per tutti i tipi di risorse	26
Riutilizzare i modelli per replicare gli stack in ambienti multipli	26
Utilizzare i moduli per riutilizzare le configurazioni delle risorse	26
Usa tipi AWS di parametri specifici	27
Utilizzare i vincoli dei parametri	27
Utilizzo degli pseudoparametri per promuovere la portabilità	27
AWS::CloudFormation::InitDa utilizzare per distribuire applicazioni software su istanze Amazon EC2	28

Utilizzare gli script helper più recenti	28
Convalidare i modelli prima di utilizzarli	29
Convalida dei modelli per la conformità ai criteri dell'organizzazione	29
Gestisci tutte le risorse dello stack tramite CloudFormation	29
Creare set di modifiche prima di aggiornare gli stack	30
Utilizzare le policy di stack	30
Utilizzare la revisione del codice e i controlli di revisione per gestire i modelli	31
Aggiorna regolarmente le tue EC2 istanze Amazon	31
Utilizzo dei modelli di	32
Dove vengono archiviati i modelli	33
Convalida dei modelli	33
Guida introduttiva ai modelli	2
Pianifica di utilizzare il modello di riferimento CloudFormation	34
Modelli di esempio	35
formato del modello	35
Struttura del modello	36
Commenti	38
Specifiche	38
Ulteriori informazioni	39
Utilizzo di espressioni regolari	39
Sezioni del modello	40
Resources	42
Parameters	50
Outputs	64
Mappings	70
Metadata	77
Rules	83
Conditions	104
Transform	111
Versione del formato	112
Description	113
Infrastructure Composer	114
Perché usare Infrastructure Composer in modalità CloudFormation console?	114
In che modo questa modalità è diversa dalla console Infrastructure Composer?	114
generatore IAc	115
Considerazioni	116

Autorizzazioni	117
Comandi di uso comune	117
Esegui la migrazione di un modello verso AWS CDK	118
Avvia una scansione delle risorse	118
Visualizza il riepilogo della scansione	123
Crea un modello dalle risorse scansionate	124
Crea uno stack dalle risorse scansionate	129
Risolve le proprietà di sola scrittura	130
Ottieni valori archiviati in altri servizi	135
Considerazioni generali	136
Ottieni il valore di testo non crittografato di Systems Manager	137
Ottieni la stringa sicura di Systems Manager	140
Ottieni il valore di Secrets Manager	143
Ottieni valori AWS	147
Sintassi	147
Pseudoparametri disponibili	148
Esempi	150
Ottieni gli output dello stack	154
Esportazione dei valori di output di uno stack e utilizzo di stack nidificati	154
Considerazioni	155
Elencazione dei valori di output esportati	155
Creazione di elenchi di stack che importano un valore di output esportato	157
Specificare le risorse esistenti in fase di esecuzione	158
Panoramica	158
Esempio	159
Considerazioni	163
Tipi di AWS parametri specifici supportati	163
Tipi di parametri Systems Manager supportati	165
Tipi di parametri di Systems Manager non supportati	166
Procedure guidate	166
Fai riferimento agli output di risorse in un altro stack CloudFormation	167
Peering con un VPC in un altro account	172
Creazione di un'applicazione dimensionata e con carico bilanciato	183
Distribuisci applicazioni su Amazon EC2	196
Aggiornamento di uno stack	206
Esegui distribuzioni ECS blue/green	241

Frammenti di modello	265
Generali	266
Dimensionamento automatico	276
AWS Console di fatturazione	309
AWS CloudFormation	313
CloudFront	320
CloudWatch	332
CloudWatch Registri	338
DynamoDB	377
Amazon EC2	383
Amazon ECS	421
Amazon EFS	444
Elastic Beanstalk	469
Sistema di bilanciamento del carico elastico	474
IAM	476
AWS Lambda	494
AWS OpsWorks	502
Amazon Redshift	511
Amazon RDS	521
Route 53	530
Amazon S3	538
Amazon SNS	546
Amazon SQS	547
Amazon Timestream	548
Windowsstack basati su	577
Stack Windows di bootstrap	578
Usa i CloudFormation tipi di risorse forniti	585
Risorse personalizzate	586
Macro di modello	640
Stack nidificati	658
Condizioni di attesa	665
Crea configurazioni di risorse riutilizzabili con i moduli	671
Considerazioni su quando utilizzare i moduli	673
Comprendere il controllo delle versioni dei moduli	673
Usa i moduli in un modello	675
Utilizzate i parametri per specificare i valori del modulo	676

Risorse del modulo di riferimento	679
Creazione e gestione degli stack	681
Interfacce per la gestione degli stack	683
Creare uno stack	683
Creazione di uno stack	684
Configurare le opzioni dello stack	687
Visualizza l'anteprima della configurazione del tuo stack	689
Visualizza le informazioni sullo stack	691
Aggiorna il tuo modello di stack	693
Comprendi i comportamenti di aggiornamento delle risorse dello stack	695
Aggiorna gli stack utilizzando i set di modifiche	697
Crea un set di modifiche	699
Visualizza un set di modifiche	705
Esegui un set di modifiche	713
Eliminare un set di modifiche	716
Esempio di set di modifiche	717
Set di modifiche per stack nidificati	730
Aggiorna direttamente gli stack	737
Annullare un aggiornamento dello stack	740
Per annullare un aggiornamento dello stack (console)	741
Per annullare un aggiornamento dello stack (AWS CLI)	741
Eliminazione di uno stack	741
Risorse correlate	743
Visualizza gli stack eliminati	743
Monitora l'avanzamento dello stack	744
Visualizza gli eventi dello stack	744
Visualizza il grafico della sequenza temporale di implementazione dello stack	752
Comprendi gli eventi di creazione degli stack	755
Monitora gli aggiornamenti dello stack	757
Rollback di un aggiornamento	759
Determinare la causa di un errore dello stack	764
Opzioni di errore degli stack	765
Riduci il tuo stack in caso di violazione degli allarmi	775
Aggiungi trigger di rollback durante la creazione o l'aggiornamento dello stack	776
Aggiungere i trigger di rollback a un set di modifiche	777
Visualizza i trigger di rollback per uno stack	777

Visualizza i trigger di rollback per un set di modifiche	778
Rileva le modifiche di configurazione non gestite agli stack e alle risorse	778
Cos'è una deviazione?	779
Codici di stato del rilevamento della deviazione	780
Considerazioni sul rilevamento della deviazione	782
Rileva la deriva su un'intera CloudFormation pila	785
Rilevamento della deviazione su singole risorse di stack	790
Risoluzione della deviazione con un'operazione di importazione	794
Importa risorse AWS	804
Importa AWS manualmente le risorse	805
Importa AWS automaticamente le risorse	844
Ripristino di un'operazione di importazione	846
Rifattorizzazione degli stack	851
Come funziona lo stack refactoring	851
Limitazioni dello stack refactoring	852
Rifattorizzazione di uno stack utilizzando il AWS Command Line Interface	856
Supporto per tipi di risorse	858
Usa i link di creazione rapida per creare pile CloudFormation	1053
Formato URL	1053
Esempio	1055
Creazione di uno stack utilizzando un link di creazione rapida	1055
Comandi di esempio per e AWS CLI PowerShell	1056
CancelUpdateStack	1057
ContinueUpdateRollback	1058
CreateStack	1059
Implementazione	1064
DeleteStack	1064
DescribeStackEvents	1066
DescribeStackResource	1067
DescribeStackResources	1069
DescribeStacks	1072
GetTemplate	1076
ListStackResources	1077
ListStacks	1079
UpdateStack	1081
ValidateTemplate	1085

Carica gli artefatti locali in un bucket S3	1088
Gestione degli stack con StackSets	1092
StackSets concetti	1093
Account amministratore e target	1093
AWS CloudFormation StackSets	1094
Modelli di autorizzazione per StackSets	1094
Istanze di stack	1095
StackSet operazioni	1096
StackSet opzioni operative	1097
Tag	1099
StackSets codici di stato	1100
Codici di stato delle istanze di stack	1101
Prerequisiti	1102
Abilita Regioni AWS che siano disabilitati per impostazione predefinita	1103
Concedere autorizzazioni gestite dal cliente	1104
Attiva l'accesso affidabile	1120
Inizia a usare un modello di esempio	1125
Prerequisiti	1126
Crea un modello StackSet con un esempio dalla console	1127
Monitora StackSet la creazione	1129
Visualizza i risultati StackSet	1130
Aggiorna il tuo StackSet	1130
Aggiungi pile al tuo StackSet	1131
Eliminazione	1132
Passaggi successivi	1134
Crea StackSets (autorizzazioni autogestite)	1134
Crea un account StackSet con autorizzazioni autogestite (console)	1135
Crea un file StackSet con autorizzazioni gestite automaticamente (AWS CLI)	1137
Crea StackSets (autorizzazioni gestite dal servizio)	1138
Considerazioni	1138
Crea un account StackSet con autorizzazioni gestite dal servizio (console)	1139
Crea un file StackSet con autorizzazioni gestite dal servizio (AWS CLI)	1142
Abilitare/disabilitare le distribuzioni automatiche	1147
Come funzionano le distribuzioni automatiche	1147
Considerazioni	1147
Abilita o disabilita le distribuzioni automatiche (console)	1148

Abilita o disabilita le distribuzioni automatiche ()AWS CLI	1148
Aggiorna StackSets	1149
Aggiorna la tua StackSet (console)	1149
Aggiorna il tuo StackSet (AWS CLI)	1151
Aggiungi pile a StackSets	1153
Aggiungi pile a StackSet (console)	1153
Aggiungi pile a () StackSet AWS CLI	1155
Sostituisci i parametri sugli stack	1156
Sostituisci i parametri negli stack (console)	1157
Sostituisci i parametri sugli stack ()AWS CLI	1159
Elimina pile da StackSets	1160
Elimina gli stack dalla tua (console) StackSet	1160
Elimina gli stack dal tuo () StackSet AWS CLI	1162
Eliminare StackSets	1164
Eliminare una StackSet (console)	1164
Eliminare un StackSet ()AWS CLI	1164
Eliminare ruoli dei servizi (opzionale)	1165
Attività di controllo dell'account target	1166
Requisiti	1166
CloudFormation modelli per la creazione di funzioni Lambda	1167
Scegli la modalità Concurrency	1168
Come funziona ogni modalità di simultaneità	1168
Scelta tra Tolleranza rigorosa ai guasti e Tolleranza flessibile ai guasti in base alla velocità di implementazione	1171
Scelta della modalità Concurrency (console)	1173
Scelta della modalità Concurrency ()AWS CLI	1174
Rilevamento della deriva attivo StackSets	1175
Come esegue il rilevamento della deriva su CloudFormation un StackSet	1175
Rileva la deriva su una (console) StackSet	1176
Rileva la deriva su un StackSet ()AWS CLI	1178
Interruzione del rilevamento della deriva su un StackSet	1185
Importa pile in StackSets	1185
Importazione di stack gestita automaticamente	1186
Importazione di stack gestita dal servizio	1189
Ripristina le importazioni dello stack	1195
Best practice	1195

Definizione del modello	1196
Creare o aggiungere pile a StackSet	1196
Aggiornamento degli stack in un StackSet	1196
Modelli di esempio	1197
Risoluzione dei problemi	1198
Motivi comuni per operazioni di stack non riuscite	1199
Nuovo tentativo di operazioni di creazione o aggiornamento d stack non riuscite	1199
L'eliminazione dell'istanza di stack non riesce	1200
L'operazione di importazione di stack ha esito negativo	1201
Numero di errori delle istanze dello stack per le operazioni StackSets	1201
Sincronizzazione degli stack con il codice sorgente Git	1208
Come funziona la sincronizzazione Git	1209
Come funziona la sincronizzazione Git	1209
Commenti sulle richieste pull	1210
File di implementazione dello stack	1211
CloudFormation file modello	1212
Repository delle definizioni dei modelli	1212
Prerequisiti	1212
Repository Git	1213
CloudFormation modello	1213
Ruolo IAM	1213
Autorizzazioni richieste	1213
Policy di attendibilità	1215
Crea uno stack dal codice sorgente del repository	1216
Crea uno stack dal codice sorgente del repository	1216
Aggiorna il tuo stack dal tuo repository Git	1218
Abilita i commenti sulle richieste pull	1219
Dashboard di stato	1220
Stato della sincronizzazione Git	1220
Eventi di sincronizzazione più recenti	1221
Stati dello stack supportati	1221
Gestione delle estensioni con il CloudFormation registro	1226
Documentazione correlata	1226
Concetti	1227
Tipi di estensione	1227
Estensioni pubbliche	1228

Estensioni attivate	1228
Visualizza le estensioni disponibili e attivate	1229
Estensioni pubbliche	1230
Ruolo IAM	1231
Utilizza automaticamente nuove versioni delle estensioni	1233
Usa gli alias per fare riferimento alle estensioni	1234
AWS CLI Comandi di uso comune per lavorare con le estensioni pubbliche	1234
Attiva un'estensione pubblica	1235
Aggiorna un'estensione pubblica	1239
Disattiva le estensioni pubbliche	1240
Estensioni private	1242
Autorizzazioni IAM	1242
AWS CLI Comandi comunemente usati per lavorare con estensioni private	1242
Registra un'estensione privata	1243
Annulla la registrazione delle estensioni private	1245
Modifica i dati di configurazione per le estensioni	1246
Autorizzazioni necessarie per utilizzare i riferimenti dinamici	1247
Modifica i dati di configurazione per un'estensione (console)	1247
Modifica i dati di configurazione per un'estensione (AWS CLI)	1248
Registrare i tipi di risorse in AWS Config	1249
Impedire la registrazione di proprietà con dati sensibili in un elemento di configurazione ...	1250
Distribuzione continua	1251
Spiegazione passo per passo: creazione di una pipeline per stack di test e produzione	1251
Prerequisiti	1252
Panoramica della spiegazione passo per passo	1252
Fase 1: modifica dell'artefatto e caricamento in un bucket S3	1253
Fase 2: creazione dello stack della pipeline	1255
Fase 3: Visualizza lo stack WordPress	1260
Fase 4: Eliminazione delle risorse	1261
Consulta anche	1262
Riferimento alle proprietà di configurazione	1262
Proprietà di configurazione (console)	1263
Proprietà di configurazione (oggetto JSON)	1266
Consulta anche	1270
AWS CloudFormation artefatti	1271
File del modello dello stack	1271

File di configurazione del modello	1272
Consulta anche	1273
Utilizzo delle funzioni di sovrascrittura dei parametri con le pipeline CodePipeline	1273
Fn::GetArtifactAtt	1274
Fn::GetParam	1275
Consulta anche	1278
Guida di riferimento ai modelli	1279
Sicurezza	1280
Proteggi gli stack dall'eliminazione	1281
Controllare chi può modificare la protezione da cessazione sugli stack	1283
Impedire gli aggiornamenti delle risorse stack	1283
Esempio di policy stack	1284
Definizione di una policy stack	1285
Impostazione di una policy stack	1289
Aggiornamento delle risorse protette	1290
Modifica di una policy stack	1294
Ulteriori esempi di policy stack	1295
Protezione dei dati	1298
Crittografia a riposo	1299
Crittografia in transito	1300
Riservatezza del traffico Internet	1300
Controlla l'accesso con IAM	1300
Definizione di policy basate sull'identità IAM per CloudFormation	1300
Accettazione delle risorse IAM nei modelli CloudFormation	1309
Gestione delle credenziali per le applicazioni in esecuzione su istanze Amazon EC2	1310
Concessione dell'accesso temporaneo (accesso federato)	1311
Esempi di policy basate su identità	1312
AWS CloudFormation ruolo di servizio	1319
Prevenzione del problema "confused deputy" tra servizi	1320
Richieste FAS e valutazione delle autorizzazioni	1322
Registrazione di chiamate API	1324
CloudFormation informazioni in CloudTrail	1325
Comprensione delle CloudFormation voci dei file di registro	1326
Sicurezza dell'infrastruttura	1330
Resilienza	1331
Convalida della conformità	1331

Analisi della configurazione e delle vulnerabilità	1332
Best practice di sicurezza	1332
Utilizza IAM per controllare gli accessi	1333
Non incorporare le credenziali nei modelli	1333
Utilizzato AWS CloudTrail per registrare CloudFormation le chiamate	1334
AWS PrivateLink	1334
Considerazioni sugli endpoint CloudFormation VPC	1334
Creazione di un endpoint VPC interfaccia per l' CloudFormation	1335
Creazione di una policy di endpoint VPC per l' CloudFormation	1336
Monitoraggio con EventBridge	1338
CloudFormation e panoramica degli eventi di sincronizzazione Git	1339
Autorizzazioni	1341
Creazione di un modello di evento personalizzato	1341
Riferimento ai dettagli sugli eventi	1342
Modifica dello stato delle risorse	1343
Modifica dello stato dello stack	1346
Modifica dello stato di rilevamento della deriva	1348
StackSet Modifica dello stato	1350
StackSet Modifica dello stato dell'istanza Stack	1352
StackSetModifica dello stato dell'operazione	1355
Modifica dello stato di Repository Sync	1356
Modifica dello stato di sincronizzazione delle risorse	1359
Quote	1363
Disponibilità delle funzionalità	1371
StackSets e macro	1372
Risoluzione dei problemi	1373
Guida alla risoluzione dei problemi	1373
Risoluzione degli errori	1374
Impossibile eliminare lo stack	1374
Errore di dipendenza	1375
AWS Config e conflitti AWS Systems Manager	1376
Errore del parametro di analisi durante il passaggio di un elenco	1376
Autorizzazioni IAM insufficienti	1377
Valore non valido o proprietà della risorsa non supportata	1377
Quota superata	1377
Errore di rollback degli stack annidati	1378

Nessun aggiornamento da eseguire	1378
Impossibile stabilizzare una risorsa durante un'operazione di creazione, aggiornamento o eliminazione dello stack	1379
Gruppo di sicurezza non esistente in VPC	1379
Impossibile eseguire il rollback dell'aggiornamento	1380
La condizione di attesa non ha ricevuto il numero richiesto di segnali da un' EC2istanza Amazon	1381
Risorsa rimossa dallo stack ma non eliminata.	1382
Contattare il supporto	1383
Risoluzione dei problemi con Amazon Q	1384
Funzionalità	1384
Come funziona	1384
Prezzi	1385
Disponibilità regionale	1385
Limitazioni	1385
Cronologia dei documenti	1386
Aggiornamenti archiviati	1413
.....	mdxxvi

Che cos'è AWS CloudFormation?

AWS CloudFormation è un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla gestione di tali risorse e più tempo alle applicazioni in esecuzione AWS. Crei un modello che descrive tutte le AWS risorse che desideri (come istanze Amazon o EC2 istanze database Amazon RDS) e CloudFormation si occupa del provisioning e della configurazione di tali risorse per te. Non è necessario creare e configurare singolarmente AWS le risorse e capire cosa dipende da cosa; si occupa di tutto. CloudFormation Gli scenari seguenti mostrano come CloudFormation può essere utile.

Semplificazione della gestione dell'infrastruttura

Per un'applicazione Web scalabile che includa anche un database back-end, puoi utilizzare un gruppo con scalabilità automatica, un load balancer Elastic Load Balancing e un'istanza database Amazon Relational Database Service. Puoi utilizzare ogni singolo servizio per il provisioning di queste risorse e dopo averle create devi configurarle affinché interagiscano. Tutte queste attività possono aggiungere difficoltà e richiedere molto tempo prima ancora che la tua applicazione sia in esecuzione.

È invece possibile creare un CloudFormation modello o modificarne uno esistente. Un modello descrive tutte le risorse e le relative proprietà. Quando utilizzi quel modello per creare uno CloudFormation stack, esegui automaticamente il CloudFormation provisioning del gruppo Auto Scaling, del load balancer e del database. Dopo che lo stack è stato creato con successo, le AWS risorse sono pronte e funzionanti. Puoi eliminare lo stack altrettanto facilmente, il che eliminerà tutte le risorse nello stack. Utilizzando CloudFormation, è possibile gestire facilmente una raccolta di risorse come una singola unità.

Replicazione rapida dell'infrastruttura

Puoi replicare le applicazioni che richiedono una disponibilità aggiuntiva in più Regioni, così se una Regione non è più disponibile, gli utenti possono comunque utilizzare le tue applicazioni in altre Regioni. La difficoltà nel replicare l'applicazione consiste nella necessità di replicare anche le risorse. Non solo è necessario registrare tutte le risorse richieste dalla tua applicazione, ma è necessario anche allestire e configurare tali risorse in ciascuna Regione.

Riutilizza il CloudFormation modello per creare le tue risorse in modo coerente e ripetibile. Per riutilizzare il modello, è sufficiente descrivere le risorse una volta e quindi allestire le stesse risorse più volte in più Regioni.

Semplicità di controllo e rilevamento delle modifiche all'infrastruttura

A volte, potresti voler aggiornare delle risorse sottostanti in modo incrementale. Ad esempio, puoi passare a un tipo di istanza con prestazioni più elevate nella configurazione di avvio di Auto Scaling, in modo da ridurre il numero massimo di istanze nel gruppo Auto Scaling. Se sorgono problemi che l'aggiornamento è completato, potrebbe essere necessario eseguire il rollback dell'infrastruttura alle impostazioni originali. Per eseguire questa operazione manualmente, è necessario ricordare quali risorse sono state modificate, ma anche sapere quali erano le impostazioni originali.

Quando si effettua il provisioning dell'infrastruttura CloudFormation, il CloudFormation modello descrive esattamente quali risorse vengono fornite e le relative impostazioni. Poiché questi modelli sono file di testo, è sufficiente tenere traccia delle differenze nei modelli per monitorare le modifiche alla tua infrastruttura, proprio come gli sviluppatori controllano le revisioni del codice sorgente. Ad esempio, puoi utilizzare un sistema di controllo della versione con i tuoi modelli così da determinare con esattezza le modifiche effettuate, l'autore e il momento. Per annullare le modifiche all'infrastruttura, è sufficiente utilizzare una versione precedente del modello.

Guida introduttiva con CloudFormation

CloudFormation è disponibile tramite la CloudFormation [console AWS CLI](#), [AWS SDKs](#), [l'API](#) e tramite diverse integrazioni.

Per un'introduzione a CloudFormation, vedi [Come CloudFormation funziona](#).

Per iniziare a usare CloudFormation, consulta [Creare il tuo primo stack](#).

Informazioni correlate

Puoi saperne di più CloudFormation in questa guida per l'utente e nelle seguenti risorse:

- Per i dettagli del prodotto e FAQs, consulta la [pagina AWS CloudFormation del prodotto](#).
- Per informazioni sui prezzi, consulta [Prezzi di AWS CloudFormation](#).

Iniziare con CloudFormation

Puoi iniziare a CloudFormation utilizzarlo creando uno stack a partire da un modello di esempio, che ti aiuterà a imparare le basi della creazione di stack. AWS Management Console Un modello è un file di testo che definisce tutte le risorse all'interno di uno stack. Uno stack è l'implementazione di un CloudFormation modello. Da un singolo modello, puoi creare più pile. Ogni stack contiene una raccolta di AWS risorse che possono essere gestite come una singola unità.

CloudFormation è un servizio gratuito; tuttavia, ti verranno addebitate le AWS risorse che includi negli stack alle tariffe correnti per ciascuna di esse. Per ulteriori informazioni sui AWS prezzi, consulta la pagina dei dettagli di ciascun prodotto all'[indirizzo http://aws.amazon.com](http://aws.amazon.com).

Argomenti

- [Come CloudFormation funziona](#)
- [Iscrizione a un Account AWS](#)
- [Creare il tuo primo stack](#)

Come CloudFormation funziona

Questo argomento descrive come CloudFormation funziona e presenta i concetti chiave che è necessario conoscere durante l'utilizzo.

Argomenti

- [Concetti chiave](#)
- [Come funziona CloudFormation](#)
- [Modi per iniziare con CloudFormation](#)

Concetti chiave

Quando lo usi CloudFormation, lavori con modelli e pile. Crei modelli per descrivere AWS le tue risorse e le loro proprietà. Ogni volta che crei uno stack, CloudFormation effettua il provisioning delle risorse descritte nel modello.

Argomenti

- [Modelli](#)

- [Stack](#)
- [Set di modifiche](#)

Modelli

Un CloudFormation modello è un file di testo in formato YAML o JSON. È possibile salvare questi file con qualsiasi estensione, ad esempio, `.yaml`, `.json`, `.template`, `.txt`. CloudFormation utilizza questi modelli come modelli per creare le tue AWS risorse. Ad esempio, in un modello, puoi descrivere un' EC2 istanza Amazon, ad esempio il tipo di istanza, l'ID AMI, le mappature dei dispositivi a blocchi e il nome della relativa coppia di EC2 chiavi Amazon. Ogni volta che si crea uno stack, è possibile specificare anche un modello che CloudFormation utilizza per creare ciò che è stato descritto nel modello.

Ad esempio, se hai creato uno stack con il seguente modello, effettua il CloudFormation provisioning di un'istanza con un ID `ami-0ff8a91507f77f867` AMI, un tipo di `t2.micro` istanza, un nome di `testkey` key pair e un volume Amazon EBS.

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Description: A sample template
Resources:
  MyEC2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: ami-0ff8a91507f77f867
      InstanceType: t2.micro
      KeyName: testkey
      BlockDeviceMappings:
        - DeviceName: /dev/sdm
          Ebs:
            VolumeType: io1
            Iops: 200
            DeleteOnTermination: false
            VolumeSize: 20
```

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
```

```

    "Description": "A sample template",
    "Resources": {
      "MyEC2Instance": {
        "Type": "AWS::EC2::Instance",
        "Properties": {
          "ImageId": "ami-0ff8a91507f77f867",
          "InstanceType": "t2.micro",
          "KeyName": "testkey",
          "BlockDeviceMappings": [
            {
              "DeviceName": "/dev/sdm",
              "Ebs": {
                "VolumeType": "io1",
                "Iops": 200,
                "DeleteOnTermination": false,
                "VolumeSize": 20
              }
            }
          ]
        }
      }
    }
  }
}

```

È anche possibile specificare più risorse in un singolo modello e configurare tali risorse in modo che funzionino insieme. Ad esempio, puoi modificare il modello precedente per includere un indirizzo IP elastico (EIP) e associarlo all' EC2 istanza Amazon, come mostrato nell'esempio seguente:

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: A sample template
Resources:
  MyEC2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: ami-0ff8a91507f77f867
      InstanceType: t2.micro
      KeyName: testkey
      BlockDeviceMappings:
        - DeviceName: /dev/sdm
          Ebs:
            VolumeType: io1

```



```

        Iops: 200
        DeleteOnTermination: false
        VolumeSize: 20
MyEIP:
  Type: 'AWS::EC2::EIP'
  Properties:
    InstanceId: !Ref MyEC2Instance

```

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "A sample template",
  "Resources": {
    "MyEC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId": "ami-0ff8a91507f77f867",
        "InstanceType": "t2.micro",
        "KeyName": "testkey",
        "BlockDeviceMappings": [
          {
            "DeviceName": "/dev/sdm",
            "Ebs": {
              "VolumeType": "io1",
              "Iops": 200,
              "DeleteOnTermination": false,
              "VolumeSize": 20
            }
          }
        ]
      }
    },
    "MyEIP": {
      "Type": "AWS::EC2::EIP",
      "Properties": {
        "InstanceId": {
          "Ref": "MyEC2Instance"
        }
      }
    }
  }
}

```

I modelli precedenti sono incentrati su una singola EC2 istanza Amazon; tuttavia, i CloudFormation modelli dispongono di funzionalità aggiuntive che puoi utilizzare per creare set complessi di risorse e riutilizzare tali modelli in più contesti. Ad esempio, puoi aggiungere parametri di input i cui valori vengono specificati quando crei uno stack. CloudFormation In altre parole, è possibile specificare un valore, ad esempio il tipo di istanza, al momento della creazione di uno stack anziché quando si crea il modello, rendendo il modello più semplice da riutilizzare in situazioni diverse.

Stack

Quando si utilizza CloudFormation, si gestiscono le risorse correlate come una singola unità denominata pila. Puoi creare, aggiornare ed eliminare una raccolta di risorse mediante la creazione, l'aggiornamento e l'eliminazione di stack. Tutte le risorse di uno stack sono definite dal modello dello stack. CloudFormation Supponi di aver creato un modello che include un gruppo Auto Scaling, un load balancer Elastic Load Balancing e un'istanza database Amazon Relational Database Service (Amazon RDS). Per creare queste risorse, crei uno stack inviando il modello che hai creato ed esegui il CloudFormation provisioning di tutte quelle risorse al posto tuo.

Set di modifiche

Per apportare modifiche alle risorse in esecuzione in uno stack, puoi aggiornare lo stack. Prima di apportare modifiche alle risorse, è possibile generare un set di modifiche, che è un riepilogo delle modifiche proposte. I set di modifiche consentono di vedere in che modo le modifiche possono influire sulle risorse in esecuzione, soprattutto nel caso di risorse critiche, prima di applicarle.

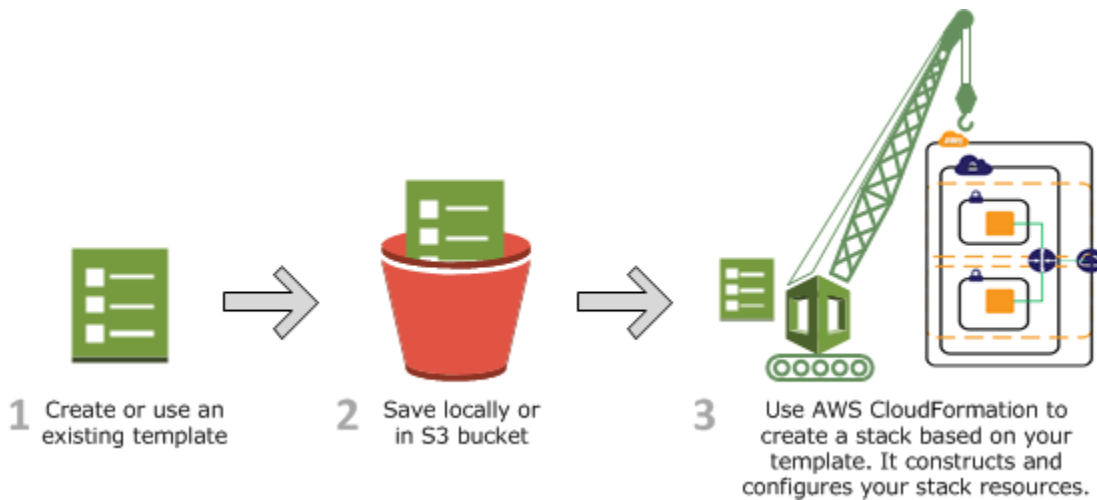
Ad esempio, se modifichi il nome di un'istanza di database Amazon RDS, CloudFormation creerà un nuovo database ed eliminerà quello precedente. Perderai i dati nel vecchio database, a meno che non abbia già eseguito il backup. Se generi un set di modifiche, vedrai che la modifica causerà la sostituzione del database e sarai in grado di pianificare le attività di conseguenza prima di aggiornare lo stack.

Come funziona CloudFormation

Quando si utilizza CloudFormation per creare lo stack, CloudFormation effettua chiamate di servizio sottostanti AWS per fornire e configurare le risorse descritte nel modello. È necessaria l'autorizzazione per creare queste risorse. Ad esempio, per creare EC2 istanze utilizzando CloudFormation, sono necessarie le autorizzazioni per creare istanze. Puoi gestire queste autorizzazioni con [AWS Identity and Access Management](#)(IAM).

Le chiamate effettuate CloudFormation sono tutte dichiarate dal modello. Ad esempio, supponiamo di avere un modello che descrive un' EC2 istanza con un tipo di `t2.micro` istanza. Quando usi

quel modello per creare uno stack, CloudFormation chiama l'API Amazon EC2 create instance e specifica il tipo di istanza come `t2.micro`. Il seguente diagramma riassume il flusso di elaborazione CloudFormation per la creazione di stack.



Per creare uno stack

1. Usa un editor di testo per creare un CloudFormation modello in formato YAML o JSON. Il modello CloudFormation descrive le risorse desiderate e le relative impostazioni. Utilizzalo [Infrastructure Composer](#) per visualizzare e convalidare il tuo modello. Questo ti aiuta ad assicurarti che il modello sia strutturato correttamente e privo di errori di sintassi. Per ulteriori informazioni, consulta [Lavorare con i CloudFormation modelli](#).
2. Salva il modello localmente o in un bucket Amazon S3.
3. Crea uno CloudFormation stack specificando la posizione del file modello, ad esempio un percorso sul tuo computer locale o un URL Amazon S3. Se il modello contiene parametri, è possibile specificare i valori di input quando si crea lo stack. I parametri ti consentono di trasferire valori al modello per personalizzare le risorse ogni volta che si crea uno stack.

Note

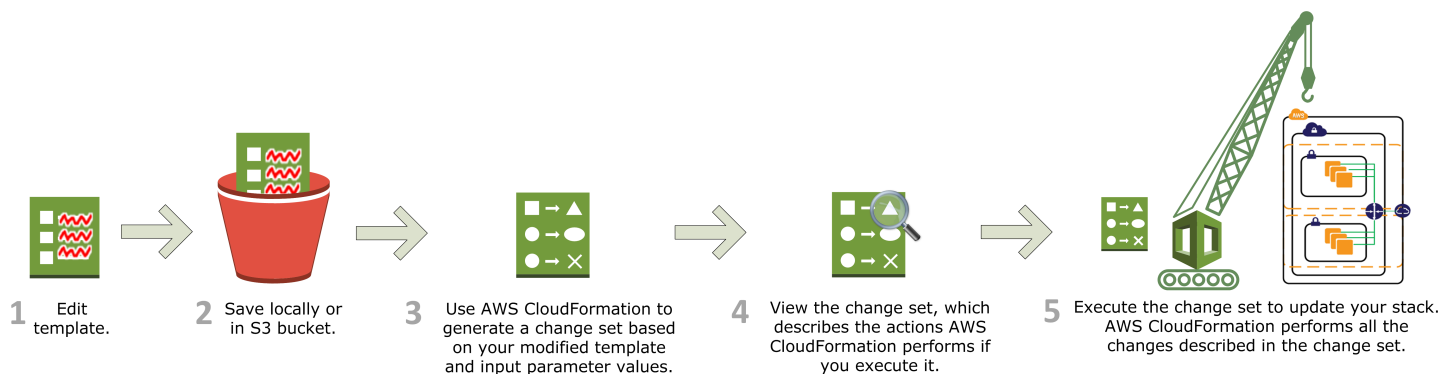
Se specifichi un file modello archiviato localmente, lo CloudFormation carica in un bucket S3 del tuo account. AWS CloudFormation crea un bucket per ogni regione in cui carichi un file modello. I bucket sono accessibili a chiunque disponga delle autorizzazioni Amazon Simple Storage Service (Amazon S3) nel tuo account. AWS Se CloudFormation è già presente un bucket creato da, il modello viene aggiunto a quel bucket.

Puoi utilizzare il tuo bucket e gestirne le autorizzazioni caricando manualmente i modelli su Amazon S3. Quindi ogni volta che crei o aggiorni uno stack, specifica l'URL Amazon S3 di un file del modello.

Dopo che tutte le risorse sono state create, CloudFormation segnala che lo stack è stato creato. È quindi possibile iniziare a utilizzare le risorse nello stack. Se la creazione dello stack non riesce, CloudFormation esegue il rollback delle modifiche eliminando le risorse create.

Aggiornamento di uno stack con un set di modifiche

Quando è necessario aggiornare le risorse del proprio stack, è possibile modificare il modello dello stack. Non è necessario creare un nuovo stack ed eliminare quello precedente. Per aggiornare uno stack, create un set di modifiche inviando una versione modificata del modello di stack originale, valori dei parametri di input diversi o entrambi. CloudFormation confronta il modello modificato con il modello originale e genera un set di modifiche. Il set di modifiche elenca le modifiche proposte. Dopo avere esaminato le modifiche, puoi avviare il set di modifiche per aggiornare lo stack oppure puoi creare un nuovo set di modifiche. Il seguente diagramma riassume il flusso di elaborazione per l'aggiornamento di stack.



Per aggiornare uno stack con un set di modifiche

1. È possibile modificare un modello di CloudFormation utilizzando [Infrastructure Composer](#) o un editor di testo. Per ulteriori informazioni, consulta [Aggiorna il modello dello stack](#).

Quando aggiorni il modello, tieni presente che gli aggiornamenti possono causare interruzioni. A seconda della risorsa e delle proprietà che si intende aggiornare, un aggiornamento potrebbe interrompere o anche sostituire una risorsa esistente. Per ulteriori informazioni, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

2. Salva il CloudFormation modello localmente o in un bucket S3.

3. Creare un set di modifiche specificando lo stack che si desidera aggiornare e la posizione del modello modificato, ad esempio un percorso sul computer locale o un URL Amazon S3. Per ulteriori informazioni sulla creazione di set di modifiche, vedi [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Note

Se specifichi un modello archiviato sul tuo computer locale, carica CloudFormation automaticamente il modello in un bucket S3 del tuo Account AWS

4. Visualizza il set di modifiche per verificare che esegua le modifiche che CloudFormation ti aspetti. Ad esempio, controlla se CloudFormation sostituirà eventuali risorse critiche dello stack. È possibile creare il numero di set di modifiche necessario per includere le modifiche desiderate.

Important

I set di modifiche non indicano se l'aggiornamento dello stack è riuscito. Ad esempio, un set di modifiche non verifica se supererai la [quota](#) di un account, se stai aggiornando una risorsa che non supporta gli aggiornamenti o se non disponi di [autorizzazioni](#) sufficienti per modificare una risorsa, il che può causare il fallimento di un aggiornamento dello stack.

5. Avvia il set di modifiche che desideri applicare al tuo stack. CloudFormation aggiorna lo stack aggiornando solo le risorse che hai modificato e segnala che lo stack è stato aggiornato con successo. Se l'aggiornamento dello stack fallisce, CloudFormation ripristina le modifiche per ripristinare lo stack all'ultimo stato di funzionamento noto.

Modi per iniziare con CloudFormation

Per creare uno CloudFormation stack Hello World con la console, vedi [Creare il tuo primo stack](#).

Per un apprendimento guidato, prova il AWS CloudFormation workshop [Getting Started with](#), che offre un'esperienza pratica con lo sviluppo di modelli.

Iscrizione a un Account AWS

Quando ti iscrivi AWS, il tuo Account AWS viene automaticamente iscritto a tutti i servizi in AWS, inclusi AWS CloudFormation. Se ne hai Account AWS già uno, passa all'argomento successivo. Se non ne hai uno Account AWS, usa la procedura seguente per crearne uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a <https://aws.amazon.com/> e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un dispositivo MFA virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta [Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente di AWS IAM Identity Center .

 Note

Per ulteriori informazioni su come gestire chi ha accesso a cosa, consulta [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#).

Creare il tuo primo stack

Questo argomento illustra come creare il primo CloudFormation stack utilizzando. AWS Management Console Seguendo questo tutorial, imparerai come fornire AWS risorse di base, monitorare gli eventi dello stack e generare output.

Per questo esempio, il CloudFormation modello è scritto in YAML. YAML è un formato leggibile dall'uomo ampiamente utilizzato per definire l'infrastruttura come codice. Man mano che approfondisci CloudFormation, potresti incontrare anche altri modelli in formato JSON, ma per questo tutorial, YAML è stato scelto per la sua leggibilità.

 Note

CloudFormation è gratuito, ma ti verranno addebitati i costi per le risorse Amazon EC2 e Amazon S3 che crei. Tuttavia, se sei alle prime armi AWS, puoi sfruttare il [piano gratuito](#) per ridurre al minimo o eliminare i costi durante questo processo di apprendimento.

Argomenti

- [Prerequisiti](#)
- [Crea uno CloudFormation stack con la console](#)
- [Monitora la creazione dello stack](#)
- [Prova il server web](#)
- [Risoluzione dei problemi](#)
- [Eliminazione](#)
- [Passaggi successivi](#)

Prerequisiti

- Devi avere accesso a un utente o ruolo IAM Account AWS con le autorizzazioni per utilizzare Amazon EC2, Amazon S3 e/o l'accesso come utente amministrativo. CloudFormation
- È necessario disporre di un Virtual Private Cloud (VPC) con accesso a Internet. Questo modello di procedura dettagliata richiede un VPC predefinito, che viene fornito automaticamente con la versione più recente. Account AWS Se non disponi di un VPC predefinito o se è stato eliminato, consulta la sezione sulla risoluzione dei problemi in questo argomento per soluzioni alternative.

Crea uno CloudFormation stack con la console

Per creare uno CloudFormation stack Hello world con la console

1. Apri la [CloudFormation console](#).
2. Scegli Crea stack.
3. Nella pagina Create stack, scegli Build from Infrastructure Composer, quindi Crea in Infrastructure Composer. In questo modo accedi a Infrastructure Composer in modalità CloudFormation console, dove puoi caricare e convalidare il modello di esempio.
4. Per caricare e convalidare il modello di esempio, procedi come segue:
 - a. Scegliete Template. Quindi, copia e incolla il seguente CloudFormation modello nell'editor di modelli:

```
AWSTemplateFormatVersion: 2010-09-09
Description: CloudFormation Template for WebServer with Security Group and EC2
  Instance

Parameters:
  LatestAmiId:
    Description: The latest Amazon Linux 2 AMI from the Parameter Store
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2'

  InstanceType:
    Description: WebServer EC2 instance type
    Type: String
    Default: t2.micro
    AllowedValues:
      - t3.micro
```

```

    - t2.micro
    ConstraintDescription: must be a valid EC2 instance type.

MyIP:
  Description: Your IP address in CIDR format (e.g. 203.0.113.1/32).
  Type: String
  MinLength: '9'
  MaxLength: '18'
  Default: 0.0.0.0/0
  AllowedPattern: '^(\d{1,3}\.){3}\d{1,3}\.\d{1,2}$'
  ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.

Resources:
  WebServerSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Allow HTTP access via my IP address
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: !Ref MyIP

  WebServer:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref LatestAmiId
      InstanceType: !Ref InstanceType
      SecurityGroupIds:
        - !Ref WebServerSecurityGroup
      UserData: !Base64 |
        #!/bin/bash
        yum update -y
        yum install -y httpd
        systemctl start httpd
        systemctl enable httpd
        echo "<html><body><h1>Hello World!</h1></body></html>" > /var/www/html/
index.html

Outputs:
  WebsiteURL:
    Value: !Join
      - ''
      - - http://

```

```
- !GetAtt WebServer.PublicDnsName
```

Description: Website URL

Prima di passare alla fase successiva, prendiamoci un momento per dare un'occhiata al modello e comprendere alcuni CloudFormation concetti chiave.

- La **Parameters** sezione dichiara i valori che possono essere passati al modello quando si crea lo stack. Le risorse specificate più avanti nel modello fanno riferimento a questi valori e utilizzano i dati. I parametri sono un modo efficace per specificare le informazioni che non si desidera memorizzare nel modello stesso. Sono anche un modo per specificare informazioni che potrebbero essere uniche per l'applicazione o la configurazione specifica che stai distribuendo.
- Il modello definisce i seguenti parametri:
 - **LatestAmiId**— Recupera l'ID AMI Amazon Linux 2 più recente dal AWS Systems Manager Parameter Store.
 - **InstanceType**— Consente la selezione del tipo di EC2 istanza (impostazione predefinita: `t2.micro`, consentita: `t3.micro`, `t2.micro`).
 - **MyIP**— Specifica l'intervallo di indirizzi IP per l'accesso HTTP (impostazione predefinita: `0.0.0.0/0`, che consente l'accesso da qualsiasi IP).
- La **Resources** sezione contiene le definizioni delle AWS risorse che si desidera creare con il modello. Le dichiarazioni di risorse sono un modo efficiente per specificare tutte queste impostazioni di configurazione in una sola volta. Quando includi dichiarazioni di risorse in un modello, puoi creare e configurare tutte le risorse dichiarate utilizzando quel modello per creare uno stack. Puoi anche creare nuovi stack dallo stesso modello per avviare configurazioni di risorse identiche.
- Questo modello crea le seguenti risorse:
 - **WebServerSecurityGroup**— Un gruppo EC2 di sicurezza che consente il traffico HTTP in entrata sulla porta 80 dall'intervallo IP specificato.
 - **WebServer**— Un' EC2 istanza con la seguente configurazione:
 - Utilizza la più recente AMI Amazon Linux 2
 - Applica il tipo di istanza selezionato
 - Aggiunge `WebServerSecurityGroup` alla `SecurityGroupIds` proprietà
 - Include uno script di dati utente per installare Apache HTTP Server

- Un nome logico viene specificato all'inizio di ogni dichiarazione di risorse e parametri. Ad esempio, `WebServerSecurityGroup` è il nome logico assegnato alla risorsa del gruppo EC2 di sicurezza. La `Ref` funzione viene quindi utilizzata per fare riferimento a risorse e parametri tramite i rispettivi nomi logici in altre parti del modello. Quando una risorsa fa riferimento a un'altra risorsa, ciò crea una dipendenza tra di esse.
 - La **Outputs** sezione definisce i valori personalizzati che vengono restituiti dopo la creazione dello stack. È possibile utilizzare i valori di output per restituire informazioni dalle risorse dello stack, ad esempio identificatori di risorse o. URLs
 - Il modello definisce un output:
 - **WebsiteURL**— L'URL del server Web distribuito, creato utilizzando il nome DNS pubblico dell' EC2istanza. La `Join` funzione aiuta a combinare il fisso `http://` con la variabile `PublicDnsName` in un'unica stringa, semplificando l'output dell'URL completo del server web.
- b. Scegli Convalida per assicurarti che il codice YAML sia valido prima di caricare il modello.
 - c. Quindi, scegli Crea modello per creare il modello e aggiungerlo a un bucket S3.
 - d. Nella finestra di dialogo che si apre, prendi nota del nome del bucket S3 in modo da poterlo eliminare in un secondo momento. Quindi, scegli Conferma e continua con. CloudFormation Questo ti porta alla CloudFormation console in cui è ora specificato il percorso S3 del tuo modello.
5. Nella pagina Crea stack, scegli Avanti.
 6. Nella pagina Specificare i dettagli dello stack, digita un nome nel campo Nome dello stack. Il nome dello stack non può contenere spazi. Per questo esempio, utilizzare **MyTestStack**.
 7. In Parametri, specificate i valori dei parametri come segue:
 - `LatestAmild`: per impostazione predefinita, è impostata sull'ultima AMI Amazon Linux 2.
 - `InstanceType`: Scegli `t2.micro` o `t3.micro` per il tipo di istanza. EC2

 Note

Se non lo utilizzi AWS, puoi utilizzare il piano gratuito per avviare e utilizzare un'`t2.micro`istanza gratuitamente per 12 mesi (nelle regioni in cui non `t2.micro` è disponibile, puoi utilizzare un'`t3.micro`istanza al di sotto del piano gratuito).

- `MyIP`: Specificate il vostro indirizzo IP pubblico effettivo con un `/32` suffisso. Il `/32` suffisso viene utilizzato nella notazione CIDR per specificare che è consentito un singolo indirizzo IP.

Significa essenzialmente consentire il traffico da e verso questo indirizzo IP specifico e nessun altro.

8. Scegli Avanti due volte per andare alla pagina Rivedi e crea. Per questo tutorial, puoi lasciare le impostazioni predefinite nella pagina Configura le opzioni dello stack così come sono.
9. Rivedi le informazioni per lo stack. Quando si è soddisfatti delle impostazioni, seleziona Submit (Invia).

Monitora la creazione dello stack

Dopo aver scelto Invia, CloudFormation inizia a creare le risorse specificate nel modello.

Il nuovo stack, **MyTestStack**, viene visualizzato nell'elenco nella parte superiore della CloudFormation console. Il suo stato dovrebbe essere `CREATE_IN_PROGRESS`. È possibile vedere lo stato dettagliato di uno stack visualizzandone gli eventi.

Visualizzazione degli eventi per lo stack

1. Sulla CloudFormation console, scegli lo stack **MyTestStack** nell'elenco.
2. Nel riquadro dei dettagli dello stack, scegliere la scheda Events (Eventi).

La console aggiorna automaticamente l'elenco di eventi con gli eventi più recenti ogni 60 secondi.

La scheda Events (Eventi) mostra tutte le fasi principali nella creazione dello stack, ordinate per orario dell'evento, con gli ultimi eventi nella parte superiore.

Il primo evento (nella parte inferiore dell'elenco di eventi) è l'inizio del processo di creazione dello stack:

```
2024-12-23 18:54 UTC-7 MyTestStack CREATE_IN_PROGRESS User initiated
```

Di seguito vengono mostrati tutti gli eventi che segnano l'inizio e il completamento della creazione di ogni risorsa. Ad esempio, la creazione dell' EC2 istanza genera le seguenti voci:

```
2024-12-23 18:59 UTC-7 WebServer CREATE_COMPLETE
```

```
2024-12-23 18:54 UTC-7 WebServer CREATE_IN_PROGRESS Resource creation initiated
```

L'EVENTO `CREATE_IN_PROGRESS` viene registrato quando CloudFormation segnala che ha iniziato a creare la risorsa. L'evento `CREATE_COMPLETE` viene registrato quando la risorsa viene creata senza errori.

Una volta CloudFormation creato con successo lo stack, vedrai il seguente evento nella parte superiore della scheda Eventi:

```
2024-12-23 19:17 UTC-7 MyTestStack CREATE_COMPLETE
```

Se non CloudFormation riesce a creare una risorsa, segnala un `CREATE_FAILED` evento e, per impostazione predefinita, ripristina lo stack ed elimina tutte le risorse che sono state create. La colonna Status Reason (Motivo dello stato) mostra il problema che ha causato l'errore.

Dopo aver creato lo stack, puoi andare alla scheda Risorse per visualizzare l'EC2 istanza e il gruppo di sicurezza che hai creato.

Prova il server web

Dopo aver creato correttamente lo stack, vai alla scheda Output nella CloudFormation console. Cerca il campo WebsiteURL. Questo conterrà l'URL pubblico della tua istanza. EC2

Apri un browser e vai all'URL elencato in WebsiteURL. Dovresti vedere un semplice "Hello World!" messaggio visualizzato nel browser.

Ciò conferma che l'EC2 istanza esegue Apache HTTP Server e serve una pagina Web di base.

Risoluzione dei problemi

Se si verifica un rollback durante la creazione dello stack, potrebbe essere dovuto alla mancanza di un VPC. Ecco come risolvere questo problema.

Nessun VPC predefinito disponibile

Il modello in questa procedura dettagliata richiede un VPC predefinito. Se la creazione dello stack fallisce a causa di errori di disponibilità del VPC o della sottorete, potresti non avere un VPC predefinito nel tuo account. Sono disponibili le seguenti opzioni:

- Crea un nuovo VPC predefinito: puoi creare un nuovo VPC predefinito tramite la console Amazon VPC. Per istruzioni, consulta [Creare un VPC predefinito nella Amazon VPC](#) User Guide.

- Modifica il modello per specificare una sottorete: se disponi di un VPC non predefinito, puoi modificare il modello per specificare in modo esplicito il VPC e la sottorete. IDs Aggiungi il seguente parametro al modello:

```
SubnetId:
  Description: The subnet ID to launch the instance into
  Type: AWS::EC2::Subnet::Id
```

Quindi, aggiorna la `WebServer` risorsa per includere l'ID della sottorete:

```
WebServer:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref LatestAmiId
    InstanceType: !Ref InstanceType
    SecurityGroupIds:
      - !Ref WebServerSecurityGroup
    SubnetId: !Ref SubnetId
    UserData: !Base64 |
      #!/bin/bash
      yum update -y
      yum install -y httpd
      systemctl start httpd
      systemctl enable httpd
      echo "<html><body><h1>Hello World!</h1></body></html>" > /var/www/html/
index.html
```

Durante la creazione dello stack, è necessario specificare una sottorete con accesso a Internet affinché il server Web sia raggiungibile.

Eliminazione

Per assicurarti che non ti vengano addebitati servizi indesiderati, puoi eseguire una pulizia eliminando lo stack e le relative risorse. Puoi anche eliminare il bucket S3 che memorizza il modello dello stack.

Eliminare lo stack e delle relative risorse

1. Apri la [CloudFormation console](#).
2. Nella pagina Pile, seleziona l'opzione accanto al nome dello stack che hai creato (**MyTestStack**), quindi scegli Elimina.

3. Quando viene richiesta la conferma, seleziona Delete (Elimina).
4. Monitora l'avanzamento del processo di eliminazione dello stack nella scheda Evento. Lo stato di **MyTestStack** cambia in DELETE_IN_PROGRESS. Una volta CloudFormation completata l'eliminazione dello stack, lo rimuove dall'elenco.

Se hai finito di lavorare con il modello di esempio e non hai più bisogno del tuo bucket Amazon S3, eliminalo. Prima di poter eliminare un bucket, devi prima svuotarlo. Lo svuotamento di un bucket comporta l'eliminazione di tutti gli oggetti in esso contenuti.

Per svuotare ed eliminare il bucket Amazon S3

1. Apri la [console Amazon S3](#).
2. Nel riquadro di navigazione sul lato sinistro della console scegliere Bucket.
3. Nell'elenco Bucket, seleziona l'opzione accanto al nome del bucket che hai creato per questo tutorial, quindi scegli Empty.
4. Nella pagina Svuota il bucket, conferma che desideri svuotare il bucket digitando **permanently delete** nel campo di testo, quindi scegli Svuota.
5. Monitorare l'avanzamento del processo di svuotamento del bucket nella pagina Svuota bucket: stato.
6. Per tornare all'elenco dei bucket, scegliere Exit (Esci).
7. Seleziona l'opzione accanto al nome del bucket, quindi scegli Elimina.
8. Quando viene richiesta la conferma, digita il nome del bucket, quindi scegli Elimina bucket.
9. Monitora l'avanzamento del processo di eliminazione del bucket dall'elenco dei bucket. Quando Amazon S3 completa l'eliminazione del bucket, lo rimuove dall'elenco.

Passaggi successivi

Complimenti! Hai creato con successo uno stack, monitorato le sue creazioni e ne hai utilizzato l'output.

Per continuare a imparare:

- Scopri di più sui modelli per crearne di personalizzati. Per ulteriori informazioni, consulta [Lavorare con i CloudFormation modelli](#).

- Prova il AWS CloudFormation workshop [Getting Started with](#) per ulteriori esercitazioni pratiche sulla creazione di modelli.
- Per una versione abbreviata di [Getting Started with AWS CloudFormation](#), consulta. [Distribuisci applicazioni su Amazon EC2](#) Questo argomento descrive lo stesso scenario di utilizzo di uno script di CloudFormation supporto per avviare un'istanza Amazon EC2. `cfn-init`

CloudFormation migliori pratiche

Le best practice sono raccomandazioni che possono aiutarti a utilizzarlo in modo CloudFormation più efficace e sicuro durante l'intero flusso di lavoro. Scopri come pianificare e organizzare gli stack, creare modelli che descrivono le risorse e le applicazioni software in esecuzione su di esse e come gestire i tuoi stack e le loro risorse. Le seguenti best practice si basano sull'esperienza reale dei clienti attuali. CloudFormation

Pianificazione e organizzazione

- [Abbreviare il ciclo di feedback per migliorare la velocità di consegna](#)
- [Organizzare gli stack per ciclo di vita e proprietà](#)
- [Utilizzare i riferimenti tra stack per l'esportazione di risorse condivise](#)
- [Utilizza IAM per controllare gli accessi](#)
- [Riutilizzare i modelli per replicare gli stack in ambienti multipli](#)
- [Verificare le quote per tutti i tipi di risorse](#)
- [Utilizzare i moduli per riutilizzare le configurazioni delle risorse](#)

Creazione di modelli

- [Non incorporare le credenziali nei modelli](#)
- [Usa tipi AWS di parametri specifici](#)
- [Utilizzare i vincoli dei parametri](#)
- [Utilizzo degli pseudoparametri per promuovere la portabilità](#)
- [AWS::CloudFormation::Init Da utilizzare per distribuire applicazioni software su istanze Amazon EC2](#)
- [Utilizzare gli script helper più recenti](#)
- [Convalidare i modelli prima di utilizzarli](#)

Gestione degli stack

- [Gestisci tutte le risorse dello stack tramite CloudFormation](#)
- [Creare set di modifiche prima di aggiornare gli stack](#)
- [Utilizzare le policy di stack](#)
- [Utilizzato AWS CloudTrail per registrare CloudFormation le chiamate](#)
- [Utilizzare la revisione del codice e i controlli di revisione per gestire i modelli](#)

- [Aggiorna regolarmente le tue EC2 istanze Amazon](#)

Abbreviare il ciclo di feedback per migliorare la velocità di consegna

Adotta pratiche e strumenti che ti aiutino ad abbreviare il ciclo di feedback per l'infrastruttura che descrivi con i modelli. CloudFormation Ciò include l'esecuzione tempestiva di linting e test dei modelli nella tua workstation; quando esegui l'operazione, hai l'opportunità di scoprire potenziali problemi di sintassi e configurazione anche prima di inviare i tuoi contributi a un repository di codici sorgente. L'individuazione anticipata di tali problemi contribuisce a evitare che raggiungano ambienti formali del ciclo di vita, ad esempio sviluppo, garanzia di qualità e produzione. Questo approccio di test anticipato e anticipo dell'errore (fail fast) offre i vantaggi di ridurre i tempi di attesa per rilavorazioni, ridurre le potenziali aree di impatto e aumentare il livello di affidabilità delle operazioni di provisioning.

Le scelte di strumenti che vi aiutano a raggiungere pratiche rapide includono [AWS CloudFormation Linter](#) (`cfn-lint`) e gli strumenti da riga di comando. [TaskCat Lo cfn-lint strumento offre la possibilità di convalidare i CloudFormation modelli in base alle specifiche delle risorse.](#) [AWS CloudFormation](#) Ciò include la verifica di valori validi per le proprietà delle risorse e procedure consigliate. I plugin per `cfn-lint` sono [disponibili per diversi editor di codice](#); questo vi dà la possibilità di visualizzare i problemi all'interno dell'editor e di ottenere un feedback diretto da linter. Puoi anche scegliere di integrarlo `cfn-lint` nella configurazione del tuo repository di codice sorgente, in modo da poter eseguire la convalida del modello quando inserisci i tuoi contributi. Per maggiori informazioni, consulta [Git pre-commit validation of AWS CloudFormation templates with cfn-lint](#). Dopo aver eseguito il linting iniziale e risolto `cfn-lint` eventuali problemi, puoi utilizzarli TaskCat per testare i tuoi modelli creando programmaticamente degli stack nel formato che preferisci. Regioni AWS TaskCat genera anche un rapporto con i voti per ogni regione scelta. pass/fail

[Per una step-by-step guida pratica su come utilizzare entrambi gli strumenti per abbreviare il ciclo di feedback, segui il laboratorio di Linting and Testing del Workshop.](#) [AWS CloudFormation](#)

Organizzare gli stack per ciclo di vita e proprietà

Usa il ciclo di vita e la proprietà delle tue AWS risorse per decidere quali risorse inserire in ogni stack. Inizialmente, è possibile inserire tutte le risorse in un unico stack, ma via via che le dimensioni e l'ambito si ampliano, la gestione di un singolo stack può essere complessa e dispendiosa in termini di tempo. Raggruppando le risorse con cicli di vita e proprietà comuni, i proprietari possono apportare modifiche ai loro set di risorse con processi e pianificazioni personali, senza interferire con altre risorse.

Ad esempio, immagina un team di sviluppatori e ingegneri che possiede un sito Web ospitato su istanze Amazon EC2 Auto Scaling con un sistema di bilanciamento del carico. Poiché il sito Web ha il proprio ciclo di vita e viene gestito dal team dei siti Web, è possibile creare uno stack per il sito Web e le sue risorse. Ora immaginiamo che il sito Web utilizza anche database di back-end ubicati in un altro stack, di proprietà e gestito dagli amministratori del database. Quando il team dei siti Web o il team di database devono aggiornare le proprie risorse, possono farlo senza influenzare lo stack dell'altra parte. Se tutte le risorse fossero in un singolo stack, coordinare e comunicare gli aggiornamenti sarebbe complicato.

Per ulteriori informazioni su come organizzare gli stack, puoi usare due framework comuni: un'architettura multilivello e un'architettura orientata ai servizi (SOA).

L'architettura multilivello organizza gli stack in più livelli orizzontali creati uno sull'altro, in cui ogni livello dipende dal livello direttamente sottostante. Possono essere presenti uno o più stack in ciascun livello, ma all'interno di ciascun livello lo stack deve disporre di risorse AWS con cicli di vita e proprietà simili.

Con un'architettura orientata ai servizi, è possibile organizzare i grandi problemi aziendali in parti semplici da gestire. Ognuna di queste parti è un servizio che ha uno scopo ben definito e rappresenta un'unità completa di funzionalità. È possibile mappare questi servizi a uno stack, ognuno con proprietari e ciclo di vita propri. Questi servizi (stack) possono essere cablati insieme in modo che possano interagire l'uno con l'altro.

Utilizzare i riferimenti tra stack per l'esportazione di risorse condivise

Quando organizzi le AWS risorse in base al ciclo di vita e alla proprietà, potresti voler creare uno stack che utilizzi risorse che si trovano in un altro stack. È possibile codificare i valori o utilizzare i parametri di input per passare i nomi delle risorse e. IDs Tuttavia, questi metodi possono rendere i modelli difficili da riutilizzare o possono aumentare i costi per attivare uno stack. Utilizza invece i riferimenti tra stack per esportare le risorse da uno stack, in modo che altri stack possano utilizzarli. Stack possono utilizzare le risorse esportate chiamandole con la funzione `Fn::ImportValue`.

Ad esempio, potresti volere un stack di rete che includa un VPC, un gruppo di sicurezza e una sottorete. Vuoi che tutte le applicazioni Web pubbliche utilizzino queste risorse. Esportando le risorse, consenti a tutti gli stack con applicazioni Web pubbliche di utilizzarle. Per ulteriori informazioni, consulta [Ottieni gli output esportati da uno stack distribuito CloudFormation](#).

Verificare le quote per tutti i tipi di risorse

Prima di avviare uno stack, assicurati di poter creare tutte le risorse che desideri senza raggiungere i limiti del tuo account. AWS Se raggiungi un limite, CloudFormation non creerà correttamente lo stack finché non aumenterai la quota o eliminerai risorse extra. Ogni servizio può avere vari limiti di cui devi essere a conoscenza prima di avviare uno stack. Ad esempio, per impostazione predefinita, puoi avviare solo 2000 CloudFormation pile per regione nel tuo Account AWS. Per ulteriori informazioni sui limiti e su come aumentare i limiti predefiniti, consulta la [Quote di servizio di AWS](#) nella Riferimenti generali di AWS.

Riutilizzare i modelli per replicare gli stack in ambienti multipli

Dopo aver configurato stack e risorse, puoi riutilizzare i modelli per replicare l'infrastruttura in più ambienti. Ad esempio, puoi creare ambienti di sviluppo, di test e di produzione per testare le modifiche prima di implementarle nella produzione. Per rendere riutilizzabili i modelli, utilizza le sezioni dedicate ai parametri, alle mappature e alle condizioni, in modo da poter personalizzare lo stack quando lo crei. Ad esempio, per i tuoi ambienti di sviluppo, puoi specificare un tipo di istanza a un costo inferiore rispetto all'ambiente di produzione, ma con tutte le altre configurazioni e impostazioni invariate. Per ulteriori informazioni su parametri, mappature e condizioni, consulta [CloudFormation sezioni modello](#).

Utilizzare i moduli per riutilizzare le configurazioni delle risorse

Con la crescita dell'infrastruttura, possono emergere schemi comuni in cui gli stessi componenti vengono dichiarati in ciascun modello. I moduli sono un modo per creare pacchetti di configurazioni delle risorse per l'inclusione su modelli di stack, in modo trasparente, gestibile e ripetibile. I moduli possono incapsulare configurazioni di servizio comuni e best practice come blocchi predefiniti modulari e personalizzabili da includere nei modelli di stack.

Questi elementi costitutivi possono riguardare una singola risorsa, come le best practice per la definizione di un'istanza Amazon Elastic Compute Cloud (Amazon EC2), oppure possono riguardare più risorse, per definire modelli comuni di architettura applicativa. Questi elementi costitutivi possono essere annidati in altri moduli, in modo da poter raggruppare le best practice in elementi costitutivi di livello superiore. CloudFormation i moduli sono disponibili nel [CloudFormation registro](#), quindi puoi usarli proprio come risorse native. Quando si utilizza un CloudFormation modulo, il modello del modulo viene espanso nel modello di consumo, il che consente di accedere alle risorse all'interno del

modulo utilizzando [Ref](#) o [Fn::GetAtt](#). Per ulteriori informazioni, consulta [Crea configurazioni di risorse riutilizzabili che possono essere incluse nei modelli con moduli CloudFormation](#).

Usa tipi AWS di parametri specifici

Se il modello richiede input per valori AWS specifici esistenti, come Amazon Virtual Private Cloud esistente IDs o il nome di una coppia di EC2 chiavi Amazon, utilizza tipi di parametri AWS specifici. Ad esempio, puoi specificare un parametro come `typeAWS::EC2::KeyPair::KeyName`, che accetta il nome di una coppia di chiavi esistente presente nella tua regione Account AWS e nella regione in cui stai creando lo stack. CloudFormation può convalidare rapidamente i valori per tipi di parametri AWS specifici prima di creare lo stack. Inoltre, se usi la CloudFormation console, CloudFormation mostra un elenco a discesa di valori validi, in modo da non dover cercare o memorizzare i nomi corretti dei IDs VPC o delle key pair. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#).

Utilizzare i vincoli dei parametri

Con i vincoli, puoi descrivere i valori di input consentiti in modo che vengano rilevati tutti i valori non validi prima di creare uno CloudFormation stack. Puoi impostare vincoli, quali lunghezza minima e massima e schemi consentiti. Ad esempio, puoi impostare vincoli sul valore del nome utente di un database perché abbia almeno 8 caratteri e contenga solo caratteri alfanumerici. Per ulteriori informazioni, consulta [CloudFormation Parameters sintassi del modello](#).

Utilizzo degli pseudoparametri per promuovere la portabilità

È possibile utilizzare gli [pseudoparametri](#) nei modelli come argomenti di [funzioni intrinseche](#), come `Ref` e `Fn::Sub`. Gli pseudo parametri sono parametri predefiniti da CloudFormation. Non vengono dichiarati nel modello. L'utilizzo di pseudo parametri nelle funzioni intrinseche aumenta la portabilità dei modelli di stack tra regioni e account.

Ad esempio, immagina di voler creare un modello in cui, per una determinata proprietà della risorsa, devi specificare il [nome della risorsa Amazon](#) (ARN) di un'altra risorsa esistente. In questo caso, la risorsa esistente è una risorsa [archivio parametri AWS Systems Manager](#) con il seguente ARN: `arn:aws:ssm:us-east-1:123456789012:parameter/MySampleParameter`. Dovrai adattare il [formato ARN](#) alla AWS partizione di destinazione, alla regione e all'ID account. Invece di codificare in modo fisso questi valori, puoi utilizzare gli pseudoparametri `AWS::Partition`, `AWS::Region` e `AWS::AccountId` per rendere il tuo modello più portabile. In questo caso,

l'esempio seguente mostra come concatenare elementi in un ARN con: CloudFormation !Sub 'arn:\${AWS::Partition}:ssm:\${AWS::Region}:\${AWS::AccountId}:parameter/MySampleParameter

Per un altro esempio, supponiamo di voler condividere risorse o configurazioni su più stack. In questo esempio, supponiamo di aver creato una [sottorete](#) per il VPC e quindi esportato il relativo ID per utilizzarlo con altri stack nella stessa regione. Account AWS In un altro stack, fai riferimento al valore esportato dell'ID di sottorete quando descrivi un'istanza Amazon. EC2 Per un esempio dettagliato dell'utilizzo del campo di output Export e della funzione intrinseca Fn::ImportValue, consulta [Fai riferimento agli output di risorse in un altro stack CloudFormation](#).

Le esportazioni dello stack devono essere uniche per account e regione. Quindi, in questo caso, puoi utilizzare lo pseudoparametro AWS::StackName per creare un prefisso per l'esportazione. Poiché anche i nomi degli stack devono essere univoci per account e regione, l'utilizzo di questo pseudo parametro come prefisso aumenta la possibilità di avere un nome di esportazione univoco, promuovendo al contempo un approccio riutilizzabile tra gli stack da cui si esportano i valori. In alternativa, puoi utilizzare un prefisso di tua scelta.

AWS::CloudFormation::Init Da utilizzare per distribuire applicazioni software su istanze Amazon EC2

Quando avvii gli stack, puoi installare e configurare applicazioni software su EC2 istanze Amazon utilizzando lo script di cfn-init supporto e la risorsa AWS::CloudFormation::Init Utilizzando AWS::CloudFormation::Init, puoi descrivere le configurazioni che desideri, invece di scrivere script delle fasi procedurali. Puoi anche aggiornare le configurazioni senza ricreare le istanze. E se qualcosa va storto con la tua configurazione, CloudFormation genera log che puoi usare per esaminare i problemi.

Nel modello, specifica gli stati di installazione e configurazione nella risorsa

AWS::CloudFormation::Init. Per una procedura dettagliata che mostra come usare cfn-init e AWS::CloudFormation::Init, vedi. [Distribuisce applicazioni su Amazon EC2](#)

Utilizzare gli script helper più recenti

Gli script di CloudFormation supporto vengono aggiornati periodicamente. Assicurati di includere il comando seguente nella proprietà UserData del modello prima di chiamare gli script helper: ti accerterai così che le istanze avviate recuperino gli script helper più recenti.

```
yum install -y aws-cfn-bootstrap
```

Per ulteriori informazioni su come ottenere gli script di supporto più recenti, consultate il [riferimento agli script di CloudFormation supporto nella Template Reference Guide](#). AWS CloudFormation

Convalidare i modelli prima di utilizzarli

Prima di utilizzare un modello per creare o aggiornare uno stack, puoi utilizzarlo per convalidarlo. CloudFormation La convalida di un modello può aiutarti a catturare la sintassi e alcuni errori semantici, come le dipendenze circolari, prima CloudFormation di creare qualsiasi risorsa. Se si utilizza la CloudFormation console, la console convalida automaticamente il modello dopo aver specificato i parametri di input. Per l' CloudFormation API AWS CLI or, utilizza il comando [validate-template](#) CLI o l'operazione [ValidateTemplate](#) API.

Durante la convalida, verifica CloudFormation innanzitutto se il modello è JSON valido. Se non lo è, CloudFormation verifica se il modello è in un formato YAML valido. Se entrambi i controlli falliscono, CloudFormation restituisce un errore di convalida del modello.

Convalida dei modelli per la conformità ai criteri dell'organizzazione

Puoi anche convalidare il modello per verificarne la conformità alle linee guida della politica dell'organizzazione. AWS CloudFormation Guard (`cfn-guard`) è uno strumento di interfaccia a riga di comando (CLI) open source che fornisce policy-as-code un linguaggio per definire regole in grado di verificare le configurazioni delle risorse sia richieste che proibite. Consente quindi di convalidare i modelli rispetto a tali regole. Ad esempio, gli amministratori possono stabilire delle regole per garantire che gli sviluppatori creino sempre dei bucket Amazon S3 crittografati.

È possibile `cfn-guard` utilizzarlo localmente, durante la modifica dei modelli, o automaticamente come parte di una CI/CD pipeline per interrompere la distribuzione di risorse non conformi.

Inoltre, `cfn-guard` include una funzionalità che consente di estrarre regole dai modelli conformi esistenti. `rulegen` CloudFormation

Per ulteriori informazioni, consulta il repository [cfn-guard su](#). GitHub

Gestisci tutte le risorse dello stack tramite CloudFormation

Dopo aver avviato uno stack, utilizza la CloudFormation [console](#), l'[API](#) o la [AWS CLI](#) per aggiornare le risorse nello stack. Non apportare modifiche alle risorse dello stack al di fuori di. CloudFormation

In caso contrario, potrebbe crearsi una mancata corrispondenza tra il modello dello stack e lo stato attuale delle risorse dello stack, con conseguenti possibili errori durante l'aggiornamento o l'eliminazione dello stack. Questo fenomeno è noto come deriva. Se viene apportata una modifica a una risorsa esterna al CloudFormation modello e si aggiorna lo stack, le modifiche apportate direttamente alla risorsa verranno eliminate e la configurazione della risorsa tornerà alla configurazione nel modello.

Per ulteriori informazioni sulla deriva, vedere. [Cos'è una deviazione?](#)

Per ulteriori informazioni sull'aggiornamento degli stack, consulta. [Aggiornamento di uno stack](#)

Creare set di modifiche prima di aggiornare gli stack

I set di modifiche consentono di vedere in che modo le modifiche proposte a uno stack potrebbero influire sulle risorse in esecuzione prima di implementarle. CloudFormation non apporta modifiche allo stack finché non esegui il set di modifiche, consentendoti di decidere se procedere con le modifiche proposte o creare un altro set di modifiche.

Utilizza i set di modifiche per verificare in che modo le modifiche possono influire sulle risorse in esecuzione, soprattutto nel caso di risorse critiche. Ad esempio, se modifichi il nome di un'istanza di database Amazon RDS, CloudFormation creerà un nuovo database ed eliminerà quello vecchio; perderai i dati nel vecchio database a meno che tu non ne abbia già eseguito il backup. Se generi un set di modifiche, vedrai che la modifica sostituirà il database. Questo può aiutarti nella pianificazione prima di aggiornare il tuo stack. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Utilizzare le policy di stack

Le policy di stack consentono di proteggere le risorse di stack critiche da aggiornamenti involontari che potrebbero causare l'interruzione o persino la sostituzione delle risorse stesse. Una policy di stack è un documento JSON che descrive quali operazioni di aggiornamento possono essere eseguite su risorse definite. Specifica una policy di stack ogni volta che crei uno stack con risorse critiche.

Durante l'aggiornamento di uno stack, devi specificare esplicitamente le risorse protette da aggiornare. In caso contrario, non verranno apportate modifiche a tali risorse. Per ulteriori informazioni, consulta [Impedire gli aggiornamenti delle risorse stack](#).

Utilizzare la revisione del codice e i controlli di revisione per gestire i modelli

I tuoi modelli di stack descrivono la configurazione delle tue AWS risorse, come i valori delle loro proprietà. Per rivedere le modifiche e mantenere un'accurata cronologia delle risorse, utilizzare la revisione del codice e i controlli di revisione. Questi metodi possono aiutarti a monitorare le modifiche tra diverse versioni dei tuoi modelli, il che è utile per tenere traccia delle modifiche alle risorse di stack. Inoltre, mantenendo una cronologia, è sempre possibile ripristinare lo stack a una determinata versione del modello.

Aggiorna regolarmente le tue EC2 istanze Amazon

Su tutte le istanze Amazon EC2 Windows e Amazon EC2 Linux create con CloudFormation, esegui regolarmente il `yum update` comando per aggiornare il pacchetto RPM. In questo modo ti assicuri di avere le correzioni e gli aggiornamenti di sicurezza più recenti.

Lavorare con i CloudFormation modelli

Un AWS CloudFormation modello definisce le AWS risorse che desideri creare, aggiornare o eliminare come parte di uno stack. È composto da diverse sezioni, ma l'unica sezione obbligatoria è la [Resources](#) sezione, che deve dichiarare almeno una risorsa.

È possibile creare modelli utilizzando i seguenti metodi:

- AWS Infrastructure Composer— Un'interfaccia visiva per la progettazione di modelli.
- Editor di testo: scrivi modelli direttamente nella sintassi JSON o YAML.
- Generatore IaC: genera modelli a partire dalle risorse fornite nel tuo account che attualmente non sono gestite da CloudFormation. Il generatore IaC funziona con un'ampia gamma di tipi di risorse supportati dall'API Cloud Control nella tua regione.

Questa sezione fornisce una guida completa su come utilizzare le diverse sezioni di un CloudFormation modello e su come iniziare a creare modelli di stack. Tratta i seguenti argomenti:

Argomenti

- [Dove vengono archiviati i modelli](#)
- [Convalida dei modelli](#)
- [Guida introduttiva ai modelli](#)
- [Modelli di esempio](#)
- [CloudFormation formato modello](#)
- [CloudFormation sezioni modello](#)
- [Crea modelli visivamente con Infrastructure Composer](#)
- [Genera modelli da risorse esistenti con il generatore IaC](#)
- [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#)
- [Ottieni AWS valori usando pseudo parametri](#)
- [Ottieni gli output esportati da uno stack distribuito CloudFormation](#)
- [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#)
- [CloudFormation procedure dettagliate](#)
- [CloudFormation frammenti di modello](#)
- [WindowsImplementa stack basati su CloudFormation](#)

- [Estendi le funzionalità del tuo modello con i CloudFormation tipi di risorse forniti](#)
- [Crea configurazioni di risorse riutilizzabili che possono essere incluse nei modelli con moduli CloudFormation](#)

Dove vengono archiviati i modelli

Bucket Amazon S3

Puoi archiviare CloudFormation i modelli in un bucket Amazon S3. Quando crei o aggiorni uno stack, puoi specificare l'URL S3 del modello anziché caricarlo direttamente.

Se carichi i modelli direttamente tramite AWS Management Console o AWS CLI, viene creato automaticamente un bucket S3. Per ulteriori informazioni, consulta [Crea uno stack dalla console CloudFormation](#).

Repository Git

Con [Git sync](#), puoi archiviare i modelli in un repository Git. Quando crei o aggiorni uno stack, puoi specificare la posizione del repository Git e il ramo contenente il modello invece di caricarlo direttamente o fare riferimento a un URL S3. CloudFormation monitora automaticamente il repository e il ramo specificati per rilevare eventuali modifiche al modello. Per ulteriori informazioni, consulta [Crea uno stack dal codice sorgente del repository con Git sync](#).

Convalida dei modelli

Convalida della sintassi

È possibile verificare la sintassi JSON o YAML del modello utilizzando il comando [validate-template](#) CLI o specificando il modello sulla console. La console esegue la convalida automaticamente. Per ulteriori informazioni, consulta [Crea uno stack dalla console CloudFormation](#).

Tuttavia, questi metodi verificano solo la sintassi del modello e non convalidano i valori delle proprietà specificati per una risorsa.

Strumenti di convalida aggiuntivi

Per convalide più complesse e verifiche basate sulle migliori pratiche, puoi utilizzare strumenti aggiuntivi come:

- [CloudFormation Linter \(cfn-lint\)](#): convalida i modelli rispetto agli schemi dei provider di risorse. [CloudFormation](#) Include il controllo dei valori validi per le proprietà delle risorse e le migliori pratiche.
- [CloudFormation Rain \(rain fmt\)](#): formatta i tuoi CloudFormation modelli secondo uno standard coerente o riformatta un modello da JSON a YAML (o da YAML a JSON). Conserva i commenti quando si utilizza YAML e, ove possibile, passa all'uso delle funzioni intrinseche alla sintassi breve.

Guida introduttiva ai modelli

Per iniziare a creare un CloudFormation modello, segui questi passaggi:

1. Scegli le risorse: identifica le AWS risorse che desideri includere nel tuo stack, come EC2 istanze VPCs, gruppi di sicurezza e altro ancora.
2. Scrivi il modello: scrivi il modello in formato JSON o YAML, definendo le risorse e le relative proprietà.
3. Salva il modello: salva il modello localmente con un'estensione di file come: `.json`, `.yaml` o `.txt`.
4. Convalida il modello: convalida il modello utilizzando i metodi descritti nella [Convalida dei modelli](#) sezione.
5. Crea uno stack: crea uno stack utilizzando il modello convalidato.

Pianifica di utilizzare il modello di riferimento CloudFormation

Durante la stesura dei modelli, è possibile trovare la documentazione sulla sintassi dettagliata per i diversi tipi di risorse nel [riferimento ai tipi di AWS risorse e proprietà](#).

Spesso, i modelli di stack richiedono funzioni intrinseche per assegnare valori di proprietà che non sono disponibili fino al runtime e attributi speciali per controllare il comportamento delle risorse.

Durante la stesura del modello, consulta le seguenti risorse come guida:

- [Riferimento alla funzione intrinseca](#): alcune funzioni intrinseche di uso comune includono:
 - `Ref`— Recupera il valore di un parametro o l'ID fisico di una risorsa.
 - `Sub`— Sostituisce i segnaposto nelle stringhe con valori effettivi.
 - `GetAtt`— Restituisce il valore di un attributo da una risorsa nel modello.
 - `Join`— Unisce un set di valori in un'unica stringa.

- [Riferimento agli attributi della risorsa](#): alcuni attributi speciali di uso comune includono:
 - DependsOn— Utilizzate questo attributo per specificare che una risorsa deve essere creata dopo l'altra.
 - DeletionPolicy— Utilizzate questo attributo per CloudFormation specificare come gestire l'eliminazione di una risorsa.

Modelli di esempio

CloudFormation fornisce modelli di stack open source che è possibile utilizzare per iniziare. Per ulteriori informazioni, consulta [Modelli AWS CloudFormation di esempio](#) sul GitHub sito Web.

Tieni presente che questi modelli non sono pensati per essere pronti per la produzione. Dovresti dedicare del tempo a imparare come funzionano, adattarli alle tue esigenze e assicurarti che soddisfino gli standard di conformità della tua azienda.

Ogni modello di questo repository supera i controlli di [CloudFormation Linter](#) (cfn-lint) e anche un set di AWS CloudFormation Guard regole di base basato sulla Center for Internet Security (CIS) Top 20, con eccezioni per alcune regole in cui era opportuno mantenere l'esempio concentrato su un singolo caso d'uso.

CloudFormation formato modello

È possibile creare CloudFormation modelli nei formati JSON o YAML. Entrambi i formati hanno lo stesso scopo ma offrono vantaggi distinti in termini di leggibilità e complessità.

- JSON: JSON è un formato di interscambio di dati leggero che è facile da analizzare e generare per le macchine. Tuttavia, può diventare complicato per gli esseri umani leggere e scrivere, specialmente per configurazioni complesse. In JSON, il modello è strutturato utilizzando parentesi `{}` e parentesi annidate `[]` per definire risorse, parametri e altri componenti. La sua sintassi richiede una dichiarazione esplicita di ogni elemento, il che può rendere il modello prolisso ma garantisce la stretta aderenza a un formato strutturato.
- YAML: YAML è progettato per essere più leggibile dall'uomo e meno prolisso rispetto a JSON. Utilizza l'indentazione anziché parentesi e parentesi per indicare l'annidamento, il che può semplificare la visualizzazione della gerarchia di risorse e parametri. YAML è spesso preferito per la sua chiarezza e facilità d'uso, specialmente quando si tratta di modelli più complessi. Tuttavia, la dipendenza di YAML dall'indentazione può portare a errori se la spaziatura non è coerente, il che richiede un'attenzione particolare per mantenere la precisione.

Struttura del modello

CloudFormation i modelli sono suddivisi in diverse sezioni e ogni sezione è progettata per contenere un tipo specifico di informazioni. Alcune sezioni devono essere dichiarate in un ordine specifico, mentre per altre l'ordine non ha importanza. Tuttavia, durante la creazione del modello, può essere utile utilizzare l'ordine logico illustrato negli esempi seguenti, poiché i valori di una sezione potrebbero fare riferimento a valori di una sezione precedente.

Durante la creazione di modelli, non utilizzate sezioni principali duplicate, come la `Resources` sezione. Sebbene CloudFormation possa accettare il modello, quest'ultimo avrà un comportamento indefinito durante l'elaborazione del modello e potrebbe fornire risorse in modo errato o restituire errori inspiegabili.

JSON

L'esempio seguente mostra la struttura di un modello in formato JSON con tutte le sezioni disponibili.

```
{
  "AWSTemplateFormatVersion" : "version date",

  "Description" : "JSON string",

  "Metadata" : {
    template metadata
  },

  "Parameters" : {
    set of parameters
  },

  "Rules" : {
    set of rules
  },

  "Mappings" : {
    set of mappings
  },

  "Conditions" : {
    set of conditions
  },
```

```
"Transform" : {  
    set of transforms  
},  
  
"Resources" : {  
    set of resources  
},  
  
"Outputs" : {  
    set of outputs  
}  
}
```

YAML

L'esempio seguente mostra la struttura di un modello in formato YAML con tutte le sezioni disponibili.

```
---  
AWSTemplateFormatVersion: version date  
  
Description:  
    String  
  
Metadata:  
    template metadata  
  
Parameters:  
    set of parameters  
  
Rules:  
    set of rules  
  
Mappings:  
    set of mappings  
  
Conditions:  
    set of conditions  
  
Transform:  
    set of transforms  
  
Resources:  
    set of resources
```


Outputs:

set of outputs

Commenti

Nei modelli in formato JSON, i commenti non sono supportati. JSON, in base alla progettazione, non include una sintassi per i commenti, il che significa che non è possibile aggiungere commenti direttamente all'interno della struttura JSON. Tuttavia, se hai bisogno di includere note esplicative o documentazione, puoi prendere in considerazione l'aggiunta di metadati. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Nei modelli in formato YAML, puoi includere commenti in linea utilizzando il simbolo. #

L'esempio seguente mostra un modello YAML con i commenti inline.

```
AWSTemplateFormatVersion: 2010-09-09
Description: A sample CloudFormation template with YAML comments.
# Resources section
Resources:
  MyEC2Instance:
    Type: AWS::EC2::Instance
    Properties:
      # Linux AMI
      ImageId: ami-1234567890abcdef0
      InstanceType: t2.micro
      KeyName: MyKey
      BlockDeviceMappings:
        - DeviceName: /dev/sdm
          Ebs:
            VolumeType: io1
            Iops: 200
            DeleteOnTermination: false
            VolumeSize: 20
```

Specifiche

CloudFormation supporta le seguenti specifiche JSON e YAML:

JSON

CloudFormation segue lo standard JSON ECMA-404. Per ulteriori informazioni sul formato JSON, consulta <http://www.json.org>.

YAML

CloudFormation supporta la specifica YAML versione 1.1 con alcune eccezioni. CloudFormation non supporta le seguenti funzionalità:

- I tag `binary`, `omap`, `pairs`, `set` e `timestamp`
- Alias
- Unioni di hash

Per ulteriori informazioni su YAML, visita il sito <https://www.yaml.org/>.

Ulteriori informazioni

Per ogni risorsa specificata nel modello, ne definisci le proprietà e i valori utilizzando le regole di sintassi specifiche di JSON o YAML. Per ulteriori informazioni sulla sintassi del modello per ogni formato, consulta [CloudFormation sezioni modello](#).

Uso delle espressioni regolari nei CloudFormation modelli

È possibile utilizzare le espressioni regolari (comunemente note come espressioni regolari) in diversi punti all'interno dei CloudFormation modelli, ad esempio per la proprietà durante la creazione di un parametro del `AllowedPattern` modello.

Tutte le espressioni regolari sono CloudFormation conformi alla sintassi regex di Java. [Per una descrizione completa della sintassi regex di Java e dei relativi costrutti, vedete `java.util.Regex.Pattern`.](#)

Se scrivete il CloudFormation modello in sintassi JSON, dovete evitare qualsiasi carattere di barra rovesciata (`\`) nell'espressione regolare aggiungendo una barra rovesciata aggiuntiva. Questo perché JSON interpreta le barre rovesciate come caratteri di escape e devi evitarli per assicurarti che vengano trattate come barre rovesciate letterali nell'espressione regolare.

Ad esempio, se si include una `\d` nell'espressione regolare per individuare un carattere cifra, nel modello JSON è necessario scrivere `\\d`.

Nell'esempio seguente, la `AllowedPattern` proprietà specifica un'espressione regolare che corrisponde a quattro caratteri consecutivi (`()`). `\d{4}` Tuttavia, poiché l'espressione regolare è definita in un modello JSON, è necessario eliminare il carattere backslash con una barra rovesciata aggiuntiva (`()`). `\\d`

```
{
  "Parameters": {
    "MyParameter": {
      "Type": "String",
      "AllowedPattern": "\\d{4}"
    }
  }
}
```

Se scrivete il CloudFormation modello con la sintassi YAML, dovete racchiudere l'espressione regolare tra virgolette singole (`«`). Non è richiesto alcun escape aggiuntivo.

```
Parameters:
  MyParameter:
    Type: String
    AllowedPattern: '\d{4}'
```

CloudFormation sezioni modello

Ogni CloudFormation modello è composto da una o più sezioni, ognuna delle quali ha uno scopo specifico.

La sezione **Risorse** è obbligatoria in ogni CloudFormation modello e costituisce il nucleo del modello. Questa sezione specifica le risorse dello stack e le relative proprietà, ad esempio un' EC2 istanza Amazon o un bucket Amazon S3. Ogni risorsa è definita con un ID logico univoco, un tipo e dettagli di configurazione specifici.

La sezione **Parametri**, sebbene facoltativa, svolge un ruolo importante nel rendere i modelli più flessibili. Consente agli utenti di passare valori in fase di esecuzione durante la creazione o l'aggiornamento di uno stack. È possibile fare riferimento a questi parametri nelle **Outputs** sezioni **Resources** and, abilitando la personalizzazione senza alterare il modello stesso. Ad esempio, è possibile utilizzare i parametri per specificare tipi di istanze o impostazioni di ambiente che variano tra le distribuzioni.

La sezione `Outputs`, anch'essa facoltativa, definisce i valori restituiti durante la visualizzazione delle proprietà di uno stack. Gli output forniscono informazioni utili, ad esempio identificatori di risorse URLs, che possono essere utilizzate per scopi operativi o per l'integrazione con altri stack. Questa sezione aiuta gli utenti a recuperare e utilizzare dettagli importanti sulle risorse create dal modello.

Altre sezioni opzionali includono le mappature, che funzionano come tabelle di ricerca per gestire i valori condizionali. Con le mappature, è possibile definire coppie chiave-valore e utilizzarle con la funzione intrinseca nelle sezioni `and`. `Fn::FindInMap Resources Outputs` Ciò è utile per gli scenari in cui è necessario regolare le configurazioni in base a condizioni come l'ambiente. Regione AWS

Le sezioni `Metadata` e `Rules`, sebbene utilizzate meno frequentemente, forniscono funzionalità aggiuntive. `Metadata` può includere informazioni aggiuntive sul modello, mentre `Rules` convalida un parametro o una combinazione di parametri durante la creazione dello stack o gli aggiornamenti, assicurandosi che soddisfino criteri specifici. La sezione `Conditions` migliora ulteriormente la flessibilità controllando se vengono create determinate risorse o se alle proprietà viene assegnato un valore in base a condizioni come il tipo di ambiente.

Infine, la sezione `Transform` viene utilizzata per applicare le macro durante l'elaborazione del modello. Per le applicazioni serverless (note anche come applicazioni Lambda), specifica la versione del [Serverless Application Model AWS \(SAM\)](#) da utilizzare. Quando si specifica una trasformazione, è possibile utilizzare la AWS SAM sintassi per dichiarare le risorse nel modello. Il modello definisce la sintassi che puoi utilizzare e la relativa modalità di elaborazione. È inoltre possibile utilizzare la `AWS::Include` trasformazione per includere frammenti di modello archiviati separatamente dal modello principale. CloudFormation

I seguenti argomenti forniscono ulteriori informazioni ed esempi per l'utilizzo di ciascuna sezione.

Argomenti

- [CloudFormation Resource sintassi del modello](#)
- [CloudFormation Parameter sintassi del modello](#)
- [CloudFormation Output sintassi del modello](#)
- [CloudFormation Mapping sintassi del modello](#)
- [CloudFormation Metadata sintassi del modello](#)
- [CloudFormation Rule sintassi del modello](#)
- [CloudFormation Condition sintassi del modello](#)
- [CloudFormation Transform sezione modello](#)

- [CloudFormation sintassi della versione in formato modello](#)
- [CloudFormation modello Description sintassi](#)

CloudFormation Resource sintassi del modello

La Resources sezione è una sezione obbligatoria di primo livello in un CloudFormation modello. Dichiara le AWS risorse che desideri CloudFormation fornire e configurare come parte del tuo stack.

Sintassi

La Resources sezione utilizza la seguente sintassi:

JSON

```
"Resources" : {  
  "LogicalResourceName1" : {  
    "Type" : "AWS::ServiceName::ResourceType",  
    "Properties" : {  
      "PropertyName1" : "PropertyValue1",  
      ...  
    }  
  },  
  
  "LogicalResourceName2" : {  
    "Type" : "AWS::ServiceName::ResourceType",  
    "Properties" : {  
      "PropertyName1" : "PropertyValue1",  
      ...  
    }  
  }  
}
```

YAML

```
Resources:  
  LogicalResourceName1:  
    Type: AWS::ServiceName::ResourceType  
    Properties:  
      PropertyName1: PropertyValue1  
      ...
```

```
LogicalResourceName2:
  Type: AWS::ServiceName::ResourceType
  Properties:
    PropertyName1: PropertyValue1
    ...
```

ID logico (chiamato anche nome logico)

All'interno di un CloudFormation modello, le risorse sono identificate in base ai rispettivi nomi di risorse logiche. Questi nomi devono essere alfanumerici (a-zA-Z0-9) e univoci all'interno del modello. I nomi logici vengono utilizzati per fare riferimento a risorse provenienti da altre sezioni del modello.

Tipo di risorsa

Ogni risorsa deve avere un Type attributo che definisce il tipo di AWS risorsa. L'Typeattributo ha il formato `AWS::ServiceName::ResourceType`. Ad esempio, l'Typeattributo per un bucket Amazon S3 è. `AWS::S3::Bucket`

Per l'elenco completo dei tipi di risorse supportati, consulta il riferimento ai tipi di [AWS risorse e proprietà](#).

Proprietà delle risorse

Le proprietà delle risorse sono opzioni aggiuntive che è possibile specificare per definire i dettagli di configurazione per il tipo di risorsa specifico. Alcune proprietà sono obbligatorie, mentre altre sono opzionali. Alcune proprietà hanno valori predefiniti, pertanto la specificazione di tali proprietà è facoltativa.

Per i dettagli sulle proprietà supportate per ogni tipo di risorsa, consultate gli argomenti di [riferimento relativi ai tipi di AWS risorse e proprietà](#).

I valori delle proprietà possono essere stringhe letterali, elenchi di stringhe, valori booleani, riferimenti dinamici, riferimenti a parametri, pseudo riferimenti o valori restituiti da una funzione. Gli esempi seguenti mostrano come dichiarare diversi tipi di valori di proprietà:

JSON

```
"Properties" : {
  "String" : "A string value",
  "Number" : 123,
  "LiteralList" : [ "first-value", "second-value" ],
  "Boolean" : true
```

```
}
```

YAML

```
Properties:
  String: A string value
  Number: 123
  LiteralList:
    - first-value
    - second-value
  Boolean: true
```

ID fisico

Oltre all'ID logico, alcune risorse hanno anche un ID fisico, che è il nome effettivamente assegnato a quella risorsa, ad esempio un ID di EC2 istanza o un nome di bucket S3. Usa quello fisico IDs per identificare le risorse al di fuori dei CloudFormation modelli, ma solo dopo che le risorse sono state create. Ad esempio, supponete di assegnare a una risorsa di EC2 istanza un ID logico di `MyEC2Instance`. Quando CloudFormation crea l'istanza, genera e assegna CloudFormation automaticamente un ID fisico (ad esempio `i-1234567890abcdef0`) all'istanza. Puoi utilizzare questo ID fisico per identificare l'istanza e visualizzarne le proprietà (come il nome DNS) utilizzando la EC2 console Amazon.

Per i bucket Amazon S3 e molte altre risorse, genera CloudFormation automaticamente un nome fisico univoco per la risorsa se non ne specifichi uno esplicitamente. Questo nome fisico si basa su una combinazione del nome dello CloudFormation stack, del nome logico della risorsa specificato nel CloudFormation modello e di un ID univoco. Ad esempio, se hai un bucket Amazon S3 con il nome logico `MyBucket` in uno stack denominato `MyStack`, CloudFormation potresti denominare il bucket con il seguente nome fisico. `MyStack-MyBucket-abcdefghijkl1`

Per le risorse che supportano nomi personalizzati, puoi assegnare i tuoi nomi fisici per aiutarti a identificare rapidamente le risorse. Ad esempio, puoi denominare un bucket S3 che memorizza i log con il nome `MyPerformanceLogs`. Per ulteriori informazioni, consulta [Tipo di nome](#).

Risorse di riferimento

Spesso è necessario impostare le proprietà di una risorsa in base al nome o alla proprietà di un'altra risorsa. Ad esempio, potresti creare un' EC2 istanza che utilizza gruppi EC2 di sicurezza o una CloudFront distribuzione supportata da un bucket S3. Tutte queste risorse possono essere create nello stesso CloudFormation modello.

CloudFormation fornisce funzioni intrinseche che è possibile utilizzare per fare riferimento ad altre risorse e alle relative proprietà. Queste funzioni consentono di creare dipendenze tra le risorse e di passare valori da una risorsa all'altra.

La funzione **Ref**

La Ref funzione viene comunemente utilizzata per recuperare una proprietà identificativa delle risorse definite all'interno dello stesso CloudFormation modello. Ciò che restituisce dipende dal tipo di risorsa. Per la maggior parte delle risorse, restituisce il nome fisico della risorsa. Tuttavia, per alcuni tipi di risorse, potrebbe restituire un valore diverso, ad esempio un indirizzo IP per una `AWS::EC2::EIP` risorsa o un Amazon Resource Name (ARN) per un argomento Amazon SNS.

Gli esempi seguenti mostrano come utilizzare la Ref funzione nelle proprietà. In ognuno di questi esempi, la Ref funzione restituirà il nome effettivo della `LogicalResourceName` risorsa dichiarata altrove nel modello. L'esempio di `!Ref` sintassi nell'esempio YAML è solo un modo più breve per scrivere la funzione. Ref

JSON

```
"Properties" : {  
    "PropertyName" : { "Ref" : "LogicalResourceName" }  
}
```

YAML

```
Properties:  
  PropertyName1:  
    Ref: LogicalResourceName  
  PropertyName2: !Ref LogicalResourceName
```

Per informazioni più dettagliate sulla Ref funzione, vedere. [Ref](#)

La funzione **Fn::GetAtt**

La Ref funzione è utile se il parametro o il valore restituito per una risorsa è esattamente quello desiderato. Tuttavia, potrebbero essere necessari altri attributi di una risorsa. Ad esempio, se desideri creare una CloudFront distribuzione con un'origine S3, devi specificare la posizione del bucket utilizzando un indirizzo in stile DNS. Una serie di risorse dispongono di attributi aggiuntivi i cui valori possono essere utilizzati nel modello. Per ottenere questi attributi, si utilizza la funzione. `Fn::GetAtt`

Gli esempi seguenti mostrano come utilizzare la `GetAtt` funzione nelle proprietà. La `Fn::GetAtt` funzione accetta due parametri, il nome logico della risorsa e il nome dell'attributo da recuperare. L'esempio di `!GetAtt` sintassi nell'esempio YAML è solo un modo più breve per scrivere la funzione. `GetAtt`

JSON

```
"Properties" : {  
  "PropertyName" : {  
    "Fn::GetAtt" : [ "LogicalResourceName", "AttributeName" ]  
  }  
}
```

YAML

```
Properties:  
  PropertyName1:  
    Fn::GetAtt:  
      - LogicalResourceName  
      - AttributeName  
  PropertyName2: !GetAtt LogicalResourceName.AttributeName
```

Per informazioni più dettagliate sulla `GetAtt` funzione, vedere. [Fn::GetAtt](#)

Esempi

Gli esempi seguenti illustrano come dichiarare le risorse e come i CloudFormation modelli possono fare riferimento ad altre risorse definite all'interno dello stesso modello e delle risorse esistenti AWS .

Argomenti

- [Dichiarazione di una singola risorsa con un nome personalizzato](#)
- [Fare riferimento ad altre risorse con la funzione Ref](#)
- [Riferimento agli attributi delle risorse utilizzando la funzione Fn::GetAtt](#)

Dichiarazione di una singola risorsa con un nome personalizzato

Gli esempi seguenti dichiarano una singola risorsa di tipo `AWS::S3::Bucket` con il nome logico. `MyBucket` La `BucketName` proprietà è impostata su `amzn-s3-demo-bucket`, che deve essere sostituita con il nome desiderato per il bucket S3.

Se utilizzi questa dichiarazione di risorse per creare uno stack, CloudFormation creerà un bucket Amazon S3 con impostazioni predefinite. Per altre risorse, come un' EC2 istanza Amazon o un gruppo Auto Scaling, sono CloudFormation necessarie ulteriori informazioni.

JSON

```
{
  "Resources": {
    "MyBucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {
        "BucketName": "amzn-s3-demo-bucket"
      }
    }
  }
}
```

YAML

```
Resources:
  MyBucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: amzn-s3-demo-bucket
```

Fare riferimento ad altre risorse con la funzione **Ref**

Gli esempi seguenti mostrano una dichiarazione di risorse che definisce un' EC2 istanza e un gruppo di sicurezza. La Ec2Instance risorsa fa riferimento alla InstanceSecurityGroup risorsa come parte della sua SecurityGroupIds proprietà utilizzando la Ref funzione. Include anche un gruppo di sicurezza esistente (sg-12a4c434) che non è dichiarato nel modello. Utilizza stringhe letterali per fare riferimento alle risorse AWS esistenti.

JSON

```
{
  "Resources": {
    "Ec2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "SecurityGroupIds": [
```

```
{
    "Ref": "InstanceSecurityGroup"
},
"sg-12a4c434"
],
"KeyName": "MyKey",
"ImageId": "ami-1234567890abcdef0"
}
},
"InstanceSecurityGroup": {
    "Type": "AWS::EC2::SecurityGroup",
    "Properties": {
        "GroupDescription": "Enable SSH access via port 22",
        "SecurityGroupIngress": [
            {
                "IpProtocol": "tcp",
                "FromPort": 22,
                "ToPort": 22,
                "CidrIp": "0.0.0.0/0"
            }
        ]
    }
}
}
```

YAML

```
Resources:
  Ec2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      SecurityGroupIds:
        - !Ref InstanceSecurityGroup
        - sg-12a4c434
      KeyName: MyKey
      ImageId: ami-1234567890abcdef0
  InstanceSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Enable SSH access via port 22
      SecurityGroupIngress:
        - IpProtocol: tcp
```

```
FromPort: 22
ToPort: 22
CidrIp: 0.0.0.0/0
```

Riferimento agli attributi delle risorse utilizzando la funzione **`Fn::GetAtt`**

Gli esempi seguenti mostrano una dichiarazione di risorsa che definisce una risorsa di CloudFront distribuzione e un bucket S3. La `MyDistribution` risorsa specifica il nome DNS della `MyBucket` risorsa utilizzando la `Fn::GetAtt` funzione per ottenere l'attributo del bucket. `DomainName` Noterai che la `Fn::GetAtt` funzione elenca i suoi due parametri in un array. Per le funzioni che richiedono più parametri, puoi utilizzare un array per specificare i parametri.

JSON

```
{
  "Resources": {
    "MyBucket": {
      "Type": "AWS::S3::Bucket"
    },
    "MyDistribution": {
      "Type": "AWS::CloudFront::Distribution",
      "Properties": {
        "DistributionConfig": {
          "Origins": [
            {
              "DomainName": {
                "Fn::GetAtt": [
                  "MyBucket",
                  "DomainName"
                ]
              },
            ],
            "Id": "MyS3Origin",
            "S3OriginConfig": {}
          ]
        },
        "Enabled": "true",
        "DefaultCacheBehavior": {
          "TargetOriginId": "MyS3Origin",
          "ForwardedValues": {
            "QueryString": "false"
          },
          "ViewerProtocolPolicy": "allow-all"
        }
      }
    }
  }
}
```

```
    }  
  }  
}  
}
```

YAML

```
Resources:  
  MyBucket:  
    Type: 'AWS::S3::Bucket'  
  MyDistribution:  
    Type: 'AWS::CloudFront::Distribution'  
    Properties:  
      DistributionConfig:  
        Origins:  
          - DomainName: !GetAtt  
            - MyBucket  
            - DomainName  
            Id: MyS3Origin  
            S3OriginConfig: {}  
        Enabled: 'true'  
        DefaultCacheBehavior:  
          TargetOriginId: MyS3Origin  
          ForwardedValues:  
            QueryString: 'false'  
          ViewerProtocolPolicy: allow-all
```

CloudFormation Parameters sintassi del modello

Utilizza la sezione `Parameters` opzionale per personalizzare i modelli. Con i parametri, puoi inserire valori personalizzati nel tuo modello ogni volta che crei o aggiorni uno stack. Utilizzando i parametri nei modelli, è possibile creare modelli riutilizzabili e flessibili che possono essere adattati a scenari specifici.

Definendo i parametri del tipo appropriato, puoi scegliere da un elenco di identificatori di risorse esistenti quando utilizzi la console per creare il tuo stack. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#).

I parametri sono un metodo comune per specificare i valori delle proprietà delle risorse dello stack. Tuttavia, è possibile che esistano impostazioni che dipendono dalla regione o piuttosto complesse da comprendere per gli utenti a causa di altre condizioni o dipendenze. In questi casi, potresti voler

inserire una logica nel modello stesso in modo che gli utenti possano specificare valori più semplici (o nessuno) per ottenere i risultati desiderati, ad esempio utilizzando una mappatura. Per ulteriori informazioni, consulta [CloudFormation Mappingssintassi del modello](#).

Sintassi

I parametri vengono dichiarati nella `Parameters` sezione di un modello, che utilizza la seguente sintassi generale:

JSON

```
"Parameters" : {  
  "ParameterLogicalID" : {  
    "Description": "Information about the parameter",  
    "Type" : "DataType",  
    "Default" : "value",  
    "AllowedValues" : ["value1", "value2"]  
  }  
}
```

YAML

```
Parameters:  
  ParameterLogicalID:  
    Description: Information about the parameter  
  Type: DataType  
  Default: value  
  AllowedValues:  
    - value1  
    - value2
```

Un parametro contiene un elenco di attributi che definiscono il valore e i vincoli rispetto al valore. L'unico attributo richiesto è `Type`, che può essere `StringNumber`, o un tipo CloudFormation di parametro fornito. È inoltre possibile aggiungere un `Description` attributo che descriva il tipo di valore da specificare. Il nome e la descrizione del parametro vengono visualizzati nella pagina *Specificare i parametri* quando si utilizza il modello nella procedura guidata *Create Stack*.

Note

Per impostazione predefinita, la CloudFormation console elenca i parametri di input in ordine alfabetico in base al relativo ID logico. Per ignorare questo

ordinamento predefinito e raggruppare i parametri correlati, puoi utilizzare la chiave `AWS::CloudFormation::Interface` dei metadati nel tuo modello. Per ulteriori informazioni, consulta [Organizzazione CloudFormation dei parametri con AWS::CloudFormation::Interface metadati](#).

Per i parametri con valori predefiniti, CloudFormation utilizza i valori predefiniti a meno che gli utenti non specifichino un altro valore. Se si omette l'attributo predefinito, agli utenti viene richiesto di specificare un valore per quel parametro. Tuttavia, richiedere all'utente di inserire un valore non garantisce che il valore sia valido. Per convalidare il valore di un parametro, potete dichiarare vincoli o specificare un AWS tipo di parametro specifico.

Per i parametri senza valori predefiniti, gli utenti devono specificare un valore per il nome della chiave al momento della creazione dello stack. In caso contrario, non CloudFormation riesce a creare lo stack e genera un'eccezione:

```
Parameters: [KeyName] must have values
```

Proprietà

AllowedPattern

Una espressione regolare che rappresenta i modelli da consentire per i tipi `String` o `CommaDelimitedList`. Se applicato su un parametro di tipo `String`, lo schema deve corrispondere all'intero valore del parametro fornito. Quando viene applicato a un parametro di tipo `CommaDelimitedList`, il modello deve corrispondere a ciascun valore nell'elenco.

Required: No

AllowedValues

Matrice contenente l'elenco dei valori consentiti per il parametro. Quando viene applicato a un parametro di tipo `String`, il valore del parametro deve essere uno dei valori consentiti. Quando viene applicato a un parametro di tipo `CommaDelimitedList`, ogni valore nell'elenco deve essere uno dei valori consentiti.

Required: No

 Note

Se utilizzi YAML e desideri utilizzare le stringhe Yes e No per AllowedValues, utilizza le virgolette singole per evitare che il parser YAML consideri questi valori booleani.

ConstraintDescription

Stringa che illustra un vincolo in caso di violazione del vincolo. Ad esempio, senza una descrizione del vincolo, un parametro associato al modello consentito `[A-Za-z0-9]+` restituisce il seguente messaggio di errore quando l'utente specifica un valore non valido:

```
Malformed input-Parameter MyParameter must match pattern [A-Za-z0-9]+
```

Se aggiungi una descrizione del vincolo, ad esempio `must only contain letters (uppercase and lowercase) and number` (solo lettere (maiuscole e minuscole) e numeri), puoi visualizzare il seguente messaggio di errore personalizzato:

```
Malformed input-Parameter MyParameter must only contain uppercase and lowercase letters and numbers
```

Required: No

Default

Valore del tipo appropriato per il modello da utilizzare se non viene specificato alcun valore al momento della creazione di uno stack. Se per il parametro definisci vincoli, devi specificare un valore conforme a tali vincoli.

Required: No

Description

Stringa contenente un massimo di 4.000 caratteri che descrive il parametro.

Required: No

MaxLength

Valore intero che determina il numero massimo di caratteri consentiti per i tipi `String`.

Required: No

MaxValue

Valore numerico che determina il valore numerico massimo consentito per i tipi `Number`.

Required: No

MinLength

Valore intero che determina il numero minimo di caratteri consentiti per i tipi `String`.

Required: No

MinValue

Valore numerico che determina il valore numerico minimo consentito per i tipi `Number`.

Required: No

NoEcho

Indica se mascherare il valore del parametro per impedirne la visualizzazione nella console, negli strumenti a riga di comando o nell'API. Se impostate l'attributo `NoEcho` su `true`, CloudFormation restituisce il valore del parametro mascherato da asterischi (`*****`) per tutte le chiamate che descrivono lo stack o gli eventi dello stack, ad eccezione delle informazioni memorizzate nelle posizioni specificate di seguito.

Required: No

Important

L'utilizzo dell'attributo `NoEcho` non maschera le informazioni memorizzate nei seguenti elementi:

- La sezione dei modelli. Metadata CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per ulteriori informazioni, vedere [Metadati](#).
- Sezione dei modelli `Outputs`. Per ulteriori informazioni, consulta [Output](#).
- Attributo Metadata di una definizione di risorsa. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Si consiglia vivamente di non utilizzare questi meccanismi per includere informazioni sensibili, come password o segreti.

 Important

Anziché incorporare informazioni riservate direttamente nei CloudFormation modelli, consigliamo di utilizzare parametri dinamici nel modello di pila per fare riferimento a informazioni sensibili archiviate e gestite all'esterno CloudFormation, ad esempio nel AWS Systems Manager Parameter Store o. AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

 Important

Consigliamo vivamente di non includere parametri NoEcho o dati sensibili, nelle proprietà delle risorse che fanno parte dell'identificatore principale di una risorsa.

Quando un NoEcho parametro è incluso in una proprietà che costituisce un identificatore di risorsa principale, è CloudFormation possibile utilizzare il valore effettivo in chiaro nell'identificatore della risorsa principale. Questo ID risorsa può apparire in qualsiasi output o destinazione derivata.

[Per determinare quali proprietà della risorsa comprendono l'identificatore principale di un tipo di risorsa, fate riferimento alla documentazione di riferimento relativa alla risorsa nel riferimento ai tipi di risorse e proprietà.AWS](#) Nella sezione Return values (Valori restituiti), il valore restituito della funzione Ref rappresenta le proprietà delle risorse che comprendono l'identificatore principale del tipo di risorsa.

Type

Tipo di dati per il parametro (DataType).

Campo obbligatorio: sì

CloudFormation supporta i seguenti tipi di parametri:

String

Stringa letterale. È possibile utilizzare i seguenti attributi per dichiarare i vincoli:MinLength,, MaxLengthDefault, AllowedValues e. AllowedPattern

Ad esempio, gli utenti possono specificare "MyUserName".

Number

Un numero intero o float. CloudFormation convalida il valore del parametro come numero; tuttavia, quando si utilizza il parametro altrove nel modello (ad esempio, utilizzando la funzione Ref intrinseca), il valore del parametro diventa una stringa.

È possibile utilizzare i seguenti attributi per dichiarare i vincoli:, e. MinValue MaxValue Default AllowedValues

Ad esempio, gli utenti possono specificare "8888".

List<Number>

Matrice di numeri interi o float separati da virgole. CloudFormation convalida il valore del parametro come numeri. Tuttavia, quando utilizzi il parametro in una posizione diversa nel modello (ad esempio, utilizzando la funzione intrinseca Ref), il valore del parametro diventa un elenco di stringhe.

Ad esempio, gli utenti possono specificare "80,20" e Ref restituisce ["80", "20"].

CommaDelimitedList

Matrice di stringhe letterali separate da virgole. Il numero totale di stringhe deve corrispondere al numero totale di virgole più uno. Ogni stringa membro non deve includere spazi.

Ad esempio, gli utenti possono specificare "test,dev,prod" e Ref restituisce ["test", "dev", "prod"].

Tipi di parametri specifici per AWS

AWS valori come i nomi delle coppie di EC2 chiavi Amazon e il VPC IDs. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione](#).

Tipi di parametri di Systems Manager

Parametri che corrispondono ai parametri esistenti in Archivio parametri Systems Manager. Si specifica una chiave del parametro Systems Manager come valore del tipo di parametro Systems Manager e si CloudFormation recupera il valore più recente da Parameter Store da utilizzare per lo stack. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione](#).

Requisiti generali per i parametri

Per l'utilizzo dei parametri sono validi i seguenti requisiti:

- È possibile avere un massimo di 200 parametri in un CloudFormation modello.
- A ogni parametro deve essere assegnato un nome logico (chiamato anche ID logico) che deve essere alfanumerico e univoco tra tutti i nomi logici all'interno del modello.
- A ogni parametro deve essere assegnato un tipo di parametro supportato da CloudFormation. Per ulteriori informazioni, consulta la sezione [Type](#).
- A ogni parametro deve essere assegnato un valore in fase di esecuzione per CloudFormation effettuare correttamente il provisioning dello stack. Facoltativamente, è possibile specificare un valore predefinito CloudFormation da utilizzare a meno che non venga fornito un altro valore.
- I parametri e i relativi riferimenti a essi devono essere dichiarati dall'interno dello stesso modello. Puoi fare riferimento ai parametri dalle sezioni Resources e Outputs del modello.

Esempi

Argomenti

- [Parametro di stringa semplice](#)
- [Parametro della password](#)
- [Parametri di riferimento](#)
- [Parametro di elenco delimitato da virgole](#)
- [Restituzione un valore da un parametro CommaDelimitedList](#)

Parametro di stringa semplice

L'esempio seguente dichiara un parametro denominato `InstanceTypeParameter` di tipo `String`. Questo parametro consente di specificare il tipo di EC2 istanza Amazon per lo stack. Se non viene fornito alcun valore durante la creazione o l'aggiornamento dello stack, CloudFormation utilizza il valore predefinito di `t2.micro`.

JSON

```
"Parameters" : {  
  "InstanceTypeParameter" : {  
    "Description" : "Enter t2.micro, m1.small, or m1.large. Default is t2.micro.",  
    "Type" : "String",  
    "Default" : "t2.micro",  
    "AllowedValues" : ["t2.micro", "m1.small", "m1.large"]  
  }  
}
```

```
}
```

YAML

```
Parameters:
  InstanceTypeParameter:
    Description: Enter t2.micro, m1.small, or m1.large. Default is t2.micro.
    Type: String
    Default: t2.micro
    AllowedValues:
      - t2.micro
      - m1.small
      - m1.large
```

Parametro della password

L'esempio seguente dichiara un parametro denominato DBPwd di tipo `String` senza alcun valore predefinito. La `NoEcho` proprietà è impostata `true` per impedire che il valore del parametro venga visualizzato nelle descrizioni degli stack. La lunghezza minima che può essere specificata è 1 e la lunghezza massima che può essere specificata è 41. Il modello consente l'uso di caratteri alfabetici in maiuscolo e minuscolo e di numeri. Questo esempio illustra anche l'uso di un'espressione regolare per la `AllowedPattern` proprietà.

JSON

```
"Parameters" : {
  "DBPwd" : {
    "NoEcho" : "true",
    "Description" : "The database admin account password",
    "Type" : "String",
    "MinLength" : "1",
    "MaxLength" : "41",
    "AllowedPattern" : "^[a-zA-Z0-9]*$"
  }
}
```

YAML

```
Parameters:
  DBPwd:
    NoEcho: true
    Description: The database admin account password
```

```
Type: String
MinLength: 1
MaxLength: 41
AllowedPattern: ^[a-zA-Z0-9]*$
```

Parametri di riferimento

Puoi utilizzare la funzione intrinseca `Ref` per fare riferimento a un parametro. CloudFormation utilizza il valore del parametro per effettuare il provisioning dello stack. Puoi fare riferimento ai parametri dalle sezioni `Resources` e `Outputs` dello stesso modello.

Nell'esempio seguente, la `InstanceType` proprietà della risorsa dell' EC2 istanza fa riferimento al valore del `InstanceTypeParameter` parametro:

JSON

```
"Ec2Instance" : {
  "Type" : "AWS::EC2::Instance",
  "Properties" : {
    "InstanceType" : { "Ref" : "InstanceTypeParameter" },
    "ImageId" : "ami-0ff8a91507f77f867"
  }
}
```

YAML

```
Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    InstanceType:
      Ref: InstanceTypeParameter
    ImageId: ami-0ff8a91507f77f867
```

Parametro di elenco delimitato da virgole

Il tipo di `CommaDelimitedList` parametro può essere utile quando è necessario fornire più valori per una singola proprietà. L'esempio seguente dichiara un parametro denominato `DbSubnetIpBlocks` con un valore predefinito di tre blocchi CIDR separati da virgole.

JSON

```
"Parameters" : {
```

```
"DbSubnetIpBlocks": {
  "Description": "Comma-delimited list of three CIDR blocks",
  "Type": "CommaDelimitedList",
  "Default": "10.0.48.0/24, 10.0.112.0/24, 10.0.176.0/24"
}
```

YAML

```
Parameters:
  DbSubnetIpBlocks:
    Description: "Comma-delimited list of three CIDR blocks"
    Type: CommaDelimitedList
    Default: "10.0.48.0/24, 10.0.112.0/24, 10.0.176.0/24"
```

Restituzione un valore da un parametro CommaDelimitedList

Per fare riferimento a un valore specifico nell'elenco delimitato da virgole di un parametro, utilizzate la funzione `Fn::Select` intrinseca nella sezione del modello. `Resources` Passate il valore di indice dell'oggetto che desiderate e un elenco di oggetti, come illustrato nell'esempio seguente.

JSON

```
{
  "Parameters": {
    "VPC": {
      "Type": "String",
      "Default": "vpc-123456"
    },
    "VpcAzs": {
      "Type": "CommaDelimitedList",
      "Default": "us-west-2a, us-west-2b, us-west-2c"
    },
    "DbSubnetIpBlocks": {
      "Type": "CommaDelimitedList",
      "Default": "172.16.0.0/26, 172.16.0.64/26, 172.16.0.128/26"
    }
  },
  "Resources": {
    "DbSubnet1": {
      "Type": "AWS::EC2::Subnet",
      "Properties": {
        "AvailabilityZone": {
```

```

        "Fn::Sub": [
            "${AWS::Region}${AZ}",
            {
                "AZ": {
                    "Fn::Select": [
                        0,
                        { "Ref": "VpcAzs" }
                    ]
                }
            }
        ],
        "VpcId": {
            "Ref": "VPC"
        },
        "CidrBlock": {
            "Fn::Select": [
                0,
                { "Ref": "DbSubnetIpBlocks" }
            ]
        }
    },
    "DbSubnet2": {
        "Type": "AWS::EC2::Subnet",
        "Properties": {
            "AvailabilityZone": {
                "Fn::Sub": [
                    "${AWS::Region}${AZ}",
                    {
                        "AZ": {
                            "Fn::Select": [
                                1,
                                { "Ref": "VpcAzs" }
                            ]
                        }
                    }
                ]
            },
            "VpcId": {
                "Ref": "VPC"
            },
            "CidrBlock": {
                "Fn::Select": [

```



```

        1,
        { "Ref": "DbSubnetIpBlocks" }
      ]
    }
  },
  "DbSubnet3": {
    "Type": "AWS::EC2::Subnet",
    "Properties": {
      "AvailabilityZone": {
        "Fn::Sub": [
          "${AWS::Region}${AZ}",
          {
            "AZ": {
              "Fn::Select": [
                2,
                { "Ref": "VpcAzs" }
              ]
            }
          }
        ]
      },
      "VpcId": {
        "Ref": "VPC"
      },
      "CidrBlock": {
        "Fn::Select": [
          2,
          { "Ref": "DbSubnetIpBlocks" }
        ]
      }
    }
  }
}

```

YAML

```

Parameters:
  VPC:
    Type: String
    Default: vpc-123456
  VpcAzs:

```

```
Type: CommaDelimitedList
Default: us-west-2a, us-west-2b, us-west-2c
DbSubnetIpBlocks:
  Type: CommaDelimitedList
  Default: 172.16.0.0/26, 172.16.0.64/26, 172.16.0.128/26
Resources:
  DbSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone: !Sub
        - ${AWS::Region}${AZ}
        - AZ: !Select
          - 0
          - !Ref VpcAzs
      VpcId: !Ref VPC
      CidrBlock: !Select
        - 0
        - !Ref DbSubnetIpBlocks
  DbSubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone: !Sub
        - ${AWS::Region}${AZ}
        - AZ: !Select
          - 1
          - !Ref VpcAzs
      VpcId: !Ref VPC
      CidrBlock: !Select
        - 1
        - !Ref DbSubnetIpBlocks
  DbSubnet3:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone: !Sub
        - ${AWS::Region}${AZ}
        - AZ: !Select
          - 2
          - !Ref VpcAzs
      VpcId: !Ref VPC
      CidrBlock: !Select
        - 2
        - !Ref DbSubnetIpBlocks
```

Risorse correlate

CloudFormation supporta anche l'uso di riferimenti dinamici per specificare dinamicamente i valori delle proprietà. Ad esempio, potrebbe essere necessario fare riferimento a stringhe sicure archiviate in Systems Manager Parameter Store. Per ulteriori informazioni, consulta [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#).

È inoltre possibile utilizzare gli pseudo parametri all'interno di una funzione Ref o di una Sub funzione per popolare dinamicamente i valori. Per ulteriori informazioni, consulta [Ottieni AWS valori usando pseudo parametri](#).

CloudFormation Outputssintassi del modello

La Outputs sezione opzionale dichiara i valori di output per lo stack. Questi valori di output possono essere utilizzati in vari modi:

- Acquisisci dettagli importanti sulle tue risorse: un output è un modo conveniente per acquisire informazioni importanti sulle tue risorse. Ad esempio, è possibile restituire l'output di un nome di bucket S3 per uno stack per semplificare la ricerca del bucket. È possibile visualizzare i valori di output nella scheda Output della CloudFormation console o utilizzando il comando [describe-stacks](#)CLI.
- Riferimenti cross-stack: [è possibile importare i valori di output in altri stack per creare riferimenti tra gli stack](#). Ciò è utile quando è necessario condividere risorse o configurazioni su più stack.

Important

CloudFormation non oscura o offusca le informazioni incluse nella sezione. Outputs Si consiglia vivamente di non utilizzare questa sezione per generare informazioni riservate, ad esempio password o segreti.

I valori di output sono disponibili al termine dell'operazione dello stack. [I valori di output dello stack non sono disponibili quando lo stato dello stack si trova in uno qualsiasi degli stati.](#)

[IN_PROGRESS](#) Si sconsiglia di stabilire dipendenze tra un runtime del servizio e il valore di output dello stack, poiché i valori di output potrebbero non essere sempre disponibili.

Sintassi

La sezione Outputs è composta dal nome di chiave Outputs. Puoi dichiarare un massimo di 200 output in un modello.

L'esempio seguente mostra la struttura della sezione Outputs.

JSON

Usa le parentesi graffe per racchiudere tutte le dichiarazioni degli output. Delimita più output con virgole.

```
"Outputs" : {  
  "OutputLogicalID" : {  
    "Description" : "Information about the value",  
    "Value" : "Value to return",  
    "Export" : {  
      "Name" : "Name of resource to export"  
    }  
  }  
}
```

YAML

```
Outputs:  
  OutputLogicalID:  
    Description: Information about the value  
    Value: Value to return  
    Export:  
      Name: Name of resource to export
```

Campi di output

La sezione Outputs può includere i seguenti campi.

ID logico (chiamato anche nome logico)

Identificatore per l'output corrente. L'ID logico deve essere un valore alfanumerico (a-z, A-Z, 0-9) univoco all'interno del modello.

Description (facoltativo)

Tipo `String` che descrive il valore di output. Il valore della dichiarazione della descrizione deve essere una stringa letterale con una lunghezza compresa tra 0 e 1024 byte. Per specificare la descrizione non è possibile utilizzare un parametro o una funzione.

Value(obbligatorio)

Valore della proprietà restituita dal comando [describe-stacks](#). Il valore di un output può includere valori letterali, riferimenti a parametri, pseudoparametri, un valore di mappatura o funzioni intrinseche.

Export (facoltativo)

Nome dell'output della risorsa da esportare in un riferimento tra stack.

Puoi utilizzare le funzioni intrinseche per personalizzare il valore Name di un'esportazione.

Per ulteriori informazioni, consulta [Ottieni gli output esportati da uno stack distribuito CloudFormation](#).

Per associare una condizione a un output, definisci la condizione nella sezione [Conditions](#) del modello.

Esempi

Negli esempi seguenti viene illustrato il funzionamento dell'output dello stack.

Argomenti

- [Output dello stack](#)
- [Personalizza il nome di esportazione utilizzando Fn::Sub](#)
- [Personalizza il nome di esportazione utilizzando Fn::Join](#)
- [Restituisce un URL costruito utilizzando Fn::Join](#)

Output dello stack

In questo esempio, l'output denominato `BackupLoadBalancerDNSName` restituisce il nome DNS della risorsa con l'ID logico `BackupLoadBalancer` solo quando la condizione `CreateProdResources` è vera. L'output denominato `InstanceID` restituisce l'ID dell'istanza con l'ID logico `EC2 EC2Instance`.

JSON

```
"Outputs" : {
  "BackupLoadBalancerDNSName" : {
    "Description": "The DNSName of the backup load balancer",
    "Value" : { "Fn::GetAtt" : [ "BackupLoadBalancer", "DNSName" ] },
    "Condition" : "CreateProdResources"
  },
  "InstanceID" : {
    "Description": "The Instance ID",
    "Value" : { "Ref" : "EC2Instance" }
  }
}
```

YAML

```
Outputs:
  BackupLoadBalancerDNSName:
    Description: The DNSName of the backup load balancer
    Value: !GetAtt BackupLoadBalancer.DNSName
    Condition: CreateProdResources
  InstanceID:
    Description: The Instance ID
    Value: !Ref EC2Instance
```

Personalizza il nome di esportazione utilizzando **Fn::Sub**

In questo esempio, l'output denominato `StackVPC` restituisce l'ID di un VPC, quindi esporta il valore dei riferimenti tra stack con il nome `VPCID` aggiunto alla fine del nome dello stack.

JSON

```
"Outputs" : {
  "StackVPC" : {
    "Description" : "The ID of the VPC",
    "Value" : { "Ref" : "MyVPC" },
    "Export" : {
      "Name" : {"Fn::Sub": "${AWS::StackName}-VPCID" }
    }
  }
}
```

YAML

```
Outputs:
  StackVPC:
    Description: The ID of the VPC
    Value: !Ref MyVPC
    Export:
      Name: !Sub "${AWS::StackName}-VPCID"
```

Per ulteriori informazioni sulla funzione `Fn::Sub`, consulta [Fn::Sub](#).

Personalizza il nome di esportazione utilizzando **`Fn::Join`**

È inoltre possibile utilizzare la `Fn::Join` funzione per costruire valori basati su parametri, attributi delle risorse e altre stringhe.

Gli esempi seguenti utilizzano la `Fn::Join` funzione per personalizzare il nome di esportazione anziché la `Fn::Sub` funzione. La `Fn::Join` funzione di esempio concatena il nome dello stack con il nome VPCID utilizzando i due punti come separatore.

JSON

```
"Outputs" : {
  "StackVPC" : {
    "Description" : "The ID of the VPC",
    "Value" : { "Ref" : "MyVPC" },
    "Export" : {
      "Name" : { "Fn::Join" : [ ":", [ { "Ref" : "AWS::StackName" }, "VPCID" ] ] }
    }
  }
}
```

YAML

```
Outputs:
  StackVPC:
    Description: The ID of the VPC
    Value: !Ref MyVPC
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", VPCID ] ]
```

Per ulteriori informazioni sulla funzione `Fn::Join`, consulta [Fn::Join](#).

Restituisce un URL costruito utilizzando **Fn::Join**

Nell'esempio seguente, per un modello che crea un WordPress sito, `InstallURL` è la stringa restituita da una chiamata di `Fn::Join` funzione che concatena `http://`, il nome DNS della risorsa `ElasticLoadBalancer` `/wp-admin/install.php`. Il valore di output dovrebbe essere simile al seguente:

```
http://mywptests-elasticl-1gb5116sl8y5v-206169572.aws-region.elb.amazonaws.com/wp-admin/install.php
```

JSON

```
{
  "Outputs": {
    "InstallURL": {
      "Value": {
        "Fn::Join": [
          "",
          [
            "http://",
            {
              "Fn::GetAtt": [
                "ElasticLoadBalancer",
                "DNSName"
              ]
            },
            "/wp-admin/install.php"
          ]
        ]
      },
      "Description": "Installation URL of the WordPress website"
    }
  }
}
```

YAML

```
Outputs:
  InstallURL:
    Value: !Join
      - ''
      - - 'http://'
```



```
- !GetAtt
- ElasticLoadBalancer
- DNSName
- /wp-admin/install.php
Description: Installation URL of the WordPress website
```

Per ulteriori informazioni sulla funzione `Fn::Join`, consulta [Fn::Join](#).

CloudFormation Mappingssintassi del modello

La Mappings sezione opzionale consente di creare coppie chiave-valore che possono essere utilizzate per specificare valori in base a determinate condizioni o dipendenze.

Un caso d'uso comune della Mappings sezione consiste nell'impostare i valori in base al Regione AWS luogo in cui viene distribuito lo stack. Ciò può essere ottenuto utilizzando lo `AWS::Region` pseudo parametro. Lo `AWS::Region` pseudo parametro è un valore che si CloudFormation risolve nella regione in cui viene creato lo stack. Gli pseudo parametri vengono risolti entro quando si crea lo stack. CloudFormation

Per recuperare i valori in una mappa, puoi utilizzare la funzione `Fn::FindInMap` intrinseca all'interno della sezione del modello. `Resources`

Sintassi

La Mappings sezione utilizza la seguente sintassi:

JSON

```
"Mappings" : {
  "MappingLogicalName" : {
    "Key1" : {
      "Name" : "Value1"
    },
    "Key2" : {
      "Name" : "Value2"
    },
    "Key3" : {
      "Name" : "Value3"
    }
  }
}
```

YAML

```
Mappings:
  MappingLogicalName:
    Key1:
      Name: Value1
    Key2:
      Name: Value2
    Key3:
      Name: Value3
```

- MappingLogicalName è il nome logico per la mappatura.
- All'interno della mappatura, ogni mappa è una chiave seguita da un'altra mappatura.
- La chiave deve essere una mappa di coppie nome-valore e univoca all'interno della mappatura.
- La coppia nome-valore è un'etichetta e il valore da mappare. Se definisci i valori, puoi mappare più di un set di valori a una chiave.
- Le chiavi nelle mappature devono essere stringhe letterali.
- I valori possono essere di tipo String o List

Note

Non puoi includere parametri, pseudoparametri o funzioni intrinseche nella sezione Mappings.

Se i valori di una mappatura non sono attualmente utilizzati dal tuo stack, non puoi aggiornare la mappatura da solo. È necessario includere modifiche che aggiungano, modificano o eliminano risorse.

Esempi

Mappatura di base

L'esempio seguente mostra una sezione Mappings con una mappa RegionMap, che contiene cinque chiavi mappate a coppie nome-valore contenenti singoli valori stringa. Le chiavi sono i nomi di Regione. Ogni coppia nome-valore è un tipo di istanza della famiglia T disponibile nella regione rappresentata dalla chiave. Le coppie nome-valore hanno un nome (InstanceType nell'esempio) e un valore.

JSON

```
"Mappings" : {
  "RegionMap" : {
    "us-east-1"      : {"InstanceType": "t2.micro"},
    "us-west-1"      : {"InstanceType": "t2.micro"},
    "eu-west-1"      : {"InstanceType": "t2.micro"},
    "eu-north-1"     : {"InstanceType": "t3.micro"},
    "me-south-1"     : {"InstanceType": "t3.micro"}
  }
}
```

YAML

```
Mappings:
  RegionMap:
    us-east-1:
      InstanceType: t2.micro
    us-west-1:
      InstanceType: t2.micro
    eu-west-1:
      InstanceType: t2.micro
    eu-north-1:
      InstanceType: t3.micro
    me-south-1:
      InstanceType: t3.micro
```

Mappatura con più valori

L'esempio seguente presenta chiavi di regione mappate su due set di valori: uno denominato MyAMI1 e l'altro. MyAMI2

JSON

```
"AMIIDMap" : {
  "us-east-1"      : {"MyAMI1" : "ami-0ff8a91507f77f867", "MyAMI2" :
"ami-0a584ac55a7631c0c"},
  "us-west-1"      : {"MyAMI1" : "ami-0bdb828fd58c52235", "MyAMI2" :
"ami-066ee5fd4a9ef77f1"},
  "eu-west-1"      : {"MyAMI1" : "ami-047bb4163c506cd98", "MyAMI2" :
"ami-0a7c483d527806435"},
  "ap-southeast-1" : {"MyAMI1" : "ami-08569b978cc4dfa10", "MyAMI2" :
"ami-0be9df32ae9f92309"},
}
```

```
"ap-northeast-1" : {"MyAMI1" : "ami-06cd52961ce9f0d85", "MyAMI2" :
"ami-053cdd503598e4a9d"}
}
```

YAML

```
AMIIDMap:
  us-east-1:
    MyAMI1: ami-0ff8a91507f77f867
    MyAMI2: ami-0a584ac55a7631c0c
  us-west-1:
    MyAMI1: ami-0bdb828fd58c52235
    MyAMI2: ami-066ee5fd4a9ef77f1
  eu-west-1:
    MyAMI1: ami-047bb4163c506cd98
    MyAMI2: ami-0a7c483d527806435
  ap-southeast-1:
    MyAMI1: ami-08569b978cc4dfa10
    MyAMI2: ami-0be9df32ae9f92309
  ap-northeast-1:
    MyAMI1: ami-06cd52961ce9f0d85
    MyAMI2: ami-053cdd503598e4a9d
```

Restituzione di un valore da una mappatura

Puoi utilizzare la funzione `Fn::FindInMap` per restituire un valore denominato in base a una chiave specificata. Il seguente modello di esempio contiene una EC2 risorsa Amazon la cui `ImageId` proprietà è assegnata dalla `FindInMap` funzione. La `FindInMap` funzione specifica `key` come regione in cui viene creato lo stack (utilizzando lo `AWS::Region` pseudo parametro) e `MyAMI1` come nome del valore a cui mappare. Per ulteriori informazioni sugli pseudoparametri, consulta [Ottieni AWS valori usando pseudo parametri](#).

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Mappings" : {
    "AMIIDMap" : {
      "us-east-1" : {"MyAMI1" : "ami-0ff8a91507f77f867", "MyAMI2" :
"ami-0a584ac55a7631c0c"},
      "us-west-1" : {"MyAMI1" : "ami-0bdb828fd58c52235", "MyAMI2" :
"ami-066ee5fd4a9ef77f1"},

```

```

    "eu-west-1"      : {"MyAMI1" : "ami-047bb4163c506cd98", "MyAMI2" :
"ami-0a7c483d527806435"},
    "ap-northeast-1" : {"MyAMI1" : "ami-06cd52961ce9f0d85", "MyAMI2" :
"ami-053cdd503598e4a9d"},
    "ap-southeast-1" : {"MyAMI1" : "ami-08569b978cc4dfa10", "MyAMI2" :
"ami-0be9df32ae9f92309"}
  }
},
"Resources" : {
  "myEC2Instance" : {
    "Type" : "AWS::EC2::Instance",
    "Properties" : {
      "ImageId" : { "Fn::FindInMap" : [ "AMIIDMap", { "Ref" : "AWS::Region" },
"MyAMI1" ]},
      "InstanceType" : "t2.micro"
    }
  }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Mappings:
  AMIIDMap:
    us-east-1:
      MyAMI1: ami-0ff8a91507f77f867
      MyAMI2: ami-0a584ac55a7631c0c
    us-west-1:
      MyAMI1: ami-0bdb828fd58c52235
      MyAMI2: ami-066ee5fd4a9ef77f1
    eu-west-1:
      MyAMI1: ami-047bb4163c506cd98
      MyAMI2: ami-0a7c483d527806435
    ap-northeast-1:
      MyAMI1: ami-06cd52961ce9f0d85
      MyAMI2: ami-053cdd503598e4a9d
    ap-southeast-1:
      MyAMI1: ami-08569b978cc4dfa10
      MyAMI2: ami-0be9df32ae9f92309
Resources:
  myEC2Instance:
    Type: "AWS::EC2::Instance"

```

Properties:

```
ImageId: !FindInMap [AMIIDMap, !Ref "AWS::Region", MyAMI1]
InstanceType: t2.micro
```

Parametro di input e Fn::FindInMap

Puoi utilizzare un parametro di input con la funzione `Fn::FindInMap` per fare riferimento a un valore specifico in una mappa. Ad esempio, supponiamo di avere un elenco di regioni e tipi di ambiente mappati a un ID di gruppo di sicurezza specifico. È possibile selezionare l'ID del gruppo di sicurezza utilizzato dallo stack utilizzando un parametro di input (`EnvironmentType`). Per determinare la regione, utilizzate lo `AWS::Region` pseudo parametro, che ottiene il valore Regione AWS in cui create lo stack.

Questo esempio dichiara anche un tipo di parametro Systems Manager che fornisce un parametro Systems Manager alias (`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`) come valore predefinito per la `ImageId` proprietà dell' EC2 istanza. Si tratta di un valore che viene CloudFormation risolto come valore ID AMI per l'ultima AMI Amazon Linux 2 nella regione in cui viene creato lo stack.

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "LatestAmiId" : {
      "Description" : "The latest Amazon Linux 2 AMI from the Parameter Store",
      "Type" : "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
      "Default" : "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2"
    },
    "EnvironmentType" : {
      "Description" : "The environment type (Dev or Prod)",
      "Type" : "String",
      "Default" : "Dev",
      "AllowedValues" : [
        "Dev",
        "Prod"
      ]
    }
  },
  "Mappings" : {
    "SecurityGroupMap" : {
      "us-east-1" : {
```

```

        "Dev" : "sg-12345678",
        "Prod" : "sg-abcdef01"
    },
    "us-west-2" : {
        "Dev" : "sg-ghijkl23",
        "Prod" : "sg-45678abc"
    }
},
"Resources" : {
    "Ec2Instance" : {
        "Type" : "AWS::EC2::Instance",
        "Properties" : {
            "ImageId" : {
                "Ref" : "LatestAmiId"
            },
            "InstanceType" : "t2.micro",
            "SecurityGroupIds" : [{ "Fn::FindInMap" : [ "SecurityGroupMap", { "Ref" :
"AWS::Region" }, { "Ref" : "EnvironmentType" } ]}]
        }
    }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Parameters:
  LatestAmiId:
    Description: The latest Amazon Linux 2 AMI from the Parameter Store
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2'
  EnvironmentType:
    Description: The environment type (Dev or Prod)
    Type: String
    Default: Dev
    AllowedValues:
      - Dev
      - Prod
Mappings:
  SecurityGroupMap:
    us-east-1:
      Dev: "sg-12345678"

```

```
    Prod: "sg-abcdef01"
  us-west-2:
    Dev: "sg-ghijkl23"
    Prod: "sg-45678abc"
Resources:
  Ec2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestAmiId
      InstanceType: t2.micro
      SecurityGroupIds:
        - !FindInMap [SecurityGroupMap, !Ref "AWS::Region", !Ref EnvironmentType]
```

Risorse correlate

Questi argomenti correlati possono essere utili per sviluppare modelli che utilizzano la funzione.

`Fn::FindInMap`

- [Fn::FindInMap](#)
- [Miglioramenti a Fn::FindInMap](#)
- [Fn::Sub](#)

CloudFormation Metadata sintassi del modello

Metadata memorizza informazioni aggiuntive utilizzando oggetti JSON o YAML. I tipi di metadati a livello di modello che puoi utilizzare nel tuo modello includono:

Metadati personalizzati

Memorizza coppie chiave-valore definite dall'utente. Ad esempio, puoi fornire informazioni aggiuntive che non influiscono sulla creazione di risorse ma offrono un contesto aggiuntivo sulle specifiche dell'infrastruttura, del team o della distribuzione.

`AWS::CloudFormation::Interface`

Definisce il raggruppamento e l'ordine dei parametri di input quando vengono visualizzati nella console. CloudFormation Per impostazione predefinita, la CloudFormation console ordina alfabeticamente i parametri in base al relativo ID logico.

`AWS::CloudFormation::Designer`

AWS CloudFormation Designer (Designer) ha raggiunto la fine del ciclo di vita il 5 febbraio 2025.

Important

Durante l'aggiornamento di uno stack non puoi aggiornare solo la sezione Metadata. Puoi aggiornarla solo quando includi modifiche che prevedono l'aggiunta, la modifica o l'eliminazione di risorse.

CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per questo motivo, si consiglia vivamente di non utilizzare questa sezione per archiviare informazioni riservate, ad esempio password o segreti.

Sintassi

Per dichiarare metadati personalizzati nel CloudFormation modello, utilizzate la seguente sintassi:

JSON

```
"Metadata" : {  
  "Instances" : {"Description" : "Information about the instances"},  
  "Databases" : {"Description" : "Information about the databases"}  
}
```

YAML

```
Metadata:  
  Instances:  
    Description: "Information about the instances"  
  Databases:  
    Description: "Information about the databases"
```

Per la sintassi di, vedere. `AWS::CloudFormation::Interface` [Organizzazione CloudFormation dei parametri con AWS::CloudFormation::Interface metadati](#)

Organizzazione CloudFormation dei parametri con **AWS::CloudFormation::Interface** metadati

`AWS::CloudFormation::Interface` è una chiave di metadati che definisce il modo in cui i parametri vengono raggruppati e ordinati nella console. CloudFormation Per impostazione predefinita, la console elenca i parametri di input in ordine alfabetico in base alla loro logica IDs quando si creano o si aggiornano gli stack nella console. Utilizzando questa chiave, è possibile

definire il raggruppamento e l'ordine dei parametri in modo che gli utenti possano specificare i valori dei parametri in modo efficace. Ad esempio, è possibile raggruppare tutti i parametri EC2 correlati in un gruppo e tutti i parametri relativi a VPC in un altro gruppo.

Nel chiave di metadati puoi specificare i gruppi da creare, i parametri da includere in ciascun gruppo e l'ordine in base al quale la console mostra ciascun parametro all'interno del relativo gruppo.

È inoltre possibile definire etichette per i parametri. Un'etichetta è un nome semplice o una descrizione che la console visualizza invece di visualizzare un ID logico del parametro. Le etichette sono utili per aiutare gli utenti a comprendere i valori da specificare per ciascun parametro. Ad esempio, è possibile creare un'etichetta per un parametro `KeyPair Select` an `EC2 key pair`.

Tutti i parametri a cui fai riferimento nella chiave di metadati devono essere dichiarati nella sezione `Parameters` del modello.

Note

Solo la CloudFormation console utilizza la chiave `AWS::CloudFormation::Interface` dei metadati. AWS CLI e le chiamate API non utilizzano questa chiave.

Sintassi

Per dichiarare questa entità nel tuo CloudFormation modello, usa la seguente sintassi:

JSON

```
"Metadata" : {
  "AWS::CloudFormation::Interface" : {
    "ParameterGroups": [
      {
        "Label": {
          "default": "Group Label"
        },
        "Parameters": [
          "Parameter1",
          "Parameter2"
        ]
      }
    ],
    "ParameterLabels": {
```

```
    "Parameter1": {  
      "default": "Friendly Name for Parameter1"  
    }  
  }  
}  
}
```

YAML

```
Metadata:  
  AWS::CloudFormation::Interface:  
    ParameterGroups:  
      - Label:  
          default: Group Label  
        Parameters:  
          - Parameter1  
          - Parameter2  
    ParameterLabels:  
      Parameter1:  
        default: Friendly Name for Parameter1
```

Proprietà

ParameterGroups

Un elenco dei tipi di gruppo di parametri dove è possibile specificare i nomi di gruppo, i parametri di ciascun gruppo e l'ordine in cui i parametri sono visualizzati.

Required: No

Label

Un nome per il gruppo di parametri.

Required: No

default

L'etichetta predefinita utilizzata dalla CloudFormation console per denominare un gruppo di parametri.

Required: No

Tipo: stringa

Parameters

Un elenco di parametri logici con distinzione tra maiuscole e minuscole IDs da includere nel gruppo. I parametri devono essere stati già definiti nella sezione `Parameters` del modello. Un parametro può essere incluso in un solo gruppo di parametri.

La console elenca i parametri che non puoi associare a un gruppo di parametri in ordine alfabetico nel gruppo `Other parameters`.

Required: No

Tipo: elenco di valori stringa

ParameterLabels

Una mappatura dei parametri e dei relativi nomi descrittivi che la CloudFormation console mostra quando uno stack viene creato o aggiornato.

Required: No

Etichetta del parametro

Un'etichetta per un parametro. L'etichetta definisce un nome o una descrizione descrittiva che la CloudFormation console mostra nella pagina `Specificare i parametri` quando uno stack viene creato o aggiornato. L'etichetta del parametro deve essere l'ID logico con distinzione tra maiuscole e minuscole di un parametro valido dichiarato nella `Parameters` sezione del modello.

Required: No

default

L'etichetta predefinita utilizzata dalla CloudFormation console per denominare un parametro.

Required: No

Tipo: stringa

Esempio

L'esempio seguente definisce due gruppi di parametri: `Network Configuration` e `Amazon EC2 Configuration`. Il gruppo `Network Configuration` include i parametri `VPCID`, `SubnetId` e `SecurityGroupID`, che sono definiti nella sezione `Parameters` del modello (non mostrato). L'ordine in cui la console mostra questi parametri viene definito dall'ordine in cui i parametri sono

elencati, a partire dal parametro VPCID. L'esempio analogamente raggruppa e ordina i parametri Amazon EC2 Configuration.

L'esempio definisce anche un'etichetta per il parametro VPCID. La console mostrerà Which VPC should this be deployed to? (In quali VPC deve essere distribuito?) anziché l'ID logico del parametro (VPCID).

JSON

```
"Metadata" : {
  "AWS::CloudFormation::Interface" : {
    "ParameterGroups" : [
      {
        "Label" : { "default" : "Network Configuration" },
        "Parameters" : [ "VPCID", "SubnetId", "SecurityGroupID" ]
      },
      {
        "Label" : { "default": "Amazon EC2 Configuration" },
        "Parameters" : [ "InstanceType", "KeyName" ]
      }
    ],
    "ParameterLabels" : {
      "VPCID" : { "default" : "Which VPC should this be deployed to?" }
    }
  }
}
```

YAML

```
Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: "Network Configuration"
        Parameters:
          - VPCID
          - SubnetId
          - SecurityGroupID
      - Label:
          default: "Amazon EC2 Configuration"
        Parameters:
          - InstanceType
          - KeyName
```

```
ParameterLabels:
  VPCID:
    default: "Which VPC should this be deployed to?"
```

Gruppi di parametri nella console

Utilizzando la chiave di metadati di questo esempio, la figura riportata di seguito mostra il modo in cui la console visualizza i gruppi di parametri al momento della creazione o dell'aggiornamento di uno stack: i gruppi di parametri nella console

CloudFormation Rules sintassi del modello

La Rules sezione è una parte facoltativa di un CloudFormation modello che abilita la logica di convalida personalizzata. Se inclusa, questa sezione contiene le funzioni delle regole che convalidano i valori dei parametri prima di CloudFormation creare o aggiornare qualsiasi risorsa.

Le regole sono utili quando i vincoli dei parametri standard sono insufficienti. Ad esempio, quando SSL è abilitato, devono essere forniti sia un certificato che un nome di dominio. Una regola può garantire il rispetto di queste dipendenze.

Sintassi

La Rules sezione utilizza la seguente sintassi:

JSON

La sezione `Rules` di un modello comporta il nome di chiave `Rules`, seguito da un segno di due punti. Usa le parentesi graffe per racchiudere tutte le dichiarazioni degli output di regola. Se dichiari più regole, queste vengono delimitate da virgole. Per ogni regola, dichiara un nome logico tra virgolette seguito da un segno di due punti e parentesi graffe che racchiudono la condizione e le asserzioni di regola.

```
{
  "Rules": {
    "LogicalRuleName1": {
      "RuleCondition": {
        "rule-specific intrinsic function": "Value"
      },
      "Assertions": [
        {
          "Assert": {
            "rule-specific intrinsic function": "Value"
          },
          "AssertDescription": "Information about this assert"
        },
        {
          "Assert": {
            "rule-specific intrinsic function": "Value"
          },
          "AssertDescription": "Information about this assert"
        }
      ]
    },
    "LogicalRuleName2": {
      "Assertions": [
        {
          "Assert": {
            "rule-specific intrinsic function": "Value"
          },
          "AssertDescription": "Information about this assert"
        }
      ]
    }
  }
}
```

YAML

```
Rules:
  LogicalRuleName1:
    RuleCondition:
      rule-specific intrinsic function: Value
    Assertions:
      - Assert:
          rule-specific intrinsic function: Value
        AssertDescription: Information about this assert
      - Assert:
          rule-specific intrinsic function: Value
        AssertDescription: Information about this assert
  LogicalRuleName2:
    Assertions:
      - Assert:
          rule-specific intrinsic function: Value
        AssertDescription: Information about this assert
```

Campi delle regole

La sezione **Rules** può includere i seguenti campi.

ID logico (chiamato anche nome logico)

Un identificatore univoco per ogni regola.

RuleCondition (facoltativo)

Una proprietà che determina quando una regola ha effetto. Se non definisci una condizione di regola, le asserzioni della regola sono sempre attivate. Per ogni regola, è possibile definire una sola condizione della regola.

Assertions(obbligatorio)

Una o più istruzioni che specificano i valori accettabili per un particolare parametro.

Assert

Una condizione che deve restituire `true`.

AssertDescription

Un messaggio visualizzato quando un'asserzione fallisce.

Funzioni intrinseche specifiche delle regole

Per definire le regole, è necessario utilizzare funzioni specifiche delle regole, che sono funzioni che possono essere utilizzate solo nella `Rules` sezione di un modello. Sebbene queste funzioni possano essere annidate, il risultato finale di una condizione o di un'asserzione della regola deve essere o `true` o `false`.

Sono disponibili le seguenti funzioni delle regole:

- [Fn::And](#)
- [Fn::Contains](#)
- [Fn::EachMemberEquals](#)
- [Fn::EachMemberIn](#)
- [Fn::Equals](#)
- [Fn::If](#)
- [Fn::Not](#)
- [Fn::Or](#)
- [Fn::RefAll](#)
- [Fn::ValueOf](#)
- [Fn::ValueOfAll](#)

Queste funzioni vengono utilizzate nella condizione o nelle asserzioni di una regola. La proprietà `condition` determina se CloudFormation applica le asserzioni. Se la condizione restituisce `true`, CloudFormation valuta le asserzioni per verificare se il valore di un parametro è valido quando un prodotto fornito viene creato o aggiornato. Se il valore di un parametro non è valido, CloudFormation non crea né aggiorna lo stack. Se la condizione restituisce un risultato positivo `false`, CloudFormation non verifica il valore del parametro e procede con l'operazione di stack.

Esempi

Argomenti

- [Verifica condizionale di un valore di parametro](#)
- [Convalida multi-parametro](#)

Verifica condizionale di un valore di parametro

Nell'esempio seguente, le due regole verificano il valore del parametro `InstanceType`. A seconda del valore del parametro `Environment` (test o prod), l'utente deve specificare `a1.medium` o `a1.large` per il parametro `InstanceType`. I parametri `InstanceType` e `Environment` devono essere dichiarati nella sezione `Parameters` dello stesso modello.

JSON

```
{
  "Rules": {
    "testInstanceType": {
      "RuleCondition": {
        "Fn::Equals": [
          {"Ref": "Environment"},
          "test"
        ]
      },
      "Assertions": [
        {
          "Assert": {
            "Fn::Contains": [
              ["a1.medium"],
              {"Ref": "InstanceType"}
            ]
          },
          "AssertDescription": "For a test environment, the instance type must be a1.medium"
        }
      ]
    },
    "prodInstanceType": {
      "RuleCondition": {
        "Fn::Equals": [
          {"Ref": "Environment"},
          "prod"
        ]
      },
      "Assertions": [
        {
          "Assert": {
            "Fn::Contains": [
              ["a1.large"],
```

```

        {"Ref": "InstanceType"}
      ]
    },
    "AssertDescription": "For a production environment, the instance type must be
a1.large"
  }
]
}
}
}
}

```

YAML

```

Rules:
  testInstanceType:
    RuleCondition: !Equals
    - !Ref Environment
    - test
    Assertions:
    - Assert:
        'Fn::Contains':
        - - a1.medium
        - !Ref InstanceType
        AssertDescription: 'For a test environment, the instance type must be
a1.medium'
  prodInstanceType:
    RuleCondition: !Equals
    - !Ref Environment
    - prod
    Assertions:
    - Assert:
        'Fn::Contains':
        - - a1.large
        - !Ref InstanceType
        AssertDescription: 'For a production environment, the instance type must be
a1.large'

```

Convalida multi-parametro

I seguenti modelli di esempio dimostrano l'uso di regole per le convalide tra parametri. Creano un sito Web di esempio in esecuzione su un gruppo di Auto Scaling con un sistema di bilanciamento del carico. Il sito Web è disponibile sulla porta 80 o 443 a seconda dei parametri di input. Le istanze

del gruppo Auto Scaling possono essere configurate per l'ascolto su qualsiasi porta (con 8888 come impostazione predefinita).

Le regole di questo modello convalidano i parametri di input prima della creazione dello stack. Verificano che tutte le sottoreti appartengano al VPC specificato e assicurano che, quando il UseSSL parametro è impostato su Yes, vengano forniti sia l'ARN del certificato SSL che il nome della zona ospitata.

Note

Se crei uno stack da questo modello, ti verranno addebitate AWS le risorse utilizzate.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "VpcId": {
      "Type": "AWS::EC2::VPC::Id",
      "Description": "VpcId of your existing Virtual Private Cloud (VPC)",
      "ConstraintDescription": "must be the VPC Id of an existing Virtual Private Cloud."
    },
    "Subnets": {
      "Type": "List<AWS::EC2::Subnet::Id>",
      "Description": "The list of SubnetIds in your Virtual Private Cloud (VPC)",
      "ConstraintDescription": "must be a list of at least two existing subnets associated with at least two different availability zones."
    },
    "InstanceType": {
      "Description": "WebServer EC2 instance type",
      "Type": "String",
      "Default": "t2.micro",
      "AllowedValues": ["t2.micro", "t3.micro"],
      "ConstraintDescription": "must be a valid EC2 instance type."
    },
    "KeyName": {
      "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instances",
      "Type": "AWS::EC2::KeyPair::KeyName",
      "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
    }
  }
}
```

```

    },
    "SSHLocation": {
      "Description": "The IP address range that can be used to SSH to the EC2
instances",
      "Type": "String",
      "MinLength": "9",
      "MaxLength": "18",
      "Default": "0.0.0.0/0",
      "AllowedPattern": "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})/(\\d{1,2})",
      "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
    },
    "UseSSL": {
      "AllowedValues": ["Yes", "No"],
      "Default": "No",
      "Description": "Select \"Yes\" to implement SSL, \"No\" to skip (default).",
      "Type": "String"
    },
    "ALBSSLCertificateARN": {
      "Default": "",
      "Description": "[Optional] The ARN of the SSL certificate to be used for the
Application Load Balancer",
      "Type": "String"
    },
    "HostedZoneName": {
      "AllowedPattern": "^$|(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\\-\\-]*[a-zA-Z0-9])\\
\\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\\-\\-]*[A-Za-z0-9])$",
      "Default": "",
      "Description": "[Optional] The domain name of a valid Hosted Zone on AWS.",
      "Type": "String"
    }
  },
  "Conditions": {
    "UseALBSSL": {"Fn::Equals": [{"Ref": "UseSSL"}, "Yes"]}
  },
  "Rules": {
    "SubnetsInVPC": {
      "Assertions": [
        {
          "Assert": {"Fn::EachMemberEquals": [{"Fn::ValueOf": ["Subnets", "VpcId"]}, {"Ref": "VpcId"}]},
          "AssertDescription": "All subnets must be in the VPC"
        }
      ]
    }
  }
},

```

```

    "ValidateHostedZone": {
      "RuleCondition": {"Fn::Equals": [{"Ref": "UseSSL"}, "Yes"]},
      "Assertions": [
        {
          "Assert": {"Fn::Not": [{"Fn::Equals": [{"Ref": "ALBSSLCertificateARN"},
""]]}],
          "AssertDescription": "ACM Certificate value cannot be empty if SSL is
required"
        },
        {
          "Assert": {"Fn::Not": [{"Fn::Equals": [{"Ref": "HostedZoneName"}, ""]]}],
          "AssertDescription": "Route53 Hosted Zone Name is mandatory when SSL is
required"
        }
      ]
    }
  },
  "Mappings": {
    "AWSAMIRegionMap": {
      "us-east-1": {"AMZN LINUXHVM": "ami-0ff8a91507f77f867"},
      "us-west-1": {"AMZN LINUXHVM": "ami-0bdb828fd58c52235"},
      "eu-west-1": {"AMZN LINUXHVM": "ami-047bb4163c506cd98"},
      "ap-southeast-1": {"AMZN LINUXHVM": "ami-08569b978cc4dfa10"}
    }
  },
  "Resources": {
    "WebServerGroup": {
      "Type": "AWS::AutoScaling::AutoScalingGroup",
      "Properties": {
        "VPCZoneIdentifier": {"Ref": "Subnets"},
        "LaunchConfigurationName": {"Ref": "LaunchConfig"},
        "MinSize": "2",
        "MaxSize": "2",
        "TargetGroupARNs": [{"Ref": "ALBTargetGroup"}]
      },
      "CreationPolicy": {
        "ResourceSignal": {"Timeout": "PT15M"}
      },
      "UpdatePolicy": {
        "AutoScalingRollingUpdate": {
          "MinInstancesInService": "1",
          "MaxBatchSize": "1",
          "PauseTime": "PT15M",
          "WaitOnResourceSignals": true
        }
      }
    }
  }
}

```

```

    }
  }
},
"LaunchConfig": {
  "Type": "AWS::AutoScaling::LaunchConfiguration",
  "Metadata": {
    "Comment": "Install a simple application",
    "AWS::CloudFormation::Init": {
      "config": {
        "packages": {"yum": {"httpd": []}},
        "files": {
          "/var/www/html/index.html": {
            "content": {"Fn::Join": ["\n", ["<h1>Congratulations, you have
successfully launched the AWS CloudFormation sample.</h1>"]]},
            "mode": "000644",
            "owner": "root",
            "group": "root"
          },
          "/etc/cfn/cfn-hup.conf": {
            "content": {"Fn::Join": ["", [
              "[main]\n",
              "stack=", {"Ref": "AWS::StackId"}, "\n",
              "region=", {"Ref": "AWS::Region"}, "\n"
            ]]},
            "mode": "000400",
            "owner": "root",
            "group": "root"
          },
          "/etc/cfn/hooks.d/cfn-auto-reloader.conf": {
            "content": {"Fn::Join": ["", [
              "[cfn-auto-reloader-hook]\n",
              "triggers=post.update\n",
              "path=Resources.LaunchConfig.Metadata.AWS::CloudFormation::Init\n",
              "action=/opt/aws/bin/cfn-init -v ",
              "      --stack ", {"Ref": "AWS::StackName"},
              "      --resource LaunchConfig ",
              "      --region ", {"Ref": "AWS::Region"}, "\n",
              "runas=root\n"
            ]]},
            "mode": "000400",
            "owner": "root",
            "group": "root"
          }
        }
      }
    }
  },
},

```

```

    "services": {
      "sysvinit": {
        "httpd": {
          "enabled": "true",
          "ensureRunning": "true"
        },
        "cfn-hup": {
          "enabled": "true",
          "ensureRunning": "true",
          "files": [
            "/etc/cfn/cfn-hup.conf",
            "/etc/cfn/hooks.d/cfn-auto-reloader.conf"
          ]
        }
      }
    },
    "Properties": {
      "ImageId": {"Fn::FindInMap": ["AWSAMIRegionMap", {"Ref": "AWS::Region"},
"AMZNLinuxHVM"]},
      "SecurityGroups": [{"Ref": "InstanceSecurityGroup"}],
      "InstanceType": {"Ref": "InstanceType"},
      "KeyName": {"Ref": "KeyName"},
      "UserData": {
        "Fn::Base64": {"Fn::Join": ["", [
          "#!/bin/bash -xe\n",
          "yum update -y aws-cfn-bootstrap\n",
          "/opt/aws/bin/cfn-init -v ",
          "    --stack ", {"Ref": "AWS::StackName"},
          "    --resource LaunchConfig ",
          "    --region ", {"Ref": "AWS::Region"}, "\n",
          "/opt/aws/bin/cfn-signal -e $? ",
          "    --stack ", {"Ref": "AWS::StackName"},
          "    --resource WebServerGroup ",
          "    --region ", {"Ref": "AWS::Region"}, "\n"
        ]]}
      }
    },
    "ELBSecurityGroup": {
      "Type": "AWS::EC2::SecurityGroup",
      "Properties": {

```



```

    "GroupDescription": "Allow access to the ELB",
    "VpcId": {"Ref": "VpcId"},
    "SecurityGroupIngress": [{
      "Fn::If": [
        "UseALBSSL",
        {
          "IpProtocol": "tcp",
          "FromPort": 443,
          "ToPort": 443,
          "CidrIp": "0.0.0.0/0"
        },
        {
          "IpProtocol": "tcp",
          "FromPort": 80,
          "ToPort": 80,
          "CidrIp": "0.0.0.0/0"
        }
      ]
    }]
  },
  "ApplicationLoadBalancer": {
    "Type": "AWS::ElasticLoadBalancingV2::LoadBalancer",
    "Properties": {
      "Subnets": {"Ref": "Subnets"},
      "SecurityGroups": [{"Ref": "ELBSecurityGroup"}]
    }
  },
  "ALBListener": {
    "Type": "AWS::ElasticLoadBalancingV2::Listener",
    "Properties": {
      "DefaultActions": [{
        "Type": "forward",
        "TargetGroupArn": {"Ref": "ALBTargetGroup"}
      }],
      "LoadBalancerArn": {"Ref": "ApplicationLoadBalancer"},
      "Port": {"Fn::If": ["UseALBSSL", 443, 80]},
      "Protocol": {"Fn::If": ["UseALBSSL", "HTTPS", "HTTP"]},
      "Certificates": [{
        "Fn::If": [
          "UseALBSSL",
          {"CertificateArn": {"Ref": "ALBSSLCertificateARN"}},
          {"Ref": "AWS::NoValue"}
        ]
      }]
    }
  }
}

```

```

    ]]
  }
},
"ALBTargetGroup": {
  "Type": "AWS::ElasticLoadBalancingV2::TargetGroup",
  "Properties": {
    "HealthCheckIntervalSeconds": 30,
    "HealthCheckTimeoutSeconds": 5,
    "HealthyThresholdCount": 3,
    "Port": 80,
    "Protocol": "HTTP",
    "UnhealthyThresholdCount": 5,
    "VpcId": {"Ref": "VpcId"}
  }
},
"InstanceSecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "Enable SSH access and HTTP access on the inbound port",
    "SecurityGroupIngress": [
      {
        "IpProtocol": "tcp",
        "FromPort": 80,
        "ToPort": 80,
        "SourceSecurityGroupId": {"Fn::Select": [0, {"Fn::GetAtt":
["ApplicationLoadBalancer", "SecurityGroups"]}]}
      },
      {
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "CidrIp": {"Ref": "SSHLocation"}
      }
    ],
    "VpcId": {"Ref": "VpcId"}
  }
},
"RecordSet": {
  "Type": "AWS::Route53::RecordSetGroup",
  "Condition": "UseALBSSL",
  "Properties": {
    "HostedZoneName": {"Fn::Join": [ "", [{"Ref": "HostedZoneName"}, "." ] ] },
    "RecordSets": [ {
      "Name": {"Fn::Join": [ "", [

```

```

        {"Fn::Select": ["0", {"Fn::Split": [".", {"Fn::GetAtt":
["ApplicationLoadBalancer", "DNSName"]}]}}],
        ". ",
        {"Ref": "HostedZoneName"},
        ". "
    ]}],
    "Type": "A",
    "AliasTarget": {
        "DNSName": {"Fn::GetAtt": ["ApplicationLoadBalancer", "DNSName"]},
        "EvaluateTargetHealth": true,
        "HostedZoneId": {"Fn::GetAtt": ["ApplicationLoadBalancer",
"CanonicalHostedZoneID"]}
    }
  ]
}
},
"Outputs": {
  "URL": {
    "Description": "URL of the website",
    "Value": {"Fn::Join": [""], [
      {"Fn::If": [
        "UseALBSSL",
        {"Fn::Join": [""], [
          "https://",
          {"Fn::Join": [""], [
            {"Fn::Select": ["0", {"Fn::Split": [".", {"Fn::GetAtt":
["ApplicationLoadBalancer", "DNSName"]}]}}],
            ". ",
            {"Ref": "HostedZoneName"},
            ". "
          ]}],
          {"Fn::Join": [""], [
            "http://",
            {"Fn::GetAtt": ["ApplicationLoadBalancer", "DNSName"]}
          ]}
        ]}
      ]}
    ]}
  }
}
}

```

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  VpcId:
    Type: AWS::EC2::VPC::Id
    Description: VpcId of your existing Virtual Private Cloud (VPC)
    ConstraintDescription: must be the VPC Id of an existing Virtual Private Cloud.
  Subnets:
    Type: List<AWS::EC2::Subnet::Id>
    Description: The list of SubnetIds in your Virtual Private Cloud (VPC)
    ConstraintDescription: >-
      must be a list of at least two existing subnets associated with at least
      two different availability zones. They should be residing in the selected
      Virtual Private Cloud.
  InstanceType:
    Description: WebServer EC2 instance type
    Type: String
    Default: t2.micro
    AllowedValues:
      - t2.micro
      - t3.micro
    ConstraintDescription: must be a valid EC2 instance type.
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instances
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  SSHLocation:
    Description: The IP address range that can be used to SSH to the EC2 instances
    Type: String
    MinLength: '9'
    MaxLength: '18'
    Default: 0.0.0.0/0
    AllowedPattern: '(\d{1,3})\.\d{1,3})\.\d{1,3})\.\d{1,3})/(\d{1,2})'
    ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
  UseSSL:
    AllowedValues:
      - 'Yes'
      - 'No'
    ConstraintDescription: Select Yes to create a HTTPS Listener
    Default: 'No'
    Description: 'Select "Yes" to implement SSL, "No" to skip (default).'
    Type: String
  ALBSSLCertificateARN:
```

```

Default: ''
Description: >-
  [Optional] The ARN of the SSL certificate to be used for the Application
  Load Balancer
Type: String
HostedZoneName:
  AllowedPattern: >-
    ^$|((([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-\-]*[a-zA-Z0-9])\.)+)([A-Za-z0-9]|[A-Za-
z0-9][A-Za-z0-9\-\-]*[A-Za-z0-9]))$
  Default: ''
  Description: '[Optional] The domain name of a valid Hosted Zone on AWS.'
  Type: String
Conditions:
  UseALBSSL: !Equals
    - !Ref UseSSL
    - 'Yes'
Rules:
  SubnetsInVPC:
    Assertions:
      - Assert:
          'Fn::EachMemberEquals':
            - 'Fn::ValueOf':
                - Subnets
                - VpcId
            - Ref: VpcId
          AssertDescription: All subnets must be in the VPC
  ValidateHostedZone:
    RuleCondition: !Equals
      - !Ref UseSSL
      - 'Yes'
    Assertions:
      - Assert: !Not
          - !Equals
            - !Ref ALBSSLCertificateARN
            - ''
          AssertDescription: ACM Certificate value cannot be empty if SSL is required
      - Assert: !Not
          - !Equals
            - !Ref HostedZoneName
            - ''
          AssertDescription: Route53 Hosted Zone Name is mandatory when SSL is required
Mappings:
  AWSAMIRegionMap:
    us-east-1:

```

```

    AMZNLinuxHVM: ami-0ff8a91507f77f867
us-west-1:
    AMZNLinuxHVM: ami-0bdb828fd58c52235
eu-west-1:
    AMZNLinuxHVM: ami-047bb4163c506cd98
ap-southeast-1:
    AMZNLinuxHVM: ami-08569b978cc4dfa10
Resources:
  WebServerGroup:
    Type: AWS::AutoScaling::AutoScalingGroup
    Properties:
      VPCZoneIdentifier: !Ref Subnets
      LaunchConfigurationName: !Ref LaunchConfig
      MinSize: '2'
      MaxSize: '2'
      TargetGroupARNs:
        - !Ref ALBTargetGroup
    CreationPolicy:
      ResourceSignal:
        Timeout: PT15M
    UpdatePolicy:
      AutoScalingRollingUpdate:
        MinInstancesInService: '1'
        MaxBatchSize: '1'
        PauseTime: PT15M
        WaitOnResourceSignals: 'true'
  LaunchConfig:
    Type: AWS::AutoScaling::LaunchConfiguration
    Metadata:
      Comment: Install a simple application
      'AWS::CloudFormation::Init':
        config:
          packages:
            yum:
              httpd: []
          files:
            /var/www/html/index.html:
              content: !Join
                - |+
                - - >-
                  <h1>Congratulations, you have successfully launched the AWS
                    CloudFormation sample.</h1>
              mode: '000644'

```

```

    owner: root
    group: root
/etc/cfn/cfn-hup.conf:
  content: !Sub |
    [main]
    stack=${AWS::StackId}
    region=${AWS::Region}
  mode: '000400'
  owner: root
  group: root
/etc/cfn/hooks.d/cfn-auto-reloader.conf:
  content: !Sub |-
    [cfn-auto-reloader-hook]
    triggers=post.update
    path=Resources.LaunchConfig.Metadata.AWS::CloudFormation::Init
    action=/opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource
LaunchConfig --region ${AWS::Region}
    runas=root
  mode: '000400'
  owner: root
  group: root
services:
  sysvinit:
    httpd:
      enabled: 'true'
      ensureRunning: 'true'
    cfn-hup:
      enabled: 'true'
      ensureRunning: 'true'
      files:
        - /etc/cfn/cfn-hup.conf
        - /etc/cfn/hooks.d/cfn-auto-reloader.conf
Properties:
  ImageId: !FindInMap
    - AWSAMIRegionMap
    - !Ref 'AWS::Region'
    - AMZNLinuxHVM
  SecurityGroups:
    - !Ref InstanceSecurityGroup
  InstanceType: !Ref InstanceType
  KeyName: !Ref KeyName
  UserData: !Base64
    Fn::Sub: |-
      #!/bin/bash -xe

```

```
    yum update -y aws-cfn-bootstrap
    /opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource LaunchConfig --
region ${AWS::Region}
    /opt/aws/bin/cfn-signal -e $? --stack ${AWS::StackName} --resource
WebServerGroup --region ${AWS::Region}
ELBSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Allow access to the ELB
    VpcId: !Ref VpcId
    SecurityGroupIngress:
      - !If
        - UseALBSSL
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: 0.0.0.0/0
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0
ApplicationLoadBalancer:
  Type: AWS::ElasticLoadBalancingV2::LoadBalancer
  Properties:
    Subnets: !Ref Subnets
    SecurityGroups:
      - !Ref ELBSecurityGroup
ALBListener:
  Type: AWS::ElasticLoadBalancingV2::Listener
  Properties:
    DefaultActions:
      - Type: forward
        TargetGroupArn: !Ref ALBTargetGroup
    LoadBalancerArn: !Ref ApplicationLoadBalancer
    Port: !If
      - UseALBSSL
      - 443
      - 80
    Protocol: !If
      - UseALBSSL
      - HTTPS
      - HTTP
    Certificates:
      - !If
```



```

    - UseALBSSL
    - CertificateArn: !Ref ALBSSLCertificateARN
    - !Ref 'AWS::NoValue'
ALBTargetGroup:
  Type: AWS::ElasticLoadBalancingV2::TargetGroup
  Properties:
    HealthCheckIntervalSeconds: 30
    HealthCheckTimeoutSeconds: 5
    HealthyThresholdCount: 3
    Port: 80
    Protocol: HTTP
    UnhealthyThresholdCount: 5
    VpcId: !Ref VpcId
InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Enable SSH access and HTTP access on the inbound port
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        SourceSecurityGroupId: !Select
          - 0
          - !GetAtt
            - ApplicationLoadBalancer
            - SecurityGroups
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: !Ref SSHLocation
    VpcId: !Ref VpcId
RecordSet:
  Type: AWS::Route53::RecordSetGroup
  Condition: UseALBSSL
  Properties:
    HostedZoneName: !Join
      - ''
      - - !Ref HostedZoneName
      - .
    RecordSets:
      - Name: !Join
          - ''
          - - !Select
              - '0'

```

```

        - !Split
        - .
        - !GetAtt
        - ApplicationLoadBalancer
        - DNSName
    - .
    - !Ref HostedZoneName
    - .
Type: A
AliasTarget:
  DNSName: !GetAtt
    - ApplicationLoadBalancer
    - DNSName
  EvaluateTargetHealth: true
  HostedZoneId: !GetAtt
    - ApplicationLoadBalancer
    - CanonicalHostedZoneID

```

Outputs:**URL:**

Description: URL of the website

Value: !Join

```

- ''
- - !If
  - UseALBSSL
  - !Join
    - ''
    - - 'https://'
    - !Join
      - ''
      - - !Select
        - '0'
        - !Split
        - .
        - !GetAtt
        - ApplicationLoadBalancer
        - DNSName
      - .
      - !Ref HostedZoneName
      - .
- !Join
  - ''
  - - 'http://'
  - !GetAtt
  - ApplicationLoadBalancer

```

- DNSName

CloudFormation Conditionssintassi del modello

La sezione `Conditions` facoltativa contiene istruzioni che definiscono le circostanze nelle quali le entità vengono create o configurate. Ad esempio, è possibile creare una condizione e associarla a una risorsa o a un output in modo da CloudFormation creare la risorsa o l'output solo se la condizione è vera. Analogamente, è possibile associare una condizione a una proprietà in modo da CloudFormation impostare la proprietà su un valore specifico solo se la condizione è vera. Se la condizione è falsa, CloudFormation imposta la proprietà su un valore alternativo specificato dall'utente.

È possibile utilizzare le condizioni quando si desidera riutilizzare un modello per creare risorse in contesti diversi, ad esempio ambienti di test o di produzione. Ad esempio, nel modello, puoi aggiungere un parametro di `EnvironmentType` input che accetta entrambi `prod` o `test` come input. Per quanto riguarda l'prodambiente, è possibile includere EC2 istanze con determinate funzionalità, mentre per l'testambiente è possibile utilizzare funzionalità ridotte per risparmiare denaro. Questa definizione delle condizioni consente di definire quali risorse vengono create e come sono configurate per ogni tipo di ambiente.

Sintassi

La sezione `Conditions` è composta dal nome di chiave `Conditions`. Ogni dichiarazione di condizione include un ID logico e una o più funzioni intrinseche.

JSON

```
"Conditions": {  
  "LogicalConditionName1": {  
    "Intrinsic function": ...  
  },  
  
  "LogicalConditionName2": {  
    "Intrinsic function": ...  
  }  
}
```

YAML

```
Conditions:
```

```
LogicalConditionName1:
  Intrinsic function:
  ...

LogicalConditionName2:
  Intrinsic function:
  ...
```

Come funzionano le condizioni

Per utilizzare le condizioni, procedi nel seguente modo:

1. Aggiungi una definizione di parametro: definisci gli input che le tue condizioni valuteranno nella **Parameters** sezione del modello. Le condizioni vengono valutate come vere o false in base ai valori dei parametri di input. Nota che gli pseudo parametri sono disponibili automaticamente e non richiedono una definizione esplicita nella sezione. **Parameters** Per ulteriori informazioni sugli pseudoparametri, consulta [Ottieni AWS valori usando pseudo parametri](#).
2. Aggiungi una definizione di condizione: definisci le condizioni nella **Conditions** sezione utilizzando funzioni intrinseche come, e. `Fn::If` `Fn::Equals` `Fn::Not` Queste condizioni determinano quando vengono CloudFormation create le risorse associate. Le condizioni possono essere basate su:
 - Valori di input o pseudo parametri
 - Altre condizioni:
 - Valori di mappatura
3. Associa condizioni a risorse o output: fai riferimento alle condizioni nelle risorse o negli output utilizzando la **Condition** chiave e l'ID logico di una condizione. Facoltativamente, utilizzalo `Fn::If` in altre parti del modello (come i valori delle proprietà) per impostare i valori in base a una condizione.

CloudFormation valuta le condizioni durante la creazione o l'aggiornamento di uno stack.

CloudFormation crea entità associate a una condizione vera e ignora le entità associate a una condizione falsa. CloudFormation rivaluta inoltre queste condizioni durante ogni aggiornamento dello stack prima di modificare qualsiasi risorsa. Le entità che rimangono associate a una condizione vera vengono aggiornate, mentre quelle che vengono associate a una condizione falsa vengono eliminate.

 Important

Durante l'aggiornamento di uno stack non puoi aggiornare solo le condizioni. Le condizioni possono essere aggiornate solo se si includono modifiche che comportano l'aggiunta, la modifica o l'eliminazione di risorse.

Funzioni intrinseche delle condizioni

Puoi utilizzare le seguenti funzioni intrinseche per definire le condizioni:

- [Fn::And](#)
- [Fn::Equals](#)
- [Fn::ForEach](#)
- [Fn::If](#)
- [Fn::Not](#)
- [Fn::Or](#)

 Note

`Fn::If` è supportata solo nell'attributo di metadati, nell'attributo delle policy di aggiornamento e nei valori di proprietà della sezione `Resources` e nelle sezioni `Outputs` di un modello.

Esempi

Argomenti

- [Creazione di risorse basata sull'ambiente](#)
- [Fornitura di risorse a più condizioni](#)

Creazione di risorse basata sull'ambiente

Gli esempi seguenti forniscono un' EC2 istanza e creano e collegano in modo condizionale un nuovo volume EBS solo se il tipo di ambiente è `prod`. Se l'ambiente lo è `test`, creano semplicemente l' EC2 istanza senza il volume aggiuntivo.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "EnvType": {
      "Description": "Environment type",
      "Default": "test",
      "Type": "String",
      "AllowedValues": [
        "prod",
        "test"
      ],
      "ConstraintDescription": "must specify prod or test"
    }
  },
  "Conditions": {
    "CreateProdResources": {
      "Fn::Equals": [
        {
          "Ref": "EnvType"
        },
        "prod"
      ]
    }
  },
  "Resources": {
    "EC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId": "ami-1234567890abcdef0"
      }
    },
    "MountPoint": {
      "Type": "AWS::EC2::VolumeAttachment",
      "Condition": "CreateProdResources",
      "Properties": {
        "InstanceId": {
          "Ref": "EC2Instance"
        },
        "VolumeId": {
          "Ref": "NewVolume"
        },
        "Device": "/dev/sdh"
      }
    }
  }
}
```

```

    }
  },
  "NewVolume": {
    "Type": "AWS::EC2::Volume",
    "Condition": "CreateProdResources",
    "Properties": {
      "Size": 100,
      "AvailabilityZone": {
        "Fn::GetAtt": [
          "EC2Instance",
          "AvailabilityZone"
        ]
      }
    }
  }
}
}
}
}
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Parameters:
  EnvType:
    Description: Environment type
    Default: test
    Type: String
    AllowedValues:
      - prod
      - test
    ConstraintDescription: must specify prod or test
Conditions:
  CreateProdResources: !Equals
    - !Ref EnvType
    - prod
Resources:
  EC2Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: ami-1234567890abcdef0
  MountPoint:
    Type: AWS::EC2::VolumeAttachment
    Condition: CreateProdResources
    Properties:

```

```
    InstanceId: !Ref EC2Instance
    VolumeId: !Ref NewVolume
    Device: /dev/sdh
  NewVolume:
    Type: AWS::EC2::Volume
    Condition: CreateProdResources
    Properties:
      Size: 100
      AvailabilityZone: !GetAtt
        - EC2Instance
        - AvailabilityZone
```

Fornitura di risorse a più condizioni

Gli esempi seguenti creano in modo condizionale un bucket S3 se viene fornito un nome di bucket e allegano una policy del bucket solo quando l'ambiente è impostato su. prod Se non viene fornito alcun nome di bucket o l'ambiente lo è, non viene test creata alcuna risorsa.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "EnvType": {
      "Type": "String",
      "AllowedValues": [
        "prod",
        "test"
      ]
    },
    "BucketName": {
      "Default": "",
      "Type": "String"
    }
  },
  "Conditions": {
    "IsProduction": {
      "Fn::Equals": [
        {
          "Ref": "EnvType"
        },
        "prod"
      ]
    }
  }
}
```



```
    },
    "CreateBucket": {
      "Fn::Not": [
        {
          "Fn::Equals": [
            {
              "Ref": "BucketName"
            },
            ""
          ]
        }
      ]
    },
    "CreateBucketPolicy": {
      "Fn::And": [
        {
          "Condition": "IsProduction"
        },
        {
          "Condition": "CreateBucket"
        }
      ]
    }
  },
  "Resources": {
    "Bucket": {
      "Type": "AWS::S3::Bucket",
      "Condition": "CreateBucket",
      "Properties": {
        "BucketName": {
          "Ref": "BucketName"
        }
      }
    },
    "Policy": {
      "Type": "AWS::S3::BucketPolicy",
      "Condition": "CreateBucketPolicy",
      "Properties": {
        "Bucket": {
          "Ref": "Bucket"
        },
        "PolicyDocument": { ... }
      }
    }
  }
}
```

```
}  
}
```

YAML

```
AWSTemplateFormatVersion: 2010-09-09  
Parameters:  
  EnvType:  
    Type: String  
    AllowedValues:  
      - prod  
      - test  
  BucketName:  
    Default: ''  
    Type: String  
Conditions:  
  IsProduction: !Equals  
    - !Ref EnvType  
    - prod  
  CreateBucket: !Not  
    - !Equals  
      - !Ref BucketName  
      - ''  
  CreateBucketPolicy: !And  
    - !Condition IsProduction  
    - !Condition CreateBucket  
Resources:  
  Bucket:  
    Type: AWS::S3::Bucket  
    Condition: CreateBucket  
    Properties:  
      BucketName: !Ref BucketName  
  Policy:  
    Type: AWS::S3::BucketPolicy  
    Condition: CreateBucketPolicy  
    Properties:  
      Bucket: !Ref Bucket  
      PolicyDocument: ...
```

CloudFormation Transform sezione modello

La Transform sezione opzionale specifica una o più macro da CloudFormation utilizzare per elaborare in qualche modo il modello.

Le macro possono eseguire operazioni semplici come la ricerca e la sostituzione del testo, oppure possono apportare trasformazioni più ampie all'intero modello. CloudFormation esegue le macro nell'ordine in cui sono specificate. Quando si crea un set di modifiche, CloudFormation genera un set di modifiche che include il contenuto del modello elaborato. Puoi quindi esaminare le modifiche ed eseguire il set di modifiche. Per ulteriori informazioni sul funzionamento delle macro, consulta [Esegui elaborazioni personalizzate su CloudFormation modelli con macro di modelli](#).

CloudFormation supporta anche le trasformazioni, che sono macro ospitate da CloudFormation. CloudFormation tratta queste trasformazioni allo stesso modo di qualsiasi macro creata in termini di ordine e ambito di esecuzione. [Per ulteriori informazioni, vedete Transform reference](#).

Per dichiarare più macro, utilizza un formato di elenco e specifica una o più macro.

Ad esempio, nell'esempio di modello riportato di seguito `AWS::Serverless`, CloudFormation valuta `MyMacro` e quindi entrambi possono elaborare i contenuti dell'intero modello grazie alla loro inclusione nella `Transform` sezione.

```
# Start of processable content for MyMacro and AWS::Serverless
Transform:
  - MyMacro
  - 'AWS::Serverless'
Resources:
  WaitCondition:
    Type: AWS::CloudFormation::WaitCondition
  MyBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      Tags: [{"key": "value"}]
      CorsConfiguration: []
  MyEc2Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: ami-1234567890abcdef0
# End of processable content for MyMacro and AWS::Serverless
```

CloudFormation sintassi della versione in formato modello

La `AWSTemplateFormatVersion` sezione (opzionale) identifica la versione del formato del modello a cui è conforme il modello. La versione del modello più recente è `2010-09-09` ed è attualmente l'unico valore valido.

La versione del formato del modello non è la stessa della versione dell'API. La versione del formato del modello può cambiare indipendentemente dalle versioni dell'API.

Il valore della dichiarazione della versione del modello deve essere una stringa letterale. Non puoi utilizzare un parametro o una funzione per specificare la versione del modello. Se non specifichi un valore, CloudFormation presuppone la versione più recente del formato del modello. Il seguente frammento è un esempio di una dichiarazione della versione del modello valida:

JSON

```
"AWSTemplateFormatVersion" : "2010-09-09"
```

YAML

```
AWSTemplateFormatVersion: 2010-09-09
```

CloudFormation modello Description sintassi

La **Description** sezione (opzionale) consente di includere una stringa di testo che descrive il modello. Questa sezione deve sempre seguire la sezione relativa alla versione del modello.

Il valore della dichiarazione della descrizione deve essere una stringa letterale con una lunghezza compresa tra 0 e 1024 byte. Non puoi utilizzare un parametro o una funzione per specificare la descrizione. Il seguente frammento è un esempio di una dichiarazione della descrizione:

Important

Durante l'aggiornamento di uno stack non puoi aggiornare solo la sezione **Description**. Puoi aggiornarla solo quando includi modifiche che prevedono l'aggiunta, la modifica o l'eliminazione di risorse.

JSON

```
"Description" : "Here are some details about the template."
```

YAML

```
Description: > Here are some details about the template.
```

Crea modelli visivamente con Infrastructure Composer

AWS Infrastructure Composer (precedentemente noto come Application Composer) consente di comporre e configurare visivamente applicazioni moderne su AWS. Invece di scrivere codice, puoi trascinare e rilasciare diverse risorse per creare visivamente la tua applicazione.

Infrastructure Composer in modalità CloudFormation console è lo strumento consigliato per lavorare visivamente con CloudFormation i modelli. Questa versione di Infrastructure Composer a cui è possibile accedere dalla CloudFormation console è un miglioramento rispetto a uno strumento precedente chiamato AWS CloudFormation Designer.

Con Infrastructure Composer in modalità CloudFormation console, puoi trascinare, rilasciare, configurare e connettere una varietà di risorse, chiamate schede, su un'area di disegno visiva. Questo approccio visivo semplifica la progettazione e la modifica dell'architettura dell'applicazione senza dover lavorare direttamente con i modelli. Per accedere a questa modalità dalla [CloudFormation console](#), seleziona Infrastructure Composer dal menu di navigazione a sinistra.

Per ulteriori informazioni, consulta [How to compose in AWS Infrastructure Composer nella Developer Guide](#). AWS Infrastructure Composer

Perché usare Infrastructure Composer in modalità CloudFormation console?

La visualizzazione dei modelli in Infrastructure Composer consente di identificare le lacune e le aree di miglioramento nei modelli e nell'architettura delle applicazioni CloudFormation. Infrastructure Composer migliora l'esperienza di sviluppo grazie alla facilità e all'efficienza della creazione e della modifica visive degli stack CloudFormation. Puoi iniziare con una bozza iniziale, creare codice distribuibile e incorporare i flussi di lavoro degli sviluppatori con il visual designer in Infrastructure Composer.

In che modo questa modalità è diversa dalla console Infrastructure Composer?

Sebbene la versione CloudFormation console di Infrastructure Composer abbia caratteristiche simili alla console Infrastructure Composer standard, ci sono alcune differenze. Le schede relative a Lambda (Lambda Function e Lambda Layer) richiedono build di codice e soluzioni di packaging che non sono disponibili in Infrastructure Composer in modalità console. CloudFormation Inoltre, la sincronizzazione locale non è disponibile in questa modalità.

Tuttavia, puoi utilizzare queste schede relative a Lambda e la funzionalità di sincronizzazione locale nella console [Infrastructure Composer](#) o in AWS Toolkit for Visual Studio Code. Per ulteriori informazioni, consulta la Guida per gli [AWS Infrastructure Composer sviluppatori e Infrastructure Composer nella Guida](#) per l'utente AWS Toolkit for Visual Studio Code.

Genera modelli da risorse esistenti con il generatore IaC

Con l'CloudFormation infrastruttura come generatore di codice (generatore IaC), puoi generare un modello utilizzando AWS risorse fornite nel tuo account che non sono già gestite da CloudFormation.

Di seguito sono riportati i vantaggi del generatore IaC:

- CloudFormation Gestisci intere applicazioni o migrale in un' AWS CDK app.
- Genera modelli senza dover descrivere una risorsa proprietà per proprietà e poi tradurli in sintassi JSON o YAML.
- Usa il modello per replicare le risorse in un nuovo account o regione.

Il processo di generazione di IaC prevede i seguenti passaggi:

1. Scansiona le risorse: il primo passaggio consiste nell'avviare una scansione delle risorse. Questa scansione è valida per tutta la regione e scade dopo 30 giorni. Durante questo periodo, puoi creare più modelli dalla stessa scansione.
2. Crea il tuo modello: per creare il modello, hai due opzioni:
 - Crea un nuovo modello da zero e aggiungi le risorse scansionate e le risorse correlate.
 - Usa uno CloudFormation stack esistente come punto di partenza e aggiungi le risorse scansionate e le risorse correlate al relativo modello.
3. Importa risorse: utilizza il modello per importare le risorse come CloudFormation pila o migrarle in un'app AWS CDK.

La funzionalità del generatore IaC è disponibile in tutte le regioni commerciali e supporta molti tipi di risorse comuni AWS. Per un elenco completo delle risorse supportate, consulta [Supporto per tipi di risorse](#).

Argomenti

- [Considerazioni](#)

- [Autorizzazioni IAM necessarie per la scansione delle risorse](#)
- [Comandi comunemente usati per la generazione, la gestione e l'eliminazione dei modelli](#)
- [Esegui la migrazione di un modello verso AWS CDK](#)
- [Avvia una scansione delle risorse con il generatore CloudFormation IAc](#)
- [Visualizza il riepilogo della scansione nella CloudFormation console](#)
- [Crea un CloudFormation modello da risorse scansionate con il generatore IAc](#)
- [Crea uno CloudFormation stack da risorse scansionate](#)
- [Risolvi le proprietà di sola scrittura](#)

Considerazioni

Puoi generare modelli JSON o YAML per AWS risorse a cui hai accesso in lettura. I modelli per la funzionalità del generatore IAc modellano le risorse cloud in modo affidabile e rapido senza dover descrivere una risorsa proprietà per proprietà.

La tabella seguente elenca le quote disponibili per la funzionalità di generazione IAc.

Nome	Scansione completa	Scansione parziale
Numero massimo di risorse che possono essere elaborate in una scansione	100.000	100.000
Numero di scansioni al giorno (per scansioni con meno di 10.000 risorse)	10	10
Numero di scansioni al giorno (per scansioni con più di 10.000 risorse)	1	1
Numero simultaneo di modelli generati per account	5	5
Numero simultaneo di risorse modellate per una generazione di modelli	5	5
Numero totale di risorse che possono essere modellate in un modello	500	500

Nome	Scansione completa	Scansione parziale
Numero massimo di modelli generati per account	1.000	1.000

 Important

Il generatore IaC supporta solo AWS le risorse supportate dall'API Cloud Control nella tua regione. Per ulteriori informazioni, consulta [Supporto per tipi di risorse](#).

Autorizzazioni IAM necessarie per la scansione delle risorse

Per scansionare le risorse con il generatore IaC, il tuo principale IAM (utente, ruolo o gruppo) deve avere:

- CloudFormation autorizzazioni di scansione
- Autorizzazioni di lettura per i servizi di destinazione AWS

L'ambito di scansione è limitato alle risorse a cui hai accesso in lettura. Le autorizzazioni mancanti non causeranno errori di scansione ma escluderanno tali risorse.

Per un esempio di policy IAM che concede le autorizzazioni di scansione e gestione dei modelli, vedi. [Consenti tutte le operazioni del generatore IaC](#)

Comandi comunemente usati per la generazione, la gestione e l'eliminazione dei modelli

I comandi comunemente usati per lavorare con il generatore IaC includono:

- [start-resource-scan](#) per avviare una scansione delle risorse dell'account in un Regione AWS.
- [describe-resource-scan](#) per monitorare lo stato di avanzamento di una scansione delle risorse.
- [list-resource-scans](#) per elencare le scansioni delle risorse in un Regione AWS.
- [list-resource-scan-resources](#) per elencare le risorse trovate durante la scansione delle risorse.
- [list-resource-scan-related-resources](#) per elencare le risorse relative alle risorse scansionate.

- [create-generated-template](#) per generare un CloudFormation modello da un insieme di risorse scansionate.
- [update-generated-template](#) per aggiornare il modello generato.
- [describe-generated-template](#) per restituire informazioni su un modello generato.
- [list-generated-templates](#) per elencare tutti i modelli generati nel tuo account e nella regione corrente.
- [delete-generated-template](#) per eliminare un modello generato.

Esegui la migrazione di un modello verso AWS CDK

AWS Cloud Development Kit (AWS CDK) è un framework di sviluppo software open source che è possibile utilizzare per sviluppare, gestire e distribuire CloudFormation risorse utilizzando i linguaggi di programmazione più diffusi.

La AWS CDK CLI fornisce un'integrazione con il generatore IAc. Usa il `cdk migrate` comando AWS CDK CLI per convertire il CloudFormation modello e creare una nuova app CDK che contenga le tue risorse. Quindi, puoi utilizzare il AWS CDK per gestire le tue risorse e distribuirle su CloudFormation.

Per ulteriori informazioni, consulta [Migrate to AWS CDK](#) nella AWS Cloud Development Kit (AWS CDK) Developer Guide.

Avvia una scansione delle risorse con il generatore CloudFormation IAc

Prima di creare un modello da risorse esistenti, è necessario avviare una scansione delle risorse per scoprire le risorse attuali e le loro relazioni.

È possibile avviare una scansione delle risorse utilizzando una delle seguenti opzioni. Per gli utenti alle prime armi del generatore IAc, consigliamo la prima opzione.

- Scansiona tutte le risorse (scansione completa): esegue la scansione di tutte le risorse esistenti nell'account e nella regione correnti. Questo processo di scansione può richiedere fino a 10 minuti per 1.000 risorse.
- Scansione di risorse specifiche (scansione parziale): seleziona manualmente i tipi di risorse da scansionare nell'account e nella regione correnti. Questa opzione offre un processo di scansione più rapido e mirato, il che la rende ideale per lo sviluppo iterativo di modelli.

Una volta completata la scansione, puoi scegliere quali risorse e le relative risorse includere nella generazione del modello. Quando si utilizza la scansione parziale, le risorse correlate saranno disponibili durante la generazione del modello solo se:

- Le hai selezionate specificamente prima di iniziare la scansione, oppure
- Erano necessari per scoprire i tipi di risorse selezionati.

Ad esempio, se si seleziona `AWS::EKS::Nodegroup` senza selezionare `AWS::EKS::Cluster`, laC Generator include automaticamente `AWS::EKS::Cluster` le risorse nella scansione perché la scoperta del gruppo di nodi richiede prima la scoperta del cluster. In tutti gli altri casi, la scansione includerà solo le risorse selezionate specificamente.

Note

Prima di continuare, conferma di disporre delle autorizzazioni necessarie per lavorare con il generatore IaC. Per ulteriori informazioni, consulta [Autorizzazioni IAM necessarie per la scansione delle risorse](#).

Argomenti

- [Avvia una scansione delle risorse \(console\)](#)
- [Avvia una scansione delle risorse \(AWS CLI\)](#)

Avvia una scansione delle risorse (console)

Per avviare una scansione delle risorse di tutti i tipi (scansione completa)

1. Apri la [pagina del generatore IaC](#) della CloudFormation console.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS quello che contiene le risorse da scansionare.
3. Dal pannello Scansioni, scegli Avvia una nuova scansione, quindi scegli Scansiona tutte le risorse.

Per avviare una scansione delle risorse di tipi specifici (scansione parziale)

1. Apri la [pagina del generatore IaC](#) della CloudFormation console.

2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS quello che contiene le risorse da scansionare.
3. Dal pannello Scansioni, scegli Avvia una nuova scansione, quindi scegli Scansiona risorse specifiche.
4. Nella finestra di dialogo Avvia scansione parziale, selezionate fino a 100 tipi di risorse, quindi scegliete Avvia scansione.

Avvia una scansione delle risorse (AWS CLI)

Per avviare una scansione delle risorse di tutti i tipi (scansione completa)

Utilizza il seguente comando [start-resource-scan](#). Sostituisci *us-east-1* con quella Regione AWS che contiene le risorse da scansionare.

```
aws cloudformation start-resource-scan --region us-east-1
```

In caso di successo, questo comando restituisce l'ARN della scansione. Annotate l'ARN della ResourceScanId proprietà. Ti serve per creare il tuo modello.

```
{
  "ResourceScanId":
    "arn:aws:cloudformation:region:account-id:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60"
}
```

Per avviare una scansione delle risorse di tipi specifici (scansione parziale)

1. Usa il seguente comando [cat](#) per memorizzare i tipi di risorse che desideri scansionare in un file JSON denominato `config.json` nella tua home directory. Di seguito è riportato un esempio di configurazione di scansione che analizza EC2 le istanze Amazon, i gruppi di sicurezza e tutte le risorse Amazon S3.

```
$ cat > config.json
[
  {
    "Types": [
      "AWS::EC2::Instance",
      "AWS::EC2::SecurityGroup",
      "AWS::S3::*"
    ]
  }
]
```

```
]
}
]
```

2. Usa il [start-resource-scan](#) comando con l'`--scan-filters` opzione, insieme al `config.json` file che hai creato, per avviare la scansione parziale. Sostituisci `us-east-1` con Regione AWS quello che contiene le risorse da scansionare.

```
aws cloudformation start-resource-scan --scan-filters file://config.json --
region us-east-1
```

In caso di successo, questo comando restituisce l'ARN della scansione. Annotate l'ARN della `ResourceScanId` proprietà. Ti serve per creare il tuo modello.

```
{
  "ResourceScanId":
    "arn:aws:cloudformation:region:account-id:resourceScan/0a699f15-489c-43ca-
a3ef-3e6ecfa5da60"
}
```

Per monitorare l'avanzamento di una scansione delle risorse

Utilizza il comando [describe-resource-scan](#). Per l'`--resource-scan-id` opzione, sostituite l'ARN di esempio con l'ARN effettivo.

```
aws cloudformation describe-resource-scan --region us-east-1 \
--resource-scan-id arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
  "ResourceScanId": "arn:aws:cloudformation:region:account-
id:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60",
  "Status": "COMPLETE",
  "StartTime": "2023-08-21T03:10:38.485000+00:00",
  "EndTime": "2023-08-21T03:20:28.485000+00:00",
  "PercentageCompleted": 100.0,
  "ResourceTypes": [
    "AWS::CloudFront::CachePolicy",
```

```

    "AWS::CloudFront::OriginRequestPolicy",
    "AWS::EC2::DHCPOptions",
    "AWS::EC2::InternetGateway",
    "AWS::EC2::KeyPair",
    "AWS::EC2::NetworkAcl",
    "AWS::EC2::NetworkInsightsPath",
    "AWS::EC2::NetworkInterface",
    "AWS::EC2::PlacementGroup",
    "AWS::EC2::Route",
    "AWS::EC2::RouteTable",
    "AWS::EC2::SecurityGroup",
    "AWS::EC2::Subnet",
    "AWS::EC2::SubnetCidrBlock",
    "AWS::EC2::SubnetNetworkAclAssociation",
    "AWS::EC2::SubnetRouteTableAssociation",
    ...
  ],
  "ResourcesRead": 676
}
```

Per una scansione parziale, l'output sarà simile al seguente:

```

{
  "ResourceScanId": "arn:aws:cloudformation:region:account-id:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60",
  "Status": "COMPLETE",
  "StartTime": "2025-03-06T18:24:19.542000+00:00",
  "EndTime": "2025-03-06T18:25:23.142000+00:00",
  "PercentageCompleted": 100.0,
  "ResourceTypes": [
    "AWS::EC2::Instance",
    "AWS::EC2::SecurityGroup",
    "AWS::S3::Bucket",
    "AWS::S3::BucketPolicy"
  ],
  "ResourcesRead": 65,
  "ScanFilters": [
    {
      "Types": [
        "AWS::EC2::Instance",
        "AWS::EC2::SecurityGroup",
        "AWS::S3::*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

Per una descrizione dei campi dell'output, consulta [DescribeResourceScan](#) l'AWS CloudFormation API Reference.

Visualizza il riepilogo della scansione nella CloudFormation console

Una volta completata la scansione, puoi visualizzare una visualizzazione delle risorse trovate durante la scansione per aiutarti a identificare la concentrazione di risorse tra diversi tipi di prodotto.

Per visualizzare le informazioni sulle risorse trovate durante la scansione

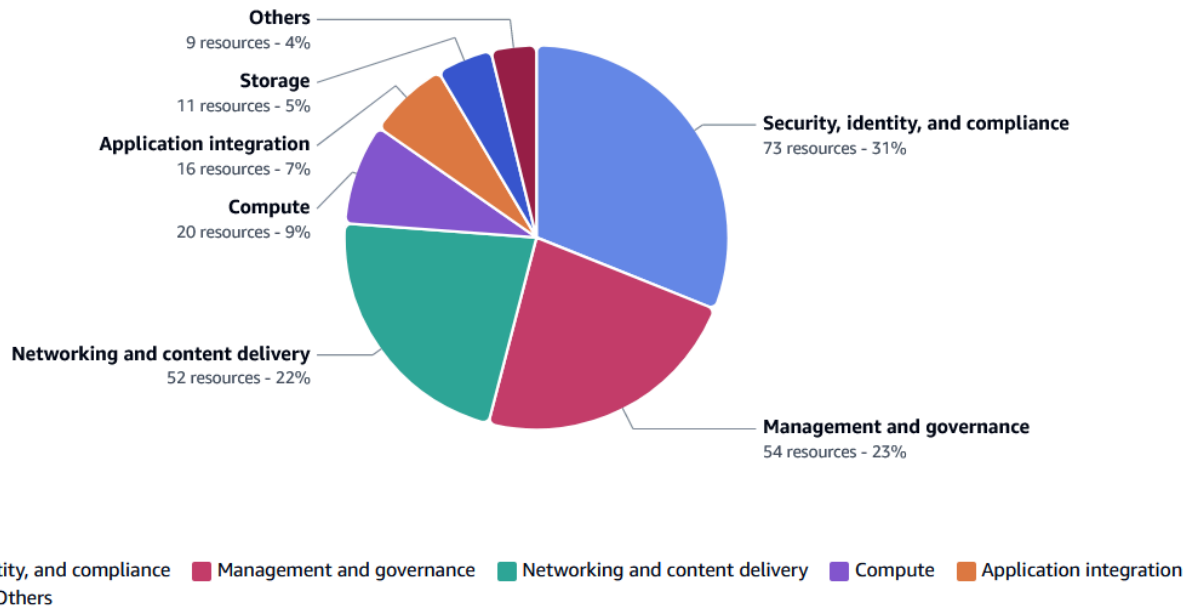
1. Aprire la [pagina del generatore IaC](#) della CloudFormation console.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS la scansione delle risorse da visualizzare.
3. Dal pannello di navigazione, scegli il generatore iAc.
4. In Suddivisione delle risorse scansionate, troverai una suddivisione visiva delle risorse scansionate per tipo di prodotto, ad esempio Compute and Storage.
5. Per personalizzare il numero di tipi di prodotto visualizzati, scegli Filtra i dati visualizzati. Questo ti aiuta a personalizzare la visualizzazione per concentrarti sui tipi di prodotto che ti interessano di più.
6. Sul lato destro della pagina è presente il pannello dei dettagli di riepilogo della scansione. Per aprire il pannello, scegli l'icona Apri pannello.

Scanned resources breakdown 235

View a visual breakdown of your scanned resources by product types. Select a product type for a further breakdown.

Filter displayed data

Filter by product type ▼



Crea un CloudFormation modello da risorse scansionate con il generatore IAc

Questo argomento spiega come creare un modello a partire da risorse che sono state scansionate utilizzando la funzionalità del generatore IAc.

Crea un modello dalle risorse scansionate (console)

Per creare un modello di pila a partire da risorse scansionate

1. Apri la [pagina del generatore IAc](#) della console. CloudFormation
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS quello che contiene le risorse scansionate.
3. Nella sezione Modelli, scegli Crea modello.
4. Scegli Inizia da un nuovo modello.
 - a. Per Nome modello, fornisci un nome per il tuo modello.

- b. (Facoltativo) Configura la politica di eliminazione e la politica di aggiornamento e sostituzione.
 - c. Scegli Avanti per aggiungere risorse scansionate al modello.
5. Per Aggiungi risorse scansionate, sfoglia l'elenco delle risorse scansionate e seleziona le risorse che desideri aggiungere al modello. Puoi filtrare le risorse per identificatore di risorsa, tipo di risorsa o tag. I filtri sono mutualmente inclusivi.
6. Dopo aver aggiunto tutte le risorse necessarie al modello, scegli Avanti per uscire dalla pagina Aggiungi risorse scansionate e passare alla pagina Aggiungi risorse correlate.
7. Consulta l'elenco consigliato di risorse correlate. Le risorse correlate, come le EC2 istanze Amazon e i gruppi di sicurezza, sono interdipendenti e in genere appartengono allo stesso carico di lavoro. Seleziona le risorse correlate che desideri includere nel modello generato.

Note

Ti suggeriamo di aggiungere tutte le risorse correlate a questo modello.

8. Esamina i dettagli del modello, le risorse scansionate e le risorse correlate.
9. Scegli Crea modello per uscire dalla pagina di revisione e creazione e creare il modello.

Crea un modello da risorse scansionate (AWS CLI)

Per creare un modello di pila a partire da risorse scansionate

1. Utilizzate il [list-resource-scan-resources](#) comando per elencare le risorse trovate durante la scansione, specificando facoltativamente l'`--resource-identifier` opzione per limitare l'output. Per l'`--resource-scan-id` opzione, sostituite l'ARN di esempio con l'ARN effettivo.

```
aws cloudformation list-resource-scan-resources \
  --resource-scan-id arn:aws:cloudformation:us-east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60 \
  --resource-identifier MyApp
```

Di seguito è riportato un esempio di risposta, in cui viene `ManagedByStack` indicato se la risorsa è CloudFormation già gestita. Copia l'output. Servirà per la fase successiva.

```
{
  "Resources": [
```



```
{
  "ResourceType": "AWS::EKS::Cluster",
  "ResourceIdentifier": {
    "ClusterName": "MyAppClusterName"
  },
  "ManagedByStack": false
},
{
  "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
  "ResourceIdentifier": {
    "AutoScalingGroupName": "MyAppASGName"
  },
  "ManagedByStack": false
}
]
```

Per una descrizione dei campi nell'output, consulta [ScannedResource](#) l'AWS CloudFormation API Reference.

- Utilizzate il `cat` comando per memorizzare i tipi di risorse e gli identificatori in un file JSON denominato `resources.json` nella vostra home directory. Di seguito è riportato un esempio di JSON basato sull'output di esempio del passaggio precedente.

```
$ cat > resources.json
[
  {
    "ResourceType": "AWS::EKS::Cluster",
    "ResourceIdentifier": {
      "ClusterName": "MyAppClusterName"
    }
  },
  {
    "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
    "ResourceIdentifier": {
      "AutoScalingGroupName": "MyAppASGName"
    }
  }
]
```

- Utilizzate il comando [list-resource-scan-related-resources](#), insieme al `resources.json` file creato, per elencare le risorse relative alle risorse analizzate.

```
aws cloudformation list-resource-scan-related-resources \
  --resource-scan-id arn:aws:cloudformation:us-east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60 \
  --resources file://resources.json
```

Di seguito è riportato un esempio di risposta, in cui `ManagedByStack` indica se CloudFormation gestisce già la risorsa. Aggiungi queste risorse al file JSON creato nel passaggio precedente. Ti servirà per creare il tuo modello.

```
{
  "RelatedResources": [
    {
      "ResourceType": "AWS::EKS::Nodegroup",
      "ResourceIdentifier": {
        "NodegroupName": "MyAppNodegroupName"
      },
      "ManagedByStack": false
    },
    {
      "ResourceType": "AWS::IAM::Role",
      "ResourceIdentifier": {
        "RoleId": "arn:aws:iam::account-id:role/MyAppIAMRole"
      },
      "ManagedByStack": false
    }
  ]
}
```

Per una descrizione dei campi nell'output, consulta [ScannedResource](#) l'AWS CloudFormation API Reference.

Note

L'elenco di risorse di input non può superare la lunghezza di 100. Per elencare le risorse correlate per più di 100 risorse, esegui il `list-resource-scan-related-resources` comando in batch di 100 e consolida i risultati.

Tieni presente che l'output può contenere risorse duplicate nell'elenco.

4. Utilizzate il [create-generated-template](#) comando per creare un nuovo modello di stack, come segue, con queste modifiche:

- Sostituisci *us-east-1* con quello Regione AWS che contiene le risorse scansionate.
- Sostituisci *MyTemplate* con il nome del modello da creare.

```
aws cloudformation create-generated-template --region us-east-1 \  
--generated-template-name MyTemplate \  
--resources file://resources.json
```

Di seguito è riportato un esempio del file `resources.json`.

```
[  
  {  
    "ResourceType": "AWS::EKS::Cluster",  
    "LogicalResourceId": "MyCluster",  
    "ResourceIdentifier": {  
      "ClusterName": "MyAppClusterName"  
    }  
  },  
  {  
    "ResourceType": "AWS::AutoScaling::AutoScalingGroup",  
    "LogicalResourceId": "MyASG",  
    "ResourceIdentifier": {  
      "AutoScalingGroupName": "MyAppASGName"  
    }  
  },  
  {  
    "ResourceType": "AWS::EKS::Nodegroup",  
    "LogicalResourceId": "MyNodegroup",  
    "ResourceIdentifier": {  
      "NodegroupName": "MyAppNodegroupName"  
    }  
  },  
  {  
    "ResourceType": "AWS::IAM::Role",  
    "LogicalResourceId": "MyRole",  
    "ResourceIdentifier": {  
      "RoleId": "arn:aws::iam::account-id:role/MyAppIAMRole"  
    }  
  }  
]
```

```
]
```

In caso di successo, questo comando restituisce quanto segue.

```
{
  "Arn":
    "arn:aws:cloudformation:region:account-id:generatedtemplate/7fc8512c-d8cb-4e02-
    b266-d39c48344e48",
  "Name": "MyTemplate"
}
```

Crea uno CloudFormation stack da risorse scansionate

Dopo aver creato il modello, puoi visualizzare in anteprima il modello generato con Infrastructure Composer prima di creare lo stack e importare le risorse scansionate. Ciò consente di visualizzare l'architettura completa dell'applicazione con le risorse e le relative relazioni. Per ulteriori informazioni su Infrastructure Composer, vedere. [Crea modelli visivamente con Infrastructure Composer](#)

Per creare lo stack e importare le risorse scansionate

1. Apri la [pagina del generatore iAc](#) della console. CloudFormation
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il modello Regione AWS per il tuo modello.
3. Scegli la scheda Modelli, quindi scegli il nome del modello per visualizzare ulteriori informazioni.
4. Nella scheda Definizione del modello, nella parte superiore della sezione Modello, puoi cambiare il modello dalla sintassi YAML a quella JSON in base alle tue preferenze.
5. Controlla i dettagli del modello per assicurarti che tutto sia configurato correttamente. Per semplificare la revisione e la comprensione del modello, puoi passare dalla visualizzazione del codice predefinita a una visualizzazione grafica dell'infrastruttura descritta nel modello utilizzando Infrastructure Composer. Per fare ciò, in Modello, scegli Canvas anziché Template.

Azioni Canvas

- Per concentrarti sui dettagli di una risorsa specifica all'interno del modello, fai doppio clic su una scheda per visualizzare il pannello delle proprietà della risorsa.
- Per disporre e organizzare visivamente le carte sulla tela, scegli Disponi nella parte superiore sinistra dell'area di disegno.

- Per ingrandire e rimpicciolire la tela, usa i controlli di zoom in basso a destra della tela.
6. Per visualizzare una risorsa specifica nella console, scegli la scheda Risorse modello, quindi scegli l'ID fisico della risorsa che vuoi guardare. Verrai indirizzato alla console relativa a quella risorsa specifica. È inoltre possibile aggiungere, rimuovere e risincronizzare le risorse nella definizione del modello dalla scheda Risorse del modello.
 7. Nella scheda Definizione del modello, il generatore IaC potrebbe emettere avvisi sulle risorse che contengono proprietà di sola scrittura. Dopo aver esaminato gli avvisi, è possibile scaricare il modello generato e apportare le modifiche necessarie. Per ulteriori informazioni, consulta [Risolvi le proprietà di sola scrittura](#).
 8. Quando sei soddisfatto della definizione del modello, nella scheda Definizione modello scegli Importa in pila, quindi scegli Avanti.
 9. Nel pannello Specificare lo stack della pagina Specificare i dettagli dello stack, immettete il nome dello stack, quindi scegliete Avanti.
 10. Esamina e inserisci i parametri per lo stack. Scegli Next (Successivo).
 11. Controlla le opzioni disponibili nella pagina Rivedi le modifiche e scegli Avanti.
 12. Controlla i tuoi dati nella pagina Rivedi e importa e scegli Importa risorse.

Risolvi le proprietà di sola scrittura

Con il generatore CloudFormation IaC, puoi generare un modello utilizzando risorse fornite nel tuo account che non sono già gestite da CloudFormation. Tuttavia, alcune proprietà delle risorse sono designate come di sola scrittura, il che significa che possono essere scritte ma non possono essere lette, ad esempio CloudFormation, da una password del database.

Quando si generano CloudFormation modelli a partire da risorse esistenti, le proprietà di sola scrittura rappresentano una sfida. Nella maggior parte dei casi, CloudFormation converte queste proprietà in parametri nel modello generato. Ciò consente di inserire le proprietà come valori dei parametri durante le operazioni di importazione. Tuttavia, esistono scenari in cui questa conversione non è possibile e CloudFormation gestisce questi casi in modo diverso.

Proprietà che si escludono a vicenda

Alcune risorse dispongono di più set di proprietà che si escludono a vicenda, almeno alcune delle quali sono di sola scrittura. In questi casi, il generatore IaC non è in grado di determinare quale insieme di proprietà esclusive è stato applicato alla risorsa durante la creazione. Ad esempio, è possibile fornire il codice per l'[AWS::Lambda::Function](#) utilizzo di uno di questi set di proprietà.

- Code/S3BucketCode/S3Keye facoltativamente Code/S3ObjectVersion
- Code/ImageUri
- Code/ZipFile

Tutte queste proprietà sono di sola scrittura. Il generatore IAc seleziona uno dei set esclusivi di proprietà e li aggiunge al modello generato. I parametri vengono aggiunti per ciascuna delle proprietà di sola scrittura. I nomi dei parametri includono OneOf e le relative descrizioni indicano che la proprietà corrispondente può essere sostituita con altre proprietà esclusive. Il generatore IAc imposta un tipo di avviso MUTUALLY_EXCLUSIVE_PROPERTIES per le proprietà incluse.

Tipi che si escludono a vicenda

In alcuni casi, una proprietà di sola scrittura può contenere più tipi di dati. Ad esempio, la Body proprietà di [AWS::ApiGateway::RestApi](#) può essere un object o un. string In questo caso, il generatore IAc include la proprietà nel modello generato utilizzando il tipo di string e imposta un tipo di avviso di MUTUALLY_EXCLUSIVE_TYPES.

Proprietà Array

Se una proprietà di sola scrittura ha un tipo di array, il generatore IAc non può includerla nel modello generato perché i parametri possono essere solo valori scalari. In questo caso, la proprietà viene omessa dal modello e viene impostato un tipo di avviso di. UNSUPPORTED_PROPERTIES

Proprietà facoltative

Per le proprietà opzionali di sola scrittura, il generatore IAc non è in grado di rilevare se la proprietà è stata utilizzata durante l'impostazione della risorsa. In questo caso, la proprietà viene omessa dal modello generato e viene impostato un tipo di avviso di. UNSUPPORTED_PROPERTIES

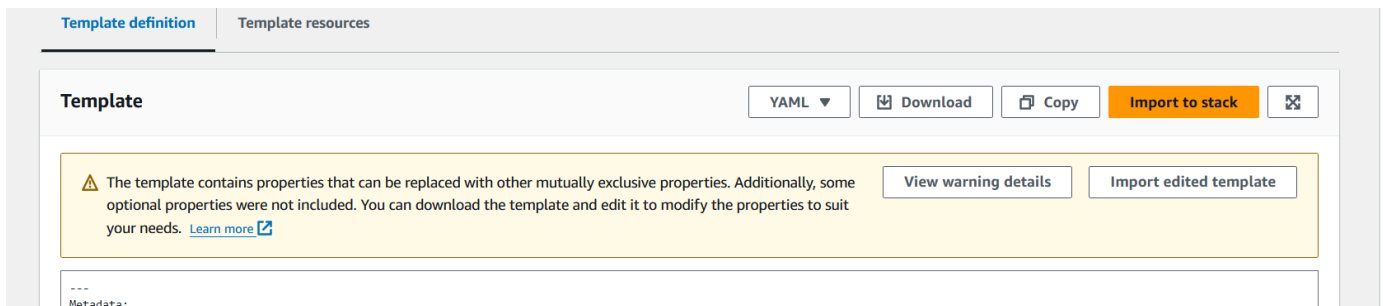
Avvertenze e fasi successive

Per determinare quali proprietà sono di sola scrittura, è necessario esaminare gli avvisi restituiti dalla console del generatore IAc. Il [riferimento ai tipi di AWS risorse e proprietà](#) non indica se una proprietà è di sola scrittura o se supporta più tipi.

In alternativa, potete vedere quali proprietà sono di sola scrittura dagli schemi dei provider di risorse. [Per scaricare gli schemi dei provider di risorse, consultate gli schemi dei CloudFormation provider di risorse.](#)

Per risolvere i problemi relativi alle proprietà di sola scrittura

1. Apri la [pagina del generatore IAc](#) della console. CloudFormation
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il modello Regione AWS per il tuo modello.
3. Scegli la scheda Modelli, quindi scegli il nome del modello che hai creato.
4. Nella scheda Definizione del modello, quando il modello generato include risorse con proprietà di sola scrittura, la console del generatore IAc visualizza un avviso con un riepilogo del tipo di problemi. Per esempio:



5. Scegli Visualizza i dettagli degli avvisi per maggiori dettagli. Le risorse con proprietà di sola scrittura sono identificate dall'ID logico utilizzato nel modello e nel tipo di risorsa generati.

Utilizza l'elenco di avvisi per identificare le risorse con proprietà di sola scrittura e analizza ogni risorsa per determinare quali modifiche (se presenti) devono essere apportate al modello generato.

Resource warnings (1)

▼ **LambdaFunction001aClambda002fd6K (AWS::Lambda::Function)** [Learn more](#)

Unsupported properties	Mutually exclusive properties
1. SnapStart/ApplyOn Applying SnapStart setting on function resource type. Possible values: [PublishedVersions, None] This property can be replaced with other types	1. Code/S3Bucket An Amazon S3 bucket in the same AWS Region as your function. The bucket can be in a different AWS account. This property can be replaced with other exclusive properties
2. Code/S3ObjectVersion For versioned objects, the version of the deployment package object to use. This property can be replaced with other exclusive properties	2. Code/S3Key The Amazon S3 key of the deployment package. This property can be replaced with other exclusive properties

6. Se il modello deve essere aggiornato per risolvere problemi con le proprietà di sola scrittura, procedi come segue:
 - a. Scegli Scarica per scaricare una copia del modello.
 - b. Modifica il modello.

- c. Una volta completate le modifiche, puoi scegliere il pulsante **Importa modello modificato** per continuare il processo di importazione.

Come risolvere i problemi relativi alle proprietà di sola scrittura nelle risorse `AWS::ApiGateway::RestAPI`

Questo argomento spiega come risolvere i problemi relativi alle proprietà di sola scrittura nelle [AWS::ApiGateway::RestAPI](#) risorse quando si utilizza il generatore IAc.

Problema

Quando un modello generato contiene `AWS::ApiGateway::RestApi` risorse, vengono generati avvisi che lo indicano e `CloneFrom` le proprietà vengono `Body` identificate `BodyS3Location` come. `UNSUPPORTED_PROPERTIES` Questo perché si tratta di proprietà opzionali di sola scrittura. Il generatore IAc non sa se queste proprietà siano mai state applicate alla risorsa. Pertanto, omette queste proprietà nel modello generato.

Risoluzione

Per impostare la `Body` proprietà per la tua API REST, aggiorna il modello generato.

1. Utilizza l'azione API Amazon [GetExport](#) API Gateway per scaricare l'API. Ad esempio, utilizzando il [aws apigateway get-export](#) AWS CLI comando. Per ulteriori informazioni, [consulta Esportazione di un'API REST da API Gateway](#) nella Guida per sviluppatori di API Gateway.
2. Recupera la `Body` proprietà dalla risposta dell'azione `GetExport` API. Caricalo in un bucket Amazon S3.
3. Scarica il modello generato.
4. Aggiungi le `BodyS3Location/Key` proprietà `BodyS3Location/Bucket` and al modello, specificando il nome del bucket e la chiave in cui `Body` è memorizzato.
5. Apri il modello generato nella console del generatore IAc e scegli **Importa modello modificato**.

Come risolvere i problemi relativi alle proprietà di sola scrittura nelle risorse `AWS::Lambda::Function`

Questo argomento spiega come risolvere i problemi relativi alle proprietà di sola scrittura nelle [AWS::Lambda::Function](#) risorse quando si utilizza il generatore IAc.

Problema

La `AWS::Lambda::Function` risorsa dispone di tre set di proprietà che si escludono a vicenda per specificare il codice Lambda:

- `Code/S3Bucket` `Code/S3Key` proprietà e, facoltativamente, la proprietà `Code/S3ObjectVersion`
- `Code/ImageUri` property
- `Code/ZipFile` property

È possibile utilizzare solo uno di questi set per una determinata `AWS::Lambda::Function` risorsa.

Il generatore IAc non è in grado di determinare quale set di proprietà esclusive di sola scrittura è stato utilizzato per creare o aggiornare la risorsa. Di conseguenza, include solo il primo set di proprietà nel modello generato. Le `Code/ZipFile` proprietà `Code/ImageUri` and vengono omesse.

Inoltre, il generatore IAc emette i seguenti avvisi:

- **MUTUALLY_EXCLUSIVE_PROPERTIES**— Lo avverte `Code/S3Bucket` e `Code/S3Key` vengono identificate come proprietà che si escludono a vicenda.
- **UNSUPPORTED_PROPERTIES**— Avverte che la proprietà non è supportata. `Code/S3ObjectVersion`

Per includere `AWS::Lambda::Function` risorse in un modello generato, è necessario scaricare e aggiornare il modello con le proprietà del codice corrette.

Risoluzione

Se memorizzi il codice Lambda in un bucket Amazon S3 e non utilizzi **`S3ObjectVersion`** la proprietà, puoi importare il modello generato senza alcuna modifica. Il generatore IAc ti chiederà il bucket e la chiave Amazon S3 come parametri del modello durante l'operazione di importazione.

Se memorizzi il codice Lambda come repository Amazon ECR, puoi aggiornare il modello utilizzando le seguenti istruzioni:

1. Scarica il modello generato.
2. Rimuove le proprietà e i parametri corrispondenti per le `Code/S3Key` proprietà `Code/S3Bucket` and dal modello generato.

3. Sostituisci le proprietà rimosse nel modello generato con la `Code/ImageUri` proprietà, specificando l'URL per il repository Amazon ECR.
4. Apri il modello generato nella console del generatore IAc e scegli il pulsante Importa modello modificato.

Se memorizzi il codice Lambda come in un file zip, puoi aggiornare il modello seguendo le seguenti istruzioni:

1. Scarica il modello generato.
2. Rimuove le proprietà e i parametri corrispondenti per le `Code/S3Key` proprietà `Code/S3Bucket` and dal modello generato.
3. Sostituite le proprietà rimosse nel modello generato con la `Code/ZipFile` proprietà.
4. Apri il modello generato nella console del generatore iAc e scegli il pulsante Importa modello modificato.

Se non disponi di una copia del codice Lambda, puoi aggiornare il modello seguendo le seguenti istruzioni:

1. Utilizza l'azione AWS Lambda [GetFunction](#) API (ad esempio, utilizzando il [aws lambda get-function](#) AWS CLI comando).
2. Nella risposta, il `RepositoryType` parametro indica S3 se il codice si trova in un bucket Amazon S3 o ECR se il codice si trova in un repository Amazon ECR.
3. Nella risposta, il `Location` parametro contiene un URL predefinito che puoi utilizzare per scaricare il pacchetto di distribuzione per 10 minuti. Scarica il codice.
4. Carica il codice in un bucket Amazon S3.
5. Esegui un'operazione di importazione con il modello generato e fornisci il nome e la chiave del bucket come valori dei parametri.

Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici

I riferimenti dinamici offrono un modo pratico per specificare i valori esterni archiviati e gestiti in altri servizi e disaccoppiare le informazioni sensibili dai modelli. `infrastructure-as-code` CloudFormation recupera il valore del riferimento specificato quando necessario durante le operazioni di stack e change set.

Con i riferimenti dinamici, è possibile:

- Usa stringhe sicure: per i dati sensibili, utilizza sempre parametri di stringa sicuri in AWS Systems Manager Parameter Store o segreti AWS Secrets Manager per garantire che i dati siano crittografati quando sono inattivi.
- Limita l'accesso: limita l'accesso ai parametri Parameter Store o ai segreti di Secrets Manager solo ai principali e ai ruoli autorizzati.
- Ruota le credenziali: ruota regolarmente i dati sensibili archiviati in Parameter Store o Secrets Manager per mantenere un elevato livello di sicurezza.
- Rotazione automatica: sfrutta le funzionalità di rotazione automatica di Secrets Manager per aggiornare e distribuire periodicamente i dati sensibili tra le applicazioni e gli ambienti.

Considerazioni generali

Di seguito sono riportate le considerazioni generali da considerare prima di specificare riferimenti dinamici nei modelli: CloudFormation

- Evita di includere riferimenti dinamici o dati sensibili nelle proprietà delle risorse che fanno parte dell'identificatore principale di una risorsa. CloudFormation può utilizzare l'effettivo valore di testo in chiaro nell'identificatore della risorsa principale, il che potrebbe rappresentare un rischio per la sicurezza. Questo ID risorsa può apparire in qualsiasi output o destinazione derivata.

Per determinare quali proprietà della risorsa costituiscono l'identificatore principale di un tipo di risorsa, fate riferimento alla documentazione di riferimento della risorsa relativa a tale [AWS risorsa](#) nel riferimento ai tipi di risorse e proprietà. Nella sezione Return values (Valori restituiti), il valore restituito della funzione Ref rappresenta le proprietà delle risorse che comprendono l'identificatore principale del tipo di risorsa.

- È possibile includere fino a 60 riferimenti dinamici in un modello di stack.
- Se utilizzi trasformazioni (come `AWS::Include` o `AWS::Serverless`), CloudFormation non risolve i riferimenti dinamici prima di applicare la trasformazione. Passa invece la stringa letterale del riferimento dinamico alla trasformazione e risolve i riferimenti quando si esegue il set di modifiche utilizzando il modello.
- I riferimenti dinamici non possono essere utilizzati per valori sicuri (come quelli archiviati in Parameter Store o Secrets Manager) nelle risorse personalizzate.
- Inoltre, i riferimenti dinamici non sono supportati nei `AWS::CloudFormation::Init` metadati e nelle EC2 UserData proprietà Amazon.

- Non creare un riferimento dinamico che termini con una barra rovesciata (\). CloudFormation non è in grado di risolvere questi riferimenti, il che causerà il fallimento delle operazioni di stack.

I seguenti argomenti forniscono informazioni e altre considerazioni sull'utilizzo dei riferimenti dinamici.

Argomenti

- [Ottieni un valore in testo semplice da Systems Manager Parameter Store](#)
- [Ottieni un valore di stringa sicuro da Systems Manager Parameter Store](#)
- [Ottieni un valore segreto o segreto da Secrets Manager](#)

Ottieni un valore in testo semplice da Systems Manager Parameter Store

Quando crei un CloudFormation modello, potresti voler utilizzare valori di testo in chiaro memorizzati in Parameter Store. Parameter Store è una funzionalità di AWS Systems Manager. Per un'introduzione a Parameter Store, vedere [AWS Systems Manager Parameter Store](#) nella Guida AWS Systems Manager per l'utente.

Per utilizzare un valore di testo semplice di Parameter Store all'interno del modello, si utilizza un riferimento ssm dinamico. Questo riferimento consente di accedere ai valori dai parametri di tipo String o StringList in Parameter Store.

Per verificare quale versione di un riferimento ssm dinamico verrà utilizzata in un'operazione di pila, create un set di modifiche per l'operazione di pila. Quindi, esaminate il modello elaborato nella scheda Modello. Per ulteriori informazioni, consulta [Creare un set di modifiche per uno CloudFormation stack](#).

Quando si utilizzano riferimenti ssm dinamici, ci sono alcune cose importanti da tenere a mente:

- CloudFormation non supporta il rilevamento della deriva sui riferimenti dinamici. Per i riferimenti ssm dinamici in cui non è stata specificata la versione del parametro, si consiglia, se si aggiorna la versione del parametro in Systems Manager, di eseguire anche un'operazione di aggiornamento dello stack su tutti gli stack che includono il riferimento ssm dinamico, per recuperare la versione più recente dei parametri.
- Per utilizzare un riferimento ssm dinamico nella Parameters sezione del CloudFormation modello, è necessario includere un numero di versione. CloudFormation non consente di fare riferimento a un valore di Parameter Store senza un numero di versione in questa sezione. In alternativa, è possibile definire il parametro come tipo di parametro Systems Manager nel modello. Quando si

esegue questa operazione, è possibile specificare una chiave del parametro Systems Manager come valore predefinito per il parametro. CloudFormation recupererà quindi la versione più recente del valore del parametro da Parameter Store, senza che sia necessario specificare un numero di versione. Questo può rendere i modelli più semplici e facili da gestire. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#).

- Per le risorse personalizzate, CloudFormation risolve i riferimenti ssm dinamici prima di inviare la richiesta alla risorsa personalizzata.
- CloudFormation non supporta l'utilizzo di riferimenti dinamici per fare riferimento a un parametro condiviso da un altro. Account AWS
- CloudFormation non supporta l'utilizzo delle etichette dei parametri di Systems Manager nei riferimenti dinamici.

Autorizzazioni

Per specificare un parametro memorizzato nell'archivio dei parametri di Systems Manager, è necessario disporre dell'autorizzazione [GetParameters](#) per richiamare il parametro specificato. Per scoprire come creare policy IAM che forniscano l'accesso a parametri specifici di Systems Manager, consulta [Restricting access to Systems Manager using IAM policies](#) nella AWS Systems Manager User Guide.

Schema di riferimento

Per fare riferimento a un valore di testo semplice memorizzato in Systems Manager Parameter Store nel CloudFormation modello, utilizzare il seguente schema ssm di riferimento.

```
{{resolve:ssm:parameter-name:version}}
```

Il riferimento deve essere conforme allo schema di espressione regolare per *parameter-name* e *version*:

```
{{resolve:ssm:[a-zA-Z0-9_.\-/+](?:\d+)?}}
```

parameter-name

Il nome del parametro in Archivio parametri . Il nome di parametro prevede la distinzione tra lettere maiuscole e minuscole.

Obbligatorio.

version

Un numero intero che specifica la versione del parametro da utilizzare. Se non specificate la versione esatta, CloudFormation utilizza la versione più recente del parametro ogni volta che create o aggiornate lo stack. Per ulteriori informazioni, consultate [Lavorare con le versioni dei parametri](#) nella Guida per l'AWS Systems Manager utente.

Facoltativo.

Esempio

L'esempio seguente crea un modello di EC2 avvio che fa riferimento a un ID AMI personalizzato memorizzato nel Parameter Store. Il riferimento dinamico recupera l'ID AMI dalla versione **2** del *golden-ami* parametro ogni volta che un'istanza viene avviata dal modello di avvio.

JSON

```
{
  "Resources": {
    "MyLaunchTemplate": {
      "Type": "AWS::EC2::LaunchTemplate",
      "Properties": {
        "LaunchTemplateName": {
          "Fn::Sub": "${AWS::StackName}-launch-template"
        },
        "LaunchTemplateData": {
          "ImageId": "${resolve:ssm:golden-ami:2}",
          "InstanceType": "t2.micro"
        }
      }
    }
  }
}
```

YAML

```
Resources:
  MyLaunchTemplate:
    Type: AWS::EC2::LaunchTemplate
    Properties:
```

```
LaunchTemplateName: !Sub ${AWS::StackName}-launch-template
LaunchTemplateData:
  ImageId: '{{resolve:ssm:golden-ami:2}}'
  InstanceType: t2.micro
```

Ottieni un valore di stringa sicuro da Systems Manager Parameter Store

In CloudFormation, puoi utilizzare dati sensibili come password o chiavi di licenza senza esporli direttamente nei tuoi modelli, archiviando i dati sensibili come «stringa sicura» in AWS Systems Manager Parameter Store. Per un'introduzione a Parameter Store, vedete [AWS Systems Manager Parameter Store](#) nella Guida per l'AWS Systems Manager utente.

Per utilizzare una stringa sicura di Parameter Store all'interno del modello, si utilizza un riferimento `ssm-secure` dinamico. CloudFormation non memorizza mai il valore effettivo della stringa sicura. Memorizza invece solo il riferimento dinamico letterale, che contiene il nome del parametro in testo semplice della stringa sicura.

Durante la creazione o gli aggiornamenti dello stack, CloudFormation accede al valore della stringa sicura secondo necessità, senza esporre il valore effettivo. Le stringhe sicure possono essere utilizzate solo per le proprietà delle risorse che supportano il `ssm-secure` modello di riferimento dinamico. Per ulteriori informazioni, consulta [Risorse che supportano schemi di parametri dinamici per stringhe sicure](#).

CloudFormation non restituisce il valore effettivo del parametro per le stringhe sicure in nessuna chiamata API. Restituisce solo il riferimento dinamico letterale. Quando si confrontano le modifiche utilizzando i set di modifiche, confronta CloudFormation solo la stringa di riferimento dinamica letterale. Non risolve e non confronta i valori effettivi delle stringhe sicure.

Quando si utilizzano riferimenti `ssm-secure` dinamici, ci sono alcune cose importanti da tenere a mente:

- CloudFormation non può accedere ai valori di Parameter Store da altri Account AWS.
- CloudFormation non supporta l'uso delle etichette dei parametri di Systems Manager o dei parametri pubblici nei riferimenti dinamici.
- Nelle `cn-northwest-1` regioni `cn-north-1` e, le stringhe sicure non sono supportate da Systems Manager.
- I riferimenti dinamici per valori sicuri, ad esempio `ssm-secure`, non sono attualmente supportati nelle risorse personalizzate.

- Se è CloudFormation necessario ripristinare un aggiornamento dello stack e la versione specificata in precedenza di un parametro di stringa sicuro non è più disponibile, l'operazione di rollback avrà esito negativo. In questi casi, sono disponibili due opzioni:
 - Utilizza `CONTINUE_UPDATE_ROLLBACK` per ignorare la risorsa.
 - Ricrea il parametro di stringa sicura in Archivio parametri Systems Manager e aggiornalo fino a che la versione del parametro è identica alla versione utilizzata nel modello. Quindi, usa `CONTINUE_UPDATE_ROLLBACK` senza saltare la risorsa.

Risorse che supportano schemi di parametri dinamici per stringhe sicure

Le risorse che supportano il modello di riferimento `ssm-secure` dinamico includono:

Risorsa	Tipo di proprietà	Proprietà
AWS::DirectoryService::MicrosoftAD		Password
AWS::DirectoryService::SimpleANNUNCIO		Password
AWS::ElastiCache::ReplicationGroup		AuthToken
AWS::IAM::User	LoginProfile	Password
AWS::KinesisFirehose::DeliveryStream	RedshiftDestinationConfiguration	Password
AWS::OpsWorks::App	Origine	Password
AWS::OpsWorks::Stack	CustomCookbooksSource	Password
AWS::OpsWorks::Stack	RdsDbInstances	DbPassword
AWS::RDS::DBCluster		MasterUserPassword
AWS::RDS::DBInstance		MasterUserPassword
AWS::Redshift::Cluster		MasterUserPassword

Schema di riferimento

Per fare riferimento a un valore di stringa sicuro da Systems Manager Parameter Store nel CloudFormation modello, utilizzare il seguente schema `ssm-secure` di riferimento.

```
{{resolve:ssm-secure:parameter-name:version}}
```

Il riferimento deve essere conforme allo schema di espressione regolare per `parameter-name` e `version`:

```
{{resolve:ssm-secure:[a-zA-Z0-9_.\-/]+(:\d+)?}}
```

`parameter-name`

Il nome del parametro in Archivio parametri . Il nome di parametro prevede la distinzione tra lettere maiuscole e minuscole.

Obbligatorio.

`version`

Un numero intero che specifica la versione del parametro da utilizzare. Se non specificate la versione esatta, CloudFormation utilizza la versione più recente del parametro ogni volta che create o aggiornate lo stack. Per ulteriori informazioni, consultate [Lavorare con le versioni dei parametri](#) nella Guida per l'AWS Systems Manager utente.

Facoltativo.

Esempio

L'esempio seguente utilizza un riferimento `ssm-secure` dinamico per impostare la password di un utente IAM su una stringa sicura memorizzata in Parameter Store. Come specificato, CloudFormation utilizzerà la versione **10** del ***IAMUserPassword*** parametro per le operazioni di stack e change set.

JSON

```
"MyIAMUser": {
  "Type": "AWS::IAM::User",
  "Properties": {
    "UserName": "MyUserName",
    "LoginProfile": {
```

```
    "Password": "{{resolve:ssm-secure:IAMUserPassword:10}}"}
  }
}
```

YAML

```
MyIAMUser:
  Type: AWS::IAM::User
  Properties:
    Username: 'MyUserName'
    LoginProfile:
      Password: '{{resolve:ssm-secure:IAMUserPassword:10}}'
```

Ottieni un valore segreto o segreto da Secrets Manager

Secrets Manager è un servizio che consente di archiviare e gestire in modo sicuro segreti come credenziali di database, password e chiavi API di terze parti. Con Secrets Manager puoi archiviare e controllare centralmente l'accesso a questi segreti, in modo da poter sostituire le credenziali con codifica fissa nel codice (incluse le password), con una chiamata API a Secrets Manager per recuperare il segreto a livello di programmazione. [Per ulteriori informazioni, consulta Cos'è? AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Per utilizzare interi segreti o valori segreti archiviati in Secrets Manager all'interno dei CloudFormation modelli, si utilizzano riferimenti `secretsmanager` dinamici.

Considerazioni

Quando si utilizzano riferimenti `secretsmanager` dinamici, è necessario tenere a mente alcune importanti considerazioni sulla sicurezza:

- Il riferimento dinamico `secretsmanager` può essere utilizzato in tutte le proprietà di risorsa. L'utilizzo del riferimento `secretsmanager` dinamico indica che né Secrets Manager né CloudFormation i log devono mantenere alcun valore segreto risolto. Tuttavia, il valore di segreto può essere visualizzato nel servizio proprietario della risorsa in cui è utilizzato. Rivedi l'utilizzo per evitare perdite di dati segreti.
- L'aggiornamento di un segreto in Secrets Manager non aggiorna automaticamente il segreto in CloudFormation. CloudFormation Per aggiornare un riferimento `secretsmanager` dinamico, è necessario eseguire un aggiornamento dello stack che aggiorni la risorsa contenente il riferimento

dinamico, aggiornando la proprietà della risorsa che contiene il riferimento `secretsmanager` dinamico o aggiornando un'altra proprietà della risorsa.

Supponiamo, ad esempio, che nel modello specifichi la proprietà `MasterPassword` di una risorsa [AWS::RDS::DBInstance](#) come riferimento dinamico `secretsmanager`, e poi crei uno stack dal modello. Successivamente puoi aggiornare il valore del segreto in Secrets Manager, ma non la risorsa `AWS::RDS::DBInstance` nel modello. In questo caso, anche se si esegue un aggiornamento dello stack, il valore segreto nella proprietà `MasterPassword` non viene aggiornato e rimane il valore segreto precedente.

Inoltre, ti consigliamo di utilizzare Secrets Manager per ruotare automaticamente il segreto per un servizio o un database protetto. Per ulteriori informazioni, consulta [Rotazione dei segreti AWS Secrets Manager](#).

- I riferimenti dinamici per valori sicuri, ad esempio `secretsmanager`, non sono attualmente supportati nelle risorse personalizzate.

Autorizzazioni

Per specificare un segreto archiviato in Secrets Manager, è necessario disporre dell'autorizzazione [GetSecretValue](#) per richiamare il segreto.

Schema di riferimento

Per fare riferimento ai segreti di Secrets Manager nel tuo CloudFormation modello, usa il seguente schema `secretsmanager` di riferimento.

```
{{resolve:secretsmanager:secret-id:secret-string:json-key:version-stage:version-id}}
```

`secret-id`

Il nome o l'ARN del segreto.

Per accedere a un segreto nel tuo Account AWS, devi solo specificare il nome del segreto. Per accedere a un segreto in un altro Account AWS, specifica l'ARN completo del segreto.

Obbligatorio.

`secret-string`

L'unico valore supportato è `SecretString`. Il valore predefinito è `SecretString`.

json-key

Il nome della chiave della coppia chiave-valore di cui intendi recuperare il valore. Se non specifichi `json-key`, CloudFormation recupera l'intero testo segreto.

Questo segmento può non includere il carattere di due punti (:).

version-stage

L'etichetta temporanea della versione del segreto da utilizzare. Secrets Manager utilizza le etichette temporanee per tenere traccia delle differenti versioni durante il processo di rotazione. Se utilizzi `version-stage`, non specificare `version-id`. Se non specifichi né `version-stage` né `version-id`, la versione di default sarà la `AWSCURRENT`.

Questo segmento può non includere il carattere di due punti (:).

version-id

L'identificatore univoco della versione del segreto da utilizzare. Se specifichi `version-id`, non è necessario specificare anche `version-stage`. Se non specifichi né `version-stage` né `version-id`, la versione di default sarà la `AWSCURRENT`.

Questo segmento può non includere il carattere di due punti (:).

Esempi

Argomenti

- [Recupero dei valori del nome utente e della password da un segreto](#)
- [Recupero dell'intero SecretString](#)
- [Recupero di un valore da una versione specifica di un segreto](#)
- [Recupero di segreti da un altro Account AWS](#)

Recupero dei valori del nome utente e della password da un segreto

L'[AWS::RDS::DBInstance](#) esempio seguente recupera i valori del nome utente e della password memorizzati nel segreto. *MySecret* La versione segreta recuperata è la versione con il valore della fase della versione di. `AWSCURRENT`

JSON

```
{
```

```

    "MyRDSInstance": {
      "Type": "AWS::RDS::DBInstance",
      "Properties": {
        "DBName": "MyRDSInstance",
        "AllocatedStorage": "20",
        "DBInstanceClass": "db.t2.micro",
        "Engine": "mysql",
        "MasterUsername":
          "{{resolve:secretsmanager:MySecret:SecretString:username}}",
        "MasterUserPassword":
          "{{resolve:secretsmanager:MySecret:SecretString:password}}"
      }
    }
  }
}

```

YAML

```

MyRDSInstance:
  Type: 'AWS::RDS::DBInstance'
  Properties:
    DBName: MyRDSInstance
    AllocatedStorage: '20'
    DBInstanceClass: db.t2.micro
    Engine: mysql
    MasterUsername: '{{resolve:secretsmanager:MySecret:SecretString:username}}'
    MasterUserPassword: '{{resolve:secretsmanager:MySecret:SecretString:password}}'

```

Recupero dell'intero SecretString

Il riferimento dinamico seguente recupera il modulo. SecretString *MySecret*

```
{{resolve:secretsmanager:MySecret}}
```

In alternativa:

```
{{resolve:secretsmanager:MySecret:::}}
```

Recupero di un valore da una versione specifica di un segreto

Il riferimento dinamico seguente recupera il *password* valore per la *AWSPREVIOUS* versione di. *MySecret*

```
{{resolve:secretsmanager:MySecret:SecretString:password:AWSPREVIOUS}}
```

Recupero di segreti da un altro Account AWS

Il riferimento dinamico seguente recupera il modulo contenuto SecretString in un *MySecret* altro. Account AWS È necessario specificare l'ARN segreto completo per accedere ai segreti in un altro. Account AWS

```
{{resolve:secretsmanager:arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret}}
```

Il riferimento dinamico seguente recupera il *password* valore di *MySecret* quello contenuto in un altro. Account AWS È necessario specificare l'ARN segreto completo per accedere ai segreti in un altro. Account AWS

```
{{resolve:secretsmanager:arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret:SecretString:password}}
```

Ottieni AWS valori usando pseudo parametri

Gli pseudo parametri sono variabili integrate che forniscono l'accesso a importanti informazioni AWS sull'ambiente, come account IDs, nomi delle regioni e dettagli dello stack, che possono cambiare tra le distribuzioni o gli ambienti.

È possibile utilizzare pseudoparametri anziché valori codificati per rendere i modelli più portabili e più facili da riutilizzare in diverse aree geografiche. Account AWS

Sintassi

È possibile fare riferimento agli pseudoparametri utilizzando la funzione intrinseca o la funzione intrinseca. Ref Fn : : Sub

Ref

La funzione Ref intrinseca utilizza la seguente sintassi generale. Per ulteriori informazioni, consulta [Ref](#).

JSON

```
{ "Ref" : "AWS::PseudoParameter" }
```

YAML

```
!Ref AWS::PseudoParameter
```

Fn: :Sub

La funzione Fn: :Sub intrinseca utilizza un formato diverso che include la `${}` sintassi dello pseudo parametro. Per ulteriori informazioni, consulta [Fn::Sub](#).

JSON

```
{ "Fn::Sub" : "${AWS::PseudoParameter}" }
```

YAML

```
!Sub '${AWS::PseudoParameter}
```

Pseudoparametri disponibili

AWS::AccountId

Restituisce l' Account AWS ID dell'account in cui viene creato lo stack, ad esempio. 123456789012

Questo pseudo parametro viene comunemente utilizzato per definire ruoli IAM, policy e altre policy relative alle risorse che coinvolgono account specifici. ARNs

AWS::NotificationARNs

Restituisce l'elenco di Amazon Resource Names (ARNs) per gli argomenti di Amazon SNS che ricevono notifiche sugli eventi dello stack. Puoi specificarli ARNs tramite l'- -notification-arns opzione presente in AWS CLI o tramite la console durante la creazione o l'aggiornamento dello stack.

A differenza di altri pseudo parametri che restituiscono un singolo valore, AWS::NotificationARNs restituisce un elenco di. ARNs Per accedere a un ARN specifico

nell'elenco, utilizzare la funzione `Fn::Select` intrinseca. Per ulteriori informazioni, consulta [Fn::Select](#).

AWS::NoValue

Rimuove la proprietà della risorsa corrispondente quando specificata come valore restituito nella funzione intrinseca `Fn::If`. Per ulteriori informazioni, consulta [Fn::If](#).

Questo pseudo parametro è particolarmente utile per creare proprietà condizionali delle risorse che devono essere incluse solo in determinate condizioni.

AWS::Partition

Restituisce la partizione in cui si trova la risorsa. Per lo standard Regioni AWS, la partizione è `aws`. Per risorse in altre partizioni, la partizione è `aws-partitionname`. Ad esempio, la partizione per le risorse nelle regioni della Cina (Pechino e Ningxia) è `aws-cn` e la partizione per le risorse nella regione AWS GovCloud (Stati Uniti occidentali) è `aws-us-gov`.

La partizione fa parte dell'ARN per le risorse. L'utilizzo `AWS::Partition` garantisce il corretto funzionamento dei modelli su diverse AWS partizioni.

AWS::Region

Restituisce una stringa che rappresenta la Regione in cui la risorsa comprendente è in fase di creazione, ad esempio `us-west-2`.

Questo è uno degli pseudo parametri più comunemente usati, in quanto consente ai modelli di adattarsi a diversi Regioni AWS modelli senza modifiche.

AWS::StackId

Restituisce l'ID (ARN) dello stack, ad esempio. `arn:aws:cloudformation:us-west-2:123456789012:stack/teststack/51af3dc0-da77-11e4-872e-1234567db123`

AWS::StackName

Restituisce il nome dello stack, ad esempio. `teststack`

Il nome dello stack viene comunemente utilizzato per creare nomi di risorse univoci facilmente identificabili come appartenenti a uno stack specifico.

AWS::URLSuffix

Restituisce il suffisso per il AWS dominio in Regione AWS cui è distribuito lo stack. Il suffisso è in genere `amazonaws.com`, ma per la regione Cina (Pechino), il suffisso è `amazonaws.com.cn`.

Questo parametro è particolarmente utile durante la creazione di endpoint URLs di AWS servizio.

Esempi

Argomenti

- [Utilizzo di base](#)
- [Uso di AWS::NotificationARNs](#)
- [Proprietà condizionali con AWS::NoValue](#)

Utilizzo di base

Gli esempi seguenti creano due risorse: un argomento Amazon SNS e un CloudWatch allarme che invia notifiche a quell'argomento. `AWS::StackName` utilizzano e `AWS::AccountId` inseriscono dinamicamente il nome dello stack, l'ID corrente e l'ID dell'account nei nomi Regione AWS, nelle descrizioni delle risorse e `AWS::Region` ARNs.

JSON

```
{
  "Resources": {
    "MyNotificationTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "DisplayName": { "Fn::Sub": "Notifications for ${AWS::StackName}" }
      }
    },
    "CPUALarm": {
      "Type": "AWS::CloudWatch::Alarm",
      "Properties": {
        "AlarmDescription": { "Fn::Sub": "Alarm for high CPU in ${AWS::Region}" },
        "AlarmName": { "Fn::Sub": "${AWS::StackName}-HighCPUALarm" },
        "MetricName": "CPUUtilization",
        "Namespace": "AWS/EC2",
        "Statistic": "Average",
        "Period": 300,

```

```

        "EvaluationPeriods": 1,
        "Threshold": 80,
        "ComparisonOperator": "GreaterThanThreshold",
        "AlarmActions": [{ "Fn::Sub": "arn:aws:sns:${AWS::Region}:
${AWS::AccountId}:${MyNotificationTopic}" }]
    }
}
}
}

```

YAML

```

Resources:
  MyNotificationTopic:
    Type: AWS::SNS::Topic
    Properties:
      DisplayName: !Sub Notifications for ${AWS::StackName}
  CPUAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmDescription: !Sub Alarm for high CPU in ${AWS::Region}
      AlarmName: !Sub ${AWS::StackName}-HighCPUAlarm
      MetricName: CPUUtilization
      Namespace: AWS/EC2
      Statistic: Average
      Period: 300
      EvaluationPeriods: 1
      Threshold: 80
      ComparisonOperator: GreaterThanThreshold
      AlarmActions:
        - !Sub arn:aws:sns:${AWS::Region}:${AWS::AccountId}:${MyNotificationTopic}

```

Uso di AWS::NotificationARNs

Gli esempi seguenti configurano un gruppo Auto Scaling per inviare notifiche, ad esempio eventi di avvio ed errori di avvio. La configurazione utilizza lo `AWS::NotificationARNs` pseudo parametro, che fornisce un elenco di ARNs argomenti di Amazon SNS specificati durante la creazione dello stack. La `Fn::Select` funzione sceglie il primo ARN da quell'elenco.

JSON

```

"myASG": {

```

```

    "Type": "AWS::AutoScaling::AutoScalingGroup",
    "Properties": {
      "LaunchTemplate": {
        "LaunchTemplateId": { "Ref": "myLaunchTemplate" },
        "Version": { "Fn::GetAtt": [ "myLaunchTemplate", "LatestVersionNumber" ] }
      },
      "MaxSize": "1",
      "MinSize": "1",
      "VPCZoneIdentifier": [
        "subnetIdAz1",
        "subnetIdAz2",
        "subnetIdAz3"
      ],
      "NotificationConfigurations" : [{
        "TopicARN" : { "Fn::Select" : [ "0", { "Ref" : "AWS::NotificationARNs" } ] },
        "NotificationTypes" : [ "autoscaling:EC2_INSTANCE_LAUNCH",
"autoscaling:EC2_INSTANCE_LAUNCH_ERROR" ]
      }]
    }
  }
}

```

YAML

```

myASG:
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    LaunchTemplate:
      LaunchTemplateId: !Ref myLaunchTemplate
      Version: !GetAtt myLaunchTemplate.LatestVersionNumber
    MinSize: '1'
    MaxSize: '1'
    VPCZoneIdentifier:
      - subnetIdAz1
      - subnetIdAz2
      - subnetIdAz3
    NotificationConfigurations:
      - TopicARN:
          Fn::Select:
            - '0'
            - Ref: AWS::NotificationARNs
        NotificationTypes:
          - autoscaling:EC2_INSTANCE_LAUNCH
          - autoscaling:EC2_INSTANCE_LAUNCH_ERROR

```

Proprietà condizionali con AWS::NoValue

Gli esempi seguenti creano un'istanza DB Amazon RDS che utilizza uno snapshot solo se viene fornito un ID snapshot. Se la UseDBSnapshot condizione risulta vera, CloudFormation utilizza il valore del DBSnapshotName parametro per la proprietà. DBSnapshotIdentifier Se la condizione risulta falsa, CloudFormation rimuove la DBSnapshotIdentifier proprietà.

JSON

```
"MyDB" : {
  "Type" : "AWS::RDS::DBInstance",
  "Properties" : {
    "AllocatedStorage" : "5",
    "DBInstanceClass" : "db.t2.small",
    "Engine" : "MySQL",
    "EngineVersion" : "5.5",
    "MasterUsername" : { "Ref" : "DBUser" },
    "MasterUserPassword" : { "Ref" : "DBPassword" },
    "DBParameterGroupName" : { "Ref" : "MyRDSParamGroup" },
    "DBSnapshotIdentifier" : {
      "Fn::If" : [
        "UseDBSnapshot",
        { "Ref" : "DBSnapshotName" },
        { "Ref" : "AWS::NoValue" }
      ]
    }
  }
}
```

YAML

```
MyDB:
  Type: AWS::RDS::DBInstance
  Properties:
    AllocatedStorage: '5'
    DBInstanceClass: db.t2.small
    Engine: MySQL
    EngineVersion: '5.5'
    MasterUsername:
      Ref: DBUser
    MasterUserPassword:
      Ref: DBPassword
    DBParameterGroupName:
```

```
Ref: MyRDSParamGroup
DBSnapshotIdentifier:
  Fn::If:
    - UseDBSnapshot
    - Ref: DBSnapshotName
    - Ref: AWS::NoValue
```

Ottieni gli output esportati da uno stack distribuito CloudFormation

Se disponi di più stack nella stessa regione Account AWS e nella stessa regione, potresti voler condividere informazioni tra di loro. Ciò è utile quando uno stack deve utilizzare le risorse create da un altro stack.

Ad esempio, potresti avere uno stack che crea risorse di rete, come sottoreti e gruppi di sicurezza, per i tuoi server web. Gli altri stack che creano i server Web effettivi possono quindi utilizzare le risorse di rete create dal primo stack. Non è necessario codificare le risorse IDs nel modello dello stack o passarle IDs come parametri di input.

Per condividere informazioni tra pile, esportate i valori di output da uno stack e li importate in un altro stack. Come funziona:

1. Nel modello del primo stack (ad esempio, lo stack di rete), definisci determinati valori da esportare utilizzando il `Export` campo nella sezione. `Outputs` Per ulteriori informazioni, consulta [CloudFormation Outputssintassi del modello](#).
2. Quando crei o aggiorni quello stack, CloudFormation esporta i valori di output, rendendoli disponibili per altri stack nella stessa regione. Account AWS
3. Nel modello dell'altro stack, si utilizza la [Fn::ImportValue](#) funzione per importare i valori esportati dal primo stack.
4. Quando crei o aggiorni il secondo stack (ad esempio, lo stack del server web), recupera CloudFormation automaticamente i valori esportati dal primo stack e li utilizza.

Per una procedura guidata e modelli di esempio, consulta [Fai riferimento agli output di risorse in un altro stack CloudFormation](#).

Esportazione dei valori di output di uno stack e utilizzo di stack nidificati

Uno stack nidificato è uno stack creato all'interno di un altro stack utilizzando la risorsa `AWS::CloudFormation::Stack`. Con gli stack nidificati, puoi distribuire e gestire tutte le risorse da

un singolo stack. Puoi utilizzare output da uno stack nel gruppo di stack nidificati come input per un altro stack del gruppo. Ciò è diverso dall'esportazione di valori.

Se desideri isolare la condivisione delle informazioni all'interno di un gruppo di stack nidificati, è consigliabile utilizzare stack nidificati. Per condividere le informazioni con altri stack (non solo nel gruppo di stack nidificati), esporta i valori. Ad esempio, puoi creare un singolo stack con una sottorete ed esportarne l'ID. Altri stack possono utilizzare quella sottorete importandone l'ID. Non è necessario che ogni stack crei la propria sottorete. Finché gli stack importano l'ID della sottorete, non è possibile modificarlo o eliminarlo.

Per ulteriori informazioni sugli stack annidati, consulta. [Dividi un modello in pezzi riutilizzabili usando pile annidate](#)

Considerazioni

Ai riferimenti tra stack si applicano le seguenti limitazioni:

- Per ognuno di essi Account AWS, `Export` i nomi devono essere univoci all'interno di una regione.
- Non puoi creare riferimenti tra stack tra Regioni. Puoi utilizzare la funzione intrinseca `Fn::ImportValue` per importare solo valori che sono stati esportati all'interno della stessa Regione.
- Per gli output, il valore della proprietà `Name` di un `Export` non può utilizzare le funzioni `Ref` o `GetAtt` che dipendono da una risorsa.

Allo stesso modo, la funzione `ImportValue` non può includere le funzioni `Ref` o `GetAtt` che dipendono da una risorsa.

- Quando un altro stack importa un valore di output, non puoi eliminare lo stack che esporta il valore di output o modificare il valore di output esportato. Tutte le importazioni devono essere eliminate prima di poter eliminare lo stack di esportazione o di modificare il valore di output.

Elencazione dei valori di output esportati

Se avete bisogno di visualizzare i valori di output esportati dagli stack, utilizzate uno dei seguenti metodi:

Per elencare i valori di output esportati (console)

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)

2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Dal riquadro di navigazione a sinistra, scegli Esportazioni.

Per elencare i valori di output esportati (AWS CLI)

Utilizza il seguente comando [list-exports](#). Sostituisci *us-east-1* con il tuo Regione AWS.

```
aws cloudformation list-exports --region us-east-1
```

Di seguito è riportato un output di esempio.

```
{
  "Exports": [
    {
      "ExportingStackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
      "Name": "private-vpc-subnet-a",
      "Value": "subnet-07b410xmplddcfa03"
    },
    {
      "ExportingStackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
      "Name": "private-vpc-subnet-b",
      "Value": "subnet-075ed3xmplebd2fb1"
    },
    {
      "ExportingStackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
      "Name": "private-vpc-vpcid",
      "Value": "vpc-011d7xmpl100e9841"
    }
  ]
}
```

CloudFormation mostra i nomi e i valori degli output esportati per la regione corrente e lo stack da cui sono stati esportati. Per utilizzare un valore di output esportato nel modello di un altro stack, potete farvi riferimento utilizzando il nome di esportazione e la funzione. Fn::ImportValue

Creazione di elenchi di stack che importano un valore di output esportato

Per eliminare o modificare i valori di output esportati, devi prima scoprire quali pile li stanno importando.

Per visualizzare gli stack che importano un valore di output esportato, utilizzate uno dei seguenti metodi:

Per elencare gli stack che importano un valore di output esportato (console)

1. [Apri la AWS CloudFormation console in https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation).
2. Dal riquadro di navigazione a sinistra, scegli Esportazioni.
3. Per vedere quali pile importano un determinato valore di esportazione, scegli il nome di esportazione per quel valore di esportazione. CloudFormation visualizza la pagina dei dettagli di esportazione, che elenca tutti gli stack che importano il valore.

Per elencare gli stack che importano un valore di output esportato (AWS CLI)

Utilizza il comando `list-imports`. `us-east-1` Sostituiscilo con il tuo Regione AWS e `private-vpc-vpcid` con il nome del valore di output esportato.

```
aws cloudformation list-imports --region us-east-1 \  
--export-name private-vpc-vpcid
```

CloudFormation restituisce un elenco di pile che stanno importando il valore.

```
{  
  "Imports": [  
    "my-app-stack"  
  ]  
}
```

Una volta individuati gli stack che importano un particolare valore esportato, è necessario modificare tali stack per rimuovere le `Fn::ImportValue` funzioni che fanno riferimento ai valori di output. Prima di poter eliminare o modificare i valori di output esportati, è necessario rimuovere tutte le importazioni che fanno riferimento a tali valori.

Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti

Durante la creazione del modello, è possibile creare parametri che richiedono agli utenti di inserire identificatori di AWS risorse esistenti o parametri di Systems Manager utilizzando i tipi di parametri specializzati forniti da CloudFormation.

Argomenti

- [Panoramica](#)
- [Esempio](#)
- [Considerazioni](#)
- [Tipi di AWS parametri specifici supportati](#)
- [Tipi di parametri Systems Manager supportati](#)
- [Tipi di parametri di Systems Manager non supportati](#)

Panoramica

In CloudFormation, è possibile utilizzare i parametri per personalizzare gli stack fornendo valori di input durante la creazione o l'aggiornamento degli stack. Questa funzionalità rende i modelli riutilizzabili e flessibili in diversi scenari.

I parametri sono definiti nella `Parameters` sezione di un CloudFormation modello. Ogni parametro ha un nome e un tipo e può avere impostazioni aggiuntive come un valore predefinito e valori consentiti. Per ulteriori informazioni, consulta [CloudFormation Parameters sintassi del modello](#).

Il tipo di parametro determina il tipo di valore di input che il parametro può accettare. Ad esempio, accetta `Number` solo valori numerici, mentre `String` accetta l'immissione di testo.

CloudFormation fornisce diversi tipi di parametri aggiuntivi che è possibile utilizzare nei modelli per fare riferimento alle AWS risorse esistenti e ai parametri di Systems Manager.

Questi tipi di parametri si dividono in due categorie:

- **AWS-tipi di parametri specifici:** CloudFormation fornisce una serie di tipi di parametri che aiutano a catturare valori non validi durante la creazione o l'aggiornamento di uno stack. Quando utilizzi questi tipi di parametri, chiunque utilizzi il tuo modello deve specificare valori validi dalla regione Account AWS e dalla regione in cui sta creando lo stack.

Se utilizzano AWS Management Console, CloudFormation fornisce un elenco precompilato di valori esistenti dal proprio account e dalla propria regione. In questo modo, l'utente non deve ricordare e digitare correttamente un nome o un ID specifico. Invece, selezionano semplicemente i valori da un elenco a discesa. In alcuni casi, possono anche cercare valori per ID, nome o valore del Name tag.

- **Tipi di parametri di Systems Manager:** fornisce CloudFormation anche tipi di parametri che corrispondono ai parametri esistenti in Systems Manager Parameter Store. Quando si utilizzano questi tipi di parametri, chiunque utilizzi il modello deve specificare una chiave Parameter Store come valore del tipo di parametro Systems Manager, CloudFormation quindi recuperare il valore più recente da Parameter Store da utilizzare nel proprio stack. Ciò può essere utile quando è necessario aggiornare frequentemente le applicazioni con nuovi valori di proprietà, come la nuova Amazon Machine Image (AMI) IDs. Per informazioni su Parameter Store, vedere [Systems Manager Parameter Store](#).

Una volta definiti i parametri nella Parameters sezione, è possibile fare riferimento ai valori dei parametri in tutto il CloudFormation modello utilizzando la Ref funzione.

Esempio

L'esempio seguente mostra un modello che utilizza i seguenti tipi di parametri.

- `AWS::EC2::VPC::Id`
- `AWS::EC2::Subnet::Id`
- `AWS::EC2::KeyPair::KeyName`
- `AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>`

Per creare uno stack da questo modello, devi specificare un ID VPC, un ID di sottorete e un nome di key pair esistenti dal tuo account. Puoi anche specificare una chiave Parameter Store esistente che faccia riferimento all'ID AMI desiderato o mantenga il valore predefinito di `/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`. Questo parametro pubblico è un alias per l'ID AMI regionale per l'ultima AMI Amazon Linux 2. Per ulteriori informazioni sui parametri pubblici, consulta [Discovering public parameters in Parameter Store](#) nella Guida per l'AWS Systems Manager utente.

JSON

```
{
  "Parameters": {
    "VpcId": {
      "Description": "ID of an existing Virtual Private Cloud (VPC).",
      "Type": "AWS::EC2::VPC::Id"
    },
    "PublicSubnetId": {
      "Description": "ID of an existing public subnet within the specified VPC.",
      "Type": "AWS::EC2::Subnet::Id"
    },
    "KeyName": {
      "Description": "Name of an existing EC2 key pair to enable SSH access to the instance.",
      "Type": "AWS::EC2::KeyPair::KeyName"
    },
    "AMIId": {
      "Description": "Name of a Parameter Store parameter that stores the ID of the Amazon Machine Image (AMI).",
      "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
      "Default": "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2"
    }
  },
  "Resources": {
    "InstanceSecurityGroup": {
      "Type": "AWS::EC2::SecurityGroup",
      "Properties": {
        "GroupDescription": "Enable SSH access via port 22",
        "VpcId": { "Ref": "VpcId" },
        "SecurityGroupIngress": [
          {
            "IpProtocol": "tcp",
            "FromPort": 22,
            "ToPort": 22,
            "CidrIp": "0.0.0.0/0"
          }
        ]
      }
    },
    "Ec2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
```

```

        "KeyName": { "Ref": "KeyName" },
        "ImageId": { "Ref": "AMIId" },
        "NetworkInterfaces": [
            {
                "AssociatePublicIpAddress": "true",
                "DeviceIndex": "0",
                "SubnetId": { "Ref": "PublicSubnetId" },
                "GroupSet": [{ "Ref": "InstanceSecurityGroup" }]
            }
        ]
    },
    "Outputs": {
        "InstanceId": {
            "Value": { "Ref": "Ec2Instance" }
        }
    }
}

```

YAML

```

Parameters:
  VpcId:
    Description: ID of an existing Virtual Private Cloud (VPC).
    Type: 'AWS::EC2::VPC::Id'
  PublicSubnetId:
    Description: ID of an existing public subnet within the specified VPC.
    Type: 'AWS::EC2::Subnet::Id'
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instance.
    Type: 'AWS::EC2::KeyPair::KeyName'
  AMIId:
    Description: Name of a Parameter Store parameter that stores the ID of the Amazon
    Machine Image (AMI).
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2'
Resources:
  InstanceSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Enable SSH access via port 22
      VpcId: !Ref VpcId

```

```

    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: 0.0.0.0/0
  Ec2Instance:
    Type: AWS::EC2::Instance
    Properties:
      KeyName: !Ref KeyName
      ImageId: !Ref AMIID
      NetworkInterfaces:
        - AssociatePublicIpAddress: "true"
          DeviceIndex: "0"
          SubnetId: !Ref PublicSubnetId
          GroupSet:
            - !Ref InstanceSecurityGroup
  Outputs:
    InstanceId:
      Value: !Ref Ec2Instance

```

AWS CLI comando per creare lo stack

Quanto segue [create-stack](#) il comando crea uno stack basato sul modello di esempio.

```

aws cloudformation create-stack --stack-name MyStack \
  --template-body file://sampletemplate.json \
  --parameters \
    ParameterKey="VpcId",ParameterValue="vpc-a123baa3" \
    ParameterKey="PublicSubnetId",ParameterValue="subnet-123a351e" \
    ParameterKey="KeyName",ParameterValue="MyKeyName" \
    ParameterKey="AMIId",ParameterValue="MyParameterKey"

```

Per utilizzare un tipo di parametro che accetta un elenco di stringhe, ad esempio `List<AWS::EC2::Subnet::Id>`, è necessario evitare le virgole all'interno di `ParameterValue` con una doppia barra rovesciata, come illustrato nell'esempio seguente.

```

--parameters ParameterKey="SubnetIDs",ParameterValue="subnet-5ea0c127\\, subnet-6194ea3b\\, subnet-c87f2be0"

```

Considerazioni

Si consiglia vivamente di utilizzare riferimenti dinamici per limitare l'accesso a definizioni di configurazione riservate, come le credenziali di terze parti. Per ulteriori informazioni, consulta [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#).

Se desideri consentire agli utenti del modello di specificare valori diversi Account AWS, non utilizzare tipi di parametri AWS specifici. Definisci invece parametri di tipo `String` o `CommaDelimitedList`.

Ci sono alcune cose da tenere a mente con i tipi di parametri di Systems Manager:

- È possibile visualizzare i valori dei parametri risolti nella scheda Parametri dello stack nella console o eseguendo [describe-stacks](#) o [describe-change-set](#). Ricorda che questi valori vengono impostati quando lo stack viene creato o aggiornato, quindi potrebbero essere diversi dai valori più recenti in Parameter Store.
- Per gli aggiornamenti dello stack, quando utilizzi l'opzione Use existing value (o impostata su `UsePreviousValue true`), ciò significa che desideri continuare a utilizzare la stessa chiave Parameter Store, non il relativo valore. CloudFormation recupera sempre il valore più recente.
- Se specifichi valori consentiti o altri vincoli, li CloudFormation convalida in base alle chiavi dei parametri specificate, ma non ai relativi valori. È necessario convalidare i valori nel Parameter Store stesso.
- Quando crei o aggiorni pile e crei set di modifiche, CloudFormation utilizza qualsiasi valore esistente in Parameter Store in quel momento. Se un parametro specificato non esiste in Parameter Store sotto quello del chiamante Account AWS, CloudFormation restituisce un errore di convalida.
- Quando si esegue un set di modifiche, CloudFormation utilizza i valori specificati nel set di modifiche. Esamina questi valori prima di eseguire il set di modifiche perché potrebbero variare in Archivio parametri tra il momento in cui crei il set di modifiche e l'esecuzione dello stesso.
- Per i parametri Parameter Store memorizzati nello stesso Account AWS, è necessario fornire il nome del parametro. Per i parametri Parameter Store condivisi da un altro utente Account AWS, è necessario fornire il parametro ARN completo.

Tipi di AWS parametri specifici supportati

CloudFormation supporta i seguenti tipi AWS specifici:

`AWS::EC2::AvailabilityZone::Name`

Zona di disponibilità, ad esempio `us-west-2a`.

`AWS::EC2::Image::Id`

Un ID EC2 immagine Amazon, ad esempio `ami-0ff8a91507f77f867`. Tieni presente che la CloudFormation console non mostra un elenco a discesa di valori per questo tipo di parametro.

`AWS::EC2::Instance::Id`

Un ID di EC2 istanza Amazon, ad esempio `i-1e731a32`.

`AWS::EC2::KeyPair::KeyName`

Un nome per una coppia di EC2 chiavi Amazon.

`AWS::EC2::SecurityGroup::GroupName`

Un nome di gruppo di sicurezza VPC predefinito, ad esempio `my-sg-abc`

`AWS::EC2::SecurityGroup::Id`

ID del gruppo di sicurezza, ad esempio `sg-a123fd85`.

`AWS::EC2::Subnet::Id`

ID della sottorete, ad esempio `subnet-123a351e`.

`AWS::EC2::Volume::Id`

ID del volume Amazon EBS, ad esempio `vol-3cdd3f56`.

`AWS::EC2::VPC::Id`

ID VPC, ad esempio `vpc-a123baa3`.

`AWS::Route53::HostedZone::Id`

ID della zona ospitata Amazon Route 53, ad esempio `Z23YXV40VPL04A`.

`List<AWS::EC2::AvailabilityZone::Name>`

Matrice di zone di disponibilità per una Regione, ad esempio `us-west-2a`, `us-west-2b`.

`List<AWS::EC2::Image::Id>`

Una serie di EC2 immagini Amazon IDs, ad esempio `ami-0ff8a91507f77f867`, `ami-0a584ac55a7631c0c`. Tieni presente che la CloudFormation console non mostra un elenco a discesa di valori per questo tipo di parametro.

`List<AWS::EC2::Instance::Id>`

Una serie di EC2 istanze Amazon IDs, ad esempio `i-1e731a32`, `i-1e731a34`.

`List<AWS::EC2::SecurityGroup::GroupName>`

Un array di nomi di gruppi di sicurezza VPC predefiniti, ad esempio `my-sg-abc`, `my-sg-def`

`List<AWS::EC2::SecurityGroup::Id>`

Una matrice di gruppi di sicurezza IDs, ad esempio `sg-a123fd85`, `sg-b456fd85`.

`List<AWS::EC2::Subnet::Id>`

Un array di sottoreti IDs, ad esempio `subnet-123a351e`, `subnet-456b351e`.

`List<AWS::EC2::Volume::Id>`

Una matrice di volumi Amazon EBS IDs, ad esempio `vol-3cdd3f56`, `vol-4cdd3f56`.

`List<AWS::EC2::VPC::Id>`

Una serie di VPC IDs, ad esempio `vpc-a123baa3`, `vpc-b456baa3`

`List<AWS::Route53::HostedZone::Id>`

Una serie di zone ospitate su Amazon Route 53 IDs, ad esempio `Z23YXV40VPL04A`, `Z23YXV40VPL04B`.

Tipi di parametri Systems Manager supportati

CloudFormation supporta i seguenti tipi di parametri Systems Manager:

`AWS::SSM::Parameter::Name`

Nome di una chiave di parametro Systems Manager. Utilizzate questo tipo di parametro solo per verificare che esista un parametro richiesto. CloudFormation non recupererà il valore effettivo associato al parametro.

`AWS::SSM::Parameter::Value<String>`

Parametro Systems Manager il cui valore è una stringa. Corrisponde al tipo di parametro `String` in Archivio parametri.


```
AWS::SSM::Parameter::Value<List<String>> o
```

```
AWS::SSM::Parameter::Value<CommaDelimitedList>
```

Parametro Systems Manager il cui valore è un elenco di stringhe. Corrisponde al tipo di parametro `StringList` in Archivio parametri.

```
AWS::SSM::Parameter::Value<AWS-specific parameter type>
```

Un parametro Systems Manager il cui valore è un tipo AWS di parametro specifico.

L'esempio seguente specifica il tipo `AWS::EC2::KeyPair::KeyName`:

- `AWS::SSM::Parameter::Value<AWS::EC2::KeyPair::KeyName>`

```
AWS::SSM::Parameter::Value<List<AWS-specific parameter type>>
```

Un parametro Systems Manager il cui valore è un elenco di tipi AWS di parametri specifici.

L'esempio seguente specifica un elenco di tipi `AWS::EC2::KeyPair::KeyName`:

- `AWS::SSM::Parameter::Value<List<AWS::EC2::KeyPair::KeyName>>`

Tipi di parametri di Systems Manager non supportati

CloudFormation non supporta il seguente tipo di parametro Systems Manager:

- Elenchi di tipi di parametri di Systems Manager, ad esempio:
`List<AWS::SSM::Parameter::Value<String>>`

Inoltre, CloudFormation non supporta la definizione dei parametri del modello come tipi di parametri `SecureString` Systems Manager. Tuttavia, è possibile specificare stringhe sicure come valori dei parametri per determinate risorse. Per ulteriori informazioni, consulta [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#).

CloudFormation procedure dettagliate

Questa documentazione fornisce una raccolta di procedure dettagliate progettate per offrirti esercitazioni pratiche con le distribuzioni in stack.

- [Fai riferimento agli output di risorse in un altro stack CloudFormation](#)— Questa procedura dettagliata mostra come fare riferimento agli output di uno stack all'interno di un altro stack.

CloudFormation. Invece di includere tutte le risorse in un unico stack, è possibile creare AWS risorse correlate in pile separate per creare modelli più modulari e riutilizzabili.

- [Peer con un VPC in un altro Account AWS](#)— Questa procedura dettagliata illustra il processo di creazione di una connessione peering Virtual Private Cloud (VPC) tra due connessioni diverse. VPCs Account AWS Il peering VPC ti aiuta a indirizzare il traffico tra VPCs e ad accedere alle risorse come se facessero parte della stessa rete.
- [Creazione di un'applicazione dimensionata e con carico bilanciato](#)— Scopri come utilizzare per CloudFormation creare un'applicazione scalabile e con carico bilanciato. Questa procedura dettagliata descrive la creazione di un gruppo di Auto Scaling, un sistema di bilanciamento del carico e altre risorse correlate per garantire che l'applicazione sia in grado di gestire carichi di traffico variabili e mantenere un'elevata disponibilità.
- [Distribuisci applicazioni su Amazon EC2](#)— Scopri come utilizzare CloudFormation per installare, configurare e avviare automaticamente la tua applicazione sulle EC2 istanze Amazon. In questo modo, puoi duplicare facilmente le distribuzioni e aggiornare le installazioni esistenti senza connetterti direttamente alle istanze.
- [Aggiornamento di uno stack](#)— Esegui una semplice progressione degli aggiornamenti a uno stack in esecuzione con CloudFormation.
- [Esegui blue/green implementazioni ECS tramite l'utilizzo CodeDeploy CloudFormation](#)— Scopri come utilizzare per CloudFormation eseguire le AWS CodeDeploy blue/green deployments on Amazon ECS. Blue/green implementazioni è un modo per aggiornare le tue applicazioni o i tuoi servizi con tempi di inattività minimi.

Fai riferimento agli output di risorse in un altro stack CloudFormation

Questa procedura dettagliata mostra come fare riferimento agli output di uno CloudFormation stack all'interno di un altro stack per creare modelli più modulari e riutilizzabili.

Invece di includere tutte le risorse in un unico stack, crei risorse correlate in pile separate. AWS. Quindi, puoi fare riferimento alle risorse richieste in uscita da altri stack. Limitando i riferimenti tra stack agli output, puoi controllare le parti di uno stack a cui fanno riferimento altri stack.

Ad esempio, potresti avere un stack di rete con un VPC, un gruppo di sicurezza e una sottorete per applicazioni Web pubbliche, nonché uno stack separato per le applicazioni Web pubbliche. Per garantire che le applicazioni Web utilizzino il gruppo di sicurezza e la sottorete dello stack di rete, è necessario creare un riferimento tra stack che consenta allo stack per le applicazioni Web di fare

riferimento agli output delle risorse dello stack di rete. Con un riferimento tra stack, non c'è necessità i proprietari degli stack per le applicazioni Web di creare o mantenere regole o asset di rete.

Per creare un riferimento tra stack, utilizza il campo di output `Export` per contrassegnare il valore dell'output di una risorsa per l'esportazione. Quindi, importa il valore tramite la funzione intrinseca `Fn::ImportValue`. Per ulteriori informazioni, consulta [Ottieni gli output esportati da uno stack distribuito CloudFormation](#).

Note

CloudFormation è un servizio gratuito. Tuttavia, ti verranno addebitate le AWS risorse che includi nei tuoi stack alla tariffa corrente per ciascuna di esse. Per ulteriori informazioni sui prezzi di AWS visita [la pagina dei dettagli per ogni prodotto](#).

Argomenti

- [Usa un modello di esempio per creare uno stack di rete](#)
- [Utilizza un modello di esempio per creare uno stack di applicazioni Web](#)
- [Verifica che lo stack funzioni come previsto](#)
- [Risolvi gli errori di mappatura AMI](#)
- [Pulizia delle risorse](#)

Usa un modello di esempio per creare uno stack di rete

Prima di iniziare questa procedura dettagliata, verifica di disporre delle autorizzazioni IAM per utilizzare tutti i seguenti servizi: Amazon VPC, Amazon e. EC2 CloudFormation

Lo stack di rete contiene il VPC, il gruppo di sicurezza e la sottorete da utilizzare nello stack delle applicazioni Web. Oltre a queste risorse, lo stack di rete crea un gateway Internet e le tabelle di instradamento per abilitare l'accesso pubblico.

È necessario creare questo stack prima di creare lo stack delle applicazioni Web. Se crei prima lo stack dell'applicazione Web, non disporrai di un gruppo di sicurezza o di una sottorete.

[Il modello di stack è disponibile al seguente URL: user- .template. https://s3.amazonaws.com/cloudformation-examples/ guide/cross-stack/SampleNetworkCrossStack](https://s3.amazonaws.com/cloudformation-examples/guide/cross-stack/SampleNetworkCrossStack) Per visualizzare le risorse che saranno create dallo stack, selezionare il link per aprire il modello. Nella `Outputs` sezione, puoi vedere le risorse di rete esportate dal modello di esempio. I nomi delle risorse esportate hanno come

prefisso il nome dello stack, qualora vengano esportate risorse di rete da altri stack. Quando gli utenti importano le risorse di rete, possono specificare da quale stack farlo.

Per creare lo stack di rete

1. Accedi a AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella pagina Stacks, scegli Crea stack in alto a destra, quindi scegli Con nuove risorse (standard).
3. Scegli un modello esistente e, nella sezione Specificare modello, scegli l'URL di Amazon S3.
4. Per l'URL di Amazon S3, incolla il seguente URL: **`https://s3.amazonaws.com/cloudformation-examples/user-guide/cross-stack/SampleNetworkCrossStack.template`**
5. Scegli Next (Successivo).
6. Per Stack name (Nome stack), digitare **SampleNetworkCrossStack**, quindi scegliere Next (Avanti).

 Note

Registrare il nome di questo stack: servirà all'avvio dello stack delle applicazioni Web.

7. Scegli Next (Successivo). Per questa procedura guidata, non è necessario aggiungere tag o specificare impostazioni avanzate.
8. Assicurarsi che il nome dello stack e l'URL del modello siano corretti e scegliere Create stack (Crea stack).

Potrebbero essere necessari alcuni minuti per CloudFormation creare il tuo stack. Attendere che tutte le risorse siano state create prima di continuare a creare lo stack delle applicazioni Web.

9. È possibile controllare l'avanzamento negli eventi per lo stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Utilizza un modello di esempio per creare uno stack di applicazioni Web

Lo stack di applicazioni Web crea un' EC2 istanza che utilizza il gruppo di sicurezza e la sottorete dello stack di rete.

È necessario creare questo stack nello stesso Regione AWS stack di rete.

Il modello di stack è disponibile dal seguente URL: <https://s3.amazonaws.com/cloudformation-examples/user-template.guide/cross-stack/SampleWebAppCrossStack> Per visualizzare le risorse che saranno create dallo stack, selezionare il link per aprire il modello. Nella Resources sezione, visualizza le proprietà dell' EC2 istanza. È possibile visualizzare il modo in cui le risorse di rete vengono importate da un altro stack utilizzando la funzione `Fn::ImportValue`.

Per creare lo stack delle applicazioni Web

1. Dalla pagina Pile, scegli Crea pila in alto a destra, quindi scegli Con nuove risorse (standard).
2. Scegli un modello esistente e, nella sezione Specificare modello, scegli l'URL di Amazon S3.
3. Per l'URL di Amazon S3, incolla il seguente URL: **`https://s3.amazonaws.com/cloudformation-examples/user-guide/cross-stack/SampleWebAppCrossStack.template`**
4. Scegli Next (Successivo).
5. Per Stack name (Nome stack), digitare **SampleWebAppCrossStack**. Nella sezione Parametri, utilizza il valore predefinito per il NetworkStackNameparametro, quindi scegli Avanti.

Il modello di esempio usa il valore del parametro per specificare da quale stack importare i valori.

6. Scegli Next (Successivo). Per questa procedura guidata, non è necessario aggiungere tag o specificare impostazioni avanzate.
7. Assicurarsi che il nome dello stack e l'URL del modello siano corretti e scegliere Create stack (Crea stack).

La creazione dello stack potrebbe richiedere alcuni minuti. CloudFormation

Verifica che lo stack funzioni come previsto

Dopo che lo stack è stato creato, visualizzare le relative risorse e annotare l'ID istanza. Per ulteriori informazioni sulla visualizzazione delle risorse dello stack, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Per verificare il gruppo di sicurezza e la sottorete dell'istanza, visualizza le proprietà dell'istanza nella [EC2 console Amazon](#). Se l'istanza utilizza il gruppo di sicurezza e la sottorete dello stack SampleNetworkCrossStack, il riferimento tra stack è stato creato senza errori.

Utilizza la console per visualizzare gli output dello stack e l'URL del sito Web di esempio per verificare che l'applicazione Web sia operativa. Per ulteriori informazioni, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Risolvi gli errori di mappatura AMI

Se ricevi l'errore `Template error: Unable to get mapping for AWSRegionArch2AMI:: [region]::HVM64`, il modello non include una mappatura AMI per il tuo Regione AWS. Invece di aggiornare la mappatura, consigliamo di utilizzare i parametri pubblici di Systems Manager per fare riferimento dinamicamente alle ultime novità: AMIs

1. Scaricate il `SampleWebAppCrossStack` modello sul computer locale da: <https://s3.amazonaws.com/cloudformation-examples/user-guide/cross-stack/SampleWebAppCrossStack.template>.
2. Eliminare l'intera sezione di `AWSRegionArch2AMI` mappatura.
3. Aggiungere il seguente parametro Systems Manager:

```
"LatestAmiId": {
  "Description": "The latest Amazon Linux 2 AMI from the Parameter Store",
  "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
  "Default": "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2"
}
```

4. Sostituisci il `ImageId` riferimento esistente:

```
"ImageId": { "Fn::FindInMap": [ "AWSRegionArch2AMI", { "Ref": "AWS::Region" } ,
  "HVM64" ] },
```

Con:

```
"ImageId": { "Ref": "LatestAmiId" },
```

Questo parametro viene risolto automaticamente nell'ultima AMI Amazon Linux 2 per la regione in cui distribuisce lo stack.

Per altre distribuzioni Linux, usa il percorso dei parametri appropriato. Per ulteriori informazioni, consulta [Discovering public parameters in Parameter Store](#) nella Guida per l'AWS Systems Manager utente.

5. Carica il modello modificato in un bucket S3 nel tuo account:

```
aws s3 cp SampleWebAppCrossStack.template s3://amzn-s3-demo-bucket/
```

6. Quando crei lo stack, specifica l'URL del modello S3 anziché l'URL di esempio.

Pulizia delle risorse

Per assicurarti che non ti vengano addebitati servizi indesiderati, elimina gli stack.

Per eliminare gli stack

1. Nella CloudFormation console, scegli lo stack. `SampleWebAppCrossStack`
2. Scegliere Actions (Operazioni), quindi Delete Stack (Elimina stack).
3. Nel messaggio di conferma, scegliere Delete (Elimina).
4. Dopo che lo stack è stato eliminato, ripeti gli stessi passaggi per lo `SampleNetworkCrossStack` stack.

Note

Attendi che lo stack venga eliminato CloudFormation completamente. `SampleWebAppCrossStack` Se l' EC2 istanza è ancora in esecuzione nel VPC, CloudFormation non eliminerà il VPC nello stack. `SampleNetworkCrossStack`

Peer con un VPC in un altro Account AWS

È possibile effettuare il peering con un Virtual Private Cloud (VPC) in un altro utilizzando. Account AWS [AWS::EC2::VPCPeeringConnection](#) In questo modo si crea una connessione di rete tra due di essi VPCs che consente di instradare il traffico tra di loro in modo che possano comunicare come se fossero all'interno della stessa rete. Una connessione di peering VPC può facilitare l'accesso ai dati e il trasferimento dei dati.

Per stabilire una connessione peering VPC, devi autorizzarne due separate Account AWS all'interno di un unico stack. CloudFormation

Per ulteriori informazioni sul peering VPC e sui suoi limiti, consulta la Amazon [VPC](#) Peering Guide.

Prerequisiti

1. Per la connessione peering sono necessari un ID VPC peer, un Account AWS peer ID e [un ruolo di accesso tra account diversi](#).

Note

Questa procedura guidata si riferisce a due account: un account che consente il peering tra più account (l'account dell'accettante) e un account che richiede la connessione in peering (l'account del richiedente).

2. Per accettare la connessione di peering VPC, devi assumere il ruolo di accesso tra più account. La risorsa si comporta nello stesso modo di una risorsa di una connessione di peering VPC nello stesso account. Per informazioni su come un amministratore IAM concede le autorizzazioni per assumere il ruolo su più account, consulta [Concedere a un utente le autorizzazioni per cambiare ruolo nella Guida per l'utente](#) IAM.

Fase 1: creazione di un VPC e di un ruolo tra più account

In questa fase vengono creati il VPC e il ruolo nell'account dell'accettante.

Per creare un VPC e un ruolo di accesso tra account

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation).
2. Dalla pagina Stacks, scegli Crea stack in alto a destra, quindi scegli Con nuove risorse (standard).
3. Per Prerequisito - Prepara modello, scegli Scegli un modello esistente, quindi Carica un file modello, Scegli file.
4. Apri un editor di testo sul tuo computer locale e aggiungi uno dei seguenti modelli. Salva il file e torna alla console per selezionarlo come file modello.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Create a VPC and an assumable role for cross account VPC peering.",

```



```

"Parameters": {
  "PeerRequesterAccountId": {
    "Type": "String"
  }
},
"Resources": {
  "vpc": {
    "Type": "AWS::EC2::VPC",
    "Properties": {
      "CidrBlock": "10.1.0.0/16",
      "EnableDnsSupport": false,
      "EnableDnsHostnames": false,
      "InstanceTenancy": "default"
    }
  },
  "peerRole": {
    "Type": "AWS::IAM::Role",
    "Properties": {
      "AssumeRolePolicyDocument": {
        "Statement": [
          {
            "Principal": {
              "AWS": {
                "Ref": "PeerRequesterAccountId"
              }
            },
            "Action": [
              "sts:AssumeRole"
            ],
            "Effect": "Allow"
          }
        ]
      },
      "Path": "/",
      "Policies": [
        {
          "PolicyName": "root",
          "PolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
              {
                "Effect": "Allow",
                "Action": "ec2:AcceptVpcPeeringConnection",
                "Resource": "*"
              }
            ]
          }
        }
      ]
    }
  }
}

```

```

    }
  ]
}
}
},
"Outputs": {
  "VPCId": {
    "Value": {
      "Ref": "vpc"
    }
  },
  "RoleARN": {
    "Value": {
      "Fn::GetAtt": [
        "peerRole",
        "Arn"
      ]
    }
  }
}
}
}
}

```

Example YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Create a VPC and an assumable role for cross account VPC peering.
Parameters:
  PeerRequesterAccountId:
    Type: String
Resources:
  vpc:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.1.0.0/16
      EnableDnsSupport: false
      EnableDnsHostnames: false
      InstanceTenancy: default
  peerRole:
    Type: AWS::IAM::Role
    Properties:

```

```

    AssumeRolePolicyDocument:
      Statement:
        - Principal:
            AWS: !Ref PeerRequesterAccountId
          Action:
            - 'sts:AssumeRole'
          Effect: Allow
      Path: /
    Policies:
      - PolicyName: root
        PolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Action: 'ec2:AcceptVpcPeeringConnection'
              Resource: '*'

Outputs:
  VPCId:
    Value: !Ref vpc
  RoleARN:
    Value: !GetAtt
      - peerRole
      - Arn

```

5. Scegli Next (Successivo).
6. Assegna un nome allo stack (ad esempio, **VPC-owner**), quindi inserisci l' Account AWS ID dell'account richiedente nel PeerRequesterAccountId campo.
7. Accettare i valori predefiniti, quindi selezionare Next (Avanti).
8. Scegli Riconosco che AWS CloudFormation potrebbe creare risorse IAM, quindi scegli Create stack.

Fase 2: creazione di un modello che include **AWS::EC2::VPCPeeringConnection**

Ora che hai creato il VPC e il ruolo interaccount, puoi effettuare il peer con il VPC utilizzandone un altro Account AWS (l'account richiedente).

Per creare un modello che includa la risorsa [AWS:EC2:: VPCPeering Connection](#)

1. Torna alla home page della AWS CloudFormation console.
2. Dalla pagina Pile, scegli Crea pila in alto a destra, quindi scegli Con nuove risorse (standard).

3. Per Prerequisito - Prepara modello, scegli Scegli un modello esistente, quindi Carica un file modello, Scegli file.
4. Apri un editor di testo sul tuo computer locale e aggiungi uno dei seguenti modelli. Salva il file e torna alla console per selezionarlo come file modello.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Create a VPC and a VPC Peering connection using the PeerRole to accept.",
  "Parameters": {
    "PeerVPCAccountId": {
      "Type": "String"
    },
    "PeerVPCId": {
      "Type": "String"
    },
    "PeerRoleArn": {
      "Type": "String"
    }
  },
  "Resources": {
    "vpc": {
      "Type": "AWS::EC2::VPC",
      "Properties": {
        "CidrBlock": "10.2.0.0/16",
        "EnableDnsSupport": false,
        "EnableDnsHostnames": false,
        "InstanceTenancy": "default"
      }
    },
    "vpcPeeringConnection": {
      "Type": "AWS::EC2::VPCPeeringConnection",
      "Properties": {
        "VpcId": {
          "Ref": "vpc"
        },
        "PeerVpcId": {
          "Ref": "PeerVPCId"
        },
        "PeerOwnerId": {
          "Ref": "PeerVPCAccountId"
        }
      }
    }
  }
}
```

```

    },
    "PeerRoleArn": {
      "Ref": "PeerRoleArn"
    }
  }
},
"Outputs": {
  "VPCId": {
    "Value": {
      "Ref": "vpc"
    }
  },
  "VPCPeeringConnectionId": {
    "Value": {
      "Ref": "vpcPeeringConnection"
    }
  }
}
}
}

```

Example YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Create a VPC and a VPC Peering connection using the PeerRole to
  accept.
Parameters:
  PeerVPCAccountId:
    Type: String
  PeerVPCId:
    Type: String
  PeerRoleArn:
    Type: String
Resources:
  vpc:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      EnableDnsSupport: false
      EnableDnsHostnames: false
      InstanceTenancy: default
  vpcPeeringConnection:
    Type: AWS::EC2::VPCPeeringConnection

```

```
Properties:
  VpcId: !Ref vpc
  PeerVpcId: !Ref PeerVPCId
  PeerOwnerId: !Ref PeerVPCAccountId
  PeerRoleArn: !Ref PeerRoleArn
Outputs:
  VPCId:
    Value: !Ref vpc
  VPCPeeringConnectionId:
    Value: !Ref vpcPeeringConnection
```

5. Scegli Next (Successivo).
6. Assegnare un nome allo stack (ad esempio, **VPC-peering-connection**).
7. Accettare i valori predefiniti, quindi selezionare Next (Avanti).
8. Scegli Riconosco che AWS CloudFormation potrebbe creare risorse IAM, quindi scegli Create stack.

Crea un modello con una politica altamente restrittiva

Potresti creare una policy altamente restrittiva per collegare in peering il VPC con un altro Account AWS.

L'esempio seguente mostra come modificare il modello del proprietario della connessione in peering del VPC (l'account dell'accettante creato nella fase 1 precedente) in modo che sia di livello più restrittivo.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Create a VPC and an assumable role for cross account VPC peering.",
  "Parameters": {
    "PeerRequesterAccountId": {
      "Type": "String"
    }
  },
  "Resources": {
    "peerRole": {
      "Type": "AWS::IAM::Role",
      "Properties": {
        "AssumeRolePolicyDocument": {
```

```

    "Statement":[
      {
        "Action":[
          "sts:AssumeRole"
        ],
        "Effect":"Allow",
        "Principal":{"
          "AWS":{"
            "Ref":"PeerRequesterAccountId"
          }
        }
      }
    ]
  },
  "Path":"/",
  "Policies":[
    {
      "PolicyDocument":{"
        "Statement":[
          {
            "Action":"ec2:acceptVpcPeeringConnection",
            "Effect":"Allow",
            "Resource":{"
              "Fn::Sub":"arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc/${vpc}"
            }
          },
          {
            "Action":"ec2:acceptVpcPeeringConnection",
            "Condition":{"
              "StringEquals":{"
                "ec2:AcceptorVpc":{"
                  "Fn::Sub":"arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc/
${vpc}"
                }
              }
            },
            "Effect":"Allow",
            "Resource":{"
              "Fn::Sub":"arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc-
peering-connection/*"
            }
          }
        ],
        "Version":"2012-10-17"
      }
    }
  ]
}

```

```

        },
        "PolicyName":"root"
      }
    ]
  }
},
"vpc":{
  "Type":"AWS::EC2::VPC",
  "Properties":{
    "CidrBlock":"10.1.0.0/16",
    "EnableDnsHostnames":false,
    "EnableDnsSupport":false,
    "InstanceTenancy":"default"
  }
}
},
"Outputs":{
  "RoleARN":{
    "Value":{
      "Fn::GetAtt":[
        "peerRole",
        "Arn"
      ]
    }
  },
  "VPCId":{
    "Value":{
      "Ref":"vpc"
    }
  }
}
}
}

```

Example YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Create a VPC and an assumable role for cross account VPC peering.
Parameters:
  PeerRequesterAccountId:
    Type: String
Resources:
  peerRole:
    Type: AWS::IAM::Role

```



```

Properties:
  AssumeRolePolicyDocument:
    Statement:
      - Action:
          - 'sts:AssumeRole'
        Effect: Allow
        Principal:
          AWS:
            Ref: PeerRequesterAccountId
    Path: /
  Policies:
    - PolicyDocument:
        Statement:
          - Action: 'ec2:acceptVpcPeeringConnection'
            Effect: Allow
            Resource:
              'Fn::Sub': 'arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc/${vpc}'
          - Action: 'ec2:acceptVpcPeeringConnection'
            Condition:
              StringEquals:
                'ec2:AcceptorVpc':
                  'Fn::Sub': 'arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc/
${vpc}'
            Effect: Allow
            Resource:
              'Fn::Sub': >-
                arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:vpc-peering-
connection/*
        Version: 2012-10-17
        PolicyName: root
    vpc:
      Type: AWS::EC2::VPC
      Properties:
        CidrBlock: 10.1.0.0/16
        EnableDnsHostnames: false
        EnableDnsSupport: false
        InstanceTenancy: default
  Outputs:
    RoleARN:
      Value:
        'Fn::GetAtt':
          - peerRole
          - Arn
    VPCId:

```

```
Value:  
  Ref: vpc
```

Per accedere al VPC, è possibile utilizzare lo stesso modello del richiedente della fase 2 precedente.

Per ulteriori informazioni, consulta [Gestione delle identità e degli accessi per il peering VPC nella Amazon VPC Peering](#) Guide.

Creazione di un'applicazione dimensionata e con carico bilanciato

Per questa procedura dettagliata, viene creato uno stack che aiuta a configurare un'applicazione dimensionata e con carico bilanciato. La procedura guidata fornisce un modello di esempio che potrai usare per creare lo stack. Il modello di esempio prevede un gruppo con dimensionamento automatico, un Application Load Balancer, gruppi di sicurezza che controllano il traffico verso il sistema di bilanciamento del carico e il gruppo con dimensionamento automatico e una configurazione di notifica Amazon SNS per pubblicare notifiche sulle attività di dimensionamento.

Questo modello crea una o più EC2 istanze Amazon e un Application Load Balancer. Se crei uno stack da questo modello, ti verranno addebitate le risorse AWS utilizzate.

Modello full stack

Cominciamo con il modello.

YAML

```
AWSTemplateFormatVersion: 2010-09-09  
Parameters:  
  InstanceType:  
    Description: The EC2 instance type  
    Type: String  
    Default: t3.micro  
    AllowedValues:  
      - t3.micro  
      - t3.small  
      - t3.medium  
  KeyName:  
    Description: Name of an existing EC2 key pair to allow SSH access to the instances  
    Type: 'AWS::EC2::KeyPair::KeyName'  
  LatestAmiId:  
    Description: The latest Amazon Linux 2 AMI from the Parameter Store  
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'  
    Default: '/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2'
```

```
OperatorEmail:
  Description: The email address to notify when there are any scaling activities
  Type: String
SSHLocation:
  Description: The IP address range that can be used to SSH to the EC2 instances
  Type: String
  MinLength: 9
  MaxLength: 18
  Default: 0.0.0.0/0
  ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
Subnets:
  Type: 'List<AWS::EC2::Subnet::Id>'
  Description: At least two public subnets in different Availability Zones in the
selected VPC
VPC:
  Type: 'AWS::EC2::VPC::Id'
  Description: A virtual private cloud (VPC) that enables resources in public subnets
to connect to the internet
Resources:
  ELBSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: ELB Security Group
      VpcId: !Ref VPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0
  EC2SecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: EC2 Security Group
      VpcId: !Ref VPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          SourceSecurityGroupId:
            Fn::GetAtt:
              - ELBSecurityGroup
              - GroupId
        - IpProtocol: tcp
          FromPort: 22
```

```
    ToPort: 22
    CidrIp: !Ref SSHLocation
EC2TargetGroup:
  Type: AWS::ElasticLoadBalancingV2::TargetGroup
  Properties:
    HealthCheckIntervalSeconds: 30
    HealthCheckProtocol: HTTP
    HealthCheckTimeoutSeconds: 15
    HealthyThresholdCount: 5
    Matcher:
      HttpCode: '200'
    Name: EC2TargetGroup
    Port: 80
    Protocol: HTTP
    TargetGroupAttributes:
      - Key: deregistration_delay.timeout_seconds
        Value: '20'
    UnhealthyThresholdCount: 3
    VpcId: !Ref VPC
ALBListener:
  Type: AWS::ElasticLoadBalancingV2::Listener
  Properties:
    DefaultActions:
      - Type: forward
        TargetGroupArn: !Ref EC2TargetGroup
    LoadBalancerArn: !Ref ApplicationLoadBalancer
    Port: 80
    Protocol: HTTP
ApplicationLoadBalancer:
  Type: AWS::ElasticLoadBalancingV2::LoadBalancer
  Properties:
    Scheme: internet-facing
    Subnets: !Ref Subnets
    SecurityGroups:
      - !GetAtt ELBSecurityGroup.GroupId
LaunchTemplate:
  Type: AWS::EC2::LaunchTemplate
  Properties:
    LaunchTemplateName: !Sub ${AWS::StackName}-launch-template
    LaunchTemplateData:
      ImageId: !Ref LatestAmiId
      InstanceType: !Ref InstanceType
      KeyName: !Ref KeyName
      SecurityGroupIds:
```

```

    - !Ref EC2SecurityGroup
  UserData:
    Fn::Base64: !Sub |
      #!/bin/bash
      yum update -y
      yum install -y httpd
      systemctl start httpd
      systemctl enable httpd
      echo "<h1>Hello World!</h1>" > /var/www/html/index.html
  NotificationTopic:
    Type: AWS::SNS::Topic
    Properties:
      Subscription:
        - Endpoint: !Ref OperatorEmail
          Protocol: email
  WebServerGroup:
    Type: AWS::AutoScaling::AutoScalingGroup
    Properties:
      LaunchTemplate:
        LaunchTemplateId: !Ref LaunchTemplate
        Version: !GetAtt LaunchTemplate.LatestVersionNumber
      MaxSize: '3'
      MinSize: '1'
      NotificationConfigurations:
        - TopicARN: !Ref NotificationTopic
          NotificationTypes: ['autoscaling:EC2_INSTANCE_LAUNCH',
'autoscaling:EC2_INSTANCE_LAUNCH_ERROR', 'autoscaling:EC2_INSTANCE_TERMINATE',
'autoscaling:EC2_INSTANCE_TERMINATE_ERROR']
      TargetGroupARNs:
        - !Ref EC2TargetGroup
      VPCZoneIdentifier: !Ref Subnets

```

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "InstanceType": {
      "Description": "The EC2 instance type",
      "Type": "String",
      "Default": "t3.micro",
      "AllowedValues": [
        "t3.micro",

```

```

        "t3.small",
        "t3.medium"
    ]
},
"KeyName":{
    "Description":"Name of an existing EC2 key pair to allow SSH access to the
instances",
    "Type":"AWS::EC2::KeyPair::KeyName"
},
"LatestAmiId":{
    "Description":"The latest Amazon Linux 2 AMI from the Parameter Store",
    "Type":"AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
    "Default":"/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2"
},
"OperatorEmail":{
    "Description":"The email address to notify when there are any scaling
activities",
    "Type":"String"
},
"SSHLocation":{
    "Description":"The IP address range that can be used to SSH to the EC2
instances",
    "Type":"String",
    "MinLength":9,
    "MaxLength":18,
    "Default":"0.0.0.0/0",
    "ConstraintDescription":"Must be a valid IP CIDR range of the form x.x.x.x/x."
},
"Subnets":{
    "Type":"List<AWS::EC2::Subnet::Id>",
    "Description":"At least two public subnets in different Availability Zones in the
selected VPC"
},
"VPC":{
    "Type":"AWS::EC2::VPC::Id",
    "Description":"A virtual private cloud (VPC) that enables resources in public
subnets to connect to the internet"
}
},
"Resources":{
    "ELBSecurityGroup":{
        "Type":"AWS::EC2::SecurityGroup",
        "Properties":{
            "GroupDescription":"ELB Security Group",

```

```
    "VpcId":{
      "Ref":"VPC"
    },
    "SecurityGroupIngress":[
      {
        "IpProtocol":"tcp",
        "FromPort":80,
        "ToPort":80,
        "CidrIp":"0.0.0.0/0"
      }
    ]
  },
  "EC2SecurityGroup":{
    "Type":"AWS::EC2::SecurityGroup",
    "Properties":{
      "GroupDescription":"EC2 Security Group",
      "VpcId":{
        "Ref":"VPC"
      },
      "SecurityGroupIngress":[
        {
          "IpProtocol":"tcp",
          "FromPort":80,
          "ToPort":80,
          "SourceSecurityGroupId":{
            "Fn::GetAtt":[
              "ELBSecurityGroup",
              "GroupId"
            ]
          }
        },
        {
          "IpProtocol":"tcp",
          "FromPort":22,
          "ToPort":22,
          "CidrIp":{
            "Ref":"SSHLocation"
          }
        }
      ]
    }
  },
  "EC2TargetGroup":{
```

```
"Type": "AWS::ElasticLoadBalancingV2::TargetGroup",
"Properties": {
  "HealthCheckIntervalSeconds": 30,
  "HealthCheckProtocol": "HTTP",
  "HealthCheckTimeoutSeconds": 15,
  "HealthyThresholdCount": 5,
  "Matcher": {
    "HttpCode": "200"
  },
  "Name": "EC2TargetGroup",
  "Port": 80,
  "Protocol": "HTTP",
  "TargetGroupAttributes": [
    {
      "Key": "deregistration_delay.timeout_seconds",
      "Value": "20"
    }
  ],
  "UnhealthyThresholdCount": 3,
  "VpcId": {
    "Ref": "VPC"
  }
},
"ALBListener": {
  "Type": "AWS::ElasticLoadBalancingV2::Listener",
  "Properties": {
    "DefaultActions": [
      {
        "Type": "forward",
        "TargetGroupArn": {
          "Ref": "EC2TargetGroup"
        }
      }
    ],
    "LoadBalancerArn": {
      "Ref": "ApplicationLoadBalancer"
    },
    "Port": 80,
    "Protocol": "HTTP"
  }
},
"ApplicationLoadBalancer": {
  "Type": "AWS::ElasticLoadBalancingV2::LoadBalancer",
```



```

    "Properties":{
      "Scheme":"internet-facing",
      "Subnets":{
        "Ref":"Subnets"
      },
      "SecurityGroups":[
        {
          "Fn::GetAtt":[
            "ELBSecurityGroup",
            "GroupId"
          ]
        }
      ]
    },
    "LaunchTemplate":{
      "Type":"AWS::EC2::LaunchTemplate",
      "Properties":{
        "LaunchTemplateName":{
          "Fn::Sub":"${AWS::StackName}-launch-template"
        },
        "LaunchTemplateData":{
          "ImageId":{
            "Ref":"LatestAmiId"
          },
          "InstanceType":{
            "Ref":"InstanceType"
          },
          "KeyName":{
            "Ref":"KeyName"
          },
          "SecurityGroupIds":[
            {
              "Ref":"EC2SecurityGroup"
            }
          ],
          "UserData":{
            "Fn::Base64":{
              "Fn::Join":[
                "",
                [
                  "#!/bin/bash\n",
                  "yum update -y\n",
                  "yum install -y httpd\n",

```

```

        "systemctl start httpd\n",
        "systemctl enable httpd\n",
        "echo \"<h1>Hello World!</h1>\n\" > /var/www/html/index.html"
    ]
  ]
}
}
}
},
"NotificationTopic":{
  "Type":"AWS::SNS::Topic",
  "Properties":{
    "Subscription":[
      {
        "Endpoint":{
          "Ref":"OperatorEmail"
        },
        "Protocol":"email"
      }
    ]
  }
},
"WebServerGroup":{
  "Type":"AWS::AutoScaling::AutoScalingGroup",
  "Properties":{
    "LaunchTemplate":{
      "LaunchTemplateId":{
        "Ref":"LaunchTemplate"
      },
      "Version":{
        "Fn::GetAtt":[
          "LaunchTemplate",
          "LatestVersionNumber"
        ]
      }
    },
    "MaxSize":"3",
    "MinSize":"1",
    "NotificationConfigurations":[
      {
        "TopicARN":{
          "Ref":"NotificationTopic"
        }
      }
    ],

```

```
        "NotificationTypes":[
            "autoscaling:EC2_INSTANCE_LAUNCH",
            "autoscaling:EC2_INSTANCE_LAUNCH_ERROR",
            "autoscaling:EC2_INSTANCE_TERMINATE",
            "autoscaling:EC2_INSTANCE_TERMINATE_ERROR"
        ]
    },
    "TargetGroupARNs":[
        {
            "Ref":"EC2TargetGroup"
        }
    ],
    "VPCZoneIdentifier":{
        "Ref":"Subnets"
    }
}
}
```

Spiegazione passo per passo del modello

La prima parte di questo modello specifica i `Parameters`. A ogni parametro deve essere assegnato un valore in fase di esecuzione per AWS CloudFormation effettuare correttamente il provisioning dello stack. Le risorse specificate più avanti nel modello fanno riferimento a questi valori e utilizzano i dati.

- `InstanceType`: il tipo di EC2 istanza fornito da Amazon EC2 Auto Scaling. Se non viene specificato, viene utilizzato il valore predefinito `t3.micro`.
- `KeyName`: una EC2 key pair esistente per consentire l'accesso SSH alle istanze.
- `LatestAmiId`: l'Amazon Machine Image (AMI) per le istanze. Se non specificato, le istanze vengono avviate con un'AMI Amazon Linux 2, utilizzando un parametro AWS Systems Manager pubblico gestito da AWS. Per ulteriori informazioni, consulta [Ricerca dei parametri pubblici](#) nella Guida per l'utente di AWS Systems Manager .
- `OperatorEmail`: l'indirizzo e-mail a cui desideri inviare le notifiche sulle attività di dimensionamento.
- `SSHLocation`: l'intervallo di indirizzi IP che può essere utilizzato per inviare SSH alle istanze.
- `Subnets`: almeno due sottoreti pubbliche in diverse zone di disponibilità.

- VPC: un cloud privato virtuale (VPC) nel tuo account che consente alle risorse nelle sottoreti pubbliche di connettersi a Internet.

Note

Puoi utilizzare il VPC e le sottoreti predefiniti per consentire alle istanze di accedere a Internet. In quest'ultimo caso, assicurati che il VPC abbia una sottorete mappata a ciascuna zona di disponibilità della Regione in cui stai lavorando. Per creare il load balancer, ti serviranno almeno due sottoreti pubbliche.

La parte successiva di questo modello specifica le `Resources`. Questa sezione specifica le risorse dello stack e le relative proprietà.

[`AWS::EC2::SecurityGroup`](#) `ELBSecurityGroup`

- `SecurityGroupIngress` contiene una regola di ingresso TCP che consente l'accesso da tutti gli indirizzi IP («`CidrIp`": «0.0.0.0/0») sulla porta 80.

[`AWS::EC2::SecurityGroup`](#) `EC2SecurityGroup`

- `SecurityGroupIngress` contiene due regole di ingresso: 1) una regola di ingresso TCP che consente l'accesso SSH (porta 22) dall'intervallo di indirizzi IP fornito per il parametro di input `SSHLocation` e 2) una regola di ingresso TCP che consente l'accesso dal sistema di bilanciamento del carico specificando il gruppo di sicurezza del sistema di bilanciamento del carico. La [`GetAtt`](#) funzione viene utilizzata per ottenere l'ID del gruppo di sicurezza con il nome logico `ELBSecurityGroup`.

[`AWS::ElasticLoadBalancingV2::TargetGroup`](#) `EC2TargetGroup`

- `PortProtocol`, e `HealthCheckProtocol` specifica la porta dell' EC2 istanza (80) e il protocollo (HTTP) verso cui `ApplicationLoadBalancer` indirizza il traffico e che Elastic Load Balancing utilizza per verificare lo stato delle EC2 istanze.
- `HealthCheckIntervalSeconds` specifica che le EC2 istanze hanno un intervallo di 30 secondi tra i controlli di integrità. Per `HealthCheckTimeoutSeconds` si intende il periodo di tempo che Elastic Load Balancing attende per una risposta della destinazione del controllo dell'integrità (15 secondi in questo esempio). Al termine del periodo di timeout, Elastic Load Balancing contrassegna

il controllo dello stato dell'istanza come EC2 non integro. Quando un' EC2 istanza non supera tre controlli di integrità consecutivi (`UnhealthyThresholdCount`), Elastic Load Balancing interrompe l'instradamento del traffico verso quell' EC2istanza fino a quando l'istanza non ha cinque controlli di integrità consecutivi (`HealthyThresholdCount`). A quel punto, Elastic Load Balancing considera l'istanza integra e ricomincia a indirizzare il traffico verso l'istanza.

- `TargetGroupAttributes` aggiorna il valore del ritardo di annullamento della registrazione del gruppo di destinazione a 20 secondi. Per impostazione predefinita, Elastic Load Balancing attende 300 secondi prima di completare il processo di annullamento della registrazione.

[AWS::ElasticLoadBalancingV2::Listener](#) risorsa `ALBListener`

- `DefaultActions` specifica la porta su cui il sistema di bilanciamento del carico ascolta, il gruppo di destinazione a cui il sistema di bilanciamento del carico inoltra le richieste e il protocollo utilizzato per instradare le richieste.

[AWS::ElasticLoadBalancingV2::LoadBalancer](#) risorsa `ApplicationLoadBalancer`

- `Subnets` prende il valore del parametro di input `Subnets` come elenco di sottoreti pubbliche in cui verranno creati i nodi del sistema di bilanciamento del carico.
- `SecurityGroup` ottiene l'ID del gruppo di sicurezza che funge da firewall virtuale per i nodi del sistema di bilanciamento del carico per controllare il traffico in entrata. La [GetAtt](#) funzione viene utilizzata per ottenere l'ID del gruppo di sicurezza con il nome logico `ELBSecurityGroup`.

[AWS::EC2::LaunchTemplate](#) risorsa `LaunchTemplate`

- `ImageId` prende il valore del parametro di input `LatestAmiId` come AMI da utilizzare.
- `KeyName` prende il valore del parametro `KeyName` di input come EC2 key pair da usare.
- `SecurityGroupIds` ottiene l'ID del gruppo di sicurezza con il nome logico `EC2SecurityGroup` che funge da firewall virtuale per consentire alle EC2 istanze di controllare il traffico in entrata.
- `UserData` è uno script di configurazione che viene eseguito dopo che l'istanza è attiva e funzionante. In questo esempio, lo script installa Apache e crea un file `index.html`.

[AWS::SNS::Topic](#) risorsa `NotificationTopic`

- `Subscription` prende il valore del parametro di input `OperatorEmail` come indirizzo e-mail del destinatario delle notifiche in caso di attività di scalabilità.

`AWS::AutoScaling::AutoScalingGroup` [di gruppo](#) `WebServerGroup`

- `MinSize` e `MaxSize` imposta il numero minimo e massimo di EC2 istanze nel gruppo Auto Scaling.
- `TargetGroupARNs` prende l'ARN del gruppo di destinazione con il nome logico `EC2TargetGroup`. Man mano che questo dimensionamento automatico si dimensiona, registra le istanze e ne annulla automaticamente la registrazione con questo gruppo di destinazione.
- `VPCZoneIdentifier` prende il valore del parametro di input `Subnets` come elenco di sottoreti pubbliche in cui è possibile creare le EC2 istanze.

Fase 1: Avvio dello stack

Prima di avviare lo stack, verifica di disporre delle autorizzazioni AWS Identity and Access Management (IAM) per utilizzare tutti i seguenti servizi: Amazon, EC2 Amazon Auto EC2 Scaling AWS Systems Manager, Elastic Load Balancing, Amazon SNS e AWS CloudFormation

La procedura seguente prevede il caricamento del modello di stack di esempio da un file. Apri un editor di testo sul tuo computer locale e aggiungi uno dei modelli. Salva il file con il nome `sampleloadbalancedappstack.template`.

Avvio del modello dello stack

1. [Accedi e apri la console all'indirizzo AWS Management Console /cloudformazione. AWS CloudFormation https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation)
2. Scegliere Create stack (Crea pila), With new resources (standard) (Con nuove risorse (standard)).
3. In Specifica modello, seleziona Carica un file di modello e poi Scegli file per caricare il file `sampleloadbalancedappstack.template`.
4. Scegli Next (Successivo).
5. Nella pagina Specifica i dettagli dello stack, immetti il nome dello stack (ad esempio, **SampleLoadBalancedAppStack**).
6. In Parametri, esamina i parametri per lo stack e fornisci i valori per tutti i parametri che non hanno valori predefiniti, tra cui `OperatorEmail`, `SSHLocationKeyName`, VPC e sottoreti.
7. Scegliere Next (Successivo) due volte.

8. Nella pagina Rivedi, verifica e conferma le impostazioni.
9. Scegli Invia.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Una volta AWS CloudFormation creato con successo lo stack, ricevi lo stato CREATE_COMPLETE.

Note

Dopo aver creato lo stack, perché l'indirizzo e-mail possa iniziare a ricevere notifiche devi confermare la sottoscrizione. Per ulteriori informazioni, consulta [Ricevi notifiche Amazon SNS quando il tuo gruppo Auto Scaling aumenta nella Amazon EC2 Auto Scaling User Guide](#).

Fase 2: Cancellazione delle risorse di esempio

Per assicurarti che non ti vengano addebitati costi per le risorse di esempio inutilizzate, elimina lo stack.

Per eliminare lo stack

1. Nella AWS CloudFormation console, seleziona lo stack. SampleLoadBalancedAppStack
2. Scegliere Delete (Elimina).
3. Nel messaggio di conferma, scegli Elimina stack.

Lo stato delle SampleLoadBalancedAppStackmodifiche a DELETE_IN_PROGRESS. Quando AWS CloudFormation completa l'eliminazione dello stack, lo rimuove dall'elenco.

Usa i modelli di esempio di questa procedura guidata per creare i tuoi modelli stack. Per ulteriori informazioni, consulta [Tutorial: Configurare un'applicazione scalata e con carico bilanciato nella Amazon Auto Scaling EC2 User Guide](#).

Distribuisci applicazioni su Amazon EC2

Puoi utilizzarlo CloudFormation per installare, configurare e avviare automaticamente le applicazioni sulle EC2 istanze Amazon. Ciò ti consente di duplicare in modo semplice le distribuzioni e di

aggiornare le installazioni esistenti senza stabilire una connessione diretta con l'istanza, risparmiando in questo modo una quantità significativa di tempo e lavoro.

CloudFormation include un set di script di supporto (`cfn-init`, `cfn-signal`, `cfn-get-metadata`, e `cfn-hup`) basati su `cloud-init`. Puoi richiamare questi script di supporto dai tuoi CloudFormation modelli per installare, configurare e aggiornare le applicazioni su EC2 istanze Amazon che si trovano nello stesso modello. Per ulteriori informazioni, consulta il riferimento agli [script di CloudFormation supporto nella Template Reference Guide](#). AWS CloudFormation

Nel [tutorial introduttivo](#), hai creato un semplice server web utilizzando uno script UserData bash di base. Sebbene ciò abbia funzionato per una semplice pagina «Hello World», le applicazioni reali spesso richiedono configurazioni più sofisticate, tra cui:

- Più pacchetti software installati nell'ordine corretto.
- File di configurazione complessi creati con contenuti specifici.
- Servizi avviati e configurati per l'esecuzione automatica.
- Gestione degli errori e convalida del processo di configurazione.

CloudFormation gli script di supporto forniscono un modo più robusto e gestibile per configurare le EC2 istanze rispetto agli script bash di base di UserData. Lo script di `cfn-init` supporto legge i dati di configurazione dai metadati del modello e li applica sistematicamente all'istanza.

In questo tutorial, imparerai come usare lo script di `cfn-init` supporto e monitorare il processo di bootstrap.

Note

CloudFormation è gratuito, ma ti verranno addebitate le EC2 risorse Amazon che crei. Tuttavia, se sei alle prime armi AWS, puoi sfruttare il [piano gratuito](#) per ridurre al minimo o eliminare i costi durante questo processo di apprendimento.

Argomenti

- [Prerequisiti](#)
- [Comprensione dei concetti di bootstrap](#)
- [Inizia con un semplice esempio di bootstrap](#)
- [Aggiungere file e comandi](#)

- [Aggiungere la sicurezza di rete](#)
- [Il modello di bootstrap completo](#)
- [Crea lo stack usando la console](#)
- [Monitora il processo di bootstrap](#)
- [Prova il server web avviato](#)
- [Risoluzione dei problemi relativi al bootstrap](#)
- [Pulizia delle risorse](#)
- [Passaggi successivi](#)

Prerequisiti

- Devi aver completato il [Creare il tuo primo stack](#) tutorial o avere un'esperienza equivalente con le nozioni di CloudFormation base.
- Devi avere accesso a un utente o ruolo IAM Account AWS con le autorizzazioni per usare Amazon EC2 e/o l'accesso come utente amministrativo. CloudFormation
- È necessario disporre di un Virtual Private Cloud (VPC) con accesso a Internet. Questo modello di tutorial richiede un VPC predefinito, che viene fornito automaticamente con la versione più recente. Account AWS Se non disponi di un VPC predefinito o se è stato eliminato, consulta la sezione sulla risoluzione dei problemi nel [Creare il tuo primo stack](#) tutorial per soluzioni alternative.

Comprensione dei concetti di bootstrap

Comprendiamo i concetti chiave che fanno funzionare il bootstrap prima di creare il modello.

Lo script helper **cfn-init**

CloudFormation fornisce script di supporto in Python che puoi usare per installare software e avviare servizi su un'istanza Amazon. EC2 Lo `cfn-init` script legge i metadati delle risorse dal modello e applica la configurazione all'istanza.

Il processo funziona nel modo seguente:

1. Definisci la configurazione nella Metadata sezione della tua EC2 risorsa.
2. Si chiama `cfn-init` dallo UserData script.
3. `cfn-init` legge i metadati e applica la configurazione.
4. L'istanza è configurata in base alle tue specifiche.

Struttura dei metadati

La configurazione è definita in una struttura specifica all'interno dell' EC2 istanza.

```
Resources:
  EC2Instance:
    Type: AWS::EC2::Instance
    Metadata:
      # Metadata section for the resource
      AWS::CloudFormation::Init:
        # Required key that cfn-init looks for
        config:
          # Configuration name (you can have multiple)
          packages:
            # Install packages
          files:
            # Create files
          commands:
            # Run commands
          services:
            # Start/stop services
```

Lo `cfn-init` script elabora queste sezioni in un ordine specifico: pacchetti, gruppi, utenti, fonti, file, comandi e quindi servizi.

Inizia con un semplice esempio di bootstrap

Cominciamo con un esempio di bootstrap minimale che installa e avvia semplicemente Apache.

```
Resources:
  EC2Instance:
    Type: AWS::EC2::Instance
    Metadata:
      AWS::CloudFormation::Init:
        config:
          packages:
            # Install Apache web server
          yum:
            httpd: []
          services:
            # Start Apache and enable it to start on boot
            sysvinit:
              httpd:
                enabled: true
                ensureRunning: true
    Properties:
      ImageId: !Ref LatestAmiId
      InstanceType: !Ref InstanceType
      UserData: !Base64
        # Script that runs when instance starts
        Fn::Sub: |
          #!/bin/bash
          yum install -y aws-cfn-bootstrap
```

```
/opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource EC2Instance --  
region ${AWS::Region}
```

Questo semplice esempio illustra i concetti fondamentali:

- `packages` la sezione installa il `httpd` pacchetto utilizzando `yum`. Funziona su Amazon Linux e altre distribuzioni Linux che utilizzano `yum`.
- `services` la sezione garantisce l'avvio e l'esecuzione automaticamente.
- `UserData` installa gli strumenti e le chiamate di bootstrap più recenti. `cfn-init`

Aggiungere file e comandi

Ora, miglioriamo il nostro esempio aggiungendo una pagina Web personalizzata e un file di registro nella `/var/log` directory dell' EC2 istanza.

Creazione di file

La `files` sezione consente di creare file sull'istanza con contenuti specifici. La barra verticale (`|`) consente di passare un blocco letterale di testo (codice HTML) come contenuto del file (`/var/www/html/index.html`).

```
files:  
  /var/www/html/index.html:  
    content: |  
      <body>  
        <h1>Congratulations, you have successfully launched the AWS CloudFormation  
sample.</h1>  
      </body>
```

Esecuzione di comandi

La `commands` sezione consente di eseguire i comandi della shell durante il processo di bootstrap. Questo comando crea un file di registro `/var/log/welcome.txt` sull' EC2 istanza. Per visualizzarlo, è necessaria una coppia di EC2 chiavi Amazon da utilizzare per l'accesso SSH e un intervallo di indirizzi IP che può essere utilizzato per l'accesso SSH all'istanza (non trattato qui).

```
commands:  
  createWelcomeLog:  
    command: "echo 'cfn-init ran successfully!' > /var/log/welcome.txt"
```

Aggiungere la sicurezza di rete

Poiché stiamo configurando un server Web, dobbiamo consentire al traffico web (HTTP) di raggiungere la nostra EC2 istanza. Per fare ciò, creeremo un gruppo di sicurezza che consente il traffico in entrata sulla porta 80 dal tuo indirizzo IP. EC2 le istanze devono anche inviare traffico verso Internet, ad esempio per installare gli aggiornamenti dei pacchetti. Per impostazione predefinita, i gruppi di sicurezza consentono tutto il traffico in uscita. Quindi assoceremo questo gruppo di sicurezza alla nostra EC2 istanza utilizzando la `SecurityGroupIds` proprietà.

```
WebServerSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Allow HTTP access from my IP address
    SecurityGroupIngress:
      - IpProtocol: tcp
        Description: HTTP
        FromPort: 80
        ToPort: 80
        CidrIp: !Ref MyIP
```

Il modello di bootstrap completo

Ora mettiamo insieme tutti i pezzi. Ecco il modello completo che combina tutti i concetti di cui abbiamo parlato.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Bootstrap an EC2 instance with Apache web server using cfn-init

Parameters:
  LatestAmiId:
    Description: The latest Amazon Linux 2 AMI from the Parameter Store
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2'

  InstanceType:
    Description: EC2 instance type
    Type: String
    Default: t2.micro
    AllowedValues:
      - t3.micro
      - t2.micro
    ConstraintDescription: must be a valid EC2 instance type.
```

MyIP:

Description: Your IP address in CIDR format (e.g. 203.0.113.1/32)

Type: String

MinLength: 9

MaxLength: 18

Default: 0.0.0.0/0

AllowedPattern: '^(\d{1,3}\.){3}\d{1,3}\.\/\d{1,2}\$'

ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.

Resources:**WebServerSecurityGroup:**

Type: AWS::EC2::SecurityGroup

Properties:

GroupDescription: Allow HTTP access from my IP address

SecurityGroupIngress:

- IpProtocol: tcp

Description: HTTP

FromPort: 80

ToPort: 80

CidrIp: !Ref MyIP

WebServer:

Type: AWS::EC2::Instance

Metadata:**AWS::CloudFormation::Init:****config:****packages:****yum:**

httpd: []

files:

/var/www/html/index.html:

content: |

<body>

<h1>Congratulations, you have successfully launched the AWS

CloudFormation sample.</h1>

</body>

commands:**createWelcomeLog:**

command: "echo 'cfn-init ran successfully!' > /var/log/welcome.txt"

services:**sysvinit:****httpd:**

enabled: true

```
        ensureRunning: true
    Properties:
        ImageId: !Ref LatestAmiId
        InstanceType: !Ref InstanceType
        SecurityGroupIds:
            - !Ref WebServerSecurityGroup
        UserData: !Base64
            Fn::Sub: |
                #!/bin/bash
                yum install -y aws-cfn-bootstrap
                /opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource WebServer --
region ${AWS::Region}
        Tags:
            - Key: Name
              Value: Bootstrap Tutorial Web Server

    Outputs:
        WebsiteURL:
            Value: !Sub 'http://${WebServer.PublicDnsName}'
            Description: EC2 instance public DNS name
```

Crea lo stack usando la console

La procedura seguente prevede il caricamento del modello di stack di esempio da un file. Apri un editor di testo sul tuo computer locale e aggiungi il modello. Salva il file con il nome `samplelinux2stack.template`.

Avvio del modello dello stack

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Scegliere Create stack (Crea pila), With new resources (standard) (Con nuove risorse (standard)).
3. In Specifica modello, seleziona Carica un file di modello e poi Scegli file per caricare il file `samplelinux2stack.template`.
4. Scegli Next (Successivo).
5. Nella pagina Specificare i dettagli dello stack, digita **BootstrapTutorialStack** come nome dello stack.
6. In Parametri, effettuate le seguenti operazioni.

- LatestAmild: Lasciate il valore predefinito.
 - InstanceType: Scegli t2.micro o t3.micro per il tipo di istanza. EC2
 - MyIP: inserisci il tuo indirizzo IP pubblico con un /32 suffisso.
7. Scegli Avanti due volte, quindi Invia per creare lo stack.

Monitora il processo di bootstrap

I processi di bootstrap richiedono più tempo rispetto ai semplici EC2 avvii perché vengono installati e configurati software aggiuntivi.

Per monitorare l'avanzamento del bootstrap

1. Nella CloudFormation console, seleziona il tuo stack e apri la scheda Eventi.
2. Tieni d'occhio l'WebServer CREATE_IN_PROGRESSevento. Il processo di bootstrap inizia dopo l'avvio dell'istanza.
3. Il processo di bootstrap richiede in genere alcuni minuti. Vedrai WebServer CREATE_COMPLETE quando sarà finito.

Se vuoi vedere cosa succede durante il processo di bootstrap, puoi controllare i log delle istanze.

Per visualizzare i log di bootstrap (opzionale)

1. Apri la [EC2 console](#) e trova la tua istanza.
2. Seleziona l'istanza, quindi scegli Azioni, Monitoraggio e risoluzione dei problemi, Ottieni il registro di sistema per vedere l'avanzamento del bootstrap.
3. Se non vedi immediatamente i log, attendi e aggiorna la pagina.

Prova il server web avviato

Quando lo stack viene visualizzatoCREATE_COMPLETE, prova il tuo server web.

Per testare il server web

1. Nella CloudFormation console, vai alla scheda Output relativa al tuo stack.
2. Fai clic sul valore WebsiteURL per aprire il tuo server web in una nuova scheda.

3. Dovresti vedere la tua pagina web personalizzata con il messaggio. Congratulations, you have successfully launched the AWS CloudFormation sample

Note

Se la pagina non viene caricata immediatamente, attendi un minuto e riprova. Il processo di bootstrap potrebbe essere ancora completato anche dopo la visualizzazione dello stack. CREATE_COMPLETE

Risoluzione dei problemi relativi al bootstrap

Se il processo di bootstrap fallisce o il server web non funziona, ecco i problemi e le soluzioni più comuni.

Problemi comuni

- La creazione dello stack non riesce: controlla la scheda Eventi per messaggi di errore specifici.
- Server Web non accessibile: verifica che l'indirizzo IP sia corretto nel MyIP parametro. Ricordati di includere /32 alla fine.
- Il processo di bootstrap fallisce: l'istanza può avviarsi ma `cfn-init` fallisce. Controlla i log di sistema come descritto nella sezione di monitoraggio.

Pulizia delle risorse

Per evitare addebiti continui, puoi eseguire la pulizia eliminando lo stack e le relative risorse.

Eliminare lo stack e delle relative risorse

1. Apri la [CloudFormation console](#).
2. Nella pagina Pile, seleziona l'opzione accanto al nome dello stack che hai creato (**BootstrapTutorialStack**), quindi scegli Elimina.
3. Quando viene richiesta la conferma, seleziona Delete (Elimina).
4. Monitora l'avanzamento del processo di eliminazione dello stack nella scheda Evento. Lo stato di **BootstrapTutorialStack** cambia in DELETE_IN_PROGRESS. Una volta CloudFormation completata l'eliminazione dello stack, lo rimuove dall'elenco.

Passaggi successivi

Complimenti! Hai imparato con successo a eseguire il bootstrap EC2 delle istanze con CloudFormation. Ora capisci:

- Come usare gli script di `cfn-init` supporto
- Come strutturare i metadati per il bootstrap
- Come installare pacchetti, creare file, eseguire comandi e gestire servizi
- Come monitorare i problemi relativi al bootstrap

Per continuare a imparare:

- Scopri come avviare uno Windows stack. Per ulteriori informazioni, consulta [Stack basati sul bootstrap Windows CloudFormation](#).
- Esplora scenari di bootstrap più complessi con più set di configurazione. Per maggiori informazioni, consulta [cfn-init](#) e [AWS::CloudFormation::Init](#) nella Template Reference Guide. AWS CloudFormation
- Scopri come segnalare lo stato di `cfn-signal` completamento del bootstrap. Per ulteriori informazioni, consulta [cfn-signal](#) nella AWS CloudFormation Template Reference Guide.

Aggiornamento di uno stack

Con CloudFormation, puoi aggiornare le proprietà delle risorse negli stack esistenti. Queste modifiche possono variare da semplici modifiche alla configurazione, come l'aggiornamento della soglia di allarme di un CloudWatch allarme, a modifiche più complesse, come l'aggiornamento dell'Amazon Machine Image (AMI) in esecuzione su un' EC2 istanza Amazon. Molte AWS risorse di un modello possono essere aggiornate e continuiamo ad aggiungere il supporto per altre.

Questa sezione descrive in dettaglio una semplice progressione di aggiornamenti di uno stack in esecuzione. Mostra come l'uso dei modelli consenta di utilizzare un sistema di controllo delle versioni per la configurazione dell' AWS infrastruttura, proprio come si utilizza il controllo della versione per il software in esecuzione. Verranno descritte le fasi seguenti:

1. [Creazione dello stack iniziale](#): creare uno stack utilizzando un'AMI Amazon Linux di base, installando il Web Server Apache e una semplice applicazione PHP tramite gli script helper CloudFormation.

2. [Aggiornamento dell'applicazione](#)— aggiorna uno dei file dell'applicazione e distribuisce il software utilizzando CloudFormation.
3. [Aggiornamento del tipo di istanza](#)— modificare il tipo di istanza dell' EC2 istanza Amazon sottostante.
4. [Aggiorna l'AMI su un' EC2istanza Amazon](#)— modifica l'Amazon Machine Image (AMI) per l' EC2 istanza Amazon nel tuo stack.
5. [Aggiunta di una coppia di chiavi a un'istanza](#)— aggiungere una coppia di EC2 chiavi Amazon all'istanza, quindi aggiornare il gruppo di sicurezza per consentire l'accesso SSH all'istanza.
6. [Modifica delle risorse dello stack](#): aggiungere e rimuovere risorse dallo stack e convertirlo in un'applicazione con load balancer e dimensionamento automatico, tramite l'aggiornamento del modello.

Un'applicazione semplice

Inizieremo creando uno stack che potremo utilizzare in tutto il resto di questa sezione. Abbiamo fornito un semplice modello che avvia un'applicazione Web PHP a istanza singola ospitata sul Web Server Apache e in esecuzione su un AMI Amazon Linux.

Il Web Server Apache, PHP e la semplice applicazione PHP vengono tutti installati dagli script helper di CloudFormation , installati per impostazione predefinita nell'AMI Amazon Linux. Il seguente frammento di modello mostra i metadati che descrivono i pacchetti e i file da installare, in questo caso il Web Server Apache e l'infrastruttura PHP dal repository Yum dell'AMI Amazon Linux. Il frammento mostra inoltre la sezione Services, che assicura che il Web Server Apache sia in esecuzione. Nella sezione Properties della definizione dell' EC2 istanza Amazon, la UserData proprietà contiene lo CloudInit script che chiama cfn-init per installare i pacchetti e i file.

```
"WebServerInstance": {
  "Type" : "AWS::EC2::Instance",
  "Metadata" : {
    "AWS::CloudFormation::Init" : {
      "config" : {
        "packages" : {
          "yum" : {
            "httpd"      : [],
            "php"        : []
          }
        }
      }
    }
  },
```

```

"files" : {

  "/var/www/html/index.php" : {
    "content" : { "Fn::Join" : ["", [
      "<?php\n",
      "echo '<h1>AWS CloudFormation sample PHP application</h1>';\n",
      "echo '<p>', { "Ref" : "WelcomeMessage" }, "</p>";\n",
      "?>\n"
    ]]],
    "mode"      : "000644",
    "owner"     : "apache",
    "group"     : "apache"
  },
},

:

"services" : {
  "sysvinit" : {
    "httpd"   : { "enabled" : "true", "ensureRunning" : "true" }
  }
}
}
},

"Properties": {
  :
  "UserData" : { "Fn::Base64" : { "Fn::Join" : ["", [
    "#!/bin/bash\n",
    "yum install -y aws-cfn-bootstrap\n",

    :

    "# Install the files and packages from the metadata\n",
    "/opt/aws/bin/cfn-init -v ",
    "      --stack ", { "Ref" : "AWS::StackName" },
    "      --resource WebServerInstance ",
    "      --region ", { "Ref" : "AWS::Region" }, "\n",
    :
  ]]]}
}

```

```
},
```

L'applicazione in sé è un esempio di due righe, "Hello World", completamente definito all'interno del modello. Per un'applicazione reale, i file possono essere archiviati su Amazon S3 GitHub o su un altro repository e referenziati dal modello. CloudFormation può scaricare pacchetti (come RPMs o RubyGems) e fare riferimento a singoli file ed espandere .zip e .tar file per creare gli artefatti dell'applicazione sull'istanza Amazon EC2.

Il modello abilita e configura il demone cfn-hup per ascoltare le modifiche alla configurazione definita nei metadati per l'istanza Amazon. EC2 Utilizzando il demone cfn-hup, puoi aggiornare il software applicativo, come la versione di Apache o PHP, oppure puoi aggiornare il file dell'applicazione PHP stesso. CloudFormation Il seguente frammento della stessa EC2 risorsa Amazon nel modello mostra le parti necessarie per configurare cfn-hup per chiamare cfn-init per aggiornare il software se vengono rilevate modifiche ai metadati:

```
"WebServerInstance": {
  "Type" : "AWS::EC2::Instance",
  "Metadata" : {
    "AWS::CloudFormation::Init" : {
      "config" : {

        :

      "files" : {

        :

        "/etc/cfn/cfn-hup.conf" : {
          "content" : { "Fn::Join" : ["", [
            "[main]\n",
            "stack=", { "Ref" : "AWS::StackName" }, "\n",
            "region=", { "Ref" : "AWS::Region" }, "\n"
          ]]],
          "mode" : "000400",
          "owner" : "root",
          "group" : "root"
        },

        "/etc/cfn/hooks.d/cfn-auto-reloader.conf" : {
          "content": { "Fn::Join" : ["", [
            "[cfn-auto-reloader-hook]\n",
```

```

        "triggers=post.update\n",
        "path=Resources.WebServerInstance.Metadata.AWS::CloudFormation::Init
\n",
        "action=/opt/aws/bin/cfn-init -s ", { "Ref" : "AWS::StackId" }, " -r
WebServerInstance ",
        " --region      ", { "Ref" : "AWS::Region" }, "\n",
        "runas=root\n"
    ]}]
    }
  },
  :
},
"Properties": {
  :
  "UserData"      : { "Fn::Base64" : { "Fn::Join" : [ "", [
  :
  "# Start up the cfn-hup daemon to listen for changes to the Web Server metadata
\n",
  "/opt/aws/bin/cfn-hup || error_exit 'Failed to start cfn-hup'\n",
  :
  ]]]}
  }
},

```

Per completare lo stack, il modello crea un gruppo EC2 di sicurezza Amazon.

```

{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS CloudFormation Sample Template: Sample template that can be used
to test EC2 updates. **WARNING** This template creates an Amazon Ec2 Instance. You
will be billed for the AWS resources used if you create a stack from this template.",

  "Parameters" : {

    "InstanceType" : {
      "Description" : "WebServer EC2 instance type",

```

```
"Type" : "String",
"Default" : "t2.small",
"AllowedValues" : [
  "t1.micro",
  "t2.nano",
  "t2.micro",
  "t2.small",
  "t2.medium",
  "t2.large",
  "m1.small",
  "m1.medium",
  "m1.large",
  "m1.xlarge",
  "m2.xlarge",
  "m2.2xlarge",
  "m2.4xlarge",
  "m3.medium",
  "m3.large",
  "m3.xlarge",
  "m3.2xlarge",
  "m4.large",
  "m4.xlarge",
  "m4.2xlarge",
  "m4.4xlarge",
  "m4.10xlarge",
  "c1.medium",
  "c1.xlarge",
  "c3.large",
  "c3.xlarge",
  "c3.2xlarge",
  "c3.4xlarge",
  "c3.8xlarge",
  "c4.large",
  "c4.xlarge",
  "c4.2xlarge",
  "c4.4xlarge",
  "c4.8xlarge",
  "g2.2xlarge",
  "g2.8xlarge",
  "r3.large",
  "r3.xlarge",
  "r3.2xlarge",
  "r3.4xlarge",
  "r3.8xlarge",
```

```

        "i2.xlarge",
        "i2.2xlarge",
        "i2.4xlarge",
        "i2.8xlarge",
        "d2.xlarge",
        "d2.2xlarge",
        "d2.4xlarge",
        "d2.8xlarge",
        "hi1.4xlarge",
        "hs1.8xlarge",
        "cr1.8xlarge",
        "cc2.8xlarge",
        "cg1.4xlarge"
    ],
    "ConstraintDescription" : "must be a valid EC2 instance type."
}
},

"Mappings" : {
    "AWSInstanceType2Arch" : {
        "t1.micro"      : { "Arch" : "HVM64" },
        "t2.nano"      : { "Arch" : "HVM64" },
        "t2.micro"      : { "Arch" : "HVM64" },
        "t2.small"     : { "Arch" : "HVM64" },
        "t2.medium"    : { "Arch" : "HVM64" },
        "t2.large"     : { "Arch" : "HVM64" },
        "m1.small"     : { "Arch" : "HVM64" },
        "m1.medium"    : { "Arch" : "HVM64" },
        "m1.large"     : { "Arch" : "HVM64" },
        "m1.xlarge"    : { "Arch" : "HVM64" },
        "m2.xlarge"     : { "Arch" : "HVM64" },
        "m2.2xlarge"   : { "Arch" : "HVM64" },
        "m2.4xlarge"   : { "Arch" : "HVM64" },
        "m3.medium"    : { "Arch" : "HVM64" },
        "m3.large"     : { "Arch" : "HVM64" },
        "m3.xlarge"    : { "Arch" : "HVM64" },
        "m3.2xlarge"   : { "Arch" : "HVM64" },
        "m4.large"     : { "Arch" : "HVM64" },
        "m4.xlarge"    : { "Arch" : "HVM64" },
        "m4.2xlarge"   : { "Arch" : "HVM64" },
        "m4.4xlarge"   : { "Arch" : "HVM64" },
        "m4.10xlarge"  : { "Arch" : "HVM64" },
        "c1.medium"    : { "Arch" : "HVM64" },
        "c1.xlarge"    : { "Arch" : "HVM64" },
    },

```

```

    "c3.large"      : { "Arch" : "HVM64" },
    "c3.xlarge"     : { "Arch" : "HVM64" },
    "c3.2xlarge"    : { "Arch" : "HVM64" },
    "c3.4xlarge"    : { "Arch" : "HVM64" },
    "c3.8xlarge"    : { "Arch" : "HVM64" },
    "c4.large"      : { "Arch" : "HVM64" },
    "c4.xlarge"     : { "Arch" : "HVM64" },
    "c4.2xlarge"    : { "Arch" : "HVM64" },
    "c4.4xlarge"    : { "Arch" : "HVM64" },
    "c4.8xlarge"    : { "Arch" : "HVM64" },
    "g2.2xlarge"    : { "Arch" : "HVMG2" },
    "g2.8xlarge"    : { "Arch" : "HVMG2" },
    "r3.large"      : { "Arch" : "HVM64" },
    "r3.xlarge"     : { "Arch" : "HVM64" },
    "r3.2xlarge"    : { "Arch" : "HVM64" },
    "r3.4xlarge"    : { "Arch" : "HVM64" },
    "r3.8xlarge"    : { "Arch" : "HVM64" },
    "i2.xlarge"     : { "Arch" : "HVM64" },
    "i2.2xlarge"    : { "Arch" : "HVM64" },
    "i2.4xlarge"    : { "Arch" : "HVM64" },
    "i2.8xlarge"    : { "Arch" : "HVM64" },
    "d2.xlarge"     : { "Arch" : "HVM64" },
    "d2.2xlarge"    : { "Arch" : "HVM64" },
    "d2.4xlarge"    : { "Arch" : "HVM64" },
    "d2.8xlarge"    : { "Arch" : "HVM64" },
    "hi1.4xlarge"   : { "Arch" : "HVM64" },
    "hs1.8xlarge"   : { "Arch" : "HVM64" },
    "cr1.8xlarge"   : { "Arch" : "HVM64" },
    "cc2.8xlarge"   : { "Arch" : "HVM64" }
  },

```

```

  "AWSRegionArch2AMI" : {
    "us-east-1"      : {"HVM64" : "ami-0ff8a91507f77f867", "HVMG2" :
"ami-0a584ac55a7631c0c"},
    "us-west-2"      : {"HVM64" : "ami-a0cfeed8", "HVMG2" :
"ami-0e09505bc235aa82d"},
    "us-west-1"      : {"HVM64" : "ami-0bdb828fd58c52235", "HVMG2" :
"ami-066ee5fd4a9ef77f1"},
    "eu-west-1"      : {"HVM64" : "ami-047bb4163c506cd98", "HVMG2" :
"ami-0a7c483d527806435"},
    "eu-west-2"      : {"HVM64" : "ami-f976839e", "HVMG2" : "NOT_SUPPORTED"},
    "eu-west-3"      : {"HVM64" : "ami-0ebc281c20e89ba4b", "HVMG2" :
"NOT_SUPPORTED"},

```



```

    "eu-central-1"      : {"HVM64" : "ami-0233214e13e500f77", "HVMG2" :
"ami-06223d46a6d0661c7"},
    "ap-northeast-1"    : {"HVM64" : "ami-06cd52961ce9f0d85", "HVMG2" :
"ami-053cdd503598e4a9d"},
    "ap-northeast-2"    : {"HVM64" : "ami-0a10b2721688ce9d2", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-northeast-3"    : {"HVM64" : "ami-0d98120a9fb693f07", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-southeast-1"    : {"HVM64" : "ami-08569b978cc4dfa10", "HVMG2" :
"ami-0be9df32ae9f92309"},
    "ap-southeast-2"    : {"HVM64" : "ami-09b42976632b27e9b", "HVMG2" :
"ami-0a9ce9fecc3d1daf8"},
    "ap-south-1"        : {"HVM64" : "ami-0912f71e06545ad88", "HVMG2" :
"ami-097b15e89dbdcfcf4"},
    "us-east-2"         : {"HVM64" : "ami-0b59bfac6be064b78", "HVMG2" :
"NOT_SUPPORTED"},
    "ca-central-1"      : {"HVM64" : "ami-0b18956f", "HVMG2" : "NOT_SUPPORTED"},
    "sa-east-1"         : {"HVM64" : "ami-07b14488da8ea02a0", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-north-1"        : {"HVM64" : "ami-0a4eaf6c4454eda75", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-northwest-1"    : {"HVM64" : "ami-6b6a7d09", "HVMG2" : "NOT_SUPPORTED"}
  }
},

"Resources" : {

  "WebServerInstance": {
    "Type" : "AWS::EC2::Instance",
    "Metadata" : {
      "Comment" : "Install a simple PHP application",
      "AWS::CloudFormation::Init" : {
        "config" : {
          "packages" : {
            "yum" : {
              "httpd"      : [],
              "php"        : []
            }
          },
          "files" : {

            "/var/www/html/index.php" : {
              "content" : { "Fn::Join" : ["", [

```

```

        "<?php\n",
        "echo '<h1>AWS CloudFormation sample PHP application</h1>';\n",
        "?>\n"
    ]],
    "mode"      : "000644",
    "owner"     : "apache",
    "group"     : "apache"
},

"/etc/cfn/cfn-hup.conf" : {
    "content" : { "Fn::Join" : [ "", [
        "[main]\n",
        "stack=", { "Ref" : "AWS::StackId" }, "\n",
        "region=", { "Ref" : "AWS::Region" }, "\n"
    ] ] },
    "mode"      : "000400",
    "owner"     : "root",
    "group"     : "root"
},

"/etc/cfn/hooks.d/cfn-auto-reloader.conf" : {
    "content": { "Fn::Join" : [ "", [
        "[cfn-auto-reloader-hook]\n",
        "triggers=post.update\n",
        "path=Resources.WebServerInstance.Metadata.AWS::CloudFormation::Init\n",
        "action=/opt/aws/bin/cfn-init -s ", { "Ref" : "AWS::StackId" }, " -r\n",
        "WebServerInstance ",
        " --region ", { "Ref" : "AWS::Region" }, "\n",
        "runas=root\n"
    ] ] },
    "mode"      : "000400",
    "owner"     : "root",
    "group"     : "root"
},

"services" : {
    "sysvinit" : {
        "httpd" : { "enabled" : "true", "ensureRunning" : "true" },
        "cfn-hup" : { "enabled" : "true", "ensureRunning" : "true",
            "files" : [ "/etc/cfn/cfn-hup.conf", "/etc/cfn/hooks.d/cfn-auto-reloader.conf" ] }
    }
}

```

```

    }
  }
},

  "Properties": {
    "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" :
"AWS::Region" },
                                { "Fn::FindInMap" : [ "AWSInstanceType2Arch", { "Ref" :
"InstanceType" }, "Arch" ] } ] },
    "InstanceType" : { "Ref" : "InstanceType" },
    "SecurityGroups" : [ { "Ref" : "WebServerSecurityGroup" } ],
    "UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [
      "#!/bin/bash -xe\n",
      "yum install -y aws-cfn-bootstrap\n",

      "# Install the files and packages from the metadata\n",
      "/opt/aws/bin/cfn-init -v ",
      "      --stack ", { "Ref" : "AWS::StackName" },
      "      --resource WebServerInstance ",
      "      --region ", { "Ref" : "AWS::Region" }, "\n",

      "# Start up the cfn-hup daemon to listen for changes to the Web Server
metadata\n",
      "/opt/aws/bin/cfn-hup || error_exit 'Failed to start cfn-hup'\n",

      "# Signal the status from cfn-init\n",
      "/opt/aws/bin/cfn-signal -e $? ",
      "      --stack ", { "Ref" : "AWS::StackName" },
      "      --resource WebServerInstance ",
      "      --region ", { "Ref" : "AWS::Region" }, "\n"
    ] ] ] }
  ] }
},
  "CreationPolicy" : {
    "ResourceSignal" : {
      "Timeout" : "PT5M"
    }
  }
},

  "WebServerSecurityGroup" : {
    "Type" : "AWS::EC2::SecurityGroup",
    "Properties" : {
      "GroupDescription" : "Enable HTTP access via port 80",
      "SecurityGroupIngress" : [

```

```
        {"IpProtocol" : "tcp", "FromPort" : "80", "ToPort" : "80", "CidrIp" :  
"0.0.0.0/0"}  
    ]  
  }  
},  
  
"Outputs" : {  
  "WebsiteURL" : {  
    "Description" : "Application URL",  
    "Value" : { "Fn::Join" : [ "", [ "http://", { "Fn::GetAtt" : [ "WebServerInstance",  
"PublicDnsName" ] } ] ] }  
  }  
}
```

Questo esempio utilizza una singola EC2 istanza Amazon, ma puoi utilizzare gli stessi meccanismi su soluzioni più complesse che utilizzano Elastic Load Balancing e Amazon EC2 Auto Scaling gruppi per gestire una raccolta di server di applicazioni. Ci sono, tuttavia, alcune considerazioni particolari per i gruppi Auto Scaling. Per ulteriori informazioni, consulta [Aggiornamento dei gruppi Auto Scaling](#).

Creazione dello stack iniziale

Ai fini di questo esempio, utilizzeremo il AWS Management Console per creare uno stack iniziale dal modello di esempio.

Warning

Il completamento di questa procedura implementerà i servizi live AWS . Ti verranno addebitate le tariffe standard di utilizzo fintanto che questi servizi sono in esecuzione.

Per creare lo stack dalla AWS Management Console

1. Copiare il modello precedente e salvarlo localmente nel sistema come file di testo. Annotare il percorso perché sarà necessario utilizzare il file in una fase successiva.
2. Accedi alla CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Selezionare Create new stack (Crea nuovo stack).

4. Nella procedura guidata Create New Stack (Crea nuovo stack), nella schermata Select Template (Seleziona modello) digitare **UpdateTutorial1** nel campo Name (Nome). Nella stessa pagina, selezionare Upload a template to Amazon S3 (Carica un modello in Amazon S3) e individuare il file scaricato nella prima fase, quindi selezionare Next (Avanti).
5. Nella schermata Specify Parameters (Specifica parametri), nella casella Instance Type (Tipo di istanza) digitare **t1.micro**. Quindi scegli Successivo.
6. Nella schermata Options (Opzioni) selezionare Next (Avanti).
7. Nella schermata Review (Rivedi) verificare che tutte le impostazioni siano quelle desiderate, quindi fare clic su Create (Crea).

Quando lo stato dello stack è CREATE_COMPLETE, la scheda di output mostra l'URL del tuo sito Web. Facendo clic sul valore dell'output WebsiteURL, si vedrà la nuova applicazione PHP funzionante.

Aggiornamento dell'applicazione

Una volta distribuito lo stack, è il momento di aggiornare l'applicazione. Apporteremo una semplice modifica al testo visualizzato dall'applicazione. Per farlo, aggiungeremo un comando echo al file index.php come illustrato in questo frammento di modello:

```
"WebServerInstance": {
  "Type" : "AWS::EC2::Instance",
  "Metadata" : {
    "AWS::CloudFormation::Init" : {
      "config" : {
        :

      "files" : {

        "/var/www/html/index.php" : {
          "content" : { "Fn::Join" : ["", [
            "<?php\n",
            "echo '<h1>AWS CloudFormation sample PHP application</h1>';\n",
            "echo '<p>Updated version via UpdateStack</p>';\n ",
            "?>\n"
          ]}},
          "mode" : "000644",
          "owner" : "apache",
          "group" : "apache"
        },
      },
    }
  },
}
```

```
        :  
    }  
},
```

Utilizza un editor di testo per modificare manualmente il file del modello salvato in locale.

A questo punto aggiorneremo lo stack.

Per aggiornare lo stack dal AWS Management Console

1. Accedi alla CloudFormation console, all'indirizzo: <https://console.aws.amazon.com/cloudformazione>.
2. Nella CloudFormation dashboard, scegli lo stack che hai creato in precedenza, quindi scegli Update Stack.
3. Nella procedura guidata Update Stack (Aggiorna stack), nella schermata Select Template (Seleziona modello) selezionare Upload a template to Amazon S3 (Carica un modello in Amazon S3), selezionare il modello modificato, quindi selezionare Next (Avanti).
4. Nella schermata Options (Opzioni) selezionare Next (Avanti).
5. Selezionare Next (Avanti) perché lo stack non dispone di una policy di stack. Tutte le risorse possono essere aggiornate senza una policy di sostituzione.
6. Nella schermata Review (Rivedi) verificare che tutte le impostazioni siano quelle desiderate, quindi selezionare Update (Aggiorna).

Se aggiorni lo stack da AWS Management Console, noterai che i parametri utilizzati per creare lo stack iniziale sono precompilati nella pagina Parametri della procedura guidata Update Stack. Se utilizzi il comando `update-stack`, assicurati di digitare gli stessi valori dei parametri che hai utilizzato originariamente per creare lo stack.

Quando lo stack si trova nello stato `UPDATE_COMPLETE`, puoi selezionare nuovamente il valore di output `WebsiteURL` per verificare che le modifiche all'applicazione abbiano avuto effetto. Per impostazione predefinita, il daemon `cfn-hup` viene eseguito ogni 15 minuti, pertanto potrebbero essere necessari fino a 15 minuti prima che l'applicazione venga modificata dopo l'aggiornamento dello stack.

Per vedere il set di risorse che sono state aggiornate, vai alla console. CloudFormation Nella scheda Events (Eventi) controlla gli eventi dello stack. In questo caso particolare, i metadati per l' EC2

istanza Amazon sono `WebServerInstance` stati aggiornati, il che ha CloudFormation comportato anche una rivalutazione delle altre risorse (`WebServerSecurityGroup`) per garantire che non vi fossero altre modifiche. Nessuna delle altre risorse dello stack è stata modificata. CloudFormation aggiornerà solo le risorse dello stack che sono interessate da eventuali modifiche allo stack. Tali modifiche possono essere dirette, ad esempio modifiche alle proprietà o ai metadati, oppure possono essere dovute a dipendenze o flussi di dati tramite `Ref` o ad altre funzioni `GetAtt` intrinseche del modello. [Per ulteriori informazioni, vedere Riferimento alla funzione intrinseca.](#)

Questo semplice aggiornamento illustra il processo; tuttavia, puoi apportare modifiche molto più complesse ai file e ai pacchetti distribuiti nelle tue istanze Amazon EC2 . Ad esempio, puoi decidere di aggiungere MySQL all'istanza, insieme al supporto PHP per MySQL. A tale scopo, è sufficiente aggiungere gli ulteriori pacchetti e file con eventuali altri servizi alla configurazione e quindi aggiornare lo stack per distribuire le modifiche. Nel seguente frammento di modello, le modifiche sono evidenziate in rosso:

```
"WebServerInstance": {
  "Type" : "AWS::EC2::Instance",
  "Metadata" : {
    "Comment" : "Install a simple PHP application",
    "AWS::CloudFormation::Init" : {
      "config" : {
        "packages" : {
          "yum" : {
            "httpd"           : [],
            "php"             : [],
            "php-mysql"       : [],
            "mysql-server"    : [],
            "mysql-libs"      : [],
            "mysql"           : []
          }
        },
        :

      "services" : {
        "sysvinit" : {
          "httpd"   : { "enabled" : "true", "ensureRunning" : "true" },
          "cfn-hup" : { "enabled" : "true", "ensureRunning" : "true",
            "files" : ["/etc/cfn/cfn-hup.conf", "/etc/cfn/hooks.d/cfn-auto-
reloader.conf"]},
          "mysqld"   : { "enabled" : "true", "ensureRunning" : "true" }
        }
      }
    }
  }
}
```

```
    }  
  }  
},  
  
  "Properties": {  
    :  
  }  
}
```

Puoi aggiornare i CloudFormation metadati per aggiornarli alle nuove versioni dei pacchetti utilizzati dall'applicazione. Negli esempi precedenti, la proprietà della versione per ogni pacchetto è vuota, a indicare che cfn-init deve installare la versione più recente del pacchetto.

```
"packages" : {  
  "yum" : {  
    "httpd"      : [],  
    "php"        : []  
  }  
}
```

È possibile specificare una stringa di versione per un pacchetto. Se modifichi la stringa della versione nelle successive chiamate di aggiornamento dello stack, verrà distribuita la nuova versione del pacchetto. Ecco un esempio di utilizzo dei numeri di versione per i RubyGems pacchetti. Qualsiasi pacchetto che supporta il controllo delle versioni può avere versioni specifiche.

```
"packages" : {  
  "rubygems" : {  
    "mysql"      : [],  
    "rubygems-update" : ["1.6.2"],  
    "rake"       : ["0.8.7"],  
    "rails"      : ["2.3.11"]  
  }  
}
```

Aggiornamento dei gruppi Auto Scaling

Se utilizzi gruppi Auto Scaling nel tuo modello, anziché risorse di EC2 istanze Amazon, l'aggiornamento dell'applicazione funzionerà esattamente nello stesso modo; tuttavia, CloudFormation non fornisce alcuna sincronizzazione o serializzazione tra le EC2 istanze Amazon in un gruppo Auto Scaling. Il daemon cfn-hup su ogni host verrà eseguito in modo indipendente e aggiornerà l'applicazione secondo la propria programmazione. Quando utilizzi cfn-hup per

aggiornare la configurazione dell'istanza, ogni istanza eseguirà gli hook di cfn-hup in base alla propria programmazione; non è previsto alcun coordinamento tra le istanze nello stack. È opportuno considerare quanto segue:

- Se le modifiche a cfn-hup vengono eseguite contemporaneamente su tutte le EC2 istanze Amazon nel gruppo Auto Scaling, il servizio potrebbe non essere disponibile durante l'aggiornamento.
- Se le modifiche di cfn-hup vengono eseguite in momenti diversi, vecchie e nuove versioni del software potrebbero essere in esecuzione nello stesso tempo.

Per evitare questi problemi, valuta di forzare un aggiornamento in sequenza sulle istanze nel gruppo Auto Scaling. Per ulteriori informazioni, consulta [Attributo UpdatePolicy](#).

Modifica delle proprietà delle risorse

Con CloudFormation, puoi modificare le proprietà di una risorsa esistente nello stack. Le seguenti sezioni descrivono vari aggiornamenti che consentono di risolvere problemi specifici; tuttavia, qualsiasi proprietà di qualsiasi risorsa che supporta l'aggiornamento nello stack può essere modificata in base alle esigenze.

Aggiornamento del tipo di istanza

Lo stack che abbiamo creato finora utilizza un'istanza Amazon EC2 t1.micro. Supponiamo che il tuo sito web appena creato stia ricevendo più traffico di quanto possa gestire un'istanza t1.micro e ora desideri passare a un tipo di istanza Amazon m1.small. EC2 Se l'architettura del tipo di istanza cambia, l'istanza verrà creata con un'altra AMI. Se controlli le mappature nel modello, vedrai che sia t1.micro che m1.small hanno le stesse architetture e utilizzano lo stesso Amazon Linux. AMIs

```
"Mappings" : {
  "AWSInstanceType2Arch" : {
    "t1.micro"      : { "Arch" : "HVM64" },
    "t2.nano"      : { "Arch" : "HVM64" },
    "t2.micro"      : { "Arch" : "HVM64" },
    "t2.small"     : { "Arch" : "HVM64" },
    "t2.medium"    : { "Arch" : "HVM64" },
    "t2.large"     : { "Arch" : "HVM64" },
    "m1.small"     : { "Arch" : "HVM64" },
    "m1.medium"    : { "Arch" : "HVM64" },
    "m1.large"     : { "Arch" : "HVM64" },
    "m1.xlarge"    : { "Arch" : "HVM64" },
    "m2.xlarge"    : { "Arch" : "HVM64" },
```

```

    "m2.2xlarge" : { "Arch" : "HVM64" },
    "m2.4xlarge" : { "Arch" : "HVM64" },
    "m3.medium"  : { "Arch" : "HVM64" },
    "m3.large"   : { "Arch" : "HVM64" },
    "m3.xlarge"  : { "Arch" : "HVM64" },
    "m3.2xlarge" : { "Arch" : "HVM64" },
    "m4.large"   : { "Arch" : "HVM64" },
    "m4.xlarge"  : { "Arch" : "HVM64" },
    "m4.2xlarge" : { "Arch" : "HVM64" },
    "m4.4xlarge" : { "Arch" : "HVM64" },
    "m4.10xlarge" : { "Arch" : "HVM64" },
    "c1.medium"  : { "Arch" : "HVM64" },
    "c1.xlarge"  : { "Arch" : "HVM64" },
    "c3.large"   : { "Arch" : "HVM64" },
    "c3.xlarge"  : { "Arch" : "HVM64" },
    "c3.2xlarge" : { "Arch" : "HVM64" },
    "c3.4xlarge" : { "Arch" : "HVM64" },
    "c3.8xlarge" : { "Arch" : "HVM64" },
    "c4.large"   : { "Arch" : "HVM64" },
    "c4.xlarge"  : { "Arch" : "HVM64" },
    "c4.2xlarge" : { "Arch" : "HVM64" },
    "c4.4xlarge" : { "Arch" : "HVM64" },
    "c4.8xlarge" : { "Arch" : "HVM64" },
    "g2.2xlarge" : { "Arch" : "HVMG2" },
    "g2.8xlarge" : { "Arch" : "HVMG2" },
    "r3.large"   : { "Arch" : "HVM64" },
    "r3.xlarge"  : { "Arch" : "HVM64" },
    "r3.2xlarge" : { "Arch" : "HVM64" },
    "r3.4xlarge" : { "Arch" : "HVM64" },
    "r3.8xlarge" : { "Arch" : "HVM64" },
    "i2.xlarge"  : { "Arch" : "HVM64" },
    "i2.2xlarge" : { "Arch" : "HVM64" },
    "i2.4xlarge" : { "Arch" : "HVM64" },
    "i2.8xlarge" : { "Arch" : "HVM64" },
    "d2.xlarge"  : { "Arch" : "HVM64" },
    "d2.2xlarge" : { "Arch" : "HVM64" },
    "d2.4xlarge" : { "Arch" : "HVM64" },
    "d2.8xlarge" : { "Arch" : "HVM64" },
    "hi1.4xlarge" : { "Arch" : "HVM64" },
    "hs1.8xlarge" : { "Arch" : "HVM64" },
    "cr1.8xlarge" : { "Arch" : "HVM64" },
    "cc2.8xlarge" : { "Arch" : "HVM64" }
  },
  "AWSRegionArch2AMI" : {

```

```

    "us-east-1"      : {"HVM64" : "ami-0ff8a91507f77f867", "HVMG2" :
"ami-0a584ac55a7631c0c"},
    "us-west-2"      : {"HVM64" : "ami-a0cfeed8", "HVMG2" :
"ami-0e09505bc235aa82d"},
    "us-west-1"      : {"HVM64" : "ami-0bdb828fd58c52235", "HVMG2" :
"ami-066ee5fd4a9ef77f1"},
    "eu-west-1"      : {"HVM64" : "ami-047bb4163c506cd98", "HVMG2" :
"ami-0a7c483d527806435"},
    "eu-west-2"      : {"HVM64" : "ami-f976839e", "HVMG2" : "NOT_SUPPORTED"},
    "eu-west-3"      : {"HVM64" : "ami-0ebc281c20e89ba4b", "HVMG2" :
"NOT_SUPPORTED"},
    "eu-central-1"    : {"HVM64" : "ami-0233214e13e500f77", "HVMG2" :
"ami-06223d46a6d0661c7"},
    "ap-northeast-1"  : {"HVM64" : "ami-06cd52961ce9f0d85", "HVMG2" :
"ami-053cdd503598e4a9d"},
    "ap-northeast-2"  : {"HVM64" : "ami-0a10b2721688ce9d2", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-northeast-3"  : {"HVM64" : "ami-0d98120a9fb693f07", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-southeast-1"  : {"HVM64" : "ami-08569b978cc4dfa10", "HVMG2" :
"ami-0be9df32ae9f92309"},
    "ap-southeast-2"  : {"HVM64" : "ami-09b42976632b27e9b", "HVMG2" :
"ami-0a9ce9fecc3d1daf8"},
    "ap-south-1"      : {"HVM64" : "ami-0912f71e06545ad88", "HVMG2" :
"ami-097b15e89dbdcfcf4"},
    "us-east-2"      : {"HVM64" : "ami-0b59bfac6be064b78", "HVMG2" :
"NOT_SUPPORTED"},
    "ca-central-1"    : {"HVM64" : "ami-0b18956f", "HVMG2" : "NOT_SUPPORTED"},
    "sa-east-1"      : {"HVM64" : "ami-07b14488da8ea02a0", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-north-1"      : {"HVM64" : "ami-0a4eaf6c4454eda75", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-northwest-1"  : {"HVM64" : "ami-6b6a7d09", "HVMG2" : "NOT_SUPPORTED"}
}

```

Usiamo il modello che abbiamo modificato nella sezione precedente per modificare il tipo di istanza. Poiché InstanceType era un parametro di input per il modello, non è necessario modificare il modello; possiamo modificare il valore del parametro nella procedura guidata Stack Update, nella pagina Specificare i parametri.

Per aggiornare lo stack dalla AWS Management Console

1. [Accedi alla CloudFormation console all'indirizzo `https://console.aws.amazon.com/cloudformation`.](https://console.aws.amazon.com/cloudformation)
2. Nella CloudFormation dashboard, scegli lo stack che hai creato in precedenza, quindi scegli Update Stack.
3. Nella procedura guidata Update Stack (Aggiorna stack), nella schermata Select Template (Seleziona modello) selezionare Use current template (Utilizza modello corrente), quindi selezionare Next (Avanti).

Viene visualizzata la pagina Specify Details (Specifica dettagli) con i parametri utilizzati per creare lo stack iniziale precompilati nella sezione Specify Parameters (Specifica parametri).

4. Modifica il valore della casella di InstanceType da `t1.micro` a `m1.small`. Quindi, seleziona Next (Successivo).
5. Nella schermata Options (Opzioni) selezionare Next (Avanti).
6. Selezionare Next (Avanti) perché lo stack non dispone di una policy di stack. Tutte le risorse possono essere aggiornate senza una policy di sostituzione.
7. Nella schermata Review (Rivedi) verificare che tutte le impostazioni siano quelle desiderate, quindi selezionare Update (Aggiorna).

Puoi modificare dinamicamente il tipo di istanza di un'istanza EC2 Amazon supportata da EBS avviando e arrestando l'istanza. CloudFormation tenta di ottimizzare la modifica aggiornando il tipo di istanza e riavviando l'istanza, in modo che l'ID dell'istanza non cambi. Quando l'istanza viene riavviata, tuttavia, l'indirizzo IP pubblico dell'istanza cambia. Per garantire che l'indirizzo IP elastico sia associato correttamente dopo la modifica, CloudFormation aggiornerà anche l'indirizzo IP elastico. Puoi vedere le modifiche nella CloudFormation console nella scheda Eventi.

Per verificare il tipo di istanza da AWS Management Console, apri la EC2 console Amazon e individua l'istanza lì.

Aggiorna l'AMI su un' EC2 istanza Amazon

Vediamo ora in che modo è possibile modificare l'Amazon Machine Image (AMI) in esecuzione nell'istanza. Inizieremo la modifica dell'AMI aggiornando lo stack per utilizzare un nuovo tipo di EC2 istanza Amazon, come `t2.medium`, che è un tipo di istanza. HVM64

Come nella sezione precedente, utilizzeremo il modello esistente per cambiare il tipo di istanza utilizzato dallo stack di esempio. Nella pagina Specify Parameters (Specifica parametri) della procedura guidata di aggiornamento dello stack, modifica il valore del tipo di istanza.

In questo caso, non possiamo semplicemente avviare e arrestare l'istanza per modificare l'AMI; CloudFormation considera questa operazione una modifica a una proprietà non modificabile della risorsa. Per apportare una modifica a una proprietà immutabile, è CloudFormation necessario avviare una risorsa sostitutiva, in questo caso una nuova EC2 istanza Amazon che esegue la nuova AMI.

Dopo l'esecuzione della nuova istanza, CloudFormation aggiorna le altre risorse dello stack in modo che puntino alla nuova risorsa. Quando vengono create tutte le nuove risorse, la vecchia risorsa viene eliminata, un processo noto come UPDATE_CLEANUP. Questa volta noterai che l'ID istanza e l'URL applicazione dell'istanza nello stack sono cambiati in conseguenza dell'aggiornamento. Gli eventi nella tabella Event (Evento) contengono una descrizione indicante che l'aggiornamento richiesto implicava la modifica di una proprietà non modificabile e pertanto è stata creata una nuova risorsa fisica, con sostituzione della precedente.

Se disponi di codice applicativo scritto nell'AMI e vuoi aggiornarlo, puoi utilizzare lo stesso meccanismo di aggiornamento dello stack per aggiornare l'AMI in modo che carichi la nuova applicazione.

Per aggiornare l'AMI per un'istanza nello stack

1. Creare una nuova AMI contenente le modifiche all'applicazione o al sistema operativo. Per ulteriori informazioni, consulta la sezione [Creazione di un'AMI supportata da Amazon EBS nella Amazon User Guide](#). EC2
2. Aggiorna il modello per incorporare la nuova AMI IDs.
3. Aggiorna lo stack, AWS Management Console come spiegato in [Aggiornamento dell'applicazione](#) o utilizzando il AWS comando [update-stack](#).

Quando aggiorni lo stack, CloudFormation rileva che l'ID AMI è cambiato e quindi attiva un aggiornamento dello stack nello stesso modo in cui abbiamo avviato quello precedente.

Aggiorna la configurazione di EC2 lancio di Amazon per un gruppo Auto Scaling

Se utilizzi gruppi di Auto Scaling anziché EC2 istanze Amazon, il processo di aggiornamento delle istanze in esecuzione è leggermente diverso. Con le risorse Auto Scaling, la configurazione delle EC2 istanze Amazon, come il tipo di istanza o l'ID AMI, è incapsulata nella configurazione di avvio di

Auto Scaling. Puoi apportare modifiche alla configurazione di avvio nello stesso modo in cui abbiamo apportato modifiche alle risorse delle EC2 istanze Amazon nelle sezioni precedenti. Tuttavia, la modifica della configurazione di avvio non ha alcun impatto sulle EC2 istanze Amazon in esecuzione nel gruppo Auto Scaling. Una configurazione di avvio aggiornata si applica solo alle nuove istanze che vengono create dopo l'aggiornamento.

Per propagare le modifiche alla configurazione di avvio a tutte le istanze nel gruppo Auto Scaling, puoi utilizzare un attributo di aggiornamento. Per ulteriori informazioni, consulta [Attributo UpdatePolicy](#).

Aggiunta di proprietà delle risorse

Finora abbiamo esaminato la modifica di proprietà esistenti di una risorsa in un modello. È possibile anche aggiungere proprietà che non sono state originariamente specificate nel modello. Per illustrare ciò, aggiungeremo una coppia di EC2 chiavi Amazon a un' EC2 istanza esistente e quindi apriremo la porta 22 nell'Amazon EC2 Security Group in modo da poter utilizzare Secure Shell (SSH) per accedere all'istanza.

Aggiunta di una coppia di chiavi a un'istanza

Per aggiungere l'accesso SSH a un'istanza Amazon EC2 esistente

1. Aggiungi due parametri aggiuntivi al modello per inserire il nome di una coppia di EC2 chiavi Amazon esistente e di una posizione SSH.

```
"Parameters" : {

    "KeyName" : {
        "Description" : "Name of an existing Amazon EC2 key pair for SSH access",
        "Type": "AWS::EC2::KeyPair::KeyName"
    },
    "SSHLocation" : {
        "Description" : " The IP address range that can be used to SSH to the EC2
instances",
        "Type": "String",
        "MinLength": "9",
        "MaxLength": "18",
        "Default": "0.0.0.0/0",
        "AllowedPattern": "((\\d{1,3})\\.\\.\\.\\.((\\d{1,3})\\.\\.\\.\\.((\\d{1,3})\\.\\.\\.\\.((\\d{1,3})/\\d{1,2})|\\d{1,2})|\\d{1,2})|\\d{1,2})|\\d{1,2})|\\d{1,2})/\\d{1,2})",
        "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x.x."
    }
}
```

```

    }
    :
  },

```

2. Aggiungi la KeyName proprietà all' EC2 istanza Amazon.

```

    "WebServerInstance": {
      "Type" : "AWS::EC2::Instance",
      :
      "Properties": {
        :
        "KeyName" : { "Ref" : "KeyName" },
        :
      }
    },

```

3. Aggiungi la porta 22 e la posizione SSH alle regole di ingresso per il gruppo di EC2 sicurezza Amazon.

```

    "WebServerSecurityGroup" : {
      "Type" : "AWS::EC2::SecurityGroup",
      "Properties" : {
        "GroupDescription" : "Enable HTTP and SSH",
        "SecurityGroupIngress" : [
          { "IpProtocol" : "tcp", "FromPort" : "22", "ToPort" : "22", "CidrIp" :
{ "Ref" : "SSHLocation" } },
          { "IpProtocol" : "tcp", "FromPort" : "80", "ToPort" : "80", "CidrIp" :
"0.0.0.0/0" }
        ]
      }
    },

```

4. Aggiorna lo stack, AWS Management Console come spiegato in [Aggiornamento dell'applicazione](#) o utilizzando il comando. AWS [update-stack](#)

Modifica delle risorse dello stack

Le esigenze dell'applicazione possono cambiare nel tempo, CloudFormation consente di modificare l'insieme di risorse che compongono lo stack. Per la dimostrazione utilizzeremo l'applicazione a istanza singola da [Aggiunta di proprietà delle risorse](#) e la convertiremo in un'applicazione con load balancer e ridimensionamento automatico tramite l'aggiornamento dello stack.

In questo modo verrà creata un'applicazione PHP semplice, a istanza singola, che utilizza un indirizzo IP elastico. Ora trasformeremo l'applicazione in un'applicazione ad alta disponibilità, con load balancer e ridimensionamento automatico tramite la modifica delle risorse durante un aggiornamento.

1. Aggiungere una risorsa Elastic Load Balancer.

```
"ElasticLoadBalancer" : {
  "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
  "Properties" : {
    "CrossZone" : "true",
    "AvailabilityZones" : { "Fn::GetAZs" : "" },
    "LBCookieStickinessPolicy" : [ {
      "PolicyName" : "CookieBasedPolicy",
      "CookieExpirationPeriod" : "30"
    } ],
    "Listeners" : [ {
      "LoadBalancerPort" : "80",
      "InstancePort" : "80",
      "Protocol" : "HTTP",
      "PolicyNames" : [ "CookieBasedPolicy" ]
    } ],
    "HealthCheck" : {
      "Target" : "HTTP:80/",
      "HealthyThreshold" : "2",
      "UnhealthyThreshold" : "5",
      "Interval" : "10",
      "Timeout" : "5"
    }
  }
}
```

2. Converti l' EC2 istanza nel modello in una configurazione di avvio con Auto Scaling. Le proprietà sono identiche, perciò è necessario solo cambiare il nome del tipo da:

```
"WebServerInstance": {
  "Type" : "AWS::EC2::Instance",
```

to:


```
"LaunchConfig": {
  "Type" : "AWS::AutoScaling::LaunchConfiguration",
```

Per chiarezza nel modello, abbiamo cambiato il nome della risorsa da `WebServerInstance` a `LaunchConfig`, quindi dovrai aggiornare il nome della risorsa a cui fanno riferimento `cfn-init` e `cfn-hup` (basta cercarlo `WebServerInstance` e sostituirlo con, ad eccezione di `cfn-signal`). `LaunchConfig` Per `cfn-signal`, dovrai segnalare il gruppo Auto Scaling `WebServerGroup` () e non l'istanza, come mostrato nel seguente frammento:

```
"# Signal the status from cfn-init\n",
"/opt/aws/bin/cfn-signal -e $? ",
"      --stack ", { "Ref" : "AWS::StackName" },
"      --resource WebServerGroup ",
"      --region ", { "Ref" : "AWS::Region" }, "\n"
```

3. Aggiungi una risorsa del gruppo con scalabilità automatica.

```
"WebServerGroup" : {
  "Type" : "AWS::AutoScaling::AutoScalingGroup",
  "Properties" : {
    "AvailabilityZones" : { "Fn::GetAZs" : "" },
    "LaunchConfigurationName" : { "Ref" : "LaunchConfig" },
    "MinSize" : "1",
    "DesiredCapacity" : "1",
    "MaxSize" : "5",
    "LoadBalancerNames" : [ { "Ref" : "ElasticLoadBalancer" } ]
  },
  "CreationPolicy" : {
    "ResourceSignal" : {
      "Timeout" : "PT15M"
    }
  },
  "UpdatePolicy": {
    "AutoScalingRollingUpdate": {
      "MinInstancesInService": "1",
      "MaxBatchSize": "1",
      "PauseTime" : "PT15M",
      "WaitOnResourceSignals": "true"
    }
  }
}
```

4. Aggiornare la definizione del gruppo di sicurezza per bloccare il traffico verso le istanze dal load balancer.

```
"WebServerSecurityGroup" : {
  "Type" : "AWS::EC2::SecurityGroup",
  "Properties" : {
    "GroupDescription" : "Enable HTTP access via port 80 locked down to the ELB
and SSH access",
    "SecurityGroupIngress" : [
      {"IpProtocol" : "tcp", "FromPort" : "80", "ToPort" : "80",
"SourceSecurityGroupOwnerId" : {"Fn::GetAtt" : ["ElasticLoadBalancer",
"SourceSecurityGroup.OwnerAlias"]},
"SourceSecurityGroupName" : {"Fn::GetAtt" : ["ElasticLoadBalancer",
"SourceSecurityGroup.GroupName"]},
      {"IpProtocol" : "tcp", "FromPort" : "22", "ToPort" : "22", "CidrIp" :
{ "Ref" : "SSHLocation"}}
    ]
  }
}
```

5. Aggiornare gli output in modo da restituire il nome DNS dell'Elastic Load Balancer come percorso dell'applicazione da:

```
"WebsiteURL" : {
  "Value" : { "Fn::Join" : [ "", [ "http://",
    { "Fn::GetAtt" : [ "WebServerInstance", "PublicDnsName" ] } ] ] },
  "Description" : "Application URL"
}
```

to:

```
"WebsiteURL" : {
  "Value" : { "Fn::Join" : [ "", [ "http://",
    { "Fn::GetAtt" : [ "ElasticLoadBalancer", "DNSName" ] } ] ] },
  "Description" : "Application URL"
}
```

Per riferimento, l'esempio seguente mostra il modello completo. Se utilizzi questo modello per aggiornare lo stack, convertirai la semplice applicazione a istanza singola in un'applicazione ad

alta disponibilità, Multi-AZ, con load balancer e dimensionamento automatico. Solo le risorse che devono essere aggiornate verranno modificate, perciò se fossero stati presenti datastore per quest'applicazione, i dati sarebbero rimasti intatti. Ora puoi utilizzarlo CloudFormation per aumentare o migliorare i tuoi stack man mano che le tue esigenze cambiano.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS CloudFormation Sample Template: Sample template that can be used
to test EC2 updates. **WARNING** This template creates an Amazon Ec2 Instance. You
will be billed for the AWS resources used if you create a stack from this template.",

  "Parameters" : {

    "KeyName": {
      "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the
instance",
      "Type": "AWS::EC2::KeyPair::KeyName",
      "ConstraintDescription" : "must be the name of an existing EC2 KeyPair."
    },

    "SSHLocation" : {
      "Description" : " The IP address range that can be used to SSH to the EC2
instances",
      "Type": "String",
      "MinLength": "9",
      "MaxLength": "18",
      "Default": "0.0.0.0/0",
      "AllowedPattern": "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})/(\\d{1,2})",
      "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
    },

    "InstanceType" : {
      "Description" : "WebServer EC2 instance type",
      "Type" : "String",
      "Default" : "t2.small",
      "AllowedValues" : [
        "t1.micro",
        "t2.nano",
        "t2.micro",
        "t2.small",
        "t2.medium",
        "t2.large",
```

```
"m1.small",
"m1.medium",
"m1.large",
"m1.xlarge",
"m2.xlarge",
"m2.2xlarge",
"m2.4xlarge",
"m3.medium",
"m3.large",
"m3.xlarge",
"m3.2xlarge",
"m4.large",
"m4.xlarge",
"m4.2xlarge",
"m4.4xlarge",
"m4.10xlarge",
"c1.medium",
"c1.xlarge",
"c3.large",
"c3.xlarge",
"c3.2xlarge",
"c3.4xlarge",
"c3.8xlarge",
"c4.large",
"c4.xlarge",
"c4.2xlarge",
"c4.4xlarge",
"c4.8xlarge",
"g2.2xlarge",
"g2.8xlarge",
"r3.large",
"r3.xlarge",
"r3.2xlarge",
"r3.4xlarge",
"r3.8xlarge",
"i2.xlarge",
"i2.2xlarge",
"i2.4xlarge",
"i2.8xlarge",
"d2.xlarge",
"d2.2xlarge",
"d2.4xlarge",
"d2.8xlarge",
"hi1.4xlarge",
```

```

        "hs1.8xlarge",
        "cr1.8xlarge",
        "cc2.8xlarge",
        "cg1.4xlarge"
    ],
    "ConstraintDescription" : "must be a valid EC2 instance type."
}
},

"Mappings" : {
    "AWSInstanceType2Arch" : {
        "t1.micro"      : { "Arch" : "HVM64" },
        "t2.nano"      : { "Arch" : "HVM64" },
        "t2.micro"      : { "Arch" : "HVM64" },
        "t2.small"     : { "Arch" : "HVM64" },
        "t2.medium"    : { "Arch" : "HVM64" },
        "t2.large"     : { "Arch" : "HVM64" },
        "m1.small"     : { "Arch" : "HVM64" },
        "m1.medium"    : { "Arch" : "HVM64" },
        "m1.large"     : { "Arch" : "HVM64" },
        "m1.xlarge"    : { "Arch" : "HVM64" },
        "m2.xlarge"    : { "Arch" : "HVM64" },
        "m2.2xlarge"   : { "Arch" : "HVM64" },
        "m2.4xlarge"   : { "Arch" : "HVM64" },
        "m3.medium"    : { "Arch" : "HVM64" },
        "m3.large"     : { "Arch" : "HVM64" },
        "m3.xlarge"    : { "Arch" : "HVM64" },
        "m3.2xlarge"   : { "Arch" : "HVM64" },
        "m4.large"     : { "Arch" : "HVM64" },
        "m4.xlarge"    : { "Arch" : "HVM64" },
        "m4.2xlarge"   : { "Arch" : "HVM64" },
        "m4.4xlarge"   : { "Arch" : "HVM64" },
        "m4.10xlarge"  : { "Arch" : "HVM64" },
        "c1.medium"    : { "Arch" : "HVM64" },
        "c1.xlarge"    : { "Arch" : "HVM64" },
        "c3.large"     : { "Arch" : "HVM64" },
        "c3.xlarge"    : { "Arch" : "HVM64" },
        "c3.2xlarge"   : { "Arch" : "HVM64" },
        "c3.4xlarge"   : { "Arch" : "HVM64" },
        "c3.8xlarge"   : { "Arch" : "HVM64" },
        "c4.large"     : { "Arch" : "HVM64" },
        "c4.xlarge"    : { "Arch" : "HVM64" },
        "c4.2xlarge"   : { "Arch" : "HVM64" },
        "c4.4xlarge"   : { "Arch" : "HVM64" },
    },

```

```

    "c4.8xlarge" : { "Arch" : "HVM64" },
    "g2.2xlarge" : { "Arch" : "HVMG2" },
    "g2.8xlarge" : { "Arch" : "HVMG2" },
    "r3.large" : { "Arch" : "HVM64" },
    "r3.xlarge" : { "Arch" : "HVM64" },
    "r3.2xlarge" : { "Arch" : "HVM64" },
    "r3.4xlarge" : { "Arch" : "HVM64" },
    "r3.8xlarge" : { "Arch" : "HVM64" },
    "i2.xlarge" : { "Arch" : "HVM64" },
    "i2.2xlarge" : { "Arch" : "HVM64" },
    "i2.4xlarge" : { "Arch" : "HVM64" },
    "i2.8xlarge" : { "Arch" : "HVM64" },
    "d2.xlarge" : { "Arch" : "HVM64" },
    "d2.2xlarge" : { "Arch" : "HVM64" },
    "d2.4xlarge" : { "Arch" : "HVM64" },
    "d2.8xlarge" : { "Arch" : "HVM64" },
    "hi1.4xlarge" : { "Arch" : "HVM64" },
    "hs1.8xlarge" : { "Arch" : "HVM64" },
    "cr1.8xlarge" : { "Arch" : "HVM64" },
    "cc2.8xlarge" : { "Arch" : "HVM64" }
  },
  "AWSRegionArch2AMI" : {
    "us-east-1" : { "HVM64" : "ami-0ff8a91507f77f867", "HVMG2" :
"ami-0a584ac55a7631c0c"},
    "us-west-2" : { "HVM64" : "ami-a0cfeed8", "HVMG2" :
"ami-0e09505bc235aa82d"},
    "us-west-1" : { "HVM64" : "ami-0bdb828fd58c52235", "HVMG2" :
"ami-066ee5fd4a9ef77f1"},
    "eu-west-1" : { "HVM64" : "ami-047bb4163c506cd98", "HVMG2" :
"ami-0a7c483d527806435"},
    "eu-west-2" : { "HVM64" : "ami-f976839e", "HVMG2" : "NOT_SUPPORTED"},
    "eu-west-3" : { "HVM64" : "ami-0ebc281c20e89ba4b", "HVMG2" :
"NOT_SUPPORTED"},
    "eu-central-1" : { "HVM64" : "ami-0233214e13e500f77", "HVMG2" :
"ami-06223d46a6d0661c7"},
    "ap-northeast-1" : { "HVM64" : "ami-06cd52961ce9f0d85", "HVMG2" :
"ami-053cdd503598e4a9d"},
    "ap-northeast-2" : { "HVM64" : "ami-0a10b2721688ce9d2", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-northeast-3" : { "HVM64" : "ami-0d98120a9fb693f07", "HVMG2" :
"NOT_SUPPORTED"},
    "ap-southeast-1" : { "HVM64" : "ami-08569b978cc4dfa10", "HVMG2" :
"ami-0be9df32ae9f92309"},

```

```

    "ap-southeast-2" : {"HVM64" : "ami-09b42976632b27e9b", "HVMG2" :
"ami-0a9ce9fecc3d1daf8"},
    "ap-south-1" : {"HVM64" : "ami-0912f71e06545ad88", "HVMG2" :
"ami-097b15e89dbdcfcf4"},
    "us-east-2" : {"HVM64" : "ami-0b59bfac6be064b78", "HVMG2" :
"NOT_SUPPORTED"},
    "ca-central-1" : {"HVM64" : "ami-0b18956f", "HVMG2" : "NOT_SUPPORTED"},
    "sa-east-1" : {"HVM64" : "ami-07b14488da8ea02a0", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-north-1" : {"HVM64" : "ami-0a4eaf6c4454eda75", "HVMG2" :
"NOT_SUPPORTED"},
    "cn-northwest-1" : {"HVM64" : "ami-6b6a7d09", "HVMG2" : "NOT_SUPPORTED"}
  }
},

"Resources" : {

  "ElasticLoadBalancer" : {
    "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
    "Properties" : {
      "CrossZone" : "true",
      "AvailabilityZones" : { "Fn::GetAZs" : "" },
      "LBCookieStickinessPolicy" : [ {
        "PolicyName" : "CookieBasedPolicy",
        "CookieExpirationPeriod" : "30"
      } ],
      "Listeners" : [ {
        "LoadBalancerPort" : "80",
        "InstancePort" : "80",
        "Protocol" : "HTTP",
        "PolicyNames" : [ "CookieBasedPolicy" ]
      } ],
      "HealthCheck" : {
        "Target" : "HTTP:80/",
        "HealthyThreshold" : "2",
        "UnhealthyThreshold" : "5",
        "Interval" : "10",
        "Timeout" : "5"
      }
    ]
  },

  "WebServerGroup" : {
    "Type" : "AWS::AutoScaling::AutoScalingGroup",

```

```

"Properties" : {
  "AvailabilityZones" : { "Fn::GetAZs" : "" },
  "LaunchConfigurationName" : { "Ref" : "LaunchConfig" },
  "MinSize" : "1",
  "DesiredCapacity" : "1",
  "MaxSize" : "5",
  "LoadBalancerNames" : [ { "Ref" : "ElasticLoadBalancer" } ]
},
"CreationPolicy" : {
  "ResourceSignal" : {
    "Timeout" : "PT15M"
  }
},
"UpdatePolicy": {
  "AutoScalingRollingUpdate": {
    "MinInstancesInService": "1",
    "MaxBatchSize": "1",
    "PauseTime" : "PT15M",
    "WaitOnResourceSignals": "true"
  }
}
},

"LaunchConfig": {
  "Type" : "AWS::AutoScaling::LaunchConfiguration",
  "Metadata" : {
    "Comment" : "Install a simple PHP application",
    "AWS::CloudFormation::Init" : {
      "config" : {
        "packages" : {
          "yum" : {
            "httpd" : [],
            "php" : []
          }
        }
      },
      "files" : {

        "/var/www/html/index.php" : {
          "content" : { "Fn::Join" : [ "", [
            "<?php\n",
            "echo '<h1>AWS CloudFormation sample PHP application</h1>';\n",
            "echo 'Updated version via UpdateStack';\n ",
            "?>\n"
          ] ] }
        }
      }
    }
  }
}

```



```

    ]}},
    "mode"      : "000644",
    "owner"     : "apache",
    "group"     : "apache"
  },

  "/etc/cfn/cfn-hup.conf" : {
    "content" : { "Fn::Join" : ["", [
      "[main]\n",
      "stack=", { "Ref" : "AWS::StackId" }, "\n",
      "region=", { "Ref" : "AWS::Region" }, "\n"
    ]}},
    "mode"      : "000400",
    "owner"     : "root",
    "group"     : "root"
  },

  "/etc/cfn/hooks.d/cfn-auto-reloader.conf" : {
    "content": { "Fn::Join" : ["", [
      "[cfn-auto-reloader-hook]\n",
      "triggers=post.update\n",
      "path=Resources.LaunchConfig.Metadata.AWS::CloudFormation::Init\n",
      "action=/opt/aws/bin/cfn-init -s ", { "Ref" : "AWS::StackId" }, " -r
LaunchConfig ",
                                     " --region      ", { "Ref" :
"AWS::Region" }, "\n",
      "runas=root\n"
    ]}}
  }
},

"services" : {
  "sysvinit" : {
    "httpd"      : { "enabled" : "true", "ensureRunning" : "true" },
    "cfn-hup"    : { "enabled" : "true", "ensureRunning" : "true",
      "files" : ["/etc/cfn/cfn-hup.conf", "/etc/cfn/hooks.d/cfn-auto-
reloader.conf"]}
  }
}
}
}
},

```

```

    "Properties": {
      "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" :
"AWS::Region" },
                                { "Fn::FindInMap" : [ "AWSInstanceType2Arch", { "Ref" :
"InstanceType" }, "Arch" ] } ] },
      "InstanceType" : { "Ref" : "InstanceType" },
      "KeyName" : { "Ref" : "KeyName" },
      "SecurityGroups" : [ {"Ref" : "WebServerSecurityGroup"} ],
      "UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [
        "#!/bin/bash -xe\n",
        "yum install -y aws-cfn-bootstrap\n",

        "# Install the files and packages from the metadata\n",
        "/opt/aws/bin/cfn-init -v ",
        "      --stack ", { "Ref" : "AWS::StackName" },
        "      --resource LaunchConfig ",
        "      --region ", { "Ref" : "AWS::Region" }, "\n",

        "# Start up the cfn-hup daemon to listen for changes to the Web Server
metadata\n",
        "/opt/aws/bin/cfn-hup || error_exit 'Failed to start cfn-hup'\n",

        "# Signal the status from cfn-init\n",
        "/opt/aws/bin/cfn-signal -e $? ",
        "      --stack ", { "Ref" : "AWS::StackName" },
        "      --resource WebServerGroup ",
        "      --region ", { "Ref" : "AWS::Region" }, "\n"
      ] ] ] }
    }
  },

  "WebServerSecurityGroup" : {
    "Type" : "AWS::EC2::SecurityGroup",
    "Properties" : {
      "GroupDescription" : "Enable HTTP access via port 80 locked down to the ELB and
SSH access",
      "SecurityGroupIngress" : [
        { "IpProtocol" : "tcp", "FromPort" : "80", "ToPort" : "80",
"SourceSecurityGroupOwnerId" : { "Fn::GetAtt" : ["ElasticLoadBalancer",
"SourceSecurityGroup.OwnerAlias"] }, "SourceSecurityGroupName" : { "Fn::GetAtt" :
["ElasticLoadBalancer", "SourceSecurityGroup.GroupName"] } },
        { "IpProtocol" : "tcp", "FromPort" : "22", "ToPort" : "22", "CidrIp" :
{ "Ref" : "SSHLocation" } }
      ]
    }
  }
}

```

```
    }  
  }  
},  
  
"Outputs" : {  
  "WebsiteURL" : {  
    "Description" : "Application URL",  
    "Value" : { "Fn::Join" : [ "", [ "http://", { "Fn::GetAtt" :  
[ "ElasticLoadBalancer", "DNSName" ] } ] ] }  
  }  
}
```

Considerazioni su disponibilità e impatto

Diverse proprietà hanno diverso impatto sulle risorse nello stack. È possibile utilizzare CloudFormation per aggiornare qualsiasi proprietà; tuttavia, prima di apportare modifiche, è opportuno considerare le seguenti domande:

1. In che modo l'aggiornamento influisce sulla risorsa stessa? Ad esempio, l'aggiornamento di una soglia di allarme renderà l'allarme inattivo durante l'aggiornamento. Come abbiamo visto, la modifica del tipo di istanza richiede l'arresto e il riavvio dell'istanza. CloudFormation utilizza le azioni di aggiornamento o modifica delle risorse sottostanti per apportare modifiche alle risorse. Per comprendere l'impatto degli aggiornamenti, è necessario verificare la documentazione delle risorse specifiche.
2. La modifica è modificabile o non modificabile? Alcune modifiche alle proprietà delle risorse, come la modifica dell'AMI su un' EC2 istanza Amazon, non sono supportate dai servizi sottostanti. In caso di modifiche modificabili, CloudFormation utilizzerà il tipo Update o Modify APIs per le risorse sottostanti. Per le modifiche immutabili alle proprietà, CloudFormation creerà nuove risorse con le proprietà aggiornate e quindi le collegherà allo stack prima di eliminare le vecchie risorse. Sebbene CloudFormation cerchi di ridurre i tempi di inattività delle risorse dello stack, la sostituzione di una risorsa è un processo in più fasi e richiederà tempo. Durante la riconfigurazione dello stack, l'applicazione non sarà completamente operativa. Ad esempio, potrebbe non essere in grado di servire richieste o accedere a un database.

Risorse correlate

Per ulteriori informazioni sull'utilizzo CloudFormation per avviare le applicazioni e sull'integrazione con altri servizi di configurazione e distribuzione come Puppet e Opscode Chef, consulta i seguenti white paper:

- [Avvio delle applicazioni tramite CloudFormation](#)
- [Integrazione con Opscode Chef CloudFormation](#)
- [Integrazione con Puppet CloudFormation](#)

Il modello utilizzato in questa sezione è un'applicazione PHP "Hello World". La libreria di modelli dispone anche di un modello di ElastiCache esempio Amazon che mostra come integrare un'applicazione PHP ElastiCache utilizzando cfn-hup e cfn-init per rispondere alle modifiche nella configurazione di Amazon ElastiCache Cache Cluster, tutte operazioni che possono essere eseguite da Update Stack.

Esegui blue/green implementazioni ECS tramite l'utilizzo CodeDeploy CloudFormation

Per aggiornare un'applicazione in esecuzione su Amazon Elastic Container Service (Amazon ECS), puoi utilizzare CodeDeploy una strategia di distribuzione blu/verde. Questa strategia aiuta a ridurre al minimo le interruzioni causate dalla modifica delle versioni delle applicazioni.

In una blue/green distribuzione, si crea un nuovo ambiente applicativo (denominato verde) accanto all'ambiente live corrente (denominato blu). Ciò consente di monitorare e testare l'ambiente verde prima di indirizzare il traffico in tempo reale dall'ambiente blu all'ambiente verde. Dopo che l'ambiente verde ha fornito traffico in tempo reale, puoi terminare in sicurezza l'ambiente blu.

Per eseguire distribuzioni CodeDeploy blu/verdi su ECS utilizzando CloudFormation, includi le seguenti informazioni nel modello di stack:

- Una sezione che descrive un hookHooks. `AWS::CodeDeploy::BlueGreen`
- Una Transform sezione che specifica la `AWS::CodeDeployBlueGreen` trasformazione.

I seguenti argomenti guidano l'utente nella configurazione di un CloudFormation modello per una distribuzione blu/verde su ECS.

Argomenti

- [Informazioni sulle blue/green distribuzioni](#)
- [Considerazioni sulla gestione delle distribuzioni blue/green di ECS utilizzando CloudFormation](#)
- [AWS::CodeDeploy::BlueGreensintassi hook](#)
- [Esempio di modello di implementazione blu/verde](#)

Informazioni sulle blue/green distribuzioni

Questo argomento fornisce una panoramica di come funziona l'esecuzione blue/green delle distribuzioni con CloudFormation. Spiega inoltre come preparare il CloudFormation modello per le distribuzioni blu/verdi.

Argomenti

- [Come funziona](#)
- [Aggiornamenti delle risorse che avviano implementazioni ecologiche](#)
- [Preparazione del modello per l'esecuzione di distribuzioni blu/verde di ECS](#)
- [Modellazione della distribuzione utilizzando le risorse blue/green CloudFormation](#)
- [Set di modifiche](#)
- [Monitoraggio degli eventi dello stack](#)
- [Autorizzazioni IAM per le distribuzioni blue/green](#)

Come funziona

Quando si utilizza CloudFormation per eseguire blue/green distribuzioni ECS tramite CodeDeploy, si inizia con la creazione di un modello di stack che definisce le risorse per gli ambienti applicativi blu e verdi, inclusa la specificazione delle impostazioni di routing e stabilizzazione del traffico da utilizzare. Successivamente, crei uno stack a partire da quel modello. Questo genera la tua applicazione blu (corrente). CloudFormation crea le risorse blu solo durante la creazione dello stack. Le risorse per una distribuzione verde non vengono create finché non sono necessarie.

Quindi, se in un futuro aggiornamento dello stack aggiorni la definizione dell'attività o le risorse del set di attività nell'applicazione blu, CloudFormation effettua le seguenti operazioni:

- Genera tutte le risorse necessarie per l'ambiente delle applicazioni verdi
- Sposta il traffico in base ai parametri di instradamento del traffico specificati

- Elimina le risorse blu

Se si verifica un errore in qualsiasi momento prima che la distribuzione verde abbia esito positivo e sia finalizzata, CloudFormation ripristina lo stack allo stato precedente all'avvio dell'intera distribuzione verde.

Aggiornamenti delle risorse che avviano implementazioni ecologiche

Quando si esegue un aggiornamento dello stack che aggiorna determinate proprietà di risorse ECS specifiche, CloudFormation avvia un processo di distribuzione ecologico. Le risorse che avviano questo processo sono:

- [AWS::ECS::TaskDefinition](#)
- [AWS::ECS::TaskSet](#)

Tuttavia, se gli aggiornamenti a queste risorse non comportano modifiche alle proprietà che richiedono la sostituzione, non verrà avviata una distribuzione ecologica. Per ulteriori informazioni, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

È importante notare che non è possibile combinare gli aggiornamenti delle risorse di cui sopra con gli aggiornamenti di altre risorse nella stessa operazione di aggiornamento dello stack. Se devi aggiornare sia le risorse elencate che altre risorse all'interno dello stesso stack, hai due opzioni:

- Eseguire due operazioni di aggiornamento separate: una che include solo gli aggiornamenti delle risorse precedenti e un aggiornamento separato dello stack che include le modifiche apportate a qualsiasi altra risorsa.
- Rimuovi le sezioni `Transform` e `Hooks` dal modello e quindi esegui l'aggiornamento dello stack. In questo caso, CloudFormation non eseguirà una distribuzione ecologica.

Preparazione del modello per l'esecuzione di distribuzioni blu/verde di ECS

Per abilitare le blue/green distribuzioni sul tuo stack, includi le seguenti sezioni nel tuo modello di stack prima di eseguire un aggiornamento dello stack.

- Aggiungi un riferimento alla trasformazione `AWS::CodeDeployBlueGreen` al tuo modello:

```
"Transform": [  
  "AWS::CodeDeployBlueGreen"
```

```
],
```

- Aggiungi una sezione `Hooks` che richiami l'hook `AWS::CodeDeploy::BlueGreen` e specifica le proprietà per la distribuzione. Per ulteriori informazioni, consulta [AWS::CodeDeploy::BlueGreensintassi hook](#).
- Nella sezione `Resources`, definisci le risorse blu e verdi per la distribuzione.

È possibile aggiungere queste sezioni quando si crea il modello per la prima volta o prima di creare lo stack medesimo; oppure è possibile aggiungerle a un modello esistente prima di eseguire un aggiornamento dello stack. Se specifichi la blue/green distribuzione per un nuovo stack, crea CloudFormation solo le risorse blu durante la creazione dello stack. Le risorse per la distribuzione verde non vengono create finché non sono necessarie durante un aggiornamento dello stack.

Modellazione della distribuzione utilizzando le risorse blue/green CloudFormation

Per eseguire una distribuzione CodeDeploy blu/verde su ECS, il CloudFormation modello deve includere le risorse che modellano la distribuzione, come un servizio Amazon ECS e un sistema di bilanciamento del carico. Per ulteriori dettagli su cosa rappresentano queste risorse, consulta [Prima di iniziare una distribuzione Amazon ECS](#) nella Guida per l'utente di AWS CodeDeploy .

Requisito	Risorsa	Obbligatorio/facoltativo	Avvia la distribuzione in caso di sostituzione? blue/green
Cluster Amazon ECS	AWS::ECS::Cluster	Facoltativo. Puoi utilizzare il cluster predefinito.	No
Servizio Amazon ECS	AWS::ECS::Service	Obbligatorio.	No
Applicazione o Network Load Balancer	AWS::ECS::ServiceLoadBalancer	Obbligatorio.	No
Listener di produzione	AWS::ElasticLoadBalancingV2::Listener	Obbligatorio.	No

Requisito	Risorsa	Obbligatorio/facoltativo	Avvia la distribuzione in caso di sostituzione? blue/green
Listener di prova	AWS::ElasticLoadBalancingV2::Listener	Facoltativo.	No
Due gruppi target	AWS::ElasticLoadBalancingV2::TargetGroup	Obbligatorio.	No
Definizione dell'attività di Amazon ECS	AWS::ECS::TaskDefinition	Obbligatorio.	Sì
Container per l'applicazione Amazon ECS	AWS::ECS::TaskDefinition Container Definition Name	Obbligatorio.	No
Porta per il set di attività di sostituzione	AWS::ECS::TaskDefinition PortMapping ContainerPort	Obbligatorio.	No

Set di modifiche

Consigliamo vivamente di creare un set di modifiche prima di eseguire un aggiornamento dello stack che inizierà una distribuzione verde. Ciò consente di visualizzare le modifiche effettive che verranno apportate allo stack prima di eseguire l'aggiornamento dello stack. Tieni presente che le modifiche alle risorse potrebbero non essere elencate nell'ordine in cui verranno eseguite durante l'aggiornamento dello stack. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Monitoraggio degli eventi dello stack

È possibile visualizzare gli eventi stack generati in ogni fase dell'implementazione ECS nella scheda Events (Eventi) della pagina Stack oppure utilizzando AWS CLI. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Autorizzazioni IAM per le distribuzioni blue/green

CloudFormation Per eseguire correttamente le distribuzioni blu-verdi, devi disporre delle seguenti autorizzazioni: CodeDeploy

- `codedeploy:Get*`
- `codedeploy:CreateCloudFormationDeployment`

Per ulteriori informazioni, consulta [Operazioni, risorse e chiavi di condizione per CodeDeploy](#) nella Documentazione di riferimento per l'autorizzazione al servizio.

Considerazioni sulla gestione delle distribuzioni blue/green di ECS utilizzando CloudFormation

Il processo di utilizzo CloudFormation per eseguire le blue/green distribuzioni ECS CodeDeploy è diverso da quello di una distribuzione ECS standard che utilizza just. CodeDeploy Per una comprensione dettagliata di queste differenze, consulta [Differenze tra le blue/green distribuzioni di Amazon ECS tramite CodeDeploy e AWS CloudFormation](#) nella Guida per l'AWS CodeDeploy utente.

Quando si gestisce la blue/green distribuzione utilizzando CloudFormation, ci sono alcune limitazioni e considerazioni da tenere a mente:

- Solo gli aggiornamenti a determinate risorse avvieranno una distribuzione ecologica. Per ulteriori informazioni, consulta [Aggiornamenti delle risorse che avviano implementazioni ecologiche](#).
- Non è possibile includere aggiornamenti alle risorse che avviano implementazioni ecologiche e aggiornamenti ad altre risorse nello stesso aggiornamento dello stack. Per ulteriori informazioni, consulta [Aggiornamenti delle risorse che avviano implementazioni ecologiche](#).
- Puoi specificare solo una singola applicazione ECS come target di distribuzione.
- I parametri i cui valori sono offuscati non CloudFormation possono essere aggiornati CodeDeploy durante una distribuzione ecologica e causeranno un errore e un errore di aggiornamento dello stack. Ciò include:
 - Parametri definiti con l'attributo NoEcho.
 - Parametri che utilizzano riferimenti dinamici per recuperare i loro valori da servizi esterni. Per ulteriori informazioni sui riferimenti dinamici, vedere. [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#)

- Per annullare una distribuzione ecologica ancora in corso, annulla l'aggiornamento dello stack in CloudFormation, non CodeDeploy o ECS. Per ulteriori informazioni, consulta [Annullare un aggiornamento dello stack](#). Dopo che un aggiornamento è terminato, non è possibile annullarlo. Tuttavia, puoi aggiornare nuovamente uno stack con qualsiasi impostazione precedente.
- Le seguenti CloudFormation funzionalità non sono attualmente supportate per i modelli che definiscono le distribuzioni ECS: blue/green
 - Dichiarazione degli [output](#) o utilizzo di [Fn:: ImportValue](#) per importare valori da altri stack.
 - Importazione di risorse. Per ulteriori informazioni sull'importazione di risorse, vedere. [Importazione di AWS risorse in una CloudFormation pila](#)
 - Utilizzo dell'AWS::CodeDeploy::BlueGreenhook in un modello che include risorse dello stack annidate. Per ulteriori informazioni sugli stack annidati, consulta. [Dividi un modello in pezzi riutilizzabili usando pile annidate](#)
 - Utilizzo dell'AWS::CodeDeploy::BlueGreenhook in una pila annidata.

AWS::CodeDeploy::BlueGreensintassi hook

La sintassi seguente descrive la struttura di un AWS::CodeDeploy::BlueGreen hook per le distribuzioni ECS. blue/green

Sintassi

```
"Hooks": {
  "Logical ID": {
    "Type": "AWS::CodeDeploy::BlueGreen",
    "Properties": {
      "TrafficRoutingConfig": {
        "Type": "Traffic routing type",
        "TimeBasedCanary": {
          "StepPercentage": Integer,
          "BakeTimeMins": Integer
        },
        "TimeBasedLinear": {
          "StepPercentage": Integer,
          "BakeTimeMins": Integer
        }
      },
      "AdditionalOptions": {"TerminationWaitTimeInMinutes": Integer},
      "LifecycleEventHooks": {
        "BeforeInstall": "FunctionName",
```

```

    "AfterInstall": "FunctionName",
    "AfterAllowTestTraffic": "FunctionName",
    "BeforeAllowTraffic": "FunctionName",
    "AfterAllowTraffic": "FunctionName"
  },
  "ServiceRole": "CodeDeployServiceRoleName",
  "Applications": [
    {
      "Target": {
        "Type": "AWS::ECS::Service",
        "LogicalID": "Logical ID of AWS::ECS::Service"
      },
      "ECSAttributes": {
        "TaskDefinitions": [
          "Logical ID of AWS::ECS::TaskDefinition (Blue)",
          "Logical ID of AWS::ECS::TaskDefinition (Green)"
        ],
        "TaskSets": [
          "Logical ID of AWS::ECS::TaskSet (Blue)",
          "Logical ID of AWS::ECS::TaskSet (Green)"
        ],
        "TrafficRouting": {
          "ProdTrafficRoute": {
            "Type": "AWS::ElasticLoadBalancingV2::Listener",
            "LogicalID": "Logical ID of AWS::ElasticLoadBalancingV2::Listener  
(Production)"
          },
          "TestTrafficRoute": {
            "Type": "AWS::ElasticLoadBalancingV2::Listener",
            "LogicalID": "Logical ID of AWS::ElasticLoadBalancingV2::Listener  
(Test)"
          },
          "TargetGroups": [
            "Logical ID of AWS::ElasticLoadBalancingV2::TargetGroup (Blue)",
            "Logical ID of AWS::ElasticLoadBalancingV2::TargetGroup (Green)"
          ]
        }
      }
    }
  ]
}

```

Proprietà

ID logico (chiamato anche nome logico)

L'ID logico di un hook dichiarato nella Hooks sezione del modello. L'ID logico deve essere un valore alfanumerico (A-Z, a-z, 0-9) univoco all'interno del modello.

Campo obbligatorio: sì

Type

Il tipo di hook. `AWS::CodeDeploy::BlueGreen`

Campo obbligatorio: sì

Properties

Proprietà dell'hook.

Campo obbligatorio: sì

TrafficRoutingConfig

Impostazioni di configurazione dell'instradamento del traffico.

Required: No

La configurazione predefinita è lo spostamento del traffico canary basato sul tempo, con una percentuale di fasi del 15% e un tempo di cottura di cinque minuti.

Type

Tipo di spostamento del traffico utilizzato dalla configurazione di distribuzione.

Valori validi: `AllAtOnce` | `TimeBasedCanary` | `TimeBasedLinear`

Campo obbligatorio: sì

TimeBasedCanary

Specifica una configurazione che sposta il traffico da una versione della distribuzione a un'altra con due incrementi.

Obbligatorio: condizionale: se si specifica `TimeBasedCanary` come tipo di instradamento del traffico, è necessario includere il parametro `TimeBasedCanary`.

StepPercentage

Percentuale di traffico da spostare nel primo incremento di una distribuzione TimeBasedCanary. La percentuale di fasi deve essere pari o superiore al 14%.

Required: No

BakeTimeMins

Numero di minuti tra il primo e il secondo spostamento di traffico di una distribuzione TimeBasedCanary.

Required: No

TimeBasedLinear

Specifica una configurazione che sposta il traffico da una versione della distribuzione a un'altra con incrementi uguali, con un numero uguale di minuti tra ciascun incremento.

Obbligatorio: condizionale: se si specifica TimeBasedLinear come tipo di instradamento del traffico, è necessario includere il parametro TimeBasedLinear.

StepPercentage

Percentuale di traffico spostata all'inizio di ogni incremento di una distribuzione TimeBasedLinear. La percentuale di fasi deve essere pari o superiore al 14%.

Required: No

BakeTimeMins

Numero di minuti tra ogni spostamento incrementale del traffico di una distribuzione TimeBasedLinear.

Required: No

AdditionalOptions

Opzioni aggiuntive per la blue/green distribuzione.

Required: No

TerminationWaitTimeInMinutes

Specifica il tempo di attesa, in minuti, prima di terminare le risorse blu.

Required: No

LifecycleEventHooks

Usa gli hook degli eventi del ciclo di vita per specificare una funzione Lambda che CodeDeploy può chiamare per convalidare una distribuzione. Puoi utilizzare la stessa funzione o un'altra per gli eventi del ciclo di vita di distribuzione. Dopo il completamento dei test di convalida, la funzione `AfterAllowTraffic` Lambda CodeDeploy richiama e fornisce il risultato `Succeeded` o `Failed`. Per ulteriori informazioni, consulta la [sezione `AppSpec 'hook'`](#) nella Guida per l'AWS CodeDeploy utente.

Required: No

`BeforeInstall`

Funzione utilizzata per eseguire attività prima della creazione del set di attività di sostituzione.

Required: No

`AfterInstall`

Funzione utilizzata per eseguire attività dopo che il set di attività di sostituzione è stato creato e a esso è stato associato uno dei gruppi target.

Required: No

`AfterAllowTestTraffic`

Funzione utilizzata per eseguire attività dopo che il listener di test ha indirizzato il traffico verso il set di attività di sostituzione.

Required: No

`BeforeAllowTraffic`

Funzione utilizzata per eseguire attività dopo che il secondo gruppo target è stato associato al set di attività di sostituzione, ma prima che il traffico venga reindirizzato al set di attività di sostituzione.

Required: No

`AfterAllowTraffic`

Funzione utilizzata per eseguire attività dopo che il secondo gruppo target ha indirizzato il traffico verso il set di attività di sostituzione.

Required: No

ServiceRole

Il ruolo di esecuzione CloudFormation da utilizzare per eseguire le distribuzioni blu-verdi. Per un elenco delle autorizzazioni necessarie, vedere. [Autorizzazioni IAM per le distribuzioni blue/green](#)

Required: No

Applications

Specifica le proprietà dell'applicazione Amazon ECS.

Campo obbligatorio: sì

Target

Campo obbligatorio: sì

Type

Il tipo di risorsa.

Campo obbligatorio: sì

LogicalID

L'ID logico della risorsa.

Campo obbligatorio: sì

ECSAttributes

Le risorse che rappresentano i vari requisiti della distribuzione dell'applicazione Amazon ECS.

Campo obbligatorio: sì

TaskDefinitions

ID logico della risorsa [AWS::ECS::TaskDefinition](#) per eseguire il container Docker che contiene l'applicazione Amazon ECS.

Campo obbligatorio: sì

TaskSets

La logica IDs delle [AWS::ECS::TaskSet](#)risorse da utilizzare come set di attività per l'applicazione.

Campo obbligatorio: sì

TrafficRouting

Specifica le risorse utilizzate per l'instradamento del traffico.

Campo obbligatorio: sì

ProdTrafficRoute

Il listener che viene utilizzato dal load balancer per indirizzare il traffico verso i gruppi target.

Campo obbligatorio: sì

Type

Il tipo di risorsa. `AWS::ElasticLoadBalancingV2::Listener`

Campo obbligatorio: sì

LogicalID

L'ID logico della risorsa.

Campo obbligatorio: sì

TestTrafficRoute

Il listener che viene utilizzato dal load balancer per indirizzare il traffico verso i gruppi target.

Campo obbligatorio: sì

Type

Il tipo di risorsa. `AWS::ElasticLoadBalancingV2::Listener`

Campo obbligatorio: sì

LogicalID

L'ID logico della risorsa.

Required: No

TargetGroups

ID logico delle risorse da utilizzare come target per instradare il traffico al target registrato.

Campo obbligatorio: sì

Esempio di modello di implementazione blu/verde

Il modello di esempio seguente configura una distribuzione CodeDeploy blu/verde su ECS, con un avanzamento del routing del traffico del 15% per fase e un periodo di stabilizzazione di 5 minuti tra ogni passaggio.

La creazione di uno stack con il modello fornirà la configurazione iniziale della distribuzione. Se in seguito sono state apportate modifiche alle proprietà della BlueTaskSet risorsa che richiedono la sostituzione di tale risorsa, CloudFormation avvierà una distribuzione ecologica come parte dell'aggiornamento dello stack.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "Vpc": { "Type": "AWS::EC2::VPC::Id" },
    "Subnet1": { "Type": "AWS::EC2::Subnet::Id" },
    "Subnet2": { "Type": "AWS::EC2::Subnet::Id" }
  },
  "Transform": [ "AWS::CodeDeployBlueGreen" ],
  "Hooks": {
    "CodeDeployBlueGreenHook": {
      "Type": "AWS::CodeDeploy::BlueGreen",
      "Properties": {
        "TrafficRoutingConfig": {
          "Type": "TimeBasedCanary",
          "TimeBasedCanary": {
            "StepPercentage": 15,
            "BakeTimeMins": 5
          }
        }
      }
    },
    "Applications": [
      {
        "Target": {
          "Type": "AWS::ECS::Service",
          "LogicalID": "ECSDemoService"
        },
        "ECSAttributes": {
          "TaskDefinitions": [ "BlueTaskDefinition", "GreenTaskDefinition" ],
```

```

        "TaskSets": [ "BlueTaskSet", "GreenTaskSet" ],
        "TrafficRouting": {
            "ProdTrafficRoute": {
                "Type": "AWS::ElasticLoadBalancingV2::Listener",
                "LogicalID": "ALBListenerProdTraffic"
            },
            "TargetGroups": [ "ALBTargetGroupBlue", "ALBTargetGroupGreen" ]
        }
    }
}
],
}
},
},
"Resources": {
    "ExampleSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Security group for ec2 access",
            "VpcId": { "Ref": "Vpc" },
            "SecurityGroupIngress": [
                {
                    "IpProtocol": "tcp",
                    "FromPort": 80,
                    "ToPort": 80,
                    "CidrIp": "0.0.0.0/0"
                },
                {
                    "IpProtocol": "tcp",
                    "FromPort": 8080,
                    "ToPort": 8080,
                    "CidrIp": "0.0.0.0/0"
                },
                {
                    "IpProtocol": "tcp",
                    "FromPort": 22,
                    "ToPort": 22,
                    "CidrIp": "0.0.0.0/0"
                }
            ]
        }
    }
},
    "ALBTargetGroupBlue": {
        "Type": "AWS::ElasticLoadBalancingV2::TargetGroup",

```

```

    "Properties":{
      "HealthCheckIntervalSeconds":5,
      "HealthCheckPath":"/",
      "HealthCheckPort":"80",
      "HealthCheckProtocol":"HTTP",
      "HealthCheckTimeoutSeconds":2,
      "HealthyThresholdCount":2,
      "Matcher":{ "HttpCode":"200" },
      "Port":80,
      "Protocol":"HTTP",
      "Tags":[{ "Key":"Group","Value":"Example" }],
      "TargetType":"ip",
      "UnhealthyThresholdCount":4,
      "VpcId":{ "Ref":"Vpc" }
    }
  },
  "ALBTargetGroupGreen":{
    "Type":"AWS::ElasticLoadBalancingV2::TargetGroup",
    "Properties":{
      "HealthCheckIntervalSeconds":5,
      "HealthCheckPath":"/",
      "HealthCheckPort":"80",
      "HealthCheckProtocol":"HTTP",
      "HealthCheckTimeoutSeconds":2,
      "HealthyThresholdCount":2,
      "Matcher":{ "HttpCode":"200" },
      "Port":80,
      "Protocol":"HTTP",
      "Tags":[{ "Key":"Group","Value":"Example" }],
      "TargetType":"ip",
      "UnhealthyThresholdCount":4,
      "VpcId":{ "Ref":"Vpc" }
    }
  },
  "ExampleALB":{
    "Type":"AWS::ElasticLoadBalancingV2::LoadBalancer",
    "Properties":{
      "Scheme":"internet-facing",
      "SecurityGroups":[{ "Ref":"ExampleSecurityGroup" }],
      "Subnets":[{ "Ref":"Subnet1" },{ "Ref":"Subnet2" }],
      "Tags":[{ "Key":"Group","Value":"Example" }],
      "Type":"application",
      "IpAddressType":"ipv4"
    }
  }
}

```

```
},
"ALBListenerProdTraffic":{
  "Type":"AWS::ElasticLoadBalancingV2::Listener",
  "Properties":{
    "DefaultActions":[
      {
        "Type":"forward",
        "ForwardConfig":{
          "TargetGroups":[
            {
              "TargetGroupArn":{ "Ref":"ALBTargetGroupBlue" },
              "Weight":1
            }
          ]
        }
      }
    ],
    "LoadBalancerArn":{ "Ref":"ExampleALB" },
    "Port":80,
    "Protocol":"HTTP"
  }
},
"ALBListenerProdRule":{
  "Type":"AWS::ElasticLoadBalancingV2::ListenerRule",
  "Properties":{
    "Actions":[
      {
        "Type":"forward",
        "ForwardConfig":{
          "TargetGroups":[
            {
              "TargetGroupArn":{ "Ref":"ALBTargetGroupBlue" },
              "Weight":1
            }
          ]
        }
      }
    ],
    "Conditions":[
      {
        "Field":"http-header",
        "HttpHeaderConfig":{
          "HttpHeaderName":"User-Agent",
          "Values":[ "Mozilla" ]
        }
      }
    ]
  }
}
```

```

        }
      }
    ],
    "ListenerArn":{ "Ref":"ALBListenerProdTraffic" },
    "Priority":1
  }
},
"ECSTaskExecutionRole":{
  "Type":"AWS::IAM::Role",
  "Properties":{
    "AssumeRolePolicyDocument":{
      "Version":"2012-10-17",
      "Statement":[
        {
          "Sid": "",
          "Effect": "Allow",
          "Principal": {
            "Service": "ecs-tasks.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  },
  "ManagedPolicyArns": [ "arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy" ]
},
"BlueTaskDefinition":{
  "Type":"AWS::ECS::TaskDefinition",
  "Properties":{
    "ExecutionRoleArn":{
      "Fn::GetAtt":[ "ECSTaskExecutionRole","Arn" ]
    },
    "ContainerDefinitions":[
      {
        "Name":"DemoApp",
        "Image":"nginxdemos/hello:latest",
        "Essential":true,
        "PortMappings":[
          {
            "HostPort":80,
            "Protocol":"tcp",
            "ContainerPort":80
          }
        ]
      }
    ]
  }
}

```

```

        ]
      }
    ],
    "RequiresCompatibilities":[ "FARGATE" ],
    "NetworkMode":"awsvpc",
    "Cpu":"256",
    "Memory":"512",
    "Family":"ecs-demo"
  }
},
"ECSDemoCluster":{
  "Type":"AWS::ECS::Cluster",
  "Properties":{}
},
"ECSDemoService":{
  "Type":"AWS::ECS::Service",
  "Properties":{
    "Cluster":{"Ref":"ECSDemoCluster" },
    "DesiredCount":1,
    "DeploymentController":{"Type":"EXTERNAL" }
  }
},
"BlueTaskSet":{
  "Type":"AWS::ECS::TaskSet",
  "Properties":{
    "Cluster":{"Ref":"ECSDemoCluster" },
    "LaunchType":"FARGATE",
    "NetworkConfiguration":{
      "AwsVpcConfiguration":{
        "AssignPublicIp":"ENABLED",
        "SecurityGroups":[{ "Ref":"ExampleSecurityGroup" }],
        "Subnets":[{ "Ref":"Subnet1" },{ "Ref":"Subnet2" }]
      }
    }
  },
  "PlatformVersion":"1.4.0",
  "Scale":{
    "Unit":"PERCENT",
    "Value":100
  },
  "Service":{"Ref":"ECSDemoService"},
  "TaskDefinition":{"Ref":"BlueTaskDefinition" },
  "LoadBalancers":[
    {
      "ContainerName":"DemoApp",

```

```

        "ContainerPort":80,
        "TargetGroupArn":{ "Ref":"ALBTargetGroupBlue" }
    }
]
}
},
"PrimaryTaskSet":{
    "Type":"AWS::ECS::PrimaryTaskSet",
    "Properties":{
        "Cluster":{ "Ref":"ECSDemoCluster" },
        "Service":{ "Ref":"ECSDemoService" },
        "TaskSetId":{ "Fn::GetAtt":[ "BlueTaskSet","Id" ]
    }
}
}
}
}
}
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Parameters:
  Vpc:
    Type: 'AWS::EC2::VPC::Id'
  Subnet1:
    Type: 'AWS::EC2::Subnet::Id'
  Subnet2:
    Type: 'AWS::EC2::Subnet::Id'
Transform:
  - 'AWS::CodeDeployBlueGreen'
Hooks:
  CodeDeployBlueGreenHook:
    Type: 'AWS::CodeDeploy::BlueGreen'
    Properties:
      TrafficRoutingConfig:
        Type: TimeBasedCanary
        TimeBasedCanary:
          StepPercentage: 15
          BakeTimeMins: 5
      Applications:
        - Target:
            Type: 'AWS::ECS::Service'
            LogicalID: ECSDemoService

```

```
ECSAttributes:
  TaskDefinitions:
    - BlueTaskDefinition
    - GreenTaskDefinition
  TaskSets:
    - BlueTaskSet
    - GreenTaskSet
  TrafficRouting:
    ProdTrafficRoute:
      Type: 'AWS::ElasticLoadBalancingV2::Listener'
      LogicalID: ALBListenerProdTraffic
    TargetGroups:
      - ALBTargetGroupBlue
      - ALBTargetGroupGreen
```

Resources:

```
ExampleSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Security group for ec2 access
    VpcId: !Ref Vpc
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        CidrIp: 0.0.0.0/0
      - IpProtocol: tcp
        FromPort: 8080
        ToPort: 8080
        CidrIp: 0.0.0.0/0
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: 0.0.0.0/0
```

```
ALBTargetGroupBlue:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    HealthCheckIntervalSeconds: 5
    HealthCheckPath: /
    HealthCheckPort: '80'
    HealthCheckProtocol: HTTP
    HealthCheckTimeoutSeconds: 2
    HealthyThresholdCount: 2
    Matcher:
      HttpCode: '200'
```



```
    Port: 80
    Protocol: HTTP
    Tags:
      - Key: Group
        Value: Example
    TargetType: ip
    UnhealthyThresholdCount: 4
    VpcId: !Ref Vpc
ALBTargetGroupGreen:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    HealthCheckIntervalSeconds: 5
    HealthCheckPath: /
    HealthCheckPort: '80'
    HealthCheckProtocol: HTTP
    HealthCheckTimeoutSeconds: 2
    HealthyThresholdCount: 2
    Matcher:
      HttpCode: '200'
    Port: 80
    Protocol: HTTP
    Tags:
      - Key: Group
        Value: Example
    TargetType: ip
    UnhealthyThresholdCount: 4
    VpcId: !Ref Vpc
ExampleALB:
  Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
  Properties:
    Scheme: internet-facing
    SecurityGroups:
      - !Ref ExampleSecurityGroup
    Subnets:
      - !Ref Subnet1
      - !Ref Subnet2
    Tags:
      - Key: Group
        Value: Example
    Type: application
    IpAddressType: ipv4
ALBListenerProdTraffic:
  Type: 'AWS::ElasticLoadBalancingV2::Listener'
  Properties:
```

```
DefaultActions:
  - Type: forward
    ForwardConfig:
      TargetGroups:
        - TargetGroupArn: !Ref ALBTargetGroupBlue
          Weight: 1
    LoadBalancerArn: !Ref ExampleALB
    Port: 80
    Protocol: HTTP
ALBListenerProdRule:
  Type: 'AWS::ElasticLoadBalancingV2::ListenerRule'
  Properties:
    Actions:
      - Type: forward
        ForwardConfig:
          TargetGroups:
            - TargetGroupArn: !Ref ALBTargetGroupBlue
              Weight: 1
    Conditions:
      - Field: http-header
        HttpHeaderConfig:
          HttpHeaderName: User-Agent
          Values:
            - Mozilla
    ListenerArn: !Ref ALBListenerProdTraffic
    Priority: 1
ECSTaskExecutionRole:
  Type: 'AWS::IAM::Role'
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Sid: ''
          Effect: Allow
          Principal:
            Service: ecs-tasks.amazonaws.com
          Action: 'sts:AssumeRole'
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy'
BlueTaskDefinition:
  Type: 'AWS::ECS::TaskDefinition'
  Properties:
    ExecutionRoleArn: !GetAtt
      - ECSTaskExecutionRole
```

```
- Arn
ContainerDefinitions:
  - Name: DemoApp
    Image: 'nginxdemos/hello:latest'
    Essential: true
    PortMappings:
      - HostPort: 80
        Protocol: tcp
        ContainerPort: 80
    RequiresCompatibilities:
      - FARGATE
    NetworkMode: awsvpc
    Cpu: '256'
    Memory: '512'
    Family: ecs-demo
ECSDemoCluster:
  Type: 'AWS::ECS::Cluster'
  Properties: {}
ECSDemoService:
  Type: 'AWS::ECS::Service'
  Properties:
    Cluster: !Ref ECSDemoCluster
    DesiredCount: 1
    DeploymentController:
      Type: EXTERNAL
BlueTaskSet:
  Type: 'AWS::ECS::TaskSet'
  Properties:
    Cluster: !Ref ECSDemoCluster
    LaunchType: FARGATE
    NetworkConfiguration:
      AwsVpcConfiguration:
        AssignPublicIp: ENABLED
        SecurityGroups:
          - !Ref ExampleSecurityGroup
        Subnets:
          - !Ref Subnet1
          - !Ref Subnet2
    PlatformVersion: 1.4.0
    Scale:
      Unit: PERCENT
      Value: 100
    Service: !Ref ECSDemoService
    TaskDefinition: !Ref BlueTaskDefinition
```

```
LoadBalancers:
  - ContainerName: DemoApp
    ContainerPort: 80
    TargetGroupArn: !Ref ALBTargetGroupBlue
PrimaryTaskSet:
  Type: 'AWS::ECS::PrimaryTaskSet'
  Properties:
    Cluster: !Ref ECSDemoCluster
    Service: !Ref ECSDemoService
    TaskSetId: !GetAtt
      - BlueTaskSet
      - Id
```

CloudFormation frammenti di modello

Questa sezione fornisce una serie di scenari di esempio che ti aiutano a capire come dichiarare varie parti del modello AWS CloudFormation . Puoi anche utilizzare i frammenti come punto di partenza per le sezioni dei tuoi modelli personalizzati.

Note

Poiché AWS CloudFormation i modelli devono essere conformi a JSON, non è previsto un carattere di continuazione di riga. La disposizione degli snippet in questo documento può essere casuale se la riga è più lunga di 68 caratteri.

Argomenti

- [Frammenti di modello generale](#)
- [frammenti di CloudFormation modello con ridimensionamento automatico](#)
- [AWS Frammenti di modello della Billing Console](#)
- [AWS CloudFormation frammenti di modello](#)
- [Frammenti CloudFront di modello Amazon](#)
- [Frammenti CloudWatch di modello Amazon](#)
- [Frammenti di modello Amazon CloudWatch Logs](#)
- [Frammenti di modello Amazon DynamoDB](#)
- [Frammenti EC2 CloudFormation di modello Amazon](#)
- [Modelli di esempio di Amazon Elastic Container Service](#)

- [Modello di esempio Amazon Elastic File System](#)
- [Frammenti di modello Elastic Beanstalk](#)
- [Frammenti di modello Elastic Load Balancing](#)
- [AWS Identity and Access Management frammenti di modello](#)
- [AWS Lambda modello](#)
- [AWS OpsWorks frammenti di modello](#)
- [Frammenti di modello Amazon Redshift](#)
- [Frammenti di modello Amazon RDS](#)
- [Frammenti di modello Route 53](#)
- [Frammenti di modello Amazon S3](#)
- [Frammenti di modello Amazon SNS](#)
- [Frammenti di modello Amazon SQS](#)
- [Frammenti di modello Amazon Timestream](#)

Frammenti di modello generale

Gli esempi seguenti mostrano diverse funzionalità dei CloudFormation modelli che non sono specifiche di un AWS servizio.

Argomenti

- [Base64proprietà codificata UserData](#)
- [Base64UserDataproprietà codificata con e AccessKeySecretKey](#)
- [Parameterssezione con un parametro di stringa letterale](#)
- [Parameterssezione con parametro di stringa con vincolo di espressione regolare](#)
- [Parameterssezione con parametri numerici con MinValue e MaxValue vincoli](#)
- [Parameterssezione con parametro numerico con vincolo AllowedValues](#)
- [Parameterssezione con un parametro letterale CommaDelimitedList](#)
- [Parameterssezione con valore del parametro basato su uno pseudo parametro](#)
- [Mappingsezione con tre mappature](#)
- [Descriptionbasato su una stringa letterale](#)
- [Outputssezione con una stringa letterale in uscita](#)
- [Outputssezione con un riferimento alla risorsa e un output di pseudo riferimento](#)

- [Outputs sezione con un output basato su una funzione, una stringa letterale, un riferimento e uno pseudo parametro](#)
- [Versione del modello](#)
- [AWSTags property](#)

Base64 proprietà codificata UserData

Questo esempio mostra l'assemblaggio di una `UserData` proprietà utilizzando le `Fn::Join` funzioni `Fn::Base64` and. I riferimenti `MyValue` e `MyName` sono parametri che devono essere definiti nella `Parameters` sezione del modello. La stringa letterale `Hello World` è solo un altro valore che questo esempio trasferisce come parte di `UserData`.

JSON

```
"UserData" : {
  "Fn::Base64" : {
    "Fn::Join" : [ ",", [
      { "Ref" : "MyValue" },
      { "Ref" : "MyName" },
      "Hello World" ] ]
  }
}
```

YAML

```
UserData:
  Fn::Base64: !Sub |
    Ref: MyValue
    Ref: MyName
    Hello World
```

Base64UserData proprietà codificata con e AccessKeySecretKey

Questo esempio mostra l'assemblaggio di una `UserData` proprietà utilizzando le `Fn::Join` funzioni `Fn::Base64` and. Include le informazioni `AccessKey` e `SecretKey`. I riferimenti `AccessKey` e `SecretKey` sono i parametri che devono essere definiti nella sezione Parametri del modello.

JSON

```
"UserData" : {
```

```

    "Fn::Base64" : {
      "Fn::Join" : [ "", [
        "ACCESS_KEY=", { "Ref" : "AccessKey" },
        "SECRET_KEY=", { "Ref" : "SecretKey" } ] ]
    }
  }
}

```

YAML

```

UserData:
  Fn::Base64: !Sub |
    ACCESS_KEY=${AccessKey}
    SECRET_KEY=${SecretKey}

```

Parameterssezione con un parametro di stringa letterale

Il seguente esempio illustra una dichiarazione della sezione parametri valida in cui viene dichiarato un singolo tipo di parametro String.

JSON

```

"Parameters" : {
  "UserName" : {
    "Type" : "String",
    "Default" : "nonadmin",
    "Description" : "Assume a vanilla user if no command-line spec provided"
  }
}

```

YAML

```

Parameters:
  UserName:
    Type: String
    Default: nonadmin
    Description: Assume a vanilla user if no command-line spec provided

```

Parameterssezione con parametro di stringa con vincolo di espressione regolare

Il seguente esempio illustra una dichiarazione della sezione parametri valida in cui viene dichiarato un singolo tipo di parametro String. Il AdminUserAccount parametro ha un valore predefinito di.

admin Il valore di parametro deve avere una lunghezza minima di 1 e una massima di 16 e contiene caratteri alfabetici e numeri, ma deve iniziare con un carattere alfabetico.

JSON

```
"Parameters" : {
  "AdminUserAccount": {
    "Default": "admin",
    "NoEcho": "true",
    "Description" : "The admin account user name",
    "Type": "String",
    "MinLength": "1",
    "MaxLength": "16",
    "AllowedPattern" : "[a-zA-Z][a-zA-Z0-9]*"
  }
}
```

YAML

```
Parameters:
  AdminUserAccount:
    Default: admin
    NoEcho: true
    Description: The admin account user name
    Type: String
    MinLength: 1
    MaxLength: 16
    AllowedPattern: '[a-zA-Z][a-zA-Z0-9]*'
```

Parameterssezione con parametri numerici con MinValue e MaxValue vincoli

Il seguente esempio illustra una dichiarazione della sezione parametri valida in cui viene dichiarato un singolo tipo di parametro Number. Il WebServerPort parametro ha un valore predefinito di 80 e un valore minimo 1 e un valore massimo 65535.

JSON

```
"Parameters" : {
  "WebServerPort": {
    "Default": "80",
    "Description" : "TCP/IP port for the web server",
    "Type": "Number",
```



```
    "MinValue": "1",  
    "MaxValue": "65535"  
  }  
}
```

YAML

```
Parameters:  
  WebServerPort:  
    Default: 80  
    Description: TCP/IP port for the web server  
    Type: Number  
    MinValue: 1  
    MaxValue: 65535
```

Parameterssezione con parametro numerico con vincolo AllowedValues

Il seguente esempio illustra una dichiarazione della sezione parametri valida in cui viene dichiarato un singolo tipo di parametro Number. Il WebServerPort parametro ha un valore predefinito di 80 e consente solo i valori di 80 e 8888.

JSON

```
"Parameters" : {  
  "WebServerPortLimited": {  
    "Default": "80",  
    "Description" : "TCP/IP port for the web server",  
    "Type": "Number",  
    "AllowedValues" : ["80", "8888"]  
  }  
}
```

YAML

```
Parameters:  
  WebServerPortLimited:  
    Default: 80  
    Description: TCP/IP port for the web server  
    Type: Number  
    AllowedValues:  
      - 80
```

- 8888

Parameters sezione con un parametro letterale CommaDelimitedList

L'esempio seguente illustra una dichiarazione di Parameters sezione valida in cui viene dichiarato un parametro CommaDelimitedList di tipo singolo. La NoEcho proprietà è impostata su TRUE, che maschererà il suo valore con asterischi (****) nell'describe-stackoutput, ad eccezione delle informazioni memorizzate nelle posizioni specificate di seguito.

Important

L'utilizzo dell'attributo NoEcho non maschera le informazioni memorizzate nei seguenti elementi:

- La Metadata sezione dei modelli. CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per ulteriori informazioni, vedere [Metadati](#).
- Sezione dei modelli Outputs. Per ulteriori informazioni, consulta [Output](#).
- Attributo Metadata di una definizione di risorsa. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Si consiglia vivamente di non utilizzare questi meccanismi per includere informazioni sensibili, come password o segreti.

Important

Anziché incorporare informazioni riservate direttamente nei CloudFormation modelli, consigliamo di utilizzare parametri dinamici nel modello di pila per fare riferimento a informazioni sensibili archiviate e gestite all'esterno CloudFormation, ad esempio nel AWS Systems Manager Parameter Store o. AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

JSON

```
"Parameters" : {  
  "UserRoles" : {  
    "Type" : "CommaDelimitedList",
```

```

        "Default" : "guest,newhire",
        "NoEcho" : "TRUE"
    }
}

```

YAML

```

Parameters:
  UserRoles:
    Type: CommaDelimitedList
    Default: "guest,newhire"
    NoEcho: true

```

Parameterssezione con valore del parametro basato su uno pseudo parametro

L'esempio seguente mostra i comandi nei dati EC2 utente che utilizzano gli pseudo parametri e.

`AWS::StackName` `AWS::Region` Per ulteriori informazioni sugli pseudoparametri, consulta [Ottieni AWS valori usando pseudo parametri](#).

JSON

```

    "UserData"      : { "Fn::Base64" : { "Fn::Join" : [ "", [
        "#!/bin/bash -xe\n",
        "yum install -y aws-cfn-bootstrap\n",

        "/opt/aws/bin/cfn-init -v ",
        "      --stack ", { "Ref" : "AWS::StackName" },
        "      --resource LaunchConfig ",
        "      --region ", { "Ref" : "AWS::Region" }, "\n",

        "/opt/aws/bin/cfn-signal -e $? ",
        "      --stack ", { "Ref" : "AWS::StackName" },
        "      --resource WebServerGroup ",
        "      --region ", { "Ref" : "AWS::Region" }, "\n"
      ] ] }
    }
}

```

YAML

```

UserData:
  Fn::Base64: !Sub |
    #!/bin/bash -xe

```

```
yum update -y aws-cfn-bootstrap
/opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource LaunchConfig --
region ${AWS::Region}
/opt/aws/bin/cfn-signal -e $? --stack ${AWS::StackName} --resource WebServerGroup
--region ${AWS::Region}
```

Mappingsezione con tre mappature

L'esempio seguente illustra una dichiarazione di Mapping sezione valida che contiene tre mappature. La mappa, quando abbinata a una chiave di mappatura Stop, SlowDown oppure Go, fornisce i valori RGB assegnati all'attributo corrispondente RGBColor.

JSON

```
"Mappings" : {
  "LightColor" : {
    "Stop" : {
      "Description" : "red",
      "RGBColor" : "RED 255 GREEN 0 BLUE 0"
    },
    "SlowDown" : {
      "Description" : "yellow",
      "RGBColor" : "RED 255 GREEN 255 BLUE 0"
    },
    "Go" : {
      "Description" : "green",
      "RGBColor" : "RED 0 GREEN 128 BLUE 0"
    }
  }
}
```

YAML

```
Mappings:
  LightColor:
    Stop:
      Description: red
      RGBColor: "RED 255 GREEN 0 BLUE 0"
    SlowDown:
      Description: yellow
      RGBColor: "RED 255 GREEN 255 BLUE 0"
    Go:
```

```
Description: green
RGBColor: "RED 0 GREEN 128 BLUE 0"
```

Description basato su una stringa letterale

L'esempio seguente illustra una dichiarazione di `Description` sezione valida in cui il valore è basato su una stringa letterale. Questo frammento può essere per modelli, parametri, risorse, proprietà o output.

JSON

```
"Description" : "Replace this value"
```

YAML

```
Description: "Replace this value"
```

Outputs sezione con una stringa letterale in uscita

Questo esempio illustra un'assegnazione di output basata su una stringa letterale.

JSON

```
"Outputs" : {
  "MyPhone" : {
    "Value" : "Please call 555-5555",
    "Description" : "A random message for aws cloudformation describe-stacks"
  }
}
```

YAML

```
Outputs:
  MyPhone:
    Value: Please call 555-5555
    Description: A random message for aws cloudformation describe-stacks
```

Outputs sezione con un riferimento alla risorsa e un output di pseudo riferimento

Questo esempio mostra una `Outputs` sezione con due assegnazioni di output. Una si basa su una risorsa e l'altra si basa su uno pseudoriferimento.

JSON

```
"Outputs" : {
  "SNSTopic" : { "Value" : { "Ref" : "MyNotificationTopic" } },
  "StackName" : { "Value" : { "Ref" : "AWS::StackName" } }
}
```

YAML

```
Outputs:
  SNSTopic:
    Value: !Ref MyNotificationTopic
  StackName:
    Value: !Ref AWS::StackName
```

Outputssezione con un output basato su una funzione, una stringa letterale, un riferimento e uno pseudo parametro

Questo esempio illustra una sezione output con un'assegnazione di output. La funzione Join viene utilizzata per concatenare il valore, utilizzando un segno di percentuale come delimitatore.

JSON

```
"Outputs" : {
  "MyOutput" : {
    "Value" : { "Fn::Join" :
      [ "%", [ "A-string", {"Ref" : "AWS::StackName" } ] ]
    }
  }
}
```

YAML

```
Outputs:
  MyOutput:
    Value: !Join [ %, [ 'A-string', !Ref 'AWS::StackName' ] ]
```

Versione del modello

Il seguente frammento mostra una dichiarazione di sezione valida. `AWSTemplateFormatVersion`

JSON

```
"AWSTemplateFormatVersion" : "2010-09-09"
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
```

AWSTags property

Questo esempio mostra una proprietà. AWS Tags Devi specificare questa proprietà all'interno della sezione proprietà di una risorsa. Quando la risorsa viene creata, verrà contrassegnata con i tag dichiarati.

JSON

```
"Tags" : [  
  {  
    "Key" : "keyname1",  
    "Value" : "value1"  
  },  
  {  
    "Key" : "keyname2",  
    "Value" : "value2"  
  }  
]
```

YAML

```
Tags:  
-  
  Key: "keyname1"  
  Value: "value1"  
-  
  Key: "keyname2"  
  Value: "value2"
```

frammenti di CloudFormation modello con ridimensionamento automatico

Con Amazon EC2 Auto Scaling, puoi scalare automaticamente EC2 le istanze Amazon, con politiche di scalabilità o con scalabilità programmata. I gruppi Auto Scaling sono raccolte di EC2

istanze Amazon che abilitano funzionalità di scalabilità automatica e gestione del parco veicoli, come politiche di scalabilità, azioni pianificate, controlli dello stato di salute, ganci del ciclo di vita e bilanciamento del carico.

Application Auto Scaling fornisce il ridimensionamento automatico di diverse risorse oltre Amazon EC2, con politiche di scalabilità o con scalabilità programmata.

Puoi creare e configurare gruppi di Auto Scaling, policy di scaling, azioni pianificate e altre risorse di auto scaling come parte della tua infrastruttura utilizzando modelli. AWS CloudFormation I modelli semplificano la gestione e l'automazione dell'implementazione di risorse con scalabilità automatica in modo ripetibile e coerente.

I seguenti frammenti di modello di esempio descrivono AWS CloudFormation risorse o componenti per Amazon Auto EC2 Scaling e Application Auto Scaling. Questi frammenti sono progettati per essere integrati in un modello e non sono destinati a essere eseguiti in modo indipendente.

Categorie dei frammenti

- [Configura le risorse di Amazon EC2 Auto Scaling con AWS CloudFormation](#)
- [Configura le risorse di Application Auto Scaling con AWS CloudFormation](#)

Configura le risorse di Amazon EC2 Auto Scaling con AWS CloudFormation

Gli esempi seguenti mostrano diversi frammenti da includere nei modelli da utilizzare con Amazon Auto EC2 Scaling.

Categorie dei frammenti

- [Creare un gruppo Auto Scaling a istanza singola](#)
- [Crea un gruppo di Auto Scaling con un sistema di bilanciamento del carico collegato](#)
- [Crea un gruppo Auto Scaling con notifiche](#)
- [Crea un gruppo Auto Scaling che utilizza un e un CreationPolicyUpdatePolicy](#)
- [Creazione di una policy di dimensionamento per fasi](#)
- [Esempi di gruppi di istanze miste](#)
- [Esempi di configurazione di avvio](#)

Creare un gruppo Auto Scaling a istanza singola

Questo esempio mostra una [AWS::AutoScaling::AutoScalingGroup](#) risorsa con una singola istanza per aiutarti a iniziare. La proprietà `VPCZoneIdentifier` del gruppo con scalabilità automatica specifica un elenco di sottoreti esistenti in diverse zone di disponibilità. È necessario specificare la sottorete applicabile IDs dal vostro account prima di creare lo stack. La `LaunchTemplate` proprietà fa riferimento a una [AWS::EC2::LaunchTemplate](#) risorsa con il nome `myLaunchTemplate` logico definito altrove nel modello.

Note

Per esempi di modelli di lancio, [Crea modelli di lancio con CloudFormation](#) consulta la sezione Amazon EC2 snippet e la sezione [Esempi](#) nella `AWS::EC2::LaunchTemplate` risorsa.

JSON

```
"myASG" : {
  "Type" : "AWS::AutoScaling::AutoScalingGroup",
  "Properties" : {
    "VPCZoneIdentifier" : [ "subnetIdAz1", "subnetIdAz2", "subnetIdAz3" ],
    "LaunchTemplate" : {
      "LaunchTemplateId" : {
        "Ref" : "myLaunchTemplate"
      },
      "Version" : {
        "Fn::GetAtt" : [
          "myLaunchTemplate",
          "LatestVersionNumber"
        ]
      }
    },
    "MaxSize" : "1",
    "MinSize" : "1"
  }
}
```

YAML

```

myASG:
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    VPCZoneIdentifier:
      - subnetIdAz1
      - subnetIdAz2
      - subnetIdAz3
    LaunchTemplate:
      LaunchTemplateId: !Ref myLaunchTemplate
      Version: !GetAtt myLaunchTemplate.LatestVersionNumber
    MaxSize: '1'
    MinSize: '1'

```

Crea un gruppo di Auto Scaling con un sistema di bilanciamento del carico collegato

Questo esempio mostra una [AWS::AutoScaling::AutoScalingGroup](#) risorsa per il bilanciamento del carico su più server. Specifica i nomi logici delle AWS risorse dichiarate altrove nello stesso modello.

1. La `VPCZoneIdentifier` proprietà specifica i nomi logici di due [AWS::EC2::Subnet](#) risorse in cui verranno create le istanze EC2 del gruppo Auto Scaling: e. `myPublicSubnet1` `myPublicSubnet2`
2. La `LaunchTemplate` proprietà specifica una [AWS::EC2::LaunchTemplate](#) risorsa con il nome logico. `myLaunchTemplate`
3. La proprietà `TargetGroupARNs` elenca i gruppi di destinazione per Application Load Balancer o Network Load Balancer utilizzati per instradare il traffico al gruppo con dimensionamento automatico. In questo esempio, viene specificato un gruppo target, una [AWS::ElasticLoadBalancingV2::TargetGroup](#) risorsa con il nome `myTargetGroup` logico.

JSON

```

"myServerGroup" : {
  "Type" : "AWS::AutoScaling::AutoScalingGroup",
  "Properties" : {
    "VPCZoneIdentifier" : [ { "Ref" : "myPublicSubnet1" }, { "Ref" :
"myPublicSubnet2" } ],
    "LaunchTemplate" : {

```

```

    "LaunchTemplateId" : {
      "Ref" : "myLaunchTemplate"
    },
    "Version" : {
      "Fn::GetAtt" : [
        "myLaunchTemplate",
        "LatestVersionNumber"
      ]
    }
  },
  "MaxSize" : "5",
  "MinSize" : "1",
  "TargetGroupARNs" : [ { "Ref" : "myTargetGroup" } ]
}

```

YAML

```

myServerGroup:
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    VPCZoneIdentifier:
      - !Ref myPublicSubnet1
      - !Ref myPublicSubnet2
    LaunchTemplate:
      LaunchTemplateId: !Ref myLaunchTemplate
      Version: !GetAtt myLaunchTemplate.LatestVersionNumber
    MaxSize: '5'
    MinSize: '1'
    TargetGroupARNs:
      - !Ref myTargetGroup

```

Consulta anche

Per un esempio dettagliato nel quale viene creato un gruppo con scalabilità automatica con una policy di dimensionamento di tracciamento della destinazione basato sul parametro predefinito `ALBRequestCountPerTarget` per Application Load Balancer, consulta la sezione [Esempi](#) nella risorsa `AWS::AutoScaling::ScalingPolicy`.

Crea un gruppo Auto Scaling con notifiche

Questo esempio mostra una [AWS::AutoScaling::AutoScalingGroup](#) risorsa che invia notifiche Amazon SNS quando si verificano gli eventi specificati. La `NotificationConfigurations`

proprietà specifica l'argomento SNS a cui AWS CloudFormation invia una notifica e gli eventi che AWS CloudFormation provocheranno l'invio delle notifiche. Quando si `NotificationTypes` verificano gli eventi specificati da, AWS CloudFormation invierà una notifica all'argomento SNS specificato da. `TopicARN` Quando avvii lo stack, AWS CloudFormation crea una [AWS::SNS::Subscription](#) risorsa (`snsTopicForAutoScalingGroup`) dichiarata all'interno dello stesso modello.

La proprietà `VPCZoneIdentifier` del gruppo con scalabilità automatica specifica un elenco di sottoreti esistenti in diverse zone di disponibilità. È necessario specificare la sottorete applicabile IDs dal vostro account prima di creare lo stack. La `LaunchTemplate` proprietà fa riferimento al nome logico di una [AWS::EC2::LaunchTemplate](#) risorsa dichiarata altrove nello stesso modello.

JSON

```
"myASG" : {
  "Type" : "AWS::AutoScaling::AutoScalingGroup",
  "DependsOn": [
    "snsTopicForAutoScalingGroup"
  ],
  "Properties" : {
    "VPCZoneIdentifier" : [ "subnetIdAz1", "subnetIdAz2", "subnetIdAz3" ],
    "LaunchTemplate" : {
      "LaunchTemplateId" : {
        "Ref" : "logicalName"
      },
      "Version" : {
        "Fn::GetAtt" : [
          "logicalName",
          "LatestVersionNumber"
        ]
      }
    },
    "MaxSize" : "5",
    "MinSize" : "1",
    "NotificationConfigurations" : [
      {
        "TopicARN" : { "Ref" : "snsTopicForAutoScalingGroup" },
        "NotificationTypes" : [
          "autoscaling:EC2_INSTANCE_LAUNCH",
          "autoscaling:EC2_INSTANCE_LAUNCH_ERROR",
          "autoscaling:EC2_INSTANCE_TERMINATE",
          "autoscaling:EC2_INSTANCE_TERMINATE_ERROR",
```

```

        "autoscaling:TEST_NOTIFICATION"
    ]
}
]
}
}

```

YAML

```

myASG:
  Type: AWS::AutoScaling::AutoScalingGroup
  DependsOn:
    - snsTopicForAutoScalingGroup
  Properties:
    VPCZoneIdentifier:
      - subnetIdAz1
      - subnetIdAz2
      - subnetIdAz3
    LaunchTemplate:
      LaunchTemplateId: !Ref logicalName
      Version: !GetAtt logicalName.LatestVersionNumber
    MaxSize: '5'
    MinSize: '1'
    NotificationConfigurations:
      - TopicARN: !Ref snsTopicForAutoScalingGroup
        NotificationTypes:
          - autoscaling:EC2_INSTANCE_LAUNCH
          - autoscaling:EC2_INSTANCE_LAUNCH_ERROR
          - autoscaling:EC2_INSTANCE_TERMINATE
          - autoscaling:EC2_INSTANCE_TERMINATE_ERROR
          - autoscaling:TEST_NOTIFICATION

```

Crea un gruppo Auto Scaling che utilizza un e un **CreationPolicyUpdatePolicy**

L'esempio seguente mostra come aggiungere CreationPolicy UpdatePolicy attributi a una [AWS::AutoScaling::AutoScalingGroup](#) risorsa.

La politica di creazione del campione impedisce al gruppo Auto Scaling di raggiungere CREATE_COMPLETE lo stato finché non AWS CloudFormation riceve un Count numero di segnali di successo quando il gruppo è pronto. Per segnalare che il gruppo con scalabilità automatica è pronto, sulle istanze viene eseguito uno script helper `cfn-signal` aggiunto ai dati utente del modello di avvio (non visualizzato). Se le istanze non inviano un segnale entro il limite specificato `Timeout`,

CloudFormation presuppone che le istanze non siano state create, la creazione della risorsa fallisce e ripristina lo stack CloudFormation .

La politica di aggiornamento di esempio indica di CloudFormation eseguire un aggiornamento continuo utilizzando la proprietà. `AutoScalingRollingUpdate` L'aggiornamento in sequenza modifica il gruppo con dimensionamento automatico in piccoli batch (per questo esempio, istanza per istanza) in base a `MaxBatchSize` e alla pausa che intercorre tra i batch di aggiornamento in base al `PauseTime`. L'`MinInstancesInService` attributo specifica il numero minimo di istanze che devono essere in servizio all'interno del gruppo Auto Scaling CloudFormation durante l'aggiornamento delle vecchie istanze.

L'attributo `WaitOnResourceSignals` viene impostato su `true`. CloudFormation deve ricevere un segnale da ogni nuova istanza entro il `PauseTime` specificato prima di procedere con l'aggiornamento. Durante l'aggiornamento dello stack, i seguenti processi di EC2 Auto Scaling sono sospesi: `HealthCheck:ReplaceUnhealthy`, `AZRebalanceAlarmNotification`, e `ScheduledActions` Nota: non sospendere i tipi di processo `Launch`, `Terminate`, o `AddToLoadBalancer` (se il Auto Scaling gruppo viene utilizzato con Elastic Load Balancing) perché in tal modo è possibile impedire il corretto funzionamento dell'aggiornamento in sequenza.

La proprietà `VPCZoneIdentifier` del gruppo con scalabilità automatica specifica un elenco di sottoreti esistenti in diverse zone di disponibilità. È necessario specificare la sottorete applicabile IDs dal proprio account prima di creare lo stack. La `LaunchTemplate` proprietà fa riferimento al nome logico di una [AWS::EC2::LaunchTemplate](#) risorsa dichiarata altrove nello stesso modello.

Per ulteriori informazioni sugli `UpdatePolicy` attributi `CreationPolicy` and, vedete [Resource attribute reference](#).

JSON

```
{
  "Resources": {
    "myASG": {
      "CreationPolicy": {
        "ResourceSignal": {
          "Count": "3",
          "Timeout": "PT15M"
        }
      },
      "UpdatePolicy": {
        "AutoScalingRollingUpdate": {
```

```

        "MinInstancesInService": "3",
        "MaxBatchSize": "1",
        "PauseTime": "PT12M5S",
        "WaitOnResourceSignals": "true",
        "SuspendProcesses": [
            "HealthCheck",
            "ReplaceUnhealthy",
            "AZRebalance",
            "AlarmNotification",
            "ScheduledActions",
            "InstanceRefresh"
        ]
    },
    "Type": "AWS::AutoScaling::AutoScalingGroup",
    "Properties": {
        "VPCZoneIdentifier": [ "subnetIdAz1", "subnetIdAz2", "subnetIdAz3" ],
        "LaunchTemplate": {
            "LaunchTemplateId": {
                "Ref": "logicalName"
            },
            "Version": {
                "Fn::GetAtt": [
                    "logicalName",
                    "LatestVersionNumber"
                ]
            }
        },
        "MaxSize": "5",
        "MinSize": "3"
    }
}
}
}
}

```

YAML

```

---
Resources:
  myASG:
    CreationPolicy:
      ResourceSignal:
        Count: '3'

```

```
    Timeout: PT15M
  UpdatePolicy:
    AutoScalingRollingUpdate:
      MinInstancesInService: '3'
      MaxBatchSize: '1'
      PauseTime: PT12M5S
      WaitOnResourceSignals: true
      SuspendProcesses:
        - HealthCheck
        - ReplaceUnhealthy
        - AZRebalance
        - AlarmNotification
        - ScheduledActions
        - InstanceRefresh
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    VPCZoneIdentifier:
      - subnetIdAz1
      - subnetIdAz2
      - subnetIdAz3
    LaunchTemplate:
      LaunchTemplateId: !Ref logicalName
      Version: !GetAtt logicalName.LatestVersionNumber
    MaxSize: '5'
    MinSize: '3'
```

Creazione di una policy di dimensionamento per fasi

Questo esempio mostra una [AWS::AutoScaling::ScalingPolicy](#) risorsa che ridimensiona il gruppo Auto Scaling utilizzando una politica di scalabilità a fasi. La proprietà `AdjustmentType` specifica `ChangeInCapacity`, il che significa che `ScalingAdjustment` rappresenta il numero di istanze da aggiungere (se `ScalingAdjustment` è positiva) o eliminare (se è negativa). In questo esempio, `ScalingAdjustment` è 1; pertanto, la policy incrementa di 1 il numero di EC2 istanze nel gruppo quando viene superata la soglia di allarme.

La [AWS::CloudWatch::Alarm](#) risorsa `CPUAlarmHigh` specifica la politica di scalabilità `ASGScalingPolicyHigh` come azione da eseguire quando l'allarme si trova in uno stato `ALARM` (). La `AlarmActions` proprietà fa riferimento al nome logico di una [AWS::AutoScaling::AutoScalingGroup](#) risorsa dichiarata altrove nello stesso modello.

JSON

```
{
  "Resources":{
    "ASGScalingPolicyHigh":{
      "Type":"AWS::AutoScaling::ScalingPolicy",
      "Properties":{
        "AutoScalingGroupName":{ "Ref":"logicalName" },
        "PolicyType":"StepScaling",
        "AdjustmentType":"ChangeInCapacity",
        "StepAdjustments":[
          {
            "MetricIntervalLowerBound":0,
            "ScalingAdjustment":1
          }
        ]
      }
    },
    "CPULAlarmHigh":{
      "Type":"AWS::CloudWatch::Alarm",
      "Properties":{
        "EvaluationPeriods":"2",
        "Statistic":"Average",
        "Threshold":"90",
        "AlarmDescription":"Scale out if CPU > 90% for 2 minutes",
        "Period":"60",
        "AlarmActions":[ { "Ref":"ASGScalingPolicyHigh" } ],
        "Namespace":"AWS/EC2",
        "Dimensions":[
          {
            "Name":"AutoScalingGroupName",
            "Value":{ "Ref":"logicalName" }
          }
        ],
        "ComparisonOperator":"GreaterThanThreshold",
        "MetricName":"CPUUtilization"
      }
    }
  }
}
```

YAML

```

---
Resources:
  ASGScalingPolicyHigh:
    Type: AWS::AutoScaling::ScalingPolicy
    Properties:
      AutoScalingGroupName: !Ref logicalName
      PolicyType: StepScaling
      AdjustmentType: ChangeInCapacity
      StepAdjustments:
        - MetricIntervalLowerBound: 0
          ScalingAdjustment: 1
  CPUAlarmHigh:
    Type: AWS::CloudWatch::Alarm
    Properties:
      EvaluationPeriods: 2
      Statistic: Average
      Threshold: 90
      AlarmDescription: 'Scale out if CPU > 90% for 2 minutes'
      Period: 60
      AlarmActions:
        - !Ref ASGScalingPolicyHigh
      Namespace: AWS/EC2
      Dimensions:
        - Name: AutoScalingGroupName
          Value:
            !Ref logicalName
      ComparisonOperator: GreaterThanThreshold
      MetricName: CPUUtilization

```

Consulta anche

Per altri modelli di esempio per le policy di dimensionamento, consulta la sezione [Esempi](#) nella risorsa `AWS::AutoScaling::ScalingPolicy`.

Esempi di gruppi di istanze miste

Create an Auto Scaling group using attribute-based instance type selection

Questo esempio mostra una [AWS::AutoScaling::AutoScalingGroup](#) risorsa che contiene le informazioni per avviare un gruppo di istanze miste utilizzando la selezione del tipo di istanza basata sugli attributi. Puoi specificare il valore minimo e massimo per la proprietà `VCpuCount` e il

valore minimo per la proprietà `MemoryMiB`. Tutti i tipi di istanza utilizzati dal gruppo con scalabilità automatica devono rispettare agli attributi dell'istanza richiesti.

La proprietà `VPCZoneIdentifier` del gruppo con scalabilità automatica specifica un elenco di sottoreti esistenti in diverse zone di disponibilità. È necessario specificare la sottorete applicabile IDs dal vostro account prima di creare lo stack. La `LaunchTemplate` proprietà fa riferimento al nome logico di una [AWS::EC2::LaunchTemplate](#) risorsa dichiarata altrove nello stesso modello.

JSON

```
{
  "Resources": {
    "myASG": {
      "Type": "AWS::AutoScaling::AutoScalingGroup",
      "Properties": {
        "VPCZoneIdentifier": [
          "subnetIdAz1",
          "subnetIdAz2",
          "subnetIdAz3"
        ],
        "MixedInstancesPolicy": {
          "LaunchTemplate": {
            "LaunchTemplateSpecification": {
              "LaunchTemplateId": {
                "Ref": "logicalName"
              },
              "Version": {
                "Fn::GetAtt": [
                  "logicalName",
                  "LatestVersionNumber"
                ]
              }
            }
          },
          "Overrides": [
            {
              "InstanceRequirements": {
                "VCpuCount": {
                  "Min": 2,
                  "Max": 4
                },
                "MemoryMiB": {
                  "Min": 2048
                }
              }
            }
          ]
        }
      }
    }
  }
}
```

```

    }
  }
]
},
"MaxSize": "5",
"MinSize": "1"
}
}
}
}

```

YAML

```

---
Resources:
  myASG:
    Type: AWS::AutoScaling::AutoScalingGroup
    Properties:
      VPCZoneIdentifier:
        - subnetIdAz1
        - subnetIdAz2
        - subnetIdAz3
      MixedInstancesPolicy:
        LaunchTemplate:
          LaunchTemplateSpecification:
            LaunchTemplateId: !Ref logicalName
            Version: !GetAtt logicalName.LatestVersionNumber
          Overrides:
            - InstanceRequirements:
                VCpuCount:
                  Min: 2
                  Max: 4
                MemoryMiB:
                  Min: 2048
      MaxSize: '5'
      MinSize: '1'

```

Esempi di configurazione di avvio

Creazione di una configurazione di avvio

Questo esempio mostra una [AWS::AutoScaling::LaunchConfiguration](#) risorsa per un gruppo Auto Scaling in cui si specificano i valori per le proprietà `ImageId`, `InstanceType`, e `SecurityGroups`. La `SecurityGroups` proprietà specifica sia il nome logico di una [AWS::EC2::SecurityGroup](#) risorsa specificato altrove nel modello, sia un gruppo di EC2 sicurezza esistente denominato `myExistingEC2SecurityGroup`.

JSON

```
"mySimpleConfig" : {
  "Type" : "AWS::AutoScaling::LaunchConfiguration",
  "Properties" : {
    "ImageId" : "ami-02354e95b3example",
    "InstanceType" : "t3.micro",
    "SecurityGroups" : [ { "Ref" : "logicalName" }, "myExistingEC2SecurityGroup" ]
  }
}
```

YAML

```
mySimpleConfig:
  Type: AWS::AutoScaling::LaunchConfiguration
  Properties:
    ImageId: ami-02354e95b3example
    InstanceType: t3.micro
    SecurityGroups:
      - !Ref logicalName
      - myExistingEC2SecurityGroup
```

Creare un gruppo Auto Scaling che utilizza una configurazione di avvio

Questo esempio mostra una [AWS::AutoScaling::AutoScalingGroup](#) risorsa con una singola istanza. La proprietà `VPCZoneIdentifier` del gruppo con scalabilità automatica specifica un elenco di sottoreti esistenti in diverse zone di disponibilità. È necessario specificare la sottorete applicabile IDs dal vostro account prima di creare lo stack. La `LaunchConfigurationName` proprietà fa riferimento a una [AWS::AutoScaling::LaunchConfiguration](#) risorsa con il nome `mySimpleConfig` logico definito nel modello.

JSON

```
"myASG" : {
  "Type" : "AWS::AutoScaling::AutoScalingGroup",
  "Properties" : {
    "VPCZoneIdentifier" : [ "subnetIdAz1", "subnetIdAz2", "subnetIdAz3" ],
    "LaunchConfigurationName" : { "Ref" : "mySimpleConfig" },
    "MaxSize" : "1",
    "MinSize" : "1"
  }
}
```

YAML

```
myASG:
  Type: AWS::AutoScaling::AutoScalingGroup
  Properties:
    VPCZoneIdentifier:
      - subnetIdAz1
      - subnetIdAz2
      - subnetIdAz3
    LaunchConfigurationName: !Ref mySimpleConfig
    MaxSize: '1'
    MinSize: '1'
```

Configura le risorse di Application Auto Scaling con AWS CloudFormation

Questa sezione fornisce esempi di AWS CloudFormation modelli per le politiche di scalabilità di Application Auto Scaling e le azioni pianificate per diverse risorse. AWS

Important

Quando nel modello è incluso uno snippet di Application Auto Scaling, potrebbe essere necessario dichiarare una dipendenza dalla risorsa scalabile specifica creata tramite il modello utilizzando l'attributo. `DependsOn` Questo sovrascrive il parallelismo predefinito e indirizza AWS CloudFormation a operare sulle risorse in un ordine specifico. In caso contrario, la configurazione di ridimensionamento potrebbe essere applicata prima che la risorsa sia stata configurata completamente.

Per ulteriori informazioni, consulta [Attributo DependsOn](#).

Categorie dei frammenti

- [Crea una politica di scalabilità per una flotta AppStream](#)
- [Crea una politica di scalabilità per un cluster Aurora DB](#)
- [Creare una politica di scalabilità per una tabella DynamoDB](#)
- [Crea una politica di scalabilità per un servizio Amazon ECS \(parametri: CPU e memoria medie\)](#)
- [Crea una politica di scalabilità per un servizio Amazon ECS \(metrica: numero medio di richieste per target\)](#)
- [Crea un'azione pianificata con un'espressione cron per una funzione Lambda](#)
- [Crea un'azione pianificata con un'espressione per una flotta Spot at](#)

Crea una politica di scalabilità per una flotta AppStream

Questo frammento mostra come creare una policy e applicarla a una

[AWS::AppStream::Fleet](#) risorsa che utilizza la risorsa.

[AWS::ApplicationAutoScaling::ScalingPolicy](#) La

[AWS::ApplicationAutoScaling::ScalableTarget](#) risorsa dichiara un obiettivo scalabile a cui viene applicata questa politica. Application Auto Scaling può scalare il numero di istanze del parco istanze a un minimo di un'istanza e un massimo di 20. La policy mantiene l'utilizzo medio della capacità del parco istanze al 75%, con tempi di raffreddamento delle operazioni di dimensionamento di 300 secondi (5 minuti).

Utilizza `Fn::Join` le funzioni Rev intrinseche per costruire la `ResourceId` proprietà con il nome logico della `AWS::AppStream::Fleet` risorsa specificato nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

JSON

```
{
  "Resources" : {
    "ScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : 20,
        "MinCapacity" : 1,
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam:${AWS::AccountId}:role/
aws-service-role/appstream.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_AppStreamFleet" },
        "ServiceNamespace" : "appstream",
```

```

    "ScalableDimension" : "appstream:fleet:DesiredCapacity",
    "ResourceId" : {
      "Fn::Join" : [
        "/",
        [
          "fleet",
          {
            "Ref" : "logicalName"
          }
        ]
      ]
    }
  },
  "ScalingPolicyAppStreamFleet" : {
    "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",
    "Properties" : {
      "PolicyName" : { "Fn::Sub" : "${AWS::StackName}-target-tracking-cpu75" },
      "PolicyType" : "TargetTrackingScaling",
      "ServiceNamespace" : "appstream",
      "ScalableDimension" : "appstream:fleet:DesiredCapacity",
      "ResourceId" : {
        "Fn::Join" : [
          "/",
          [
            "fleet",
            {
              "Ref" : "logicalName"
            }
          ]
        ]
      }
    },
    "TargetTrackingScalingPolicyConfiguration" : {
      "TargetValue" : 75,
      "PredefinedMetricSpecification" : {
        "PredefinedMetricType" : "AppStreamAverageCapacityUtilization"
      },
      "ScaleInCooldown" : 300,
      "ScaleOutCooldown" : 300
    }
  }
}

```


}

YAML

```

---
Resources:
  ScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 20
      MinCapacity: 1
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-
service-role/appstream.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_AppStreamFleet'
      ServiceNamespace: appstream
      ScalableDimension: appstream:fleet:DesiredCapacity
      ResourceId: !Join
        - /
        - - fleet
          - !Ref logicalName
  ScalingPolicyAppStreamFleet:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    Properties:
      PolicyName: !Sub ${AWS::StackName}-target-tracking-cpu75
      PolicyType: TargetTrackingScaling
      ServiceNamespace: appstream
      ScalableDimension: appstream:fleet:DesiredCapacity
      ResourceId: !Join
        - /
        - - fleet
          - !Ref logicalName
      TargetTrackingScalingPolicyConfiguration:
        TargetValue: 75
        PredefinedMetricSpecification:
          PredefinedMetricType: AppStreamAverageCapacityUtilization
        ScaleInCooldown: 300
        ScaleOutCooldown: 300

```

Crea una politica di scalabilità per un cluster Aurora DB

In questo frammento, registri una risorsa. [AWS::RDS::DBCluster](#) La [AWS::ApplicationAutoScaling::ScalableTarget](#) risorsa indica che il cluster DB

deve essere ridimensionato dinamicamente per avere da una a otto repliche Aurora. Inoltre, applichi una politica di scalabilità del tracciamento degli obiettivi al cluster che utilizza la risorsa.

[AWS::ApplicationAutoScaling::ScalingPolicy](#)

In questa configurazione, il parametro predefinito `RDSReaderAverageCPUUtilization` viene utilizzato per regolare un cluster di database Aurora; in base a un utilizzo medio della CPU del 40 per cento in tutte le repliche Aurora; in quel cluster di database Aurora. La configurazione fornisce un periodo di attesa di riduzione di 10 minuti e un periodo di attesa di aumento di 5 minuti.

Questo esempio utilizza la funzione `Fn::Sub` intrinseca per costruire la `ResourceId` proprietà con il nome logico della `AWS::RDS::DBCluster` risorsa specificata nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

JSON

```
{
  "Resources" : {
    "ScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : 8,
        "MinCapacity" : 1,
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam:${AWS::AccountId}:role/
aws-service-role/rds.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_RDSCluster" },
        "ServiceNamespace" : "rds",
        "ScalableDimension" : "rds:cluster:ReadReplicaCount",
        "ResourceId" : { "Fn::Sub" : "cluster:${logicalName}" }
      }
    },
    "ScalingPolicyDBCluster" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",
      "Properties" : {
        "PolicyName" : { "Fn::Sub" : "${AWS::StackName}-target-tracking-cpu40" },
        "PolicyType" : "TargetTrackingScaling",
        "ServiceNamespace" : "rds",
        "ScalableDimension" : "rds:cluster:ReadReplicaCount",
        "ResourceId" : { "Fn::Sub" : "cluster:${logicalName}" },
        "TargetTrackingScalingPolicyConfiguration" : {
          "TargetValue" : 40,
          "PredefinedMetricSpecification" : {
            "PredefinedMetricType" : "RDSReaderAverageCPUUtilization"
          }
        }
      }
    }
  }
}
```

```

        "ScaleInCooldown" : 600,
        "ScaleOutCooldown" : 300
    }
}
}
}
}

```

YAML

```

---
Resources:
  ScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 8
      MinCapacity: 1
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/rds.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_RDSCluster'
      ServiceNamespace: rds
      ScalableDimension: rds:cluster:ReadReplicaCount
      ResourceId: !Sub cluster:${logicalName}
  ScalingPolicyDBCluster:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    Properties:
      PolicyName: !Sub ${AWS::StackName}-target-tracking-cpu40
      PolicyType: TargetTrackingScaling
      ServiceNamespace: rds
      ScalableDimension: rds:cluster:ReadReplicaCount
      ResourceId: !Sub cluster:${logicalName}
      TargetTrackingScalingPolicyConfiguration:
        TargetValue: 40
        PredefinedMetricSpecification:
          PredefinedMetricType: RDSReaderAverageCPUUtilization
        ScaleInCooldown: 600
        ScaleOutCooldown: 300

```

Creare una politica di scalabilità per una tabella DynamoDB

Questo frammento mostra come creare una policy con il `TargetTrackingScaling` tipo di policy e applicarla a una [AWS::DynamoDB::Table](#) risorsa che utilizza la risorsa. [AWS::ApplicationAutoScaling::ScalingPolicy](#) La

[`AWS::ApplicationAutoScaling::ScalableTarget`](#) risorsa dichiara un obiettivo scalabile a cui viene applicata questa politica, con un minimo di cinque unità di capacità di scrittura e un massimo di 15. La policy di dimensionamento ridimensiona la capacità di throughput di scrittura della tabella per mantenere l'utilizzo target al 50% in base al parametro predefinito `DynamoDBWriteCapacityUtilization`.

Utilizza `Fn::Join` le funzioni `Ref` intrinseche per costruire la `ResourceId` proprietà con il nome logico della `AWS::DynamoDB::Table` risorsa specificata nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

Note

Per ulteriori informazioni su come creare un AWS CloudFormation modello per le risorse DynamoDB, consulta il [post del blog How to use AWS CloudFormation to configure auto scaling for Amazon DynamoDB tables and index on the Database Blog](#). AWS

JSON

```
{
  "Resources" : {
    "WriteCapacityScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : 15,
        "MinCapacity" : 5,
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam::${AWS::AccountId}:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable" },
        "ServiceNamespace" : "dynamodb",
        "ScalableDimension" : "dynamodb:table:WriteCapacityUnits",
        "ResourceId" : {
          "Fn::Join" : [
            "/",
            [
              "table",
              {
                "Ref" : "logicalName"
              }
            ]
          ]
        }
      }
    }
  }
}
```

```
    }  
  }  
},  
"WriteScalingPolicy" : {  
  "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",  
  "Properties" : {  
    "PolicyName" : "WriteScalingPolicy",  
    "PolicyType" : "TargetTrackingScaling",  
    "ScalingTargetId" : { "Ref" : "WriteCapacityScalableTarget" },  
    "TargetTrackingScalingPolicyConfiguration" : {  
      "TargetValue" : 50.0,  
      "ScaleInCooldown" : 60,  
      "ScaleOutCooldown" : 60,  
      "PredefinedMetricSpecification" : {  
        "PredefinedMetricType" : "DynamoDBWriteCapacityUtilization"  
      }  
    }  
  }  
}  
}  
}
```

YAML

```

---
Resources:
  WriteCapacityScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 15
      MinCapacity: 5
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-
service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable'
      ServiceNamespace: dynamodb
      ScalableDimension: dynamodb:table:WriteCapacityUnits
      ResourceId: !Join
        - /
        - - table
          - !Ref LogicalName
    WriteScalingPolicy:
      Type: AWS::ApplicationAutoScaling::ScalingPolicy

```

Properties:

```

PolicyName: WriteScalingPolicy
PolicyType: TargetTrackingScaling
ScalingTargetId: !Ref WriteCapacityScalableTarget
TargetTrackingScalingPolicyConfiguration:
  TargetValue: 50.0
  ScaleInCooldown: 60
  ScaleOutCooldown: 60
  PredefinedMetricSpecification:
    PredefinedMetricType: DynamoDBWriteCapacityUtilization

```

Crea una politica di scalabilità per un servizio Amazon ECS (parametri: CPU e memoria medie)

Questo frammento mostra come creare una policy e applicarla a una risorsa che utilizza la risorsa [AWS::ECS::Service](#) [AWS::ApplicationAutoScaling::ScalingPolicy](#). La [AWS::ApplicationAutoScaling::ScalableTarget](#) risorsa dichiara un obiettivo scalabile a cui viene applicata questa politica. Dimensionamento automatico delle applicazioni può ridimensionare il numero di attività a un minimo di 1 e un massimo di 6.

Vengono creati due criteri di ridimensionamento con il tipo di criterio `TargetTrackingScaling`. Le policy vengono utilizzate per dimensionare il servizio ECS in base all'utilizzo medio della CPU e della memoria del servizio. Utilizza `Fn::Join` le funzioni `Ref` intrinseche per costruire la `ResourceId` proprietà con i nomi logici delle risorse [AWS::ECS::Cluster](#) (`myContainerCluster`) e `AWS::ECS::Service` (`myService`) specificate nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

JSON

```

{
  "Resources" : {
    "ECSScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : "6",
        "MinCapacity" : "1",
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam::${AWS::AccountId}:role/
aws-service-role/ecs.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_ECSService" },
        "ServiceNamespace" : "ecs",
        "ScalableDimension" : "ecs:service:DesiredCount",
        "ResourceId" : {
          "Fn::Join" : [

```

```

        "/",
        [
            "service",
            {
                "Ref" : "myContainerCluster"
            },
            {
                "Fn::GetAtt" : [
                    "myService",
                    "Name"
                ]
            }
        ]
    ]
}
},
"ServiceScalingPolicyCPU" : {
    "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",
    "Properties" : {
        "PolicyName" : { "Fn::Sub" : "${AWS::StackName}-target-tracking-cpu70" },
        "PolicyType" : "TargetTrackingScaling",
        "ScalingTargetId" : { "Ref" : "ECSScalableTarget" },
        "TargetTrackingScalingPolicyConfiguration" : {
            "TargetValue" : 70.0,
            "ScaleInCooldown" : 180,
            "ScaleOutCooldown" : 60,
            "PredefinedMetricSpecification" : {
                "PredefinedMetricType" : "ECSServiceAverageCPUUtilization"
            }
        }
    }
},
"ServiceScalingPolicyMem" : {
    "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",
    "Properties" : {
        "PolicyName" : { "Fn::Sub" : "${AWS::StackName}-target-tracking-mem90" },
        "PolicyType" : "TargetTrackingScaling",
        "ScalingTargetId" : { "Ref" : "ECSScalableTarget" },
        "TargetTrackingScalingPolicyConfiguration" : {
            "TargetValue" : 90.0,
            "ScaleInCooldown" : 180,
            "ScaleOutCooldown" : 60,
            "PredefinedMetricSpecification" : {

```

```

        "PredefinedMetricType" : "ECSServiceAverageMemoryUtilization"
    }
}
}
}
}
}
}

```

YAML

```

---
Resources:
  ECSScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 6
      MinCapacity: 1
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/ecs.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_ECSService'
      ServiceNamespace: ecs
      ScalableDimension: 'ecs:service:DesiredCount'
      ResourceId: !Join
        - /
        - - service
          - !Ref myContainerCluster
          - !GetAtt myService.Name
  ServiceScalingPolicyCPU:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    Properties:
      PolicyName: !Sub ${AWS::StackName}-target-tracking-cpu70
      PolicyType: TargetTrackingScaling
      ScalingTargetId: !Ref ECSScalableTarget
      TargetTrackingScalingPolicyConfiguration:
        TargetValue: 70.0
        ScaleInCooldown: 180
        ScaleOutCooldown: 60
        PredefinedMetricSpecification:
          PredefinedMetricType: ECSServiceAverageCPUUtilization
  ServiceScalingPolicyMem:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    Properties:
      PolicyName: !Sub ${AWS::StackName}-target-tracking-mem90

```



```

PolicyType: TargetTrackingScaling
ScalingTargetId: !Ref ECSScalableTarget
TargetTrackingScalingPolicyConfiguration:
  TargetValue: 90.0
  ScaleInCooldown: 180
  ScaleOutCooldown: 60
  PredefinedMetricSpecification:
    PredefinedMetricType: ECSServiceAverageMemoryUtilization

```

Crea una politica di scalabilità per un servizio Amazon ECS (metrica: numero medio di richieste per target)

Nell'esempio seguente viene applicato a un servizio ECS un criterio di scalabilità di tracciamento della destinazione con il parametro predefinito `ALBRequestCountPerTarget`. La policy viene utilizzata per aggiungere capacità al servizio ECS quando il conteggio di richieste per target (al minuto) supera il valore previsto. Poiché il valore di `DisableScaleIn` è impostato su `true`, la policy di monitoraggio target non rimuoverà capacità dal target scalabile.

Utilizza `Fn::Join` le funzioni `Fn::GetAtt` intrinseche per costruire la `ResourceLabel` proprietà con i nomi logici delle risorse

[`AWS::ElasticLoadBalancingV2::LoadBalancer`](#)(`myLoadBalancer`) e

[`AWS::ElasticLoadBalancingV2::TargetGroup`](#)(`myTargetGroup`) specificate nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

Le proprietà `MaxCapacity` e `MinCapacity` della destinazione scalabile e la proprietà `TargetValue` dei valori dei parametri di riferimento del criterio di ridimensionamento che vengono passati al modello durante la creazione o l'aggiornamento di uno stack.

JSON

```

{
  "Resources" : {
    "ECSScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : { "Ref" : "MaxCount" },
        "MinCapacity" : { "Ref" : "MinCount" },
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam:${AWS::AccountId}:role/
aws-service-role/ecs.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_ECSService" },
        "ServiceNamespace" : "ecs",
        "ScalableDimension" : "ecs:service:DesiredCount",

```

```

    "ResourceId" : {
      "Fn::Join" : [
        "/",
        [
          "service",
          {
            "Ref" : "myContainerCluster"
          },
          {
            "Fn::GetAtt" : [
              "myService",
              "Name"
            ]
          }
        ]
      ]
    }
  },
  "ServiceScalingPolicyALB" : {
    "Type" : "AWS::ApplicationAutoScaling::ScalingPolicy",
    "Properties" : {
      "PolicyName" : "alb-requests-per-target-per-minute",
      "PolicyType" : "TargetTrackingScaling",
      "ScalingTargetId" : { "Ref" : "ECSScalableTarget" },
      "TargetTrackingScalingPolicyConfiguration" : {
        "TargetValue" : { "Ref" : "ALBPolicyTargetValue" },
        "ScaleInCooldown" : 180,
        "ScaleOutCooldown" : 30,
        "DisableScaleIn" : true,
        "PredefinedMetricSpecification" : {
          "PredefinedMetricType" : "ALBRequestCountPerTarget",
          "ResourceLabel" : {
            "Fn::Join" : [
              "/",
              [
                {
                  "Fn::GetAtt" : [
                    "myLoadBalancer",
                    "LoadBalancerFullName"
                  ]
                }
              ]
            ],
            {
              "Fn::GetAtt" : [

```

```
"myTargetGroup",  
"TargetGroupName"  
]  
}  
]  
]  
}  
}  
}  
}  
}  
}  
}
```

YAML

```

---
Resources:
  ECSScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: !Ref MaxCount
      MinCapacity: !Ref MinCount
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/ecs.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_ECSService'
      ServiceNamespace: ecs
      ScalableDimension: 'ecs:service:DesiredCount'
      ResourceId: !Join
        - /
        - - service
          - !Ref myContainerCluster
          - !GetAtt myService.Name
  ServiceScalingPolicyALB:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    Properties:
      PolicyName: alb-requests-per-target-per-minute
      PolicyType: TargetTrackingScaling
      ScalingTargetId: !Ref ECSScalableTarget
      TargetTrackingScalingPolicyConfiguration:
        TargetValue: !Ref ALBPolicyTargetValue
        ScaleInCooldown: 180
        ScaleOutCooldown: 30

```

```

DisableScaleIn: true
PredefinedMetricSpecification:
  PredefinedMetricType: ALBRequestCountPerTarget
  ResourceLabel: !Join
    - '/'
    - - !GetAtt myLoadBalancer.LoadBalancerFullName
      - !GetAtt myTargetGroup.TargetGroupFullName

```

Crea un'azione pianificata con un'espressione cron per una funzione Lambda

Questo frammento registra la concorrenza fornita per una funzione alias () denominata utilizzando la risorsa. [AWS::Lambda::AliasBLUEAWS::ApplicationAutoScaling::ScalableTarget](#) Viene creata anche un'operazione pianificata con una pianificazione ricorrente utilizzando un'espressione cron. Il fuso orario per la pianificazione ricorrente è UTC.

Utilizza Fn::Join le funzioni Ref intrinseche della RoleARN proprietà per specificare l'ARN del ruolo collegato al servizio. Utilizza la funzione Fn::Sub intrinseca per costruire la ResourceId proprietà con il nome logico della [AWS::Serverless::Function](#) risorsa [AWS::Lambda::Function](#) specificata nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

Note

Non è possibile allocare la concorrenza assegnata su un alias che punta alla versione non pubblicata (). \$LATEST

Per ulteriori informazioni su come creare un AWS CloudFormation modello per le risorse Lambda, consulta il post di blog [Scheduling AWS Lambda Provisioned Concurrency for recurring peak usage on the Compute Blog](#). AWS

JSON

```

{
  "ScalableTarget" : {
    "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
    "Properties" : {
      "MaxCapacity" : 250,
      "MinCapacity" : 0,
      "RoleARN" : {
        "Fn::Join" : [

```

```

        ":",
        [
            "arn:aws:iam:",
            {
                "Ref" : "AWS::AccountId"
            },
            "role/aws-service-role/lambda.application-autoscaling.amazonaws.com/"
        ],
        "AWS::ServiceRoleForApplicationAutoScaling_LambdaConcurrency"
    ],
    ],
    },
    "ServiceNamespace" : "lambda",
    "ScalableDimension" : "lambda:function:ProvisionedConcurrency",
    "ResourceId" : { "Fn::Sub" : "function:${logicalName}:BLUE" },
    "ScheduledActions" : [
        {
            "ScalableTargetAction" : {
                "MinCapacity" : "250"
            },
            "ScheduledActionName" : "my-scale-out-scheduled-action",
            "Schedule" : "cron(0 18 * * ? *)",
            "EndTime" : "2022-12-31T12:00:00.000Z"
        }
    ]
}
}
}
}

```

YAML

```

ScalableTarget:
  Type: AWS::ApplicationAutoScaling::ScalableTarget
  Properties:
    MaxCapacity: 250
    MinCapacity: 0
    RoleARN: !Join
      - ':'
      - - 'arn:aws:iam:'
        - !Ref 'AWS::AccountId'
        - role/aws-service-role/lambda.application-autoscaling.amazonaws.com/
    AWS::ServiceRoleForApplicationAutoScaling_LambdaConcurrency
    ServiceNamespace: lambda
    ScalableDimension: lambda:function:ProvisionedConcurrency

```

```

ResourceId: !Sub function:${logicalName}:BLUE
ScheduledActions:
  - ScalableTargetAction:
      MinCapacity: 250
      ScheduledActionName: my-scale-out-scheduled-action
      Schedule: 'cron(0 18 * * ? *)'
      EndTime: '2022-12-31T12:00:00.000Z'

```

Crea un'azione pianificata con un'espressione per una flotta Spot **at**

Questo frammento mostra come creare due azioni pianificate che si verificano una sola volta per una [AWS::EC2::SpotFleet](#) risorsa che utilizza la [AWS::ApplicationAutoScaling::ScalableTarget](#) risorsa. Il fuso orario per ogni operazione pianificata occasionale è UTC.

Utilizza `Fn::Join` le funzioni `Ref` intrinseche per costruire la `ResourceId` proprietà con il nome logico della `AWS::EC2::SpotFleet` risorsa specificato nello stesso modello. Per ulteriori informazioni, vedere Riferimento alla funzione [intrinseca](#).

Note

La richiesta della serie di istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste `one-time` o i blocchi Spot.

JSON

```

{
  "Resources" : {
    "SpotFleetScalableTarget" : {
      "Type" : "AWS::ApplicationAutoScaling::ScalableTarget",
      "Properties" : {
        "MaxCapacity" : 0,
        "MinCapacity" : 0,
        "RoleARN" : { "Fn::Sub" : "arn:aws:iam::${AWS::AccountId}:role/aws-service-role/ec2.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest" },
        "ServiceNamespace" : "ec2",
        "ScalableDimension" : "ec2:spot-fleet-request:TargetCapacity",
        "ResourceId" : {
          "Fn::Join" : [
            "/",

```

```

        [
            "spot-fleet-request",
            {
                "Ref" : "logicalName"
            }
        ]
    ],
    "ScheduledActions" : [
        {
            "ScalableTargetAction" : {
                "MaxCapacity" : "10",
                "MinCapacity" : "10"
            },
            "ScheduledActionName" : "my-scale-out-scheduled-action",
            "Schedule" : "at(2022-05-20T13:00:00)"
        },
        {
            "ScalableTargetAction" : {
                "MaxCapacity" : "0",
                "MinCapacity" : "0"
            },
            "ScheduledActionName" : "my-scale-in-scheduled-action",
            "Schedule" : "at(2022-05-20T21:00:00)"
        }
    ]
}
}
}
}
}

```

YAML

```

---
Resources:
  SpotFleetScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 0
      MinCapacity: 0
      RoleARN:
        Fn::Sub: 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest'

```

```

ServiceNamespace: ec2
ScalableDimension: 'ec2:spot-fleet-request:TargetCapacity'
ResourceId: !Join
  - /
  - - spot-fleet-request
    - !Ref logicalName
ScheduledActions:
  - ScalableTargetAction:
      MaxCapacity: 10
      MinCapacity: 10
      ScheduledActionName: my-scale-out-scheduled-action
      Schedule: 'at(2022-05-20T13:00:00)'
  - ScalableTargetAction:
      MaxCapacity: 0
      MinCapacity: 0
      ScheduledActionName: my-scale-in-scheduled-action
      Schedule: 'at(2022-05-20T21:00:00)'

```

AWS Frammenti di modello della Billing Console

Questo esempio crea un piano tariffario con una regola di determinazione del prezzo di markup globale del 10%. Questo piano tariffario è collegato al gruppo di fatturazione. Il gruppo di fatturazione presenta anche due voci personalizzate che applicano un addebito di \$ 10 e un addebito del 10% oltre al costo totale del gruppo di fatturazione.

JSON

```

{
  "Parameters": {
    "LinkedAccountIds": {
      "Type": "ListNumber"
    },
    "PrimaryAccountId": {
      "Type": "Number"
    }
  },
  "Resources": {
    "TestPricingRule": {
      "Type": "AWS::BillingConductor::PricingRule",
      "Properties": {
        "Name": "TestPricingRule",
        "Description": "Test pricing rule created through Cloudformation. Mark
everything by 10%.",

```



```

        "Type": "MARKUP",
        "Scope": "GLOBAL",
        "ModifierPercentage": 10
    }
},
"TestPricingPlan": {
    "Type": "AWS::BillingConductor::PricingPlan",
    "Properties": {
        "Name": "TestPricingPlan",
        "Description": "Test pricing plan created through Cloudformation.",
        "PricingRuleArns": [
            {"Fn::GetAtt": ["TestPricingRule", "Arn"]}
        ]
    }
},
"TestBillingGroup": {
    "Type": "AWS::BillingConductor::BillingGroup",
    "Properties": {
        "Name": "TestBillingGroup",
        "Description": "Test billing group created through Cloudformation with 1
linked account. The linked account is also the primary account.",
        "PrimaryAccountId": {
            "Ref": "PrimaryAccountId"
        },
        "AccountGrouping": {
            "LinkedAccountIds": null
        },
        "ComputationPreference": {
            "PricingPlanArn": {
                "Fn::GetAtt": ["TestPricingPlan", "Arn"]
            }
        }
    }
},
"TestFlatCustomLineItem": {
    "Type": "AWS::BillingConductor::CustomLineItem",
    "Properties": {
        "Name": "TestFlatCustomLineItem",
        "Description": "Test flat custom line item created through Cloudformation
for a $10 charge.",
        "BillingGroupArn": {
            "Fn::GetAtt": ["TestBillingGroup", "Arn"]
        },
        "CustomLineItemChargeDetails": {

```

```
        "Flat": {
            "ChargeValue": 10
        },
        "Type": "FEE"
    }
}
},
"TestPercentageCustomLineItem": {
    "Type": "AWS::BillingConductor::CustomLineItem",
    "Properties": {
        "Name": "TestPercentageCustomLineItem",
        "Description": "Test percentage custom line item created through Cloudformation for a %10 additional charge on the overall total bill of the billing group.",
        "BillingGroupArn": {
            "Fn::GetAtt": ["TestBillingGroup", "Arn"]
        },
        "CustomLineItemChargeDetails": {
            "Percentage": {
                "PercentageValue": 10,
                "ChildAssociatedResources": [
                    {"Fn::GetAtt": ["TestBillingGroup", "Arn"]}
                ]
            },
            "Type": "FEE"
        }
    }
}
}
```

YAML

```
Parameters:
  LinkedAccountIds:
    Type: ListNumber
  PrimaryAccountId:
    Type: Number
Resources:
  TestPricingRule:
    Type: 'AWS::BillingConductor::PricingRule'
    Properties:
      Name: 'TestPricingRule'
```

```
    Description: 'Test pricing rule created through Cloudformation. Mark everything
by 10%.'
    Type: 'MARKUP'
    Scope: 'GLOBAL'
    ModifierPercentage: 10
TestPricingPlan:
  Type: 'AWS::BillingConductor::PricingPlan'
  Properties:
    Name: 'TestPricingPlan'
    Description: 'Test pricing plan created through Cloudformation.'
    PricingRuleArns:
      - !GetAtt TestPricingRule.Arn
TestBillingGroup:
  Type: 'AWS::BillingConductor::BillingGroup'
  Properties:
    Name: 'TestBillingGroup'
    Description: 'Test billing group created through Cloudformation with 1 linked
account. The linked account is also the primary account.'
    PrimaryAccountId: !Ref PrimaryAccountId
    AccountGrouping:
      LinkedAccountIds: !Ref LinkedAccountIds
    ComputationPreference:
      PricingPlanArn: !GetAtt TestPricingPlan.Arn
TestFlatCustomLineItem:
  Type: 'AWS::BillingConductor::CustomLineItem'
  Properties:
    Name: 'TestFlatCustomLineItem'
    Description: 'Test flat custom line item created through Cloudformation for a $10
charge.'
    BillingGroupArn: !GetAtt TestBillingGroup.Arn
    CustomLineItemChargeDetails:
      Flat:
        ChargeValue: 10
        Type: 'FEE'
TestPercentageCustomLineItem:
  Type: 'AWS::BillingConductor::CustomLineItem'
  Properties:
    Name: 'TestPercentageCustomLineItem'
    Description: 'Test percentage custom line item created through Cloudformation for
a %10 additional charge on the overall total bill of the billing group.'
    BillingGroupArn: !GetAtt TestBillingGroup.Arn
    CustomLineItemChargeDetails:
      Percentage:
        PercentageValue: 10
```

```
ChildAssociatedResources:
  - !GetAtt TestBillingGroup.Arn
Type: 'FEE'
```

AWS CloudFormation frammenti di modello

Argomenti

- [Stack nidificati](#)
- [Condizione di attesa](#)

Stack nidificati

Nidificazione di uno stack in un modello

Questo modello di esempio contiene una risorsa stack nidificata denominata myStack. Quando AWS CloudFormation crea uno stack dal modello, crea ilmyStack, il cui modello è specificato nella TemplateURL proprietà. Il valore di output StackRef restituisce l'ID dello stack per myStack e il valore OutputFromNestedStack restituisce il valore di output BucketName dalla risorsa myStack. Il Outputs.*nestedstackoutputname* formato è riservato per specificare i valori di output dagli stack annidati e può essere utilizzato ovunque all'interno del modello contenitore.

Per ulteriori informazioni, consulta [AWS::CloudFormation::Stack](#).

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "myStack" : {
      "Type" : "AWS::CloudFormation::Stack",
      "Properties" : {
        "TemplateURL" : "https://s3.amazonaws.com/cloudformation-templates-us-east-1/
S3_Bucket.template",
        "TimeoutInMinutes" : "60"
      }
    }
  },
  "Outputs": {
    "StackRef": {"Value": { "Ref" : "myStack"}},
    "OutputFromNestedStack" : {
```

```

        "Value" : { "Fn::GetAtt" : [ "myStack", "Outputs.BucketName" ] }
    }
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  myStack:
    Type: AWS::CloudFormation::Stack
    Properties:
      TemplateURL: https://s3.amazonaws.com/cloudformation-templates-us-east-1/
S3_Bucket.template
      TimeoutInMinutes: '60'
Outputs:
  StackRef:
    Value: !Ref myStack
  OutputFromNestedStack:
    Value: !GetAtt myStack.Outputs.BucketName

```

Nidificazione di un stack con i parametri di input in un modello

In questo esempio il modello contiene una risorsa di stack che specifica i parametri di input. Quando AWS CloudFormation crea uno stack da questo modello, utilizza le coppie di valori dichiarate all'interno della `Parameters` proprietà come parametri di input per il modello utilizzato per creare lo stack. `myStackWithParams` In questo esempio vengono specificati i parametri `InstanceType` e `KeyName`.

Per ulteriori informazioni, consulta [AWS::CloudFormation::Stack](#).

JSON

```

{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "myStackWithParams" : {
      "Type" : "AWS::CloudFormation::Stack",
      "Properties" : {
        "TemplateURL" : "https://s3.amazonaws.com/cloudformation-templates-us-east-1/EC2ChooseAMI.template",
        "Parameters" : {

```

```
        "InstanceType" : "t2.micro",
        "KeyName" : "mykey"
    }
}
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  myStackWithParams:
    Type: AWS::CloudFormation::Stack
    Properties:
      TemplateURL: https://s3.amazonaws.com/cloudformation-templates-us-east-1/
        EC2ChooseAMI.template
      Parameters:
        InstanceType: t2.micro
        KeyName: mykey
```

Condizione di attesa

Utilizzo di una condizione di attesa con un' EC2istanza Amazon

Important

Per le risorse Amazon EC2 e Auto Scaling, ti consigliamo di utilizzare un CreationPolicy attributo anziché le condizioni di attesa. Aggiungi un CreationPolicy attributo a tali risorse e utilizza lo script di supporto cfn-signal per segnalare quando il processo di creazione di un'istanza è stato completato correttamente.

Se non puoi utilizzare una politica di creazione, visualizzi il seguente modello di esempio, che dichiara un' EC2 istanza Amazon con una condizione di attesa. La condizione di myWaitCondition attesa viene utilizzata myWaitConditionHandle per la segnalazione, utilizza l'Dependsonattributo per specificare che la condizione di attesa verrà attivata dopo la creazione della risorsa dell' EC2 istanza Amazon e utilizza la Timeout proprietà per specificare una durata di 4500 secondi per la condizione di attesa. Inoltre, l'URL predefinito che segnala la condizione di attesa viene passato all' EC2 istanza Amazon con la UserData proprietà della Ec2Instance risorsa, consentendo così

a un'applicazione o a uno script in esecuzione su quell' EC2 istanza Amazon di recuperare l'URL predefinito e utilizzarlo per segnalare l'esito positivo o negativo della condizione di attesa. Devi utilizzare `cfn-signal` o creare l'applicazione o lo script che segnala la condizione di attesa. Il valore di uscita `ApplicationData` contiene i dati trasmessi dal segnale della condizione di attesa.

Per ulteriori informazioni, consulta [Creare condizioni di attesa in un CloudFormation modello](#).

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Mappings" : {
    "RegionMap" : {
      "us-east-1" : {
        "AMI" : "ami-0ff8a91507f77f867"
      },
      "us-west-1" : {
        "AMI" : "ami-0bdb828fd58c52235"
      },
      "eu-west-1" : {
        "AMI" : "ami-047bb4163c506cd98"
      },
      "ap-northeast-1" : {
        "AMI" : "ami-06cd52961ce9f0d85"
      },
      "ap-southeast-1" : {
        "AMI" : "ami-08569b978cc4dfa10"
      }
    }
  },
  "Resources" : {
    "Ec2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "UserData" : { "Fn::Base64" : {"Ref" : "myWaitHandle"} },
        "ImageId" : { "Fn::FindInMap" : [ "RegionMap", { "Ref" :
"AWS::Region" }, "AMI" ] }
      }
    },
    "myWaitHandle" : {
      "Type" : "AWS::CloudFormation::WaitConditionHandle",
      "Properties" : {

```

```

    },
    "myWaitCondition" : {
      "Type" : "AWS::CloudFormation::WaitCondition",
      "DependsOn" : "Ec2Instance",
      "Properties" : {
        "Handle" : { "Ref" : "myWaitHandle" },
        "Timeout" : "4500"
      }
    }
  },
  "Outputs" : {
    "ApplicationData" : {
      "Value" : { "Fn::GetAtt" : [ "myWaitCondition", "Data" ] },
      "Description" : "The data passed back as part of signalling the
WaitCondition."
    }
  }
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Mappings:
  RegionMap:
    us-east-1:
      AMI: ami-0ff8a91507f77f867
    us-west-1:
      AMI: ami-0bdb828fd58c52235
    eu-west-1:
      AMI: ami-047bb4163c506cd98
    ap-northeast-1:
      AMI: ami-06cd52961ce9f0d85
    ap-southeast-1:
      AMI: ami-08569b978cc4dfa10
Resources:
  Ec2Instance:
    Type: AWS::EC2::Instance
    Properties:
      UserData:
        Fn::Base64: !Ref myWaitHandle
      ImageId:
        Fn::FindInMap:
          - RegionMap

```



```

    - Ref: AWS::Region
    - AMI
  myWaitHandle:
    Type: AWS::CloudFormation::WaitConditionHandle
    Properties: {}
  myWaitCondition:
    Type: AWS::CloudFormation::WaitCondition
    DependsOn: Ec2Instance
    Properties:
      Handle: !Ref myWaitHandle
      Timeout: '4500'
  Outputs:
    ApplicationData:
      Value: !GetAtt myWaitCondition.Data
      Description: The data passed back as part of signalling the WaitCondition.

```

Utilizzo dello script helper `cfn-signal` per segnalare una condizione di attesa

Questo esempio mostra una `cfn-signal` riga di comando che segnala il successo di una condizione di attesa. È necessario definire la riga di comando nella `UserData` proprietà dell' EC2 istanza.

JSON

```

"UserData": {
  "Fn::Base64": {
    "Fn::Join": [
      "",
      [
        "#!/bin/bash -xe\n",
        "/opt/aws/bin/cfn-signal --exit-code 0 '",
        {
          "Ref": "myWaitHandle"
        },
        "'\n"
      ]
    ]
  }
}

```

YAML

```

UserData:

```

```
'Fn::Base64':
  'Fn::Join':
    - ''
    - - |
        #!/bin/bash -xe
        - /opt/aws/bin/cfn-signal --exit-code 0 '
        - Ref: myWaitHandle
        - |
        '
```

Utilizzo di Curl per segnalare una condizione di attesa

Nell'esempio seguente viene mostrata una riga di comando Curl che segnala l'operazione riuscita a una condizione di attesa.

```
curl -T /tmp/a "https://cloudformation-waitcondition-test.s3.amazonaws.com/
arn%3Aaws%3Acloudformation%3Aus-east-1%3A034017226601%3Astack
%2Fstack-gosar-20110427004224-test-stack-with-WaitCondition--VEYW
%2Fe498ce60-70a1-11e0-81a7-5081d0136786%2FmyWaitConditionHandle?
Expires=1303976584&AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=ik1twT6hpS4cgNAw7wy0oRejVoo
%3D"
```

Dove il file /tmp/a contiene la seguente struttura JSON:

```
{
  "Status" : "SUCCESS",
  "Reason" : "Configuration Complete",
  "UniqueId" : "ID1234",
  "Data" : "Application has completed configuration."
}
```

In questo esempio viene mostrata una riga di comando Curl che invia lo stesso segnale di operazione riuscita, con la differenza che come parametro invia la struttura JSON sulla riga di comando.

```
curl -X PUT -H 'Content-Type:' --data-binary '{"Status" : "SUCCESS","Reason" :
"Configuration Complete","UniqueId" : "ID1234","Data" : "Application
has completed configuration."}' "https://cloudformation-waitcondition-
test.s3.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-east-1%3A034017226601%3Astack
%2Fstack-gosar-20110427004224-test-stack-with-WaitCondition--VEYW
%2Fe498ce60-70a1-11e0-81a7-5081d0136786%2FmyWaitConditionHandle?
Expires=1303976584&AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=ik1twT6hpS4cgNAw7wy0oRejVoo
%3D"
```

Frammenti CloudFront di modello Amazon

Usa questi frammenti di modello di esempio con la tua risorsa di CloudFront distribuzione Amazon in. AWS CloudFormation Per ulteriori informazioni, consulta il [riferimento ai tipi di CloudFront risorse Amazon](#).

Argomenti

- [Risorsa di CloudFront distribuzione Amazon con origine Amazon S3](#)
- [Risorsa CloudFront di distribuzione Amazon con origine personalizzata](#)
- [CloudFront Distribuzione Amazon con supporto multiorigine](#)
- [CloudFront Distribuzione Amazon con una funzione Lambda come origine](#)
- [Consulta anche](#)

Risorsa di CloudFront distribuzione Amazon con origine Amazon S3

Il seguente modello di esempio mostra una CloudFront [distribuzione](#) Amazon che utilizza un [S3Origin e una legacy Origin](#) Access Identity (OAI). Per informazioni sull'utilizzo del controllo dell'accesso all'origine (OAC), consulta [Restricting access to an Amazon Simple Storage Service origin \(Limitazione dell'accesso a un'origine di Amazon Simple Storage Service\)](#) nella Amazon CloudFront Developer Guide.

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "myDistribution" : {
      "Type" : "AWS::CloudFront::Distribution",
      "Properties" : {
        "DistributionConfig" : {
          "Origins" : [ {
            "DomainName" : "amzn-s3-demo-bucket.s3.amazonaws.com",
            "Id" : "myS3Origin",
            "S3OriginConfig" : {
              "OriginAccessIdentity" : "origin-access-identity/cloudfront/E127EXAMPLE51Z"
            }
          }
        ],
        "Enabled" : "true",
```

```
"Comment" : "Some comment",
"DefaultRootObject" : "index.html",
"Logging" : {
    "IncludeCookies" : "false",
    "Bucket" : "amzn-s3-demo-logging-bucket.s3.amazonaws.com",
    "Prefix" : "myprefix"
},
"Aliases" : [ "mysite.example.com", "yoursite.example.com" ],
"DefaultCacheBehavior" : {
    "AllowedMethods" : [ "DELETE", "GET", "HEAD", "OPTIONS",
"PATCH", "POST", "PUT" ],
    "TargetOriginId" : "myS3Origin",
    "ForwardedValues" : {
        "QueryString" : "false",
        "Cookies" : { "Forward" : "none" }
    },
    "TrustedSigners" : [ "1234567890EX", "1234567891EX" ],
    "ViewerProtocolPolicy" : "allow-all"
},
"PriceClass" : "PriceClass_200",
"Restrictions" : {
    "GeoRestriction" : {
        "RestrictionType" : "whitelist",
        "Locations" : [ "AQ", "CV" ]
    }
},
"ViewerCertificate" : { "CloudFrontDefaultCertificate" : "true" }
}
}
}
```

YAML

```
AWS::Template::FormatVersion: '2010-09-09'
Resources:
  myDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Origins:
          - DomainName: amzn-s3-demo-bucket.s3.amazonaws.com
```

```
Id: myS3Origin
S3OriginConfig:
  OriginAccessIdentity: origin-access-identity/cloudfront/E127EXAMPLE51Z
Enabled: 'true'
Comment: Some comment
DefaultRootObject: index.html
Logging:
  IncludeCookies: 'false'
  Bucket: amzn-s3-demo-logging-bucket.s3.amazonaws.com
  Prefix: myprefix
Aliases:
- mysite.example.com
- yoursite.example.com
DefaultCacheBehavior:
  AllowedMethods:
  - DELETE
  - GET
  - HEAD
  - OPTIONS
  - PATCH
  - POST
  - PUT
  TargetOriginId: myS3Origin
  ForwardedValues:
    QueryString: 'false'
    Cookies:
      Forward: none
  TrustedSigners:
  - 1234567890EX
  - 1234567891EX
  ViewerProtocolPolicy: allow-all
PriceClass: PriceClass_200
Restrictions:
  GeoRestriction:
    RestrictionType: whitelist
    Locations:
    - AQ
    - CV
ViewerCertificate:
  CloudFrontDefaultCertificate: 'true'
```

Risorsa CloudFront di distribuzione Amazon con origine personalizzata

Il seguente modello di esempio mostra una CloudFront [distribuzione](#) Amazon che utilizza un [CustomOrigin](#).

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "myDistribution" : {
      "Type" : "AWS::CloudFront::Distribution",
      "Properties" : {
        "DistributionConfig" : {
          "Origins" : [ {
            "DomainName" : "www.example.com",
            "Id" : "myCustomOrigin",
            "CustomOriginConfig" : {
              "HTTPPort" : "80",
              "HTTPSPort" : "443",
              "OriginProtocolPolicy" : "http-only"
            }
          } ],
          "Enabled" : "true",
          "Comment" : "Somecomment",
          "DefaultRootObject" : "index.html",
          "Logging" : {
            "IncludeCookies" : "true",
            "Bucket" : "amzn-s3-demo-logging-bucket.s3.amazonaws.com",
            "Prefix" : "myprefix"
          },
          "Aliases" : [
            "mysite.example.com",
            "*.yoursite.example.com"
          ],
          "DefaultCacheBehavior" : {
            "TargetOriginId" : "myCustomOrigin",
            "SmoothStreaming" : "false",
            "ForwardedValues" : {
              "QueryString" : "false",
              "Cookies" : { "Forward" : "all" }
            }
          },
          "TrustedSigners" : [
```

```
        "1234567890EX",
        "1234567891EX"
    ],
    "ViewerProtocolPolicy" : "allow-all"
},
"CustomErrorResponses" : [ {
    "ErrorCode" : "404",
    "ResponsePagePath" : "/error-pages/404.html",
    "ResponseCode" : "200",
    "ErrorCachingMinTTL" : "30"
} ],
"PriceClass" : "PriceClass_200",
"Restrictions" : {
    "GeoRestriction" : {
        "RestrictionType" : "whitelist",
        "Locations" : [ "AQ", "CV" ]
    }
},
"ViewerCertificate": { "CloudFrontDefaultCertificate" : "true" }
}
}
}
```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  myDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Origins:
          - DomainName: www.example.com
            Id: myCustomOrigin
            CustomOriginConfig:
              HTTPPort: '80'
              HTTPSPort: '443'
              OriginProtocolPolicy: http-only
        Enabled: 'true'
        Comment: Somecomment
        DefaultRootObject: index.html

```

```

Logging:
  IncludeCookies: 'true'
  Bucket: amzn-s3-demo-logging-bucket.s3.amazonaws.com
  Prefix: myprefix
Aliases:
- mysite.example.com
- "*.yoursite.example.com"
DefaultCacheBehavior:
  TargetOriginId: myCustomOrigin
  SmoothStreaming: 'false'
  ForwardedValues:
    QueryString: 'false'
    Cookies:
      Forward: all
  TrustedSigners:
    - 1234567890EX
    - 1234567891EX
  ViewerProtocolPolicy: allow-all
CustomErrorResponses:
- ErrorCode: '404'
  ResponsePagePath: "/error-pages/404.html"
  ResponseCode: '200'
  ErrorCachingMinTTL: '30'
PriceClass: PriceClass_200
Restrictions:
  GeoRestriction:
    RestrictionType: whitelist
    Locations:
      - AQ
      - CV
ViewerCertificate:
  CloudFrontDefaultCertificate: 'true'

```

CloudFront Distribuzione Amazon con supporto multiorigine

Il seguente modello di esempio mostra come dichiarare una CloudFront [distribuzione con supporto](#) multiorigine. In [DistributionConfig](#), viene fornito un elenco di origini e viene impostato un [DefaultCacheBehavior](#).

JSON

```

{
  "AWSTemplateFormatVersion" : "2010-09-09",

```



```

"Resources" : {
  "myDistribution" : {
    "Type" : "AWS::CloudFront::Distribution",
    "Properties" : {
      "DistributionConfig" : {
        "Origins" : [ {
          "Id" : "myS3Origin",
          "DomainName" : "amzn-s3-demo-bucket.s3.amazonaws.com",
          "S3OriginConfig" : {
            "OriginAccessIdentity" : "origin-access-identity/
cloudfront/E127EXAMPLE51Z"
          }
        },
        {
          "Id" : "myCustomOrigin",
          "DomainName" : "www.example.com",
          "CustomOriginConfig" : {
            "HTTPPort" : "80",
            "HTTPSPort" : "443",
            "OriginProtocolPolicy" : "http-only"
          }
        }
      ],
      "Enabled" : "true",
      "Comment" : "Some comment",
      "DefaultRootObject" : "index.html",
      "Logging" : {
        "IncludeCookies" : "true",
        "Bucket" : "amzn-s3-demo-logging-bucket.s3.amazonaws.com",
        "Prefix" : "myprefix"
      },
      "Aliases" : [ "mysite.example.com", "yoursite.example.com" ],
      "DefaultCacheBehavior" : {
        "TargetOriginId" : "myS3Origin",
        "ForwardedValues" : {
          "QueryString" : "false",
          "Cookies" : { "Forward" : "all" }
        },
        "TrustedSigners" : [ "1234567890EX", "1234567891EX" ],
        "ViewerProtocolPolicy" : "allow-all",
        "MinTTL" : "100",
        "SmoothStreaming" : "true"
      },
      "CacheBehaviors" : [ {

```

```

        "AllowedMethods" : [ "DELETE", "GET", "HEAD", "OPTIONS",
"PATCH", "POST", "PUT" ],
        "TargetOriginId" : "myS3Origin",
        "ForwardedValues" : {
            "QueryString" : "true",
            "Cookies" : { "Forward" : "none" }
        },
        "TrustedSigners" : [ "1234567890EX", "1234567891EX" ],
        "ViewerProtocolPolicy" : "allow-all",
        "MinTTL" : "50",
        "PathPattern" : "images1/*.jpg"
    },
    {
        "AllowedMethods" : [ "DELETE", "GET", "HEAD", "OPTIONS",
"PATCH", "POST", "PUT" ],
        "TargetOriginId" : "myCustomOrigin",
        "ForwardedValues" : {
            "QueryString" : "true",
            "Cookies" : { "Forward" : "none" }
        },
        "TrustedSigners" : [ "1234567890EX", "1234567891EX" ],
        "ViewerProtocolPolicy" : "allow-all",
        "MinTTL" : "50",
        "PathPattern" : "images2/*.jpg"
    }
],
"CustomErrorResponses" : [ {
    "ErrorCode" : "404",
    "ResponsePagePath" : "/error-pages/404.html",
    "ResponseCode" : "200",
    "ErrorCachingMinTTL" : "30"
} ],
"PriceClass" : "PriceClass_All",
"ViewerCertificate" : { "CloudFrontDefaultCertificate" : "true" }
}
}
}
}
}
}
}
}
}
}

```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
```

Resources:**myDistribution:**

Type: AWS::CloudFront::Distribution

Properties:**DistributionConfig:****Origins:**

- Id: myS3Origin

DomainName: amzn-s3-demo-bucket.s3.amazonaws.com

S3OriginConfig:

OriginAccessIdentity: origin-access-identity/cloudfront/E127EXAMPLE51Z

- Id: myCustomOrigin

DomainName: www.example.com

CustomOriginConfig:

HTTPPort: '80'

HTTPSPort: '443'

OriginProtocolPolicy: http-only

Enabled: 'true'

Comment: Some comment

DefaultRootObject: index.html

Logging:

IncludeCookies: 'true'

Bucket: amzn-s3-demo-logging-bucket.s3.amazonaws.com

Prefix: myprefix

Aliases:

- mysite.example.com
- yoursite.example.com

DefaultCacheBehavior:

TargetOriginId: myS3Origin

ForwardedValues:

QueryString: 'false'

Cookies:

Forward: all

TrustedSigners:

- 1234567890EX
- 1234567891EX

ViewerProtocolPolicy: allow-all

MinTTL: '100'

SmoothStreaming: 'true'

CacheBehaviors:

- AllowedMethods:

- DELETE
- GET
- HEAD
- OPTIONS

```
- PATCH
- POST
- PUT
TargetOriginId: myS3Origin
ForwardedValues:
  QueryString: 'true'
  Cookies:
    Forward: none
TrustedSigners:
- 1234567890EX
- 1234567891EX
ViewerProtocolPolicy: allow-all
MinTTL: '50'
PathPattern: images1/*.jpg
- AllowedMethods:
- DELETE
- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT
TargetOriginId: myCustomOrigin
ForwardedValues:
  QueryString: 'true'
  Cookies:
    Forward: none
TrustedSigners:
- 1234567890EX
- 1234567891EX
ViewerProtocolPolicy: allow-all
MinTTL: '50'
PathPattern: images2/*.jpg
CustomErrorResponses:
- ErrorCode: '404'
  ResponsePagePath: "/error-pages/404.html"
  ResponseCode: '200'
  ErrorCachingMinTTL: '30'
PriceClass: PriceClass_All
ViewerCertificate:
  CloudFrontDefaultCertificate: 'true'
```

CloudFront Distribuzione Amazon con una funzione Lambda come origine

L'esempio seguente crea una CloudFront distribuzione che fronteggia l'URL di una funzione Lambda specificato (fornito come parametro), abilitando l'accesso, la memorizzazione nella cache, la compressione e la consegna globale solo tramite HTTPS. Configura l'URL Lambda come origine HTTPS personalizzata e applica una politica di memorizzazione nella cache AWS standard. La distribuzione è ottimizzata per le prestazioni con HTTP/2 e IPv6 supporta e restituisce il nome di CloudFront dominio, consentendo agli utenti di accedere alla funzione Lambda tramite un endpoint sicuro supportato da CDN. Per ulteriori informazioni, consulta [Usare Amazon CloudFront with AWS Lambda as origin per accelerare le tue applicazioni web](#) sul AWS blog.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "LambdaEndpoint": {
      "Type": "String",
      "Description": "The Lambda function URL endpoint without the 'https://'"
    }
  },
  "Resources": {
    "MyDistribution": {
      "Type": "AWS::CloudFront::Distribution",
      "Properties": {
        "DistributionConfig": {
          "PriceClass": "PriceClass_All",
          "HttpVersion": "http2",
          "IPV6Enabled": true,
          "Origins": [
            {
              "DomainName": {
                "Ref": "LambdaEndpoint"
              },
              "Id": "LambdaOrigin",
              "CustomOriginConfig": {
                "HTTPSPort": 443,
                "OriginProtocolPolicy": "https-only"
              }
            }
          ]
        },
        "Enabled": "true",
```

```

        "DefaultCacheBehavior": {
            "TargetOriginId": "LambdaOrigin",
            "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e58f6",
            "ViewerProtocolPolicy": "redirect-to-https",
            "SmoothStreaming": "false",
            "Compress": "true"
        }
    },
    "Outputs": {
        "CloudFrontDomain": {
            "Description": "CloudFront default domain name configured",
            "Value": {
                "Fn::Sub": "https://${MyDistribution.DomainName}/"
            }
        }
    }
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Parameters:
  LambdaEndpoint:
    Type: String
    Description: The Lambda function URL endpoint without the 'https://'
Resources:
  MyDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        PriceClass: PriceClass_All
        HttpVersion: http2
        IPV6Enabled: true
        Origins:
          - DomainName: !Ref LambdaEndpoint
            Id: LambdaOrigin
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
        Enabled: 'true'

```

```
DefaultCacheBehavior:
  TargetOriginId: LambdaOrigin
  CachePolicyId: '658327ea-f89d-4fab-a63d-7e88639e58f6'
  ViewerProtocolPolicy: redirect-to-https
  SmoothStreaming: 'false'
  Compress: 'true'
```

Outputs:

```
CloudFrontDomain:
  Description: CloudFront default domain name configured
  Value: !Sub https://${MyDistribution.DomainName}/
```

Consulta anche

Per un esempio di aggiunta di un alias personalizzato a un record di Route 53 per creare un nome descrittivo per una CloudFront distribuzione, consulta [Alias: record di risorse impostato per una distribuzione CloudFront](#).

Frammenti CloudWatch di modello Amazon

Usa questi frammenti di modello di esempio per descrivere le tue CloudWatch risorse Amazon in. AWS CloudFormation Per ulteriori informazioni, consulta il [riferimento ai tipi di CloudWatch risorse Amazon](#).

Argomenti

- [Allarme di fatturazione](#)
- [Allarme di utilizzo della CPU](#)
- [Ripristino di un'istanza Amazon Elastic Compute Cloud](#)
- [Creazione di un pannello di controllo di base](#)
- [Crea una dashboard con widget side-by-side](#)

Allarme di fatturazione

Nel seguente esempio, Amazon CloudWatch invia una notifica via e-mail quando gli addebiti AWS sul tuo account superano la soglia di allarme. Per ricevere notifiche di utilizzo, abilita avvisi di fatturazione. Per ulteriori informazioni, consulta [Creare un allarme di fatturazione per monitorare i AWS costi stimati](#) nella Amazon CloudWatch User Guide. >

JSON

```
"SpendingAlarm": {
  "Type": "AWS::CloudWatch::Alarm",
  "Properties": {
    "AlarmDescription": { "Fn::Join": [ "", [
      "Alarm if AWS spending is over $",
      { "Ref": "AlarmThreshold" }
    ] ] },
    "Namespace": "AWS/Billing",
    "MetricName": "EstimatedCharges",
    "Dimensions": [{
      "Name": "Currency",
      "Value": "USD"
    } ],
    "Statistic": "Maximum",
    "Period": "21600",
    "EvaluationPeriods": "1",
    "Threshold": { "Ref": "AlarmThreshold" },
    "ComparisonOperator": "GreaterThanOrEqualToThreshold",
    "AlarmActions": [{
      "Ref": "BillingAlarmNotification"
    } ],
    "InsufficientDataActions": [{
      "Ref": "BillingAlarmNotification"
    } ]
  }
}
```

YAML

```
SpendingAlarm:
  Type: AWS::CloudWatch::Alarm
  Properties:
    AlarmDescription:
      'Fn::Join':
        - ''
        - - Alarm if AWS spending is over $
          - !Ref: AlarmThreshold
    Namespace: AWS/Billing
    MetricName: EstimatedCharges
    Dimensions:
      - Name: Currency
```



```

    Value: USD
    Statistic: Maximum
    Period: '21600'
    EvaluationPeriods: '1'
    Threshold:
      !Ref: "AlarmThreshold"
    ComparisonOperator: GreaterThanThreshold
    AlarmActions:
      - !Ref: "BillingAlarmNotification"
    InsufficientDataActions:
      - !Ref: "BillingAlarmNotification"

```

Allarme di utilizzo della CPU

Il seguente frammento di esempio crea un allarme che invia una notifica quando l'utilizzo medio della CPU di un' EC2 istanza Amazon supera il 90% per più di 60 secondi in tre periodi di valutazione.

JSON

```

"CPUALarm" : {
  "Type" : "AWS::CloudWatch::Alarm",
  "Properties" : {
    "AlarmDescription" : "CPU alarm for my instance",
    "AlarmActions" : [ { "Ref" : "logical name of an AWS::SNS::Topic resource" } ],
    "MetricName" : "CPUUtilization",
    "Namespace" : "AWS/EC2",
    "Statistic" : "Average",
    "Period" : "60",
    "EvaluationPeriods" : "3",
    "Threshold" : "90",
    "ComparisonOperator" : "GreaterThanThreshold",
    "Dimensions" : [ {
      "Name" : "InstanceId",
      "Value" : { "Ref" : "logical name of an AWS::EC2::Instance resource" }
    } ]
  }
}

```

YAML

```

CPUALarm:
  Type: AWS::CloudWatch::Alarm
  Properties:

```

```

AlarmDescription: CPU alarm for my instance
AlarmActions:
- !Ref: "logical name of an AWS::SNS::Topic resource"
MetricName: CPUUtilization
Namespace: AWS/EC2
Statistic: Average
Period: '60'
EvaluationPeriods: '3'
Threshold: '90'
ComparisonOperator: GreaterThanThreshold
Dimensions:
- Name: InstanceId
  Value: !Ref: "logical name of an AWS::EC2::Instance resource"

```

Ripristino di un'istanza Amazon Elastic Compute Cloud

Il seguente CloudWatch allarme ripristina un' EC2 istanza quando presenta errori di controllo dello stato per 15 minuti consecutivi. Per ulteriori informazioni sulle azioni di allarme, consulta [Crea allarmi per interrompere, terminare, riavviare o ripristinare un' EC2 istanza](#) nella Amazon CloudWatch User Guide.

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters" : {
    "RecoveryInstance" : {
      "Description" : "The EC2 instance ID to associate this alarm with.",
      "Type" : "AWS::EC2::Instance::Id"
    }
  },
  "Resources": {
    "RecoveryTestAlarm": {
      "Type": "AWS::CloudWatch::Alarm",
      "Properties": {
        "AlarmDescription": "Trigger a recovery when instance status check fails for 15 consecutive minutes.",
        "Namespace": "AWS/EC2" ,
        "MetricName": "StatusCheckFailed_System",
        "Statistic": "Minimum",
        "Period": "60",
        "EvaluationPeriods": "15",
        "ComparisonOperator": "GreaterThanThreshold",

```

```

        "Threshold": "0",
        "AlarmActions": [ {"Fn::Join" : ["", ["arn:aws:automate:", { "Ref" :
"AWS::Region" }, ":ec2:recover" ]]} ],
        "Dimensions": [{"Name": "InstanceId","Value": {"Ref": "RecoveryInstance"}}]
    }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Parameters:
  RecoveryInstance:
    Description: The EC2 instance ID to associate this alarm with.
    Type: AWS::EC2::Instance::Id
Resources:
  RecoveryTestAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmDescription: Trigger a recovery when instance status check fails for 15
        consecutive minutes.
      Namespace: AWS/EC2
      MetricName: StatusCheckFailed_System
      Statistic: Minimum
      Period: '60'
      EvaluationPeriods: '15'
      ComparisonOperator: GreaterThanThreshold
      Threshold: '0'
      AlarmActions: [ !Sub "arn:aws:automate:${AWS::Region}:ec2:recover" ]
      Dimensions:
        - Name: InstanceId
          Value: !Ref: RecoveryInstance

```

Creazione di un pannello di controllo di base

L'esempio seguente crea una CloudWatch dashboard semplice con un widget metrico che mostra l'utilizzo della CPU e un widget di testo che mostra un messaggio.

JSON

```

{
  "BasicDashboard": {

```

```

    "Type": "AWS::CloudWatch::Dashboard",
    "Properties": {
      "DashboardName": "Dashboard1",
      "DashboardBody": "{\n\"widgets\": [{\n\"type\": \"metric\", \"x\": 0, \"y\": 0,\n\"width\": 12, \"height\": 6, \"properties\": {\n\"metrics\": [\n\"AWS/EC2\", \"CPUUtilization\", \"InstanceId\", \"i-012345\"], \"period\": 300, \"stat\": \"Average\", \"region\": \"us-east-1\", \"title\": \"EC2 Instance CPU\"}], \"type\": \"text\", \"x\": 0, \"y\": 7, \"width\": 3, \"height\": 3, \"properties\": {\n\"markdown\": \"Hello world\"}}]}}"
    }
  }
}

```

YAML

```

BasicDashboard:
  Type: AWS::CloudWatch::Dashboard
  Properties:
    DashboardName: Dashboard1
    DashboardBody: '{"widgets":
[{"type":"metric","x":0,"y":0,"width":12,"height":6,"properties":{"metrics":[{"AWS/
EC2","CPUUtilization","InstanceId","i-012345"}],"period":300,"stat":"Average","region":"us-
east-1","title":"EC2 Instance CPU"}],
{"type":"text","x":0,"y":7,"width":3,"height":3,"properties":{"markdown":"Hello
world"}}]}'

```

Crea una dashboard con widget side-by-side

Nell'esempio seguente viene creato un pannello di controllo con due widget parametro visualizzati affiancati.

JSON

```

{
  "DashboardSideBySide": {
    "Type": "AWS::CloudWatch::Dashboard",
    "Properties": {
      "DashboardName": "Dashboard1",
      "DashboardBody": "{\n\"widgets\": [{\n\"type\": \"metric\", \"x\": 0, \"y\": 0,\n\"width\": 12, \"height\": 6, \"properties\": {\n\"metrics\": [\n\"AWS/EC2\", \"CPUUtilization\", \"InstanceId\", \"i-012345\"], \"period\": 300, \"stat\": \"Average\", \"region\": \"us-east-1\", \"title\": \"EC2 Instance CPU\"}], \"type\": \"metric\", \"x\": 12, \"y\": 0, \"width\": 12, \"height\": 6, \"properties\": {\n\"metrics\": [\n\"AWS/S3\", \"BucketSizeBytes\",

```

```
\ "BucketName\","\ "amzn-s3-demo-bucket\"]] ,\ "period\ ":86400,\ "stat\ ": \ "Maximum\ ",\ "region\ ": \ "us-east-1\ ",\ "title\ ": \ "amzn-s3-demo-bucket bytes\ "}}]]"
    }
  }
}
```

YAML

```
DashboardSideBySide:
  Type: AWS::CloudWatch::Dashboard
  Properties:
    DashboardName: Dashboard1
    DashboardBody: '{"widgets":
[{"type":"metric","x":0,"y":0,"width":12,"height":6,"properties":{"metrics":[["AWS/
EC2","CPUUtilization","InstanceId","i-012345"]], "period":300,"stat":"Average","region":"us-
east-1","title":"EC2 Instance CPU"}},
{"type":"metric","x":12,"y":0,"width":12,"height":6,"properties":
{"metrics":[["AWS/S3","BucketSizeBytes","BucketName","amzn-s3-demo-
bucket"]], "period":86400,"stat":"Maximum","region":"us-east-1","title":"amzn-s3-demo-
bucket bytes"}}]]}'
```

Frammenti di modello Amazon CloudWatch Logs

Amazon CloudWatch Logs può monitorare il sistema, l'applicazione e i file di log personalizzati da EC2 istanze Amazon o da altre fonti. Puoi utilizzarlo AWS CloudFormation per fornire e gestire gruppi di log e filtri metrici. Per ulteriori informazioni su Amazon CloudWatch Logs, consulta la [Amazon CloudWatch Logs User Guide](#).

Argomenti

- [Invia log a Logs da un' CloudWatch istanza Linux](#)
- [Invia i log a Logs da un'istanza di Windows CloudWatch](#)
- [Consulta anche](#)

Invia log a Logs da un' CloudWatch istanza Linux

Il modello seguente descrive un server Web e i relativi parametri personalizzati. Gli eventi di log del server Web forniscono i dati per i parametri personalizzati. Per inviare eventi di registro a una metrica personalizzata, il UserData campo installa un agente CloudWatch Logs sull'istanza Amazon.

EC2 Le informazioni di configurazione per l'agente, ad esempio la posizione del file di log del server, il nome del gruppo di log e il nome del flusso di log, vengono definiti nel file `/tmp/cwlogs/apacheaccess.conf`. Il flusso di log viene creato una volta che il server Web inizia a inviare eventi di log al file `/var/log/httpd/access_log`.

Note

Una nota sulle autorizzazioni: l'istanza `WebServerHost` fa riferimento al profilo dell'istanza `LogRoleInstanceProfile`, che a sua volta fa riferimento al ruolo `LogRole`. `LogRole` specifica l'autorizzazione `s3:GetObject` per `arn:aws:s3::*`.

Questa autorizzazione è necessaria perché `WebServerHost` scarica l'agente CloudWatch Logs (`awslogs-agent-setup.py`) da Amazon S3 nella `UserData` sezione.

I due filtri di parametri descrivono in che modo le informazioni di log vengono trasformate in parametri CloudWatch. Il parametro 404 conta il numero di occorrenze 404. Il parametro delle dimensioni monitora le dimensioni di una richiesta. I due CloudWatch allarmi invieranno notifiche se ci sono più di due 404 entro 2 minuti o se la dimensione media della richiesta supera i 3500 KB nell'arco di 10 minuti.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "AWS CloudFormation Sample Template for CloudWatch Logs.",
  "Parameters": {
    "KeyName": {
      "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instances",
      "Type": "AWS::EC2::KeyPair::KeyName",
      "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
    },
    "SSHLocation": {
      "Description": "The IP address range that can be used to SSH to the EC2 instances",
      "Type": "String",
      "MinLength": "9",
      "MaxLength": "18",
      "Default": "0.0.0.0/0",
      "AllowedPattern": "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})/(\\d{1,2})",

```

```

        "ConstraintDescription": "must be a valid IP CIDR range of the form
x.x.x.x/x."
    },
    "OperatorEmail": {
        "Description": "Email address to notify if there are any scaling
operations",
        "Type": "String"
    }
},
"Mappings": {
    "RegionMap": {
        "us-east-1": {
            "AMI": "ami-0ff8a91507f77f867"
        },
        "us-west-1": {
            "AMI": "ami-0bdb828fd58c52235"
        },
        "us-west-2": {
            "AMI": "ami-a0cfeed8"
        },
        "eu-west-1": {
            "AMI": "ami-047bb4163c506cd98"
        },
        "ap-southeast-1": {
            "AMI": "ami-08569b978cc4dfa10"
        },
        "ap-southeast-2": {
            "AMI": "ami-09b42976632b27e9b"
        },
        "ap-northeast-1": {
            "AMI": "ami-06cd52961ce9f0d85"
        },
        "sa-east-1": {
            "AMI": "ami-07b14488da8ea02a0"
        },
        "eu-central-1": {
            "AMI": "ami-0233214e13e500f77"
        }
    }
},
"Resources": {
    "LogRole": {
        "Type": "AWS::IAM::Role",
        "Properties": {

```

```

    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": [
              "ec2.amazonaws.com"
            ]
          },
          "Action": [
            "sts:AssumeRole"
          ]
        }
      ]
    },
    "Path": "/",
    "Policies": [
      {
        "PolicyName": "LogRolePolicy",
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                "logs:Create*",
                "logs:PutLogEvents",
                "s3:GetObject"
              ],
              "Resource": [
                "arn:aws:logs:*:*:*:*",
                "arn:aws:s3:::*"
              ]
            }
          ]
        }
      }
    ]
  },
  "LogRoleInstanceProfile": {
    "Type": "AWS::IAM::InstanceProfile",
    "Properties": {

```



```

        "Path": "/",
        "Roles": [
            {
                "Ref": "LogRole"
            }
        ]
    },
    "WebServerSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Enable HTTP access via port 80 and SSH access via
port 22",
            "SecurityGroupIngress": [
                {
                    "IpProtocol": "tcp",
                    "FromPort": 80,
                    "ToPort": 80,
                    "CidrIp": "0.0.0.0/0"
                },
                {
                    "IpProtocol": "tcp",
                    "FromPort": 22,
                    "ToPort": 22,
                    "CidrIp": {
                        "Ref": "SSHLocation"
                    }
                }
            ]
        }
    },
    "WebServerHost": {
        "Type": "AWS::EC2::Instance",
        "Metadata": {
            "Comment": "Install a simple PHP application",
            "AWS::CloudFormation::Init": {
                "config": {
                    "packages": {
                        "yum": {
                            "httpd": [],
                            "php": []
                        }
                    },
                    "files": {

```

```

"/tmp/cwlogs/apacheaccess.conf": {
  "content": {
    "Fn::Join": [
      "",
      [
        "[general]\n",
        "state_file= /var/awslogs/agent-state\n",
        "[/var/log/httpd/access_log]\n",
        "file = /var/log/httpd/access_log\n",
        "log_group_name = ",
        {
          "Ref": "WebServerLogGroup"
        },
        "\n",
        "log_stream_name = {instance_id}/apache.log\n",

        "datetime_format = %d/%b/%Y:%H:%M:%S"
      ]
    ]
  },
  "mode": "000400",
  "owner": "apache",
  "group": "apache"
},
"/var/www/html/index.php": {
  "content": {
    "Fn::Join": [
      "",
      [
        "<?php\n",
        "echo '<h1>AWS CloudFormation sample PHP\n",

        "application</h1>';\n",

        "?>\n"
      ]
    ]
  },
  "mode": "000644",
  "owner": "apache",
  "group": "apache"
},
"/etc/cfn/cfn-hup.conf": {
  "content": {
    "Fn::Join": [
      "",

```

```

        [
            "[main]\n",
            "stack=",
            {
                "Ref": "AWS::StackId"
            },
            "\n",
            "region=",
            {
                "Ref": "AWS::Region"
            },
            "\n"
        ]
    ],
    "mode": "000400",
    "owner": "root",
    "group": "root"
},
"/etc/cfn/hooks.d/cfn-auto-reloader.conf": {
    "content": {
        "Fn::Join": [
            "",
            [
                "[cfn-auto-reloader-hook]\n",
                "triggers=post.update\n",
                "\npath=Resources.WebServerHost.Metadata.AWS::CloudFormation::Init\n",
                "action=/opt/aws/bin/cfn-init -s ",
                {
                    "Ref": "AWS::StackId"
                },
                " -r WebServerHost ",
                " --region      ",
                {
                    "Ref": "AWS::Region"
                },
                "\n",
                "runas=root\n"
            ]
        ]
    }
},

```

```

        "services": {
            "sysvinit": {
                "httpd": {
                    "enabled": "true",
                    "ensureRunning": "true"
                },
                "sendmail": {
                    "enabled": "false",
                    "ensureRunning": "false"
                }
            }
        }
    },
    "CreationPolicy": {
        "ResourceSignal": {
            "Timeout": "PT5M"
        }
    },
    "Properties": {
        "ImageId": {
            "Fn::FindInMap": [
                "RegionMap",
                {
                    "Ref": "AWS::Region"
                }
            ],
            "AMI"
        },
        "KeyName": {
            "Ref": "KeyName"
        },
        "InstanceType": "t1.micro",
        "SecurityGroups": [
            {
                "Ref": "WebServerSecurityGroup"
            }
        ],
        "IamInstanceProfile": {
            "Ref": "LogRoleInstanceProfile"
        },
        "UserData": {
            "Fn::Base64": {

```

```

    "Fn::Join": [
      "",
      [
        "#!/bin/bash -xe\n",
        "# Get the latest CloudFormation package\n",
        "yum install -y aws-cfn-bootstrap\n",
        "# Start cfn-init\n",
        "/opt/aws/bin/cfn-init -s ",
        {
          "Ref": "AWS::StackId"
        },
        " -r WebServerHost ",
        " --region ",
        {
          "Ref": "AWS::Region"
        },
        " || error_exit 'Failed to run cfn-init'\n",
        "# Start up the cfn-hup daemon to listen for changes to
the EC2 instance metadata\n",
        "/opt/aws/bin/cfn-hup || error_exit 'Failed to start
cfn-hup'\n",
        "# Get the CloudWatch Logs agent\n",
        "wget https://s3.amazonaws.com/aws-cloudwatch/
downloads/latest/awslogs-agent-setup.py\n",
        "# Install the CloudWatch Logs agent\n",
        "python awslogs-agent-setup.py -n -r ",
        {
          "Ref": "AWS::Region"
        },
        " -c /tmp/cwlogs/apacheaccess.conf || error_exit
'Failed to run CloudWatch Logs agent setup'\n",
        "# All done so signal success\n",
        "/opt/aws/bin/cfn-signal -e $? ",
        "      --stack ",
        {
          "Ref": "AWS::StackName"
        },
        "      --resource WebServerHost ",
        "      --region ",
        {
          "Ref": "AWS::Region"
        },
        "\n"
      ]
    ]

```

```

        ]
      }
    }
  },
  "WebServerLogGroup": {
    "Type": "AWS::Logs::LogGroup",
    "Properties": {
      "RetentionInDays": 7
    }
  },
  "404MetricFilter": {
    "Type": "AWS::Logs::MetricFilter",
    "Properties": {
      "LogGroupName": {
        "Ref": "WebServerLogGroup"
      },
      "FilterPattern": "[ip, identity, user_id, timestamp, request,
status_code = 404, size, ...]",
      "MetricTransformations": [
        {
          "MetricValue": "1",
          "MetricNamespace": "test/404s",
          "MetricName": "test404Count"
        }
      ]
    }
  },
  "BytesTransferredMetricFilter": {
    "Type": "AWS::Logs::MetricFilter",
    "Properties": {
      "LogGroupName": {
        "Ref": "WebServerLogGroup"
      },
      "FilterPattern": "[ip, identity, user_id, timestamp, request,
status_code, size, ...]",
      "MetricTransformations": [
        {
          "MetricValue": "$size",
          "MetricNamespace": "test/BytesTransferred",
          "MetricName": "testBytesTransferred"
        }
      ]
    }
  }
}

```

```
    },
    "404Alarm": {
      "Type": "AWS::CloudWatch::Alarm",
      "Properties": {
        "AlarmDescription": "The number of 404s is greater than 2 over 2
minutes",
        "MetricName": "test404Count",
        "Namespace": "test/404s",
        "Statistic": "Sum",
        "Period": "60",
        "EvaluationPeriods": "2",
        "Threshold": "2",
        "AlarmActions": [
          {
            "Ref": "AlarmNotificationTopic"
          }
        ],
        "ComparisonOperator": "GreaterThanThreshold"
      }
    },
    "BandwidthAlarm": {
      "Type": "AWS::CloudWatch::Alarm",
      "Properties": {
        "AlarmDescription": "The average volume of traffic is greater 3500 KB
over 10 minutes",
        "MetricName": "testBytesTransferred",
        "Namespace": "test/BytesTransferred",
        "Statistic": "Average",
        "Period": "300",
        "EvaluationPeriods": "2",
        "Threshold": "3500",
        "AlarmActions": [
          {
            "Ref": "AlarmNotificationTopic"
          }
        ],
        "ComparisonOperator": "GreaterThanThreshold"
      }
    },
    "AlarmNotificationTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "Subscription": [
          {
```

```

        "Endpoint": {
            "Ref": "OperatorEmail"
        },
        "Protocol": "email"
    }
]
}
},
"Outputs": {
    "InstanceId": {
        "Description": "The instance ID of the web server",
        "Value": {
            "Ref": "WebServerHost"
        }
    },
    "WebsiteURL": {
        "Value": {
            "Fn::Join": [
                "",
                [
                    "http://",
                    {
                        "Fn::GetAtt": [
                            "WebServerHost",
                            "PublicDnsName"
                        ]
                    }
                ]
            ]
        },
        "Description": "URL for newly created LAMP stack"
    },
    "PublicIP": {
        "Description": "Public IP address of the web server",
        "Value": {
            "Fn::GetAtt": [
                "WebServerHost",
                "PublicIp"
            ]
        }
    },
    "CloudWatchLogGroupName": {
        "Description": "The name of the CloudWatch log group",

```



```

        "Value": {
            "Ref": "WebServerLogGroup"
        }
    }
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: AWS CloudFormation Sample Template for CloudWatch Logs.
Parameters:
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instances
    Type: 'AWS::EC2::KeyPair::KeyName'
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  SSHLocation:
    Description: The IP address range that can be used to SSH to the EC2 instances
    Type: String
    MinLength: '9'
    MaxLength: '18'
    Default: 0.0.0.0/0
    AllowedPattern: '(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})/(\d{1,2})'
    ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
  OperatorEmail:
    Description: Email address to notify if there are any scaling operations
    Type: String
Mappings:
  RegionMap:
    us-east-1:
      AMI: ami-0ff8a91507f77f867
    us-west-1:
      AMI: ami-0bdb828fd58c52235
    us-west-2:
      AMI: ami-a0cfeed8
    eu-west-1:
      AMI: ami-047bb4163c506cd98
    ap-southeast-1:
      AMI: ami-08569b978cc4dfa10
    ap-southeast-2:
      AMI: ami-09b42976632b27e9b
    ap-northeast-1:
      AMI: ami-06cd52961ce9f0d85

```

```
sa-east-1:
  AMI: ami-07b14488da8ea02a0
eu-central-1:
  AMI: ami-0233214e13e500f77
Resources:
  LogRole:
    Type: 'AWS::IAM::Role'
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      Path: /
    Policies:
      - PolicyName: LogRolePolicy
        PolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Action:
                - 'logs:Create*'
                - 'logs:PutLogEvents'
                - 's3:GetObject'
              Resource:
                - 'arn:aws:logs:*:*:*'
                - 'arn:aws:s3::*:*'
  LogRoleInstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Path: /
      Roles:
        - !Ref LogRole
  WebServerSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Enable HTTP access via port 80 and SSH access via port 22
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 80
```

```

    ToPort: 80
    CidrIp: 0.0.0.0/0
  - IpProtocol: tcp
    FromPort: 22
    ToPort: 22
    CidrIp: !Ref SSHLocation
WebServerHost:
  Type: 'AWS::EC2::Instance'
Metadata:
  Comment: Install a simple PHP application
  'AWS::CloudFormation::Init':
    config:
      packages:
        yum:
          httpd: []
          php: []
      files:
        /tmp/cwlogs/apacheaccess.conf:
          content: !Join
            - ''
            - - |
                [general]
            - |
                state_file= /var/awslogs/agent-state
            - |
                [/var/log/httpd/access_log]
            - |
                file = /var/log/httpd/access_log
            - 'log_group_name = '
            - !Ref WebServerLogGroup
            - |+

            - |
                log_stream_name = {instance_id}/apache.log
            - 'datetime_format = %d/%b/%Y:%H:%M:%S'
        mode: '000400'
        owner: apache
        group: apache
        /var/www/html/index.php:
          content: !Join
            - ''
            - - |
                <?php
            - |

```

```

        echo '<h1>AWS CloudFormation sample PHP application</h1>';
    - |
    ?>
mode: '000644'
owner: apache
group: apache
/etc/cfn/cfn-hup.conf:
content: !Join
- ''
- - |
    [main]
- stack=
- !Ref 'AWS::StackId'
- |+

- region=
- !Ref 'AWS::Region'
- |+

mode: '000400'
owner: root
group: root
/etc/cfn/hooks.d/cfn-auto-reloader.conf:
content: !Join
- ''
- - |
    [cfn-auto-reloader-hook]
- |
    triggers=post.update
- >
    path=Resources.WebServerHost.Metadata.AWS::CloudFormation::Init
- 'action=/opt/aws/bin/cfn-init -s '
- !Ref 'AWS::StackId'
- ' -r WebServerHost '
- ' --region      '
- !Ref 'AWS::Region'
- |+

- |
    runas=root
services:
  sysvinit:
    httpd:
      enabled: 'true'

```

```

        ensureRunning: 'true'
    sendmail:
        enabled: 'false'
        ensureRunning: 'false'
CreationPolicy:
    ResourceSignal:
        Timeout: PT5M
Properties:
    ImageId: !FindInMap
        - RegionMap
        - !Ref 'AWS::Region'
        - AMI
    KeyName: !Ref KeyName
    InstanceType: t1.micro
    SecurityGroups:
        - !Ref WebServerSecurityGroup
    IamInstanceProfile: !Ref LogRoleInstanceProfile
    UserData: !Base64
        'Fn::Join':
            - ''
            - - |
                  #!/bin/bash -xe
                - |
                  # Get the latest CloudFormation package
                - |
                  yum install -y aws-cfn-bootstrap
                - |
                  # Start cfn-init
                - '/opt/aws/bin/cfn-init -s '
                - !Ref 'AWS::StackId'
                - ' -r WebServerHost '
                - ' --region '
                - !Ref 'AWS::Region'
                - |2
                  || error_exit 'Failed to run cfn-init'
            - >
                  # Start up the cfn-hup daemon to listen for changes to the EC2
                  instance metadata
                - |
                  /opt/aws/bin/cfn-hup || error_exit 'Failed to start cfn-hup'
                - |
                  # Get the CloudWatch Logs agent
            - >
                  wget

```

```

        https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-
setup.py
    - |
      # Install the CloudWatch Logs agent
    - 'python awslogs-agent-setup.py -n -r '
    - '!Ref 'AWS::Region'
    - |2
      -c /tmp/cwlogs/apacheaccess.conf || error_exit 'Failed to run CloudWatch
Logs agent setup'
    - |
      # All done so signal success
    - '/opt/aws/bin/cfn-signal -e $? '
    - '          --stack '
    - '!Ref 'AWS::StackName'
    - '          --resource WebServerHost '
    - '          --region '
    - '!Ref 'AWS::Region'
    - |+

WebServerLogGroup:
  Type: 'AWS::Logs::LogGroup'
  Properties:
    RetentionInDays: 7
404MetricFilter:
  Type: 'AWS::Logs::MetricFilter'
  Properties:
    LogGroupName: !Ref WebServerLogGroup
    FilterPattern: >-
      [ip, identity, user_id, timestamp, request, status_code = 404, size,
      ...]
    MetricTransformations:
      - MetricValue: '1'
        MetricNamespace: test/404s
        MetricName: test404Count
BytesTransferredMetricFilter:
  Type: 'AWS::Logs::MetricFilter'
  Properties:
    LogGroupName: !Ref WebServerLogGroup
    FilterPattern: '[ip, identity, user_id, timestamp, request, status_code,
size, ...]'
    MetricTransformations:
      - MetricValue: $size
        MetricNamespace: test/BytesTransferred
        MetricName: testBytesTransferred

```

404Alarm:

Type: 'AWS::CloudWatch::Alarm'

Properties:

AlarmDescription: The number of 404s is greater than 2 over 2 minutes

MetricName: test404Count

Namespace: test/404s

Statistic: Sum

Period: '60'

EvaluationPeriods: '2'

Threshold: '2'

AlarmActions:

- !Ref AlarmNotificationTopic

ComparisonOperator: GreaterThanThreshold

BandwidthAlarm:

Type: 'AWS::CloudWatch::Alarm'

Properties:

AlarmDescription: The average volume of traffic is greater 3500 KB over 10 minutes

MetricName: testBytesTransferred

Namespace: test/BytesTransferred

Statistic: Average

Period: '300'

EvaluationPeriods: '2'

Threshold: '3500'

AlarmActions:

- !Ref AlarmNotificationTopic

ComparisonOperator: GreaterThanThreshold

AlarmNotificationTopic:

Type: 'AWS::SNS::Topic'

Properties:**Subscription:**

- Endpoint: !Ref OperatorEmail

Protocol: email

Outputs:**InstanceId:**

Description: The instance ID of the web server

Value: !Ref WebServerHost

WebsiteURL:

Value: !Join

- ''

- - 'http://'

- !GetAtt

- WebServerHost

- PublicDnsName

```

    Description: URL for newly created LAMP stack
PublicIP:
    Description: Public IP address of the web server
    Value: !GetAtt
        - WebServerHost
        - PublicIp
CloudWatchLogGroupName:
    Description: The name of the CloudWatch log group
    Value: !Ref WebServerLogGroup

```

Invia i log a Logs da un'istanza di Windows CloudWatch

Il modello seguente configura i CloudWatch log per un'istanza di Windows 2012R2.

L'agente CloudWatch Logs su Windows (agente SSM su Windows 2012R2 e Windows 2016 AMIs) invia i log solo dopo l'avvio, quindi i log generati prima dell'avvio non vengono inviati. A questo proposito, il modello aiuta a garantire che l'agente venga avviato prima della scrittura dei log da:

- Impostazione della configurazione dell'agente come prima voce config in configSets cfn-init.
- Utilizzo di waitAfterCompletion per inserire una pausa dopo il comando che avvia l'agente.

JSON

```

{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Description": "Sample template that sets up and configures CloudWatch logs on Windows 2012R2 instance.",
    "Parameters": {
        "KeyPair": {
            "Description": "Name of an existing EC2 KeyPair to enable RDP access to the instances",
            "Type": "AWS::EC2::KeyPair::KeyName",
            "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
        },
        "RDPLocation": {
            "Description": "The IP address range that can be used to RDP to the EC2 instances",
            "Type": "String",
            "MinLength": "9",
            "MaxLength": "18",
            "Default": "0.0.0.0/0",

```



```

        "AllowedPattern": "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})/(\\d{1,2})",
        "ConstraintDescription": "must be a valid IP CIDR range of the form
x.x.x.x/x.",
    },
    "OperatorEmail": {
        "Description": "Email address to notify if there are any scaling
operations",
        "Type": "String"
    }
},
"Mappings": {
    "AWSAMIRegionMap": {
        "ap-northeast-1": {
            "WS2012R2": "ami-09e7006451ad8bf4d"
        },
        "ap-northeast-2": {
            "WS2012R2": "ami-0754980e4d02153f9"
        },
        "ap-south-1": {
            "WS2012R2": "ami-00ad91b37d56c1d08"
        },
        "ap-southeast-1": {
            "WS2012R2": "ami-09e7006451ad8bf4d"
        },
        "ap-southeast-2": {
            "WS2012R2": "ami-000d23d3067008aea"
        },
        "ca-central-1": {
            "WS2012R2": "ami-0d8e70862465b9da0"
        },
        "eu-central-1": {
            "WS2012R2": "ami-0c0f322f5676ba254"
        },
        "eu-west-1": {
            "WS2012R2": "ami-0a46adf18f8875ad6"
        },
        "eu-west-2": {
            "WS2012R2": "ami-0651428174d9438e9"
        },
        "sa-east-1": {
            "WS2012R2": "ami-08ebd138109a6c223"
        },
        "us-east-1": {

```

```

        "WS2012R2": "ami-0ef6fb504535468b2"
    },
    "us-east-2": {
        "WS2012R2": "ami-0f466c6044f510bd3"
    },
    "us-west-1": {
        "WS2012R2": "ami-026f68ef6465e6c09"
    },
    "us-west-2": {
        "WS2012R2": "ami-0274ca53943a86543"
    }
}
},
"Resources": {
    "WebServerSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Enable HTTP access via port 80 and RDP access via
port 3389",
            "SecurityGroupIngress": [
                {
                    "IpProtocol": "tcp",
                    "FromPort": "80",
                    "ToPort": "80",
                    "CidrIp": "0.0.0.0/0"
                },
                {
                    "IpProtocol": "tcp",
                    "FromPort": "3389",
                    "ToPort": "3389",
                    "CidrIp": {
                        "Ref": "RDPLocation"
                    }
                }
            ]
        }
    },
    "LogRole": {
        "Type": "AWS::IAM::Role",
        "Properties": {
            "AssumeRolePolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {

```

```

        "Effect": "Allow",
        "Principal": {
            "Service": [
                "ec2.amazonaws.com"
            ]
        },
        "Action": [
            "sts:AssumeRole"
        ]
    }
]
},
"ManagedPolicyArns": [
    "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
],
"Path": "/",
"Policies": [
    {
        "PolicyName": "LogRolePolicy",
        "PolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "logs:Create*",
                        "logs:PutLogEvents",
                        "s3:GetObject"
                    ],
                    "Resource": [
                        "arn:aws:logs:*:*:*",
                        "arn:aws:s3:::*"
                    ]
                }
            ]
        }
    }
]
},
"LogRoleInstanceProfile": {
    "Type": "AWS::IAM::InstanceProfile",
    "Properties": {
        "Path": "/",

```

```

        "Roles": [
            {
                "Ref": "LogRole"
            }
        ]
    },
    "WebServerHost": {
        "Type": "AWS::EC2::Instance",
        "CreationPolicy": {
            "ResourceSignal": {
                "Timeout": "PT15M"
            }
        }
    },
    "Metadata": {
        "AWS::CloudFormation::Init": {
            "configSets": {
                "config": [
                    "00-ConfigureCWLogs",
                    "01-InstallWebServer",
                    "02-ConfigureApplication",
                    "03-Finalize"
                ]
            },
            "00-ConfigureCWLogs": {
                "files": {
                    "C:\\Program Files\\Amazon\\SSM\\Plugins\\awsCloudWatch\\
\\AWS.EC2.Windows.CloudWatch.json": {
                        "content": {
                            "Fn::Sub": "{\n  \"EngineConfiguration
\": {\n    \"Components\": [\n      {\n        \"FullName\":
\\\"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch
\\",\n        \"Id\": \"ApplicationEventLog\",\n        \"Parameters\":
{\n          \"Levels\": \"7\",\n          \"LogName\": \"Application
\\",\n        }\n      },\n      {\n        \"FullName\":
\\\"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch
\\",\n        \"Id\": \"SystemEventLog\",\n        \"Parameters\":
{\n          \"Levels\": \"7\",\n          \"LogName\": \"System
\\",\n        }\n      },\n      {\n        \"FullName\":
\\\"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch
\\",\n        \"Id\": \"SecurityEventLog\",\n        \"Parameters\":
{\n          \"Levels\": \"7\",\n          \"LogName\": \"Security
\\",\n        }\n      }\n    }\n  }\n}"

```

```

\","Id\":"EC2ConfigLog\","Parameters
\":" {
  \"CultureName\": \"en-US\",
  \"Encoding\": \"ASCII\",
  \"Filter\": \"EC2ConfigLog.txt\",
  \"LogDirectoryPath\": \"C:\\\\Program Files\\\\Amazon
  \\\\"Ec2ConfigService\\\\\\Logs\",
  \"TimeZoneKind\": \"UTC\",
  \"TimestampFormat\": \"yyyy-MM-ddTHH:mm:ss.fffZ\",
  }
  },
  {
    \"FullName\":
    \"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch
  },
  \"Id\": \"CfnInitLog\",
  \"Parameters\": {
    \"CultureName\": \"en-US\",
    \"Encoding\":
    \"ASCII\",
    \"Filter\": \"cfn-init.log\",
    \"LogDirectoryPath\": \"C:\\\\cfn\\\\\\log\",
    \"TimeZoneKind
  \": \"Local\",
    \"TimestampFormat\": \"yyyy-MM-dd HH:mm:ss,fff
  \"
    }
    },
    {
      \"FullName\":
      \"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch
  },
  \"Id\": \"IISLogs\",
  \"Parameters\": {
    \"CultureName\": \"en-US\",
    \"Encoding\": \"UTF-8\",
    \"Filter\": \"\",
    \"LineCount\": \"3\",
    \"LogDirectoryPath\": \"C:\\\\inetpub\\\\\\logs\\\\\\LogFiles\\\\\\W3SVC1\",
    \"TimeZoneKind\": \"UTC\",
    \"TimestampFormat\": \"yyyy-MM-
  dd HH:mm:ss\",
  }
  },
  {
    \"FullName\":
    \"AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComponent,AWS.
  },
  \"Id\": \"MemoryPerformanceCounter\",
  \"Parameters\": {
    \"CategoryName\": \"Memory\",
    \"CounterName
  \": \"Available MBytes\",
    \"DimensionName\": \"\",
    \"DimensionValue\": \"\",
    \"InstanceName\": \"\",
    \"MetricName\": \"Memory\",
    \"Unit\":
    \"Megabytes\",
  }
  },
  {
    \"FullName
  \": \"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch\",
    \"Id\": \"CloudWatchApplicationEventLog\",
    \"Parameters
  \": {
    \"AccessKey\": \"\",
    \"LogGroup\":
    \"${LogGroup}\",
    \"LogStream\": \"{instance_id}/ApplicationEventLog
  \",
    \"Region\": \"${AWS::Region}\",
    \"SecretKey
  \": \"\"
  }
  },
  {
    \"FullName\":
    \"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch\",
    \"Id\": \"CloudWatchSystemEventLog\",
    \"Parameters
  \": {
    \"AccessKey\": \"\",
    \"LogGroup\":
    \"${LogGroup}\",
    \"LogStream\": \"{instance_id}/SystemEventLog
  \",
    \"Region\": \"${AWS::Region}\",
    \"SecretKey
  \": \"\"
  }
  },
  {
    \"FullName\":
    \"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch\",
    \"Id\": \"CloudWatchSecurityEventLog\",
    \"Parameters
  \": {
    \"AccessKey\": \"\",
    \"LogGroup\":
    \"${LogGroup}\",
    \"LogStream\": \"{instance_id}/SecurityEventLog

```

```

\","\\n
\\": \\""\\n
\\AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch\\",
\\n
\\Id\\": \\CloudWatchEC2ConfigLog\\",\\n
\\Parameters
\\": {\\n
\\AccessKey\\": \\",\\n
\\LogGroup\\":
\\${LogGroup}\\",\\n
\\LogStream\\": \\{instance_id}/EC2ConfigLog\\",
\\n
\\Region\\": \\${AWS::Region}\\",\\n
\\SecretKey
\\": \\""\\n
}\\n
}\\n
}\\n
\\FullName
\\": \\AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch
\\",\\n
\\Id\\": \\CloudWatchCfnInitLog\\",\\n
\\Parameters
\\": {\\n
\\AccessKey\\": \\",\\n
\\LogGroup\\":
\\${LogGroup}\\",\\n
\\LogStream\\": \\{instance_id}/CfnInitLog\\",
\\n
\\Region\\": \\${AWS::Region}\\",\\n
\\SecretKey
\\": \\""\\n
}\\n
}\\n
}\\n
\\FullName
\\": \\AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch
\\",\\n
\\Id\\": \\CloudWatchIISLogs\\",\\n
\\Parameters
\\": {\\n
\\AccessKey\\": \\",\\n
\\LogGroup\\":
\\${LogGroup}\\",\\n
\\LogStream\\": \\{instance_id}/IISLogs\\",\\n
\\Region\\": \\${AWS::Region}\\",\\n
\\SecretKey
\\": \\""\\n
}\\n
}\\n
}\\n
\\FullName\\":
\\AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputComponent,AWS.EC2.Windows.CloudWatch
\\",\\n
\\Id\\": \\CloudWatch\\",\\n
\\Parameters\\": {\\n
\\AccessKey\\": \\",\\n
\\Namespace\\": \\Windows/
Default\\",\\n
\\Region\\": \\${AWS::Region}\\",\\n
\\SecretKey\\": \\""\\n
}\\n
}\\n
]\\n
]\\n
\\Flows\\": {\\n
\\Flows\\": [\\n
\\ApplicationEventLog,CloudWatchApplicationEventLog
\\",\\n
\\SystemEventLog,CloudWatchSystemEventLog\\",\\n
\\SecurityEventLog,CloudWatchSecurityEventLog\\",\\n
\\EC2ConfigLog,CloudWatchEC2ConfigLog\\",\\n
\\CfnInitLog,CloudWatchCfnInitLog\\",\\n
\\IISLogs,CloudWatchIISLogs\\",\\n
\\MemoryPerformanceCounter,CloudWatch\\""\\n
]\\n
}\\n
\\PollInterval\\": \\00:00:05\\""\\n
}\\n
\\IsEnabled\\": true\\n}\\n"
}
}
},
"commands": {
"0-enableSSM": {
"command": "powershell.exe -Command \\Set-Service -Name
AmazonSSMAgent -StartupType Automatic\\",
"waitAfterCompletion": "0"
},
"1-restartSSM": {
"command": "powershell.exe -Command \\Restart-Service
AmazonSSMAgent \\",

```

```

        "waitAfterCompletion": "30"
    }
}
},
"01-InstallWebServer": {
    "commands": {
        "01_install_webserver": {
            "command": "powershell.exe -Command \"Install-
WindowsFeature Web-Server -IncludeAllSubFeature\\\"\",
            "waitAfterCompletion": "0"
        }
    }
},
"02-ConfigureApplication": {
    "files": {
        "c:\\Inetpub\\wwwroot\\index.htm": {
            "content": "<html> <head> <title>Test Application
Page</title> </head> <body> <h1>Congratulations !! Your IIS server is configured.</h1>
</body> </html>"
        }
    }
},
"03-Finalize": {
    "commands": {
        "00_signal_success": {
            "command": {
                "Fn::Sub": "cfn-signal.exe -e 0 --resource
WebServerHost --stack ${AWS::StackName} --region ${AWS::Region}"
            },
            "waitAfterCompletion": "0"
        }
    }
}
},
"Properties": {
    "KeyName": {
        "Ref": "KeyPair"
    },
    "ImageId": {
        "Fn::FindInMap": [
            "AWSAMIRegionMap",
            {
                "Ref": "AWS::Region"
            }
        ]
    }
}
}

```

```

        },
        "WS2012R2"
    ]
},
"InstanceType": "t2.xlarge",
"SecurityGroupIds": [
    {
        "Ref": "WebServerSecurityGroup"
    }
],
"IamInstanceProfile": {
    "Ref": "LogRoleInstanceProfile"
},
"UserData": {
    "Fn::Base64": {
        "Fn::Sub": "<script>\nwmic product where \"description='Amazon
SSM Agent' \" uninstall\nwmic product where \"description='aws-cfn-bootstrap'
\" uninstall \nstart /wait c:\\\\Windows\\\\system32\\\\msiexec /passive /qn /i
https://s3.amazonaws.com/cloudformation-examples/aws-cfn-bootstrap-win64-latest.msi
\npowershell.exe -Command \"iwr https://s3.amazonaws.com/ec2-downloads-windows/
SSMAgent/latest/windows_amd64/AmazonSSMAgentSetup.exe -UseBasicParsing -OutFile C:
\\\\AmazonSSMAgentSetup.exe\" \nstart /wait C:\\\\AmazonSSMAgentSetup.exe /install /
quiet\ncfn-init.exe -v -c config -s ${AWS::StackName} --resource WebServerHost --region
${AWS::Region} \n</script>\n"
    }
}
},
"LogGroup": {
    "Type": "AWS::Logs::LogGroup",
    "Properties": {
        "RetentionInDays": 7
    }
},
"404MetricFilter": {
    "Type": "AWS::Logs::MetricFilter",
    "Properties": {
        "LogGroupName": {
            "Ref": "LogGroup"
        },
        "FilterPattern": "[timestamps, serverip, method, uri, query, port,
dash, clientip, useragent, status_code = 404, ...]",
        "MetricTransformations": [
            {

```



```

        "MetricValue": "1",
        "MetricNamespace": "test/404s",
        "MetricName": "test404Count"
    }
]
},
"404Alarm": {
    "Type": "AWS::CloudWatch::Alarm",
    "Properties": {
        "AlarmDescription": "The number of 404s is greater than 2 over 2
minutes",
        "MetricName": "test404Count",
        "Namespace": "test/404s",
        "Statistic": "Sum",
        "Period": "60",
        "EvaluationPeriods": "2",
        "Threshold": "2",
        "AlarmActions": [
            {
                "Ref": "AlarmNotificationTopic"
            }
        ],
        "ComparisonOperator": "GreaterThanThreshold"
    }
},
"AlarmNotificationTopic": {
    "Type": "AWS::SNS::Topic",
    "Properties": {
        "Subscription": [
            {
                "Endpoint": {
                    "Ref": "OperatorEmail"
                },
                "Protocol": "email"
            }
        ]
    }
},
"Outputs": {
    "InstanceId": {
        "Description": "The instance ID of the web server",
        "Value": {

```

```

        "Ref": "WebServerHost"
    },
    "WebsiteURL": {
        "Value": {
            "Fn::Sub": "http://${WebServerHost.PublicDnsName}"
        },
        "Description": "URL for newly created IIS web server"
    },
    "PublicIP": {
        "Description": "Public IP address of the web server",
        "Value": {
            "Fn::GetAtt": [
                "WebServerHost",
                "PublicIp"
            ]
        }
    },
    "CloudWatchLogGroupName": {
        "Description": "The name of the CloudWatch log group",
        "Value": {
            "Ref": "LogGroup"
        }
    }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: >-
  Sample template that sets up and configures CloudWatch logs on Windows 2012R2
  instance instance.
Parameters:
  KeyPair:
    Description: Name of an existing EC2 KeyPair to enable RDP access to the instances
    Type: 'AWS::EC2::KeyPair::KeyName'
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  RDPLocation:
    Description: The IP address range that can be used to RDP to the EC2 instances
    Type: String
    MinLength: '9'
    MaxLength: '18'

```

```
Default: 0.0.0.0/0
AllowedPattern: '(\d{1,3})\.\d{1,3})\.\d{1,3})\.\d{1,3})/(\d{1,2})'
ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
```

OperatorEmail:

Description: Email address to notify if there are any scaling operations

Type: String

Mappings:**AWSAMIRegionMap:****ap-northeast-1:**

WS2012R2: ami-09e7006451ad8bf4d

ap-northeast-2:

WS2012R2: ami-0754980e4d02153f9

ap-south-1:

WS2012R2: ami-00ad91b37d56c1d08

ap-southeast-1:

WS2012R2: ami-09e7006451ad8bf4d

ap-southeast-2:

WS2012R2: ami-000d23d3067008aea

ca-central-1:

WS2012R2: ami-0d8e70862465b9da0

eu-central-1:

WS2012R2: ami-0c0f322f5676ba254

eu-west-1:

WS2012R2: ami-0a46adf18f8875ad6

eu-west-2:

WS2012R2: ami-0651428174d9438e9

sa-east-1:

WS2012R2: ami-08ebd138109a6c223

us-east-1:

WS2012R2: ami-0ef6fb504535468b2

us-east-2:

WS2012R2: ami-0f466c6044f510bd3

us-west-1:

WS2012R2: ami-026f68ef6465e6c09

us-west-2:

WS2012R2: ami-0274ca53943a86543

Resources:**WebServerSecurityGroup:**

Type: 'AWS::EC2::SecurityGroup'

Properties:

GroupDescription: Enable HTTP access via port 80 and RDP access via port 3389

SecurityGroupIngress:

- IpProtocol: tcp

FromPort: '80'

```
        ToPort: '80'
        CidrIp: 0.0.0.0/0
    - IpProtocol: tcp
      FromPort: '3389'
      ToPort: '3389'
      CidrIp: !Ref RDPLocation
LogRole:
  Type: 'AWS::IAM::Role'
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - 'sts:AssumeRole'
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore'
  Path: /
  Policies:
    - PolicyName: LogRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - 'logs:Create*'
              - 'logs:PutLogEvents'
              - 's3:GetObject'
            Resource:
              - 'arn:aws:logs:*:*:*'
              - 'arn:aws:s3:::*'
LogRoleInstanceProfile:
  Type: 'AWS::IAM::InstanceProfile'
  Properties:
    Path: /
    Roles:
      - !Ref LogRole
WebServerHost:
  Type: 'AWS::EC2::Instance'
  CreationPolicy:
    ResourceSignal:
```

```

    Timeout: PT15M
Metadata:
  'AWS::CloudFormation::Init':
    configSets:
      config:
        - 00-ConfigureCWLogs
        - 01-InstallWebServer
        - 02-ConfigureApplication
        - 03-Finalize
    00-ConfigureCWLogs:
      files:
        'C:\Program Files\Amazon\SSM\Plugins\awsCloudWatch
\AWS.EC2.Windows.CloudWatch.json':
          content: !Sub |
            {
              "EngineConfiguration": {
                "Components": [
                  {
                    "FullName":
"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
                    "Id": "ApplicationEventLog",
                    "Parameters": {
                      "Levels": "7",
                      "LogName": "Application"
                    }
                  },
                  {
                    "FullName":
"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
                    "Id": "SystemEventLog",
                    "Parameters": {
                      "Levels": "7",
                      "LogName": "System"
                    }
                  },
                  {
                    "FullName":
"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
                    "Id": "SecurityEventLog",
                    "Parameters": {
                      "Levels": "7",
                      "LogName": "Security"
                    }
                  }
                ]
              }
            }

```

```

        {
            "FullName":
"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
            "Id": "EC2ConfigLog",
            "Parameters": {
                "CultureName": "en-US",
                "Encoding": "ASCII",
                "Filter": "EC2ConfigLog.txt",
                "LogDirectoryPath": "C:\\Program Files\\Amazon\\
\\Ec2ConfigService\\Logs",
                "TimeZoneKind": "UTC",
                "TimestampFormat": "yyyy-MM-ddTHH:mm:ss.fffZ:"
            }
        },
        {
            "FullName":
"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
            "Id": "CfnInitLog",
            "Parameters": {
                "CultureName": "en-US",
                "Encoding": "ASCII",
                "Filter": "cfn-init.log",
                "LogDirectoryPath": "C:\\cfn\\log",
                "TimeZoneKind": "Local",
                "TimestampFormat": "yyyy-MM-dd HH:mm:ss,fff"
            }
        },
        {
            "FullName":
"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
            "Id": "IISLogs",
            "Parameters": {
                "CultureName": "en-US",
                "Encoding": "UTF-8",
                "Filter": "",
                "LineCount": "3",
                "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\
\\W3SVC1",
                "TimeZoneKind": "UTC",
                "TimestampFormat": "yyyy-MM-dd HH:mm:ss"
            }
        },
        {

```

```

        "FullName":
"AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComponent,AWS.E
        "Id": "MemoryPerformanceCounter",
        "Parameters": {
            "CategoryName": "Memory",
            "CounterName": "Available MBytes",
            "DimensionName": "",
            "DimensionValue": "",
            "InstanceName": "",
            "MetricName": "Memory",
            "Unit": "Megabytes"
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchApplicationEventLog",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",
            "LogStream": "{instance_id}/ApplicationEventLog",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchSystemEventLog",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",
            "LogStream": "{instance_id}/SystemEventLog",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchSecurityEventLog",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",

```

```

        "LogStream": "{instance_id}/SecurityEventLog",
        "Region": "${AWS::Region}",
        "SecretKey": ""
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchEC2ConfigLog",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",
            "LogStream": "{instance_id}/EC2ConfigLog",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchCfnInitLog",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",
            "LogStream": "{instance_id}/CfnInitLog",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
        "Id": "CloudWatchIISLogs",
        "Parameters": {
            "AccessKey": "",
            "LogGroup": "${LogGroup}",
            "LogStream": "{instance_id}/IISLogs",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    {
        "FullName":
"AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputComponent,AWS.EC2.Windows.CloudWatch",

```



```

        "Id": "CloudWatch",
        "Parameters": {
            "AccessKey": "",
            "Namespace": "Windows/Default",
            "Region": "${AWS::Region}",
            "SecretKey": ""
        }
    },
    "Flows": {
        "Flows": [
            "ApplicationEventLog,CloudWatchApplicationEventLog",
            "SystemEventLog,CloudWatchSystemEventLog",
            "SecurityEventLog,CloudWatchSecurityEventLog",
            "EC2ConfigLog,CloudWatchEC2ConfigLog",
            "CfnInitLog,CloudWatchCfnInitLog",
            "IISLogs,CloudWatchIISLogs",
            "MemoryPerformanceCounter,CloudWatch"
        ]
    },
    "PollInterval": "00:00:05"
},
"IsEnabled": true
}
commands:
  0-enableSSM:
    command: >-
      powershell.exe -Command "Set-Service -Name AmazonSSMAgent
        -StartupType Automatic"
    waitAfterCompletion: '0'
  1-restartSSM:
    command: powershell.exe -Command "Restart-Service AmazonSSMAgent "
    waitAfterCompletion: '30'
01-InstallWebServer:
  commands:
    01_install_webserver:
      command: >-
        powershell.exe -Command "Install-WindowsFeature Web-Server
          -IncludeAllSubFeature"
      waitAfterCompletion: '0'
02-ConfigureApplication:
  files:
    'c:\Inetpub\wwwroot\index.htm':
      content: >-

```

```

        <html> <head> <title>Test Application Page</title> </head>
        <body> <h1>Congratulations !! Your IIS server is
        configured.</h1> </body> </html>
03-Finalize:
  commands:
    00_signal_success:
      command: !Sub >-
        cfn-signal.exe -e 0 --resource WebServerHost --stack
        ${AWS::StackName} --region ${AWS::Region}
      waitAfterCompletion: '0'
Properties:
  KeyName: !Ref KeyPair
  ImageId: !FindInMap
    - AWSAMIRegionMap
    - !Ref 'AWS::Region'
    - WS2012R2
  InstanceType: t2.xlarge
  SecurityGroupIds:
    - !Ref WebServerSecurityGroup
  IamInstanceProfile: !Ref LogRoleInstanceProfile
  UserData: !Base64
    'Fn::Sub': >
      <script>

        wmic product where "description='Amazon SSM Agent' " uninstall

        wmic product where "description='aws-cfn-bootstrap' " uninstall

        start /wait c:\\Windows\\system32\\msiexec /passive /qn /i
        https://s3.amazonaws.com/cloudformation-examples/aws-cfn-bootstrap-win64-
latest.msi

        powershell.exe -Command "iwr
        https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/windows_amd64/
AmazonSSMAgentSetup.exe
        -UseBasicParsing -OutFile C:\\AmazonSSMAgentSetup.exe"

        start /wait C:\\AmazonSSMAgentSetup.exe /install /quiet

        cfn-init.exe -v -c config -s ${AWS::StackName} --resource
        WebServerHost --region ${AWS::Region}

      </script>
  LogGroup:

```

```
Type: 'AWS::Logs::LogGroup'
Properties:
  RetentionInDays: 7
404MetricFilter:
  Type: 'AWS::Logs::MetricFilter'
  Properties:
    LogGroupName: !Ref LogGroup
    FilterPattern: >-
      [timestamps, serverip, method, uri, query, port, dash, clientip,
       useragent, status_code = 404, ...]
    MetricTransformations:
      - MetricValue: '1'
        MetricNamespace: test/404s
        MetricName: test404Count
404Alarm:
  Type: 'AWS::CloudWatch::Alarm'
  Properties:
    AlarmDescription: The number of 404s is greater than 2 over 2 minutes
    MetricName: test404Count
    Namespace: test/404s
    Statistic: Sum
    Period: '60'
    EvaluationPeriods: '2'
    Threshold: '2'
    AlarmActions:
      - !Ref AlarmNotificationTopic
    ComparisonOperator: GreaterThanThreshold
AlarmNotificationTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: !Ref OperatorEmail
        Protocol: email
Outputs:
  InstanceId:
    Description: The instance ID of the web server
    Value: !Ref WebServerHost
  WebsiteURL:
    Value: !Sub 'http://${WebServerHost.PublicDnsName}'
    Description: URL for newly created IIS web server
  PublicIP:
    Description: Public IP address of the web server
    Value: !GetAtt
      - WebServerHost
```

```
- PublicIp
CloudWatchLogGroupName:
  Description: The name of the CloudWatch log group
  Value: !Ref LogGroup
```

Consulta anche

Per ulteriori informazioni sulle risorse Logs, consulta o. CloudWatch

[AWS::Logs::LogGroup](#)[AWS::Logs::MetricFilter](#)

Frammenti di modello Amazon DynamoDB

Argomenti

- [Application Auto Scaling con una tabella Amazon DynamoDB](#)
- [Consulta anche](#)

Application Auto Scaling con una tabella Amazon DynamoDB

In questo esempio Application Auto Scaling viene configurato per una risorsa `AWS::DynamoDB::Table`. Il modello definisce una policy di dimensionamento `TargetTrackingScaling` che aumenta il throughput `WriteCapacityUnits` della tabella.

JSON

```
{
  "Resources": {
    "DDBTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "AttributeDefinitions": [
          {
            "AttributeName": "ArtistId",
            "AttributeType": "S"
          },
          {
            "AttributeName": "Concert",
            "AttributeType": "S"
          },
          {
            "AttributeName": "TicketSales",
            "AttributeType": "S"
          }
        ]
      }
    }
  }
}
```

```

        }
    ],
    "KeySchema": [
        {
            "AttributeName": "ArtistId",
            "KeyType": "HASH"
        },
        {
            "AttributeName": "Concert",
            "KeyType": "RANGE"
        }
    ],
    "GlobalSecondaryIndexes": [
        {
            "IndexName": "GSI",
            "KeySchema": [
                {
                    "AttributeName": "TicketSales",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "ProjectionType": "KEYS_ONLY"
            },
            "ProvisionedThroughput": {
                "ReadCapacityUnits": 5,
                "WriteCapacityUnits": 5
            }
        }
    ],
    "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 5
    }
},
"WriteCapacityScalableTarget": {
    "Type": "AWS::ApplicationAutoScaling::ScalableTarget",
    "Properties": {
        "MaxCapacity": 15,
        "MinCapacity": 5,
        "ResourceId": {
            "Fn::Join": [
                "/",

```

```

        [
            "table",
            {
                "Ref": "DDBTable"
            }
        ]
    ],
    "RoleARN": {
        "Fn::GetAtt": [
            "ScalingRole",
            "Arn"
        ]
    },
    "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
    "ServiceNamespace": "dynamodb"
},
"ScalingRole": {
    "Type": "AWS::IAM::Role",
    "Properties": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": [
                            "application-autoscaling.amazonaws.com"
                        ]
                    },
                    "Action": [
                        "sts:AssumeRole"
                    ]
                }
            ]
        }
    },
    "Path": "/",
    "Policies": [
        {
            "PolicyName": "root",
            "PolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [

```

```

    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:SetAlarmState",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource": "*"
    }
  ]
}

},
"WriteScalingPolicy": {
  "Type": "AWS::ApplicationAutoScaling::ScalingPolicy",
  "Properties": {
    "PolicyName": "WriteAutoScalingPolicy",
    "PolicyType": "TargetTrackingScaling",
    "ScalingTargetId": {
      "Ref": "WriteCapacityScalableTarget"
    },
    "TargetTrackingScalingPolicyConfiguration": {
      "TargetValue": 50,
      "ScaleInCooldown": 60,
      "ScaleOutCooldown": 60,
      "PredefinedMetricSpecification": {
        "PredefinedMetricType": "DynamoDBWriteCapacityUtilization"
      }
    }
  }
}
}
}
}

```

YAML

Resources:

```
DDBTable:
  Type: AWS::DynamoDB::Table
  Properties:
    AttributeDefinitions:
      -
        AttributeName: "ArtistId"
        AttributeType: "S"
      -
        AttributeName: "Concert"
        AttributeType: "S"
      -
        AttributeName: "TicketSales"
        AttributeType: "S"
    KeySchema:
      -
        AttributeName: "ArtistId"
        KeyType: "HASH"
      -
        AttributeName: "Concert"
        KeyType: "RANGE"
    GlobalSecondaryIndexes:
      -
        IndexName: "GSI"
        KeySchema:
          -
            AttributeName: "TicketSales"
            KeyType: "HASH"
        Projection:
          ProjectionType: "KEYS_ONLY"
        ProvisionedThroughput:
          ReadCapacityUnits: 5
          WriteCapacityUnits: 5
    ProvisionedThroughput:
      ReadCapacityUnits: 5
      WriteCapacityUnits: 5
  WriteCapacityScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    Properties:
      MaxCapacity: 15
      MinCapacity: 5
      ResourceId: !Join
        - /
        - - table
        - !Ref DDBTable
```



```
    RoleARN: !GetAtt ScalingRole.Arn
    ScalableDimension: dynamodb:table:WriteCapacityUnits
    ServiceNamespace: dynamodb
ScalingRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        -
          Effect: "Allow"
          Principal:
            Service:
              - application-autoscaling.amazonaws.com
          Action:
            - "sts:AssumeRole"
    Path: "/"
  Policies:
    -
      PolicyName: "root"
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          -
            Effect: "Allow"
            Action:
              - "dynamodb:DescribeTable"
              - "dynamodb:UpdateTable"
              - "cloudwatch:PutMetricAlarm"
              - "cloudwatch:DescribeAlarms"
              - "cloudwatch:GetMetricStatistics"
              - "cloudwatch:SetAlarmState"
              - "cloudwatch>DeleteAlarms"
            Resource: "*"
WriteScalingPolicy:
  Type: AWS::ApplicationAutoScaling::ScalingPolicy
  Properties:
    PolicyName: WriteAutoScalingPolicy
    PolicyType: TargetTrackingScaling
    ScalingTargetId: !Ref WriteCapacityScalableTarget
    TargetTrackingScalingPolicyConfiguration:
      TargetValue: 50.0
      ScaleInCooldown: 60
      ScaleOutCooldown: 60
```

```
PredefinedMetricSpecification:  
  PredefinedMetricType: DynamoDBWriteCapacityUtilization
```

Consulta anche

Per ulteriori informazioni, consulta il post del blog [How to use AWS CloudFormation to configure auto scaling for DynamoDB table and index on the Database Blog](#). AWS

Per ulteriori informazioni sulle risorse DynamoDB, vedere. [AWS::DynamoDB::Table](#)

Frammenti EC2 CloudFormation di modello Amazon

Amazon EC2 fornisce capacità di elaborazione scalabile in Cloud AWS. Puoi usare Amazon EC2 per avviare tutti o pochi server virtuali di cui hai bisogno, configurare sicurezza e rete e gestire lo storage. Questi server virtuali, noti come istanze, possono eseguire una varietà di sistemi operativi e applicazioni, e possono essere personalizzati per soddisfare requisiti specifici. Amazon ti EC2 consente di scalare verso l'alto o verso il basso per gestire i cambiamenti nei requisiti o i picchi di utilizzo.

Puoi definire e fornire EC2 istanze Amazon come parte della tua infrastruttura utilizzando CloudFormation modelli. I modelli semplificano la gestione e l'automazione della distribuzione delle EC2 risorse Amazon in modo ripetibile e coerente.

I seguenti frammenti di modello di esempio descrivono CloudFormation risorse o componenti per Amazon. EC2 Questi frammenti sono progettati per essere integrati in un modello e non sono destinati a essere eseguiti in modo indipendente.

Categorie dei frammenti

- [Configura le EC2 istanze Amazon con CloudFormation](#)
- [Crea modelli di lancio con CloudFormation](#)
- [Gestisci i gruppi di sicurezza con CloudFormation](#)
- [Alloca e associa indirizzi IP elastici con CloudFormation](#)
- [Configura le risorse Amazon VPC con CloudFormation](#)

Configura le EC2 istanze Amazon con CloudFormation

I seguenti frammenti mostrano come configurare le EC2 istanze Amazon utilizzando CloudFormation

Categorie dei frammenti

- [EC2Configurazioni generali di Amazon](#)
- [Specifica della mappatura dei dispositivi a blocchi per un'istanza](#)

EC2Configurazioni generali di Amazon

I seguenti frammenti mostrano le configurazioni generali per l'utilizzo delle istanze Amazon EC2 . CloudFormation

Frammenti di esempio

- [Crea un' EC2 istanza Amazon in una zona di disponibilità specificata](#)
- [Configura un' EC2 istanza Amazon con tag con un volume EBS e dati utente](#)
- [Definisci il nome della tabella DynamoDB nei dati utente per il lancio dell'istanza Amazon EC2](#)
- [Creazione di un volume Amazon EBS con DeletionPolicy](#)

Crea un' EC2 istanza Amazon in una zona di disponibilità specificata

Il seguente frammento crea un' EC2 istanza Amazon nella zona di disponibilità specificata utilizzando una [AWS::EC2::Instance](#) risorsa. Il codice per la zona di disponibilità è il codice della Regione seguito da un identificatore con una lettera. Puoi avviare un'istanza in una singola zona di disponibilità.

JSON

```
"Ec2Instance": {
  "Type": "AWS::EC2::Instance",
  "Properties": {
    "AvailabilityZone": "aa-example-1a",
    "ImageId": "ami-1234567890abcdef0"
  }
}
```

YAML

```
Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    AvailabilityZone: aa-example-1a
    ImageId: ami-1234567890abcdef0
```

Configura un' EC2 istanza Amazon con tag con un volume EBS e dati utente

Il seguente frammento crea un' EC2 istanza Amazon con un tag, un volume EBS e dati utente.

Utilizza una risorsa. [AWS::EC2::Instance](#) Nello stesso modello, è necessario definire una [AWS::EC2::SecurityGroup](#)risorsa, una [AWS::SNS::Topic](#)risorsa e una [AWS::EC2::Volume](#)risorsa. Il KeyName deve essere definito nella sezione Parameters del modello.

I tag possono aiutarti a classificare AWS le risorse in base alle tue preferenze, ad esempio per scopo, proprietario o ambiente. I dati utente consentono di fornire script o dati personalizzati a un'istanza durante il lancio. Questi dati aiutano ad automatizzare le attività, configurare il software, installare i pacchetti e compiere altre azioni su un'istanza durante l'inizializzazione.

Per ulteriori informazioni sull'etichettatura delle tue risorse, consulta [Tagga le tue EC2 risorse Amazon](#) nella Amazon EC2 User Guide.

Per informazioni sui dati utente, consulta [Usa i metadati dell'istanza per gestire l' EC2 istanza](#) nella Amazon EC2 User Guide.

JSON

```
"Ec2Instance": {
  "Type": "AWS::EC2::Instance",
  "Properties": {
    "KeyName": { "Ref": "KeyName" },
    "SecurityGroups": [ { "Ref": "Ec2SecurityGroup" } ],
    "UserData": {
      "Fn::Base64": {
        "Fn::Join": [ ":", [
          "PORT=80",
          "TOPIC=",
          { "Ref": "MySNSTopic" }
        ]
        ]
      }
    },
    "InstanceType": "aa.size",
    "AvailabilityZone": "aa-example-1a",
    "ImageId": "ami-1234567890abcdef0",
    "Volumes": [
      {
        "VolumeId": { "Ref": "MyVolumeResource" },
        "Device": "/dev/sdk"
      }
    ]
  }
}
```

```
    ],
    "Tags": [ { "Key": "Name", "Value": "MyTag" } ]
  }
}
```

YAML

```
Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    KeyName: !Ref KeyName
    SecurityGroups:
      - !Ref Ec2SecurityGroup
    UserData:
      Fn::Base64:
        Fn::Join:
          - ":"
          - - "PORT=80"
            - "TOPIC="
            - !Ref MySNSTopic
    InstanceType: aa.size
    AvailabilityZone: aa-example-1a
    ImageId: ami-1234567890abcdef0
    Volumes:
      - VolumeId: !Ref MyVolumeResource
        Device: "/dev/sdk"
    Tags:
      - Key: Name
        Value: MyTag
```

Definisci il nome della tabella DynamoDB nei dati utente per il lancio dell'istanza Amazon EC2

Il seguente frammento crea un' EC2 istanza Amazon e definisce un nome di tabella DynamoDB nei dati utente da passare all'istanza all'avvio. Utilizza una risorsa. [AWS::EC2::Instance](#) È possibile definire parametri o valori dinamici nei dati utente per passare un' EC2 istanza all'avvio.

Per ulteriori informazioni sui dati utente, consulta [Usa i metadati dell'istanza per gestire l' EC2 istanza](#) nella Amazon EC2 User Guide.

JSON

```
"Ec2Instance": {
```

```

    "Type": "AWS::EC2::Instance",
    "Properties": {
      "UserData": {
        "Fn::Base64": {
          "Fn::Join": [
            "",
            [
              "TableName=",
              {
                "Ref": "DynamoDBTableName"
              }
            ]
          ]
        },
        "AvailabilityZone": "aa-example-1a",
        "ImageId": "ami-1234567890abcdef0"
      }
    }
  }
}

```

YAML

```

Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    UserData:
      Fn::Base64:
        Fn::Join:
          - ''
          - - 'TableName='
            - Ref: DynamoDBTableName
    AvailabilityZone: aa-example-1a
    ImageId: ami-1234567890abcdef0

```

Creazione di un volume Amazon EBS con **DeletionPolicy**

I seguenti frammenti creano un volume Amazon EBS utilizzando una risorsa Amazon. EC2 [AWS::EC2::Volume](#). Puoi utilizzare le proprietà `Size` o `SnapshotID` per definire il volume, ma non entrambe. Un attributo `DeletionPolicy` viene impostato per creare uno snapshot del volume quando lo stack viene eliminato.

Per ulteriori informazioni sull'attributo `DeletionPolicy`, consulta l'[attributo DeletionPolicy](#).

Per ulteriori informazioni sulla creazione di volumi Amazon EBS, consulta [Creazione di un volume Amazon EBS](#).

JSON

Questo frammento crea un volume Amazon EBS con una dimensione specificata. La dimensione è impostata su 10, ma è possibile regolarla in base alle esigenze. La [AWS::EC2::Volume](#) risorsa consente di specificare la dimensione o l'ID di uno snapshot, ma non entrambi.

```
"MyEBSVolume": {
  "Type": "AWS::EC2::Volume",
  "Properties": {
    "Size": "10",
    "AvailabilityZone": {
      "Ref": "AvailabilityZone"
    }
  },
  "DeletionPolicy": "Snapshot"
}
```

Questo frammento crea un volume Amazon EBS utilizzando un ID snapshot fornito. La [AWS::EC2::Volume](#) risorsa consente di specificare la dimensione o l'ID di un'istantanea, ma non entrambi.

```
"MyEBSVolume": {
  "Type": "AWS::EC2::Volume",
  "Properties": {
    "SnapshotId" : "snap-1234567890abcdef0",
    "AvailabilityZone": {
      "Ref": "AvailabilityZone"
    }
  },
  "DeletionPolicy": "Snapshot"
}
```

YAML

Questo frammento crea un volume Amazon EBS con una dimensione specificata. La dimensione è impostata su 10, ma è possibile regolarla in base alle esigenze. La [AWS::EC2::Volume](#) risorsa consente di specificare la dimensione o l'ID di un'istantanea, ma non entrambi.

```
MyEBSVolume:
```

```
Type: AWS::EC2::Volume
Properties:
  Size: 10
  AvailabilityZone:
    Ref: AvailabilityZone
  DeletionPolicy: Snapshot
```

Questo frammento crea un volume Amazon EBS utilizzando un ID snapshot fornito. La [AWS::EC2::Volume](#) risorsa consente di specificare la dimensione o l'ID di un'istantanea, ma non entrambi.

```
MyEBSVolume:
  Type: AWS::EC2::Volume
  Properties:
    SnapshotId: snap-1234567890abcdef0
    AvailabilityZone:
      Ref: AvailabilityZone
    DeletionPolicy: Snapshot
```

Specifica della mappatura dei dispositivi a blocchi per un'istanza

Una mappatura dei dispositivi a blocchi definisce i dispositivi a blocchi, inclusi i volumi di archivio dell'istanza e i volumi EBS, da collegare a un'istanza. Puoi specificare una mappatura dei dispositivi a blocchi quando crei un'AMI in modo che la mappatura venga utilizzata da tutte le istanze avviate dall'AMI. In alternativa, puoi specificare una mappatura dei dispositivi a blocchi quando avvii un'istanza, in modo che la mappatura sostituisca quella specificata nell'AMI da cui è stata avviata l'istanza.

Puoi utilizzare i seguenti frammenti di modello per specificare le mappature dei dispositivi a blocchi per i tuoi volumi EBS o Instance Store utilizzando la proprietà di una risorsa.

BlockDeviceMappings [AWS::EC2::Instance](#)

Per ulteriori informazioni sulle mappature dei dispositivi a blocchi, consulta [Bloccare le mappature dei dispositivi per i volumi sulle EC2 istanze Amazon nella Amazon User Guide](#). EC2

Scenari

- [Specifica le mappature dei dispositivi a blocchi per due volumi EBS](#)
- [Specifica la mappatura dei dispositivi a blocchi per un volume di archivio dell'istanza](#)

Specifica le mappature dei dispositivi a blocchi per due volumi EBS

JSON

```
"Ec2Instance": {
  "Type": "AWS::EC2::Instance",
  "Properties": {
    "ImageId": {
      "Fn::FindInMap": [
        "AWSRegionArch2AMI",
        { "Ref": "AWS::Region" },
        {
          "Fn::FindInMap": [
            "AWSInstanceType2Arch",
            { "Ref": "InstanceType" },
            "Arch"
          ]
        }
      ]
    },
    "KeyName": { "Ref": "KeyName" },
    "InstanceType": { "Ref": "InstanceType" },
    "SecurityGroups": [{ "Ref": "Ec2SecurityGroup" }],
    "BlockDeviceMappings": [
      {
        "DeviceName": "/dev/sda1",
        "Ebs": { "VolumeSize": "50" }
      },
      {
        "DeviceName": "/dev/sdm",
        "Ebs": { "VolumeSize": "100" }
      }
    ]
  }
}
```

YAML

```
EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
```

```

    ImageId: !FindInMap [AWSRegionArch2AMI, !Ref 'AWS::Region', !FindInMap
[AWSInstanceType2Arch, !Ref InstanceType, Arch]]
    KeyName: !Ref KeyName
    InstanceType: !Ref InstanceType
    SecurityGroups:
      - !Ref Ec2SecurityGroup
    BlockDeviceMappings:
      -
        DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
      -
        DeviceName: /dev/sdm
        Ebs:
          VolumeSize: 100

```

Specifica la mappatura dei dispositivi a blocchi per un volume di archivio dell'istanza

JSON

```

"Ec2Instance" : {
  "Type" : "AWS::EC2::Instance",
  "Properties" : {
    "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" : "AWS::Region" },
"HVM64" ] },
    "KeyName" : { "Ref" : "KeyName" },
    "InstanceType": { "Ref": "InstanceType" },
    "SecurityGroups" : [{ "Ref" : "Ec2SecurityGroup" }],
    "BlockDeviceMappings" : [
      {
        "DeviceName" : "/dev/sdc",
        "VirtualName" : "ephemeral0"
      }
    ]
  }
}

```

YAML

```

EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !FindInMap

```

```

- AWSRegionArch2AMI
- !Ref AWS::Region
- HVM64
KeyName: !Ref KeyName
InstanceType: !Ref InstanceType
SecurityGroups:
- !Ref Ec2SecurityGroup
BlockDeviceMappings:
- DeviceName: /dev/sdc
  VirtualName: ephemeral0

```

Crea modelli di lancio con CloudFormation

Questa sezione fornisce un esempio per la creazione di un modello di EC2 lancio Amazon utilizzando CloudFormation. I modelli di lancio consentono di creare modelli per la configurazione e il provisioning delle EC2 istanze Amazon all'interno. AWS Con i modelli di avvio, puoi memorizzare i parametri di avvio in modo da non doverli specificare ogni volta che avvii un'istanza. Per altri esempi, consulta la sezione [Esempi](#) nella `AWS::EC2::LaunchTemplate` risorsa.

Per ulteriori informazioni sui modelli di lancio, consulta [i parametri di avvio delle istanze Store nei modelli di EC2 lancio di](#) Amazon nella Amazon EC2 User Guide.

Per informazioni sulla creazione di modelli di lancio da utilizzare con i gruppi Auto Scaling, consulta i modelli di [lancio di Auto Scaling](#) nella Amazon Auto EC2 Scaling User Guide.

Categorie dei frammenti

- [Crea un modello di lancio che specifichi gruppi di sicurezza, tag, dati utente e un ruolo IAM](#)

Crea un modello di lancio che specifichi gruppi di sicurezza, tag, dati utente e un ruolo IAM

Questo frammento mostra una `AWS::EC2::LaunchTemplate` risorsa che contiene le informazioni di configurazione per avviare un'istanza. Puoi specificare i valori per le proprietà `ImageId`, `InstanceType`, `SecurityGroups`, `UserData` e `TagSpecifications`. La `SecurityGroups` proprietà specifica un gruppo di EC2 sicurezza esistente e un nuovo gruppo di sicurezza. La `Ref` funzione ottiene l'ID della `AWS::EC2::SecurityGroup` risorsa `myNewEC2SecurityGroup` dichiarata altrove nel modello di stack.

Il modello di avvio include una sezione per i dati utente personalizzati. In questa sezione puoi passare attività di configurazione e script che vengono eseguiti all'avvio di un'istanza. In questo esempio, i dati utente installano l' AWS Systems Manager agente e lo avviano.

Il modello di lancio include anche un ruolo IAM che consente alle applicazioni in esecuzione su istanze di eseguire azioni per conto dell'utente. Questo esempio mostra una [AWS::IAM::Role](#) risorsa per il modello di avvio, che utilizza la `IamInstanceProfile` proprietà per specificare il ruolo IAM. La `Ref` funzione ottiene il nome della [AWS::IAM::InstanceProfile](#) risorsa `myInstanceProfile`. Per configurare le autorizzazioni del ruolo IAM, è necessario specificare un valore per la proprietà `ManagedPolicyArns`.

JSON

```
{
  "Resources":{
    "myLaunchTemplate":{
      "Type":"AWS::EC2::LaunchTemplate",
      "Properties":{
        "LaunchTemplateName":{"Fn::Sub": "${AWS::StackName}-launch-template" },
        "LaunchTemplateData":{
          "ImageId":"ami-02354e95b3example",
          "InstanceType":"t3.micro",
          "IamInstanceProfile":{
            "Name":{
              "Ref":"myInstanceProfile"
            }
          },
          "SecurityGroupIds":[
            {
              "Ref":"myNewEC2SecurityGroup"
            },
            "sg-083cd3bfb8example"
          ],
          "UserData":{
            "Fn::Base64":{
              "Fn::Join": [
                "", [
                  "#!/bin/bash\n",
                  "cd /tmp\n",
                  "yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm\n",
                  "systemctl enable amazon-ssm-agent\n",
                  "systemctl start amazon-ssm-agent\n"
                ]
              ]
            }
          }
        }
      }
    },
  },
}
```

```
    "TagSpecifications":[
      {
        "ResourceType":"instance",
        "Tags":[
          {
            "Key":"environment",
            "Value":"development"
          }
        ]
      },
      {
        "ResourceType":"volume",
        "Tags":[
          {
            "Key":"environment",
            "Value":"development"
          }
        ]
      }
    ]
  },
  "myInstanceRole":{
    "Type":"AWS::IAM::Role",
    "Properties":{
      "RoleName":"InstanceRole",
      "AssumeRolePolicyDocument":{
        "Version":"2012-10-17",
        "Statement":[
          {
            "Effect":"Allow",
            "Principal":{
              "Service":[
                "ec2.amazonaws.com"
              ]
            },
            "Action":[
              "sts:AssumeRole"
            ]
          }
        ]
      }
    ]
  },
  "ManagedPolicyArns":[
```

```

        "arn:aws:iam::aws:policy/myCustomerManagedPolicy"
    ]
}
},
"myInstanceProfile":{
    "Type":"AWS::IAM::InstanceProfile",
    "Properties":{
        "Path":"/",
        "Roles":[
            {
                "Ref":"myInstanceRole"
            }
        ]
    }
}
}
}
}
}
}
}

```

YAML

```

---
Resources:
  myLaunchTemplate:
    Type: AWS::EC2::LaunchTemplate
    Properties:
      LaunchTemplateName: !Sub ${AWS::StackName}-launch-template
      LaunchTemplateData:
        ImageId: ami-02354e95b3example
        InstanceType: t3.micro
        IamInstanceProfile:
          Name: !Ref myInstanceProfile
        SecurityGroupIds:
          - !Ref myNewEC2SecurityGroup
          - sg-083cd3bfb8example
        UserData:
          Fn::Base64: !Sub |
            #!/bin/bash
            cd /tmp
            yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
            latest/linux_amd64/amazon-ssm-agent.rpm
            systemctl enable amazon-ssm-agent
            systemctl start amazon-ssm-agent
      TagSpecifications:

```

```
- ResourceType: instance
  Tags:
    - Key: environment
      Value: development
- ResourceType: volume
  Tags:
    - Key: environment
      Value: development
myInstanceRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: InstanceRole
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: 'Allow'
          Principal:
            Service:
              - 'ec2.amazonaws.com'
          Action:
            - 'sts:AssumeRole'
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/myCustomerManagedPolicy'
myInstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: '/'
    Roles:
      - !Ref myInstanceRole
```

Gestisci i gruppi di sicurezza con CloudFormation

I seguenti frammenti mostrano come gestire i gruppi di sicurezza e CloudFormation le EC2 istanze Amazon per controllare l'accesso alle tue risorse. AWS

Categorie dei frammenti

- [Associare un' EC2istanza Amazon a un gruppo di sicurezza](#)
- [Creazione di gruppi di sicurezza con regole di ingresso](#)
- [Creazione di un Elastic Load Balancer con una regola di ingresso al gruppo di sicurezza](#)

Associare un' EC2istanza Amazon a un gruppo di sicurezza

I seguenti frammenti di esempio mostrano come associare un' EC2 istanza Amazon a un gruppo di sicurezza Amazon VPC predefinito utilizzando CloudFormation

Frammenti di esempio

- [Associa un' EC2 istanza Amazon a un gruppo di sicurezza VPC predefinito](#)
- [Crea un' EC2 istanza Amazon con un volume e un gruppo di sicurezza collegati](#)

Associa un' EC2 istanza Amazon a un gruppo di sicurezza VPC predefinito

Il seguente frammento crea un Amazon VPC, una sottorete all'interno del VPC e un'istanza Amazon. EC2 Il VPC viene creato utilizzando una risorsa [AWS::EC2::VPC](#). L'intervallo di indirizzi IP per il VPC è definito nel modello più grande e viene richiamato dal parametro MyVPCCIDRRange.

Una sottorete viene creata all'interno del VPC utilizzando una risorsa [AWS::EC2::Subnet](#). La sottorete è associata al VPC, a cui si fa riferimento come MyVPC.

Un' EC2 istanza viene avviata all'interno del VPC e della sottorete utilizzando una risorsa. [AWS::EC2::Instance](#) Questa risorsa specifica l'Amazon Machine Image (AMI) da utilizzare per avviare l'istanza, la sottorete in cui verrà eseguita l'istanza e il gruppo di sicurezza da associare all'istanza. La Fn::FindInMap funzione viene utilizzata per recuperare i valori dalla AWSRegionToAMI mappatura definita nel modello per determinare il valore della ImageId risorsa. [AWS::EC2::Instance](#)

L'ID del gruppo di sicurezza viene ottenuto utilizzando la funzione Fn::GetAtt, che recupera il gruppo di sicurezza predefinito dalla risorsa MyVPC.

L'istanza viene inserita all'interno della risorsa MySubnet definita nel frammento.

Quando crei un VPC utilizzando CloudFormation, crea AWS automaticamente risorse predefinite all'interno del VPC, incluso un gruppo di sicurezza predefinito. Tuttavia, quando si definisce un VPC all'interno di un CloudFormation modello, è possibile che non si abbia accesso a queste risorse predefinite al momento IDs della creazione del modello. Per accedere e utilizzare le risorse predefinite specificate nel modello, puoi utilizzare funzioni intrinseche come Fn::GetAtt. Questa funzione consente di lavorare con le risorse predefinite create automaticamente da CloudFormation.

JSON

```
"MyVPC": {
```



```
"Type": "AWS::EC2::VPC",
"Properties": {
  "CidrBlock": {
    "Ref": "MyVPCCIDRRange"
  },
  "EnableDnsSupport": false,
  "EnableDnsHostnames": false,
  "InstanceTenancy": "default"
},
},
"MySubnet": {
  "Type": "AWS::EC2::Subnet",
  "Properties": {
    "CidrBlock": {
      "Ref": "MyVPCCIDRRange"
    },
    "VpcId": {
      "Ref": "MyVPC"
    }
  }
},
},
"MyInstance": {
  "Type": "AWS::EC2::Instance",
  "Properties": {
    "ImageId": {
      "Fn::FindInMap": [
        "AWSRegionToAMI",
        {
          "Ref": "AWS::Region"
        },
        "64"
      ]
    },
    "SecurityGroupIds": [
      {
        "Fn::GetAtt": [
          "MyVPC",
          "DefaultSecurityGroup"
        ]
      }
    ],
    "SubnetId": {
      "Ref": "MySubnet"
    }
  }
}
```

```
}  
}
```

YAML

```
MyVPC:  
  Type: AWS::EC2::VPC  
  Properties:  
    CidrBlock:  
      Ref: MyVPCCIDRRange  
    EnableDnsSupport: false  
    EnableDnsHostnames: false  
    InstanceTenancy: default  
MySubnet:  
  Type: AWS::EC2::Subnet  
  Properties:  
    CidrBlock:  
      Ref: MyVPCCIDRRange  
    VpcId:  
      Ref: MyVPC  
MyInstance:  
  Type: AWS::EC2::Instance  
  Properties:  
    ImageId:  
      Fn::FindInMap:  
        - AWSRegionToAMI  
        - Ref: AWS::Region  
        - "64"  
    SecurityGroupIds:  
      - Fn::GetAtt:  
          - MyVPC  
          - DefaultSecurityGroup  
    SubnetId:  
      Ref: MySubnet
```

Crea un' EC2 istanza Amazon con un volume e un gruppo di sicurezza collegati

Il seguente frammento crea un' EC2 istanza Amazon utilizzando una [AWS::EC2::Instance](#) risorsa, che viene lanciata da un AMI designato. L'istanza è associata a un gruppo di sicurezza che consente il traffico SSH in entrata sulla porta 22 da un indirizzo IP specificato, utilizzando una risorsa. [AWS::EC2::SecurityGroup](#) Crea un volume Amazon EBS da 100 GB utilizzando una

[AWS::EC2::Volume](#) risorsa. Il volume viene creato nella stessa zona di disponibilità dell'istanza, come specificato dalla funzione `GetAtt`, e viene montato sull'istanza sul dispositivo `/dev/sdh`.

Per ulteriori informazioni sulla creazione di volumi Amazon EBS, consulta [Creazione di un volume Amazon EBS](#).

JSON

```
"Ec2Instance": {
  "Type": "AWS::EC2::Instance",
  "Properties": {
    "SecurityGroups": [
      {
        "Ref": "InstanceSecurityGroup"
      }
    ],
    "ImageId": "ami-1234567890abcdef0"
  }
},
"InstanceSecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "Enable SSH access via port 22",
    "SecurityGroupIngress": [
      {
        "IpProtocol": "tcp",
        "FromPort": "22",
        "ToPort": "22",
        "CidrIp": "192.0.2.0/24"
      }
    ]
  }
},
"NewVolume": {
  "Type": "AWS::EC2::Volume",
  "Properties": {
    "Size": "100",
    "AvailabilityZone": {
      "Fn::GetAtt": [
        "Ec2Instance",
        "AvailabilityZone"
      ]
    }
  }
}
```

```

    }
  },
  "MountPoint": {
    "Type": "AWS::EC2::VolumeAttachment",
    "Properties": {
      "InstanceId": {
        "Ref": "Ec2Instance"
      },
      "VolumeId": {
        "Ref": "NewVolume"
      },
      "Device": "/dev/sdh"
    }
  }
}

```

YAML

```

Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    SecurityGroups:
      - !Ref InstanceSecurityGroup
    ImageId: ami-1234567890abcdef0
InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Enable SSH access via port 22
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: 192.0.2.0/24
NewVolume:
  Type: AWS::EC2::Volume
  Properties:
    Size: 100
    AvailabilityZone: !GetAtt [Ec2Instance, AvailabilityZone]
MountPoint:
  Type: AWS::EC2::VolumeAttachment
  Properties:
    InstanceId: !Ref Ec2Instance
    VolumeId: !Ref NewVolume
    Device: /dev/sdh

```

Creazione di gruppi di sicurezza con regole di ingresso

I frammenti di esempio seguenti mostrano come configurare i gruppi di sicurezza con regole di ingresso specifiche utilizzando CloudFormation.

Frammenti

- [Creazione di un gruppo di sicurezza con regole di ingresso per l'accesso SSH e HTTP](#)
- [Creazione di un gruppo di sicurezza con regole di ingresso per l'accesso HTTP e SSH da intervalli CIDR specificati](#)
- [Crea gruppi di sicurezza con riferimenti incrociati e regole di ingresso](#)

Creazione di un gruppo di sicurezza con regole di ingresso per l'accesso SSH e HTTP

Il seguente frammento descrive due regole di ingresso per gruppi di sicurezza che utilizzano una risorsa. [AWS::EC2::SecurityGroup](#) La prima regola di ingresso consente l'accesso SSH (porta 22) da un gruppo di sicurezza esistente denominato `MyAdminSecurityGroup`, di proprietà dell'account con il numero di AWS account. 1111-2222-3333 La seconda regola di ingresso consente l'accesso HTTP (porta 80) da un gruppo di sicurezza diverso denominato `MySecurityGroupCreatedInCFN`, creato nello stesso modello. La funzione `Ref` viene utilizzata per fare riferimento al nome logico del gruppo di sicurezza creato nello stesso modello.

Nella prima regola di ingresso, è necessario aggiungere un valore per entrambe le proprietà `SourceSecurityGroupName` e `SourceSecurityGroupOwnerId`. Nella seconda regola di ingresso, `MySecurityGroupCreatedInCFNTemplate` fa riferimento a un gruppo di sicurezza diverso, creato nello stesso modello. Verifica che il nome logico `MySecurityGroupCreatedInCFNTemplate` corrisponda al nome logico effettivo della risorsa del gruppo di sicurezza specificata nel modello più grande.

Per ulteriori informazioni sui gruppi di sicurezza, consulta i [gruppi EC2 di sicurezza Amazon per le tue EC2 istanze Amazon](#) nella Amazon EC2 User Guide.

JSON

```
"SecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "Allow connections from specified source security group",
    "SecurityGroupIngress": [
      {
```

```

        "IpProtocol": "tcp",
        "FromPort": "22",
        "ToPort": "22",
        "SourceSecurityGroupName": "MyAdminSecurityGroup",
        "SourceSecurityGroupOwnerId": "1111-2222-3333"
    },
    {
        "IpProtocol": "tcp",
        "FromPort": "80",
        "ToPort": "80",
        "SourceSecurityGroupName": {
            "Ref": "MySecurityGroupCreatedInCFNTemplate"
        }
    }
]
}
}

```

YAML

```

SecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Allow connections from specified source security group
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: '22'
        ToPort: '22'
        SourceSecurityGroupName: MyAdminSecurityGroup
        SourceSecurityGroupOwnerId: '1111-2222-3333'
      - IpProtocol: tcp
        FromPort: '80'
        ToPort: '80'
        SourceSecurityGroupName:
          Ref: MySecurityGroupCreatedInCFNTemplate

```

Creazione di un gruppo di sicurezza con regole di ingresso per l'accesso HTTP e SSH da intervalli CIDR specificati

Il seguente frammento crea un gruppo di sicurezza per un' EC2 istanza Amazon con due regole in entrata. Le regole in entrata consentono il traffico TCP in ingresso sulle porte specificate dagli intervalli CIDR designati. Una [AWS::EC2::SecurityGroup](#) risorsa viene utilizzata per specificare le

regole. È possibile specificare un protocollo per ciascuna regola. Per TCP, è necessario anche specificare una porta o un intervallo di porte. Se non si specifica un gruppo di sicurezza di origine o un intervallo CIDR, lo stack verrà avviato correttamente, ma la regola non verrà applicata al gruppo di sicurezza.

Per ulteriori informazioni sui gruppi di sicurezza, consulta i [gruppi EC2 di sicurezza Amazon per le tue EC2 istanze Amazon](#) nella Amazon EC2 User Guide.

JSON

```
"ServerSecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "Allow connections from specified CIDR ranges",
    "SecurityGroupIngress": [
      {
        "IpProtocol": "tcp",
        "FromPort": "80",
        "ToPort": "80",
        "CidrIp": "192.0.2.0/24"
      },
      {
        "IpProtocol": "tcp",
        "FromPort": "22",
        "ToPort": "22",
        "CidrIp": "192.0.2.0/24"
      }
    ]
  }
}
```

YAML

```
ServerSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Allow connections from specified CIDR ranges
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        CidrIp: 192.0.2.0/24
      - IpProtocol: tcp
```

```

FromPort: 22
ToPort: 22
CidrIp: 192.0.2.0/24

```

Crea gruppi di sicurezza con riferimenti incrociati e regole di ingresso

Il seguente frammento utilizza la [AWS::EC2::SecurityGroup](#) risorsa per creare due gruppi di EC2 sicurezza Amazon e. SGroup1 SGroup2 [Le regole di ingresso che consentono la comunicazione tra i due gruppi di sicurezza vengono create utilizzando la AWS::EC2::SecurityGroup risorsa Ingress](#). SGroup1Ingress stabilisce una regola di ingresso SGroup1 che consente il traffico TCP in entrata sulla porta 80 dal gruppo di sicurezza di origine,. SGroup2 SGroup2Ingress stabilisce una regola di ingresso SGroup2 che consente il traffico TCP in entrata sulla porta 80 dal gruppo di sicurezza di origine,. SGroup1

JSON

```

"SGroup1": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "EC2 instance access"
  }
},
"SGroup2": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "EC2 instance access"
  }
},
"SGroup1Ingress": {
  "Type": "AWS::EC2::SecurityGroupIngress",
  "Properties": {
    "GroupName": {
      "Ref": "SGroup1"
    },
    "IpProtocol": "tcp",
    "ToPort": "80",
    "FromPort": "80",
    "SourceSecurityGroupName": {
      "Ref": "SGroup2"
    }
  }
},

```



```

"SGroup2Ingress": {
  "Type": "AWS::EC2::SecurityGroupIngress",
  "Properties": {
    "GroupName": {
      "Ref": "SGroup2"
    },
    "IpProtocol": "tcp",
    "ToPort": "80",
    "FromPort": "80",
    "SourceSecurityGroupName": {
      "Ref": "SGroup1"
    }
  }
}
}

```

YAML

```

SGroup1:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: EC2 Instance access
SGroup2:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: EC2 Instance access
SGroup1Ingress:
  Type: AWS::EC2::SecurityGroupIngress
  Properties:
    GroupName: !Ref SGroup1
    IpProtocol: tcp
    ToPort: 80
    FromPort: 80
    SourceSecurityGroupName: !Ref SGroup2
SGroup2Ingress:
  Type: AWS::EC2::SecurityGroupIngress
  Properties:
    GroupName: !Ref SGroup2
    IpProtocol: tcp
    ToPort: 80
    FromPort: 80
    SourceSecurityGroupName: !Ref SGroup1

```

Creazione di un Elastic Load Balancer con una regola di ingresso al gruppo di sicurezza

Il modello seguente crea una [AWS::ElasticLoadBalancing::LoadBalancer](#) risorsa nella zona di disponibilità specificata. La [AWS::ElasticLoadBalancing::LoadBalancer](#) risorsa è configurata per ascoltare il traffico HTTP sulla porta 80 e indirizzare le richieste alle istanze anche sulla porta 80. Elastic Load Balancer è responsabile del bilanciamento del carico del traffico HTTP in entrata tra le istanze.

Inoltre, questo modello genera una [AWS::EC2::SecurityGroup](#) risorsa associata al load balancer. Questo gruppo di sicurezza viene creato con un'unica regola di ingresso, descritta come `ELB ingress group`, che consente il traffico TCP in entrata sulla porta 80. L'origine di questa regola di ingresso viene definita utilizzando la funzione `Fn::GetAtt` per recuperare gli attributi dalla risorsa di bilanciamento del carico. `SourceSecurityGroupOwnerId` utilizza `Fn::GetAtt` per ottenere l'`OwnerAlias` del gruppo di sicurezza di origine del sistema di bilanciamento del carico. `SourceSecurityGroupName` utilizza `Fn::GetAtt` per ottenere il `GroupName` del gruppo di sicurezza di origine dell'ELB.

Questa configurazione garantisce una comunicazione sicura tra l'ELB e le istanze.

Per ulteriori informazioni su Elastic Load Balancing, consulta la [Guida per l'utente di Elastic Load Balancing](#).

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "MyELB": {
      "Type": "AWS::ElasticLoadBalancing::LoadBalancer",
      "Properties": {
        "AvailabilityZones": [
          "aa-example-1a"
        ],
        "Listeners": [
          {
            "LoadBalancerPort": "80",
            "InstancePort": "80",
            "Protocol": "HTTP"
          }
        ]
      }
    }
  }
}
```

```
},  
  "MyELBIngressGroup": {  
    "Type": "AWS::EC2::SecurityGroup",  
    "Properties": {  
      "GroupDescription": "ELB ingress group",  
      "SecurityGroupIngress": [  
        {  
          "IpProtocol": "tcp",  
          "FromPort": 80,  
          "ToPort": 80,  
          "SourceSecurityGroupId": {  
            "Fn::GetAtt": [  
              "MyELB",  
              "SourceSecurityGroup.OwnerAlias"  
            ]  
          },  
          "SourceSecurityGroupName": {  
            "Fn::GetAtt": [  
              "MyELB",  
              "SourceSecurityGroup.GroupName"  
            ]  
          }  
        }  
      ]  
    }  
  }  
}  
  
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'

Resources:

  MyELB:
    Type: 'AWS::ElasticLoadBalancing::LoadBalancer'
    Properties:
      AvailabilityZones:
        - aa-example-1a
      Listeners:
        - LoadBalancerPort: '80'
          InstancePort: '80'
          Protocol: HTTP

  MyELBIngressGroup:
```

```
Type: 'AWS::EC2::SecurityGroup'
Properties:
  GroupDescription: ELB ingress group
  SecurityGroupIngress:
    - IpProtocol: tcp
      FromPort: '80'
      ToPort: '80'
      SourceSecurityGroupOwnerId:
        Fn::GetAtt:
          - MyELB
          - SourceSecurityGroup.OwnerAlias
      SourceSecurityGroupName:
        Fn::GetAtt:
          - MyELB
          - SourceSecurityGroup.GroupName
```

Alloca e associa indirizzi IP elastici con CloudFormation

I seguenti frammenti di modello sono esempi relativi agli indirizzi IP elastici (EIPs) in Amazon. EC2. Questi esempi riguardano l'allocazione, l'associazione e la gestione delle EIPs istanze.

Frammenti di esempio

- [Alloca un indirizzo IP elastico e associalo a un'istanza Amazon EC2](#)
- [Associa un indirizzo IP elastico a un' EC2 istanza Amazon specificando l'indirizzo IP](#)
- [Associa un indirizzo IP elastico a un' EC2 istanza Amazon specificando l'ID di allocazione dell'indirizzo IP](#)

Alloca un indirizzo IP elastico e associalo a un'istanza Amazon EC2

Il seguente frammento alloca un indirizzo Amazon EC2 Elastic IP (EIP) e lo associa a un'istanza Amazon EC2 utilizzando una risorsa. [AWS::EC2::EIP](#). Puoi allocare un indirizzo EIP da un pool di indirizzi di proprietà AWS o da un pool di indirizzi creato da un intervallo di indirizzi pubblico da te utilizzato AWS per utilizzarlo con AWS le tue risorse utilizzando Bring [your](#) own IP IPv4 address (BYOIP). In questo esempio, l'EIP viene allocato da un pool di indirizzi di proprietà di AWS.

Per ulteriori informazioni sugli indirizzi IP elastici, consulta [l'indirizzo IP elastico](#) nella Amazon EC2 User Guide.

JSON

```
"ElasticIP": {
  "Type": "AWS::EC2::EIP",
  "Properties": {
    "InstanceId": {
      "Ref": "Ec2Instance"
    }
  }
}
```

YAML

```
ElasticIP:
  Type: AWS::EC2::EIP
  Properties:
    InstanceId: !Ref Ec2Instance
```

Associa un indirizzo IP elastico a un' EC2 istanza Amazon specificando l'indirizzo IP

Il seguente frammento associa un indirizzo IP Amazon EC2 Elastic esistente a un' EC2istanza utilizzando una risorsa [AWS::EC2::EIPAssociation](#) Per utilizzare un indirizzo IP elastico, occorre prima allocarlo per l'uso nel proprio account. Un indirizzo IP elastico può essere associato a un'istanza singola.

JSON

```
"IPAssoc": {
  "Type": "AWS::EC2::EIPAssociation",
  "Properties": {
    "InstanceId": {
      "Ref": "Ec2Instance"
    },
    "EIP": "192.0.2.0"
  }
}
```

YAML

```
IPAssoc:
  Type: AWS::EC2::EIPAssociation
  Properties:
```

```
InstanceId: !Ref EC2Instance
EIP: 192.0.2.0
```

Associa un indirizzo IP elastico a un' EC2 istanza Amazon specificando l'ID di allocazione dell'indirizzo IP

Il seguente frammento associa un indirizzo IP elastico esistente a un' EC2istanza Amazon specificando l'ID di allocazione utilizzando una risorsa [AWS::EC2::EIPAssociation](#). Un ID di allocazione viene assegnato a un indirizzo IP elastico al momento dell'allocazione dell'indirizzo IP elastico.

JSON

```
"IPAssoc": {
  "Type": "AWS::EC2::EIPAssociation",
  "Properties": {
    "InstanceId": {
      "Ref": "Ec2Instance"
    },
    "AllocationId": "eipalloc-1234567890abcdef0"
  }
}
```

YAML

```
IPAssoc:
  Type: AWS::EC2::EIPAssociation
  Properties:
    InstanceId: !Ref EC2Instance
    AllocationId: eipalloc-1234567890abcdef0
```

Configura le risorse Amazon VPC con CloudFormation

Questa sezione fornisce esempi per configurare le risorse Amazon VPC utilizzando CloudFormation. VPCs consentono di creare una rete virtuale all'interno AWS di una rete virtuale e questi frammenti mostrano come configurare alcuni aspetti per VPCs soddisfare i requisiti di rete.

Frammenti di esempio

- [Abilita l'accesso a Internet IPv6 solo in uscita in un VPC](#)
- [Frammenti di modello di interfaccia di rete elastica \(ENI\)](#)

Abilita l'accesso a Internet IPv6 solo in uscita in un VPC

Un gateway Internet solo in uscita consente alle istanze all'interno di un VPC di accedere a Internet e impedire che le risorse su Internet comunichino con le istanze. Il seguente frammento consente l'accesso a Internet IPv6 solo in uscita dall'interno di un VPC. Crea un VPC con un intervallo di IPv4 indirizzi `10.0.0/16` utilizzando una risorsa [AWS::EC2::VPC](#). Una tabella di routing è associata a questa risorsa VPC utilizzando una [AWS::EC2::RouteTable](#) risorsa. La tabella di routing gestisce i percorsi per le istanze all'interno del VPC. An [AWS::EC2::EgressOnlyInternetGateway](#) viene utilizzato per creare un gateway Internet solo in uscita per consentire la IPv6 comunicazione per il traffico in uscita dalle istanze all'interno del VPC, impedendo al contempo il traffico in entrata. Viene specificata una [AWS::EC2::Router](#) risorsa per creare un IPv6 percorso nella tabella delle rotte che indirizza tutto il traffico in uscita () verso il gateway Internet di sola uscita IPv6. `:::/0`

Per ulteriori informazioni sui gateway Internet solo in uscita, consulta [Abilitare il IPv6 traffico in uscita utilizzando un gateway Internet solo in uscita nella Amazon VPC User Guide](#).

JSON

```
"DefaultIpv6Route": {
  "Type": "AWS::EC2::Route",
  "Properties": {
    "DestinationIpv6CidrBlock": ":::/0",
    "EgressOnlyInternetGatewayId": {
      "Ref": "EgressOnlyInternetGateway"
    },
    "RouteTableId": {
      "Ref": "RouteTable"
    }
  }
},
"EgressOnlyInternetGateway": {
  "Type": "AWS::EC2::EgressOnlyInternetGateway",
  "Properties": {
    "VpcId": {
      "Ref": "VPC"
    }
  }
},
"RouteTable": {
  "Type": "AWS::EC2::RouteTable",
  "Properties": {
    "VpcId": {
```

```

        "Ref": "VPC"
      }
    }
  },
  "VPC": {
    "Type": "AWS::EC2::VPC",
    "Properties": {
      "CidrBlock": "10.0.0.0/16"
    }
  }
}

```

YAML

```

DefaultIpv6Route:
  Type: "AWS::EC2::Route"
  Properties:
    DestinationIpv6CidrBlock: "::/0"
    EgressOnlyInternetGatewayId:
      Ref: "EgressOnlyInternetGateway"
    RouteTableId:
      Ref: "RouteTable"
EgressOnlyInternetGateway:
  Type: "AWS::EC2::EgressOnlyInternetGateway"
  Properties:
    VpcId:
      Ref: "VPC"
RouteTable:
  Type: "AWS::EC2::RouteTable"
  Properties:
    VpcId:
      Ref: "VPC"
VPC:
  Type: "AWS::EC2::VPC"
  Properties:
    CidrBlock: "10.0.0.0/16"

```

Frammenti di modello di interfaccia di rete elastica (ENI)

Crea un' EC2 istanza Amazon con interfacce di rete elastiche collegate () ENIs

Lo snippet di esempio seguente crea un' EC2 istanza Amazon utilizzando una [AWS::EC2::Instance](#) risorsa nel VPC e nella sottorete Amazon specificati. Collega due interfacce di rete (ENIs) all'istanza, associa gli indirizzi IP elastici alle istanze tramite l'interfaccia allegata

e configura il gruppo di sicurezza per l'ENIsaccesso SSH e HTTP. I dati utente vengono forniti all'istanza come parte della configurazione di avvio al momento della creazione dell'istanza. I dati utente includono uno script codificato in formato base64 per garantire che venga passato all'istanza. All'avvio dell'istanza, lo script viene eseguito automaticamente come parte del processo di bootstrap. Installa `ec2-net-utils`, configura le interfacce di rete e avvia il servizio HTTP.

Per determinare l'Amazon Machine Image (AMI) appropriata in base alla Regione selezionata, il frammento utilizza una funzione `Fn::FindInMap` che cerca i valori in una mappatura `RegionMap`. Questa mappatura deve essere definita nel modello più grande. Le due interfacce di rete vengono create utilizzando risorse. [AWS::EC2::NetworkInterface](#) Gli indirizzi IP elastici vengono specificati utilizzando [AWS::EC2::EIP](#) le risorse allocate al vpc dominio. Questi indirizzi IP elastici sono associati alle interfacce di rete che utilizzano [AWS::EC2::EIPAssociation](#) risorse.

La sezione `Outputs` definisce i valori o le risorse a cui si desidera accedere dopo la creazione dello stack. In questo frammento, l'output definito è `InstancePublicIp`, che rappresenta l'indirizzo IP pubblico dell' EC2 istanza creata dallo stack. [È possibile recuperare questo output nella scheda Output della AWS CloudFormation console o utilizzando il comando `describe-stacks`.](#)

Per ulteriori informazioni sulle interfacce di rete elastiche, consulta [Interfacce di rete Elastiche](#).

JSON

```
"Resources": {
  "ControlPortAddress": {
    "Type": "AWS::EC2::EIP",
    "Properties": {
      "Domain": "vpc"
    }
  },
  "AssociateControlPort": {
    "Type": "AWS::EC2::EIPAssociation",
    "Properties": {
      "AllocationId": {
        "Fn::GetAtt": [
          "ControlPortAddress",
          "AllocationId"
        ]
      },
      "NetworkInterfaceId": {
        "Ref": "controlXface"
      }
    }
  }
}
```

```
    },
    "WebPortAddress": {
      "Type": "AWS::EC2::EIP",
      "Properties": {
        "Domain": "vpc"
      }
    },
    "AssociateWebPort": {
      "Type": "AWS::EC2::EIPAssociation",
      "Properties": {
        "AllocationId": {
          "Fn::GetAtt": [
            "WebPortAddress",
            "AllocationId"
          ]
        },
        "NetworkInterfaceId": {
          "Ref": "webXface"
        }
      }
    },
    "SSHSecurityGroup": {
      "Type": "AWS::EC2::SecurityGroup",
      "Properties": {
        "VpcId": {
          "Ref": "VpcId"
        },
        "GroupDescription": "Enable SSH access via port 22",
        "SecurityGroupIngress": [
          {
            "CidrIp": "0.0.0.0/0",
            "FromPort": 22,
            "IpProtocol": "tcp",
            "ToPort": 22
          }
        ]
      }
    },
    "WebSecurityGroup": {
      "Type": "AWS::EC2::SecurityGroup",
      "Properties": {
        "VpcId": {
          "Ref": "VpcId"
        }
      }
    },
```

```

        "GroupDescription": "Enable HTTP access via user-defined port",
        "SecurityGroupIngress": [
            {
                "CidrIp": "0.0.0.0/0",
                "FromPort": 80,
                "IpProtocol": "tcp",
                "ToPort": 80
            }
        ]
    },
    "controlXface": {
        "Type": "AWS::EC2::NetworkInterface",
        "Properties": {
            "SubnetId": {
                "Ref": "SubnetId"
            },
            "Description": "Interface for controlling traffic such as SSH",
            "GroupSet": [
                {
                    "Fn::GetAtt": [
                        "SSHSecurityGroup",
                        "GroupId"
                    ]
                }
            ],
            "SourceDestCheck": true,
            "Tags": [
                {
                    "Key": "Network",
                    "Value": "Control"
                }
            ]
        }
    },
    "webXface": {
        "Type": "AWS::EC2::NetworkInterface",
        "Properties": {
            "SubnetId": {
                "Ref": "SubnetId"
            },
            "Description": "Interface for web traffic",
            "GroupSet": [
                {

```

```

        "Fn::GetAtt": [
            "WebSecurityGroup",
            "GroupId"
        ]
    },
    ],
    "SourceDestCheck": true,
    "Tags": [
        {
            "Key": "Network",
            "Value": "Web"
        }
    ]
}
},
"Ec2Instance": {
    "Type": "AWS::EC2::Instance",
    "Properties": {
        "ImageId": {
            "Fn::FindInMap": [
                "RegionMap",
                {
                    "Ref": "AWS::Region"
                }
            ],
            "AMI"
        }
    },
    "KeyName": {
        "Ref": "KeyName"
    },
    "NetworkInterfaces": [
        {
            "NetworkInterfaceId": {
                "Ref": "controlXface"
            },
            "DeviceIndex": "0"
        },
        {
            "NetworkInterfaceId": {
                "Ref": "webXface"
            },
            "DeviceIndex": "1"
        }
    ]
},
],

```

```

        "Tags": [
            {
                "Key": "Role",
                "Value": "Test Instance"
            }
        ],
        "UserData": {
            "Fn::Base64": {
                "Fn::Sub": "#!/bin/bash -xe\nyum install ec2-net-utils -y\nec2ifup
eth1\nservice httpd start\n"
            }
        }
    }
},
"Outputs": {
    "InstancePublicIp": {
        "Description": "Public IP Address of the EC2 Instance",
        "Value": {
            "Fn::GetAtt": [
                "Ec2Instance",
                "PublicIp"
            ]
        }
    }
}
}

```

YAML

```

Resources:
  ControlPortAddress:
    Type: 'AWS::EC2::EIP'
    Properties:
      Domain: vpc
  AssociateControlPort:
    Type: 'AWS::EC2::EIPAssociation'
    Properties:
      AllocationId:
        Fn::GetAtt:
          - ControlPortAddress
          - AllocationId
      NetworkInterfaceId:
        Ref: controlXface

```

```
WebPortAddress:
  Type: 'AWS::EC2::EIP'
  Properties:
    Domain: vpc
AssociateWebPort:
  Type: 'AWS::EC2::EIPAssociation'
  Properties:
    AllocationId:
      Fn::GetAtt:
        - WebPortAddress
        - AllocationId
    NetworkInterfaceId:
      Ref: webXface
SSHSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    VpcId:
      Ref: VpcId
    GroupDescription: Enable SSH access via port 22
    SecurityGroupIngress:
      - CidrIp: 0.0.0.0/0
        FromPort: 22
        IpProtocol: tcp
        ToPort: 22
WebSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    VpcId:
      Ref: VpcId
    GroupDescription: Enable HTTP access via user-defined port
    SecurityGroupIngress:
      - CidrIp: 0.0.0.0/0
        FromPort: 80
        IpProtocol: tcp
        ToPort: 80
controlXface:
  Type: 'AWS::EC2::NetworkInterface'
  Properties:
    SubnetId:
      Ref: SubnetId
    Description: Interface for controlling traffic such as SSH
    GroupSet:
      - Fn::GetAtt:
          - SSHSecurityGroup
```

```
    - GroupId
SourceDestCheck: true
Tags:
  - Key: Network
    Value: Control
webXface:
  Type: 'AWS::EC2::NetworkInterface'
  Properties:
    SubnetId:
      Ref: SubnetId
    Description: Interface for web traffic
    GroupSet:
      - Fn::GetAtt:
          - WebSecurityGroup
          - GroupId
    SourceDestCheck: true
    Tags:
      - Key: Network
        Value: Web
Ec2Instance:
  Type: AWS::EC2::Instance
  Properties:
    ImageId:
      Fn::FindInMap:
        - RegionMap
        - Ref: AWS::Region
        - AMI
    KeyName:
      Ref: KeyName
    NetworkInterfaces:
      - NetworkInterfaceId:
          Ref: controlXface
          DeviceIndex: "0"
      - NetworkInterfaceId:
          Ref: webXface
          DeviceIndex: "1"
    Tags:
      - Key: Role
        Value: Test Instance
    UserData:
      Fn::Base64: !Sub |
        #!/bin/bash -xe
        yum install ec2-net-utils -y
        ec2ifup eth1
```

```
service httpd start
```

Outputs:

```
InstancePublicIp:
```

```
Description: Public IP Address of the EC2 Instance
```

```
Value:
```

```
Fn::GetAtt:
```

- Ec2Instance
- PublicIp

Modelli di esempio di Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) è un servizio di gestione dei container che semplifica l'esecuzione, l'arresto e la gestione di contenitori Docker su un cluster di istanze Amazon Elastic Compute Cloud (Amazon). EC2

Crea un cluster con Amazon AL2 023 ECS-Optimized-AMI

Definisci un cluster che utilizza un provider di capacità che lancia AL2 023 istanze su Amazon. EC2

Important

Per l'AMI più recente IDs, consulta l'AMI ottimizzata per [Amazon ECS](#) nella Amazon Elastic Container Service Developer Guide.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "EC2 ECS cluster that starts out empty, with no EC2 instances yet. An ECS capacity provider automatically launches more EC2 instances as required on the fly when you request ECS to launch services or standalone tasks.",
  "Parameters": {
    "InstanceType": {
      "Type": "String",
      "Description": "EC2 instance type",
      "Default": "t2.medium",
      "AllowedValues": [
        "t1.micro",
        "t2.2xlarge",
        "t2.large",
        "t2.medium",

```



```

        "t2.micro",
        "t2.nano",
        "t2.small",
        "t2.xlarge",
        "t3.2xlarge",
        "t3.large",
        "t3.medium",
        "t3.micro",
        "t3.nano",
        "t3.small",
        "t3.xlarge"
    ]
},
"DesiredCapacity": {
    "Type": "Number",
    "Default": "0",
    "Description": "Number of EC2 instances to launch in your ECS cluster."
},
"MaxSize": {
    "Type": "Number",
    "Default": "100",
    "Description": "Maximum number of EC2 instances that can be launched in your
ECS cluster."
},
"ECSAMI": {
    "Description": "The Amazon Machine Image ID used for the cluster",
    "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
    "Default": "/aws/service/ecs/optimized-ami/amazon-linux-2023/recommended/
image_id"
},
"VpcId": {
    "Type": "AWS::EC2::VPC::Id",
    "Description": "VPC ID where the ECS cluster is launched",
    "Default": "vpc-1234567890abcdef0"
},
"SubnetIds": {
    "Type": "List<AWS::EC2::Subnet::Id>",
    "Description": "List of subnet IDs where the EC2 instances will be launched",
    "Default": "subnet-021345abcdef67890"
}
},
"Resources": {
    "ECSCluster": {
        "Type": "AWS::ECS::Cluster",

```

```
    "Properties": {
      "ClusterSettings": [
        {
          "Name": "containerInsights",
          "Value": "enabled"
        }
      ]
    },
  },
  "ECSAutoScalingGroup": {
    "Type": "AWS::AutoScaling::AutoScalingGroup",
    "DependsOn": [
      "ECSCluster",
      "EC2Role"
    ],
    "Properties": {
      "VPCZoneIdentifier": {
        "Ref": "SubnetIds"
      },
      "LaunchTemplate": {
        "LaunchTemplateId": {
          "Ref": "ContainerInstances"
        },
        "Version": {
          "Fn::GetAtt": [
            "ContainerInstances",
            "LatestVersionNumber"
          ]
        }
      },
      "MinSize": 0,
      "MaxSize": {
        "Ref": "MaxSize"
      },
      "DesiredCapacity": {
        "Ref": "DesiredCapacity"
      },
      "NewInstancesProtectedFromScaleIn": true
    },
    "UpdatePolicy": {
      "AutoScalingReplacingUpdate": {
        "WillReplace": "true"
      }
    }
  }
}
```

```

    },
    "ContainerInstances": {
      "Type": "AWS::EC2::LaunchTemplate",
      "Properties": {
        "LaunchTemplateName": "asg-launch-template",
        "LaunchTemplateData": {
          "ImageId": {
            "Ref": "ECSAMI"
          },
          "InstanceType": {
            "Ref": "InstanceType"
          },
          "IamInstanceProfile": {
            "Name": {
              "Ref": "EC2InstanceProfile"
            }
          },
          "SecurityGroupIds": [
            {
              "Ref": "ContainerHostSecurityGroup"
            }
          ],
          "UserData": {
            "Fn::Base64": {
              "Fn::Sub": "
#!/bin/bash -xe\n
echo ECS_CLUSTER=${ECSCluster}

>> /etc/ecs/ecs.config\n
yum install -y aws-cfn-bootstrap\n
/opt/aws/bin/cfn-init -
v --stack ${AWS::StackId} --resource ContainerInstances --configsets full_install --
region ${AWS::Region} &\n"
            }
          },
          "MetadataOptions": {
            "HttpEndpoint": "enabled",
            "HttpTokens": "required"
          }
        }
      }
    },
    "EC2InstanceProfile": {
      "Type": "AWS::IAM::InstanceProfile",
      "Properties": {
        "Path": "/",
        "Roles": [
          {
            "Ref": "EC2Role"
          }
        ]
      }
    }
  }
}

```

```

        }
    ]
}
},
"CapacityProvider": {
    "Type": "AWS::ECS::CapacityProvider",
    "Properties": {
        "AutoScalingGroupProvider": {
            "AutoScalingGroupArn": {
                "Ref": "ECSAutoScalingGroup"
            },
        },
        "ManagedScaling": {
            "InstanceWarmupPeriod": 60,
            "MinimumScalingStepSize": 1,
            "MaximumScalingStepSize": 100,
            "Status": "ENABLED",
            "TargetCapacity": 100
        },
        "ManagedTerminationProtection": "ENABLED"
    }
},
},
"CapacityProviderAssociation": {
    "Type": "AWS::ECS::ClusterCapacityProviderAssociations",
    "Properties": {
        "CapacityProviders": [
            {
                "Ref": "CapacityProvider"
            }
        ],
        "Cluster": {
            "Ref": "ECSCluster"
        },
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": {
                    "Ref": "CapacityProvider"
                },
                "Weight": 1
            }
        ]
    }
},
},

```

```

"ContainerHostSecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "GroupDescription": "Access to the EC2 hosts that run containers",
    "VpcId": {
      "Ref": "VpcId"
    }
  }
},
"EC2Role": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": [
              "ec2.amazonaws.com"
            ]
          },
          "Action": [
            "sts:AssumeRole"
          ]
        }
      ]
    },
    "Path": "/",
    "ManagedPolicyArns": [
      "arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role",
      "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
    ]
  }
},
"ECSTaskExecutionRole": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": [

```

```

        "ecs-tasks.amazonaws.com"
    ],
    },
    "Action": [
        "sts:AssumeRole"
    ],
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": {
                "Fn::Sub": "arn:${AWS::Partition}:ecs:
${AWS::Region}:${AWS::AccountId}:*"
            }
        },
        "StringEquals": {
            "aws:SourceAccount": {
                "Fn::Sub": "${AWS::AccountId}"
            }
        }
    }
}

],
},
"Path": "/",
"ManagedPolicyArns": [
    "arn:aws:iam::aws:policy/service-role/
AmazonECSTaskExecutionRolePolicy"
]
}
}
},
"Outputs": {
    "ClusterName": {
        "Description": "The ECS cluster into which to launch resources",
        "Value": "ECSCluster"
    },
    "ECSTaskExecutionRole": {
        "Description": "The role used to start up a task",
        "Value": "ECSTaskExecutionRole"
    },
    "CapacityProvider": {
        "Description": "The cluster capacity provider that the service should use to
request capacity when it wants to start up a task",
        "Value": "CapacityProvider"
    }
}

```

```
}  
}
```

YAML

AWSTemplateFormatVersion: 2010-09-09

Description: EC2 ECS cluster that starts out empty, with no EC2 instances yet.

An ECS capacity provider automatically launches more EC2 instances as required on the fly when you request ECS to launch services or standalone tasks.

Parameters:

InstanceType:

Type: String

Description: EC2 instance type

Default: "t2.medium"

AllowedValues:

- t1.micro
- t2.2xlarge
- t2.large
- t2.medium
- t2.micro
- t2.nano
- t2.small
- t2.xlarge
- t3.2xlarge
- t3.large
- t3.medium
- t3.micro
- t3.nano
- t3.small
- t3.xlarge

DesiredCapacity:

Type: Number

Default: "0"

Description: Number of EC2 instances to launch in your ECS cluster.

MaxSize:

Type: Number

Default: "100"

Description: Maximum number of EC2 instances that can be launched in your ECS cluster.

ECSAMI:

Description: The Amazon Machine Image ID used for the cluster

Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>

```
    Default: /aws/service/ecs/optimized-ami/amazon-linux-2023/recommended/image_id
VpcId:
  Type: AWS::EC2::VPC::Id
  Description: VPC ID where the ECS cluster is launched
  Default: vpc-1234567890abcdef0
SubnetIds:
  Type: List<AWS::EC2::Subnet::Id>
  Description: List of subnet IDs where the EC2 instances will be launched
  Default: "subnet-021345abcdef67890"
Resources:
# This is authorizes ECS to manage resources on your
# account on your behalf. This role is likely already created on your account
# ECSRole:
#   Type: AWS::IAM::ServiceLinkedRole
#   Properties:
#     AWSServiceName: 'ecs.amazonaws.com'

# ECS Resources
ECSCluster:
  Type: AWS::ECS::Cluster
  Properties:
    ClusterSettings:
      - Name: containerInsights
        Value: enabled

# Autoscaling group. This launches the actual EC2 instances that will register
# themselves as members of the cluster, and run the docker containers.
ECSAutoScalingGroup:
  Type: AWS::AutoScaling::AutoScalingGroup
  DependsOn:
    # This is to ensure that the ASG gets deleted first before these
    # resources, when it comes to stack teardown.
    - ECSCluster
    - EC2Role
  Properties:
    VPCZoneIdentifier:
      Ref: SubnetIds
    LaunchTemplate:
      LaunchTemplateId: !Ref ContainerInstances
      Version: !GetAtt ContainerInstances.LatestVersionNumber
    MinSize: 0
    MaxSize:
      Ref: MaxSize
    DesiredCapacity:
```



```

    Ref: DesiredCapacity
    NewInstancesProtectedFromScaleIn: true
  UpdatePolicy:
    AutoScalingReplacingUpdate:
      WillReplace: "true"
# The config for each instance that is added to the cluster
ContainerInstances:
  Type: AWS::EC2::LaunchTemplate
  Properties:
    LaunchTemplateName: "asg-launch-template"
    LaunchTemplateData:
      ImageId:
        Ref: ECSAMI
      InstanceType:
        Ref: InstanceType
      IamInstanceProfile:
        Name: !Ref EC2InstanceProfile
      SecurityGroupIds:
        - !Ref ContainerHostSecurityGroup
      # This injected configuration file is how the EC2 instance
      # knows which ECS cluster on your AWS account it should be joining
      UserData:
        Fn::Base64: !Sub |
          #!/bin/bash -xe
          echo ECS_CLUSTER=${ECSCluster} >> /etc/ecs/ecs.config
          yum install -y aws-cfn-bootstrap
          /opt/aws/bin/cfn-init -v --stack ${AWS::StackId} --resource
ContainerInstances --configsets full_install --region ${AWS::Region} &
          # Disable IMDSv1, and require IMDSv2
      MetadataOptions:
        HttpEndpoint: enabled
        HttpTokens: required
    EC2InstanceProfile:
      Type: AWS::IAM::InstanceProfile
      Properties:
        Path: /
        Roles:
          - !Ref EC2Role
# Create an ECS capacity provider to attach the ASG to the ECS cluster
# so that it autoscales as we launch more containers
CapacityProvider:
  Type: AWS::ECS::CapacityProvider
  Properties:
    AutoScalingGroupProvider:

```

```
    AutoScalingGroupArn: !Ref ECSAutoScalingGroup
    ManagedScaling:
      InstanceWarmupPeriod: 60
      MinimumScalingStepSize: 1
      MaximumScalingStepSize: 100
      Status: ENABLED
      # Percentage of cluster reservation to try to maintain
      TargetCapacity: 100
    ManagedTerminationProtection: ENABLED
  # Create a cluster capacity provider association so that the cluster
  # will use the capacity provider
  CapacityProviderAssociation:
    Type: AWS::ECS::ClusterCapacityProviderAssociations
    Properties:
      CapacityProviders:
        - !Ref CapacityProvider
      Cluster: !Ref ECSCluster
      DefaultCapacityProviderStrategy:
        - Base: 0
          CapacityProvider: !Ref CapacityProvider
          Weight: 1
  # A security group for the EC2 hosts that will run the containers.
  # This can be used to limit incoming traffic to or outgoing traffic
  # from the container's host EC2 instance.
  ContainerHostSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the EC2 hosts that run containers
      VpcId:
        Ref: VpcId
  # Role for the EC2 hosts. This allows the ECS agent on the EC2 hosts
  # to communicate with the ECS control plane, as well as download the docker
  # images from ECR to run on your host.
  EC2Role:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
```

```

    Path: /
    ManagedPolicyArns:
      # See reference: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/
security-iam-awsmanpol.html#security-iam-awsmanpol-AmazonEC2ContainerServiceforEC2Role
      - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
      # This managed policy allows us to connect to the instance using SSM
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
    # This is a role which is used within Fargate to allow the Fargate agent
    # to download images, and upload logs.
    ECSTaskExecutionRole:
      Type: AWS::IAM::Role
      Properties:
        AssumeRolePolicyDocument:
          Statement:
            - Effect: Allow
              Principal:
                Service:
                  - ecs-tasks.amazonaws.com
              Action:
                - sts:AssumeRole
              Condition:
                ArnLike:
                  aws:SourceArn: !Sub arn:${AWS::Partition}:ecs:${AWS::Region}:
${AWS::AccountId}:*
                StringEquals:
                  aws:SourceAccount: !Sub ${AWS::AccountId}
          Path: /
          # This role enables all features of ECS. See reference:
          # https://docs.aws.amazon.com/AmazonECS/latest/developerguide/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonECSTaskExecutionRolePolicy
          ManagedPolicyArns:
            - arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy
    Outputs:
      ClusterName:
        Description: The ECS cluster into which to launch resources
        Value: ECSCluster
      ECSTaskExecutionRole:
        Description: The role used to start up a task
        Value: ECSTaskExecutionRole
      CapacityProvider:
        Description: The cluster capacity provider that the service should use to
        request capacity when it wants to start up a task
        Value: CapacityProvider

```

Implementa un servizio

Il modello seguente definisce un servizio che utilizza il provider di capacità per richiedere la capacità AL2 023 su cui eseguire. I contenitori verranno lanciati sulle istanze AL2 023 non appena saranno online:

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "An example service that deploys in AWS VPC networking mode on EC2 capacity. Service uses a capacity provider to request EC2 instances to run on. Service runs with networking in private subnets, but still accessible to the internet via a load balancer hosted in public subnets.",
  "Parameters": {
    "VpcId": {
      "Type": "String",
      "Description": "The VPC that the service is running inside of"
    },
    "PublicSubnetIds": {
      "Type": "List<AWS::EC2::Subnet::Id>",
      "Description": "List of public subnet ID's to put the load balancer in"
    },
    "PrivateSubnetIds": {
      "Type": "List<AWS::EC2::Subnet::Id>",
      "Description": "List of private subnet ID's that the AWS VPC tasks are in"
    },
    "ClusterName": {
      "Type": "String",
      "Description": "The name of the ECS cluster into which to launch capacity."
    },
    "ECSTaskExecutionRole": {
      "Type": "String",
      "Description": "The role used to start up an ECS task"
    },
    "CapacityProvider": {
      "Type": "String",
      "Description": "The cluster capacity provider that the service should use to request capacity when it wants to start up a task"
    },
    "ServiceName": {
      "Type": "String",
      "Default": "web",
```

```

        "Description": "A name for the service"
    },
    "ImageUrl": {
        "Type": "String",
        "Default": "public.ecr.aws/docker/library/nginx:latest",
        "Description": "The url of a docker image that contains the application
process that will handle the traffic for this service"
    },
    "ContainerCpu": {
        "Type": "Number",
        "Default": 256,
        "Description": "How much CPU to give the container. 1024 is 1 CPU"
    },
    "ContainerMemory": {
        "Type": "Number",
        "Default": 512,
        "Description": "How much memory in megabytes to give the container"
    },
    "ContainerPort": {
        "Type": "Number",
        "Default": 80,
        "Description": "What port that the application expects traffic on"
    },
    "DesiredCount": {
        "Type": "Number",
        "Default": 2,
        "Description": "How many copies of the service task to run"
    }
},
"Resources": {
    "TaskDefinition": {
        "Type": "AWS::ECS::TaskDefinition",
        "Properties": {
            "Family": {
                "Ref": "ServiceName"
            },
            "Cpu": {
                "Ref": "ContainerCpu"
            },
            "Memory": {
                "Ref": "ContainerMemory"
            },
            "NetworkMode": "awsvpc",
            "RequiresCompatibilities": [

```

```
    "EC2"
  ],
  "ExecutionRoleArn": {
    "Ref": "ECSTaskExecutionRole"
  },
  "ContainerDefinitions": [
    {
      "Name": {
        "Ref": "ServiceName"
      },
      "Cpu": {
        "Ref": "ContainerCpu"
      },
      "Memory": {
        "Ref": "ContainerMemory"
      },
      "Image": {
        "Ref": "ImageUrl"
      },
      "PortMappings": [
        {
          "ContainerPort": {
            "Ref": "ContainerPort"
          },
          "HostPort": {
            "Ref": "ContainerPort"
          }
        }
      ],
      "LogConfiguration": {
        "LogDriver": "awslogs",
        "Options": {
          "mode": "non-blocking",
          "max-buffer-size": "25m",
          "awslogs-group": {
            "Ref": "LogGroup"
          },
          "awslogs-region": {
            "Ref": "AWS::Region"
          },
          "awslogs-stream-prefix": {
            "Ref": "ServiceName"
          }
        }
      }
    }
  ]
}
```

```

        }
    }
]
},
"Service": {
    "Type": "AWS::ECS::Service",
    "DependsOn": "PublicLoadBalancerListener",
    "Properties": {
        "ServiceName": {
            "Ref": "ServiceName"
        },
        "Cluster": {
            "Ref": "ClusterName"
        },
        "PlacementStrategies": [
            {
                "Field": "attribute:ecs.availability-zone",
                "Type": "spread"
            },
            {
                "Field": "cpu",
                "Type": "binpack"
            }
        ],
        "CapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": {
                    "Ref": "CapacityProvider"
                },
                "Weight": 1
            }
        ],
        "NetworkConfiguration": {
            "AwsvpcConfiguration": {
                "SecurityGroups": [
                    {
                        "Ref": "ServiceSecurityGroup"
                    }
                ],
                "Subnets": {
                    "Ref": "PrivateSubnetIds"
                }
            }
        }
    }
}

```

```

        }
    },
    "DeploymentConfiguration": {
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 75
    },
    "DesiredCount": {
        "Ref": "DesiredCount"
    },
    "TaskDefinition": {
        "Ref": "TaskDefinition"
    },
    "LoadBalancers": [
        {
            "ContainerName": {
                "Ref": "ServiceName"
            },
            "ContainerPort": {
                "Ref": "ContainerPort"
            },
            "TargetGroupArn": {
                "Ref": "ServiceTargetGroup"
            }
        }
    ]
},
"ServiceSecurityGroup": {
    "Type": "AWS::EC2::SecurityGroup",
    "Properties": {
        "GroupDescription": "Security group for service",
        "VpcId": {
            "Ref": "VpcId"
        }
    }
},
"ServiceTargetGroup": {
    "Type": "AWS::ElasticLoadBalancingV2::TargetGroup",
    "Properties": {
        "HealthCheckIntervalSeconds": 6,
        "HealthCheckPath": "/",
        "HealthCheckProtocol": "HTTP",
        "HealthCheckTimeoutSeconds": 5,
        "HealthyThresholdCount": 2,

```



```

        "TargetType": "ip",
        "Port": {
            "Ref": "ContainerPort"
        },
        "Protocol": "HTTP",
        "UnhealthyThresholdCount": 10,
        "VpcId": {
            "Ref": "VpcId"
        },
        "TargetGroupAttributes": [
            {
                "Key": "deregistration_delay.timeout_seconds",
                "Value": 0
            }
        ]
    },
    "PublicLoadBalancerSG": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Access to the public facing load balancer",
            "VpcId": {
                "Ref": "VpcId"
            },
            "SecurityGroupIngress": [
                {
                    "CidrIp": "0.0.0.0/0",
                    "IpProtocol": -1
                }
            ]
        }
    },
    "PublicLoadBalancer": {
        "Type": "AWS::ElasticLoadBalancingV2::LoadBalancer",
        "Properties": {
            "Scheme": "internet-facing",
            "LoadBalancerAttributes": [
                {
                    "Key": "idle_timeout.timeout_seconds",
                    "Value": "30"
                }
            ],
            "Subnets": {
                "Ref": "PublicSubnetIds"
            }
        }
    }
}

```

```

    },
    "SecurityGroups": [
      {
        "Ref": "PublicLoadBalancerSG"
      }
    ]
  },
  "PublicLoadBalancerListener": {
    "Type": "AWS::ElasticLoadBalancingV2::Listener",
    "Properties": {
      "DefaultActions": [
        {
          "Type": "forward",
          "ForwardConfig": {
            "TargetGroups": [
              {
                "TargetGroupArn": {
                  "Ref": "ServiceTargetGroup"
                },
                "Weight": 100
              }
            ]
          }
        }
      ],
      "LoadBalancerArn": {
        "Ref": "PublicLoadBalancer"
      },
      "Port": 80,
      "Protocol": "HTTP"
    }
  },
  "ServiceIngressfromLoadBalancer": {
    "Type": "AWS::EC2::SecurityGroupIngress",
    "Properties": {
      "Description": "Ingress from the public ALB",
      "GroupId": {
        "Ref": "ServiceSecurityGroup"
      },
      "IpProtocol": -1,
      "SourceSecurityGroupId": {
        "Ref": "PublicLoadBalancerSG"
      }
    }
  }
}

```

```

    }
  },
  "LogGroup": {
    "Type": "AWS::Logs::LogGroup"
  }
}
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Description: >-
  An example service that deploys in AWS VPC networking mode on EC2 capacity.
  Service uses a capacity provider to request EC2 instances to run on. Service
  runs with networking in private subnets, but still accessible to the internet
  via a load balancer hosted in public subnets.
Parameters:
  VpcId:
    Type: String
    Description: The VPC that the service is running inside of
  PublicSubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
    Description: List of public subnet ID's to put the load balancer in
  PrivateSubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
    Description: List of private subnet ID's that the AWS VPC tasks are in
  ClusterName:
    Type: String
    Description: The name of the ECS cluster into which to launch capacity.
  ECSTaskExecutionRole:
    Type: String
    Description: The role used to start up an ECS task
  CapacityProvider:
    Type: String
    Description: >-
      The cluster capacity provider that the service should use to request
      capacity when it wants to start up a task
  ServiceName:
    Type: String
    Default: web
    Description: A name for the service
  ImageUrl:
    Type: String

```

```
Default: 'public.ecr.aws/docker/library/nginx:latest'
Description: >-
    The url of a docker image that contains the application process that will
    handle the traffic for this service
ContainerCpu:
    Type: Number
    Default: 256
    Description: How much CPU to give the container. 1024 is 1 CPU
ContainerMemory:
    Type: Number
    Default: 512
    Description: How much memory in megabytes to give the container
ContainerPort:
    Type: Number
    Default: 80
    Description: What port that the application expects traffic on
DesiredCount:
    Type: Number
    Default: 2
    Description: How many copies of the service task to run
Resources:
    TaskDefinition:
        Type: 'AWS::ECS::TaskDefinition'
        Properties:
            Family: !Ref ServiceName
            Cpu: !Ref ContainerCpu
            Memory: !Ref ContainerMemory
            NetworkMode: awsvpc
            RequiresCompatibilities:
                - EC2
            ExecutionRoleArn: !Ref ECSTaskExecutionRole
            ContainerDefinitions:
                - Name: !Ref ServiceName
                  Cpu: !Ref ContainerCpu
                  Memory: !Ref ContainerMemory
                  Image: !Ref ImageUrl
                  PortMappings:
                      - ContainerPort: !Ref ContainerPort
                        HostPort: !Ref ContainerPort
                  LogConfiguration:
                      LogDriver: awslogs
                      Options:
                          mode: non-blocking
                          max-buffer-size: 25m
```

```
    awslogs-group: !Ref LogGroup
    awslogs-region: !Ref AWS::Region
    awslogs-stream-prefix: !Ref ServiceName

Service:
  Type: AWS::ECS::Service
  DependsOn: PublicLoadBalancerListener
  Properties:
    ServiceName: !Ref ServiceName
    Cluster: !Ref ClusterName
    PlacementStrategies:
      - Field: 'attribute:ecs.availability-zone'
        Type: spread
      - Field: cpu
        Type: binpack
    CapacityProviderStrategy:
      - Base: 0
        CapacityProvider: !Ref CapacityProvider
        Weight: 1
    NetworkConfiguration:
      AwsvpcConfiguration:
        SecurityGroups:
          - !Ref ServiceSecurityGroup
        Subnets: !Ref PrivateSubnetIds
    DeploymentConfiguration:
      MaximumPercent: 200
      MinimumHealthyPercent: 75
    DesiredCount: !Ref DesiredCount
    TaskDefinition: !Ref TaskDefinition
    LoadBalancers:
      - ContainerName: !Ref ServiceName
        ContainerPort: !Ref ContainerPort
        TargetGroupArn: !Ref ServiceTargetGroup

ServiceSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Security group for service
    VpcId: !Ref VpcId

ServiceTargetGroup:
  Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
  Properties:
    HealthCheckIntervalSeconds: 6
    HealthCheckPath: /
    HealthCheckProtocol: HTTP
    HealthCheckTimeoutSeconds: 5
```

```
    HealthyThresholdCount: 2
    TargetType: ip
    Port: !Ref ContainerPort
    Protocol: HTTP
    UnhealthyThresholdCount: 10
    VpcId: !Ref VpcId
    TargetGroupAttributes:
      - Key: deregistration_delay.timeout_seconds
        Value: 0
PublicLoadBalancerSG:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Access to the public facing load balancer
    VpcId: !Ref VpcId
    SecurityGroupIngress:
      - CidrIp: 0.0.0.0/0
        IpProtocol: -1
PublicLoadBalancer:
  Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
  Properties:
    Scheme: internet-facing
    LoadBalancerAttributes:
      - Key: idle_timeout.timeout_seconds
        Value: '30'
    Subnets: !Ref PublicSubnetIds
    SecurityGroups:
      - !Ref PublicLoadBalancerSG
PublicLoadBalancerListener:
  Type: 'AWS::ElasticLoadBalancingV2::Listener'
  Properties:
    DefaultActions:
      - Type: forward
        ForwardConfig:
          TargetGroups:
            - TargetGroupArn: !Ref ServiceTargetGroup
              Weight: 100
    LoadBalancerArn: !Ref PublicLoadBalancer
    Port: 80
    Protocol: HTTP
ServiceIngressfromLoadBalancer:
  Type: 'AWS::EC2::SecurityGroupIngress'
  Properties:
    Description: Ingress from the public ALB
    GroupId: !Ref ServiceSecurityGroup
```

```
IpProtocol: -1
SourceSecurityGroupId: !Ref PublicLoadBalancerSG
LogGroup:
  Type: 'AWS::Logs::LogGroup'
```

Modello di esempio Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) è un servizio di storage di file per istanze Amazon Elastic Compute Cloud (Amazon EC2). Con Amazon EFS le tue applicazioni dispongono di storage quando serve, perché la capacità di storage aumenta e si riduce automaticamente con l'aggiunta e la rimozione di file.

Il seguente modello di esempio distribuisce EC2 istanze (in un gruppo Auto Scaling) associate a un file system Amazon EFS. Per associare le istanze al file system, le istanze eseguono lo script helper `cfn-init`, che scarica e installa il pacchetto `yum nfs-utils`, crea una nuova directory e quindi utilizza il nome DNS del file system per montare il file system in tale directory. Il nome DNS del file system si risolve nell'indirizzo IP di una destinazione di montaggio nella zona di disponibilità dell' EC2istanza Amazon. Per ulteriori informazioni sulla struttura del nome DNS, consulta [Montaggio del file system](#) nella Guida per l'utente di Amazon Elastic File System.

Per misurare l'attività del Network File System, il modello include CloudWatch metriche Amazon personalizzate. Crea inoltre un VPC, una sottorete e i gruppi di sicurezza. Per consentire alle istanze di comunicare con il file system, il VPC deve avere il DNS abilitato e la destinazione di montaggio e EC2 le istanze devono trovarsi nella stessa zona di disponibilità (AZ), specificata dalla sottorete.

Il gruppo di sicurezza del target di montaggio consente una connessione di rete alla porta TCP 2049, necessaria per consentire a un client di montare un NFSv4 file system. Per ulteriori informazioni sui gruppi di sicurezza per EC2 le istanze e gli obiettivi di montaggio, consulta la sezione [Sicurezza](#) nella [Amazon Elastic File System User Guide](#).

Note

Se effettui un aggiornamento alla destinazione di montaggio che ne causa la sostituzione, le istanze o le applicazioni che utilizzano il file system associato potrebbero venire interrotte. Questo può causare la perdita di scritture non confermate con commit. Per evitare interruzioni, arresta le istanze quando aggiorni la destinazione di montaggio impostando la capacità desiderata su zero. In questo modo le istanze possono disinstallare il file system prima che la destinazione di montaggio venga eliminata. Al termine dell'aggiornamento

del montaggio, avvia le istanze in un aggiornamento successivo impostando la capacità desiderata.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "This template creates an Amazon EFS file system and mount target and associates it with Amazon EC2 instances in an Auto Scaling group. **WARNING** This template creates Amazon EC2 instances and related resources. You will be billed for the AWS resources used if you create a stack from this template.",
  "Parameters": {
    "InstanceType" : {
      "Description" : "WebServer EC2 instance type",
      "Type" : "String",
      "Default" : "t2.small",
      "AllowedValues" : [
        "t1.micro",
        "t2.nano",
        "t2.micro",
        "t2.small",
        "t2.medium",
        "t2.large",
        "m1.small",
        "m1.medium",
        "m1.large",
        "m1.xlarge",
        "m2.xlarge",
        "m2.2xlarge",
        "m2.4xlarge",
        "m3.medium",
        "m3.large",
        "m3.xlarge",
        "m3.2xlarge",
        "m4.large",
        "m4.xlarge",
        "m4.2xlarge",
        "m4.4xlarge",
        "m4.10xlarge",
        "c1.medium",
        "c1.xlarge",
        "c3.large",
```



```

        "c3.xlarge",
        "c3.2xlarge",
        "c3.4xlarge",
        "c3.8xlarge",
        "c4.large",
        "c4.xlarge",
        "c4.2xlarge",
        "c4.4xlarge",
        "c4.8xlarge",
        "g2.2xlarge",
        "g2.8xlarge",
        "r3.large",
        "r3.xlarge",
        "r3.2xlarge",
        "r3.4xlarge",
        "r3.8xlarge",
        "i2.xlarge",
        "i2.2xlarge",
        "i2.4xlarge",
        "i2.8xlarge",
        "d2.xlarge",
        "d2.2xlarge",
        "d2.4xlarge",
        "d2.8xlarge",
        "hi1.4xlarge",
        "hs1.8xlarge",
        "cr1.8xlarge",
        "cc2.8xlarge",
        "cg1.4xlarge"
    ],
    "ConstraintDescription" : "must be a valid EC2 instance type."
},
"KeyName": {
    "Type": "AWS::EC2::KeyPair::KeyName",
    "Description": "Name of an existing EC2 key pair to enable SSH access to the EC2
instances"
},
"AsgMaxSize": {
    "Type": "Number",
    "Description": "Maximum size and initial desired capacity of Auto Scaling Group",
    "Default": "2"
},
"SSHLocation" : {

```

```

    "Description" : "The IP address range that can be used to connect to the EC2
instances by using SSH",
    "Type": "String",
    "MinLength": "9",
    "MaxLength": "18",
    "Default": "0.0.0.0/0",
    "AllowedPattern": "(\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})\\. (\\d{1,3})/(\\d{1,2})",
    "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."
  },
  "VolumeName" : {
    "Description" : "The name to be used for the EFS volume",
    "Type": "String",
    "MinLength": "1",
    "Default": "myEFSvolume"
  },
  "MountPoint" : {
    "Description" : "The Linux mount point for the EFS volume",
    "Type": "String",
    "MinLength": "1",
    "Default": "myEFSvolume"
  }
},
"Mappings" : {
  "AWSInstanceType2Arch" : {
    "t1.micro"      : { "Arch" : "HVM64" },
    "t2.nano"      : { "Arch" : "HVM64" },
    "t2.micro"      : { "Arch" : "HVM64" },
    "t2.small"     : { "Arch" : "HVM64" },
    "t2.medium"    : { "Arch" : "HVM64" },
    "t2.large"     : { "Arch" : "HVM64" },
    "m1.small"     : { "Arch" : "HVM64" },
    "m1.medium"    : { "Arch" : "HVM64" },
    "m1.large"     : { "Arch" : "HVM64" },
    "m1.xlarge"    : { "Arch" : "HVM64" },
    "m2.xlarge"    : { "Arch" : "HVM64" },
    "m2.2xlarge"   : { "Arch" : "HVM64" },
    "m2.4xlarge"   : { "Arch" : "HVM64" },
    "m3.medium"    : { "Arch" : "HVM64" },
    "m3.large"     : { "Arch" : "HVM64" },
    "m3.xlarge"    : { "Arch" : "HVM64" },
    "m3.2xlarge"   : { "Arch" : "HVM64" },
    "m4.large"     : { "Arch" : "HVM64" },
    "m4.xlarge"    : { "Arch" : "HVM64" },
    "m4.2xlarge"   : { "Arch" : "HVM64" },

```

```

    "m4.4xlarge" : { "Arch" : "HVM64" },
    "m4.10xlarge" : { "Arch" : "HVM64" },
    "c1.medium" : { "Arch" : "HVM64" },
    "c1.xlarge" : { "Arch" : "HVM64" },
    "c3.large" : { "Arch" : "HVM64" },
    "c3.xlarge" : { "Arch" : "HVM64" },
    "c3.2xlarge" : { "Arch" : "HVM64" },
    "c3.4xlarge" : { "Arch" : "HVM64" },
    "c3.8xlarge" : { "Arch" : "HVM64" },
    "c4.large" : { "Arch" : "HVM64" },
    "c4.xlarge" : { "Arch" : "HVM64" },
    "c4.2xlarge" : { "Arch" : "HVM64" },
    "c4.4xlarge" : { "Arch" : "HVM64" },
    "c4.8xlarge" : { "Arch" : "HVM64" },
    "g2.2xlarge" : { "Arch" : "HVMG2" },
    "g2.8xlarge" : { "Arch" : "HVMG2" },
    "r3.large" : { "Arch" : "HVM64" },
    "r3.xlarge" : { "Arch" : "HVM64" },
    "r3.2xlarge" : { "Arch" : "HVM64" },
    "r3.4xlarge" : { "Arch" : "HVM64" },
    "r3.8xlarge" : { "Arch" : "HVM64" },
    "i2.xlarge" : { "Arch" : "HVM64" },
    "i2.2xlarge" : { "Arch" : "HVM64" },
    "i2.4xlarge" : { "Arch" : "HVM64" },
    "i2.8xlarge" : { "Arch" : "HVM64" },
    "d2.xlarge" : { "Arch" : "HVM64" },
    "d2.2xlarge" : { "Arch" : "HVM64" },
    "d2.4xlarge" : { "Arch" : "HVM64" },
    "d2.8xlarge" : { "Arch" : "HVM64" },
    "hi1.4xlarge" : { "Arch" : "HVM64" },
    "hs1.8xlarge" : { "Arch" : "HVM64" },
    "cr1.8xlarge" : { "Arch" : "HVM64" },
    "cc2.8xlarge" : { "Arch" : "HVM64" }
  },
  "AWSRegionArch2AMI" : {
    "us-east-1" : { "HVM64" : "ami-0ff8a91507f77f867", "HVMG2" :
"ami-0a584ac55a7631c0c"},
    "us-west-2" : { "HVM64" : "ami-a0cfeed8", "HVMG2" :
"ami-0e09505bc235aa82d"},
    "us-west-1" : { "HVM64" : "ami-0bdb828fd58c52235", "HVMG2" :
"ami-066ee5fd4a9ef77f1"},
    "eu-west-1" : { "HVM64" : "ami-047bb4163c506cd98", "HVMG2" :
"ami-0a7c483d527806435"},
    "eu-west-2" : { "HVM64" : "ami-f976839e", "HVMG2" : "NOT_SUPPORTED"},

```

```

        "eu-west-3"      : {"HVM64" : "ami-0ebc281c20e89ba4b", "HVMG2" :
"NOT_SUPPORTED"},
        "eu-central-1"   : {"HVM64" : "ami-0233214e13e500f77", "HVMG2" :
"ami-06223d46a6d0661c7"},
        "ap-northeast-1" : {"HVM64" : "ami-06cd52961ce9f0d85", "HVMG2" :
"ami-053cdd503598e4a9d"},
        "ap-northeast-2" : {"HVM64" : "ami-0a10b2721688ce9d2", "HVMG2" :
"NOT_SUPPORTED"},
        "ap-northeast-3" : {"HVM64" : "ami-0d98120a9fb693f07", "HVMG2" :
"NOT_SUPPORTED"},
        "ap-southeast-1" : {"HVM64" : "ami-08569b978cc4dfa10", "HVMG2" :
"ami-0be9df32ae9f92309"},
        "ap-southeast-2" : {"HVM64" : "ami-09b42976632b27e9b", "HVMG2" :
"ami-0a9ce9fecc3d1daf8"},
        "ap-south-1"     : {"HVM64" : "ami-0912f71e06545ad88", "HVMG2" :
"ami-097b15e89dbdcfcf4"},
        "us-east-2"      : {"HVM64" : "ami-0b59bfac6be064b78", "HVMG2" :
"NOT_SUPPORTED"},
        "ca-central-1"   : {"HVM64" : "ami-0b18956f", "HVMG2" : "NOT_SUPPORTED"},
        "sa-east-1"      : {"HVM64" : "ami-07b14488da8ea02a0", "HVMG2" :
"NOT_SUPPORTED"},
        "cn-north-1"     : {"HVM64" : "ami-0a4eaf6c4454eda75", "HVMG2" :
"NOT_SUPPORTED"},
        "cn-northwest-1" : {"HVM64" : "ami-6b6a7d09", "HVMG2" : "NOT_SUPPORTED"}
    }
},
"Resources": {
    "CloudWatchPutMetricsRole" : {
        "Type" : "AWS::IAM::Role",
        "Properties" : {
            "AssumeRolePolicyDocument" : {
                "Statement" : [ {
                    "Effect" : "Allow",
                    "Principal" : {
                        "Service" : [ "ec2.amazonaws.com" ]
                    },
                    "Action" : [ "sts:AssumeRole" ]
                } ]
            },
            "Path" : "/"
        }
    },
    "CloudWatchPutMetricsRolePolicy" : {
        "Type" : "AWS::IAM::Policy",

```

```

    "Properties" : {
      "PolicyName" : "CloudWatch_PutMetricData",
      "PolicyDocument" : {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "CloudWatchPutMetricData",
            "Effect": "Allow",
            "Action": ["cloudwatch:PutMetricData"],
            "Resource": ["*"]
          }
        ]
      },
      "Roles" : [ { "Ref" : "CloudWatchPutMetricsRole" } ]
    }
  },
  "CloudWatchPutMetricsInstanceProfile" : {
    "Type" : "AWS::IAM::InstanceProfile",
    "Properties" : {
      "Path" : "/",
      "Roles" : [ { "Ref" : "CloudWatchPutMetricsRole" } ]
    }
  },
  "VPC": {
    "Type": "AWS::EC2::VPC",
    "Properties": {
      "EnableDnsSupport" : "true",
      "EnableDnsHostnames" : "true",
      "CidrBlock": "10.0.0.0/16",
      "Tags": [ { "Key": "Application", "Value": { "Ref": "AWS::StackId" } } ]
    }
  },
  "InternetGateway" : {
    "Type" : "AWS::EC2::InternetGateway",
    "Properties" : {
      "Tags" : [
        { "Key" : "Application", "Value" : { "Ref" : "AWS::StackName" } },
        { "Key" : "Network", "Value" : "Public" }
      ]
    }
  },
  "GatewayToInternet" : {
    "Type" : "AWS::EC2::VPCGatewayAttachment",
    "Properties" : {

```

```

    "VpcId" : { "Ref" : "VPC" },
    "InternetGatewayId" : { "Ref" : "InternetGateway" }
  },
  "RouteTable":{
    "Type":"AWS::EC2::RouteTable",
    "Properties":{
      "VpcId": {"Ref":"VPC"}
    }
  },
  "SubnetRouteTableAssoc": {
    "Type" : "AWS::EC2::SubnetRouteTableAssociation",
    "Properties" : {
      "RouteTableId" : {"Ref":"RouteTable"},
      "SubnetId" : {"Ref":"Subnet"}
    }
  },
  "InternetGatewayRoute": {
    "Type":"AWS::EC2::Route",
    "Properties":{
      "DestinationCidrBlock":"0.0.0.0/0",
      "RouteTableId":{"Ref":"RouteTable"},
      "GatewayId":{"Ref":"InternetGateway"}
    }
  },
  "Subnet": {
    "Type": "AWS::EC2::Subnet",
    "Properties": {
      "VpcId": { "Ref": "VPC" },
      "CidrBlock": "10.0.0.0/24",
      "Tags": [ { "Key": "Application", "Value": { "Ref": "AWS::StackId" } } ]
    }
  },
  "InstanceSecurityGroup": {
    "Type": "AWS::EC2::SecurityGroup",
    "Properties": {
      "VpcId": { "Ref": "VPC" },
      "GroupDescription": "Enable SSH access via port 22",
      "SecurityGroupIngress": [
        { "IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "CidrIp": { "Ref":
"SSHLocation" } },
        { "IpProtocol": "tcp", "FromPort": 80, "ToPort": 80, "CidrIp": "0.0.0.0/0" }
      ]
    }
  }

```

```

},
"MountTargetSecurityGroup": {
  "Type": "AWS::EC2::SecurityGroup",
  "Properties": {
    "VpcId": { "Ref": "VPC" },
    "GroupDescription": "Security group for mount target",
    "SecurityGroupIngress": [
      {
        "IpProtocol": "tcp",
        "FromPort": 2049,
        "ToPort": 2049,
        "CidrIp": "0.0.0.0/0"
      }
    ]
  }
},
"FileSystem": {
  "Type": "AWS::EFS::FileSystem",
  "Properties": {
    "PerformanceMode": "generalPurpose",
    "FileSystemTags": [
      {
        "Key": "Name",
        "Value": { "Ref" : "VolumeName" }
      }
    ]
  }
},
"MountTarget": {
  "Type": "AWS::EFS::MountTarget",
  "Properties": {
    "FileSystemId": { "Ref": "FileSystem" },
    "SubnetId": { "Ref": "Subnet" },
    "SecurityGroups": [ { "Ref": "MountTargetSecurityGroup" } ]
  }
},
"LaunchConfiguration": {
  "Type": "AWS::AutoScaling::LaunchConfiguration",
  "Metadata" : {
    "AWS::CloudFormation::Init" : {
      "configSets" : {
        "MountConfig" : [ "setup", "mount" ]
      },
      "setup" : {

```

```

    "packages" : {
      "yum" : {
        "nfs-utils" : []
      }
    },
    "files" : {
      "/home/ec2-user/post_nfsstat" : {
        "content" : { "Fn::Join" : [ "", [
          "#!/bin/bash\n",
          "\n",
          "INPUT=\"$(cat)\"\n",
          "CW_JSON_OPEN='{ \"Namespace\": \"EFS\", \"MetricData\": [ '\n",
          "CW_JSON_CLOSE=' ] }'\n",
          "CW_JSON_METRIC=' '\n",
          "METRIC_COUNTER=0\n",
          "\n",
          "for COL in 1 2 3 4 5 6; do\n",
          "\n",
          "  COUNTER=0\n",
          "  METRIC_FIELD=$COL\n",
          "  DATA_FIELD=$(( $COL + ( $COL - 1 ) ) )\n",
          "\n",
          "  while read line; do\n",
          "    if [[ COUNTER -gt 0 ]]; then\n",
          "\n",
          "      LINE=`echo $line | tr -s ' ' '\n`,
          "      AWS_COMMAND=\"aws cloudwatch put-metric-data --region ",
{ "Ref": "AWS::Region" }, "\n",
          "      MOD=$(( $COUNTER % 2 ))\n",
          "\n",
          "      if [ $MOD -eq 1 ]; then\n",
          "        METRIC_NAME=`echo $LINE | cut -d ' ' -f $METRIC_FIELD`\n",
          "\n",
          "        else\n",
          "          METRIC_VALUE=`echo $LINE | cut -d ' ' -f $DATA_FIELD`\n",
          "          fi\n",
          "\n",
          "          if [[ -n \"$METRIC_NAME\" && -n \"$METRIC_VALUE\" ]]; then\n",
          "\n",
          "            INSTANCE_ID=$(curl -s http://169.254.169.254/latest/meta-
data/instance-id)\n",
          "            CW_JSON_METRIC=\"$CW_JSON_METRIC { \\\"MetricName\\\": \\\"
\\\"$METRIC_NAME\\\", \\\"Dimensions\\\": [{\\\"Name\\\": \\\"InstanceId\\\", \\\"Value\\\"
\\\": \\\"$INSTANCE_ID\\\"} ], \\\"Value\\\": $METRIC_VALUE },\n",

```



```

        unset METRIC_NAME\n",
        unset METRIC_VALUE\n",
        "\n",
        METRIC_COUNTER=$((METRIC_COUNTER+1))\n",
        if [ $METRIC_COUNTER -eq 20 ]; then\n",
        # 20 is max metric collection size, so we have to
submit here\n",
        aws cloudwatch put-metric-data --region ", { "Ref":
"AWS::Region" }, " --cli-input-json \"`echo $CW_JSON_OPEN ${CW_JSON_METRIC%?}
$CW_JSON_CLOSE`\n",
        "\n",
        # reset\n",
        METRIC_COUNTER=0\n",
        CW_JSON_METRIC=' '\n",
        fi\n",
        fi \n",
        "\n",
        "\n",
        "\n",
        COUNTER=$((COUNTER+1))\n",
        fi\n",
        "\n",
        if [[ \"$line\" == \"Client nfs v4:\" ]]; then\n",
        # the next line is the good stuff \n",
        COUNTER=$((COUNTER+1))\n",
        fi\n",
        done <<< \"$INPUT\"\n",
        done\n",
        "\n",
        # submit whatever is left\n",
        aws cloudwatch put-metric-data --region ", { "Ref":
"AWS::Region" }, " --cli-input-json \"`echo $CW_JSON_OPEN ${CW_JSON_METRIC%?}
$CW_JSON_CLOSE`\"
    ] ] },
    "mode": "000755",
    "owner": "ec2-user",
    "group": "ec2-user"
},
"/home/ec2-user/crontab" : {
    "content" : { "Fn::Join" : [ "", [
        "* * * * * /usr/sbin/nfsstat | /home/ec2-user/post_nfsstat\n"
    ] ] },
    "owner": "ec2-user",
    "group": "ec2-user"
}

```

```

    }
  },
  "commands" : {
    "01_createdir" : {
      "command" : {"Fn::Join" : [ "", [ "mkdir /", { "Ref" :
"MountPoint" }]]]}
    }
  },
  "mount" : {
    "commands" : {
      "01_mount" : {
        "command" : { "Fn::Sub": "sudo mount -t nfs4 -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2 ${FileSystem}.efs.
${AWS::Region}.amazonaws.com:/ /${MountPoint}" }
      },
      "02_permissions" : {
        "command" : {"Fn::Join" : [ "", [ "chown ec2-user:ec2-user /",
{ "Ref" : "MountPoint" }]]]}
      }
    }
  },
  "Properties": {
    "AssociatePublicIpAddress" : true,
    "ImageId": {
      "Fn::FindInMap": [ "AWSRegionArch2AMI", { "Ref": "AWS::Region" }, {
        "Fn::FindInMap": [ "AWSInstanceType2Arch", { "Ref": "InstanceType" },
"Arch" ]
      } ]
    },
    "InstanceType": { "Ref": "InstanceType" },
    "KeyName": { "Ref": "KeyName" },
    "SecurityGroups": [ { "Ref": "InstanceSecurityGroup" } ],
    "IamInstanceProfile" : { "Ref" : "CloudWatchPutMetricsInstanceProfile" },
    "UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [
      "#!/bin/bash -xe\n",
      "yum install -y aws-cfn-bootstrap\n",

      "/opt/aws/bin/cfn-init -v ",
      "      --stack ", { "Ref" : "AWS::StackName" },
      "      --resource LaunchConfiguration ",
      "      --configsets MountConfig ",

```

```

        "        --region ", { "Ref" : "AWS::Region" }, "\n",

        "crontab /home/ec2-user/crontab\n",

        "/opt/aws/bin/cfn-signal -e $? ",
        "        --stack ", { "Ref" : "AWS::StackName" },
        "        --resource AutoScalingGroup ",
        "        --region ", { "Ref" : "AWS::Region" }, "\n"
    ]]]}
}
},
"AutoScalingGroup": {
    "Type": "AWS::AutoScaling::AutoScalingGroup",
    "DependsOn": ["MountTarget", "GatewayToInternet"],
    "CreationPolicy" : {
        "ResourceSignal" : {
            "Timeout" : "PT15M",
            "Count" : { "Ref": "AsgMaxSize" }
        }
    },
    "Properties": {
        "VPCZoneIdentifier": [ { "Ref": "Subnet" } ],
        "LaunchConfigurationName": { "Ref": "LaunchConfiguration" },
        "MinSize": "1",
        "MaxSize": { "Ref": "AsgMaxSize" },
        "DesiredCapacity": { "Ref": "AsgMaxSize" },
        "Tags": [ {
            "Key": "Name",
            "Value": "EFS FileSystem Mounted Instance",
            "PropagateAtLaunch": "true"
        } ]
    }
}
},
"Outputs" : {
    "MountTargetID" : {
        "Description" : "Mount target ID",
        "Value" : { "Ref" : "MountTarget" }
    },
    "FileSystemID" : {
        "Description" : "File system ID",
        "Value" : { "Ref" : "FileSystem" }
    }
}
}

```

```
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Description: This template creates an Amazon EFS file system and mount target and  
  associates it with Amazon EC2 instances in an Auto Scaling group. **WARNING** This  
  template creates Amazon EC2 instances and related resources. You will be billed  
  for the AWS resources used if you create a stack from this template.
```

```
Parameters:
```

```
  InstanceType:
```

```
    Description: WebServer EC2 instance type
```

```
    Type: String
```

```
    Default: t2.small
```

```
    AllowedValues:
```

- t1.micro
- t2.nano
- t2.micro
- t2.small
- t2.medium
- t2.large
- m1.small
- m1.medium
- m1.large
- m1.xlarge
- m2.xlarge
- m2.2xlarge
- m2.4xlarge
- m3.medium
- m3.large
- m3.xlarge
- m3.2xlarge
- m4.large
- m4.xlarge
- m4.2xlarge
- m4.4xlarge
- m4.10xlarge
- c1.medium
- c1.xlarge
- c3.large
- c3.xlarge
- c3.2xlarge
- c3.4xlarge

- c3.8xlarge
- c4.large
- c4.xlarge
- c4.2xlarge
- c4.4xlarge
- c4.8xlarge
- g2.2xlarge
- g2.8xlarge
- r3.large
- r3.xlarge
- r3.2xlarge
- r3.4xlarge
- r3.8xlarge
- i2.xlarge
- i2.2xlarge
- i2.4xlarge
- i2.8xlarge
- d2.xlarge
- d2.2xlarge
- d2.4xlarge
- d2.8xlarge
- hi1.4xlarge
- hs1.8xlarge
- cr1.8xlarge
- cc2.8xlarge
- cg1.4xlarge

ConstraintDescription: must be a valid EC2 instance type.

KeyName:

Type: AWS::EC2::KeyPair::KeyName

Description: Name of an existing EC2 key pair to enable SSH access to the ECS instances

AsgMaxSize:

Type: Number

Description: Maximum size and initial desired capacity of Auto Scaling Group

Default: '2'

SSHLocation:

Description: The IP address range that can be used to connect to the EC2 instances by using SSH

Type: String

MinLength: '9'

MaxLength: '18'

Default: 0.0.0.0/0

AllowedPattern: "(\d{1,3})\.\.(\d{1,3})\.\.(\d{1,3})\.\.(\d{1,3})/(\d{1,2})"

ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.

```
VolumeName:
  Description: The name to be used for the EFS volume
  Type: String
  MinLength: '1'
  Default: myEFSvolume
MountPoint:
  Description: The Linux mount point for the EFS volume
  Type: String
  MinLength: '1'
  Default: myEFSvolume
Mappings:
  AWSInstanceType2Arch:
    t1.micro:
      Arch: HVM64
    t2.nano:
      Arch: HVM64
    t2.micro:
      Arch: HVM64
    t2.small:
      Arch: HVM64
    t2.medium:
      Arch: HVM64
    t2.large:
      Arch: HVM64
    m1.small:
      Arch: HVM64
    m1.medium:
      Arch: HVM64
    m1.large:
      Arch: HVM64
    m1.xlarge:
      Arch: HVM64
    m2.xlarge:
      Arch: HVM64
    m2.2xlarge:
      Arch: HVM64
    m2.4xlarge:
      Arch: HVM64
    m3.medium:
      Arch: HVM64
    m3.large:
      Arch: HVM64
    m3.xlarge:
      Arch: HVM64
```

```
m3.2xlarge:
  Arch: HVM64
m4.large:
  Arch: HVM64
m4.xlarge:
  Arch: HVM64
m4.2xlarge:
  Arch: HVM64
m4.4xlarge:
  Arch: HVM64
m4.10xlarge:
  Arch: HVM64
c1.medium:
  Arch: HVM64
c1.xlarge:
  Arch: HVM64
c3.large:
  Arch: HVM64
c3.xlarge:
  Arch: HVM64
c3.2xlarge:
  Arch: HVM64
c3.4xlarge:
  Arch: HVM64
c3.8xlarge:
  Arch: HVM64
c4.large:
  Arch: HVM64
c4.xlarge:
  Arch: HVM64
c4.2xlarge:
  Arch: HVM64
c4.4xlarge:
  Arch: HVM64
c4.8xlarge:
  Arch: HVM64
g2.2xlarge:
  Arch: HVMG2
g2.8xlarge:
  Arch: HVMG2
r3.large:
  Arch: HVM64
r3.xlarge:
  Arch: HVM64
```

```
r3.2xlarge:
  Arch: HVM64
r3.4xlarge:
  Arch: HVM64
r3.8xlarge:
  Arch: HVM64
i2.xlarge:
  Arch: HVM64
i2.2xlarge:
  Arch: HVM64
i2.4xlarge:
  Arch: HVM64
i2.8xlarge:
  Arch: HVM64
d2.xlarge:
  Arch: HVM64
d2.2xlarge:
  Arch: HVM64
d2.4xlarge:
  Arch: HVM64
d2.8xlarge:
  Arch: HVM64
hi1.4xlarge:
  Arch: HVM64
hs1.8xlarge:
  Arch: HVM64
cr1.8xlarge:
  Arch: HVM64
cc2.8xlarge:
  Arch: HVM64
AWSRegionArch2AMI:
us-east-1:
  HVM64: ami-0ff8a91507f77f867
  HVMG2: ami-0a584ac55a7631c0c
us-west-2:
  HVM64: ami-a0cfeed8
  HVMG2: ami-0e09505bc235aa82d
us-west-1:
  HVM64: ami-0bdb828fd58c52235
  HVMG2: ami-066ee5fd4a9ef77f1
eu-west-1:
  HVM64: ami-047bb4163c506cd98
  HVMG2: ami-0a7c483d527806435
eu-west-2:
```



```
HVM64: ami-f976839e
HVMG2: NOT_SUPPORTED
eu-west-3:
  HVM64: ami-0ebc281c20e89ba4b
  HVMG2: NOT_SUPPORTED
eu-central-1:
  HVM64: ami-0233214e13e500f77
  HVMG2: ami-06223d46a6d0661c7
ap-northeast-1:
  HVM64: ami-06cd52961ce9f0d85
  HVMG2: ami-053cdd503598e4a9d
ap-northeast-2:
  HVM64: ami-0a10b2721688ce9d2
  HVMG2: NOT_SUPPORTED
ap-northeast-3:
  HVM64: ami-0d98120a9fb693f07
  HVMG2: NOT_SUPPORTED
ap-southeast-1:
  HVM64: ami-08569b978cc4dfa10
  HVMG2: ami-0be9df32ae9f92309
ap-southeast-2:
  HVM64: ami-09b42976632b27e9b
  HVMG2: ami-0a9ce9fecc3d1daf8
ap-south-1:
  HVM64: ami-0912f71e06545ad88
  HVMG2: ami-097b15e89dbdcfcf4
us-east-2:
  HVM64: ami-0b59bfac6be064b78
  HVMG2: NOT_SUPPORTED
ca-central-1:
  HVM64: ami-0b18956f
  HVMG2: NOT_SUPPORTED
sa-east-1:
  HVM64: ami-07b14488da8ea02a0
  HVMG2: NOT_SUPPORTED
cn-north-1:
  HVM64: ami-0a4eaf6c4454eda75
  HVMG2: NOT_SUPPORTED
cn-northwest-1:
  HVM64: ami-6b6a7d09
  HVMG2: NOT_SUPPORTED
```

Resources:

```
CloudWatchPutMetricsRole:
  Type: AWS::IAM::Role
```

Properties:**AssumeRolePolicyDocument:****Statement:**

- Effect: Allow

Principal:**Service:**

- ec2.amazonaws.com

Action:

- sts:AssumeRole

Path: "/"

CloudWatchPutMetricsRolePolicy:

Type: AWS::IAM::Policy

Properties:

PolicyName: CloudWatch_PutMetricData

PolicyDocument:

Version: '2012-10-17'

Statement:

- Sid: CloudWatchPutMetricData

Effect: Allow

Action:

- cloudwatch:PutMetricData

Resource:

- "*"

Roles:

- Ref: CloudWatchPutMetricsRole

CloudWatchPutMetricsInstanceProfile:

Type: AWS::IAM::InstanceProfile

Properties:

Path: "/"

Roles:

- Ref: CloudWatchPutMetricsRole

VPC:

Type: AWS::EC2::VPC

Properties:

EnableDnsSupport: 'true'

EnableDnsHostnames: 'true'

CidrBlock: 10.0.0.0/16

Tags:

- Key: Application

Value:

Ref: AWS::StackId

InternetGateway:

Type: AWS::EC2::InternetGateway

Properties:

```
    Tags:
      - Key: Application
        Value:
          Ref: AWS::StackName
      - Key: Network
        Value: Public
  GatewayToInternet:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId:
        Ref: VPC
      InternetGatewayId:
        Ref: InternetGateway
  RouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId:
        Ref: VPC
  SubnetRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId:
        Ref: RouteTable
      SubnetId:
        Ref: Subnet
  InternetGatewayRoute:
    Type: AWS::EC2::Route
    Properties:
      DestinationCidrBlock: 0.0.0.0/0
      RouteTableId:
        Ref: RouteTable
      GatewayId:
        Ref: InternetGateway
  Subnet:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId:
        Ref: VPC
      CidrBlock: 10.0.0.0/24
      Tags:
        - Key: Application
          Value:
            Ref: AWS::StackId
  InstanceSecurityGroup:
```

```
Type: AWS::EC2::SecurityGroup
Properties:
  VpcId:
    Ref: VPC
  GroupDescription: Enable SSH access via port 22
  SecurityGroupIngress:
    - IpProtocol: tcp
      FromPort: 22
      ToPort: 22
      CidrIp:
        Ref: SSHLocation
    - IpProtocol: tcp
      FromPort: 80
      ToPort: 80
      CidrIp: 0.0.0.0/0
MountTargetSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    VpcId:
      Ref: VPC
    GroupDescription: Security group for mount target
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 2049
        ToPort: 2049
        CidrIp: 0.0.0.0/0
FileSystem:
  Type: AWS::EFS::FileSystem
  Properties:
    PerformanceMode: generalPurpose
    FileSystemTags:
      - Key: Name
        Value:
          Ref: VolumeName
MountTarget:
  Type: AWS::EFS::MountTarget
  Properties:
    FileSystemId:
      Ref: FileSystem
    SubnetId:
      Ref: Subnet
    SecurityGroups:
      - Ref: MountTargetSecurityGroup
LaunchConfiguration:
```

Type: AWS::AutoScaling::LaunchConfiguration

Metadata:

AWS::CloudFormation::Init:

configSets:

MountConfig:

- setup
- mount

setup:

packages:

yum:

nfs-utils: []

files:

"/home/ec2-user/post_nfsstat":

content: !Sub |

#!/bin/bash

INPUT="\$(cat)"

CW_JSON_OPEN='{ "Namespace": "EFS", "MetricData": ['

CW_JSON_CLOSE='] }'

CW_JSON_METRIC=''

METRIC_COUNTER=0

for COL in 1 2 3 4 5 6; do

COUNTER=0

METRIC_FIELD=\$COL

DATA_FIELD=\$((\$COL + (\$COL - 1)))

while read line; do

if [[COUNTER -gt 0]]; then

LINE=`echo \$line | tr -s ' ' `

AWS_COMMAND="aws cloudwatch put-metric-data --region

\${AWS::Region}"

MOD=\$((\$COUNTER % 2))

if [\$MOD -eq 1]; then

METRIC_NAME=`echo \$LINE | cut -d ' ' -f \$METRIC\_FIELD`

else

METRIC_VALUE=`echo \$LINE | cut -d ' ' -f \$DATA\_FIELD`

fi

if [[-n "\$METRIC_NAME" && -n "\$METRIC_VALUE"]]; then

```

        INSTANCE_ID=$(curl -s http://169.254.169.254/latest/meta-data/
instance-id)

        CW_JSON_METRIC="$CW_JSON_METRIC { \"MetricName\": \"$METRIC_NAME
\", \"Dimensions\": [{\"Name\": \"InstanceId\", \"Value\": \"$INSTANCE_ID\"} ], \"Value
\": $METRIC_VALUE },"

        unset METRIC_NAME
        unset METRIC_VALUE

        METRIC_COUNTER=$((METRIC_COUNTER+1))
        if [ $METRIC_COUNTER -eq 20 ]; then
            # 20 is max metric collection size, so we have to submit here
            aws cloudwatch put-metric-data --region ${AWS::Region} --cli-
input-json "`echo $CW_JSON_OPEN ${!CW_JSON_METRIC%?} $CW_JSON_CLOSE`"

            # reset
            METRIC_COUNTER=0
            CW_JSON_METRIC=''
        fi
    fi

    COUNTER=$((COUNTER+1))
fi

if [[ "$line" == "Client nfs v4:" ]]; then
    # the next line is the good stuff
    COUNTER=$((COUNTER+1))
fi
done <<< "$INPUT"
done

# submit whatever is left
aws cloudwatch put-metric-data --region ${AWS::Region} --cli-input-json
"`echo $CW_JSON_OPEN ${!CW_JSON_METRIC%?} $CW_JSON_CLOSE`"
mode: '000755'
owner: ec2-user
group: ec2-user
"/home/ec2-user/crontab":
content: "* * * * * /usr/sbin/nfsstat | /home/ec2-user/post_nfsstat\n"
owner: ec2-user
group: ec2-user
commands:
    01_createdir:

```

```

        command: !Sub "mkdir /${MountPoint}"
    mount:
        commands:
            01_mount:
                command: !Sub >
                    mount -t nfs4 -o nfsvers=4.1 ${FileSystem}.efs.
${AWS::Region}.amazonaws.com:/ /${MountPoint}
            02_permissions:
                command: !Sub "chown ec2-user:ec2-user /${MountPoint}"
Properties:
    AssociatePublicIpAddress: true
    ImageId:
        Fn::FindInMap:
            - AWSRegionArch2AMI
            - Ref: AWS::Region
            - Fn::FindInMap:
                - AWSInstanceType2Arch
                - Ref: InstanceType
                - Arch
    InstanceType:
        Ref: InstanceType
    KeyName:
        Ref: KeyName
    SecurityGroups:
        - Ref: InstanceSecurityGroup
    IamInstanceProfile:
        Ref: CloudWatchPutMetricsInstanceProfile
    UserData:
        Fn::Base64: !Sub |
            #!/bin/bash -xe
            yum install -y aws-cfn-bootstrap
            /opt/aws/bin/cfn-init -v --stack ${AWS::StackName} --resource
LaunchConfiguration --configsets MountConfig --region ${AWS::Region}
            crontab /home/ec2-user/crontab
            /opt/aws/bin/cfn-signal -e $? --stack ${AWS::StackName} --resource
AutoScalingGroup --region ${AWS::Region}
    AutoScalingGroup:
        Type: AWS::AutoScaling::AutoScalingGroup
        DependsOn:
            - MountTarget
            - GatewayToInternet
        CreationPolicy:
            ResourceSignal:
                Timeout: PT15M

```

```
    Count:
      Ref: AsgMaxSize
  Properties:
    VPCZoneIdentifier:
      - Ref: Subnet
    LaunchConfigurationName:
      Ref: LaunchConfiguration
    MinSize: '1'
    MaxSize:
      Ref: AsgMaxSize
    DesiredCapacity:
      Ref: AsgMaxSize
    Tags:
      - Key: Name
        Value: EFS FileSystem Mounted Instance
        PropagateAtLaunch: 'true'
  Outputs:
    MountTargetID:
      Description: Mount target ID
      Value:
        Ref: MountTarget
    FileSystemID:
      Description: File system ID
      Value:
        Ref: FileSystem
```

Frammenti di modello Elastic Beanstalk

Con Elastic Beanstalk, puoi distribuire e gestire rapidamente le applicazioni senza preoccuparti dell'infrastruttura che esegue tali AWS applicazioni. Il seguente modello di esempio può aiutarti a descrivere le risorse Elastic Beanstalk nel tuo modello. AWS CloudFormation

PHP di esempio Elastic Beanstalk

Il modello di esempio seguente distribuisce un'applicazione Web PHP di esempio archiviata in un bucket Amazon S3. L'ambiente è anche un ambiente con scalabilità automatica e bilanciamento del carico, con un minimo di due istanze Amazon EC2 e un massimo di sei. Mostra un ambiente Elastic Beanstalk che utilizza una configurazione di avvio legacy. Per informazioni sull'utilizzo di un modello di lancio, consulta [Launch Templates](#) nella Developer Guide.AWS Elastic Beanstalk

Sostituire *solution-stack* con un nome dello stack di soluzioni (versione della piattaforma). Per un elenco degli stack di soluzioni disponibili, usa il AWS CLI comando `aws elasticbeanstalk list-available-solution-stacks`.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "sampleApplication": {
      "Type": "AWS::ElasticBeanstalk::Application",
      "Properties": {
        "Description": "AWS Elastic Beanstalk Sample Application"
      }
    },
    "sampleApplicationVersion": {
      "Type": "AWS::ElasticBeanstalk::ApplicationVersion",
      "Properties": {
        "ApplicationName": {
          "Ref": "sampleApplication"
        },
        "Description": "AWS ElasticBeanstalk Sample Application Version",
        "SourceBundle": {
          "S3Bucket": {
            "Fn::Sub": "elasticbeanstalk-samples-${AWS::Region}"
          },
          "S3Key": "php-newsample-app.zip"
        }
      }
    },
    "sampleConfigurationTemplate": {
      "Type": "AWS::ElasticBeanstalk::ConfigurationTemplate",
      "Properties": {
        "ApplicationName": {
          "Ref": "sampleApplication"
        },
        "Description": "AWS ElasticBeanstalk Sample Configuration Template",
        "OptionSettings": [
          {
            "Namespace": "aws:autoscaling:asg",
            "OptionName": "MinSize",
            "Value": "2"
          }
        ]
      }
    }
  }
}
```

```

        {
            "Namespace": "aws:autoscaling:asg",
            "OptionName": "MaxSize",
            "Value": "6"
        },
        {
            "Namespace": "aws:elasticbeanstalk:environment",
            "OptionName": "EnvironmentType",
            "Value": "LoadBalanced"
        },
        {
            "Namespace": "aws:autoscaling:launchconfiguration",
            "OptionName": "IamInstanceProfile",
            "Value": {
                "Ref": "MyInstanceProfile"
            }
        }
    ],
    "SolutionStackName": "solution-stack"
}
},
"sampleEnvironment": {
    "Type": "AWS::ElasticBeanstalk::Environment",
    "Properties": {
        "ApplicationName": {
            "Ref": "sampleApplication"
        },
        "Description": "AWS ElasticBeanstalk Sample Environment",
        "TemplateName": {
            "Ref": "sampleConfigurationTemplate"
        },
        "VersionLabel": {
            "Ref": "sampleApplicationVersion"
        }
    }
},
"MyInstanceRole": {
    "Type": "AWS::IAM::Role",
    "Properties": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",

```

```
        "Principal": {
            "Service": [
                "ec2.amazonaws.com"
            ]
        },
        "Action": [
            "sts:AssumeRole"
        ]
    }
]
},
"description": "Beanstalk EC2 role",
"managedPolicyArns": [
    "arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier",
    "arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker",
    "arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier"
]
}
},
"myInstanceProfile": {
    "type": "AWS::IAM::InstanceProfile",
    "properties": {
        "roles": [
            {
                "ref": "MyInstanceRole"
            }
        ]
    }
}
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'

Resources:
  sampleApplication:
    Type: AWS::ElasticBeanstalk::Application
    Properties:
      Description: AWS Elastic Beanstalk Sample Application
  sampleApplicationVersion:
    Type: AWS::ElasticBeanstalk::ApplicationVersion
    Properties:
```

```
  ApplicationName:
    Ref: sampleApplication
  Description: AWS ElasticBeanstalk Sample Application Version
  SourceBundle:
    S3Bucket: !Sub "elasticbeanstalk-samples-${AWS::Region}"
    S3Key: php-newsample-app.zip
sampleConfigurationTemplate:
  Type: AWS::ElasticBeanstalk::ConfigurationTemplate
  Properties:
    ApplicationName:
      Ref: sampleApplication
    Description: AWS ElasticBeanstalk Sample Configuration Template
    OptionSettings:
      - Namespace: aws:autoscaling:asg
        OptionName: MinSize
        Value: '2'
      - Namespace: aws:autoscaling:asg
        OptionName: MaxSize
        Value: '6'
      - Namespace: aws:elasticbeanstalk:environment
        OptionName: EnvironmentType
        Value: LoadBalanced
      - Namespace: aws:autoscaling:launchconfiguration
        OptionName: IamInstanceProfile
        Value: !Ref MyInstanceProfile
    SolutionStackName: solution-stack
sampleEnvironment:
  Type: AWS::ElasticBeanstalk::Environment
  Properties:
    ApplicationName:
      Ref: sampleApplication
    Description: AWS ElasticBeanstalk Sample Environment
    TemplateName:
      Ref: sampleConfigurationTemplate
    VersionLabel:
      Ref: sampleApplicationVersion
MyInstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
```

```

    Service:
      - ec2.amazonaws.com
    Action:
      - sts:AssumeRole
    Description: Beanstalk EC2 role
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier
      - arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker
      - arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier
    MyInstanceProfile:
      Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref MyInstanceRole

```

Frammenti di modello Elastic Load Balancing

Risorsa load balancer Elastic Load Balancing

In questo esempio viene illustrato un load balancer Elastic Load Balancing con un singolo listener e senza istanze.

JSON

```

"MyLoadBalancer" : {
  "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
  "Properties" : {
    "AvailabilityZones" : [ "us-east-1a" ],
    "Listeners" : [ {
      "LoadBalancerPort" : "80",
      "InstancePort" : "80",
      "Protocol" : "HTTP"
    } ]
  }
}

```

YAML

```

MyLoadBalancer:
  Type: AWS::ElasticLoadBalancing::LoadBalancer
  Properties:
    AvailabilityZones:

```

```
- "us-east-1a"
Listeners:
- LoadBalancerPort: '80'
  InstancePort: '80'
  Protocol: HTTP
```

Risorsa load balancer Elastic Load Balancing con controllo dello stato

Questo esempio mostra un load balancer Elastic Load Balancing con due EC2 istanze Amazon, un singolo listener e un controllo dello stato.

JSON

```
"MyLoadBalancer" : {
  "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
  "Properties" : {
    "AvailabilityZones" : [ "us-east-1a" ],
    "Instances" : [
      { "Ref" : "logical name of AWS::EC2::Instance resource 1" },
      { "Ref" : "logical name of AWS::EC2::Instance resource 2" }
    ],
    "Listeners" : [ {
      "LoadBalancerPort" : "80",
      "InstancePort" : "80",
      "Protocol" : "HTTP"
    } ],
    "HealthCheck" : {
      "Target" : "HTTP:80/",
      "HealthyThreshold" : "3",
      "UnhealthyThreshold" : "5",
      "Interval" : "30",
      "Timeout" : "5"
    }
  }
}
```

YAML

```
MyLoadBalancer:
  Type: AWS::ElasticLoadBalancing::LoadBalancer
  Properties:
```

```
AvailabilityZones:
- "us-east-1a"
Instances:
- Ref: logical name of AWS::EC2::Instance resource 1
- Ref: logical name of AWS::EC2::Instance resource 2
Listeners:
- LoadBalancerPort: '80'
  InstancePort: '80'
  Protocol: HTTP
HealthCheck:
  Target: HTTP:80/
  HealthyThreshold: '3'
  UnhealthyThreshold: '5'
  Interval: '30'
  Timeout: '5'
```

AWS Identity and Access Management frammenti di modello

Questa sezione contiene frammenti di AWS Identity and Access Management modello.

Argomenti

- [Dichiarazione di una risorsa utente IAM](#)
- [Dichiarazione di una risorsa chiave di accesso IAM](#)
- [Dichiarazione di una risorsa di gruppo IAM](#)
- [Aggiunta di utenti a un gruppo](#)
- [Dichiarazione di una policy IAM](#)
- [Dichiarazione di una policy di un bucket Amazon S3](#)
- [Dichiarazione di una policy di un argomento Amazon SNS](#)
- [Dichiarazione di una policy Amazon SQS](#)
- [Esempi di modello per i ruoli IAM](#)

Important

Durante la creazione o l'aggiornamento di uno stack con un modello contenente risorse IAM, devi prendere atto dell'utilizzo delle funzionalità IAM. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).

Dichiarazione di una risorsa utente IAM

Questo frammento di codice mostra come dichiarare una risorsa [AWS::IAM::User](#) per creare un utente IAM. L'utente viene dichiarato con il percorso ("/") e un profilo di login che utilizza la password (myP@ssW0rd).

Il documento di policy `giveaccesstoqueueonly` consente all'utente di eseguire tutte le operazioni di Amazon SQS nella risorsa della coda Amazon SQS `myqueue` e rifiuta l'accesso a tutte le altre risorse della coda Amazon SQS. La funzione `Fn::GetAtt` ottiene l'attributo ARN della risorsa [AWS::SQS::Queue](#) `myqueue`.

Il documento di policy `giveaccesstotopiconly` viene aggiunto all'utente per consentirgli di eseguire tutte le operazioni di Amazon SNS nella risorsa dell'argomento Amazon SNS `mytopic` e rifiutare l'accesso a tutte le altre risorse della coda Amazon SNS. La funzione `Ref` ottiene l'attributo ARN della risorsa [AWS::SNS::Topic](#) `mytopic`.

JSON

```
"myuser" : {
  "Type" : "AWS::IAM::User",
  "Properties" : {
    "Path" : "/",
    "LoginProfile" : {
      "Password" : "myP@ssW0rd"
    },
    "Policies" : [ {
      "PolicyName" : "giveaccesstoqueueonly",
      "PolicyDocument" : {
        "Version": "2012-10-17",
        "Statement" : [ {
          "Effect" : "Allow",
          "Action" : [ "sqs:*" ],
          "Resource" : [ {
            "Fn::GetAtt" : [ "myqueue", "Arn" ]
          } ]
        }, {
          "Effect" : "Deny",
          "Action" : [ "sqs:*" ],
          "NotResource" : [ {
            "Fn::GetAtt" : [ "myqueue", "Arn" ]
          } ]
        } ]
      }
    } ]
  }
}
```



```

    ] }
  }, {
    "PolicyName" : "giveaccesstotopiconly",
    "PolicyDocument" : {
      "Version": "2012-10-17",
      "Statement" : [ {
        "Effect" : "Allow",
        "Action" : [ "sns:*" ],
        "Resource" : [ { "Ref" : "mytopic" } ]
      }, {
        "Effect" : "Deny",
        "Action" : [ "sns:*" ],
        "NotResource" : [ { "Ref" : "mytopic" } ]
      } ]
    }
  } ]
}
}
}

```

YAML

```

myuser:
  Type: AWS::IAM::User
  Properties:
    Path: "/"
    LoginProfile:
      Password: myP@ssW0rd
    Policies:
      - PolicyName: giveaccesstoqueueonly
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - sqs:*
              Resource:
                - !GetAtt myqueue.Arn
            - Effect: Deny
              Action:
                - sqs:*
              NotResource:
                - !GetAtt myqueue.Arn
      - PolicyName: giveaccesstotopiconly

```

```
PolicyDocument:
  Version: '2012-10-17'
  Statement:
    - Effect: Allow
      Action:
        - sns:*
      Resource:
        - !Ref mytopic
    - Effect: Deny
      Action:
        - sns:*
      NotResource:
        - !Ref mytopic
```

Dichiarazione di una risorsa chiave di accesso IAM

Questo frammento mostra una risorsa [AWS::IAM::AccessKey](#). La risorsa `myaccesskey` crea una chiave di accesso e la assegna a un utente IAM dichiarato come risorsa [AWS::IAM::User](#) nel modello.

JSON

```
"myaccesskey" : {
  "Type" : "AWS::IAM::AccessKey",
  "Properties" : {
    "UserName" : { "Ref" : "myuser" }
  }
}
```

YAML

```
myaccesskey:
  Type: AWS::IAM::AccessKey
  Properties:
    UserName:
      !Ref myuser
```

Puoi ottenere la chiave segreta per una risorsa `AWS::IAM::AccessKey` utilizzando la funzione `Fn::GetAtt`. Uno dei modi per recuperare la chiave segreta è inserirla in un valore `Output`. Puoi ottenere la chiave di accesso utilizzando la funzione `Ref`. Le seguenti dichiarazioni del valore `Output` ottengono la chiave di accesso e la chiave segreta per `myaccesskey`.

JSON

```
"AccessKeyformyaccesskey" : {
  "Value" : { "Ref" : "myaccesskey" }
},
"SecretKeyformyaccesskey" : {
  "Value" : {
    "Fn::GetAtt" : [ "myaccesskey", "SecretAccessKey" ]
  }
}
```

YAML

```
AccessKeyformyaccesskey:
  Value:
    !Ref myaccesskey
SecretKeyformyaccesskey:
  Value: !GetAtt myaccesskey.SecretAccessKey
```

Puoi anche passare la chiave di AWS accesso e la chiave segreta a un' EC2 istanza Amazon o a un gruppo di Auto Scaling definito nel modello. La seguente dichiarazione [AWS::EC2::Instance](#) utilizza la proprietà `UserData` per passare la chiave di accesso e la chiave segreta per la risorsa `myaccesskey`.

JSON

```
"myinstance" : {
  "Type" : "AWS::EC2::Instance",
  "Properties" : {
    "AvailabilityZone" : "us-east-1a",
    "ImageId" : "ami-0ff8a91507f77f867",
    "UserData" : {
      "Fn::Base64" : {
        "Fn::Join" : [
          "", [
            "ACCESS_KEY=", {
              "Ref" : "myaccesskey"
            },
            "&",
            "SECRET_KEY=",
            {
```

```
"Fn::GetAtt" : [
    "myaccesskey",
    "SecretAccessKey"
]
}
```

YAML

```
myinstance:
  Type: AWS::EC2::Instance
  Properties:
    AvailabilityZone: "us-east-1a"
    ImageId: ami-0ff8a91507f77f867
    UserData:
      Fn::Base64: !Sub "ACCESS_KEY=${myaccesskey}&SECRET_KEY=
${myaccesskey.SecretAccessKey}"
```

Dichiarazione di una risorsa di gruppo IAM

Questo frammento mostra una risorsa [AWS::IAM::Group](#). Il gruppo ha un percorso ("/myapplication/"). Il documento di policy myapppolicy viene aggiunto al gruppo per consentire agli utenti del gruppo di eseguire tutte le operazioni di Amazon SQS nella risorsa della coda Amazon SQS myqueue e rifiutare l'accesso a tutte le altre risorse Amazon SQS eccetto myqueue.

Per assegnare una policy a una risorsa, IAM richiede l'ARN (Amazon Resource Name) per la risorsa. Nel frammento, la funzione `Fn::GetAtt` ottiene l'ARN della coda della risorsa `AWS::SQS::Queue`.

JSON

```
"mygroup" : {
  "Type" : "AWS::IAM::Group",
  "Properties" : {
    "Path" : "/myapplication/",
    "Policies" : [ {
      "PolicyName" : "myappppolicy",
```

```

    "PolicyDocument" : {
      "Version": "2012-10-17",
      "Statement" : [ {
        "Effect" : "Allow",
        "Action" : [ "sqs:*" ],
        "Resource" : [ {
          "Fn::GetAtt" : [ "myqueue", "Arn" ]
        } ]
      },
      {
        "Effect" : "Deny",
        "Action" : [ "sqs:*" ],
        "NotResource" : [ { "Fn::GetAtt" : [ "myqueue", "Arn" ] } ]
      }
    ]
  }
}

```

YAML

```

mygroup:
  Type: AWS::IAM::Group
  Properties:
    Path: "/myapplication/"
    Policies:
      - PolicyName: myapppolicy
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - sqs:*
              Resource: !GetAtt myqueue.Arn
            - Effect: Deny
              Action:
                - sqs:*
              NotResource: !GetAtt myqueue.Arn

```

Aggiunta di utenti a un gruppo

La risorsa [AWS::IAM::UserToGroupAddition](#) aggiunge utenti a un gruppo. Nel seguente frammento, la risorsa `addUserToGroup` aggiunge i seguenti utenti a un gruppo esistente denominato

myexistinggroup2: l'utente esistente existinguser1 e l'utente myuser dichiarato come risorsa [AWS::IAM::User](#) nel modello.

JSON

```
"addUserToGroup" : {
  "Type" : "AWS::IAM::UserToGroupAddition",
  "Properties" : {
    "GroupName" : "myexistinggroup2",
    "Users" : [ "existinguser1", { "Ref" : "myuser" } ]
  }
}
```

YAML

```
addUserToGroup:
  Type: AWS::IAM::UserToGroupAddition
  Properties:
    GroupName: myexistinggroup2
    Users:
      - existinguser1
      - !Ref myuser
```

Dichiarazione di una policy IAM

Questo frammento mostra come creare una policy e applicarla a più gruppi utilizzando una risorsa [AWS::IAM::Policy](#) denominata mypolicy. La risorsa mypolicy include una proprietà PolicyDocument che consente le operazioni GetObject, PutObject e PutObjectAcl sugli oggetti nel bucket S3 rappresentato dall'ARN arn:aws:s3:::myAWSBucket. La risorsa mypolicy applica la policy a un gruppo esistente denominato myexistinggroup1 e a un gruppo mygroup che viene dichiarato nel modello come una risorsa [AWS::IAM::Group](#). Questo esempio mostra come applicare una policy a un gruppo utilizzando la proprietà Groups; tuttavia, è anche possibile utilizzare la proprietà Users per aggiungere un documento della policy a un elenco di utenti.

JSON

```
"mypolicy" : {
  "Type" : "AWS::IAM::Policy",
  "Properties" : {
    "PolicyName" : "mygrouppolicy",
```

```

    "PolicyDocument" : {
      "Version": "2012-10-17",
      "Statement" : [ {
        "Effect" : "Allow",
        "Action" : [
          "s3:GetObject" , "s3:PutObject" , "s3:PutObjectAcl" ],
        "Resource" : "arn:aws:s3:::myAWSBucket/*"
      } ]
    },
    "Groups" : [ "myexistinggroup1", { "Ref" : "mygroup" } ]
  }
}

```

YAML

```

mypolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyName: mygrouppolicy
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Action:
            - s3:GetObject
            - s3:PutObject
            - s3:PutObjectAcl
          Resource: arn:aws:s3:::myAWSBucket/*
    Groups:
      - myexistinggroup1
      - !Ref mygroup

```

Dichiarazione di una policy di un bucket Amazon S3

Questo frammento mostra come creare una policy e applicarla a un bucket Amazon S3 utilizzando la risorsa [AWS::S3::BucketPolicy](#). La risorsa `mybucketpolicy` dichiara un documento di policy che consente all'utente IAM `user1` di eseguire l'operazione `GetObject` su tutti gli oggetti nel bucket S3 a cui la policy viene applicata. Nel frammento, la funzione `Fn::GetAtt` ottiene l'ARN della risorsa `user1`. La risorsa `mybucketpolicy` applica la policy alla risorsa `AWS::S3::BucketPolicy` `mybucket`. La funzione `Ref` ottiene il nome del bucket della risorsa `mybucket`.

JSON

```
"mybucketpolicy" : {
  "Type" : "AWS::S3::BucketPolicy",
  "Properties" : {
    "PolicyDocument" : {
      "Id" : "MyPolicy",
      "Version": "2012-10-17",
      "Statement" : [ {
        "Sid" : "ReadAccess",
        "Action" : [ "s3:GetObject" ],
        "Effect" : "Allow",
        "Resource" : { "Fn::Join" : [
          "", [ "arn:aws:s3:::", { "Ref" : "mybucket" } , "/*" ]
        ] },
        "Principal" : {
          "AWS" : { "Fn::GetAtt" : [ "user1", "Arn" ] }
        }
      } ]
    },
    "Bucket" : { "Ref" : "mybucket" }
  }
}
```

YAML

```
mybucketpolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    PolicyDocument:
      Id: MyPolicy
      Version: '2012-10-17'
      Statement:
        - Sid: ReadAccess
          Action:
            - s3:GetObject
          Effect: Allow
          Resource: !Sub "arn:aws:s3:::${mybucket}/*"
          Principal:
            AWS: !GetAtt user1.Arn
    Bucket: !Ref mybucket
```


Dichiarazione di una policy di un argomento Amazon SNS

Questo frammento mostra come creare una policy e applicarla a un argomento Amazon SNS utilizzando la risorsa [AWS::SNS::TopicPolicy](#). La risorsa `mysnspolicy` include una proprietà `PolicyDocument` che consente alla risorsa [AWS::IAM::User](#) `myuser` di eseguire l'operazione `Publish` su una risorsa [AWS::SNS::Topic](#) `mytopic`. Nel frammento, la funzione `Fn::GetAtt` ottiene l'ARN per la risorsa `myuser` e la funzione `Ref` ottiene l'ARN per la risorsa `mytopic`.

JSON

```
"mysnspolicy" : {
  "Type" : "AWS::SNS::TopicPolicy",
  "Properties" : {
    "PolicyDocument" : {
      "Id" : "MyTopicPolicy",
      "Version" : "2012-10-17",
      "Statement" : [ {
        "Sid" : "My-statement-id",
        "Effect" : "Allow",
        "Principal" : {
          "AWS" : { "Fn::GetAtt" : [ "myuser", "Arn" ] }
        },
        "Action" : "sns:Publish",
        "Resource" : "*"
      } ]
    },
    "Topics" : [ { "Ref" : "mytopic" } ]
  }
}
```

YAML

```
mysnspolicy:
  Type: AWS::SNS::TopicPolicy
  Properties:
    PolicyDocument:
      Id: MyTopicPolicy
      Version: '2012-10-17'
      Statement:
        - Sid: My-statement-id
          Effect: Allow
          Principal:
```

```
AWS: !GetAtt myuser.Arn
Action: sns:Publish
Resource: "*"
Topics:
- !Ref mytopic
```

Dichiarazione di una policy Amazon SQS

Questo frammento mostra come creare una policy e applicarla a una coda Amazon SQS utilizzando la risorsa [AWS::SQS::QueuePolicy](#). La proprietà `PolicyDocument` consente all'utente esistente `myapp` (specificato dal relativo ARN) di eseguire l'operazione `SendMessage` su una coda esistente, specificata tramite il relativo URL e su una risorsa [AWS::SQS::Queue](#) `myqueue`. La funzione [Ref](#) ottiene l'URL per la risorsa `myqueue`.

JSON

```
"mysqspolicy" : {
  "Type" : "AWS::SQS::QueuePolicy",
  "Properties" : {
    "PolicyDocument" : {
      "Id" : "MyQueuePolicy",
      "Version" : "2012-10-17",
      "Statement" : [ {
        "Sid" : "Allow-User-SendMessage",
        "Effect" : "Allow",
        "Principal" : {
          "AWS" : "arn:aws:iam::123456789012:user/myapp"
        },
        "Action" : [ "sqs:SendMessage" ],
        "Resource" : "*"
      } ]
    },
    "Queues" : [
      "https://sqs.us-east-2aws-region.amazonaws.com/123456789012/myexistingqueue",
      { "Ref" : "myqueue" }
    ]
  }
}
```

YAML

```
mysqspolicy:
```

```
Type: AWS::SQS::QueuePolicy
Properties:
  PolicyDocument:
    Id: MyQueuePolicy
    Version: '2012-10-17'
    Statement:
      - Sid: Allow-User-SendMessage
        Effect: Allow
        Principal:
          AWS: arn:aws:iam::123456789012:user/myapp
        Action:
          - sqs:SendMessage
        Resource: "*"
  Queues:
    - https://sqs.aws-region.amazonaws.com/123456789012/myexistingqueue
    - !Ref myqueue
```

Esempi di modello per i ruoli IAM

Questa sezione fornisce esempi di CloudFormation modelli per i ruoli IAM per le EC2 istanze.

Per ulteriori informazioni, consulta [i ruoli IAM per Amazon EC2](#) nella Amazon EC2 User Guide.

Ruolo IAM con EC2

In questo esempio, il profilo dell'istanza è referenziato dalla `IamInstanceProfile` proprietà dell'EC2 istanza. Sia la policy dell'istanza che del ruolo fanno riferimento a [AWS::IAM::Role](#).

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "myEC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Version": "2009-05-15",
      "Properties": {
        "ImageId": "ami-0ff8a91507f77f867",
        "InstanceType": "m1.small",
        "Monitoring": "true",
        "DisableApiTermination": "false",
        "IamInstanceProfile": {
          "Ref": "RootInstanceProfile"
        }
      }
    }
  }
}
```

```

    }
  },
  "RootRole": {
    "Type": "AWS::IAM::Role",
    "Properties": {
      "AssumeRolePolicyDocument": {
        "Version" : "2012-10-17",
        "Statement": [ {
          "Effect": "Allow",
          "Principal": {
            "Service": [ "ec2.amazonaws.com" ]
          },
          "Action": [ "sts:AssumeRole" ]
        } ]
      },
      "Path": "/"
    }
  },
  "RolePolicies": {
    "Type": "AWS::IAM::Policy",
    "Properties": {
      "PolicyName": "root",
      "PolicyDocument": {
        "Version" : "2012-10-17",
        "Statement": [ {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*"
        } ]
      },
      "Roles": [ { "Ref": "RootRole" } ]
    }
  },
  "RootInstanceProfile": {
    "Type": "AWS::IAM::InstanceProfile",
    "Properties": {
      "Path": "/",
      "Roles": [ { "Ref": "RootRole" } ]
    }
  }
}

```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  myEC2Instance:
    Type: AWS::EC2::Instance
    Version: '2009-05-15'
    Properties:
      ImageId: ami-0ff8a91507f77f867
      InstanceType: m1.small
      Monitoring: 'true'
      DisableApiTermination: 'false'
      IamInstanceProfile:
        !Ref RootInstanceProfile
  RootRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: "/"
  RolePolicies:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: root
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action: "*"
            Resource: "*"
      Roles:
        - !Ref RootRole
  RootInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: "/"
      Roles:
```

- !Ref RootRole

Ruolo IAM con il gruppo Auto Scaling

In questo esempio, il profilo dell'istanza è referenziato dalla `IamInstanceProfile` proprietà di una configurazione di avvio di Amazon EC2 Auto Scaling.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "myLCOne": {
      "Type": "AWS::AutoScaling::LaunchConfiguration",
      "Version": "2009-05-15",
      "Properties": {
        "ImageId": "ami-0ff8a91507f77f867",
        "InstanceType": "m1.small",
        "InstanceMonitoring": "true",
        "IamInstanceProfile": { "Ref": "RootInstanceProfile" }
      }
    },
    "myASGrpOne": {
      "Type": "AWS::AutoScaling::AutoScalingGroup",
      "Version": "2009-05-15",
      "Properties": {
        "AvailabilityZones": [ "us-east-1a" ],
        "LaunchConfigurationName": { "Ref": "myLCOne" },
        "MinSize": "0",
        "MaxSize": "0",
        "HealthCheckType": "EC2",
        "HealthCheckGracePeriod": "120"
      }
    },
    "RootRole": {
      "Type": "AWS::IAM::Role",
      "Properties": {
        "AssumeRolePolicyDocument": {
          "Version" : "2012-10-17",
          "Statement": [ {
            "Effect": "Allow",
            "Principal": {
              "Service": [ "ec2.amazonaws.com" ]
            }
          }
        ]
      }
    }
  }
}
```

```

        },
        "Action": [ "sts:AssumeRole" ]
      } ]
    },
    "Path": "/"
  }
},
"RolePolicies": {
  "Type": "AWS::IAM::Policy",
  "Properties": {
    "PolicyName": "root",
    "PolicyDocument": {
      "Version" : "2012-10-17",
      "Statement": [ {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
      } ]
    },
    "Roles": [ { "Ref": "RootRole" } ]
  }
},
"RootInstanceProfile": {
  "Type": "AWS::IAM::InstanceProfile",
  "Properties": {
    "Path": "/",
    "Roles": [ { "Ref": "RootRole" } ]
  }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  myLCOne:
    Type: AWS::AutoScaling::LaunchConfiguration
    Version: '2009-05-15'
    Properties:
      ImageId: ami-0ff8a91507f77f867
      InstanceType: m1.small
      InstanceMonitoring: 'true'

```

```
IamInstanceProfile:
  !Ref RootInstanceProfile
myASGrpOne:
  Type: AWS::AutoScaling::AutoScalingGroup
  Version: '2009-05-15'
  Properties:
    AvailabilityZones:
      - "us-east-1a"
    LaunchConfigurationName:
      !Ref myLCOne
    MinSize: '0'
    MaxSize: '0'
    HealthCheckType: EC2
    HealthCheckGracePeriod: '120'
RootRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: "/"
RolePolicies:
  Type: AWS::IAM::Policy
  Properties:
    PolicyName: root
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Action: "*"
          Resource: "*"
    Roles:
      - !Ref RootRole
RootInstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: "/"
    Roles:
```


- !Ref RootRole

AWS Lambda modello

Il modello seguente utilizza una funzione AWS Lambda (Lambda) e una risorsa personalizzata per aggiungere un nuovo gruppo di sicurezza a un elenco di gruppi di sicurezza esistenti. Questa funzione è utile per creare un elenco di gruppi di sicurezza in modo dinamico, così che l'elenco includa sia i nuovi gruppi di sicurezza sia quelli già esistenti. Ad esempio, è possibile passare un elenco di gruppi di sicurezza esistenti come valore di parametro, aggiungere il nuovo valore all'elenco e quindi associare tutti i valori a un'istanza. EC2 Per ulteriori informazioni sul tipo di risorsa della funzione Lambda, vedere. [AWS::Lambda::Function](#)

Nell'esempio, quando CloudFormation crea la risorsa AllSecurityGroups personalizzata, CloudFormation richiama la funzione LambdaAppendItemToListFunction. CloudFormation passa l'elenco dei gruppi di sicurezza esistenti e un nuovo gruppo di sicurezza (NewSecurityGroup) alla funzione, che aggiunge il nuovo gruppo di sicurezza all'elenco e quindi restituisce l'elenco modificato. CloudFormation utilizza l'elenco modificato per associare tutti i gruppi di sicurezza alla MyEC2Instance risorsa.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "ExistingSecurityGroups": {
      "Type": "List<AWS::EC2::SecurityGroup::Id>"
    },
    "ExistingVPC": {
      "Type": "AWS::EC2::VPC::Id",
      "Description": "The VPC ID that includes the security groups in the ExistingSecurityGroups parameter."
    },
    "InstanceType": {
      "Type": "String",
      "Default": "t2.micro",
      "AllowedValues": [
        "t2.micro",
        "m1.small"
      ]
    }
  },
}
```

```
"Mappings": {
  "AWSInstanceType2Arch": {
    "t2.micro": {
      "Arch": "HVM64"
    },
    "m1.small": {
      "Arch": "HVM64"
    }
  },
  "AWSRegionArch2AMI": {
    "us-east-1": {
      "HVM64": "ami-0ff8a91507f77f867",
      "HVMG2": "ami-0a584ac55a7631c0c"
    },
    "us-west-2": {
      "HVM64": "ami-a0cfeed8",
      "HVMG2": "ami-0e09505bc235aa82d"
    },
    "us-west-1": {
      "HVM64": "ami-0bdb828fd58c52235",
      "HVMG2": "ami-066ee5fd4a9ef77f1"
    },
    "eu-west-1": {
      "HVM64": "ami-047bb4163c506cd98",
      "HVMG2": "ami-0a7c483d527806435"
    },
    "eu-central-1": {
      "HVM64": "ami-0233214e13e500f77",
      "HVMG2": "ami-06223d46a6d0661c7"
    },
    "ap-northeast-1": {
      "HVM64": "ami-06cd52961ce9f0d85",
      "HVMG2": "ami-053cdd503598e4a9d"
    },
    "ap-southeast-1": {
      "HVM64": "ami-08569b978cc4dfa10",
      "HVMG2": "ami-0be9df32ae9f92309"
    },
    "ap-southeast-2": {
      "HVM64": "ami-09b42976632b27e9b",
      "HVMG2": "ami-0a9ce9fecc3d1daf8"
    },
    "sa-east-1": {
      "HVM64": "ami-07b14488da8ea02a0",
```

```

        "HVMG2": "NOT_SUPPORTED"
    },
    "cn-north-1": {
        "HVM64": "ami-0a4eaf6c4454eda75",
        "HVMG2": "NOT_SUPPORTED"
    }
}
},
"Resources": {
    "SecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Allow HTTP traffic to the host",
            "VpcId": {
                "Ref": "ExistingVPC"
            },
            "SecurityGroupIngress": [
                {
                    "IpProtocol": "tcp",
                    "FromPort": 80,
                    "ToPort": 80,
                    "CidrIp": "0.0.0.0/0"
                }
            ],
            "SecurityGroupEgress": [
                {
                    "IpProtocol": "tcp",
                    "FromPort": 80,
                    "ToPort": 80,
                    "CidrIp": "0.0.0.0/0"
                }
            ]
        }
    },
    "AllSecurityGroups": {
        "Type": "Custom::Split",
        "Properties": {
            "ServiceToken": {
                "Fn::GetAtt": [
                    "AppendItemToListFunction",
                    "Arn"
                ]
            },
            "List": {

```

```

        "Ref": "ExistingSecurityGroups"
    },
    "AppendedItem": {
        "Ref": "SecurityGroup"
    }
}
},
"AppendItemToListFunction": {
    "Type": "AWS::Lambda::Function",
    "Properties": {
        "Handler": "index.handler",
        "Role": {
            "Fn::GetAtt": [
                "LambdaExecutionRole",
                "Arn"
            ]
        },
        "Code": {
            "ZipFile": {
                "Fn::Join": [
                    "",
                    [
                        "var response = require('cfn-response');",
                        "exports.handler = function(event, context) {",
                        "    var responseData = {Value:",
event.ResourceProperties.List};",
                        "    ",
                        responseData.Value.push(event.ResourceProperties.AppendedItem);",
                        "    response.send(event, context, response.SUCCESS,",
responseData);",
                        "};"
                    ]
                ]
            }
        },
        "Runtime": "nodejs20.x"
    }
},
"MyEC2Instance": {
    "Type": "AWS::EC2::Instance",
    "Properties": {
        "ImageId": {
            "Fn::FindInMap": [
                "AWSRegionArch2AMI",

```

```

        {
            "Ref": "AWS::Region"
        },
        {
            "Fn::FindInMap": [
                "AWSInstanceType2Arch",
                {
                    "Ref": "InstanceType"
                },
                "Arch"
            ]
        }
    ],
    "SecurityGroupIds": {
        "Fn::GetAtt": [
            "AllSecurityGroups",
            "Value"
        ]
    },
    "InstanceType": {
        "Ref": "InstanceType"
    }
},
"LambdaExecutionRole": {
    "Type": "AWS::IAM::Role",
    "Properties": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": [
                            "lambda.amazonaws.com"
                        ]
                    },
                    "Action": [
                        "sts:AssumeRole"
                    ]
                }
            ]
        }
    }
},

```

```

        "Path": "/",
        "Policies": [
            {
                "PolicyName": "root",
                "PolicyDocument": {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Action": [
                                "logs:*"
                            ],
                            "Resource": "arn:aws:logs:*:*:*"
                        }
                    ]
                }
            }
        ],
        "Outputs": {
            "AllSecurityGroups": {
                "Description": "Security Groups that are associated with the EC2 instance",
                "Value": {
                    "Fn::Join": [
                        ",",
                        [
                            {
                                "Fn::GetAtt": [
                                    "AllSecurityGroups",
                                    "Value"
                                ]
                            }
                        ]
                    ]
                }
            }
        }
    }
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Parameters:

```

ExistingSecurityGroups:

Type: List<AWS::EC2::SecurityGroup::Id>

ExistingVPC:

Type: AWS::EC2::VPC::Id

Description: The VPC ID that includes the security groups in the ExistingSecurityGroups parameter.

InstanceType:

Type: String

Default: t2.micro

AllowedValues:

- t2.micro
- m1.small

Mappings:**AWSInstanceType2Arch:**

t2.micro:

Arch: HVM64

m1.small:

Arch: HVM64

AWSRegionArch2AMI:

us-east-1:

HVM64: ami-0ff8a91507f77f867

HVMG2: ami-0a584ac55a7631c0c

us-west-2:

HVM64: ami-a0cfeed8

HVMG2: ami-0e09505bc235aa82d

us-west-1:

HVM64: ami-0bdb828fd58c52235

HVMG2: ami-066ee5fd4a9ef77f1

eu-west-1:

HVM64: ami-047bb4163c506cd98

HVMG2: ami-0a7c483d527806435

eu-central-1:

HVM64: ami-0233214e13e500f77

HVMG2: ami-06223d46a6d0661c7

ap-northeast-1:

HVM64: ami-06cd52961ce9f0d85

HVMG2: ami-053cdd503598e4a9d

ap-southeast-1:

HVM64: ami-08569b978cc4dfa10

HVMG2: ami-0be9df32ae9f92309

ap-southeast-2:

HVM64: ami-09b42976632b27e9b

HVMG2: ami-0a9ce9fecc3d1daf8

sa-east-1:

```

    HVM64: ami-07b14488da8ea02a0
    HVMG2: NOT_SUPPORTED
  cn-north-1:
    HVM64: ami-0a4eaf6c4454eda75
    HVMG2: NOT_SUPPORTED
Resources:
  SecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Allow HTTP traffic to the host
      VpcId: !Ref ExistingVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0
      SecurityGroupEgress:
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0
  AllSecurityGroups:
    Type: Custom::Split
    Properties:
      ServiceToken: !GetAtt AppendItemToListFunction.Arn
      List: !Ref ExistingSecurityGroups
      AppendedItem: !Ref SecurityGroup
  AppendItemToListFunction:
    Type: AWS::Lambda::Function
    Properties:
      Handler: index.handler
      Role: !GetAtt LambdaExecutionRole.Arn
      Code:
        ZipFile: !Join
          - ''
          - - var response = require('cfn-response');
            - exports.handler = function(event, context) {
              - '  var responseData = {Value: event.ResourceProperties.List};'
              - '    responseData.Value.push(event.ResourceProperties.AppendedItem);'
              - '    response.send(event, context, response.SUCCESS, responseData);'
              - '};'
            - ''
      Runtime: nodejs20.x
  MyEC2Instance:
    Type: AWS::EC2::Instance

```



```

Properties:
  ImageId: !FindInMap
    - AWSRegionArch2AMI
    - !Ref AWS::Region
    - !FindInMap
      - AWSInstanceType2Arch
      - !Ref InstanceType
      - Arch
  SecurityGroupIds: !GetAtt AllSecurityGroups.Value
  InstanceType: !Ref InstanceType
LambdaExecutionRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - lambda.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
  Policies:
    - PolicyName: root
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - logs:*
            Resource: arn:aws:logs:*:*:*
Outputs:
  AllSecurityGroups:
    Description: Security Groups that are associated with the EC2 instance
    Value: !Join
      - ', '
      - !GetAtt AllSecurityGroups.Value

```

AWS OpsWorks frammenti di modello

AWS OpsWorks è un servizio di gestione delle applicazioni che semplifica un'ampia gamma di attività come la configurazione del software, la distribuzione delle applicazioni, la scalabilità e il monitoraggio.

CloudFormation è un servizio di gestione delle risorse che è possibile utilizzare per gestire AWS OpsWorks risorse, come AWS OpsWorks pile, livelli, app e istanze.

AWS OpsWorks app PHP di esempio

Il seguente modello di esempio distribuisce un'applicazione web AWS OpsWorks PHP di esempio archiviata in un repository Git pubblico. Lo AWS OpsWorks stack include due server di applicazioni con un sistema di bilanciamento del carico che distribuisce il traffico in entrata in modo uniforme tra i server. Lo AWS OpsWorks stack include anche un server di database MySQL back-end per archiviare i dati. Per ulteriori informazioni sull'applicazione AWS OpsWorks di esempio, consulta [Procedura guidata: nozioni di base su AWSAWS OpsWorks mediante la creazione di uno stack del server di applicazione](#) nella Guida per l'utente di AWS OpsWorks .

Note

Le `DefaultInstanceProfileArn` proprietà `ServiceRoleArn` and fanno riferimento ai ruoli IAM creati dopo il primo utilizzo AWS OpsWorks .

L'esempio definisce il parametro `MysqlRootPassword` con la proprietà `NoEcho` impostata su `true`. Se imposti l'`NoEcho` attributo su `true`, CloudFormation restituisce il valore del parametro mascherato da asterischi (`*****`) per tutte le chiamate che descrivono lo stack o gli eventi dello stack.

Important

Anziché incorporare informazioni sensibili direttamente nei CloudFormation modelli, consigliamo di utilizzare parametri dinamici nel modello dello stack per fare riferimento a informazioni sensibili archiviate e gestite all'esterno CloudFormation, ad esempio nel Parameter Store o. AWS Systems Manager AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "ServiceRole": {
      "Default": "aws-opsworks-service-role",
      "Description": "The OpsWorks service role",
```

```

    "Type": "String",
    "MinLength": "1",
    "MaxLength": "64",
    "AllowedPattern": "[a-zA-Z][a-zA-Z0-9]*",
    "ConstraintDescription": "must begin with a letter and contain only alphanumeric
characters."
  },
  "InstanceRole": {
    "Default": "aws-opsworks-ec2-role",
    "Description": "The OpsWorks instance role",
    "Type": "String",
    "MinLength": "1",
    "MaxLength": "64",
    "AllowedPattern": "[a-zA-Z][a-zA-Z0-9]*",
    "ConstraintDescription": "must begin with a letter and contain only alphanumeric
characters."
  },
  "AppName": {
    "Default": "myapp",
    "Description": "The app name",
    "Type": "String",
    "MinLength": "1",
    "MaxLength": "64",
    "AllowedPattern": "[a-zA-Z][a-zA-Z0-9]*",
    "ConstraintDescription": "must begin with a letter and contain only alphanumeric
characters."
  },
  "MysqlRootPassword" : {
    "Description" : "MysqlRootPassword",
    "NoEcho" : "true",
    "Type" : "String"
  }
},
"Resources": {
  "myStack": {
    "Type": "AWS::OpsWorks::Stack",
    "Properties": {
      "Name": {
        "Ref": "AWS::StackName"
      },
      "ServiceRoleArn": {
        "Fn::Join": [
          "", ["arn:aws:iam::", {"Ref": "AWS::AccountId"}],
          ":role/", {"Ref": "ServiceRole"}]
        ]
      }
    }
  }
}

```

```

    ]
  },
  "DefaultInstanceProfileArn": {
    "Fn::Join": [
      "", [
        "arn:aws:iam::", {"Ref": "AWS::AccountId"},
        ":instance-profile/", {"Ref": "InstanceRole"}
      ]
    ]
  },
  "UseCustomCookbooks": "true",
  "CustomCookbooksSource": {
    "Type": "git",
    "Url": "git://github.com/amazonwebservices/opsworks-example-cookbooks.git"
  }
},
"myLayer": {
  "Type": "AWS::OpsWorks::Layer",
  "DependsOn": "myApp",
  "Properties": {
    "StackId": {"Ref": "myStack"},
    "Type": "php-app",
  },
  "Shortname" : "php-app",
  "EnableAutoHealing" : "true",
  "AutoAssignElasticIps" : "false",
  "AutoAssignPublicIps" : "true",
  "Name": "MyPHPApp",
  "CustomRecipes" : {
    "Configure" : ["phpapp::appsetup"]
  }
},
"DBLayer" : {
  "Type" : "AWS::OpsWorks::Layer",
  "DependsOn": "myApp",
  "Properties" : {
    "StackId" : {"Ref": "myStack"},
    "Type" : "db-master",
  },
  "Shortname" : "db-layer",
  "EnableAutoHealing" : "true",
  "AutoAssignElasticIps" : "false",
  "AutoAssignPublicIps" : "true",
  "Name" : "MyMySQL",
  "CustomRecipes" : {
    "Setup" : ["phpapp::dbsetup"]
  }
}

```

```

    },
    "Attributes" : {
        "MysqlRootPassword" : {"Ref":"MysqlRootPassword"},
        "MysqlRootPasswordUbiquitous": "true"
    },
    "VolumeConfigurations":[{"MountPoint":"/vol/
mysql", "NumberOfDisks":1, "Size":10}]
    }
},
"ELBAttachment" : {
    "Type" : "AWS::OpsWorks::ElasticLoadBalancerAttachment",
    "Properties" : {
        "ElasticLoadBalancerName" : { "Ref" : "ELB" },
        "LayerId" : { "Ref" : "myLayer" }
    }
},
"ELB" : {
    "Type": "AWS::ElasticLoadBalancing::LoadBalancer",
    "Properties": {
        "AvailabilityZones": { "Fn::GetAZs" : "" } ,
        "Listeners": [{
            "LoadBalancerPort": "80",
            "InstancePort": "80",
            "Protocol": "HTTP",
            "InstanceProtocol": "HTTP"
        }],
        "HealthCheck": {
            "Target": "HTTP:80/",
            "HealthyThreshold": "2",
            "UnhealthyThreshold": "10",
            "Interval": "30",
            "Timeout": "5"
        }
    }
},
"myAppInstance1": {
    "Type": "AWS::OpsWorks::Instance",
    "Properties": {
        "StackId": {"Ref": "myStack"},
        "LayerIds": [{"Ref": "myLayer"}],
        "InstanceType": "m1.small"
    }
},
"myAppInstance2": {

```

```

    "Type": "AWS::OpsWorks::Instance",
    "Properties": {
      "StackId": {"Ref": "myStack"},
      "LayerIds": [{"Ref": "myLayer"}],
      "InstanceType": "m1.small"
    }
  },
  "myDBInstance": {
    "Type": "AWS::OpsWorks::Instance",
    "Properties": {
      "StackId": {"Ref": "myStack"},
      "LayerIds": [{"Ref": "DBLayer"}],
      "InstanceType": "m1.small"
    }
  },
  "myApp" : {
    "Type" : "AWS::OpsWorks::App",
    "Properties" : {
      "StackId" : {"Ref": "myStack"},
      "Type" : "php",
      "Name" : {"Ref": "AppName"},
      "AppSource" : {
        "Type" : "git",
        "Url" : "git://github.com/amazonwebservices/opsworks-demo-php-simple-
app.git",
        "Revision" : "version2"
      },
      "Attributes" : {
        "DocumentRoot" : "web"
      }
    }
  }
}

```

YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Parameters:
  ServiceRole:
    Default: aws-opsworks-service-role
    Description: The OpsWorks service role
    Type: String

```

```
    MinLength: '1'
    MaxLength: '64'
    AllowedPattern: "[a-zA-Z][a-zA-Z0-9-]*"
    ConstraintDescription: must begin with a letter and contain only alphanumeric
        characters.
InstanceRole:
    Default: aws-opsworks-ec2-role
    Description: The OpsWorks instance role
    Type: String
    MinLength: '1'
    MaxLength: '64'
    AllowedPattern: "[a-zA-Z][a-zA-Z0-9-]*"
    ConstraintDescription: must begin with a letter and contain only alphanumeric
        characters.
AppName:
    Default: myapp
    Description: The app name
    Type: String
    MinLength: '1'
    MaxLength: '64'
    AllowedPattern: "[a-zA-Z][a-zA-Z0-9-]*"
    ConstraintDescription: must begin with a letter and contain only alphanumeric
        characters.
MysqlRootPassword:
    Description: MysqlRootPassword
    NoEcho: 'true'
    Type: String
Resources:
    myStack:
        Type: AWS::OpsWorks::Stack
        Properties:
            Name:
                Ref: AWS::StackName
            ServiceRoleArn: !Sub "arn:aws:iam::${AWS::AccountId}:role/${ServiceRole}"
            DefaultInstanceProfileArn: !Sub "arn:aws:iam::${AWS::AccountId}:instance-profile/
                ${InstanceRole}"
            UseCustomCookbooks: 'true'
            CustomCookbooksSource:
                Type: git
                Url: git://github.com/amazonwebservices/opsworks-example-cookbooks.git
    myLayer:
        Type: AWS::OpsWorks::Layer
        DependsOn: myApp
        Properties:
```

```
StackId:
  Ref: myStack
Type: php-app
Shortname: php-app
EnableAutoHealing: 'true'
AutoAssignElasticIps: 'false'
AutoAssignPublicIps: 'true'
Name: MyPHPApp
CustomRecipes:
  Configure:
    - phpapp::appsetup
DBLayer:
  Type: AWS::OpsWorks::Layer
  DependsOn: myApp
  Properties:
    StackId:
      Ref: myStack
    Type: db-master
    Shortname: db-layer
    EnableAutoHealing: 'true'
    AutoAssignElasticIps: 'false'
    AutoAssignPublicIps: 'true'
    Name: MyMySQL
    CustomRecipes:
      Setup:
        - phpapp::dbsetup
    Attributes:
      MysqlRootPassword:
        Ref: MysqlRootPassword
      MysqlRootPasswordUbiquitous: 'true'
    VolumeConfigurations:
      - MountPoint: "/vol/mysql"
        NumberOfDisks: 1
        Size: 10
ELBAttachment:
  Type: AWS::OpsWorks::ElasticLoadBalancerAttachment
  Properties:
    ElasticLoadBalancerName:
      Ref: ELB
    LayerId:
      Ref: myLayer
ELB:
  Type: AWS::ElasticLoadBalancing::LoadBalancer
  Properties:
```



```
AvailabilityZones:
  Fn::GetAZs: ''
Listeners:
- LoadBalancerPort: '80'
  InstancePort: '80'
  Protocol: HTTP
  InstanceProtocol: HTTP
HealthCheck:
  Target: HTTP:80/
  HealthyThreshold: '2'
  UnhealthyThreshold: '10'
  Interval: '30'
  Timeout: '5'
myAppInstance1:
  Type: AWS::OpsWorks::Instance
  Properties:
    StackId:
      Ref: myStack
    LayerIds:
    - Ref: myLayer
    InstanceType: m1.small
myAppInstance2:
  Type: AWS::OpsWorks::Instance
  Properties:
    StackId:
      Ref: myStack
    LayerIds:
    - Ref: myLayer
    InstanceType: m1.small
myDBInstance:
  Type: AWS::OpsWorks::Instance
  Properties:
    StackId:
      Ref: myStack
    LayerIds:
    - Ref: DBLayer
    InstanceType: m1.small
myApp:
  Type: AWS::OpsWorks::App
  Properties:
    StackId:
      Ref: myStack
    Type: php
    Name:
```

```
    Ref: AppName
  AppSource:
    Type: git
    Url: git://github.com/amazonwebservices/opsworks-demo-php-simple-app.git
    Revision: version2
  Attributes:
    DocumentRoot: web
```

Frammenti di modello Amazon Redshift

Amazon Redshift è un servizio di data warehouse nel cloud in scala petabyte interamente gestito. Puoi utilizzare AWS CloudFormation per eseguire il provisioning dei cluster Amazon Redshift e gestirli.

Cluster Amazon Redshift

Il modello di esempio seguente crea un cluster Amazon Redshift in base ai valori dei parametri specificati durante la creazione dello stack. Il gruppo di parametri di cluster associato al cluster Amazon Redshift attiva la registrazione delle attività degli utenti. Il modello, inoltre, avvia i cluster Amazon Redshift in un Amazon VPC definito nel modello. Il VPC include un gateway Internet in modo che sia possibile accedere ai cluster Amazon Redshift da Internet. Tuttavia, è necessario anche abilitare la comunicazione tra il cluster e il gateway Internet, operazione che viene eseguita dalla voce della tabella di routing.

Note

Il modello include la condizione `IsMultiNodeCluster`, pertanto il parametro `NumberOfNodes` viene dichiarato solo quando il valore del parametro `ClusterType` è impostato su `multi-node`.

L'esempio definisce il parametro `MysqlRootPassword` con la proprietà `NoEcho` impostata su `true`. Se si imposta l'attributo `NoEcho` su `true`, CloudFormation restituisce il valore del parametro mascherato come asterischi (*****) per tutte le chiamate che descrivono lo stack o gli eventi stack, ad eccezione delle informazioni archiviate nelle posizioni specificate di seguito.

Important

L'utilizzo dell'attributo `NoEcho` non maschera le informazioni memorizzate nei seguenti elementi:

- La sezione dei Metadata modelli. CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per ulteriori informazioni, vedere [Metadati](#).
- Sezione dei modelli Outputs. Per ulteriori informazioni, consulta [Output](#).
- Attributo Metadata di una definizione di risorsa. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Si consiglia vivamente di non utilizzare questi meccanismi per includere informazioni sensibili, come password o segreti.

Important

Invece di incorporare informazioni riservate direttamente nei CloudFormation modelli, consigliamo di utilizzare parametri dinamici nel modello di pila per fare riferimento a informazioni sensibili archiviate e gestite all'esterno CloudFormation, ad esempio nel AWS Systems Manager Parameter Store o. AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters" : {
    "DatabaseName" : {
      "Description" : "The name of the first database to be created when the cluster is
created",
      "Type" : "String",
      "Default" : "dev",
      "AllowedPattern" : "([a-z]|[0-9])+"
    },
    "ClusterType" : {
      "Description" : "The type of cluster",
      "Type" : "String",
      "Default" : "single-node",
      "AllowedValues" : [ "single-node", "multi-node" ]
    },
    "NumberOfNodes" : {
```

```
"Description" : "The number of compute nodes in the cluster. For multi-node clusters, the NumberOfNodes parameter must be greater than 1",
    "Type" : "Number",
    "Default" : "1"
},
"NodeType" : {
    "Description" : "The type of node to be provisioned",
    "Type" : "String",
    "Default" : "ds2.xlarge",
    "AllowedValues" : [ "ds2.xlarge", "ds2.8xlarge", "dc1.large", "dc1.8xlarge" ]
},
"MasterUsername" : {
    "Description" : "The user name that is associated with the master user account for the cluster that is being created",
    "Type" : "String",
    "Default" : "defaultuser",
    "AllowedPattern" : "([a-z])([a-z]|[0-9])*"
},
"MasterUserPassword" : {
    "Description" : "The password that is associated with the master user account for the cluster that is being created.",
    "Type" : "String",
    "NoEcho" : "true"
},
"InboundTraffic" : {
    "Description" : "Allow inbound traffic to the cluster from this CIDR range.",
    "Type" : "String",
    "MinLength": "9",
    "MaxLength": "18",
    "Default" : "0.0.0.0/0",
    "AllowedPattern" : "(\\d{1,3})\\.\\.\\.\\.((\\d{1,3})\\.\\.\\.\\.((\\d{1,3})\\.\\.\\.\\.((\\d{1,3})\\.\\.\\.\\.((\\d{1,2})|)?)?)?)?)?",
    "ConstraintDescription" : "must be a valid CIDR range of the form x.x.x.x/x."
},
"PortNumber" : {
    "Description" : "The port number on which the cluster accepts incoming connections.",
    "Type" : "Number",
    "Default" : "5439"
}
},
"Conditions" : {
    "IsMultiNodeCluster" : {
        "Fn::Equals" : [{ "Ref" : "ClusterType" }, "multi-node"]
    }
}
```

```

    }
  },
  "Resources" : {
    "RedshiftCluster" : {
      "Type" : "AWS::Redshift::Cluster",
      "DependsOn" : "AttachGateway",
      "Properties" : {
        "ClusterType" : { "Ref" : "ClusterType" },
        "NumberOfNodes" : { "Fn::If" : [ "IsMultiNodeCluster", { "Ref" :
"NumberOfNodes" }, { "Ref" : "AWS::NoValue" } ]}],
        "NodeType" : { "Ref" : "NodeType" },
        "DBName" : { "Ref" : "DatabaseName" },
        "MasterUsername" : { "Ref" : "MasterUsername" },
        "MasterUserPassword" : { "Ref" : "MasterUserPassword" },
        "ClusterParameterGroupName" : { "Ref" : "RedshiftClusterParameterGroup" },
        "VpcSecurityGroupIds" : [ { "Ref" : "SecurityGroup" } ],
        "ClusterSubnetGroupName" : { "Ref" : "RedshiftClusterSubnetGroup" },
        "PubliclyAccessible" : "true",
        "Port" : { "Ref" : "PortNumber" }
      }
    },
    "RedshiftClusterParameterGroup" : {
      "Type" : "AWS::Redshift::ClusterParameterGroup",
      "Properties" : {
        "Description" : "Cluster parameter group",
        "ParameterGroupFamily" : "redshift-1.0",
        "Parameters" : [{
          "ParameterName" : "enable_user_activity_logging",
          "ParameterValue" : "true"
        }]
      }
    },
    "RedshiftClusterSubnetGroup" : {
      "Type" : "AWS::Redshift::ClusterSubnetGroup",
      "Properties" : {
        "Description" : "Cluster subnet group",
        "SubnetIds" : [ { "Ref" : "PublicSubnet" } ]
      }
    },
    "VPC" : {
      "Type" : "AWS::EC2::VPC",
      "Properties" : {
        "CidrBlock" : "10.0.0.0/16"
      }
    }
  }
}

```

```
},
"PublicSubnet" : {
  "Type" : "AWS::EC2::Subnet",
  "Properties" : {
    "CidrBlock" : "10.0.0.0/24",
    "VpcId" : { "Ref" : "VPC" }
  }
},
"SecurityGroup" : {
  "Type" : "AWS::EC2::SecurityGroup",
  "Properties" : {
    "GroupDescription" : "Security group",
    "SecurityGroupIngress" : [ {
      "CidrIp" : { "Ref": "InboundTraffic" },
      "FromPort" : { "Ref" : "PortNumber" },
      "ToPort" : { "Ref" : "PortNumber" },
      "IpProtocol" : "tcp"
    } ],
    "VpcId" : { "Ref" : "VPC" }
  }
},
"myInternetGateway" : {
  "Type" : "AWS::EC2::InternetGateway"
},
"AttachGateway" : {
  "Type" : "AWS::EC2::VPCGatewayAttachment",
  "Properties" : {
    "VpcId" : { "Ref" : "VPC" },
    "InternetGatewayId" : { "Ref" : "myInternetGateway" }
  }
},
"PublicRouteTable" : {
  "Type" : "AWS::EC2::RouteTable",
  "Properties" : {
    "VpcId" : {
      "Ref" : "VPC"
    }
  }
},
"PublicRoute" : {
  "Type" : "AWS::EC2::Route",
  "DependsOn" : "AttachGateway",
  "Properties" : {
    "RouteTableId" : {
```

```

        "Ref" : "PublicRouteTable"
    },
    "DestinationCidrBlock" : "0.0.0.0/0",
    "GatewayId" : {
        "Ref" : "myInternetGateway"
    }
}
},
"PublicSubnetRouteTableAssociation" : {
    "Type" : "AWS::EC2::SubnetRouteTableAssociation",
    "Properties" : {
        "SubnetId" : {
            "Ref" : "PublicSubnet"
        },
        "RouteTableId" : {
            "Ref" : "PublicRouteTable"
        }
    }
}
},
"Outputs" : {
    "ClusterEndpoint" : {
        "Description" : "Cluster endpoint",
        "Value" : { "Fn::Join" : [ ":", [ { "Fn::GetAtt" : [ "RedshiftCluster",
"Endpoint.Address" ] }, { "Fn::GetAtt" : [ "RedshiftCluster",
"Endpoint.Port" ] } ] ] }
    },
    "ClusterName" : {
        "Description" : "Name of cluster",
        "Value" : { "Ref" : "RedshiftCluster" }
    },
    "ParameterGroupName" : {
        "Description" : "Name of parameter group",
        "Value" : { "Ref" : "RedshiftClusterParameterGroup" }
    },
    "RedshiftClusterSubnetGroupName" : {
        "Description" : "Name of cluster subnet group",
        "Value" : { "Ref" : "RedshiftClusterSubnetGroup" }
    },
    "RedshiftClusterSecurityGroupName" : {
        "Description" : "Name of cluster security group",
        "Value" : { "Ref" : "SecurityGroup" }
    }
}
}

```

```
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Parameters:
  DatabaseName:
    Description: The name of the first database to be created when the cluster is
      created
    Type: String
    Default: dev
    AllowedPattern: "([a-z]|[0-9])+\"
  ClusterType:
    Description: The type of cluster
    Type: String
    Default: single-node
    AllowedValues:
      - single-node
      - multi-node
  NumberOfNodes:
    Description: The number of compute nodes in the cluster. For multi-node clusters,
      the NumberOfNodes parameter must be greater than 1
    Type: Number
    Default: '1'
  NodeType:
    Description: The type of node to be provisioned
    Type: String
    Default: ds2.xlarge
    AllowedValues:
      - ds2.xlarge
      - ds2.8xlarge
      - dc1.large
      - dc1.8xlarge
  MasterUsername:
    Description: The user name that is associated with the master user account for
      the cluster that is being created
    Type: String
    Default: defaultuser
    AllowedPattern: "([a-z])([a-z]|[0-9])*"
  MasterUserPassword:
    Description: The password that is associated with the master user account for
      the cluster that is being created.
    Type: String
```



```
NoEcho: 'true'
InboundTraffic:
    Description: Allow inbound traffic to the cluster from this CIDR range.
    Type: String
    MinLength: '9'
    MaxLength: '18'
    Default: 0.0.0.0/0
    AllowedPattern: "(\\d{1,3})\\.((\\d{1,3})\\.((\\d{1,3})\\.((\\d{1,3})/(\\d{1,2})))"
    ConstraintDescription: must be a valid CIDR range of the form x.x.x.x/x.
PortNumber:
    Description: The port number on which the cluster accepts incoming connections.
    Type: Number
    Default: '5439'
Conditions:
    IsMultiNodeCluster:
        Fn::Equals:
            - Ref: ClusterType
            - multi-node
Resources:
    RedshiftCluster:
        Type: AWS::Redshift::Cluster
        DependsOn: AttachGateway
        Properties:
            ClusterType:
                Ref: ClusterType
            NumberOfNodes:
                Fn::If:
                    - IsMultiNodeCluster
                    - Ref: NumberOfNodes
                    - Ref: AWS::NoValue
            NodeType:
                Ref: NodeType
            DBName:
                Ref: DatabaseName
            MasterUsername:
                Ref: MasterUsername
            MasterUserPassword:
                Ref: MasterUserPassword
            ClusterParameterGroupName:
                Ref: RedshiftClusterParameterGroup
            VpcSecurityGroupIds:
                - Ref: SecurityGroup
            ClusterSubnetGroupName:
                Ref: RedshiftClusterSubnetGroup
```

```
    PubliclyAccessible: 'true'
    Port:
      Ref: PortNumber
  RedshiftClusterParameterGroup:
    Type: AWS::Redshift::ClusterParameterGroup
    Properties:
      Description: Cluster parameter group
      ParameterGroupFamily: redshift-1.0
      Parameters:
        - ParameterName: enable_user_activity_logging
          ParameterValue: 'true'
  RedshiftClusterSubnetGroup:
    Type: AWS::Redshift::ClusterSubnetGroup
    Properties:
      Description: Cluster subnet group
      SubnetIds:
        - Ref: PublicSubnet
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
  PublicSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: 10.0.0.0/24
      VpcId:
        Ref: VPC
  SecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security group
      SecurityGroupIngress:
        - CidrIp:
            Ref: InboundTraffic
          FromPort:
            Ref: PortNumber
          ToPort:
            Ref: PortNumber
          IpProtocol: tcp
      VpcId:
        Ref: VPC
  myInternetGateway:
    Type: AWS::EC2::InternetGateway
  AttachGateway:
```

```
Type: AWS::EC2::VPCGatewayAttachment
Properties:
  VpcId:
    Ref: VPC
  InternetGatewayId:
    Ref: myInternetGateway
PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId:
      Ref: VPC
PublicRoute:
  Type: AWS::EC2::Route
  DependsOn: AttachGateway
  Properties:
    RouteTableId:
      Ref: PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId:
      Ref: myInternetGateway
PublicSubnetRouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    SubnetId:
      Ref: PublicSubnet
    RouteTableId:
      Ref: PublicRouteTable
Outputs:
  ClusterEndpoint:
    Description: Cluster endpoint
    Value: !Sub "${RedshiftCluster.Endpoint.Address}:${RedshiftCluster.Endpoint.Port}"
  ClusterName:
    Description: Name of cluster
    Value:
      Ref: RedshiftCluster
  ParameterGroupName:
    Description: Name of parameter group
    Value:
      Ref: RedshiftClusterParameterGroup
  RedshiftClusterSubnetGroupName:
    Description: Name of cluster subnet group
    Value:
      Ref: RedshiftClusterSubnetGroup
  RedshiftClusterSecurityGroupName:
```

```
Description: Name of cluster security group
Value:
  Ref: SecurityGroup
```

Consulta anche

[AWS::Redshift::Cluster](#)

Frammenti di modello Amazon RDS

Argomenti

- [Risorsa di un'istanza database Amazon RDS](#)
- [Risorsa di un'istanza database \(DB\) Oracle Database Amazon RDS](#)
- [Risorsa del DBSecurity gruppo Amazon RDS per la gamma CIDR](#)
- [Gruppo Amazon RDS con un DBSecurity gruppo di EC2 sicurezza Amazon](#)
- [Gruppi di sicurezza VPC multipli](#)
- [Istanza database Amazon RDS in un gruppo di sicurezza VPC](#)

Risorsa di un'istanza database Amazon RDS

In questo esempio viene visualizzata una risorsa dell'istanza database Amazon RDS con password utente principale gestita. Per ulteriori informazioni, consulta [Gestione delle password con Amazon RDS e AWS Secrets Manager](#) nella Guida per l'utente di Amazon RDS e [Gestione delle password con Amazon Aurora e AWS Secrets Manager](#) nella Guida per l'utente di Amazon Aurora. Poiché la EngineVersion proprietà opzionale non è specificata, per questa istanza database viene utilizzata la versione del motore predefinita. Per dettagli sulla versione predefinita del motore e altre impostazioni predefinite, consulta [Create DBInstance](#). La DBSecurityGroups proprietà autorizza l'accesso alla rete alle AWS::RDS::DBSecurityGroup risorse MyDbSecurityByEC2SecurityGroup denominate and. MyDbSecurityBy CIDRIPGroup Per informazioni dettagliate, consultare [AWS::RDS::DBInstance](#). La risorsa DB Instance ha anche un DeletionPolicy attributo impostato su. Snapshot Con il Snapshot DeletionPolicy set, AWS CloudFormation scatterà un'istantanea di questa istanza DB prima di eliminarla durante l'eliminazione dello stack.

JSON

```
"MyDB" : {
```

```

"Type" : "AWS::RDS::DBInstance",
"Properties" : {
  "DBSecurityGroups" : [
    {"Ref" : "MyDbSecurityByEC2SecurityGroup"}, {"Ref" :
"MyDbSecurityByCIDRIPGroup"} ],
  "AllocatedStorage" : "5",
  "DBInstanceClass" : "db.t2.small",
  "Engine" : "MySQL",
  "MasterUsername" : "MyName",
  "ManageMasterUserPassword" : true,
  "MasterUserSecret" : {
    "KmsKeyId" : {"Ref" : "KMSKey"}
  }
},
"DeletionPolicy" : "Snapshot"
}

```

YAML

```

MyDB:
  Type: AWS::RDS::DBInstance
  Properties:
    DBSecurityGroups:
      - Ref: MyDbSecurityByEC2SecurityGroup
      - Ref: MyDbSecurityByCIDRIPGroup
    AllocatedStorage: '5'
    DBInstanceClass: db.t2.small
    Engine: MySQL
    MasterUsername: MyName
    ManageMasterUserPassword: true
    MasterUserSecret:
      KmsKeyId: !Ref KMSKey
    DeletionPolicy: Snapshot

```

Risorsa di un'istanza database (DB) Oracle Database Amazon RDS

In questo esempio viene creata una risorsa dell'istanza database Oracle Database con password utente principale gestita. Per ulteriori informazioni, consulta la sezione [Gestione delle password con Amazon AWS Secrets Manager](#) nella Guida per l'utente di Amazon RDS. L'esempio specifica l'Engineas oracle-ee con un modello di licenza di. bring-your-own-license [Per i dettagli sulle impostazioni per le istanze di Oracle Database DB, vedere Create. DBInstance](#) La proprietà DBSecurity Groups autorizza l'accesso alla rete alle AWS::RDS::DBSecurityGroup risorse

denominate and. MyDbSecurityBy EC2 SecurityGroup MyDbSecurityBy CIDRIPGroup Per informazioni dettagliate, consultare [AWS::RDS::DBInstance](#). La risorsa DB Instance ha anche un DeletionPolicy attributo impostato su. Snapshot Con il Snapshot DeletionPolicy set, AWS CloudFormation scatterà un'istantanea di questa istanza DB prima di eliminarla durante l'eliminazione dello stack.

JSON

```
"MyDB" : {
  "Type" : "AWS::RDS::DBInstance",
  "Properties" : {
    "DBSecurityGroups" : [
      {"Ref" : "MyDbSecurityByEC2SecurityGroup"}, {"Ref" :
"MyDbSecurityByCIDRIPGroup"} ],
    "AllocatedStorage" : "5",
    "DBInstanceClass" : "db.t2.small",
    "Engine" : "oracle-ee",
    "LicenseModel" : "bring-your-own-license",
    "MasterUsername" : "master",
    "ManageMasterUserPassword" : true,
    "MasterUserSecret" : {
      "KmsKeyId" : {"Ref" : "KMSKey"}
    }
  },
  "DeletionPolicy" : "Snapshot"
}
```

YAML

```
MyDB:
  Type: AWS::RDS::DBInstance
  Properties:
    DBSecurityGroups:
      - Ref: MyDbSecurityByEC2SecurityGroup
      - Ref: MyDbSecurityByCIDRIPGroup
    AllocatedStorage: '5'
    DBInstanceClass: db.t2.small
    Engine: oracle-ee
    LicenseModel: bring-your-own-license
    MasterUsername: master
    ManageMasterUserPassword: true
    MasterUserSecret:
```

```
KmsKeyId: !Ref KMSKey
DeletionPolicy: Snapshot
```

Risorsa del DBSecurity gruppo Amazon RDS per la gamma CIDR

Questo esempio mostra una DBSecurityGroup risorsa Amazon RDS con autorizzazione all'ingresso per l'intervallo CIDR specificato nel formato. ddd.ddd.ddd.ddd/dd [Per i dettagli, consulta AWS: :RDS:: DBSecurity Group and Ingress.](#)

JSON

```
"MyDbSecurityByCIDRIPGroup" : {
  "Type" : "AWS::RDS::DBSecurityGroup",
  "Properties" : {
    "GroupDescription" : "Ingress for CIDRIP",
    "DBSecurityGroupIngress" : {
      "CIDRIP" : "192.168.0.0/32"
    }
  }
}
```

YAML

```
MyDbSecurityByCIDRIPGroup:
  Type: AWS::RDS::DBSecurityGroup
  Properties:
    GroupDescription: Ingress for CIDRIP
    DBSecurityGroupIngress:
      CIDRIP: "192.168.0.0/32"
```

Gruppo Amazon RDS con un DBSecurity gruppo di EC2 sicurezza Amazon

Questo esempio mostra una risorsa [AWS: :RDS:: DBSecurity Group](#) con autorizzazione all'ingresso da un gruppo di EC2 sicurezza Amazon a cui fa riferimento. MyEc2SecurityGroup

Per fare ciò, definisci un gruppo di EC2 sicurezza e poi usi la Ref funzione intrinseca per fare riferimento al gruppo di sicurezza all'interno del tuo. EC2 DBSecurityGroup

JSON

```
"DBInstance" : {
```

```

    "Type": "AWS::RDS::DBInstance",
    "Properties": {
      "DBName"          : { "Ref" : "DBName" },
      "Engine"          : "MySQL",
      "MasterUsername"  : { "Ref" : "DBUsername" },
      "DBInstanceClass" : { "Ref" : "DBClass" },
      "DBSecurityGroups" : [ { "Ref" : "DBSecurityGroup" } ],
      "AllocatedStorage" : { "Ref" : "DBAllocatedStorage" },
      "MasterUserPassword": { "Ref" : "DBPassword" }
    }
  },

  "DBSecurityGroup": {
    "Type": "AWS::RDS::DBSecurityGroup",
    "Properties": {
      "DBSecurityGroupIngress": {
        "EC2SecurityGroupName": {
          "Fn::GetAtt": ["WebServerSecurityGroup", "GroupName"]
        }
      },
      "GroupDescription" : "Frontend Access"
    }
  },

  "WebServerSecurityGroup" : {
    "Type" : "AWS::EC2::SecurityGroup",
    "Properties" : {
      "GroupDescription" : "Enable HTTP access via port 80 and SSH access",
      "SecurityGroupIngress" : [
        { "IpProtocol" : "tcp", "FromPort" : 80, "ToPort" : 80, "CidrIp" :
"0.0.0.0/0"},
        { "IpProtocol" : "tcp", "FromPort" : 22, "ToPort" : 22, "CidrIp" : "0.0.0.0/0"}
      ]
    }
  }
}

```

YAML

Questo esempio è estratto dal seguente esempio completo:

[Drupal_Single_Instance_With_RDS.template](#)

```

DBInstance:
  Type: AWS::RDS::DBInstance

```



```

Properties:
  DBName:
    Ref: DBName
  Engine: MySQL
  MasterUsername:
    Ref: DBUsername
  DBInstanceClass:
    Ref: DBClass
  DBSecurityGroups:
    - Ref: DBSecurityGroup
  AllocatedStorage:
    Ref: DBAllocatedStorage
  MasterUserPassword:
    Ref: DBPassword
DBSecurityGroup:
  Type: AWS::RDS::DBSecurityGroup
  Properties:
    DBSecurityGroupIngress:
      EC2SecurityGroupName:
        Ref: WebServerSecurityGroup
      GroupDescription: Frontend Access
WebServerSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Enable HTTP access via port 80 and SSH access
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        CidrIp: 0.0.0.0/0
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: 0.0.0.0/0

```

Gruppi di sicurezza VPC multipli

Questo esempio mostra una risorsa [AWS::RDS::DBSecurity Group](#) con autorizzazione all'ingresso per più gruppi di EC2 sicurezza Amazon VPC in [AWS::RDS::DBSecurity GroupIngress](#)

JSON

```
{
```

```

"Resources" : {
  "DBInstance" : {
    "Type" : "AWS::RDS::DBInstance",
    "Properties" : {
      "AllocatedStorage" : "5",
      "DBInstanceClass" : "db.t2.small",
      "DBName" : { "Ref" : "MyDBName" },
      "DBSecurityGroups" : [ { "Ref" : "DbSecurityByEC2SecurityGroup" } ],
      "DBSubnetGroupName" : { "Ref" : "MyDBSubnetGroup" },
      "Engine" : "MySQL",
      "MasterUserPassword": { "Ref" : "MyDBPassword" },
      "MasterUsername" : { "Ref" : "MyDBUsername" }
    },
    "DeletionPolicy" : "Snapshot"
  },
  "DbSecurityByEC2SecurityGroup" : {
    "Type" : "AWS::RDS::DBSecurityGroup",
    "Properties" : {
      "GroupDescription" : "Ingress for Amazon EC2 security group",
      "EC2VpcId" : { "Ref" : "MyVPC" },
      "DBSecurityGroupIngress" : [ {
        "EC2SecurityGroupId" : "sg-b0ff1111",
        "EC2SecurityGroupOwnerId" : "111122223333"
      }, {
        "EC2SecurityGroupId" : "sg-ffd72222",
        "EC2SecurityGroupOwnerId" : "111122223333"
      } ]
    }
  }
}

```

YAML

```

Resources:
  DBInstance:
    Type: AWS::RDS::DBInstance
    Properties:
      AllocatedStorage: '5'
      DBInstanceClass: db.t2.small
      DBName:
        Ref: MyDBName
      DBSecurityGroups:

```

```

- Ref: DbSecurityByEC2SecurityGroup
DBSubnetGroupName:
  Ref: MyDBSubnetGroup
Engine: MySQL
MasterUserPassword:
  Ref: MyDBPassword
MasterUsername:
  Ref: MyDBUsername
DeletionPolicy: Snapshot
DbSecurityByEC2SecurityGroup:
  Type: AWS::RDS::DBSecurityGroup
  Properties:
    GroupDescription: Ingress for Amazon EC2 security group
    EC2VpcId:
      Ref: MyVPC
    DBSecurityGroupIngress:
      - EC2SecurityGroupId: sg-b0ff1111
        EC2SecurityGroupOwnerId: '111122223333'
      - EC2SecurityGroupId: sg-ffd72222
        EC2SecurityGroupOwnerId: '111122223333'

```

Istanza database Amazon RDS in un gruppo di sicurezza VPC

Questo esempio mostra un'istanza di database Amazon RDS associata a un gruppo di sicurezza Amazon EC2 VPC.

JSON

```

{
  "DBEC2SecurityGroup": {
    "Type": "AWS::EC2::SecurityGroup",
    "Properties" : {
      "GroupDescription": "Open database for access",
      "SecurityGroupIngress" : [{
        "IpProtocol" : "tcp",
        "FromPort" : 3306,
        "ToPort" : 3306,
        "SourceSecurityGroupName" : { "Ref" : "WebServerSecurityGroup" }
      }]
    }
  },
  "DBInstance" : {
    "Type": "AWS::RDS::DBInstance",

```

```

    "Properties": {
      "DBName"           : { "Ref" : "DBName" },
      "Engine"           : "MySQL",
      "MultiAZ"          : { "Ref": "MultiAZDatabase" },
      "MasterUsername"   : { "Ref" : "DBUser" },
      "DBInstanceClass"  : { "Ref" : "DBClass" },
      "AllocatedStorage" : { "Ref" : "DBAllocatedStorage" },
      "MasterUserPassword": { "Ref" : "DBPassword" },
      "VPCSecurityGroups" : [ { "Fn::GetAtt": [ "DBEC2SecurityGroup", "GroupId" ] } ]
    }
  }
}

```

YAML

```

DBEC2SecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Open database for access
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 3306
        ToPort: 3306
        SourceSecurityGroupName:
          Ref: WebServerSecurityGroup
DBInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName:
      Ref: DBName
    Engine: MySQL
    MultiAZ:
      Ref: MultiAZDatabase
    MasterUsername:
      Ref: DBUser
    DBInstanceClass:
      Ref: DBClass
    AllocatedStorage:
      Ref: DBAllocatedStorage
    MasterUserPassword:
      Ref: DBPassword
    VPCSecurityGroups:
      - !GetAtt DBEC2SecurityGroup.GroupId

```

Frammenti di modello Route 53

Argomenti

- [Set di record della risorsa Amazon Route 53 che utilizza il nome o l'ID della zona ospitata](#)
- [Utilizzo RecordSetGroup per impostare set di record di risorse ponderati](#)
- [Utilizzo RecordSetGroup per impostare un set di record di risorse alias](#)
- [Alias: record di risorse impostato per una distribuzione CloudFront](#)

Set di record della risorsa Amazon Route 53 che utilizza il nome o l'ID della zona ospitata

Quando crei un set di record di risorse Amazon Route 53, devi specificare la zona ospitata in cui desideri aggiungerlo. CloudFormation fornisce due modi per specificare una zona ospitata:

- Puoi specificare esplicitamente la zona ospitata utilizzando la proprietà `HostedZoneId`.
- È possibile CloudFormation trovare la zona ospitata utilizzando la `HostedZoneName` proprietà. Se si utilizza la `HostedZoneName` proprietà e sono presenti più zone ospitate con lo stesso nome, CloudFormation non crea lo stack.

Aggiungere utilizzando RecordSet HostedZoneId

Questo esempio aggiunge un set di record di risorse Amazon Route 53 contenente un SPF record per il nome di dominio `mysite.example.com` che utilizza la `HostedZoneId` proprietà per specificare la zona ospitata.

JSON

```
"myDNSRecord" : {
  "Type" : "AWS::Route53::RecordSet",
  "Properties" :
  {
    "HostedZoneId" : "Z3DG6IL3SJCGPX",
    "Name" : "mysite.example.com.",
    "Type" : "SPF",
    "TTL" : "900",
    "ResourceRecords" : [ "\"v=spf1 ip4:192.168.0.1/16 -all\"" ]
  }
}
```

YAML

```
myDNSRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: Z3DG6IL3SJCGPX
    Name: mysite.example.com.
    Type: SPF
    TTL: '900'
    ResourceRecords:
      - '"v=spf1 ip4:192.168.0.1/16 -all"'
```

Aggiungere RecordSet utilizzando HostedZoneName

In questo esempio viene aggiunto un set di record della risorsa Amazon Route 53 per il nome di dominio "mysite.example.com" utilizzando la proprietà HostedZoneName per specificare la zona ospitata.

JSON

```
"myDNSRecord2" : {
  "Type" : "AWS::Route53::RecordSet",
  "Properties" : {
    "HostedZoneName" : "example.com.",
    "Name" : "mysite.example.com.",
    "Type" : "A",
    "TTL" : "900",
    "ResourceRecords" : [
      "192.168.0.1",
      "192.168.0.2"
    ]
  }
}
```

YAML

```
myDNSRecord2:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneName: example.com.
    Name: mysite.example.com.
    Type: A
```

```
TTL: '900'  
ResourceRecords:  
- 192.168.0.1  
- 192.168.0.2
```

Utilizzo RecordSetGroup per impostare set di record di risorse ponderati

Questo esempio utilizza un [AWS::Route53::RecordSetgruppo](#) per impostare due record CNAME per «example.com». zona ospitata. La proprietà RecordSets contiene il set di record CNAME per il nome DNS "mysite.example.com". Ogni set di record contiene un identificatore (SetIdentifier) e un peso (Weight). La proporzione di traffico Internet instradato alle risorse si basa sui seguenti calcoli:

- Frontend One: $140 / (140 + 60) = 140 / 200 = 70\%$
- Frontend Two: $60 / (140 + 60) = 60 / 200 = 30\%$

Per ulteriori informazioni sui set di record di risorse ponderati, consulta [Instradamento ponderato](#) nella Guida per lo sviluppatore di Amazon Route 53.

JSON

```
"myDNSOne" : {  
  "Type" : "AWS::Route53::RecordSetGroup",  
  "Properties" : {  
    "HostedZoneName" : "example.com.",  
    "Comment" : "Weighted RR for my frontends.",  
    "RecordSets" : [  
      {  
        "Name" : "mysite.example.com.",  
        "Type" : "CNAME",  
        "TTL" : "900",  
        "SetIdentifier" : "Frontend One",  
        "Weight" : "140",  
        "ResourceRecords" : ["example-ec2.amazonaws.com"]  
      },  
      {  
        "Name" : "mysite.example.com.",  
        "Type" : "CNAME",  
        "TTL" : "900",  
        "SetIdentifier" : "Frontend Two",  
        "Weight" : "60",
```

```

        "ResourceRecords" : ["example-ec2-larger.amazonaws.com"]
    }
]
}
}

```

YAML

```

myDNSOne:
  Type: AWS::Route53::RecordSetGroup
  Properties:
    HostedZoneName: example.com.
    Comment: Weighted RR for my frontends.
    RecordSets:
      - Name: mysite.example.com.
        Type: CNAME
        TTL: '900'
        SetIdentifier: Frontend One
        Weight: '140'
        ResourceRecords:
          - example-ec2.amazonaws.com
      - Name: mysite.example.com.
        Type: CNAME
        TTL: '900'
        SetIdentifier: Frontend Two
        Weight: '60'
        ResourceRecords:
          - example-ec2-larger.amazonaws.com

```

Utilizzo RecordSetGroup per impostare un set di record di risorse alias

Negli esempi seguenti viene utilizzato un [AWS::Route53::RecordSetgruppo](#) per impostare un set di record di risorse alias denominato `example.com` che indirizza il traffico verso un sistema di bilanciamento del carico ELB versione 1 (classico) e un sistema di bilanciamento del carico versione 2 (applicazione o rete). La [AliasTarget](#) proprietà specifica l'ID e il nome DNS della zona ospitata utilizzando la `myELB LoadBalancer` funzione intrinseca. `GetAtt` `GetAtt` recupera diverse proprietà della `myELB` risorsa, a seconda che si stia indirizzando il traffico verso un sistema di bilanciamento del carico della versione 1 o della versione 2:

- load balancer Versione 1: `CanonicalHostedZoneNameID` e `DNSName`
- load balancer Versione 2: `CanonicalHostedZoneID` e `DNSName`

Per ulteriori informazioni sui set di record di risorse alias, consulta [Scelta tra record alias e non alias](#) nella Guida per gli sviluppatori di Route 53.

JSON per il load balancer Versione 1

```

"myELB" : {
  "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
  "Properties" : {
    "AvailabilityZones" : [ "us-east-1a" ],
    "Listeners" : [ {
      "LoadBalancerPort" : "80",
      "InstancePort" : "80",
      "Protocol" : "HTTP"
    } ]
  }
},
"myDNS" : {
  "Type" : "AWS::Route53::RecordSetGroup",
  "Properties" : {
    "HostedZoneName" : "example.com.",
    "Comment" : "Zone apex alias targeted to myELB LoadBalancer.",
    "RecordSets" : [
      {
        "Name" : "example.com.",
        "Type" : "A",
        "AliasTarget" : {
          "HostedZoneId" : { "Fn::GetAtt" : ["myELB",
"CanonicalHostedZoneNameID"] },
          "DNSName" : { "Fn::GetAtt" : ["myELB","DNSName"] }
        }
      }
    ]
  }
}

```

YAML per il load balancer Versione 1

```

myELB:
  Type: AWS::ElasticLoadBalancing::LoadBalancer
  Properties:
    AvailabilityZones:
      - "us-east-1a"
    Listeners:

```

```

- LoadBalancerPort: '80'
  InstancePort: '80'
  Protocol: HTTP
myDNS:
  Type: AWS::Route53::RecordSetGroup
  Properties:
    HostedZoneName: example.com.
    Comment: Zone apex alias targeted to myELB LoadBalancer.
  RecordSets:
    - Name: example.com.
      Type: A
      AliasTarget:
        HostedZoneId: !GetAtt 'myELB.CanonicalHostedZoneNameID'
        DNSName: !GetAtt 'myELB.DNSName'

```

JSON per il load balancer Versione 2

```

"myELB" : {
  "Type" : "AWS::ElasticLoadBalancing::LoadBalancer",
  "Properties" : {
    "Subnets" : [
      {"Ref": "SubnetAZ1"},
      {"Ref" : "SubnetAZ2"}
    ]
  }
},
"myDNS" : {
  "Type" : "AWS::Route53::RecordSetGroup",
  "Properties" : {
    "HostedZoneName" : "example.com.",
    "Comment" : "Zone apex alias targeted to myELB LoadBalancer.",
    "RecordSets" : [
      {
        "Name" : "example.com.",
        "Type" : "A",
        "AliasTarget" : {
          "HostedZoneId" : { "Fn::GetAtt" : ["myELB",
"CanonicalHostedZoneID"] },
          "DNSName" : { "Fn::GetAtt" : ["myELB","DNSName"] }
        }
      }
    ]
  }
}

```

```
}
```

YAML per il load balancer Versione 2

```
myELB:
  Type: AWS::ElasticLoadBalancingV2::LoadBalancer
  Properties:
    Subnets:
      - Ref: SubnetAZ1
      - Ref: SubnetAZ2
myDNS:
  Type: AWS::Route53::RecordSetGroup
  Properties:
    HostedZoneName: example.com.
    Comment: Zone apex alias targeted to myELB LoadBalancer.
    RecordSets:
      - Name: example.com.
        Type: A
        AliasTarget:
          HostedZoneId: !GetAtt 'myELB.CanonicalHostedZoneID'
          DNSName: !GetAtt 'myELB.DNSName'
```

Alias: record di risorse impostato per una distribuzione CloudFront

L'esempio seguente crea un record di alias A che indirizza un nome di dominio personalizzato a una distribuzione esistente CloudFront. `myHostedZoneID` si presume che sia un riferimento a una `AWS::Route53::HostedZone` risorsa effettiva nello stesso modello o un parametro. `myCloudFrontDistributions` si riferisce a una `AWS::CloudFront::Distribution` risorsa all'interno dello stesso modello. Il record di alias utilizza lo standard CloudFront hosted zone ID (`Z2FDTNDATAQYW2`) e risolve automaticamente il nome di dominio della distribuzione utilizzando `Fn::GetAtt`. Questa configurazione consente di instradare il traffico web dal dominio personalizzato alla CloudFront distribuzione senza richiedere un indirizzo IP.

Note

Quando si creano set di record di risorse alias, è necessario specificare `Z2FDTNDATAQYW2` la `HostedZoneId` proprietà. I set di record di risorse alias per non CloudFront possono essere creati in un'area privata.

JSON

```
{
  "myDNS": {
    "Type": "AWS::Route53::RecordSetGroup",
    "Properties": {
      "HostedZoneId": {
        "Ref": "myHostedZoneID"
      },
      "RecordSets": [
        {
          "Name": {
            "Ref": "myRecordSetDomainName"
          },
          "Type": "A",
          "AliasTarget": {
            "HostedZoneId": "Z2FDTNDATAQYW2",
            "DNSName": {
              "Fn::GetAtt": [
                "myCloudFrontDistribution",
                "DomainName"
              ]
            },
            "EvaluateTargetHealth": false
          }
        }
      ]
    }
  }
}
```

YAML

```
myDNS:
  Type: AWS::Route53::RecordSetGroup
  Properties:
    HostedZoneId: !Ref myHostedZoneID
    RecordSets:
      - Name: !Ref myRecordSetDomainName
        Type: A
        AliasTarget:
          HostedZoneId: Z2FDTNDATAQYW2
          DNSName: !GetAtt
```

```
- myCloudFrontDistribution
- DomainName
EvaluateTargetHealth: false
```

Frammenti di modello Amazon S3

Usa questi modelli di esempio di Amazon S3 per descrivere i tuoi bucket Amazon S3 con CloudFormation. Per altri esempi, consulta la sezione [Esempi](#) nella risorsa `AWS::S3::Bucket`.

Argomenti

- [Creazione di un bucket Amazon S3 con impostazioni predefinite](#)
- [Creazione di un bucket Amazon S3 per l'hosting di siti Web con DeletionPolicy](#)
- [Creazione di un sito Web statico utilizzando un dominio personalizzato](#)

Creazione di un bucket Amazon S3 con impostazioni predefinite

Questo esempio utilizza `AWS::S3::Bucket` per creare un bucket con impostazioni predefinite.

JSON

```
"myS3Bucket" : {
  "Type" : "AWS::S3::Bucket"
}
```

YAML

```
MyS3Bucket:
  Type: AWS::S3::Bucket
```

Creazione di un bucket Amazon S3 per l'hosting di siti Web con **DeletionPolicy**

Questo esempio crea un bucket come sito Web e disabilita Block Public Access (le autorizzazioni di lettura pubbliche sono necessarie per i bucket configurati per l'hosting di siti Web). Al bucket viene quindi aggiunta una policy pubblica per i bucket. Poiché questa risorsa bucket ha un `DeletionPolicy` attributo impostato su `Retain`, non CloudFormation eliminerà questo bucket quando elimina lo stack. La Output sezione utilizza `Fn::GetAtt` per recuperare l'`WebsiteURL` attributo e `DomainName` l'attributo della risorsa `S3Bucket`.

Note

Gli esempi seguenti presuppongono che le impostazioni BlockPublicPolicy e RestrictPublicBuckets Block Public Access siano state disabilitate a livello di account.

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "S3Bucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {
        "PublicAccessBlockConfiguration": {
          "BlockPublicAcls": false,
          "BlockPublicPolicy": false,
          "IgnorePublicAcls": false,
          "RestrictPublicBuckets": false
        },
        "WebsiteConfiguration": {
          "IndexDocument": "index.html",
          "ErrorDocument": "error.html"
        }
      },
      "DeletionPolicy": "Retain",
      "UpdateReplacePolicy": "Retain"
    },
    "BucketPolicy": {
      "Type": "AWS::S3::BucketPolicy",
      "Properties": {
        "PolicyDocument": {
          "Id": "MyPolicy",
          "Version": "2012-10-17",
          "Statement": [
            {
              "Sid": "PublicReadForGetBucketObjects",
              "Effect": "Allow",
              "Principal": "*",
              "Action": "s3:GetObject",
              "Resource": {
                "Fn::Join": [
                  "",
```

```

        [
            "arn:aws:s3:::",
            {
                "Ref": "S3Bucket"
            },
            "/*"
        ]
    ],
    "Bucket": {
        "Ref": "S3Bucket"
    }
},
"Outputs": {
    "WebsiteURL": {
        "Value": {
            "Fn::GetAtt": [
                "S3Bucket",
                "WebsiteURL"
            ]
        },
        "Description": "URL for website hosted on S3"
    },
    "S3BucketSecureURL": {
        "Value": {
            "Fn::Join": [
                "",
                [
                    "https://",
                    {
                        "Fn::GetAtt": [
                            "S3Bucket",
                            "DomainName"
                        ]
                    }
                ]
            ]
        },
        "Description": "Name of S3 bucket to hold website content"
    }
}

```

```

    }
  }
}
```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      PublicAccessBlockConfiguration:
        BlockPublicAcls: false
        BlockPublicPolicy: false
        IgnorePublicAcls: false
        RestrictPublicBuckets: false
      WebsiteConfiguration:
        IndexDocument: index.html
        ErrorDocument: error.html
      DeletionPolicy: Retain
      UpdateReplacePolicy: Retain
  BucketPolicy:
    Type: 'AWS::S3::BucketPolicy'
    Properties:
      PolicyDocument:
        Id: MyPolicy
        Version: 2012-10-17
        Statement:
          - Sid: PublicReadForGetBucketObjects
            Effect: Allow
            Principal: '*'
            Action: 's3:GetObject'
            Resource: !Join
              - '-'
              - - 'arn:aws:s3:::'
                - !Ref S3Bucket
              - '/*'
      Bucket: !Ref S3Bucket
Outputs:
  WebsiteURL:
    Value: !GetAtt
    - S3Bucket
    - WebsiteURL
```



```

Description: URL for website hosted on S3
S3BucketSecureURL:
  Value: !Join
    - ''
    - - 'https://'
      - !GetAtt
        - S3Bucket
        - DomainName
Description: Name of S3 bucket to hold website content

```

Creazione di un sito Web statico utilizzando un dominio personalizzato

Puoi utilizzare Route 53 con un dominio registrato. L'esempio seguente presuppone che tu abbia già creato una zona ospitata in Route 53 per il dominio. L'esempio crea due bucket per l'hosting di siti Web. Il root bucket ospita i contenuti, mentre l'altro bucket reindirizza le richieste `www.domainname.com` al root bucket. I set di record eseguono la mappatura del nome di dominio all'endpoint Amazon S3.

Sarà necessario aggiungere una policy del bucket, come illustrato negli esempi precedenti.

Per ulteriori informazioni sull'utilizzo di un dominio personalizzato, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#) nella Amazon Simple Storage Service User Guide.

Note

Gli esempi seguenti presuppongono che le impostazioni `BlockPublicPolicy` e `RestrictPublicBuckets` Block Public Access siano state disabilitate a livello di account.

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Mappings" : {
    "RegionMap" : {
      "us-east-1" : { "S3hostedzoneID" : "Z3AQBSTGFYJSTF", "websiteendpoint" :
"s3-website-us-east-1.amazonaws.com" },
      "us-west-1" : { "S3hostedzoneID" : "Z2F56UZL2M1ACD", "websiteendpoint" :
"s3-website-us-west-1.amazonaws.com" },
      "us-west-2" : { "S3hostedzoneID" : "Z3BJ6K6RIION7M", "websiteendpoint" :
"s3-website-us-west-2.amazonaws.com" },

```

```

        "eu-west-1" : { "S3hostedzoneID" : "Z1BKCTXD74EZPE", "websiteendpoint" :
"s3-website-eu-west-1.amazonaws.com" },
        "ap-southeast-1" : { "S3hostedzoneID" : "Z300J2DXBE1FTB",
"websiteendpoint" : "s3-website-ap-southeast-1.amazonaws.com" },
        "ap-southeast-2" : { "S3hostedzoneID" : "Z1WCIGYICN2BYD",
"websiteendpoint" : "s3-website-ap-southeast-2.amazonaws.com" },
        "ap-northeast-1" : { "S3hostedzoneID" : "Z2M4EHUR26P7ZW",
"websiteendpoint" : "s3-website-ap-northeast-1.amazonaws.com" },
        "sa-east-1" : { "S3hostedzoneID" : "Z31GFT0UA1I2HV", "websiteendpoint" :
"s3-website-sa-east-1.amazonaws.com" }
    }
},
"Parameters": {
    "RootDomainName": {
        "Description": "Domain name for your website (example.com)",
        "Type": "String"
    }
},
"Resources": {
    "RootBucket": {
        "Type": "AWS::S3::Bucket",
        "Properties": {
            "BucketName" : {"Ref":"RootDomainName"},
            "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
                "RestrictPublicBuckets": false
            },
            "WebsiteConfiguration": {
                "IndexDocument":"index.html",
                "ErrorDocument":"404.html"
            }
        }
    },
    "WWWBucket": {
        "Type": "AWS::S3::Bucket",
        "Properties": {
            "BucketName": {
                "Fn::Join": [ "", [ "www.", {"Ref":"RootDomainName"} ] ]
            },
            "AccessControl": "BucketOwnerFullControl",
            "WebsiteConfiguration": {
                "RedirectAllRequestsTo": {

```

```

        "HostName": {"Ref": "RootBucket"}
    }
}
},
"myDNS": {
    "Type": "AWS::Route53::RecordSetGroup",
    "Properties": {
        "HostedZoneName": {
            "Fn::Join": ["", [{"Ref": "RootDomainName"}, "."]]
        },
        "Comment": "Zone apex alias.",
        "RecordSets": [
            {
                "Name": {"Ref": "RootDomainName"},
                "Type": "A",
                "AliasTarget": {
                    "HostedZoneId": {"Fn::FindInMap" : [ "RegionMap", { "Ref" :
"AWS::Region" }, "S3hostedzoneID"]},
                    "DNSName": {"Fn::FindInMap" : [ "RegionMap", { "Ref" :
"AWS::Region" }, "websiteendpoint"]}
                }
            },
            {
                "Name": {
                    "Fn::Join": ["", ["www.", {"Ref": "RootDomainName"}]]
                },
                "Type": "CNAME",
                "TTL" : "900",
                "ResourceRecords" : [
                    {"Fn::GetAtt": ["WWWBucket", "DomainName"]}
                ]
            }
        ]
    }
}
},
"Outputs": {
    "WebsiteURL": {
        "Value": {"Fn::GetAtt": ["RootBucket", "WebsiteURL"]},
        "Description": "URL for website hosted on S3"
    }
}
}

```

```
}
```

YAML

```
Parameters:
  RootDomainName:
    Description: Domain name for your website (example.com)
    Type: String
Mappings:
  RegionMap:
    us-east-1:
      S3hostedzoneID: Z3AQBSTGIFYJSTF
      websiteendpoint: s3-website-us-east-1.amazonaws.com
    us-west-1:
      S3hostedzoneID: Z2F56UZL2M1ACD
      websiteendpoint: s3-website-us-west-1.amazonaws.com
    us-west-2:
      S3hostedzoneID: Z3BJ6K6RIION7M
      websiteendpoint: s3-website-us-west-2.amazonaws.com
    eu-west-1:
      S3hostedzoneID: Z1BKCTXD74EZPE
      websiteendpoint: s3-website-eu-west-1.amazonaws.com
    ap-southeast-1:
      S3hostedzoneID: Z300J2DXBE1FTB
      websiteendpoint: s3-website-ap-southeast-1.amazonaws.com
    ap-southeast-2:
      S3hostedzoneID: Z1WCIGYICN2BYD
      websiteendpoint: s3-website-ap-southeast-2.amazonaws.com
    ap-northeast-1:
      S3hostedzoneID: Z2M4EHUR26P7ZW
      websiteendpoint: s3-website-ap-northeast-1.amazonaws.com
    sa-east-1:
      S3hostedzoneID: Z31GFT0UA1I2HV
      websiteendpoint: s3-website-sa-east-1.amazonaws.com
Resources:
  RootBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Ref RootDomainName
      PublicAccessBlockConfiguration:
        BlockPublicAcls: false
        BlockPublicPolicy: false
        IgnorePublicAcls: false
```

```

    RestrictPublicBuckets: false
  WebsiteConfiguration:
    IndexDocument: index.html
    ErrorDocument: 404.html
WWWBucket:
  Type: AWS::S3::Bucket
  Properties:
    BucketName: !Sub
      - www.${Domain}
      - Domain: !Ref RootDomainName
    AccessControl: BucketOwnerFullControl
    WebsiteConfiguration:
      RedirectAllRequestsTo:
        HostName: !Ref RootBucket
myDNS:
  Type: AWS::Route53::RecordSetGroup
  Properties:
    HostedZoneName: !Sub
      - ${Domain}.
      - Domain: !Ref RootDomainName
    Comment: Zone apex alias.
    RecordSets:
      - Name: !Ref RootDomainName
        Type: A
        AliasTarget:
          HostedZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', S3hostedzoneID]
          DNSName: !FindInMap [ RegionMap, !Ref 'AWS::Region', websiteendpoint]
      - Name: !Sub
          - www.${Domain}
          - Domain: !Ref RootDomainName
        Type: CNAME
        TTL: 900
        ResourceRecords:
          - !GetAtt WWWBucket.DomainName
Outputs:
  WebsiteURL:
    Value: !GetAtt RootBucket.WebsiteURL
    Description: URL for website hosted on S3

```

Frammenti di modello Amazon SNS

Questo esempio illustra una risorsa di argomento Amazon SNS. È necessario un indirizzo e-mail valido.

JSON

```
"MySNSTopic" : {
  "Type" : "AWS::SNS::Topic",
  "Properties" : {
    "Subscription" : [ {
      "Endpoint" : "add valid email address",
      "Protocol" : "email"
    } ]
  }
}
```

YAML

```
MySNSTopic:
  Type: AWS::SNS::Topic
  Properties:
    Subscription:
      - Endpoint: "add valid email address"
        Protocol: email
```

Frammenti di modello Amazon SQS

Questo esempio illustra una coda Amazon SQS.

JSON

```
"MyQueue" : {
  "Type" : "AWS::SQS::Queue",
  "Properties" : {
    "VisibilityTimeout" : "value"
  }
}
```

YAML

```
MyQueue:
  Type: AWS::SQS::Queue
  Properties:
    VisibilityTimeout: value
```

Frammenti di modello Amazon Timestream

Amazon Timestream for InfluxDB consente agli sviluppatori di applicazioni DevOps e ai team di eseguire facilmente database AWS InfluxDB completamente gestiti su applicazioni di serie temporali in tempo reale utilizzando l'open source. APIs Puoi creare rapidamente un database InfluxDB che gestisca carichi di lavoro impegnativi in serie temporali. Con poche semplici chiamate API, puoi configurare, migrare, gestire e scalare un database InfluxDB AWS con patch, backup e ripristino automatizzati del software. [Puoi trovare questi esempi anche su -influxdb on. awslabs/amazon-timestream-tools/tree/mainline/integrations/cloudformation/timestream](https://github.com/aws-labs/amazon-timestream-tools/tree/mainline/integrations/cloudformation/timestream) GitHub

Argomenti

- [Esempio minimo con valori predefiniti](#)
- [Esempio più completo con parametri](#)

Questi AWS CloudFormation modelli creano le seguenti risorse necessarie per creare, connettersi e monitorare correttamente un'istanza Amazon Timestream for InfluxDB:

Amazon VPC

- VPC
- Uno o più Subnet
- InternetGateway
- RouteTable
- SecurityGroup

Amazon S3

- Bucket

Amazon Timestream

- InfluxDBInstance

Esempio minimo con valori predefiniti

Questo esempio implementa un'istanza multi-AZ accessibile pubblicamente utilizzando valori predefiniti quando possibile.

JSON

```
{
  "Metadata": {
    "AWS::CloudFormation::Interface": {
      "ParameterGroups": [
        {
          "Label": {"default": "Amazon Timestream for InfluxDB Configuration"},
          "Parameters": [
            "DbInstanceName",
            "InfluxDBPassword"
          ]
        }
      ],
      "ParameterLabels": {
        "VPCCIDR": {"default": "VPC CIDR"}
      }
    }
  },
  "Parameters": {
    "DbInstanceName": {
      "Description": "The name that uniquely identifies the DB instance when interacting with the Amazon Timestream for InfluxDB API and CLI commands. This name will also be a prefix included in the endpoint. DB instance names must be unique per customer and per Region.",
      "Type": "String",
      "Default": "mydbinstance",
      "MinLength": 3,
      "MaxLength": 40,
      "AllowedPattern": "^[a-zA-z][a-zA-Z0-9]*(-[a-zA-Z0-9]+)*$"
    },
    "InfluxDBPassword": {
      "Description": "The password of the initial admin user created in InfluxDB. This password will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS Secrets Manager in your account.",
      "Type": "String",
      "NoEcho": true,

```



```

    "MinLength": 8,
    "MaxLength": 64,
    "AllowedPattern": "^[a-zA-Z0-9]+$"
  },
},
"Resources": {
  "VPC": {
    "Type": "AWS::EC2::VPC",
    "Properties": {"CidrBlock": "10.0.0.0/16"}
  },
  "InternetGateway": {"Type": "AWS::EC2::InternetGateway"},
  "InternetGatewayAttachment": {
    "Type": "AWS::EC2::VPCGatewayAttachment",
    "Properties": {
      "InternetGatewayId": {"Ref": "InternetGateway"},
      "VpcId": {"Ref": "VPC"}
    }
  },
},
"Subnet1": {
  "Type": "AWS::EC2::Subnet",
  "Properties": {
    "VpcId": {"Ref": "VPC"},
    "AvailabilityZone": {
      "Fn::Select": [
        0,
        {"Fn::GetAZs": ""}
      ]
    },
    "CidrBlock": {
      "Fn::Select": [
        0,
        {
          "Fn::Cidr": [
            {
              "Fn::GetAtt": [
                "VPC",
                "CidrBlock"
              ]
            },
            2,
            12
          ]
        }
      ]
    }
  }
}
]
```

```

    },
    "MapPublicIpOnLaunch": true
  }
},
"Subnet2": {
  "Type": "AWS::EC2::Subnet",
  "Properties": {
    "VpcId": {"Ref": "VPC"},
    "AvailabilityZone": {
      "Fn::Select": [
        1,
        {"Fn::GetAZs": ""}
      ]
    },
  },
  "CidrBlock": {
    "Fn::Select": [
      1,
      {
        "Fn::Cidr": [
          {
            "Fn::GetAtt": [
              "VPC",
              "CidrBlock"
            ]
          },
          2,
          12
        ]
      }
    ]
  },
  "MapPublicIpOnLaunch": true
},
"RouteTable": {
  "Type": "AWS::EC2::RouteTable",
  "Properties": {
    "VpcId": {"Ref": "VPC"}
  }
},
"DefaultRoute": {
  "Type": "AWS::EC2::Route",
  "DependsOn": "InternetGatewayAttachment",
  "Properties": {

```

```
    "RouteTableId": {"Ref": "RouteTable"},
    "DestinationCidrBlock": "0.0.0.0/0",
    "GatewayId": {"Ref": "InternetGateway"}
  },
  "Subnet1RouteTableAssociation": {
    "Type": "AWS::EC2::SubnetRouteTableAssociation",
    "Properties": {
      "RouteTableId": {"Ref": "RouteTable"},
      "SubnetId": {"Ref": "Subnet1"}
    }
  },
  "Subnet2RouteTableAssociation": {
    "Type": "AWS::EC2::SubnetRouteTableAssociation",
    "Properties": {
      "RouteTableId": {"Ref": "RouteTable"},
      "SubnetId": {"Ref": "Subnet2"}
    }
  },
  "InfluxDBSecurityGroup": {
    "Type": "AWS::EC2::SecurityGroup",
    "Properties": {
      "GroupName": "influxdb-sg",
      "GroupDescription": "Security group allowing port 8086 ingress for InfluxDB",
      "VpcId": {"Ref": "VPC"}
    }
  },
  "InfluxDBSecurityGroupIngress": {
    "Type": "AWS::EC2::SecurityGroupIngress",
    "Properties": {
      "GroupId": {"Ref": "InfluxDBSecurityGroup"},
      "IpProtocol": "tcp",
      "CidrIp": "0.0.0.0/0",
      "FromPort": 8086,
      "ToPort": 8086
    }
  },
  "InfluxDBLogsS3Bucket": {
    "Type": "AWS::S3::Bucket",
    "DeletionPolicy": "Retain"
  },
  "InfluxDBLogsS3BucketPolicy": {
    "Type": "AWS::S3::BucketPolicy",
    "Properties": {
```

```

    "Bucket": {"Ref": "InfluxDBLogsS3Bucket"},
    "PolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Action": "s3:PutObject",
          "Effect": "Allow",
          "Resource": {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}/InfluxLogs/*"},
          "Principal": {"Service": "timestream-influxdb.amazonaws.com"}
        },
        {
          "Action": "s3:*",
          "Effect": "Deny",
          "Resource": [
            {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}/*"},
            {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}"}
          ],
          "Principal": "*",
          "Condition": {
            "Bool": {"aws:SecureTransport": false}
          }
        }
      ]
    }
  },
  "DbInstance": {
    "Type": "AWS::Timestream::InfluxDBInstance",
    "DependsOn": "InfluxDBLogsS3BucketPolicy",
    "Properties": {
      "AllocatedStorage": 20,
      "DbInstanceType": "db.influx.medium",
      "Name": {"Ref": "DbInstanceName"},
      "Password": {"Ref": "InfluxDBPassword"},
      "PubliclyAccessible": true,
      "DeploymentType": "WITH_MULTIAZ_STANDBY",
      "VpcSecurityGroupIds": [
        {"Ref": "InfluxDBSecurityGroup"}
      ],
      "VpcSubnetIds": [
        {"Ref": "Subnet1"},
        {"Ref": "Subnet2"}
      ]
    }
  },

```

```

        "LogDeliveryConfiguration": {
            "S3Configuration": {
                "BucketName": {"Ref": "InfluxDBLogsS3Bucket"},
                "Enabled": true
            }
        }
    },
    "Outputs": {
        "VPC": {
            "Description": "A reference to the VPC used to create network resources",
            "Value": {"Ref": "VPC"}
        },
        "Subnets": {
            "Description": "A list of the subnets created",
            "Value": {
                "Fn::Join": [
                    ",",
                    [
                        {"Ref": "Subnet1"},
                        {"Ref": "Subnet2"}
                    ]
                ]
            }
        },
        "Subnet1": {
            "Description": "A reference to the subnet in the 1st Availability Zone",
            "Value": {"Ref": "Subnet1"}
        },
        "Subnet2": {
            "Description": "A reference to the subnet in the 2nd Availability Zone",
            "Value": {"Ref": "Subnet2"}
        },
        "InfluxDBSecurityGroup": {
            "Description": "Security group with port 8086 ingress rule",
            "Value": {"Ref": "InfluxDBSecurityGroup"}
        },
        "InfluxDBLogsS3Bucket": {
            "Description": "S3 Bucket containing InfluxDB logs from the DB instance",
            "Value": {"Ref": "InfluxDBLogsS3Bucket"}
        },
        "DbInstance": {
            "Description": "A reference to the Timestream for InfluxDB DB instance",

```

```

    "Value": {"Ref": "DbInstance"}
  },
  "InfluxAuthParametersSecretArn": {
    "Description": "The Amazon Resource Name (ARN) of the AWS Secrets Manager secret
containing the initial InfluxDB authorization parameters. The secret value is a JSON
formatted key-value pair holding InfluxDB authorization values: organization, bucket,
username, and password.",
    "Value": {
      "Fn::GetAtt": [
        "DbInstance",
        "InfluxAuthParametersSecretArn"
      ]
    }
  },
  "Endpoint": {
    "Description": "The endpoint URL to connect to InfluxDB",
    "Value": {
      "Fn::Join": [
        "",
        [
          "https://",
          {
            "Fn::GetAtt": [
              "DbInstance",
              "Endpoint"
            ]
          },
          ":8086"
        ]
      ]
    }
  }
}

```

YAML

```

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      -
        Label:
          default: "Amazon Timestream for InfluxDB Configuration"

```

Parameters:

- DbInstanceName
- InfluxDBPassword

ParameterLabels:**VPCCIDR:**

default: VPC CIDR

Parameters:**DbInstanceName:**

Description: The name that uniquely identifies the DB instance when interacting with the Amazon Timestream for InfluxDB API and CLI commands. This name will also be a prefix included in the endpoint. DB instance names must be unique per customer and per Region.

Type: String

Default: mydbinstance

MinLength: 3

MaxLength: 40

AllowedPattern: `^[a-zA-z][a-zA-Z0-9]*(-[a-zA-Z0-9]+)*$`

InfluxDBPassword:

Description: The password of the initial admin user created in InfluxDB. This password will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS Secrets Manager in your account.

Type: String

NoEcho: true

MinLength: 8

MaxLength: 64

AllowedPattern: `^[a-zA-Z0-9]+$`

Resources:**VPC:**

Type: AWS::EC2::VPC

Properties:

CidrBlock: 10.0.0.0/16

InternetGateway:

Type: AWS::EC2::InternetGateway

InternetGatewayAttachment:

Type: AWS::EC2::VPCElasticNetworkInterfaceAttachment

Properties:

InternetGatewayId: !Ref InternetGateway

VpcId: !Ref VPC

Subnet1:

Type: AWS::EC2::Subnet

Properties:

```
VpcId: !Ref VPC
AvailabilityZone: !Select [0, !GetAZs '']
CidrBlock: !Select [0, !Cidr [!GetAtt VPC.CidrBlock, 2, 12 ]]
MapPublicIpOnLaunch: true
Subnet2:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [1, !GetAZs '']
    CidrBlock: !Select [1, !Cidr [!GetAtt VPC.CidrBlock, 2, 12 ]]
    MapPublicIpOnLaunch: true
RouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
DefaultRoute:
  Type: AWS::EC2::Route
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref RouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway
Subnet1RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref RouteTable
    SubnetId: !Ref Subnet1
Subnet2RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref RouteTable
    SubnetId: !Ref Subnet2
InfluxDBSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupName: "influxdb-sg"
    GroupDescription: "Security group allowing port 8086 ingress for InfluxDB"
    VpcId: !Ref VPC
InfluxDBSecurityGroupIngress:
  Type: AWS::EC2::SecurityGroupIngress
  Properties:
    GroupId: !Ref InfluxDBSecurityGroup
    IpProtocol: tcp
    CidrIp: 0.0.0.0/0
```



```

    FromPort: 8086
    ToPort: 8086
  InfluxDBLogsS3Bucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
  InfluxDBLogsS3BucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref InfluxDBLogsS3Bucket
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Action: "s3:PutObject"
            Effect: Allow
            Resource: !Sub arn:aws:s3:::${InfluxDBLogsS3Bucket}/InfluxLogs/*
            Principal:
              Service: timestream-influxdb.amazonaws.com
          - Action: "s3:*"
            Effect: Deny
            Resource:
              - !Sub arn:aws:s3:::${InfluxDBLogsS3Bucket}/*
              - !Sub arn:aws:s3:::${InfluxDBLogsS3Bucket}
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport: false
  DbInstance:
    Type: AWS::Timestream::InfluxDBInstance
    DependsOn: InfluxDBLogsS3BucketPolicy
    Properties:
      AllocatedStorage: 20
      DbInstanceType: db.influx.medium
      Name: !Ref DbInstanceName
      Password: !Ref InfluxDBPassword
      PubliclyAccessible: true
      DeploymentType: WITH_MULTIAZ_STANDBY
      VpcSecurityGroupIds:
        - !Ref InfluxDBSecurityGroup
      VpcSubnetIds:
        - !Ref Subnet1
        - !Ref Subnet2
      LogDeliveryConfiguration:
        S3Configuration:
          BucketName: !Ref InfluxDBLogsS3Bucket

```

```
Enabled: true
```

Outputs:**# Network Resources****VPC:**

```
Description: A reference to the VPC used to create network resources
```

```
Value: !Ref VPC
```

Subnets:

```
Description: A list of the subnets created
```

```
Value: !Join [",", [!Ref Subnet1, !Ref Subnet2]]
```

Subnet1:

```
Description: A reference to the subnet in the 1st Availability Zone
```

```
Value: !Ref Subnet1
```

Subnet2:

```
Description: A reference to the subnet in the 2nd Availability Zone
```

```
Value: !Ref Subnet2
```

InfluxDBSecurityGroup:

```
Description: Security group with port 8086 ingress rule
```

```
Value: !Ref InfluxDBSecurityGroup
```

Timestream for InfluxDB Resources**InfluxDBLogsS3Bucket:**

```
Description: S3 Bucket containing InfluxDB logs from the DB instance
```

```
Value: !Ref InfluxDBLogsS3Bucket
```

DbInstance:

```
Description: A reference to the Timestream for InfluxDB DB instance
```

```
Value: !Ref DbInstance
```

InfluxAuthParametersSecretArn:

```
Description: "The Amazon Resource Name (ARN) of the AWS Secrets Manager secret containing the initial InfluxDB authorization parameters. The secret value is a JSON formatted key-value pair holding InfluxDB authorization values: organization, bucket, username, and password."
```

```
Value: !GetAtt DbInstance.InfluxAuthParametersSecretArn
```

Endpoint:

```
Description: The endpoint URL to connect to InfluxDB
```

```
Value: !Join ["", ["https://", !GetAtt DbInstance.Endpoint, ":8086"]]
```

Esempio più completo con parametri

Questo modello di esempio modifica dinamicamente le risorse di rete in base ai parametri forniti. I parametri includono `PubliclyAccessible` e `DeploymentType`

JSON

```
{
  "Metadata": {
    "AWS::CloudFormation::Interface": {
      "ParameterGroups": [
        {
          "Label": {"default": "Network Configuration"},
          "Parameters": ["VPCCIDR"]
        },
        {
          "Label": {"default": "Amazon Timestream for InfluxDB Configuration"},
          "Parameters": [
            "DbInstanceName",
            "InfluxDBUsername",
            "InfluxDBPassword",
            "InfluxDBOrganization",
            "InfluxDBBucket",
            "DbInstanceType",
            "DbStorageType",
            "AllocatedStorage",
            "PubliclyAccessible",
            "DeploymentType"
          ]
        }
      ],
      "ParameterLabels": {
        "VPCCIDR": {"default": "VPC CIDR"}
      }
    }
  },
  "Parameters": {
    "VPCCIDR": {
      "Description": "Please enter the IP range (CIDR notation) for the new VPC",
      "Type": "String",
      "Default": "10.0.0.0/16"
    },
    "DbInstanceName": {
      "Description": "The name that uniquely identifies the DB instance when interacting with the Amazon Timestream for InfluxDB API and CLI commands. This name will also be a prefix included in the endpoint. DB instance names must be unique per customer and per Region.",
      "Type": "String",
      "Default": "mydbinstance",

```

```

    "MinLength": 3,
    "MaxLength": 40,
    "AllowedPattern": "^[a-zA-z][a-zA-Z0-9]*(-[a-zA-Z0-9]+)*$"
  },
  "InfluxDBUsername": {
    "Description": "The username of the initial admin user created in InfluxDB. Must start with a letter and can't end with a hyphen or contain two consecutive hyphens. For example, my-user1. This username will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS Secrets Manager in your account.",
    "Type": "String",
    "Default": "admin",
    "MinLength": 1,
    "MaxLength": 64
  },
  "InfluxDBPassword": {
    "Description": "The password of the initial admin user created in InfluxDB. This password will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS Secrets Manager in your account.",
    "Type": "String",
    "NoEcho": true,
    "MinLength": 8,
    "MaxLength": 64,
    "AllowedPattern": "^[a-zA-Z0-9]+$"
  },
  "InfluxDBOrganization": {
    "Description": "The name of the initial organization for the initial admin user in InfluxDB. An InfluxDB organization is a workspace for a group of users.",
    "Type": "String",
    "Default": "org",
    "MinLength": 1,
    "MaxLength": 64
  },
  "InfluxDBBucket": {
    "Description": "The name of the initial InfluxDB bucket. All InfluxDB data is stored in a bucket. A bucket combines the concept of a database and a retention period (the duration of time that each data point persists). A bucket belongs to an organization.",
    "Type": "String",
    "Default": "bucket",
    "MinLength": 2,
    "MaxLength": 64,

```

```

    "AllowedPattern": "^[^_\\\\""][^\\\\""]*$"
  },
  "DeploymentType": {
    "Description": "Specifies whether the Timestream for InfluxDB is deployed as
Single-AZ or with a MultiAZ Standby for High availability",
    "Type": "String",
    "Default": "WITH_MULTIAZ_STANDBY",
    "AllowedValues": [
      "SINGLE_AZ",
      "WITH_MULTIAZ_STANDBY"
    ]
  },
  "AllocatedStorage": {
    "Description": "The amount of storage to allocate for your DB storage type in GiB
(gibibytes).",
    "Type": "Number",
    "Default": 400,
    "MinValue": 20,
    "MaxValue": 16384
  },
  "DbInstanceType": {
    "Description": "The Timestream for InfluxDB DB instance type to run InfluxDB
on.",
    "Type": "String",
    "Default": "db.influx.medium",
    "AllowedValues": [
      "db.influx.medium",
      "db.influx.large",
      "db.influx.xlarge",
      "db.influx.2xlarge",
      "db.influx.4xlarge",
      "db.influx.8xlarge",
      "db.influx.12xlarge",
      "db.influx.16xlarge"
    ]
  },
  "DbStorageType": {
    "Description": "The Timestream for InfluxDB DB storage type to read and write
InfluxDB data.",
    "Type": "String",
    "Default": "InfluxIOIncludedT1",
    "AllowedValues": [
      "InfluxIOIncludedT1",
      "InfluxIOIncludedT2",

```

```

        "InfluxIOIncludedT3"
    ]
},
"PubliclyAccessible": {
    "Description": "Configures the DB instance with a public IP to facilitate
access.",
    "Type": "String",
    "Default": true,
    "AllowedValues": [
        true,
        false
    ]
}
},
"Conditions": {
    "IsMultiAZ": {
        "Fn::Equals": [
            {"Ref": "DeploymentType"},
            "WITH_MULTIAZ_STANDBY"
        ]
    },
    "IsPublic": {
        "Fn::Equals": [
            {"Ref": "PubliclyAccessible"},
            true
        ]
    }
},
"Resources": {
    "VPC": {
        "Type": "AWS::EC2::VPC",
        "Properties": {
            "CidrBlock": {"Ref": "VPCCIDR"}
        }
    },
    "InternetGateway": {
        "Type": "AWS::EC2::InternetGateway",
        "Condition": "IsPublic"
    },
    "InternetGatewayAttachment": {
        "Type": "AWS::EC2::VPCGatewayAttachment",
        "Condition": "IsPublic",
        "Properties": {
            "InternetGatewayId": {"Ref": "InternetGateway"},

```

```

    "VpcId": {"Ref": "VPC"}
  },
  "Subnet1": {
    "Type": "AWS::EC2::Subnet",
    "Properties": {
      "VpcId": {"Ref": "VPC"},
      "AvailabilityZone": {
        "Fn::Select": [
          0,
          {"Fn::GetAZs": ""}
        ]
      },
      "CidrBlock": {
        "Fn::Select": [
          0,
          {
            "Fn::Cidr": [
              {
                "Fn::GetAtt": [
                  "VPC",
                  "CidrBlock"
                ]
              },
              2,
              12
            ]
          }
        ]
      },
      "MapPublicIpOnLaunch": {
        "Fn::If": [
          "IsPublic",
          true,
          false
        ]
      }
    }
  },
  "Subnet2": {
    "Type": "AWS::EC2::Subnet",
    "Condition": "IsMultiAZ",
    "Properties": {
      "VpcId": {"Ref": "VPC"},

```

```
    "AvailabilityZone": {
      "Fn::Select": [
        1,
        {"Fn::GetAZs": ""}
      ]
    },
    "CidrBlock": {
      "Fn::Select": [
        1,
        {
          "Fn::Cidr": [
            {
              "Fn::GetAtt": [
                "VPC",
                "CidrBlock"
              ]
            },
            2,
            12
          ]
        }
      ]
    },
    "MapPublicIpOnLaunch": {
      "Fn::If": [
        "IsPublic",
        true,
        false
      ]
    }
  },
  "RouteTable": {
    "Type": "AWS::EC2::RouteTable",
    "Properties": {
      "VpcId": {"Ref": "VPC"}
    }
  },
  "DefaultRoute": {
    "Type": "AWS::EC2::Route",
    "Condition": "IsPublic",
    "DependsOn": "InternetGatewayAttachment",
    "Properties": {
      "RouteTableId": {"Ref": "RouteTable"},
```



```

        "DestinationCidrBlock": "0.0.0.0/0",
        "GatewayId": {"Ref": "InternetGateway"}
    },
    "Subnet1RouteTableAssociation": {
        "Type": "AWS::EC2::SubnetRouteTableAssociation",
        "Properties": {
            "RouteTableId": {"Ref": "RouteTable"},
            "SubnetId": {"Ref": "Subnet1"}
        }
    },
    "Subnet2RouteTableAssociation": {
        "Type": "AWS::EC2::SubnetRouteTableAssociation",
        "Condition": "IsMultiAZ",
        "Properties": {
            "RouteTableId": {"Ref": "RouteTable"},
            "SubnetId": {"Ref": "Subnet2"}
        }
    },
    "InfluxDBSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupName": "influxdb-sg",
            "GroupDescription": "Security group allowing port 8086 ingress for InfluxDB",
            "VpcId": {"Ref": "VPC"}
        }
    },
    "InfluxDBSecurityGroupIngress": {
        "Type": "AWS::EC2::SecurityGroupIngress",
        "Properties": {
            "GroupId": {"Ref": "InfluxDBSecurityGroup"},
            "IpProtocol": "tcp",
            "CidrIp": "0.0.0.0/0",
            "FromPort": 8086,
            "ToPort": 8086
        }
    },
    "InfluxDBLogsS3Bucket": {
        "Type": "AWS::S3::Bucket",
        "DeletionPolicy": "Retain"
    },
    "InfluxDBLogsS3BucketPolicy": {
        "Type": "AWS::S3::BucketPolicy",
        "Properties": {

```

```

    "Bucket": {"Ref": "InfluxDBLogsS3Bucket"},
    "PolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Action": "s3:PutObject",
          "Effect": "Allow",
          "Resource": {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}/InfluxLogs/*"},
          "Principal": {"Service": "timestream-influxdb.amazonaws.com"}
        },
        {
          "Action": "s3:*",
          "Effect": "Deny",
          "Resource": [
            {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}/*"},
            {"Fn::Sub": "arn:aws:s3:::${InfluxDBLogsS3Bucket}"}
          ],
          "Principal": "*",
          "Condition": {
            "Bool": {"aws:SecureTransport": false}
          }
        }
      ]
    }
  },
  "DbInstance": {
    "Type": "AWS::Timestream::InfluxDBInstance",
    "DependsOn": "InfluxDBLogsS3BucketPolicy",
    "Properties": {
      "DbStorageType": {"Ref": "DbStorageType"},
      "AllocatedStorage": {"Ref": "AllocatedStorage"},
      "DbInstanceType": {"Ref": "DbInstanceType"},
      "Name": {"Ref": "DbInstanceName"},
      "Username": {"Ref": "InfluxDBUsername"},
      "Password": {"Ref": "InfluxDBPassword"},
      "Organization": {"Ref": "InfluxDBOrganization"},
      "Bucket": {"Ref": "InfluxDBBucket"},
      "PubliclyAccessible": {
        "Fn::If": [
          "IsPublic",
          true,
          false
        ]
      }
    }
  }
}

```

```

    ]
  },
  "DeploymentType": {"Ref": "DeploymentType"},
  "VpcSecurityGroupIds": [
    {"Ref": "InfluxDBSecurityGroup"}
  ],
  "VpcSubnetIds": {
    "Fn::If": [
      "IsMultiAZ",
      [
        {"Ref": "Subnet1"},
        {"Ref": "Subnet2"}
      ],
      [
        {"Ref": "Subnet1"}
      ]
    ]
  },
  "LogDeliveryConfiguration": {
    "S3Configuration": {
      "BucketName": {"Ref": "InfluxDBLogsS3Bucket"},
      "Enabled": true
    }
  }
}
},
"Outputs": {
  "VPC": {
    "Description": "A reference to the VPC used to create network resources",
    "Value": {"Ref": "VPC"}
  },
  "Subnets": {
    "Description": "A list of the subnets created",
    "Value": {
      "Fn::If": [
        "IsMultiAZ",
        {
          "Fn::Join": [
            ",",
            [
              {"Ref": "Subnet1"},
              {"Ref": "Subnet2"}
            ]
          ]
        }
      ]
    }
  }
}

```

```

        ]
      },
      {"Ref": "Subnet1"}
    ]
  },
  "Subnet1": {
    "Description": "A reference to the subnet in the 1st Availability Zone",
    "Value": {"Ref": "Subnet1"}
  },
  "Subnet2": {
    "Condition": "IsMultiAZ",
    "Description": "A reference to the subnet in the 2nd Availability Zone",
    "Value": {"Ref": "Subnet2"}
  },
  "InfluxDBSecurityGroup": {
    "Description": "Security group with port 8086 ingress rule",
    "Value": {"Ref": "InfluxDBSecurityGroup"}
  },
  "InfluxDBLogsS3Bucket": {
    "Description": "S3 Bucket containing InfluxDB logs from the DB instance",
    "Value": {"Ref": "InfluxDBLogsS3Bucket"}
  },
  "DbInstance": {
    "Description": "A reference to the Timestream for InfluxDB DB instance",
    "Value": {"Ref": "DbInstance"}
  },
  "InfluxAuthParametersSecretArn": {
    "Description": "The Amazon Resource Name (ARN) of the AWS Secrets Manager secret
containing the initial InfluxDB authorization parameters. The secret value is a JSON
formatted key-value pair holding InfluxDB authorization values: organization, bucket,
username, and password.",
    "Value": {
      "Fn::GetAtt": [
        "DbInstance",
        "InfluxAuthParametersSecretArn"
      ]
    }
  },
  "Endpoint": {
    "Description": "The endpoint URL to connect to InfluxDB",
    "Value": {
      "Fn::Join": [
        "",

```

```

    [
      "https://",
      {
        "Fn::GetAtt": [
          "DbInstance",
          "Endpoint"
        ]
      },
      ":8086"
    ]
  ]
}
}
}
}
}

```

YAML

```

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      -
        Label:
          default: "Network Configuration"
        Parameters:
          - VPCCIDR
      -
        Label:
          default: "Amazon Timestream for InfluxDB Configuration"
        Parameters:
          - DbInstanceName
          - InfluxDBUsername
          - InfluxDBPassword
          - InfluxDBOrganization
          - InfluxDBBucket
          - DbInstanceType
          - DbStorageType
          - AllocatedStorage
          - PubliclyAccessible
          - DeploymentType
    ParameterLabels:
      VPCCIDR:
        default: VPC CIDR

```

Parameters:**# Network Configuration****VPCCIDR:**

Description: Please enter the IP range (CIDR notation) for the new VPC

Type: String

Default: 10.0.0.0/16

Timestream for InfluxDB Configuration**DbInstanceName:**

Description: The name that uniquely identifies the DB instance when interacting with the Amazon Timestream for InfluxDB API and CLI commands. This name will also be a prefix included in the endpoint. DB instance names must be unique per customer and per Region.

Type: String

Default: mydbinstance

MinLength: 3

MaxLength: 40

AllowedPattern: ^[a-zA-z][a-zA-Z0-9]*(-[a-zA-Z0-9+])*

InfluxDB initial user configurations**InfluxDBUsername:**

Description: The username of the initial admin user created in InfluxDB. Must start with a letter and can't end with a hyphen or contain two consecutive hyphens. For example, my-user1. This username will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS Secrets Manager in your account.

Type: String

Default: admin

MinLength: 1

MaxLength: 64

InfluxDBPassword:

Description: The password of the initial admin user created in InfluxDB. This password will allow you to access the InfluxDB UI to perform various administrative tasks and also use the InfluxDB CLI to create an operator token. These attributes will be stored in a Secret created in AWS in your account.

Type: String

NoEcho: true

MinLength: 8

MaxLength: 64

AllowedPattern: ^[a-zA-Z0-9]+\$

InfluxDBOrganization:

Description: The name of the initial organization for the initial admin user in InfluxDB. An InfluxDB organization is a workspace for a group of users.

Type: String

Default: org

MinLength: 1

MaxLength: 64

InfluxDBBucket:

Description: The name of the initial InfluxDB bucket. All InfluxDB data is stored in a bucket. A bucket combines the concept of a database and a retention period (the duration of time that each data point persists). A bucket belongs to an organization.

Type: String

Default: bucket

MinLength: 2

MaxLength: 64

AllowedPattern: ^[^_"]\[^\"]]*\$

DeploymentType:

Description: Specifies whether the Timestream for InfluxDB is deployed as Single-AZ or with a MultiAZ Standby for High availability

Type: String

Default: WITH_MULTIAZ_STANDBY

AllowedValues:

- SINGLE_AZ
- WITH_MULTIAZ_STANDBY

AllocatedStorage:

Description: The amount of storage to allocate for your DB storage type in GiB (gibibytes).

Type: Number

Default: 400

MinValue: 20

MaxValue: 16384

DbInstanceType:

Description: The Timestream for InfluxDB DB instance type to run InfluxDB on.

Type: String

Default: db.influx.medium

AllowedValues:

- db.influx.medium
- db.influx.large
- db.influx.xlarge
- db.influx.2xlarge
- db.influx.4xlarge
- db.influx.8xlarge
- db.influx.12xlarge
- db.influx.16xlarge

DbStorageType:

Description: The Timestream for InfluxDB DB storage type to read and write InfluxDB data.

Type: String

Default: InfluxIOIncludedT1

AllowedValues:

- InfluxIOIncludedT1
- InfluxIOIncludedT2
- InfluxIOIncludedT3

PubliclyAccessible:

Description: Configures the DB instance with a public IP to facilitate access.

Type: String

Default: true

AllowedValues:

- true
- false

Conditions:

IsMultiAZ: !Equals [!Ref DeploymentType, WITH_MULTIAZ_STANDBY]

IsPublic: !Equals [!Ref PubliclyAccessible, true]

Resources:

VPC:

Type: AWS::EC2::VPC

Properties:

CidrBlock: !Ref VPCCIDR

InternetGateway:

Type: AWS::EC2::InternetGateway

Condition: IsPublic

InternetGatewayAttachment:

Type: AWS::EC2::VPCGatewayAttachment

Condition: IsPublic

Properties:

InternetGatewayId: !Ref InternetGateway

VpcId: !Ref VPC

Subnet1:

Type: AWS::EC2::Subnet

Properties:

VpcId: !Ref VPC

AvailabilityZone: !Select [0, !GetAZs '']

CidrBlock: !Select [0, !Cidr [!GetAtt VPC.CidrBlock, 2, 12]]

MapPublicIpOnLaunch: !If [IsPublic, true, false]

Subnet2:

Type: AWS::EC2::Subnet

Condition: IsMultiAZ

Properties:

VpcId: !Ref VPC

AvailabilityZone: !Select [1, !GetAZs '']


```
CidrBlock: !Select [1, !Cidr [!GetAtt VPC.CidrBlock, 2, 12 ]]
MapPublicIpOnLaunch: !If [IsPublic, true, false]
RouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
DefaultRoute:
  Type: AWS::EC2::Route
  Condition: IsPublic
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref RouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway
Subnet1RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref RouteTable
    SubnetId: !Ref Subnet1
Subnet2RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Condition: IsMultiAZ
  Properties:
    RouteTableId: !Ref RouteTable
    SubnetId: !Ref Subnet2
InfluxDBSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupName: "influxdb-sg"
    GroupDescription: "Security group allowing port 8086 ingress for InfluxDB"
    VpcId: !Ref VPC
InfluxDBSecurityGroupIngress:
  Type: AWS::EC2::SecurityGroupIngress
  Properties:
    GroupId: !Ref InfluxDBSecurityGroup
    IpProtocol: tcp
    CidrIp: 0.0.0.0/0
    FromPort: 8086
    ToPort: 8086
InfluxDBLogsS3Bucket:
  Type: AWS::S3::Bucket
  DeletionPolicy: Retain
InfluxDBLogsS3BucketPolicy:
  Type: AWS::S3::BucketPolicy
```

Properties:**Bucket:** !Ref InfluxDBLogsS3Bucket**PolicyDocument:****Version:** '2012-10-17'**Statement:**

- **Action:** "s3:PutObject"
- Effect:** Allow
- Resource:** !Sub arn:aws:s3:::\${InfluxDBLogsS3Bucket}/InfluxLogs/*
- Principal:**
 - Service:** timestream-influxdb.amazonaws.com
- **Action:** "s3:*"
- Effect:** Deny
- Resource:**
 - !Sub arn:aws:s3:::\${InfluxDBLogsS3Bucket}/*
 - !Sub arn:aws:s3:::\${InfluxDBLogsS3Bucket}
- Principal:** "*"
 - Condition:**
 - Bool:**
 - aws:SecureTransport: false

DbInstance:**Type:** AWS::Timestream::InfluxDBInstance**DependsOn:** InfluxDBLogsS3BucketPolicy**Properties:****DbStorageType:** !Ref DbStorageType**AllocatedStorage:** !Ref AllocatedStorage**DbInstanceType:** !Ref DbInstanceType**Name:** !Ref DbInstanceName**Username:** !Ref InfluxDBUsername**Password:** !Ref InfluxDBPassword**Organization:** !Ref InfluxDBOrganization**Bucket:** !Ref InfluxDBBucket**PubliclyAccessible:** !If [IsPublic, true, false]**DeploymentType:** !Ref DeploymentType**VpcSecurityGroupIds:**

- !Ref InfluxDBSecurityGroup

VpcSubnetIds: !If

- IsMultiAZ
-
- !Ref Subnet1
- !Ref Subnet2
-
- !Ref Subnet1

LogDeliveryConfiguration:**S3Configuration:**

```
BucketName: !Ref InfluxDBLogsS3Bucket
Enabled: true
```

Outputs:**# Network Resources****VPC:**

```
Description: A reference to the VPC used to create network resources
Value: !Ref VPC
```

Subnets:

```
Description: A list of the subnets created
Value: !If
  - IsMultiAZ
  - !Join [",", [!Ref Subnet1, !Ref Subnet2]]
  - !Ref Subnet1
```

Subnet1:

```
Description: A reference to the subnet in the 1st Availability Zone
Value: !Ref Subnet1
```

Subnet2:

```
Condition: IsMultiAZ
Description: A reference to the subnet in the 2nd Availability Zone
Value: !Ref Subnet2
```

InfluxDBSecurityGroup:

```
Description: Security group with port 8086 ingress rule
Value: !Ref InfluxDBSecurityGroup
```

Timestream for InfluxDB Resources**InfluxDBLogsS3Bucket:**

```
Description: S3 Bucket containing InfluxDB logs from the DB instance
Value: !Ref InfluxDBLogsS3Bucket
```

DbInstance:

```
Description: A reference to the Timestream for InfluxDB DB instance
Value: !Ref DbInstance
```

InfluxAuthParametersSecretArn:

```
Description: "The Amazon Resource Name (ARN) of the AWS Secrets Manager secret
containing the initial InfluxDB authorization parameters. The secret value is a JSON
formatted key-value pair holding InfluxDB authorization values: organization, bucket,
username, and password."
```

```
Value: !GetAtt DbInstance.InfluxAuthParametersSecretArn
```

Endpoint:

```
Description: The endpoint URL to connect to InfluxDB
Value: !Join [""], ["https://", !GetAtt DbInstance.Endpoint, ":8086"]]
```

WindowsImplementa stack basati su CloudFormation

Questa pagina fornisce collegamenti alla documentazione tecnica di riferimento per CloudFormation le risorse comunemente utilizzate nelle distribuzioni Windows basate.

CloudFormation fornisce supporto per l'implementazione e la gestione Microsoft Windows degli stack tramite. Infrastructure as Code (IaC) Puoi utilizzarlo CloudFormation per il provisioning automatico di EC2 istanze Windows basate, su SQL Server Amazon RDS e tramite. Microsoft Active Directory AWS Directory Service

AWS fornisce Amazon Machine Images (AMIs) preconfigurate specificamente per Windows le piattaforme per aiutarti a distribuire rapidamente applicazioni su Amazon. EC2 Queste AMIs includono Microsoft impostazioni predefinite e personalizzazioni AWS specifiche. Con CloudFormation, puoi scegliere un'AMI appropriata, avviare un'istanza e accedervi tramite Remote Desktop Connection, proprio come faresti con qualsiasi altraWindows Server. AMIs Contiene componenti software essenziali, tra cui EC2Launch (le versioni variano in base all'Windows Serveredizione) e vari driver di rete, di archiviazione e grafici per garantire prestazioni e compatibilità ottimali con AWS i servizi. AWS Systems Manager CloudFormation AWS Strumenti per PowerShell Per ulteriori informazioni, consulta l'[AWSWindowsAMI Reference](#).

CloudFormation supporta anche strumenti di configurazione software, come gli UserData script, che possono eseguire PowerShell o eseguire comandi in batch al primo avvio di un' EC2 istanza. Offre inoltre script di supporto (cfn-init, cfn-signalcfn-get-metadata, ecfn-hup) e supporta i `AWS::CloudFormation::Init` metadati per la gestione di pacchetti, file e servizi sulle istanze. Windows

Per gli ambienti aziendali, CloudFormation consente l'aggiunta di domini, la gestione delle licenze tramite modelli di Windows licenza e la gestione EC2 sicura delle credenziali con. AWS Secrets Manager In combinazione con modelli con controllo della versione e implementazioni ripetibili, CloudFormation aiuta le organizzazioni a mantenere ambienti coerenti, sicuri e scalabili su più account. Windows Regioni AWS

Per i dettagli sulle CloudFormation risorse comunemente utilizzate nelle distribuzioni Windows basate, consulta i seguenti argomenti di riferimento tecnico.

Tipo di risorsa	Descrizione
AWS::EC2::Instance	Per avviare le istanze Windows EC2 .

Tipo di risorsa	Descrizione
AWS::EC2::SecurityGroup	Per definire le regole del firewall per Windows i carichi di lavoro.
AWS::AutoScaling::AutoScalingGroup (Gruppo)	Per scalare le istanze. Windows EC2
AWS::EC2::LaunchTemplate	
AWS::DirectoryService::MicrosoftAD	Per la distribuzione. Microsoft Active Directory
AWS::FSx::FileSystem	Per la distribuzione su Windows File FSx Server.
AWS::RDS::DBInstance	Per il provisioning SQL Server su Amazon RDS.
AWS::CloudFormation::Init	Utilizzato all'interno EC2 dei metadati per la configurazione delle istanze. Per ulteriori informazioni, consulta Stack basati sul bootstrap Windows CloudFormation .
AWS::SecretsManager::Secret	Per la gestione sicura di credenziali e password. Windows
AWS::SSM::Parameter	Per archiviare i valori di configurazione in modo sicuro.
AWS::IAM::InstanceProfile AWS::IAM::Role	Per concedere autorizzazioni alle applicazioni in esecuzione su istanze. EC2

Stack basati sul bootstrap Windows CloudFormation

Questo argomento descrive come avviare uno Windows stack e risolvere i problemi relativi alla creazione di uno stack.

Argomenti

- [EC2 Dati utente nelle istanze](#)
- [CloudFormation script di supporto](#)
- [Esempio di bootstrap di uno stack Windows](#)

- [Gestisci i servizi Windows](#)
- [Risolvi i problemi relativi alla creazione degli stack](#)

EC2 Dati utente nelle istanze

I dati utente sono una EC2 funzionalità di Amazon che consente di trasmettere script o informazioni di configurazione a un' EC2 istanza al momento dell'avvio.

Ad esempio Windows EC2 :

- I dati utente vengono eseguiti come script batch.
- È possibile utilizzare comandi batch (utilizzando `<script>` tag) o PowerShell script (utilizzando `<powershell>` tag).
- L'esecuzione degli script è gestita da EC2Launch

Important

Se stai creando la tua Windows AMI da utilizzare con CloudFormation, assicurati che la versione EC2Launch v2 sia configurata correttamente. EC2Launchv2 è necessaria per consentire agli strumenti di CloudFormation bootstrap di inizializzare e configurare Windows correttamente le istanze durante la creazione dello stack. Per ulteriori informazioni, consulta [Utilizzare l'agente EC2Launch v2 per eseguire attività durante l'avvio di un'istanza EC2 Windows](#) nella Amazon EC2 User Guide.

Per informazioni su AWS Windows AMIs, consulta l'[AWSWindowsAMI Reference](#).

CloudFormation script di supporto

Gli script di supporto sono utilità per la configurazione delle istanze durante il processo di bootstrap. Utilizzati con i dati EC2 degli utenti di Amazon, offrono potenti opzioni di configurazione.

CloudFormation fornisce i seguenti script di supporto in Python che puoi usare per installare software e avviare servizi su un' EC2 istanza Amazon che crei come parte del tuo stack:

- `cfn-init`— Utilizzabile per recuperare e interpretare i metadati delle risorse, installare pacchetti, creare file e avviare servizi.

- `cfn-signal`— Da utilizzare per segnalare con un `CreationPolicy` o `WaitCondition`, in modo da poter sincronizzare altre risorse nello stack quando la risorsa o l'applicazione prerequisita è pronta.
- `cfn-get-metadata`— Utilizzato per recuperare i metadati per una risorsa o il percorso verso una chiave specifica.
- `cfn-hup`— Utilizzato per verificare la presenza di aggiornamenti ai metadati ed eseguire hook personalizzati quando vengono rilevate modifiche.

Puoi chiamare gli script direttamente dal tuo modello. Lo script funziona in combinazione con i metadati delle risorse definiti nello stesso modello. Gli script vengono eseguiti sull' EC2istanza Amazon durante il processo di creazione dello stack.

Per ulteriori informazioni, consulta il riferimento agli [script di CloudFormation supporto nella Template Reference](#) Guide.AWS CloudFormation

Esempio di bootstrap di uno stack Windows

Esaminiamo frammenti di esempio di un modello di SharePoint server che esegue le seguenti azioni:

- Configura i file di inizializzazione: `cfn-credentials`, e. `cfn-hup.conf` `cfn-auto-reloader.conf`
- Scarica e installa un pacchetto come SharePoint Foundation sull'istanza del server.
- Utilizza `WaitCondition` a per garantire che le risorse siano pronte.
- Crea un utente e un gruppo di sicurezza IAM per l'accesso all'istanza.
- Recupera un IP per l'istanza con Amazon Elastic IP (EIP).

Lo script di `cfn-init` supporto viene utilizzato per eseguire ognuna di queste azioni, in base alle informazioni contenute nella `AWS::CloudFormation::Init` risorsa del modello.

La `AWS::CloudFormation::Init` sezione ha un nome `SharePointFoundation` e inizia con una dichiarazione standard:

```
"SharePointFoundation": {  
  "Type" : "AWS::EC2::Instance",  
  "Metadata" : {  
    "AWS::CloudFormation::Init" : {
```

```
"config" : {
```

Successivamente, `AWS::CloudFormation::Init` viene dichiarata la `files` sezione di:

```
"files" : {
  "c:\\cfn\\cfn-hup.conf" : {
    "content" : { "Fn::Join" : [ "", [
      "[main]\\n",
      "stack=", { "Ref" : "AWS::StackName" }, "\\n",
      "region=", { "Ref" : "AWS::Region" }, "\\n"
    ] ] }
  },
  "c:\\cfn\\hooks.d\\cfn-auto-reloader.conf" : {
    "content": { "Fn::Join" : [ "", [
      "[cfn-auto-reloader-hook]\\n",
      "triggers=post.update\\n",
      "path=Resources.SharePointFoundation.Metadata.AWS::CloudFormation::Init\\n",
      "action=cfn-init.exe -v -s ", { "Ref" : "AWS::StackName" },
      " -r SharePointFoundation",
      " --region ", { "Ref" : "AWS::Region" }, "\\n"
    ] ] }
  },
  "C:\\SharePoint\\SharePointFoundation2010.exe" : {
    "source" : "http://d3adzpja92utk0.cloudfront.net/SharePointFoundation.exe"
  }
},
```

Qui vengono creati tre file e collocati nella directory C:\cfn sull'istanza del server. Tali file sono:

- `cfn-hup.conf`, il file di configurazione per `cfn-hup`.
- `cfn-auto-reloader.conf`, il file di configurazione per l'hook utilizzato da `cfn-hup` per avviare un aggiornamento (chiamata `cfn-init`) quando i metadati contenuti cambiano.

```
AWS::CloudFormation::Init
```

È inoltre disponibile un file che viene scaricato nel server: `SharePointFoundation.exe`. Questo file viene utilizzato per l'installazione SharePoint sull'istanza del server.

 Important

Poiché i percorsi Windows utilizzano il carattere barra rovesciata ('\'), è necessario ricordarsi sempre di evitare correttamente tutte le barre rovesciate antepoendo un'altra

barra rovesciata ogni volta che si fa riferimento a un percorso nel modello. Windows CloudFormation

La prossima è la sezione, che sono i comandi. `commands cmd.exe`

```
"commands" : {
  "1-extract" : {
    "command" : "C:\\\\SharePoint\\\\SharePointFoundation2010.exe /extract:C:\\\\SharePoint\\
\\SPF2010 /quiet /log:C:\\\\SharePoint\\\\SharePointFoundation2010-extract.log"
  },
  "2-prereq" : {
    "command" : "C:\\\\SharePoint\\\\SPF2010\\\\PrerequisiteInstaller.exe /unattended"
  },
  "3-install" : {
    "command" : "C:\\\\SharePoint\\\\SPF2010\\\\setup.exe /config C:\\\\SharePoint\\\\SPF2010\\
\\Files\\\\SetupSilent\\\\config.xml"
  }
}
```

Poiché i comandi nell'istanza vengono elaborati in ordine alfabetico in base al nome, ogni comando è preceduto da un numero che indica l'ordine di esecuzione desiderato. Quindi, possiamo assicurarci che il pacchetto di installazione venga prima estratto, tutti i prerequisiti vengano quindi installati e infine che SharePoint venga avviata l'installazione di.

La prossima è la sezione `Properties`:

```
"Properties": {
  "InstanceType" : { "Ref" : "InstanceType" },
  "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" : "AWS::Region" },
    { "Fn::FindInMap" : [ "AWSInstanceType2Arch", { "Ref" :
"InstanceType" }, "Arch" ] } ] },
  "SecurityGroups" : [ {"Ref" : "SharePointFoundationSecurityGroup"} ],
  "KeyName" : { "Ref" : "KeyPairName" },
  "UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [
    "<script>\n",

    "cfn-init.exe -v -s ", { "Ref" : "AWS::StackName" },
    " -r SharePointFoundation",
    " --region ", { "Ref" : "AWS::Region" }, "\n",

    "cfn-signal.exe -e %ERRORLEVEL% ", { "Fn::Base64" : { "Ref" :
"SharePointFoundationWaitHandle" } }, "\n",
```

```

    "</script>"
  ]]]}
}

```

In questa sezione, la `UserData` proprietà contiene uno `cmd.exe` script che verrà eseguito da `cfn-init`, circondato da `<script>` tag. È possibile utilizzare uno Windows PowerShell script qui invece circondandolo di `<powershell>` tag. Per gli Windows stack, è necessario codificare nuovamente l'URL del gestore della condizione di attesa in base a 64.

`SharePointFoundationWaitHandle` è referenziato qui ed è eseguito con `cfn-signal`. `WaitConditionHandle` e associati `WaitCondition` vengono dichiarati di seguito nel modello:

```

"SharePointFoundationWaitHandle" : {
  "Type" : "AWS::CloudFormation::WaitConditionHandle"
},

"SharePointFoundationWaitCondition" : {
  "Type" : "AWS::CloudFormation::WaitCondition",
  "DependsOn" : "SharePointFoundation",
  "Properties" : {
    "Handle" : {"Ref" : "SharePointFoundationWaitHandle"},
    "Timeout" : "3600"
  }
}

```

Poiché l'esecuzione di tutti i passaggi e l'installazione SharePoint potrebbero richiedere del tempo, ma non un'ora intera, occorre `WaitCondition` attendere un'ora (3600 secondi) prima del timeout.

Se tutto va bene, viene utilizzato un IP elastico per fornire l'accesso all'istanza: SharePoint

```

"Outputs" : {
  "SharePointFoundationURL" : {
    "Value" : { "Fn::Join" : [ "", [ "http://", { "Ref" :
"SharePointFoundationEIP" } ] ] },
    "Description" : "SharePoint Team Site URL. Please retrieve Administrator password of
the instance and use it to access the URL"
  }
}

```

Una volta completata la creazione dello stack, l'indirizzo IP fornito da EIP verrà visualizzato nella scheda Output della console. CloudFormation Tuttavia, prima di poter accedere all'istanza, è

necessario recuperare la password di amministratore temporanea generata per l'istanza. Per ulteriori informazioni, consulta [Connect to your Windows instance using RDP](#) nella Amazon EC2 User Guide.

Gestisci i servizi Windows

WindowsI servizi vengono gestiti allo stesso modo dei servizi Linux, tranne per il fatto che si utilizza una windows chiave anzichésysvinit. L'esempio seguente avvia il cfn-hup servizio, lo imposta su Automatico e riavvia il servizio se cfn-init modifica i c:\cfn\hooks.d\cfn-auto-reloader.conf file c:\cfn\cfn-hup.conf o di configurazione.

```
"services" : {
  "windows" : {
    "cfn-hup" : {
      "enabled" : "true",
      "ensureRunning" : "true",
      "files" : ["c:\\cfn\\cfn-hup.conf", "c:\\cfn\\hooks.d\\cfn-auto-reloader.conf"]
    }
  }
}
```

È possibile gestire altri Windows servizi allo stesso modo utilizzando il nome, non il nome visualizzato, per fare riferimento al servizio.

Risolvi i problemi relativi alla creazione degli stack

Se lo stack fallisce durante la creazione, il comportamento predefinito prevede il rollback in caso di errore. Sebbene sia in genere una buona impostazione predefinita perché evita costi non necessari, rende difficile il debug del motivo dell'errore di creazione dello stack.

Per disattivare questo comportamento durante la creazione o l'aggiornamento dello stack con la CloudFormation console, scegli l'opzione Preserva risorse con successo nella sezione Opzioni di errore dello stack. Per ulteriori informazioni, consulta [Scegli come gestire gli errori durante il provisioning delle risorse](#). Ciò consente di accedere all'istanza e visualizzare i file di registro per individuare i problemi riscontrati durante l'esecuzione degli script di avvio.

Log importanti da guardare sono:

- Il log di EC2 configurazione all'indirizzo %ProgramData%\Amazon\EC2Launch\log\agent.log
- Il log cfn-init in C:\cfn\log\cfn-init.log

Per ulteriori log, consulta i seguenti argomenti nella Amazon EC2 User Guide:

- [EC2Launchstruttura delle cartelle](#)
- [EC2Launchstruttura delle cartelle v2](#)

Estendi le funzionalità del tuo modello con i CloudFormation tipi di risorse forniti

CloudFormation offre diversi tipi di risorse che puoi utilizzare nel tuo modello di stack per estenderne le funzionalità oltre a quelle di un semplice modello di stack.

Questi tipi di risorse includono:

Tipo di risorsa	Descrizione	Documentazione
Risorse personali zzate	Il tipo di <code>AWS::CloudFormation::CustomResource</code> risorsa consente di creare risorse personalizzate in grado di eseguire attività di approvvigionamento specifiche o includere risorse che non sono disponibili come tipi di CloudFormation risorse.	Risorse personali zzate
Macro	Il tipo di <code>AWS::CloudFormation::Macro</code> risorsa definisce un pezzo di codice riutilizzabile in grado di eseguire elaborazioni personalizzate sui CloudFormation modelli. Le macro possono modificare i modelli, generare risorse aggiuntive o eseguire altre operazioni personalizzate durante la creazione o gli aggiornamenti degli stack.	Macro di modello
Stack nidificati	Il tipo di <code>AWS::CloudFormation::Stack</code> risorsa consente di creare pile annidate all'interno dei CloudFormation modelli per architetture di stack più modulari e riutilizzabili.	Stack nidificati

Tipo di risorsa	Descrizione	Documentazione
StackSet	Il tipo di <code>AWS::CloudFormation::StackSet</code> risorsa crea o aggiorna a CloudFormation StackSet, che è un contenitore per stack che può essere distribuito su più regioni. Account AWS	Gestione degli stack con StackSets
Condizione di attesa	Il tipo di <code>AWS::CloudFormation::WaitCondition</code> risorsa sospende la creazione o l'aggiornamento dello stack finché non viene soddisfatta una condizione specifica, ad esempio il completamento con successo di un processo di lunga durata o la disponibilità di risorse esterne.	Condizioni di attesa
Attendi la gestione delle condizioni	Il tipo di <code>AWS::CloudFormation::WaitConditionHandle</code> risorsa interagisce con il tipo di <code>AWS::CloudFormation::WaitCondition</code> risorsa. Fornisce un URL predefinito che viene utilizzato per inviare segnali che indicano che è stata soddisfatta una condizione specifica. Questi segnali consentono di procedere con la creazione o l'aggiornamento dello stack.	Condizioni di attesa

Crea una logica di provisioning personalizzata con risorse personalizzate

Le risorse personalizzate consentono di scrivere una logica di provisioning personalizzata nei CloudFormation modelli e di CloudFormation eseguirla ogni volta che si crea, aggiorna (se è stata modificata la risorsa personalizzata) o si elimina uno stack. Ciò può essere utile quando i requisiti di provisioning coinvolgono logiche o flussi di lavoro complessi che non possono essere espressi con CloudFormation i tipi di risorse integrati.

Ad esempio, potresti voler includere risorse che non sono disponibili come tipi di CloudFormation risorse. Puoi includere tali risorse utilizzando le risorse personalizzate. In questo modo, puoi comunque gestire tutte le risorse correlate in un unico stack.

Per definire una risorsa personalizzata nel CloudFormation modello, si utilizza il tipo di [Custom::MyCustomResourceTypeName](#)risorsa [AWS::CloudFormation::CustomResource](#). Le risorse personalizzate richiedono una proprietà, il token di servizio, che specifica a dove vengono CloudFormation inviate le richieste, ad esempio un argomento Amazon SNS o una funzione Lambda.

I seguenti argomenti forniscono informazioni su come utilizzare le risorse personalizzate.

Argomenti

- [Funzionamento delle risorse personalizzate](#)
- [Timeout di risposta](#)
- [Risorse personalizzate supportate da Amazon SNS](#)
- [Risorse personalizzate supportate da Lambda](#)
- [Riferimento a risorse personalizzate](#)

Note

Il CloudFormation registro e le risorse personalizzate offrono ciascuno i propri vantaggi. Le risorse personalizzate offrono i seguenti vantaggi:

- Non è necessario registrare la risorsa.
- Puoi includere un'intera risorsa come parte di un modello senza registrarti.
- Supporta le Create operazioniUpdate, e Delete

I vantaggi offerti dalle risorse basate sul registro includono quanto segue:

- Supporta la modellazione, il provisioning e la gestione di risorse applicative di terze parti
- Supporta le operazioni CreateReadUpdate, Delete e List (CRUDL)
- Supporta il rilevamento della deriva su tipi di risorse private e di terze parti

A differenza delle risorse personalizzate, le risorse basate sul Registro di sistema non dovranno associare un argomento Amazon SNS o una funzione Lambda per eseguire operazioni CRUDL. Per ulteriori informazioni, consulta [Gestione delle estensioni con il CloudFormation registro](#).

Funzionamento delle risorse personalizzate

Il processo generale per la configurazione di una nuova risorsa personalizzata include i seguenti passaggi. Questi passaggi prevedono due ruoli: il fornitore di risorse personalizzate proprietario della risorsa personalizzata e lo sviluppatore del modello che crea un modello che include un tipo di risorsa personalizzato. Può trattarsi della stessa persona, ma in caso contrario, il fornitore di risorse personalizzate dovrebbe collaborare con lo sviluppatore del modello.

1. Il provider di risorse personalizzate scrive la logica che determina come gestire le richieste CloudFormation ed eseguire azioni sulla risorsa personalizzata.
2. Il provider di risorse personalizzato crea l'argomento Amazon SNS o la funzione Lambda a cui CloudFormation inviare richieste. L'argomento Amazon SNS o la funzione Lambda devono trovarsi nella stessa regione in cui verrà creato lo stack.
3. Il provider di risorse personalizzate fornisce l'argomento Amazon SNS ARN o l'ARN della funzione Lambda allo sviluppatore del modello.
4. Lo sviluppatore del modello definisce la risorsa personalizzata nel proprio modello. CloudFormation Ciò include un token di servizio e tutti i parametri dei dati di input. Il token di servizio e la struttura dei dati di input sono definiti dal fornitore di risorse personalizzato. Il token di servizio specifica l'argomento di Amazon SNS ARN o l'ARN della funzione Lambda ed è sempre obbligatorio, ma i dati di input sono facoltativi a seconda della risorsa personalizzata.

Ora, ogni volta che qualcuno utilizza il modello per creare, aggiornare o eliminare la risorsa personalizzata, CloudFormation invia una richiesta al token di servizio specificato e quindi attende una risposta prima di procedere con l'operazione stack.

Di seguito viene riepilogato il flusso per la creazione di uno stack dal modello:

1. CloudFormation invia una richiesta al token di servizio specificato. La richiesta include informazioni come il tipo di richiesta e un URL Amazon Simple Storage Service prefirato, a cui la risorsa personalizzata invia le risposte. Per ulteriori informazioni sugli elementi inclusi nella richiesta, consulta [Oggetti di richieste di risorse personalizzate](#).

I seguenti dati di esempio mostrano cosa CloudFormation include una Create richiesta. In questo esempio, `ResourceProperties` consente di CloudFormation creare un payload personalizzato da inviare alla funzione Lambda.

```
{  
  "RequestType" : "Create",
```

```
"ResponseURL" : "http://pre-signed-S3-url-for-response",
"StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
"RequestId" : "unique id for this create request",
"ResourceType" : "Custom::TestResource",
"LogicalResourceId" : "MyTestResource",
"ResourceProperties" : {
  "Name" : "Value",
  "List" : [ "1", "2", "3" ]
}
```

2. Il provider di risorse personalizzato elabora la CloudFormation richiesta e restituisce una risposta SUCCESS o FAILED all'URL prefirato. custom resource provider fornisce la risposta in un file in formato JSON e lo carica sull'URL S3 prefirato. Per ulteriori informazioni, consulta [Uploading objects with presigned URLs](#) nella Amazon Simple Storage Service User Guide.

Nella risposta, custom resource provider può anche includere coppie nome-valore a cui template developer può accedere. Ad esempio, la risposta può includere i dati di output nel caso in cui la richiesta sia andata a buon fine o un messaggio di errore nel caso in cui la richiesta abbia avuto esito negativo. Per ulteriori informazioni sulle risposte, consulta [Oggetti di risposta di risorse personalizzate](#).

Important

Se le coppie nome-valore contengono informazioni riservate, è necessario utilizzare il campo NoEcho per mascherare l'output della risorsa personalizzata. Altrimenti, i valori sono visibili attraverso i valori delle proprietà di APIs quella superficie (ad esempio DescribeStackEvents).

Per ulteriori informazioni sull'utilizzo per NoEcho mascherare informazioni riservate, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

custom resource provider è responsabile dell'ascolto e della risposta alla richiesta. Ad esempio, per le notifiche di Amazon SNS, il provider di risorse personalizzate deve ascoltare e rispondere alle notifiche inviate a un argomento specifico ARN. CloudFormation attende e ascolta una risposta nella posizione URL prefirata.

I seguenti dati di esempio mostrano ciò che una risorsa personalizzata può includere in una risposta:


```
{
  "Status" : "SUCCESS",
  "PhysicalResourceId" : "TestResource1",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "unique id for this create request",
  "LogicalResourceId" : "MyTestResource",
  "Data" : {
    "OutputName1" : "Value1",
    "OutputName2" : "Value2",
  }
}
```

3. Dopo aver ricevuto una SUCCESS risposta, CloudFormation procede con l'operazione stack. Se viene restituita una risposta FAILED o nessuna risposta, l'operazione ha esito negativo. Qualsiasi dato di output dalla risorsa personalizzata viene memorizzato nella posizione dell'URL prefissato. Lo sviluppatore del modello può recuperare tali dati utilizzando la funzione [Fn::GetAtt](#)

Note

Se lo utilizzi AWS PrivateLink, le risorse personalizzate nel VPC devono avere accesso a bucket S3 CloudFormation specifici. Le risorse personalizzate devono inviare le risposte a un Amazon S3 preregistrato. Se non possono inviare risposte ad Amazon S3, CloudFormation non riceveranno alcuna risposta e l'operazione di stack avrà esito negativo. Per ulteriori informazioni, consulta [Accesso CloudFormation tramite un endpoint di interfaccia \(AWS PrivateLink\)](#).

Timeout di risposta

Il timeout predefinito per la risorsa personalizzata è di 3600 secondi (1 ora). Se non viene ricevuta alcuna risposta durante questo periodo, l'operazione stack ha esito negativo.

È possibile modificare il valore di timeout in base al tempo previsto per la risposta della risorsa personalizzata. Ad esempio, quando si esegue il provisioning di una risorsa personalizzata che richiama una funzione Lambda che dovrebbe rispondere entro cinque minuti, è possibile impostare un timeout di cinque minuti nel modello dello stack specificando la proprietà `ServiceTimeout`. Per ulteriori informazioni, consulta [Oggetti di richieste di risorse personalizzate](#). In questo modo, se c'è un

errore nella funzione Lambda che la blocca, l'operazione stack CloudFormation fallirà dopo cinque minuti invece di attendere l'intera ora.

Tuttavia, fai attenzione a non impostare un valore di timeout troppo basso. Per evitare timeout imprevisti, assicurati che la risorsa personalizzata disponga di tempo sufficiente per eseguire le azioni necessarie e restituire una risposta.

Risorse personalizzate supportate da Amazon SNS

L'argomento seguente mostra come configurare una risorsa personalizzata con un token di servizio che specifica l'argomento Amazon SNS a CloudFormation cui inviare le richieste. Imparerai anche la sequenza di eventi e messaggi inviati e ricevuti a seguito della creazione, degli aggiornamenti e dell'eliminazione di stack di risorse personalizzati.

Con le risorse personalizzate e Amazon SNS, puoi abilitare scenari quali l'aggiunta di nuove risorse a uno stack e l'inserimento di dati dinamici in uno stack. Ad esempio, quando crei uno stack, CloudFormation puoi inviare una `Create` richiesta a un argomento monitorato da un'applicazione in esecuzione su un' EC2 istanza Amazon. La notifica Amazon SNS abilita le attività di provisioning aggiuntive nell'applicazione, come il recupero di un pool di indirizzi IP elastici consentiti. Al termine, l'applicazione invia una risposta (e tutti i dati di output) che notifica di CloudFormation procedere con l'operazione di stack.

Quando specifichi un argomento Amazon SNS come destinazione di una risorsa personalizzata, CloudFormation invia messaggi all'argomento SNS specificato durante le operazioni di stack che coinvolgono la risorsa personalizzata. Per elaborare questi messaggi ed eseguire le azioni necessarie, è necessario disporre di un endpoint supportato sottoscritto all'argomento SNS.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#). Per informazioni su Amazon SNS e sul suo funzionamento, consulta la [Amazon Simple Notification Service Developer Guide](#).

Utilizzo di Amazon SNS per creare risorse personalizzate

Argomenti

- [Fase 1: creazione dello stack](#)
- [Fase 2: aggiornamenti degli stack](#)
- [Fase 3: eliminazione dello stack](#)

Fase 1: creazione dello stack

1. Lo sviluppatore del modello crea uno CloudFormation stack che contiene una risorsa personalizzata.

Nell'esempio di modello riportato di seguito, utilizziamo il nome del tipo di risorsa personalizzato `Custom::SeleniumTester` per la risorsa personalizzata con ID `MySeleniumTest` logico. I nomi dei tipi di risorse personalizzate devono essere alfanumerici e possono avere una lunghezza massima di 60 caratteri.

Il tipo di risorsa personalizzato viene dichiarato con un token di servizio, proprietà opzionali specifiche del provider e GetAtt attributi facoltativi [Fn::](#) definiti dal provider di risorse personalizzato. Queste proprietà e questi attributi possono essere utilizzati per trasmettere le informazioni da template developer a custom resource provider e viceversa. Il token di servizio specifica un argomento di Amazon SNS configurato dal provider di risorse.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "MySeleniumTest" : {
      "Type": "Custom::SeleniumTester",
      "Version" : "1.0",
      "Properties" : {
        "ServiceToken": "arn:aws:sns:us-west-2:123456789012:CRTest",
        "seleniumTester" : "SeleniumTest()",
        "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/",
"http://search.mysite.com" ],
        "frequencyOfTestsPerHour" : [ "3", "2", "4" ]
      }
    }
  },
  "Outputs" : {
    "topItem" : {
      "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "resultsPage"] }
    },
    "numRespondents" : {
      "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "lastUpdate"] }
    }
  }
}
```

 Note

I nomi e i valori dei dati a cui si accede con `Fn::GetAtt` vengono restituiti dal provider di risorse personalizzato durante la risposta del provider a CloudFormation. Se custom resource provider è una terza parte, template developer deve ottenere i nomi dei valori restituiti da custom resource provider.

2. CloudFormation invia una notifica Amazon SNS al provider di risorse con una "RequestType" : "Create" che contiene informazioni sullo stack, le proprietà personalizzate delle risorse dal modello di stack e un URL S3 per la risposta.

L'argomento SNS che viene utilizzato per inviare la notifica è compreso nel modello della proprietà `ServiceToken`. Per evitare l'utilizzo di un valore hardcoded, un template developer può utilizzare un parametro del modello in modo che il valore venga inserito all'avvio dello stack.

Nel seguente esempio viene mostrata una richiesta Create della risorsa personalizzata contenente un nome di tipo risorsa personalizzato, `Custom::SeleniumTester`, creata con `LogicalResourceId` di `MySeleniumTester`:

```
{
  "RequestType" : "Create",
  "ResponseURL" : "http://pre-signed-S3-url-for-response",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "unique id for this create request",
  "ResourceType" : "Custom::SeleniumTester",
  "LogicalResourceId" : "MySeleniumTester",
  "ResourceProperties" : {
    "seleniumTester" : "SeleniumTest()",
    "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/", "http://
search.mysite.com" ],
    "frequencyOfTestsPerHour" : [ "3", "2", "4" ]
  }
}
```

Per informazioni dettagliate sull'oggetto della richiesta per le Create richieste, consulta l'argomento. [Crea una richiesta di risorse CloudFormation personalizzate](#)

3. Il custom resource provider elabora i dati inviati dallo template developer e determina se la richiesta Create è andata a buon fine. Il provider di risorse utilizza quindi l'URL S3 inviato da CloudFormation per inviare una risposta di SUCCESS o FAILED.

A seconda del tipo di risposta, possono essere visualizzati diversi campi in CloudFormation. Per informazioni sui campi di risposta per un particolare tipo di richiesta, consulta la documentazione relativa a quel tipo di richiesta nella [Tipi di richieste di risorse personalizzate](#) sezione.

In risposta a una richiesta di creazione o aggiornamento, il custom resource provider può restituire elementi di dati nel campo [Data](#) della risposta. Queste sono coppie nome/valore e i nomi corrispondono agli attributi Fn::GetAtt utilizzati con la risorsa personalizzata nel modello di stack. I valori sono i dati che vengono restituiti quando il template developer chiama Fn::GetAtt nella risorsa con il nome attributo.

Di seguito è riportato un esempio di risposta della risorsa personalizzata:

```
{
  "Status" : "SUCCESS",
  "PhysicalResourceId" : "Tester1",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "unique id for this create request",
  "LogicalResourceId" : "MySeleniumTester",
  "Data" : {
    "resultsPage" : "http://www.myexampledomain/test-results/guid",
    "lastUpdate" : "2012-11-14T03:30Z"
  }
}
```

Per informazioni dettagliate sull'oggetto di risposta per Create le richieste, consultate l'[Crea una richiesta di risorse CloudFormation personalizzate](#) argomento.

Nei campi StackId, RequestId e LogicalResourceId il testo della richiesta deve essere copiato parola per parola.

4. CloudFormation dichiara lo stato dello stack come CREATE_COMPLETE o. CREATE_FAILED Se lo stack è stato creato con successo, lo sviluppatore del modello può utilizzare i valori di output della risorsa personalizzata creata accedendovi con [Fn::GetAtt](#)

Ad esempio, il modello di risorsa personalizzata utilizzato per illustrazione usa Fn::GetAtt per copiare gli output delle risorse nell'output dello stack:

```
"Outputs" : {  
  "topItem" : {  
    "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "resultsPage"] }  
  },  
  "numRespondents" : {  
    "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "lastUpdate"] }  
  }  
}
```

Fase 2: aggiornamenti degli stack

Per aggiornare uno stack esistente, devi inviare un modello che specifichi gli aggiornamenti per le proprietà delle risorse dello stack, come illustrato nell'esempio seguente. CloudFormation aggiorna solo le risorse che hanno modifiche specificate nel modello. Per ulteriori informazioni, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

Puoi aggiornare le risorse personalizzate che richiedono una sostituzione della risorsa fisica sottostante. Quando aggiorni una risorsa personalizzata in un CloudFormation modello, CloudFormation invia una richiesta di aggiornamento a quella risorsa personalizzata. Se una risorsa personalizzata richiede una sostituzione, la nuova risorsa personalizzata deve inviare una risposta con il nuovo ID fisico. Quando CloudFormation riceve la risposta, confronta il valore di `PhysicalResourceId` della vecchia e della nuova risorsa personalizzata. Se sono diversi, CloudFormation riconosce l'aggiornamento come sostitutivo e invia una richiesta di eliminazione alla vecchia risorsa, come mostrato in [Fase 3: eliminazione dello stack](#).

Note

Se non hai apportato modifiche alla risorsa personalizzata, CloudFormation non le invierà richieste durante un aggiornamento dello stack.

1. Il template developer avvia un aggiornamento dello stack contenente una risorsa personalizzata. Durante l'esecuzione di un aggiornamento, lo template developer può specificare nuove proprietà nel modello di stack.

Di seguito è disponibile un esempio di `Update` del modello di stack tramite un tipo di risorsa personalizzata:

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "MySeleniumTest" : {
      "Type": "Custom::SeleniumTester",
      "Version" : "1.0",
      "Properties" : {
        "ServiceToken": "arn:aws:sns:us-west-2:123456789012:CRTest",
        "seleniumTester" : "SeleniumTest()",
        "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/",
          "http://search.mysite.com",
            "http://mynewsite.com" ],
        "frequencyOfTestsPerHour" : [ "3", "2", "4", "3" ]
      }
    }
  },
  "Outputs" : {
    "topItem" : {
      "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "resultsPage"] }
    },
    "numRespondents" : {
      "Value" : { "Fn::GetAtt" : ["MySeleniumTest", "lastUpdate"] }
    }
  }
}
```

2. CloudFormation invia una notifica Amazon SNS al provider di risorse con una "RequestType" : "Update" che contiene informazioni simili alla Create chiamata, tranne per il fatto che il `OldResourceProperties` campo contiene le vecchie proprietà della risorsa e `ResourceProperties` contiene le proprietà delle risorse aggiornate (se presenti).

Di seguito è riportato un esempio di richiesta Update:

```
{
  "RequestType" : "Update",
  "ResponseURL" : "http://pre-signed-S3-url-for-response",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "uniqueid for this update request",
  "LogicalResourceId" : "MySeleniumTester",
  "ResourceType" : "Custom::SeleniumTester",
  "PhysicalResourceId" : "Tester1",
```

```

"ResourceProperties" : {
  "seleniumTester" : "SeleniumTest()",
  "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/", "http://
search.mysite.com",
    "http://mynewsite.com" ],
  "frequencyOfTestsPerHour" : [ "3", "2", "4", "3" ]
},
"OldResourceProperties" : {
  "seleniumTester" : "SeleniumTest()",
  "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/", "http://
search.mysite.com" ],
  "frequencyOfTestsPerHour" : [ "3", "2", "4" ]
}
}

```

Per informazioni dettagliate sull'oggetto della richiesta per Update e le richieste, consulta l'[Richiesta di aggiornamento per risorse CloudFormation personalizzate](#) argomento.

3. Il provider di risorse personalizzate elabora i dati inviati da CloudFormation. La risorsa personalizzata esegue l'aggiornamento e invia una risposta SUCCESS o FAILED all'URL S3. CloudFormation quindi confronta le PhysicalResourceIDs vecchie e nuove risorse personalizzate. Se sono diverse, CloudFormation riconosce che l'aggiornamento richiede una sostituzione e invia una richiesta di eliminazione alla vecchia risorsa. L'esempio seguente mostra la risposta di un custom resource provider a una richiesta Update.

```

{
  "Status" : "SUCCESS",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "uniqueid for this update request",
  "LogicalResourceId" : "MySeleniumTester",
  "PhysicalResourceId" : "Tester2"
}

```

Per informazioni dettagliate sull'oggetto di risposta per Update e le richieste, consultate l'[Richiesta di aggiornamento per risorse CloudFormation personalizzate](#) argomento.

Nei campi StackId, RequestId e LogicalResourceId il testo della richiesta deve essere copiato parola per parola.

4. CloudFormation dichiara lo stato dello stack come UPDATE_COMPLETE o. UPDATE_FAILED. Se l'aggiornamento ha esito negativo, viene eseguito il rollback dello stack. Se lo stack è stato

aggiornato senza errori, il template developer può accedere ai nuovi valori di output delle risorse personalizzate create con `Fn::GetAtt`.

Fase 3: eliminazione dello stack

1. Il template developer elimina un aggiornamento dello stack contenente una risorsa personalizzata. CloudFormation ottiene le proprietà attuali specificate nel modello dello stack insieme all'argomento `SNS` e si prepara per effettuare una richiesta al provider di risorse personalizzate.
2. CloudFormation invia una notifica Amazon SNS al provider di risorse con una `"RequestType"` : `"Delete"` che contiene informazioni correnti sullo stack, le proprietà personalizzate delle risorse dal modello di stack e un URL S3 per la risposta.

Ogni volta che elimini uno stack o effettui un aggiornamento che rimuove o sostituisce la risorsa personalizzata, CloudFormation confronta le risorse personalizzate vecchie e nuove `PhysicalResourceId`. Se sono diverse, CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione per la vecchia risorsa (`OldPhysicalResource`), come illustrato nell'esempio seguente di richiesta. `Delete`

```
{
  "RequestType" : "Delete",
  "ResponseURL" : "http://pre-signed-S3-url-for-response",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "unique id for this delete request",
  "ResourceType" : "Custom::SeleniumTester",
  "LogicalResourceId" : "MySeleniumTester",
  "PhysicalResourceId" : "Tester1",
  "ResourceProperties" : {
    "seleniumTester" : "SeleniumTest()",
    "endpoints" : [ "http://mysite.com", "http://myecommercesite.com/", "http://search.mysite.com",
      "http://mynewsite.com" ],
    "frequencyOfTestsPerHour" : [ "3", "2", "4", "3" ]
  }
}
```

Per informazioni dettagliate sull'oggetto della richiesta per `Delete` le richieste, consultate [l'Eliminare la richiesta di risorse CloudFormation personalizzate](#) argomento.

`DescribeStackResource`, `DescribeStackResources` e `ListStackResources` mostrano il nome definito dall'utente se è stato specificato.

- Il provider di risorse personalizzate elabora i dati inviati da CloudFormation e determina se la `Delete` richiesta ha avuto esito positivo. Il provider di risorse utilizza quindi l'URL S3 inviato da CloudFormation per inviare una risposta di uno `SUCCESS` o `FAILED`. Per eliminare uno stack con una risorsa personalizzata, il custom resource provider deve rispondere a una richiesta di eliminazione.

Nel seguente esempio viene mostrata la risposta di un custom resource provider a una richiesta `Delete`:

```
{
  "Status" : "SUCCESS",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10",
  "RequestId" : "unique id for this delete request",
  "LogicalResourceId" : "MySeleniumTester",
  "PhysicalResourceId" : "Tester1"
}
```

Per informazioni dettagliate sull'oggetto di risposta per `Delete` le richieste, consultate l'[Eliminare la richiesta di risorse CloudFormation personalizzate](#) argomento.

Nei campi `StackId`, `RequestId` e `LogicalResourceId` il testo della richiesta deve essere copiato parola per parola.

- CloudFormation dichiara lo stato dello stack come `DELETE_COMPLETE` o `DELETE_FAILED`

Risorse personalizzate supportate da Lambda

Quando associ una funzione Lambda a una risorsa personalizzata, la funzione viene richiamata ogni volta che la risorsa personalizzata viene creata, aggiornata o eliminata. CloudFormation chiama un'API Lambda per richiamare la funzione e per trasmettere tutti i dati della richiesta (ad esempio il tipo di richiesta e le proprietà delle risorse) alla funzione. La potenza e la personalizzazione delle funzioni Lambda, combinate con, CloudFormation consentono un'ampia gamma di scenari, come la ricerca dinamica delle IDs AMI durante la creazione dello stack o l'implementazione e l'utilizzo di funzioni di utilità, come le funzioni di inversione delle stringhe.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#)

Argomenti

- [Procedura dettagliata: crea un meccanismo di ritardo con una risorsa personalizzata supportata da Lambda](#)
- [Modulo cfn-response](#)

Procedura dettagliata: crea un meccanismo di ritardo con una risorsa personalizzata supportata da Lambda

Questa procedura dettagliata mostra come configurare e avviare una risorsa personalizzata supportata da Lambda utilizzando un modello di esempio. CloudFormation Questo modello crea un meccanismo di ritardo che sospende le distribuzioni degli stack per un periodo di tempo specificato. Questo può essere utile quando è necessario introdurre ritardi intenzionali durante l'approvvigionamento delle risorse, ad esempio quando si attende che le risorse si stabilizzino prima che vengano create risorse dipendenti.

Note

Sebbene in precedenza le risorse personalizzate supportate da Lambda fossero consigliate per il recupero dell'AMI IDs, ora consigliamo di utilizzare i parametri. AWS Systems Manager Questo approccio rende i modelli più riutilizzabili e facili da gestire. Per ulteriori informazioni, consulta [Ottieni un valore in testo semplice da Systems Manager Parameter Store](#).

Argomenti

- [Panoramica](#)
- [Modello di esempio](#)
- [Procedura dettagliata del modello di esempio](#)
- [Prerequisiti](#)
- [Avvio dello stack](#)
- [Pulizia delle risorse](#)
- [Informazioni correlate](#)

Panoramica

Il modello di stack di esempio utilizzato in questa procedura dettagliata crea una risorsa personalizzata supportata da Lambda. Questa risorsa personalizzata introduce un ritardo configurabile (60 secondi per impostazione predefinita) durante la creazione dello stack. Il ritardo si verifica durante gli aggiornamenti dello stack solo quando le proprietà della risorsa personalizzata vengono modificate.

Il modello fornisce le seguenti risorse:

- una risorsa personalizzata,
- una funzione Lambda e
- un ruolo IAM che consente a Lambda di scrivere i log. CloudWatch

Definisce inoltre due uscite:

- Il tempo effettivo di attesa della funzione.
- Un identificatore univoco generato durante ogni esecuzione della funzione Lambda.

Note

CloudFormation è un servizio gratuito, ma Lambda addebita in base al numero di richieste per le funzioni e al tempo di esecuzione del codice. [Per ulteriori informazioni sui prezzi di Lambda, consulta AWS Lambda la pagina dei prezzi.](#)

Modello di esempio

Puoi vedere il modello di esempio di risorse personalizzate supportato da Lambda con il meccanismo di ritardo di seguito:

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "LambdaExecutionRole": {
      "Type": "AWS::IAM::Role",
```

```

    "Properties": {
      "AssumeRolePolicyDocument": {
        "Statement": [{
          "Effect": "Allow",
          "Principal": { "Service": ["lambda.amazonaws.com"] },
          "Action": ["sts:AssumeRole"]
        }]
      },
      "Path": "/",
      "Policies": [{
        "PolicyName": "AllowLogs",
        "PolicyDocument": {
          "Statement": [{
            "Effect": "Allow",
            "Action": ["logs:*"],
            "Resource": "*"
          }]
        }
      }]
    },
    "CFNWaiter": {
      "Type": "AWS::Lambda::Function",
      "Properties": {
        "Handler": "index.handler",
        "Runtime": "python3.9",
        "Timeout": 900,
        "Role": { "Fn::GetAtt": ["LambdaExecutionRole", "Arn"] },
        "Code": {
          "ZipFile": { "Fn::Join": ["\n", [
            "from time import sleep",
            "import json",
            "import cfnresponse",
            "import uuid",
            "",
            "def handler(event, context):",
            "    wait_seconds = 0",
            "    id = str(uuid.uuid1())",
            "    if event[\"RequestType\"] in [\"Create\", \"Update\"]:",
            "        wait_seconds = int(event[\"ResourceProperties\"].get(\"WaitSeconds\",
0))),",
            "        sleep(wait_seconds)",
            "        response = {",
            "            \"TimeWaited\": wait_seconds,",

```

```

        "    \"Id\": id ",
        "  }",
        "    cfnresponse.send(event, context, cfnresponse.SUCCESS, response,
\"Waiter-\"+id)"
      ]}]
    }
  },
  "CFNWaiterCustomResource": {
    "Type": "AWS::CloudFormation::CustomResource",
    "Properties": {
      "ServiceToken": { "Fn::GetAtt": ["CFNWaiter", "Arn"] },
      "WaitSeconds": 60
    }
  }
},
"Outputs": {
  "TimeWaited": {
    "Value": { "Fn::GetAtt": ["CFNWaiterCustomResource", "TimeWaited"] },
    "Export": { "Name": "TimeWaited" }
  },
  "WaiterId": {
    "Value": { "Fn::GetAtt": ["CFNWaiterCustomResource", "Id"] },
    "Export": { "Name": "WaiterId" }
  }
}
}
}

```

YAML

```

AWSTemplateFormatVersion: "2010-09-09"
Resources:
  LambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "lambda.amazonaws.com"
            Action:
              - "sts:AssumeRole"

```

```

    Path: "/"
    Policies:
      - PolicyName: "AllowLogs"
        PolicyDocument:
          Statement:
            - Effect: "Allow"
              Action:
                - "logs:*"
              Resource: "*"
CFNWaiter:
  Type: AWS::Lambda::Function
  Properties:
    Handler: index.handler
    Runtime: python3.9
    Timeout: 900
    Role: !GetAtt LambdaExecutionRole.Arn
    Code:
      ZipFile:
        !Sub |
        from time import sleep
        import json
        import cfnresponse
        import uuid

        def handler(event, context):
            wait_seconds = 0
            id = str(uuid.uuid1())
            if event["RequestType"] in ["Create", "Update"]:
                wait_seconds = int(event["ResourceProperties"].get("WaitSeconds", 0))
                sleep(wait_seconds)
            response = {
                "TimeWaited": wait_seconds,
                "Id": id
            }
            cfnresponse.send(event, context, cfnresponse.SUCCESS, response,
"Waiter-"+id)
  CFNWaiterCustomResource:
    Type: "AWS::CloudFormation::CustomResource"
    Properties:
      ServiceToken: !GetAtt CFNWaiter.Arn
      WaitSeconds: 60
Outputs:
  TimeWaited:
    Value: !GetAtt CFNWaiterCustomResource.TimeWaited

```

```

    Export:
      Name: TimeWaited
    WaiterId:
      Value: !GetAtt CFNWaiterCustomResource.Id
    Export:
      Name: WaiterId

```

Procedura dettagliata del modello di esempio

I seguenti frammenti spiegano le parti pertinenti del modello di esempio per aiutarti a capire come la funzione Lambda è associata a una risorsa personalizzata e a comprendere l'output.

[AWS::Lambda::Function](#) risorsa CFNWaiter

La `AWS::Lambda::Function` risorsa specifica il codice sorgente della funzione, il nome del gestore, l'ambiente di runtime e il ruolo di esecuzione Amazon Resource Name (ARN).

La `Handler` proprietà è impostata su `index.handler` poiché utilizza un codice sorgente Python. [Per ulteriori informazioni sugli identificatori di gestori accettati quando si utilizzano codici sorgente di funzioni in linea, vedere Code. AWS::Lambda::Function](#)

Il `Runtime` è specificato `python3.9` poiché il file sorgente è un codice Python.

`Timeout` È impostato su 900 secondi.

La `Role` proprietà utilizza la `Fn::GetAtt` funzione per ottenere l'ARN del ruolo di `LambdaExecutionRole` esecuzione dichiarato nella `AWS::IAM::Role` risorsa nel modello.

La `Code` proprietà definisce il codice della funzione in linea utilizzando una funzione Python. La funzione Python nel modello di esempio esegue le seguenti operazioni:

- Crea un ID univoco utilizzando l'UUID
- Controlla se la richiesta è una richiesta di creazione o aggiornamento
- Dormi per la durata specificata per `WaitSeconds` durante `Create` o `Update` richieste
- Restituisce il tempo di attesa e l'ID univoco

JSON

```

...
  "CFNWaiter": {
    "Type": "AWS::Lambda::Function",

```



```

"Properties": {
  "Handler": "index.handler",
  "Runtime": "python3.9",
  "Timeout": 900,
  "Role": { "Fn::GetAtt": ["LambdaExecutionRole", "Arn"] },
  "Code": {
    "ZipFile": { "Fn::Join": ["\n", [
      "from time import sleep",
      "import json",
      "import cfnresponse",
      "import uuid",
      "",
      "def handler(event, context):",
      "  wait_seconds = 0",
      "  id = str(uuid.uuid1())",
      "  if event[\"RequestType\"] in [\"Create\", \"Update\"]:",
      "    wait_seconds = int(event[\"ResourceProperties\"].get(\"WaitSeconds\",
0))),",
      "    sleep(wait_seconds)",
      "    response = {",
      "      \"TimeWaited\": wait_seconds,",
      "      \"Id\": id ",
      "    }",
      "    cfnresponse.send(event, context, cfnresponse.SUCCESS, response,
\"Waiter-\"+id)"
    ]]]
  }
},
...

```

YAML

```

...
CFNWaiter:
  Type: AWS::Lambda::Function
  Properties:
    Handler: index.handler
    Runtime: python3.9
    Timeout: 900
    Role: !GetAtt LambdaExecutionRole.Arn
    Code:
      ZipFile:

```

```

!Sub |
from time import sleep
import json
import cfnresponse
import uuid

def handler(event, context):
    wait_seconds = 0
    id = str(uuid.uuid1())
    if event["RequestType"] in ["Create", "Update"]:
        wait_seconds = int(event["ResourceProperties"].get("WaitSeconds", 0))
        sleep(wait_seconds)
    response = {
        "TimeWaited": wait_seconds,
        "Id": id
    }
    cfnresponse.send(event, context, cfnresponse.SUCCESS, response,
"Waiter-"+id)
...

```

[AWS::IAM::Role](#) risorsa LambdaExecutionRole

La `AWS::IAM::Role` risorsa crea un ruolo di esecuzione per la funzione Lambda, che include una politica di assunzione del ruolo che consente a Lambda di utilizzarla. Contiene anche una politica che consente l' CloudWatch accesso ai log.

JSON

```

...
"LambdaExecutionRole": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Statement": [{
        "Effect": "Allow",
        "Principal": { "Service": ["lambda.amazonaws.com"] },
        "Action": ["sts:AssumeRole"]
      }]
    },
    "Path": "/",
    "Policies": [{
      "PolicyName": "AllowLogs",

```

```

    "PolicyDocument": {
      "Statement": [{
        "Effect": "Allow",
        "Action": ["logs:*"],
        "Resource": "*"
      }]
    }
  }
},
...

```

YAML

```

...
LambdaExecutionRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "lambda.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    Path: "/"
    Policies:
      - PolicyName: "AllowLogs"
        PolicyDocument:
          Statement:
            - Effect: "Allow"
              Action:
                - "logs:*"
              Resource: "*"
...

```

[AWS::CloudFormation::CustomResource](#)risorsa CFNWaiterCustomResource

La risorsa personalizzata si collega alla funzione Lambda con il relativo ARN utilizzando. !

GetAtt CFNWaiter.Arn Implementerà un tempo di attesa di 60 secondi per le operazioni

di creazione e aggiornamento, come impostato. `WaitSeconds` La risorsa verrà richiamata per un'operazione di aggiornamento solo se le proprietà vengono modificate.

JSON

```
...
  "CFNWaiterCustomResource": {
    "Type": "AWS::CloudFormation::CustomResource",
    "Properties": {
      "ServiceToken": { "Fn::GetAtt": ["CFNWaiter", "Arn"] },
      "WaitSeconds": 60
    }
  },
  ...
```

YAML

```
...
CFNWaiterCustomResource:
  Type: "AWS::CloudFormation::CustomResource"
  Properties:
    ServiceToken: !GetAtt CFNWaiter.Arn
    WaitSeconds: 60
...
```

Outputs

Gli `Outputs` elementi di questo modello sono `TimeWaited` e `WaiterId`. Il `TimeWaited` valore utilizza una `Fn::GetAtt` funzione per fornire la quantità di tempo effettivamente attesa dalla risorsa cameriere. `WaiterId` Utilizza una `Fn::GetAtt` funzione per fornire l'ID univoco generato e associato all'esecuzione.

JSON

```
...
"Outputs": {
  "TimeWaited": {
    "Value": { "Fn::GetAtt": ["CFNWaiterCustomResource", "TimeWaited"] },
    "Export": { "Name": "TimeWaited" }
  }
}
```

```
    },
    "WaiterId": {
      "Value": { "Fn::GetAtt": ["CFNWaiterCustomResource", "Id"] },
      "Export": { "Name": "WaiterId" }
    }
  }
}
...

```

YAML

```
...
Outputs:
  TimeWaited:
    Value: !GetAtt CFNWaiterCustomResource.TimeWaited
    Export:
      Name: TimeWaited
  WaiterId:
    Value: !GetAtt CFNWaiterCustomResource.Id
    Export:
      Name: WaiterId
...

```

Prerequisiti

È necessario disporre delle autorizzazioni IAM per utilizzare tutti i servizi corrispondenti, come CloudFormation Lambda e.

Avvio dello stack

Per creare lo stack

1. Trova il modello che preferisci (YAML o JSON) dalla [Modello di esempio](#) sezione e salvalo sul tuo computer con il nome. `samplelambdabackedcustomresource.template`
2. Apri la console all' CloudFormation indirizzo. <https://console.aws.amazon.com/cloudformation/>
3. Nella pagina Pile, scegli Crea pila in alto a destra, quindi scegli Con nuove risorse (standard).
4. Per Prerequisito - Prepara modello, scegli Scegli un modello esistente.
5. Per Specificare il modello, scegli Carica un file modello, quindi scegli Scegli file.
6. Seleziona il file `samplelambdabackedcustomresource.template` modello che hai salvato in precedenza.

7. Scegli Next (Successivo).
8. Per il nome dello stack, digitate **SampleCustomResourceStack** e scegliete Avanti.
9. Per questa procedura guidata, non è necessario aggiungere tag o specificare impostazioni avanzate, quindi selezionare Next (Avanti).
10. Assicurati che il nome dello stack sia corretto, quindi scegli Crea.

La creazione dello stack potrebbe richiedere alcuni minuti. CloudFormation È possibile controllare l'avanzamento negli eventi per lo stack. Per ulteriori informazioni, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Se la creazione dello stack ha esito positivo, vengono create tutte le risorse dello stack, ad esempio la funzione Lambda e la risorsa personalizzata. Hai utilizzato correttamente una funzione Lambda e una risorsa personalizzata.

[Se la funzione Lambda restituisce un errore, visualizza i log della funzione nella CloudWatch console Logs](#). Il nome del flusso di log è l'ID fisico della risorsa personalizzata, che puoi trovare visualizzando le risorse dello stack. Per ulteriori informazioni, consulta [Visualizza i dati di log](#) nella Amazon CloudWatch User Guide.

Pulizia delle risorse

Elimina lo stack per cancellare tutte le risorse dello stack create in modo da non pagare per le risorse superflue.

Per eliminare lo stack

1. Dalla CloudFormation console, scegli lo SampleCustomResourceStackstack.
2. Scegliere Actions (Operazioni) e poi Delete Stack (Elimina stack).
3. Nel messaggio di conferma, scegliere Yes, Delete (Sì, elimina).

Tutte le risorse create vengono eliminate.

Ora che hai capito come creare e usare una risorsa personalizzata supportata da Lambda, puoi usare il modello e il codice di esempio di questa procedura dettagliata per creare e sperimentare altri stack e funzioni.

Informazioni correlate

- [CloudFormation Riferimento a risorse personalizzate](#)

- [AWS::CloudFormation::CustomResource](#)

Modulo **cfn-response**

Nel CloudFormation modello, puoi specificare una funzione Lambda come destinazione di una risorsa personalizzata. Quando si utilizza la `ZipFile` proprietà per specificare il codice sorgente [della funzione](#), è possibile caricare il `cfn-response` modulo per inviare risposte dalla funzione Lambda a una risorsa personalizzata. Il `cfn-response` modulo è una libreria che semplifica l'invio di risposte alla risorsa personalizzata che ha richiamato la funzione Lambda. Il modulo ha un `send` metodo che invia un [oggetto di risposta](#) a una risorsa personalizzata tramite un URL prefirmato Amazon S3 (the). `ResponseURL`

Il modulo `cfn-response` è disponibile solo quando si utilizza la proprietà `ZipFile` per scrivere il codice d'origine. Il modulo non è disponibile per il codice di origine archiviato in bucket Amazon S3. Per il codice nei bucket, è necessario scrivere funzioni proprie per inviare le risposte.

Note

Dopo l'esecuzione del metodo `send`, la funzione Lambda termina, perciò tutto quello che si scrive dopo quel metodo verrà ignorato.

Caricamento del modulo **cfn-response**

Per le funzioni Node.js, utilizza la funzione `require()` per caricare il modulo `cfn-response`. Ad esempio, il seguente esempio di codice crea un oggetto `cfn-response` con il nome `response`:

```
var response = require('cfn-response');
```

Per Python, utilizza l'istruzione `import` per caricare il modulo `cfnresponse`, come mostrato nel seguente esempio:

Note

Utilizzare questa istruzione di importazione esatta. Se si utilizzano altre varianti di istruzione di importazione, CloudFormation non include il modulo di risposta.

```
import cfnresponse
```

Parametri del metodo **send**

Si possono utilizzare i seguenti parametri con il metodo `send`:

`event`

I campi in una [richiesta di risorse personalizzata](#).

`context`

Un oggetto, specifico per le funzioni Lambda, che è possibile utilizzare per specificare quando la funzione e qualsiasi callback hanno completato l'esecuzione o per accedere alle informazioni dall'interno dell'ambiente di esecuzione Lambda. Per ulteriori informazioni, consulta [Creazione di funzioni Lambda con Node.js](#) nella AWS Lambda Developer Guide.

`responseStatus`

Se la funzione è stata completata. Utilizza le costanti del modulo `cfnresponse` per specificare lo stato: `SUCCESS` per esecuzioni di successo e `FAILED` per esecuzioni non riuscite.

`responseData`

Il campo `Data` di un [oggetto di risposta](#) della risorsa personalizzata. I dati corrispondono a un elenco di coppie nome-valore.

`physicalResourceId`

Facoltativo. L'ID univoco della risorsa personalizzata che ha invocato la funzione. Per impostazione predefinita, il modulo utilizza il nome del flusso di log di Amazon CloudWatch Logs associato alla funzione Lambda.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

`noEcho`

Facoltativo. Indica se nascondere o meno l'output della risorsa personalizzata quando viene recuperata utilizzando la funzione `Fn::GetAtt`. Se impostato su `true`, tutti i valori restituiti

vengono mascherati con asterischi (****), ad eccezione delle informazioni archiviate nelle posizioni specificate di seguito. Di default, il valore è `false`.

Important

L'utilizzo dell'attributo `NoEcho` non maschera le informazioni memorizzate nei seguenti elementi:

- La sezione dei Metadata modelli. CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per ulteriori informazioni, vedere [Metadati](#).
- Sezione dei modelli `Outputs`. Per ulteriori informazioni, consulta [Output](#).
- Attributo Metadata di una definizione di risorsa. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Si consiglia vivamente di non utilizzare questi meccanismi per includere informazioni sensibili, come password o segreti.

Per ulteriori informazioni sull'utilizzo per `NoEcho` mascherare informazioni riservate, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

Esempi

Node.js

In questo esempio Node.js, la funzione in linea Lambda utilizza un valore di input e lo moltiplica per 5. Le funzioni in linea sono particolarmente utili per le funzioni più piccole perché consentono di specificare il codice di origine direttamente nel modello, invece di creare un pacchetto e caricarlo in un bucket Amazon S3. La funzione utilizza il metodo `cfn-response send` per inviare il risultato alla risorsa personalizzata che la richiama.

JSON

```
"ZipFile": { "Fn::Join": ["", [  
  "var response = require('cfn-response');",  
  "exports.handler = function(event, context) {",  
    "  var input = parseInt(event.ResourceProperties.Input);",  
    "  var responseData = {Value: input * 5};",  
    "  response.send(event, context, response.SUCCESS, responseData);",  
  ]}] }
```

```
"};"
[]}]
```

YAML

```
ZipFile: >
  var response = require('cfn-response');
  exports.handler = function(event, context) {
    var input = parseInt(event.ResourceProperties.Input);
    var responseData = {Value: input * 5};
    response.send(event, context, response.SUCCESS, responseData);
  };
```

Python

In questo esempio Python, la funzione inline Lambda utilizza un valore intero e lo moltiplica per 5.

JSON

```
"ZipFile" : { "Fn::Join" : ["\n", [
  "import json",
  "import cfnresponse",
  "def handler(event, context):",
  "    responseValue = int(event['ResourceProperties']['Input']) * 5",
  "    responseData = {}",
  "    responseData['Data'] = responseValue",
  "    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,",
  "\"CustomResourcePhysicalID\"")
]]}
```

YAML

```
ZipFile: |
  import json
  import cfnresponse
  def handler(event, context):
    responseValue = int(event['ResourceProperties']['Input']) * 5
    responseData = {}
    responseData['Data'] = responseValue
    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
    "CustomResourcePhysicalID")
```

Codice di origine del modulo

Argomenti

- [Codice sorgente asincrono di Node.js](#)
- [Codice sorgente Node.js](#)
- [Codice sorgente Python](#)

Codice sorgente asincrono di Node.js

Di seguito è riportato il codice sorgente del modulo di risposta per le funzioni Node.js se il gestore è asincrono. Esaminarlo per comprendere ciò che il modulo fa e per facilitare l'implementazione di funzioni di risposta personalizzate.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: MIT-0

exports.SUCCESS = "SUCCESS";
exports.FAILED = "FAILED";

exports.send = function(event, context, responseStatus, responseData,
    physicalResourceId, noEcho) {

    return new Promise((resolve, reject) => {
        var responseBody = JSON.stringify({
            Status: responseStatus,
            Reason: "See the details in CloudWatch Log Stream: " +
context.logStreamName,
            PhysicalResourceId: physicalResourceId || context.logStreamName,
            StackId: event.StackId,
            RequestId: event.RequestId,
            LogicalResourceId: event.LogicalResourceId,
            NoEcho: noEcho || false,
            Data: responseData
        });

        console.log("Response body:\n", responseBody);

        var https = require("https");
        var url = require("url");

        var parsedUrl = url.parse(event.ResponseURL);
```

```

    var options = {
      hostname: parsedUrl.hostname,
      port: 443,
      path: parsedUrl.path,
      method: "PUT",
      headers: {
        "content-type": "",
        "content-length": responseBody.length
      }
    };

    var request = https.request(options, function(response) {
      console.log("Status code: " + parseInt(response.statusCode));
      resolve(context.done());
    });

    request.on("error", function(error) {
      console.log("send(..) failed executing https.request(..): " +
        maskCredentialsAndSignature(error));
      reject(context.done(error));
    });

    request.write(responseBody);
    request.end();
  })
}

function maskCredentialsAndSignature(message) {
  return message.replace(/X-Amz-Credential=[^\s]+/i, 'X-Amz-Credential=*****')
    .replace(/X-Amz-Signature=[^\s]+/i, 'X-Amz-Signature=*****');
}

```

Codice sorgente Node.js

Di seguito è riportato il codice sorgente del modulo di risposta per le funzioni Node.js se il gestore non è asincrono. Esaminarlo per comprendere ciò che il modulo fa e per facilitare l'implementazione di funzioni di risposta personalizzate.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: MIT-0

exports.SUCCESS = "SUCCESS";
exports.FAILED = "FAILED";

```

```
exports.send = function(event, context, responseStatus, responseData,
    physicalResourceId, noEcho) {

    var responseBody = JSON.stringify({
        Status: responseStatus,
        Reason: "See the details in CloudWatch Log Stream: " + context.logStreamName,
        PhysicalResourceId: physicalResourceId || context.logStreamName,
        StackId: event.StackId,
        RequestId: event.RequestId,
        LogicalResourceId: event.LogicalResourceId,
        NoEcho: noEcho || false,
        Data: responseData
    });

    console.log("Response body:\n", responseBody);

    var https = require("https");
    var url = require("url");

    var parsedUrl = url.parse(event.ResponseURL);
    var options = {
        hostname: parsedUrl.hostname,
        port: 443,
        path: parsedUrl.path,
        method: "PUT",
        headers: {
            "content-type": "",
            "content-length": responseBody.length
        }
    };

    var request = https.request(options, function(response) {
        console.log("Status code: " + parseInt(response.statusCode));
        context.done();
    });

    request.on("error", function(error) {
        console.log("send(..) failed executing https.request(..): " +
            maskCredentialsAndSignature(error));
        context.done();
    });

    request.write(responseBody);
```

```
request.end();  
}
```

Codice sorgente Python

Quanto segue è il codice sorgente del modulo di risposta per le funzioni Python:

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
# SPDX-License-Identifier: MIT-0  
  
from __future__ import print_function  
import urllib3  
import json  
import re  
  
SUCCESS = "SUCCESS"  
FAILED = "FAILED"  
  
http = urllib3.PoolManager()  
  
def send(event, context, responseStatus, responseData, physicalResourceId=None,  
        noEcho=False, reason=None):  
    responseUrl = event['ResponseURL']  
  
    responseBody = {  
        'Status' : responseStatus,  
        'Reason' : reason or "See the details in CloudWatch Log Stream:  
{}".format(context.log_stream_name),  
        'PhysicalResourceId' : physicalResourceId or context.log_stream_name,  
        'StackId' : event['StackId'],  
        'RequestId' : event['RequestId'],  
        'LogicalResourceId' : event['LogicalResourceId'],  
        'NoEcho' : noEcho,  
        'Data' : responseData  
    }  
  
    json_responseBody = json.dumps(responseBody)  
  
    print("Response body:")  
    print(json_responseBody)  
  
    headers = {  
        'content-type' : '',
```

```
        'content-length' : str(len(json_responseBody))
    }

    try:
        response = http.request('PUT', returnUrl, headers=headers,
                                body=json_responseBody)
        print("Status code:", response.status)

    except Exception as e:

        print("send(..) failed executing http.request(..):",
              mask_credentials_and_signature(e))

def mask_credentials_and_signature(message):
    message = re.sub(r'X-Amz-Credential=[^\s]+', 'X-Amz-Credential=*****', message,
                     flags=re.IGNORECASE)
    return re.sub(r'X-Amz-Signature=[^\s]+', 'X-Amz-Signature=*****', message,
                  flags=re.IGNORECASE)
```

Riferimento a risorse personalizzate

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Questa sezione fornisce informazioni su:

- I campi di richiesta e risposta JSON che vengono utilizzati in messaggi inviati da e verso CloudFormation quando viene fornita una risorsa personalizzata.
- I campi attesi per richieste e risposte per il custom resource provider in risposta a creazione, aggiornamento ed eliminazione dello stack.

Argomenti

- [Oggetti di richieste di risorse personalizzate](#)
- [Oggetti di risposta di risorse personalizzate](#)
- [Tipi di richieste di risorse personalizzate](#)

Oggetti di richieste di risorse personalizzate

Questo argomento descrive le proprietà dell'oggetto di richiesta per una risorsa CloudFormation personalizzata.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Proprietà delle richieste dello sviluppatore del modello

Lo sviluppatore del modello utilizza la CloudFormation risorsa [AWS::CloudFormation::CustomResource](#), per specificare una risorsa personalizzata in un modello.

In `AWS::CloudFormation::CustomResource`, tutte le proprietà vengono definite dal custom resource provider. C'è una sola proprietà obbligatoria: `ServiceToken`.

`ServiceTimeout`

Il tempo massimo, in secondi, che può trascorrere prima del timeout di un'operazione personalizzata su una risorsa.

Il valore deve essere un numero intero compreso tra 1 e 3600. Il valore predefinito è 3600 secondi (1 ora).

Required: No

Tipo: stringa

`ServiceToken`

Il token di servizio, ad esempio l'ARN di un argomento Amazon SNS o l'ARN della funzione Lambda. Il token di servizio deve provenire dalla stessa regione dello stack.

Campo obbligatorio: sì

Tipo: stringa

Tutti gli altri campi delle proprietà della risorsa sono opzionali e vengono inviati, testualmente, al custom resource provider nel campo `ResourceProperties` della richiesta. Il provider definisce i nomi e i contenuti validi di questi campi.

Campi delle richieste del provider di risorse personalizzate

Questi campi vengono inviati nelle richieste JSON CloudFormation al provider di risorse personalizzate nell'argomento SNS che il provider ha configurato per questo scopo.

RequestType

Il tipo di richiesta è impostato dall'operazione CloudFormation stack (create-stack, update-stack o delete-stack) avviata dallo sviluppatore del modello per lo stack che contiene la risorsa personalizzata.

Deve essere un valore tra: Create, Update o Delete. Per ulteriori informazioni, consulta [Tipi di richieste di risorse personalizzate](#).

Campo obbligatorio: sì

Tipo: stringa

ResponseURL

L'URL di risposta identifica un bucket S3 predefinito che riceve risposte dal fornitore di risorse personalizzato a. AWS CloudFormation

Campo obbligatorio: sì

Tipo: stringa

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata.

La combinazione di StackId con RequestId costituisce un valore che puoi utilizzare per identificare in modo univoco una richiesta in una particolare risorsa personalizzata.

Campo obbligatorio: sì

Tipo: stringa

RequestId

Un ID univoco per la richiesta.

La combinazione di StackId con RequestId costituisce un valore che puoi utilizzare per identificare in modo univoco una richiesta in una particolare risorsa personalizzata.

Campo obbligatorio: sì

Tipo: stringa

ResourceType

Il tipo di risorsa scelta dallo sviluppatore del modello della risorsa personalizzata nel modello CloudFormation . I nomi dei tipi di risorsa personalizzata possono contenere fino a 60 caratteri e possono includere caratteri alfanumerici, oltre ai caratteri seguenti: _@- .

Campo obbligatorio: sì

Tipo: stringa

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questa proprietà viene fornita per facilitare la comunicazione tra il provider di risorse personalizzate e il template developer.

Campo obbligatorio: sì

Tipo: stringa

PhysicalResourceId

Un ID fisico custom resource provider-defined richiesto che è univoco per quel fornitore.

Il valore restituito per un PhysicalResourceId può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

Obbligatorio: inviato sempre con le richieste Update e Delete e mai con Create.

Tipo: stringa

ResourceProperties

Questo campo contiene il contenuto dell'oggetto Properties inviato dal template developer. I suoi contenuti vengono definiti dal provider di risorse personalizzate.

Required: No

Tipo: JSON object

OldResourceProperties

Usato solo per le richieste Update. Contiene le proprietà delle risorse dichiarate prima della richiesta di aggiornamento.

Campo obbligatorio: sì

Tipo: JSON object

Oggetti di risposta di risorse personalizzate

Questo argomento descrive le proprietà dell'oggetto di risposta per una risorsa CloudFormation personalizzata.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Campi di risposta del provider di risorse personalizzate

Di seguito sono elencate le proprietà del provider di risorse personalizzate durante l'invio del file alla JSON all'URL prefissato. Per ulteriori informazioni sul caricamento di oggetti utilizzando presigned URLs, consulta [Uploading objects with presigned nella](#) Amazon URLs Simple Storage Service User Guide.

Note

La dimensione totale del corpo della risposta non può superare 4096 byte.

Status

Il valore di status inviato dal fornitore di risorse personalizzate in risposta a una richiesta generata. AWS CloudFormation

Deve essere SUCCESS o FAILED.

Campo obbligatorio: sì

Tipo: stringa

Reason

Descrive il motivo di una risposta con esito negativo.

Campo obbligatorio: richiesto se Status è FAILED. Altrimenti, è facoltativo.

Tipo: stringa

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un PhysicalResourceId può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

Campo obbligatorio: sì

Tipo: stringa

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

Campo obbligatorio: sì

Tipo: stringa

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

Campo obbligatorio: sì

Tipo: stringa

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

Campo obbligatorio: sì

Tipo: stringa

NoEcho

Facoltativo. Indica se nascondere o meno l'output della risorsa personalizzata quando viene recuperata utilizzando la funzione `Fn::GetAtt`. Se impostato su `true`, tutti i valori restituiti sono mascherati da asterischi (`*****`), ad eccezione di quelli memorizzati nella sezione del *Metadata* modello. AWS CloudFormation non trasforma, modifica o oscura le informazioni incluse nella sezione. Metadata Il valore predefinito è `false`.

Per ulteriori informazioni sull'utilizzo di NoEcho per mascherare le informazioni sensibili, consulta la best practice [Non incorporare le credenziali nei modelli](#).

Required: No

Tipo: Booleano

Data

Facoltativo. Le coppie nome-valore definite dal provider di risorse personalizzate da inviare con la risposta. Puoi accedere ai valori forniti qui in base al nome nel modello con `Fn::GetAtt`.

 Important

Se le coppie nome-valore contengono informazioni riservate, è necessario utilizzare il campo NoEcho per mascherare l'output della risorsa personalizzata. Altrimenti, i valori sono visibili attraverso API e valori delle proprietà della superficie (ad esempio `DescribeStackEvents`).

Required: No

Tipo: JSON object

Tipi di richieste di risorse personalizzate

Il tipo di richiesta viene inviato nel `RequestType` campo dell'[oggetto di richiesta](#) inviato da AWS CloudFormation quando lo sviluppatore del modello crea, aggiorna o elimina uno stack che contiene una risorsa personalizzata.

Ogni tipo di richiesta possiede uno specifico set di campi che viene inviato con la richiesta, tra cui un URL Amazon S3 per la risposta del provider di risorse personalizzate. Il provider deve rispondere al bucket S3 con un FAILED risultato SUCCESS or prima della fine del periodo di timeout. Se non viene ricevuta alcuna risposta prima della fine del periodo di timeout, la richiesta verrà considerata non riuscita e l'operazione di stack avrà esito negativo. Ogni risultato ha anche un particolare set di campi previsto da CloudFormation

Questa sezione fornisce informazioni sui campi di richiesta e risposta, con esempi per ogni tipo di richiesta.

Argomenti

- [Crea una richiesta di risorse CloudFormation personalizzate](#)
- [Eliminare la richiesta di risorse CloudFormation personalizzate](#)
- [Richiesta di aggiornamento per risorse CloudFormation personalizzate](#)

Crea una richiesta di risorse CloudFormation personalizzate

Quando lo sviluppatore del modello crea uno stack contenente una risorsa personalizzata, CloudFormation invia una richiesta al fornitore di risorse personalizzate con RequestType set to Create. Questa richiesta si verifica in particolare quando viene creata la risorsa personalizzata.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Richiesta

Le richieste di creazione contengono i seguenti campi:

RequestType

Create.

RequestId

Un ID univoco per la richiesta.

ResponseURL

L'URL di risposta identifica un bucket S3 predefinito che riceve risposte dal fornitore di risorse personalizzato a. AWS CloudFormation

ResourceType

Il tipo di risorsa scelta dallo sviluppatore del modello della risorsa personalizzata nel modello CloudFormation . I nomi dei tipi di risorsa personalizzata possono contenere fino a 60 caratteri e possono includere caratteri alfanumerici, oltre ai caratteri seguenti: _@-.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation .

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata.

ResourceProperties

Questo campo contiene il contenuto dell'oggetto `Properties` inviato dal template developer. I suoi contenuti vengono definiti dal provider di risorse personalizzate.

Esempio

```
{
  "RequestType" : "Create",
  "RequestId" : "unique id for this create request",
  "ResponseURL" : "pre-signed-url-for-create-response",
  "ResourceType" : "Custom::MyCustomResourceType",
  "LogicalResourceId" : "name of resource in template",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10",
  "ResourceProperties" : {
    "key1" : "string",
    "key2" : [ "list" ],
    "key3" : { "key4" : "map" }
  }
}
```

Risposte

Riuscito

Quando la richiesta di creazione viene completata, deve essere inviata una risposta al bucket Amazon S3 con i seguenti campi:

Status

Deve essere SUCCESS.

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

NoEcho

Facoltativo. Indica se nascondere o meno l'output della risorsa personalizzata quando viene recuperata utilizzando la funzione `Fn::GetAtt`. Se impostato su `true`, tutti i valori restituiti sono mascherati da asterischi (`*****`), ad eccezione di quelli memorizzati nella sezione del *Metadata* modello. AWS CloudFormation non trasforma, modifica o oscura le informazioni incluse nella sezione. *Metadata* Il valore predefinito è `false`.

Per ulteriori informazioni sull'utilizzo per `NoEcho` mascherare informazioni riservate, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

Data

Facoltativo. Le coppie nome-valore definite dal provider di risorse personalizzate da inviare con la risposta. Puoi accedere ai valori forniti qui in base al nome nel modello con `Fn::GetAtt`.

Important

Se le coppie nome-valore contengono informazioni riservate, è necessario utilizzare il campo `NoEcho` per mascherare l'output della risorsa personalizzata. Altrimenti, i valori sono visibili attraverso API e i valori delle proprietà della superficie (ad esempio `DescribeStackEvents`).

Esempio

```
{
  "Status" : "SUCCESS",
  "RequestId" : "unique id for this create request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "required vendor-defined physical id that is unique for that vendor",
  "Data" : {
    "keyThatCanBeUsedInGetAtt1" : "data for key 1",
    "keyThatCanBeUsedInGetAtt2" : "data for key 2"
  }
}
```

Non riuscito

Quando la richiesta di creazione non riesce, deve essere inviata una risposta al bucket S3 con i seguenti campi:

Status

Deve essere `FAILED`.

Reason

Descrive il motivo di una risposta con esito negativo.

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

Esempio

```
{
  "Status" : "FAILED",
  "Reason" : "Required failure reason string",
  "RequestId" : "unique id for this create request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "required vendor-defined physical id that is unique for that vendor"
}
```

Eliminare la richiesta di risorse CloudFormation personalizzate

Quando lo sviluppatore del modello elimina lo stack o rimuove la risorsa personalizzata dallo stack, CloudFormation invia una richiesta al fornitore di risorse personalizzate con `RequestType` set to `Delete`. Per eliminare uno stack con una risorsa personalizzata, il custom resource provider deve rispondere a una richiesta di eliminazione.

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#)

Richiesta

Le richieste di eliminazione contengono i seguenti campi:

`RequestType`

`Delete`.

`RequestId`

Un ID univoco per la richiesta.

`ResponseURL`

L'URL di risposta identifica un bucket S3 predefinito che riceve risposte dal fornitore di risorse personalizzato a. AWS CloudFormation

`ResourceType`

Il tipo di risorsa scelta dallo sviluppatore del modello della risorsa personalizzata nel modello CloudFormation . I nomi dei tipi di risorsa personalizzata possono contenere fino a 60 caratteri e possono includere caratteri alfanumerici, oltre ai caratteri seguenti: `_@-`.

`LogicalResourceId`

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation .

`StackId`

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata.

`PhysicalResourceId`

Un ID fisico custom resource provider-defined richiesto che è univoco per quel fornitore.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

ResourceProperties

Questo campo contiene il contenuto dell'oggetto `Properties` inviato dal template developer. I suoi contenuti vengono definiti dal provider di risorse personalizzate.

Esempio

```
{
  "RequestType" : "Delete",
  "RequestId" : "unique id for this delete request",
  "ResponseURL" : "pre-signed-url-for-delete-response",
  "ResourceType" : "Custom::MyCustomResourceType",
  "LogicalResourceId" : "name of resource in template",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10",
  "PhysicalResourceId" : "custom resource provider-defined physical id",
  "ResourceProperties" : {
    "key1" : "string",
    "key2" : [ "list" ],
    "key3" : { "key4" : "map" }
  }
}
```

Risposte

Riuscito

Quando la richiesta di eliminazione viene completata, una risposta deve essere inviata al bucket S3 con i seguenti campi:

Status

Deve essere SUCCESS.

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

Esempio

```
{
  "Status" : "SUCCESS",
  "RequestId" : "unique id for this delete request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "custom resource provider-defined physical id"
}
```

Non riuscito

Quando la richiesta di eliminazione non riesce, una risposta deve essere inviata al bucket S3 con i seguenti campi:

Status

Deve essere FAILED.

Reason

Il motivo dell'errore.

RequestId

Il valore RequestId copiato dalla [richiesta di eliminazione](#).

LogicalResourceId

Il valore LogicalResourceId copiato dalla [richiesta di eliminazione](#).

StackId

Il valore StackId copiato dalla [richiesta di eliminazione](#).

PhysicalResourceId

Un ID fisico definito dal provider di risorse personalizzate obbligatorio che è univoco per tale provider.

Esempio

```
{
  "Status" : "FAILED",
  "Reason" : "Required failure reason string",
  "RequestId" : "unique id for this delete request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "custom resource provider-defined physical id"
}
```

Richiesta di aggiornamento per risorse CloudFormation personalizzate

Quando lo sviluppatore del modello apporta modifiche alle proprietà di una risorsa personalizzata all'interno del modello e aggiorna lo stack, CloudFormation invia una richiesta al fornitore di risorse personalizzate con RequestType set to Update. Ciò significa che il codice di risorsa personalizzato non deve rilevare le modifiche nelle risorse perché sa che le sue proprietà sono cambiate in base al tipo di richiesta. Update

Per un'introduzione alle risorse personalizzate e al loro funzionamento, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Richiesta

Le richieste di aggiornamento contengono i seguenti campi:

RequestType

Update.

RequestId

Un ID univoco per la richiesta.

ResponseURL

L'URL di risposta identifica un bucket S3 predefinito che riceve risposte dal fornitore di risorse personalizzato a. AWS CloudFormation

ResourceType

Il tipo di risorsa scelta dallo sviluppatore del modello della risorsa personalizzata nel modello CloudFormation . I nomi dei tipi di risorsa personalizzata possono contenere fino a 60 caratteri e possono includere caratteri alfanumerici, oltre ai caratteri seguenti: _@-. Non puoi modificare il tipo durante un aggiornamento.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation .

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata.

PhysicalResourceId

Un ID fisico custom resource provider-defined richiesto che è univoco per quel fornitore.

Il valore restituito per un PhysicalResourceId può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

ResourceProperties

I nuovi valori delle proprietà delle risorse dichiarati dallo sviluppatore del modello nel CloudFormation modello aggiornato.

OldResourceProperties

I valori delle proprietà delle risorse precedentemente dichiarati dallo sviluppatore del modello nel CloudFormation modello.

Esempio

```
{
  "RequestType" : "Update",
  "RequestId" : "unique id for this update request",
  "ResponseURL" : "pre-signed-url-for-update-response",
  "ResourceType" : "Custom::MyCustomResourceType",
  "LogicalResourceId" : "name of resource in template",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10",
  "PhysicalResourceId" : "custom resource provider-defined physical id",
  "ResourceProperties" : {
    "key1" : "new-string",
    "key2" : [ "new-list" ],
    "key3" : { "key4" : "new-map" }
  },
  "OldResourceProperties" : {
    "key1" : "string",
    "key2" : [ "list" ],
    "key3" : { "key4" : "map" }
  }
}
```

Risposte

Riuscito

Se il provider di risorse personalizzate è in grado di aggiornare correttamente la risorsa, CloudFormation si aspetta che lo stato venga impostato su SUCCESS nella risposta.

Status

Deve essere SUCCESS.

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

NoEcho

Facoltativo. Indica se nascondere o meno l'output della risorsa personalizzata quando viene recuperata utilizzando la funzione `Fn::GetAtt`. Se impostato su `true`, tutti i valori restituiti sono mascherati da asterischi (`*****`), ad eccezione di quelli memorizzati nella sezione del *Metadata* modello. AWS CloudFormation non trasforma, modifica o oscura le informazioni incluse nella sezione. *Metadata* Il valore predefinito è `false`.

Per ulteriori informazioni sull'utilizzo per `NoEcho` mascherare informazioni riservate, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

Data

Facoltativo. Le coppie nome-valore definite dal provider di risorse personalizzate da inviare con la risposta. Puoi accedere ai valori forniti qui in base al nome nel modello con `Fn::GetAtt`.

 Important

Se le coppie nome-valore contengono informazioni riservate, è necessario utilizzare il campo `NoEcho` per mascherare l'output della risorsa personalizzata. Altrimenti, i valori sono visibili attraverso API e i valori delle proprietà della superficie (ad esempio `DescribeStackEvents`).

Esempio

```
{
  "Status" : "SUCCESS",
  "RequestId" : "unique id for this update request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "custom resource provider-defined physical id",
  "Data" : {
    "keyThatCanBeUsedInGetAtt1" : "data for key 1",
    "keyThatCanBeUsedInGetAtt2" : "data for key 2"
  }
}
```

Non riuscito

Se la risorsa non può essere aggiornata con un nuovo set di proprietà, CloudFormation si aspetta che lo stato venga impostato su `FAILED`, insieme a un motivo di errore nella risposta.

Status

Deve essere `FAILED`.

Reason

Descrive il motivo di una risposta con esito negativo.

RequestId

Un ID univoco per la richiesta. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

LogicalResourceId

Il nome (ID logico) scelto dallo sviluppatore del modello della risorsa personalizzata nel modello AWS CloudFormation . Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

StackId

Il nome della risorsa Amazon (ARN) che identifica lo stack che contiene la risorsa personalizzata. Questo valore di risposta deve essere copiato parola per parola dalla richiesta.

PhysicalResourceId

Questo valore deve essere un identificativo univoco per il fornitore di risorse personalizzate e può avere una dimensione massima di 1 KB. Il valore deve essere una stringa non vuota e deve essere identico per tutte le risposte per la stessa risorsa.

Il valore restituito per un `PhysicalResourceId` può modificare le operazioni personalizzate di aggiornamento delle risorse. Se il valore restituito è lo stesso, viene considerato un aggiornamento normale. Se il valore restituito è diverso, AWS CloudFormation riconosce l'aggiornamento come sostituto e invia una richiesta di eliminazione alla vecchia risorsa. Per ulteriori informazioni, consulta [AWS::CloudFormation::CustomResource](#).

Esempio

```
{
  "Status" : "FAILED",
  "Reason" : "Required failure reason string",
  "RequestId" : "unique id for this update request (copied from request)",
  "LogicalResourceId" : "name of resource in template (copied from request)",
  "StackId" : "arn:aws:cloudformation:us-west-2:123456789012:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10 (copied from request)",
  "PhysicalResourceId" : "custom resource provider-defined physical id"
}
```

Esegui elaborazioni personalizzate su CloudFormation modelli con macro di modelli

Con le macro, puoi eseguire elaborazioni personalizzate sui modelli, da azioni semplici come find-and-replace operazioni a trasformazioni estese di interi modelli.

Per avere un'idea della gamma di possibilità, prendete in considerazione le AWS::Serverless trasformazioni AWS::Include and, che sono macro ospitate da: CloudFormation

- [AWS::IncludeTransform](#) ti consente di inserire frammenti di template boilerplate nei tuoi modelli.
- [AWS::ServerlessTransform](#) prende un intero modello scritto nella sintassi AWS Serverless Application Model (AWS SAM) e lo trasforma e lo espande in un modello conforme. CloudFormation [Per ulteriori informazioni sulle applicazioni serverless e, consulta la Developer Guide. AWS SAMAWS Serverless Application Model](#)

Argomenti

- [Fatturazione](#)
- [Esempi di macro](#)
- [Risorse correlate](#)
- [Panoramica delle CloudFormation macro](#)
- [Creare una definizione di CloudFormation macro](#)
- [Esempio di semplice macro di sostituzione di stringhe](#)
- [Risolvi i problemi relativi al modello elaborato](#)

Fatturazione

Quando una macro viene eseguita, al proprietario della funzione Lambda vengono addebitati i costi relativi all'esecuzione di quella funzione.

Le AWS::Serverless trasformazioni AWS::Include e sono macro ospitate da. CloudFormation Il loro utilizzo non comporta alcun costo.

Esempi di macro

[Oltre agli esempi in questa sezione, nel nostro repository puoi trovare macro di esempio, tra cui codice sorgente e modelli. GitHub](#) Questi esempi vengono forniti "così come sono" per scopi didattici.

Risorse correlate

- [AWS::CloudFormation::Macro](#)

- [CloudFormation Transformazione sezione modello](#)
- [Fn::Transform](#)
- [Trasformazione AWS::Serverless](#)
- [Trasformazione AWS::Include](#)

Panoramica delle CloudFormation macro

L'elaborazione di modelli mediante macro comporta due fasi principali: la creazione della macro stessa e quindi l'utilizzo della macro per eseguire l'elaborazione sui modelli.

Per creare una definizione di macro, è necessario creare quanto segue:

- Una funzione Lambda per eseguire l'elaborazione del modello. Questa funzione Lambda accetta un frammento di modello o un intero modello e qualsiasi parametro supplementare che definisci. Restituisce quindi l'intero modello o il frammento di modello elaborato come risposta.
- Una risorsa di tipo [AWS::CloudFormation::Macro](#), che consente agli utenti di chiamare la funzione Lambda dall'interno CloudFormation dei modelli. Questa risorsa specifica l'ARN della funzione Lambda da richiamare per questa macro nonché ulteriori proprietà facoltative per facilitare il debug. Per creare questa risorsa all'interno di un account, crea un modello che includa la `AWS::CloudFormation::Macro` risorsa, quindi crea uno stack o un set di stack con le autorizzazioni gestite automaticamente dal modello. AWS CloudFormation StackSets attualmente non supporta la creazione o l'aggiornamento di set di stack con autorizzazioni gestite dai servizi da modelli che fanno riferimento alle macro.

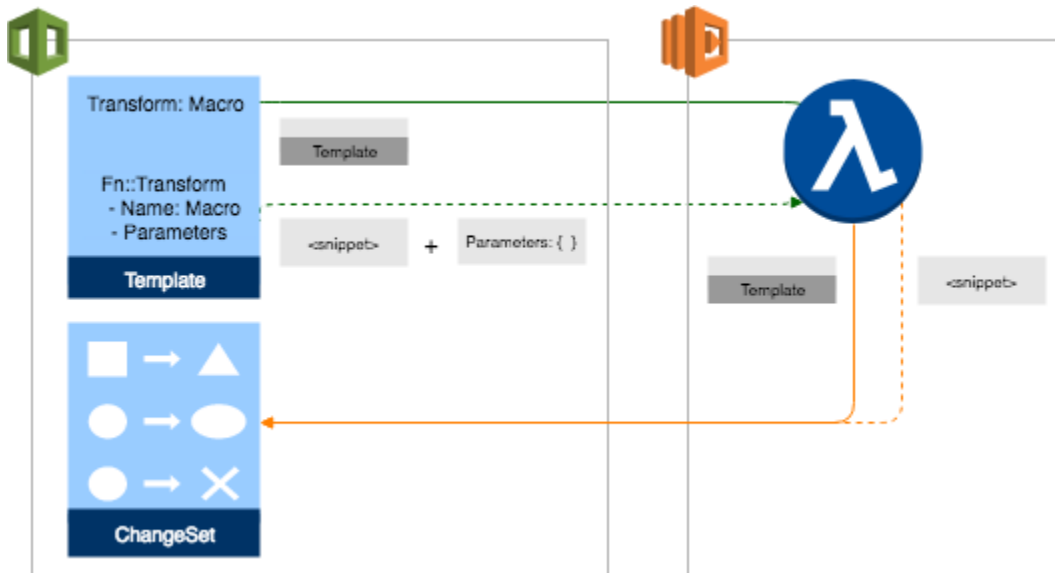
Per utilizzare una macro, fai riferimento alla macro nel modello:

- Per elaborare una sezione, o parte, di un modello, fate riferimento alla macro in una `Fn::Transform` funzione posizionata rispetto al contenuto del modello che desiderate trasformare. Quando utilizzi `Fn::Transform`, puoi anche passare qualsiasi parametro specificato di cui necessita.
- Per elaborare un intero modello, fai riferimento alla macro nella sezione [Transform](#) del modello.

Quindi, crea in genere un set di modifiche ed eseguilo. (L'elaborazione di macro può aggiungere molteplici risorse di cui potresti non essere a conoscenza. Per assicurarti di essere a conoscenza di tutte le modifiche introdotte dalle macro, ti consigliamo di utilizzare set di modifiche). CloudFormation passa il contenuto di modello specificato, insieme a eventuali altri parametri definiti, alla funzione

Lambda indicata nella risorsa di macro. La funzione Lambda restituisce il contenuto di modello elaborato, che si tratti di un frammento o di un intero modello.

Dopo aver richiamato tutte le macro del modello, CloudFormation genera un set di modifiche che include il contenuto del modello elaborato. Dopo aver esaminato il set di modifiche, esegui le modifiche.



Come creare pile direttamente

Per creare o aggiornare uno stack utilizzando un modello che fa riferimento a macro, crea un set di modifiche e quindi esegui. Un set di modifiche descrive le operazioni eseguite da CloudFormation in base al modello elaborato. L'elaborazione di macro può aggiungere molteplici risorse di cui potresti non essere a conoscenza. Per assicurarti di essere a conoscenza di tutte le modifiche introdotte dalle macro, ti consigliamo di utilizzare set di modifiche. Dopo aver esaminato il set di modifiche, puoi eseguirlo per applicare le modifiche.

Una macro può aggiungere risorse IAM al modello. Per queste risorse, CloudFormation richiede [l'accettazione delle funzionalità](#). Poiché non è CloudFormation possibile sapere quali risorse vengono aggiunte prima di elaborare il modello, potrebbe essere necessario riconoscere le funzionalità IAM al momento della creazione del set di modifiche, a seconda che le macro di riferimento contengano risorse IAM. In questo modo, quando si esegue il set di modifiche, CloudFormation dispone delle funzionalità necessarie per creare risorse IAM.

Per creare o aggiornare uno stack direttamente da un modello elaborato senza prima esaminare le modifiche proposte in un set di modifiche, specifica la `CAPABILITY_AUTO_EXPAND` funzionalità durante una `UpdateStack` richiesta `CreateStack` or. È sufficiente creare stack direttamente da un

modello di stack che contiene macro se si conosce l'elaborazione della macro. Non puoi utilizzare set di modifiche con macro di set di stack; è necessario aggiornare il set di stack direttamente.

Per ulteriori informazioni, consulta [CreateStack](#) o [UpdateStack](#) consulta l'AWS CloudFormation API Reference.

Important

Se il modello di set di stack contiene riferimenti a una o più macro, devi creare il set di stack direttamente dal modello elaborato, senza prima esaminare le modifiche risultanti in un set di modifiche. L'elaborazione di macro può aggiungere molteplici risorse di cui potresti non essere a conoscenza. Prima di creare o aggiornare un set di stack da un modello che fa riferimento direttamente alle macro, assicurarsi di sapere che elaborazione eseguono le macro.

Per ridurre il numero di passaggi necessari per l'avvio di stack a partire da modelli che fanno riferimento a macro, puoi utilizzare i package comandi `and. deploy` AWS CLI Per ulteriori informazioni, consultare [Carica gli artefatti locali in un bucket S3 con AWS CLI](#) e [Crea una pila che includa le trasformazioni](#).

Considerazioni

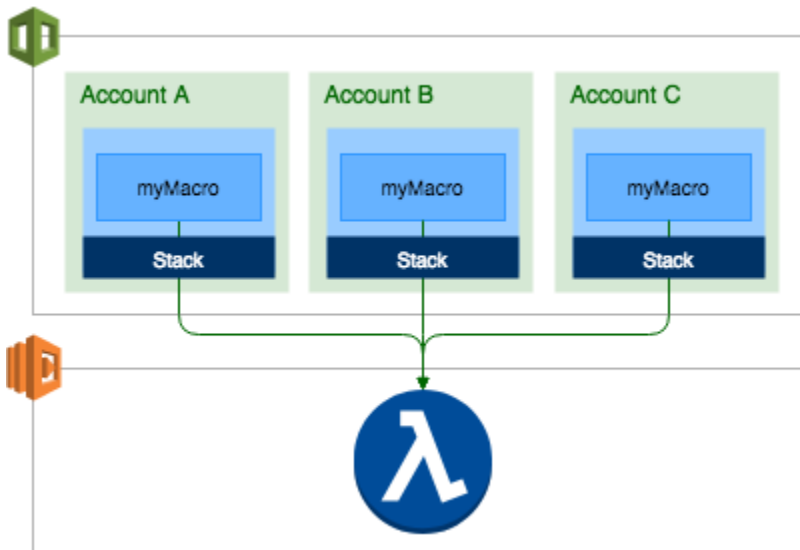
Quando lavorate con le macro, tenete presente le seguenti note e limitazioni:

- Le macro sono supportate solo Regioni AWS dove è disponibile Lambda. Per l'elenco delle Regioni in cui Lambda è disponibile, consulta l'argomento relativo a [endpoint e quote di AWS Lambda](#).
- Qualsiasi frammento di modello elaborato deve essere in formato JSON valido.
- Qualsiasi frammento di modello elaborato deve superare controlli di convalida per un'operazione di creazione o aggiornamento di stack e creazione o aggiornamento di set di stack.
- CloudFormation risolve prima le macro e poi elabora il modello. Il modello risultante deve essere in formato JSON valido e non deve superare il limite di dimensioni stabilito.
- A causa dell'ordine in cui CloudFormation elabora gli elementi di un modello, una macro non può includere moduli nel contenuto del modello elaborato a cui ritorna. CloudFormation Per ulteriori informazioni, consulta [Ordine di valutazione delle macro](#).
- Quando si utilizza la funzione di ripristino dell'aggiornamento, CloudFormation utilizza una copia del modello originale. Il rollback del modello originale viene eseguito anche se il frammento incluso è stato modificato.

- L'inclusione di macro all'interno delle macro non funziona perché non elaboriamo le macro in modo ricorsivo.
- La funzione intrinseca `Fn::ImportValue` non è attualmente supportata nelle macro.
- Le funzioni intrinseche incluse nel modello sono valutate dopo le macro. Pertanto, il contenuto di modello elaborato restituito dalla macro può includere chiamate alle funzioni intrinseche, che vengono valutate normalmente.
- StackSets attualmente non supporta la creazione o l'aggiornamento di set di stack con autorizzazioni gestite dai servizi da modelli che fanno riferimento alle macro. CloudFormation

Ambito e autorizzazioni dell'account macro

Puoi utilizzare le macro solo nell'account in cui sono state create come risorsa. Il nome della macro deve essere univoco in un determinato account. Tuttavia, puoi rendere disponibile la stessa funzionalità in vari account abilitando l'accesso tra più account sulla funzione Lambda sottostante e quindi creando definizioni di macro che fanno riferimento a quella funzione in molteplici account. Nell'esempio seguente, tre account contengono definizioni di macro che puntano alla stessa funzione Lambda.



Per creare una definizione di macro, l'utente deve disporre delle autorizzazioni per creare uno stack o set di stack nell'account specificato.

CloudFormation Per eseguire correttamente una macro inclusa in un modello, l'utente deve disporre delle Invoke autorizzazioni per la funzione Lambda sottostante. Per evitare un potenziale aumento delle autorizzazioni, CloudFormation impersona l'utente durante l'esecuzione della macro.

Per ulteriori informazioni, consulta la sezione [Gestione delle autorizzazioni AWS Lambda nella Guida per gli AWS Lambda sviluppatori](#) e [Azioni, risorse e chiavi di condizione nel Service Authorization Reference](#). AWS Lambda

Creare una definizione di CloudFormation macro

Quando si crea una definizione di macro, la definizione della macro rende disponibile la funzione Lambda sottostante nell'account specificato in modo che la CloudFormation richiami per elaborare i modelli.

Mappatura degli eventi

Quando CloudFormation richiama la funzione Lambda di una macro, invia una richiesta in formato JSON con la seguente struttura:

```
{
  "region" : "us-east-1",
  "accountId" : "$ACCOUNT_ID",
  "fragment" : { ... },
  "transformId" : "$TRANSFORM_ID",
  "params" : { ... },
  "requestId" : "$REQUEST_ID",
  "templateParameterValues" : { ... }
}
```

- **region**

La Regione in cui si trova la macro.

- **accountId**

L'ID account dell'account da cui la macro richiama la funzione Lambda.

- **fragment**

Il contenuto di modello disponibile per l'elaborazione personalizzata, in formato JSON.

- Per le macro incluse nella sezione `Transform` del modello, si tratta dell'intero modello tranne la sezione `Transform`.
- Per le macro incluse nella chiamata della funzione intrinseca `Fn::Transform`, include tutti i nodi di pari livello (e i relativi figli) in base alla posizione della funzione intrinseca nel modello ad eccezione della funzione `Fn::Transform`. Per ulteriori informazioni, consulta [Ambito del modello di macro](#).

- `transformId`

Il nome della macro che richiama questa funzione.

- `params`

Per le chiamate di `Fn::Transform` funzione, qualsiasi parametro specificato per la funzione. CloudFormation non valuta questi parametri prima di passarli alla funzione.

Per le macro incluse nella sezione `Transform` del modello, questa sezione è vuota.

- `requestId`

L'ID della richiesta che richiama questa funzione.

- `templateParameterValues`

Qualsiasi parametro specificato nella [Parameters](#) sezione del modello. CloudFormation valuta questi parametri prima di passarli alla funzione.

Formato della risposta

CloudFormation si aspetta che la funzione Lambda restituisca una risposta nel seguente formato JSON:

```
{
  "requestId" : "$REQUEST_ID",
  "status" : "$STATUS",
  "fragment" : { ... },
  "errorMessage": "optional error message for failures"
}
```

- `requestId`

L'ID della richiesta che richiama questa funzione. Deve corrispondere all'ID della richiesta fornito da CloudFormation quando si richiama la funzione.

- `status`

Lo stato della richiesta (senza distinzione tra maiuscole e minuscole). Dovrebbe essere impostato su. `success` CloudFormation considera ogni altra risposta come un fallimento.

- `fragment`

Il contenuto del modello elaborato CloudFormation da includere nel modello elaborato, inclusi i fratelli. CloudFormation sostituisce il contenuto del modello passato alla funzione Lambda con il frammento di modello che riceve nella risposta Lambda.

Il contenuto di modello elaborato deve essere in formato JSON valido e l'inclusione dello stesso nel modello elaborato deve generare un modello valido.

Se la funzione non modifica effettivamente il contenuto di modello che CloudFormation passa alla stessa, ma è ancora necessario includere quel contenuto nel modello elaborato, la funzione deve restituire quel contenuto a CloudFormation nella relativa risposta.

- `errorMessage`

Il messaggio di errore che spiega perché la trasformazione non è riuscita. CloudFormation visualizza questo messaggio di errore nel riquadro Eventi della pagina dei Dettagli dello stack per lo stack.

Per esempio:

```
Error creating change set: Transform
    Account AWS account
    number::macro name failed with:
    error message string.
```

Crea una definizione di macro

Per creare una definizione di CloudFormation macro

1. [Crea una funzione Lambda](#) che gestirà l'elaborazione dei contenuti del modello. Può elaborare qualsiasi parte di un modello, fino all'intero modello.
2. Crea un CloudFormation modello contenente un tipo di `AWS::CloudFormation::Macro` risorsa e specifica le `FunctionName` proprietà `Name` and. La `FunctionName` proprietà deve contenere l'ARN della funzione Lambda da richiamare quando viene eseguita la macro. CloudFormation
3. (Facoltativo) Per facilitare il debug, potete anche specificare le `LogRoleArn` proprietà `LogGroupName` and durante la creazione del tipo di risorsa per la `AWS::CloudFormation::Macro` macro. Queste proprietà consentono di specificare il gruppo di log CloudWatch Logs a cui CloudFormation inviare le informazioni di registrazione degli errori

quando si richiama la funzione Lambda sottostante della macro e il ruolo da CloudFormation assumere quando si inviano le voci di registro a tali registri.

4. [Crea uno stack](#) utilizzando il modello con la macro nell'account in cui desideri utilizzarlo. Oppure, [crea uno stack set con autorizzazioni autogestite](#) utilizzando il modello con la macro nell'account amministratore, quindi crea istanze stack negli account di destinazione.
5. Dopo aver CloudFormation creato con successo gli stack che contengono la definizione della macro, la macro è disponibile per l'uso all'interno di tali account. Puoi utilizzare una macro facendo riferimento alla stessa in un modello, nella posizione appropriata relativa al contenuto del modello che desideri elaborare.

Ambito del modello di macro

Le macro a cui si fa riferimento nella sezione Transform di un modello possono elaborare l'intero contenuto di quel modello.

Le macro a cui si fa riferimento in una funzione Fn::Transform possono elaborare il contenuto di qualsiasi elemento di pari livello (inclusi i figli) di quella funzione Fn::Transform nel modello.

Ad esempio, nell'esempio di modello seguente, AWS::Include può elaborare tutte le proprietà MyBucket in base alla posizione della funzione Fn::Transform che la contiene. MyMacro può elaborare il contenuto dell'intero modello per via della relativa inclusione nella sezione Transform.

```
# Start of processable content for MyMacro
AWSTemplateFormatVersion: 2010-09-09
Transform: [MyMacro]
Resources:
  WaitCondition:
    Type: AWS::CloudFormation::WaitCondition
  MyBucket:
    Type: AWS::S3::Bucket
    # Start of processable content for AWS::Include
    Properties:
      BucketName: amzn-s3-demo-bucket1
      Tags: [{"key": "value"}]
      'Fn::Transform':
        - Name: 'AWS::Include'
          Parameters:
            Location: s3://amzn-s3-demo-bucket2/MyFileName.yaml
      CorsConfiguration: []
    # End of processable content for AWS::Include
```

```
MyEc2Instance:
  Type: AWS::EC2::Instance
  Properties:
    ImageID: ami-1234567890abcdef0
# End of processable content for MyMacro
```

Ordine di valutazione delle macro

È possibile fare riferimento a più macro in un determinato modello, incluse le trasformazioni ospitate da CloudFormation, ad esempio [AWS::Include](#) e [AWS::Serverless](#)

Le macro vengono valutate nell'ordine, secondo la relativa posizione nel modello, da quella più nidificata a quella più generale. Le macro nella stessa posizione nel modello vengono valutate in serie in base all'ordine in cui sono elencate.

Le trasformazioni come `AWS::Include` e `AWS::Transform` vengono gestite come qualsiasi altra macro in termini di ordine e ambito dell'operazione.

Ad esempio, nell'esempio di modello riportato di seguito, CloudFormation valuta per prima cosa la `PolicyAdder` macro, perché è la macro con il nido più profondo del modello. CloudFormation quindi valuta `MyMacro` prima della valutazione `AWS::Serverless` perché è elencata in precedenza nella sezione `AWS::Serverless Transform`

```
AWSTemplateFormatVersion: 2010-09-09
Transform: [MyMacro, AWS::Serverless]
Resources:
  WaitCondition:
    Type: AWS::CloudFormation::WaitCondition
  MyBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      Tags: [{"key": "value"}]
      'Fn::Transform':
        - Name: PolicyAdder
      CorsConfiguration: []
  MyEc2Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageID: ami-1234567890abcdef0
```

Esempio di semplice macro di sostituzione di stringhe

L'esempio seguente illustra il processo di utilizzo delle macro, dalla definizione della macro in un modello, alla creazione di una funzione Lambda per la macro e quindi all'utilizzo della macro in un modello.

In questo esempio, creeremo una macro semplice che inserisce la stringa specificata al posto del contenuto di destinazione specificato nel modello elaborato. Quindi la utilizzeremo per inserire un campo `WaitHandleCondition` vuoto nella posizione specificata nel modello elaborato.

Creazione di una macro

Prima di utilizzare una macro, dobbiamo prima completare due operazioni: creare la funzione Lambda che esegue l'elaborazione del modello desiderata e quindi rendere disponibile tale funzione CloudFormation Lambda creando una definizione di macro.

L'esempio di modello seguente contiene la definizione del nostro esempio di macro. Per rendere disponibile la macro in uno specifico Account AWS, create uno stack dal modello. La definizione della macro specifica il nome della macro, una breve descrizione e fa riferimento all'ARN della funzione Lambda CloudFormation che viene richiamata quando questa macro viene utilizzata in un modello. (Non abbiamo incluso una `LogRoleARN` proprietà `LogGroupName` o per la registrazione degli errori.)

In questo esempio, supponiamo che lo stack creato da questo modello abbia un nome. `JavaMacroFunc` Poiché la `Name` proprietà macro è impostata sul nome dello stack, anche la macro risultante viene `JavaMacroFunc` denominata.

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Macro:
    Type: AWS::CloudFormation::Macro
    Properties:
      Name: !Sub '${AWS::StackName}'
      Description: Adds a blank WaitConditionHandle named WaitHandle
      FunctionName: 'arn:aws:lambda:us-east-1:012345678910:function:JavaMacroFunc'
```

Utilizzo della macro

Per utilizzare la nostra macro, la includiamo in un modello utilizzando la funzione `Fn::Transform` intrinseca.

Quando creiamo uno stack utilizzando il modello seguente, CloudFormation richiama la nostra macro di esempio. La funzione Lambda sottostante sostituisce una stringa specificata con un'altra stringa specificata. In questo caso, il risultato è una risorsa `AWS::CloudFormation::WaitConditionHandle` vuota che viene inserita nel modello elaborato.

```
Parameters:
  ExampleParameter:
    Type: String
    Default: 'SampleMacro'

Resources:
  2a:
    Fn::Transform:
      Name: "JavaMacroFunc"
      Parameters:
        replacement: 'AWS::CloudFormation::WaitConditionHandle'
        target: '$$REPLACEMENT$$'
      Type: '$$REPLACEMENT$$'
```

- La macro da richiamare è specificata come `JavaMacroFunc`, che proviene dal precedente esempio di definizione di macro.
- Alla macro vengono passati due parametri, `target` e `replacement`, che rappresentano la stringa di destinazione e il valore di sostituzione desiderato.
- La macro può funzionare sul contenuto del nodo `Type` in quanto `Type` è un elemento di pari livello della funzione `Fn::Transform` che fa riferimento alla macro.
- La risorsa `AWS::CloudFormation::WaitConditionHandle` risultante è denominata `2a`.
- Il modello contiene inoltre un parametro di modello, `ExampleParameter`, a cui la macro ha accesso (ma che non utilizza in questo caso).

Dati di input Lambda

Quando CloudFormation elabora il nostro modello di esempio durante la creazione dello stack, passa la seguente mappatura degli eventi alla funzione Lambda a cui si fa riferimento nella definizione della macro. `JavaMacroFunc`

- `region` : `us-east-1`
- `accountId` : `012345678910`
- `fragment` :

```
{
  "Type": "$$REPLACEMENT$$"
}
```

- `transformId` : 012345678910::JavaMacroFunc
- `params` :

```
{
  "replacement": "AWS::CloudFormation::WaitConditionHandle",
  "target": "$$REPLACEMENT$$"
}
```

- `requestId` : 5dba79b5-f117-4de0-9ce4-d40363bfb6ab
- `templateParameterValues` :

```
{
  "ExampleParameter": "SampleMacro"
}
```

fragment contiene codice JSON che rappresenta il frammento di modello che la macro può elaborare. Questo frammento comprende elementi di pari livello della chiamata di funzione `Fn::Transform`, ma non la chiamata stessa. Inoltre, `params` contiene codice JSON che rappresenta i parametri di macro. In questo caso, sostituzione e destinazione. Analogamente, `templateParameterValues` contiene codice JSON che rappresenta i parametri specificati per il modello nel complesso.

Codice funzione Lambda

Di seguito è riportato il codice effettivo per la funzione Lambda alla base della macro di `JavaMacroFunc` esempio. L'esempio esegue l'iterazione del frammento di modello incluso nella risposta (che sia in un formato di stringa, elenco o mappa), alla ricerca della stringa di destinazione specificata. Se trova la stringa di destinazione specificata, la funzione Lambda sostituisce la stringa di destinazione con la stringa di sostituzione specificata. In caso contrario, la funzione lascia il frammento di modello invariato. Quindi, la funzione restituisce una mappa delle proprietà previste, illustrate in dettaglio di seguito, a CloudFormation.

```
package com.macroexample.lambda.demo;
```



```
import java.util.List;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.Map;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

public class LambdaFunctionHandler implements RequestHandler<Map<String, Object>,
    Map<String, Object>> {

    private static final String REPLACEMENT = "replacement";
    private static final String TARGET = "target";
    private static final String PARAMS = "params";
    private static final String FRAGMENT = "fragment";
    private static final String REQUESTID = "requestId";
    private static final String STATUS = "status";
    private static final String SUCCESS = "SUCCESS";
    private static final String FAILURE = "FAILURE";

    @Override
    public Map<String, Object> handleRequest(Map<String, Object> event, Context
context) {
        // TODO: implement your handler
        final Map<String, Object> responseMap = new HashMap<String, Object>();
        responseMap.put(REQUESTID, event.get(REQUESTID));
        responseMap.put(STATUS, FAILURE);
        try {
            if (!event.containsKey(PARAMS)) {
                throw new RuntimeException("Params are required");
            }

            final Map<String, Object> params = (Map<String, Object>) event.get(PARAMS);
            if (!params.containsKey(REPLACEMENT) || !params.containsKey(TARGET)) {
                throw new RuntimeException("replacement or target under Params are
required");
            }

            final String replacement = (String) params.get(REPLACEMENT);
            final String target = (String) params.get(TARGET);
            final Object fragment = event.getOrDefault(FRAGMENT, new HashMap<String,
Object>());
            final Object retFragment;
            if (fragment instanceof String) {
                retFragment = iterateAndReplace(replacement, target, (String) fragment);
            }
        }
    }
}
```

```

        } else if (fragment instanceof List) {
            retFragment = iterateAndReplace(replacement, target, (List<Object>) fragment);
        } else if (fragment instanceof Map) {
            retFragment = iterateAndReplace(replacement, target, (Map<String, Object>)
fragment);
        } else {
            retFragment = fragment;
        }

        responseMap.put(STATUS, SUCCESS);
        responseMap.put(FRAGMENT, retFragment);
        return responseMap;
    } catch (Exception e) {
        e.printStackTrace();
        context.getLogger().log(e.getMessage());
        return responseMap;
    }
}

private Map<String, Object> iterateAndReplace(final String replacement, final
String target, final Map<String, Object> fragment) {
    final Map<String, Object> retFragment = new HashMap<String, Object>();
    final List<String> replacementKeys = new ArrayList<>();
    fragment.forEach((k, v) -> {
        if (v instanceof String) {
            retFragment.put(k, iterateAndReplace(replacement, target, (String)v));
        } else if (v instanceof List) {
            retFragment.put(k, iterateAndReplace(replacement, target, (List<Object>)v));
        } else if (v instanceof Map ) {
            retFragment.put(k, iterateAndReplace(replacement, target, (Map<String, Object>)
v));
        } else {
            retFragment.put(k, v);
        }
    });
    return retFragment;
}

private List<Object> iterateAndReplace(final String replacement, final String
target, final List<Object> fragment) {
    final List<Object> retFragment = new ArrayList<>();
    fragment.forEach(o -> {
        if (o instanceof String) {
            retFragment.add(iterateAndReplace(replacement, target, (String) o));
        } else if (o instanceof List) {

```

```

        retFragment.add(iterateAndReplace(replacement, target, (List<Object>) o));
    } else if (o instanceof Map) {
        retFragment.add(iterateAndReplace(replacement, target, (Map<String, Object>)
o));
    } else {
        retFragment.add(o);
    }
    });
    return retFragment;
}

private String iterateAndReplace(final String replacement, final String target,
final String fragment) {
    System.out.println(replacement + " == " + target + " == " + fragment );
    if (fragment != null AND_AND fragment.equals(target))
        return replacement;
    return fragment;
}
}

```

Risposta della funzione Lambda

Di seguito è riportata la mappatura a cui torna la funzione Lambda CloudFormation per l'elaborazione.

- `requestId` : 5dba79b5-f117-4de0-9ce4-d40363bfb6ab
- `status` : SUCCESS
- `fragment` :

```

{
  "Type": "AWS::CloudFormation::WaitConditionHandle"
}

```

Le `requestId` corrispondenze inviate da CloudFormation e il `status` valore di SUCCESS indicano che la funzione Lambda ha elaborato correttamente il frammento di modello incluso nella richiesta. In questa risposta, `fragment` contiene codice JSON che rappresenta il contenuto da inserire nel modello elaborato al posto del frammento del modello originale.

Modello elaborato risultante

Dopo aver CloudFormation ricevuto una risposta corretta dalla funzione Lambda, inserisce il frammento di modello restituito nel modello elaborato.

Di seguito è riportato il modello elaborato risultante per il nostro esempio. La chiamata alla funzione `Fn::Transform` intrinseca che faceva riferimento alla macro non è più `JavaMacroFunc` inclusa. Il frammento di modello restituito dalla funzione Lambda è incluso nella posizione appropriata, con il risultato che il contenuto `"Type": "$$REPLACEMENT$$"` è stato sostituito con `"Type": "AWS::CloudFormation::WaitConditionHandle"`.

```
{
  "Parameters": {
    "ExampleParameter": {
      "Default": "SampleMacro",
      "Type": "String"
    }
  },
  "Resources": {
    "2a": {
      "Type": "AWS::CloudFormation::WaitConditionHandle"
    }
  }
}
```

Risolvi i problemi relativi al modello elaborato

Quando si utilizza una macro, il modello elaborato è disponibile nella CloudFormation console.

La fase di un modello indica lo stato di elaborazione:

- **Original:** il modello che l'utente ha originariamente inviato per creare o aggiornare lo stack o set di stack.
- **Processed:** il modello CloudFormation utilizzato per creare o aggiornare lo stack o lo stack set dopo l'elaborazione di tutte le macro a cui si fa riferimento. Il modello elaborato è in formato JSON, anche se il modello originale è in formato YAML.

Per la risoluzione dei problemi, utilizzate il modello elaborato. Se un modello non fa riferimento a macro, il modello originale e quello elaborato sono identici.

Per ulteriori informazioni, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Per utilizzare il modello AWS CLI per ottenere il modello elaborato, usa il [get-template](#) comando.

Limitazione delle dimensioni

La dimensione massima per un modello di stack elaborato è di 51.200 byte quando viene passata direttamente a una richiesta `CreateStack`, `UpdateStack` o `ValidateTemplate`, oppure 1 MB quando viene passata come un oggetto S3 usando un URL del modello Amazon S3. Tuttavia, durante l'elaborazione CloudFormation aggiorna lo stato temporaneo del modello in quanto elabora in serie le macro contenute nel modello. Per questo motivo, le dimensioni del modello durante l'elaborazione possono temporaneamente superare le dimensioni consentite di un modello completamente elaborato. CloudFormation consente un certo buffer per questi modelli in corso di elaborazione. Tuttavia, è opportuno progettare i modelli e le macro tenendo presenti le dimensioni massime consentite per un modello di stack elaborato.

Se CloudFormation restituisce un `Transformation data limit exceeded` errore durante l'elaborazione del modello, significa che il modello ha superato la dimensione massima CloudFormation consentita durante l'elaborazione.

Per risolvere questo problema, valutare se eseguire le seguenti operazioni:

- Ristrutturare il modello in più modelli per evitare di superare le dimensioni massime per i modelli in corso di elaborazione. Ad esempio:
 - Utilizzare modelli di stack nidificati per incapsulare parti del modello. Per ulteriori informazioni, consulta [Dividi un modello in pezzi riutilizzabili usando pile annidate](#).
 - Creare più stack e utilizzare riferimenti tra stack per scambiare informazioni tra loro. Per ulteriori informazioni, consulta [Fai riferimento agli output di risorse in un altro stack CloudFormation](#).
- Ridurre la dimensione del frammento di modello restituito da una determinata macro.
CloudFormation non altera il contenuto dei frammenti restituiti dalle macro.

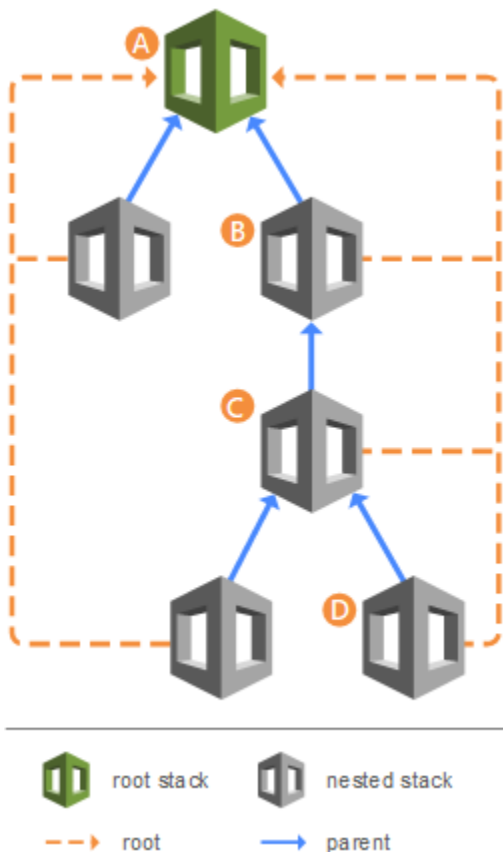
Dividi un modello in pezzi riutilizzabili usando pile annidate

Man mano che la tua infrastruttura cresce, potresti ritrovarti a creare ripetutamente configurazioni di risorse identiche su più modelli. Per evitare questa ridondanza, puoi separare queste configurazioni comuni in modelli dedicati. Quindi, puoi utilizzare la [AWS::CloudFormation::Stack](#) risorsa in altri modelli per fare riferimento a questi modelli dedicati, creando pile annidate.

Ad esempio, supponete di avere una configurazione di bilanciamento del carico che utilizzate per la maggior parte degli stack. Invece di copiare e incollare le stesse configurazioni nei modelli, puoi creare un modello dedicato per il sistema di load balancer. Quindi, puoi fare riferimento a questo modello all'interno di altri modelli che richiedono la stessa configurazione del load balancer.

Gli stack annidati possono a loro volta contenere altri stack nidificati, dando luogo a una gerarchia di pile, come illustrato nel diagramma seguente. Lo stack principale è lo stack di primo livello a cui appartengono in ultima analisi tutti gli stack nidificati. Ogni stack nidificato ha uno stack principale immediato. Per il primo livello di stack nidificati, lo stack principale è anche lo stack principale.

- Lo stack A è lo stack padre per tutti gli altri stack nidificati della gerarchia.
- Per lo stack B, lo stack A è sia lo stack padre che lo stack radice.
- Per lo stack D, lo stack C è lo stack padre; mentre per lo stack C, lo stack padre è lo stack B.



Argomenti

- [Esempio prima e dopo di suddivisione di un modello](#)
- [Esempio di architettura di stack annidati](#)

- [Esecuzione di operazioni di stack su stack annidati](#)
- [Informazioni correlate](#)

Esempio prima e dopo di suddivisione di un modello

Questo esempio dimostra come è possibile prendere un unico CloudFormation modello di grandi dimensioni e riorganizzarlo in un design più strutturato e riutilizzabile utilizzando modelli annidati. Inizialmente, il modello «Before nesting stacks» mostra tutte le risorse definite in un unico file. Questo può diventare complicato e difficile da gestire man mano che il numero di risorse aumenta. Il modello «After nesting stacks» suddivide le risorse in modelli più piccoli e separati. Ogni stack annidato gestisce un insieme specifico di risorse correlate, rendendo la struttura generale più organizzata e facile da gestire.

Prima di nidificare le pile	Dopo aver annidato le pile
<pre>AWSTemplateFormatVersion: 2010-09-09 Parameters: InstanceType: Type: String Default: t2.micro Description: The EC2 instance type Environment: Type: String Default: Production Description: The deployment environment Resources: MyEC2Instance: Type: AWS::EC2::Instance Properties: ImageId: ami-1234567890abcdef0 InstanceType: !Ref InstanceType MyS3Bucket: Type: AWS::S3::Bucket</pre>	<pre>AWSTemplateFormatVersion: 2010-09-09 Resources: MyFirstNestedStack: Type: AWS::CloudFormation::Stack Properties: TemplateURL: https://s3.amazonaws.com/ <i>amzn-s3-demo-bucket</i> /first-nested-stack.yaml Parameters: # Pass parameters to the nested stack if needed InstanceType: t3.micro MySecondNestedStack: Type: AWS::CloudFormation::Stack Properties: TemplateURL: https://s3.amazonaws.com/ <i>amzn-s3-demo-bucket</i> /second-nested-stack.yaml Parameters: # Pass parameters to the nested stack if needed Environment: Testing DependsOn: MyFirstNestedStack</pre>

Esempio di architettura di stack annidati

Questa sezione illustra un'architettura di stack nidificata costituita da uno stack di primo livello che fa riferimento a uno stack nidificato. Lo stack annidato implementa una funzione Lambda Node.js, riceve un valore di parametro dallo stack di primo livello e restituisce un output esposto attraverso lo stack di primo livello.

Argomenti

- [Passaggio 1: creare un modello per lo stack annidato sul sistema locale](#)
- [Fase 2: Creare un modello per lo stack di primo livello sul sistema locale](#)
- [Fase 3: Package e distribuzione dei modelli](#)

Passaggio 1: creare un modello per lo stack annidato sul sistema locale

L'esempio seguente mostra il formato del modello di stack annidato.

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Description: Nested stack template for Lambda function deployment
Parameters:
  MemorySize:
    Type: Number
    Default: 128
    MinValue: 128
    MaxValue: 10240
    Description: Lambda function memory allocation (128-10240 MB)
Resources:
  LambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Sub "${AWS::StackName}-Function"
      Runtime: nodejs18.x
      Handler: index.handler
      Role: !GetAtt LambdaExecutionRole.Arn
      Code:
        ZipFile: |
          exports.handler = async (event) => {
            return {
              statusCode: 200,
              body: JSON.stringify('Hello from Lambda!')
```



```

    };
  };
  MemorySize: !Ref MemorySize
  LambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  Outputs:
    LambdaArn:
      Description: ARN of the created Lambda function
      Value: !GetAtt LambdaFunction.Arn

```

Fase 2: Creare un modello per lo stack di primo livello sul sistema locale

L'esempio seguente mostra il formato del modello di stack di primo livello e la [AWS::CloudFormation::Stack](#) risorsa che fa riferimento allo stack creato nel passaggio precedente.

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Top-level stack template that deploys a nested stack
Resources:
  NestedStack:
    Type: AWS::CloudFormation::Stack
    Properties:
      TemplateURL: /path_to_template/nested-template.yaml
      Parameters:
        MemorySize: 256
  Outputs:
    NestedStackLambdaArn:
      Description: ARN of the Lambda function from nested stack
      Value: !GetAtt NestedStack.Outputs.LambdaArn

```

Fase 3: Package e distribuzione dei modelli

Note

Quando si lavora con i modelli a livello locale, il AWS CLI package comando può aiutarti a preparare i modelli per la distribuzione. Gestisce automaticamente il caricamento di elementi locali su Amazon S3 (TemplateURLincluso) e genera un nuovo file modello con riferimenti aggiornati a queste posizioni S3. Per ulteriori informazioni, consulta [Carica gli artefatti locali in un bucket S3 con AWS CLI](#).

Successivamente, puoi utilizzare il [package](#) comando per caricare il modello annidato in un bucket Amazon S3.

```
aws cloudformation package \  
  --s3-bucket amzn-s3-demo-bucket \  
  --template /path_to_template/top-level-template.yaml \  
  --output-template-file packaged-template.yaml \  
  --output json
```

Il comando genera un nuovo modello nel percorso specificato da. `--output-template-file`. Sostituisce il TemplateURL riferimento con la posizione Amazon S3, come illustrato di seguito.

Modello risultante

```
AWSTemplateFormatVersion: 2010-09-09  
Description: Top-level stack template that deploys a nested stack  
Resources:  
  NestedStack:  
    Type: AWS::CloudFormation::Stack  
    Properties:  
      TemplateURL: https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket/8b3bb7aa7abfc6e37e2d06b869484bed.template  
      Parameters:  
        MemorySize: 256  
Outputs:  
  NestedStackLambdaArn:  
    Description: ARN of the Lambda function from nested stack  
    Value:  
      Fn::GetAtt:  
        - NestedStack
```

- Outputs.LambdaArn

Dopo aver eseguito il `package` comando, puoi distribuire il modello elaborato utilizzando il comando [deploy](#). Per gli stack annidati che contengono risorse IAM, è necessario riconoscere le funzionalità IAM includendo l'opzione `--capabilities`.

```
aws cloudformation deploy \  
  --template-file packaged-template.yaml \  
  --stack-name stack-name \  
  --capabilities CAPABILITY_NAMED_IAM
```

Esecuzione di operazioni di stack su stack annidati

Quando si lavora con pile annidate, è necessario gestirle con attenzione durante le operazioni. Alcune operazioni relative agli stack, come gli aggiornamenti degli stack, devono essere avviate dallo stack principale anziché eseguite direttamente sugli stack nidificati. Quando aggiorni uno stack principale, verranno aggiornati solo gli stack nidificati con modifiche al modello.

Inoltre, la presenza degli stack annidati può influire sulle operazioni sullo stack principale. Ad esempio, se uno stack nidificato rimane bloccato nello `UPDATE_ROLLBACK_IN_PROGRESS` stato, lo stack principale aspetterà che lo stack nidificato completi il suo rollback prima di continuare. Prima di procedere con le operazioni di aggiornamento, assicurati di disporre delle autorizzazioni IAM per annullare un aggiornamento dello stack nel caso in cui venga ripristinato. Per ulteriori informazioni, consulta [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#).

Utilizza le seguenti procedure per trovare lo stack principale e gli stack annidati.

Per visualizzare lo stack radice di uno stack nidificato

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo / cloudformazione. `https://console.aws.amazon.com`](#)
2. Nella pagina Stacks, scegli il nome dello stack annidato di cui vuoi visualizzare lo stack principale.

Gli stack nidificati mostrano NESTED sopra il nome dello stack.

3. Nella scheda Informazioni sullo stack, nella sezione Panoramica, scegliete il nome dello stack elencato come Root stack.

Per visualizzare gli stack nidificati che appartengono a uno stack radice

1. Dalla pila principale di cui desideri visualizzare gli stack annidati, scegli la scheda Risorse.
2. Nella colonna Tipo, cerca risorse di tipo. `AWS::CloudFormation::Stack`

Informazioni correlate

- [Nidificazione di uno stack esistente](#)
- [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#)
- [Continua il rollback dopo gli aggiornamenti dello stack annidato non riusciti](#)
- [Errore di rollback degli stack annidati](#)

Creare condizioni di attesa in un CloudFormation modello

Questo argomento spiega come creare una condizione di attesa in un modello per coordinare la creazione di risorse dello stack o tenere traccia dell'avanzamento di un processo di configurazione. Ad esempio, puoi iniziare la creazione di un'altra risorsa al parziale completamento della configurazione di un'applicazione oppure puoi inviare segnali durante un processo di installazione e configurazione per monitorarne l'avanzamento.

Quando CloudFormation crea uno stack che include una condizione di attesa:

- Crea una condizione di attesa proprio come qualsiasi altra risorsa e imposta lo stato della condizione di attesa su `CREATE_IN_PROGRESS`.
- CloudFormation attende che riceva il numero richiesto di segnali di successo o che il periodo di timeout della condizione di attesa sia scaduto.
- Se riceve il numero richiesto di segnali di successo prima della scadenza del periodo di timeout:
 - Attendi che lo stato della condizione venga modificato in `CREATE_COMPLETE`
 - La creazione dello stack continua
- Se il timeout scade o viene ricevuto un segnale di errore:
 - Lo stato della condizione di attesa cambia in `CREATE_FAILED`
 - Stack torna indietro

Important

Per le risorse Amazon EC2 e Auto Scaling, ti consigliamo di utilizzare un CreationPolicy attributo anziché le condizioni di attesa. Aggiungi un CreationPolicy attributo a tali risorse e utilizza lo script di supporto cfn-signal per segnalare quando il processo di creazione di un'istanza è stato completato correttamente.

Per ulteriori informazioni, consulta [Attributo CreationPolicy](#).

Note

Se lo utilizzi AWS PrivateLink, le risorse nel VPC che rispondono alle condizioni di attesa devono avere accesso a bucket Amazon Simple Storage Service (Amazon S3) S3 CloudFormation specifici. Le risorse devono inviare le risposte della condizione di attesa a un URL Amazon S3 prefissato. Se non sono in grado di inviare risposte per Amazon S3, CloudFormation non riceverà una risposta e il funzionamento dello stack ha esito negativo. Per ulteriori informazioni, consulta [Accesso CloudFormation tramite un endpoint di interfaccia \(\)AWS PrivateLink](#) e [Controllo dell'accesso dagli endpoint VPC con policy bucket](#).

Argomenti

- [Creazione di una condizione di attesa nel modello](#)
- [Sintassi del segnale di condizione di attesa](#)
- [Accesso ai dati del segnale](#)

Creazione di una condizione di attesa nel modello

1. Maniglia delle condizioni di attesa

Si inizia definendo una [AWS::CloudFormation::WaitConditionHandle](#) risorsa nel modello dello stack. Questa risorsa genera l'URL predefinito necessario per l'invio di segnali. Ciò consente di inviare un segnale senza dover fornire AWS le proprie credenziali. Per esempio:

Resources:

MyWaitHandle:

Type: AWS::CloudFormation::WaitConditionHandle

2. Condizione di attesa

Successivamente, definisci una [AWS::CloudFormation::WaitCondition](#) risorsa nel modello dello stack. La struttura di base di `AWS::CloudFormation::WaitCondition` è la seguente:

```
MyWaitCondition:  
  Type: AWS::CloudFormation::WaitCondition  
  Properties:  
    Handle: String  
    Timeout: String  
    Count: Integer
```

La `AWS::CloudFormation::WaitCondition` risorsa ha due proprietà obbligatorie e una proprietà opzionale.

- `Handle`(obbligatorio) — Un riferimento a una `WaitConditionHandle` dichiarazione nel modello.
- `Timeout`(obbligatorio) — Il numero di secondi di attesa CloudFormation per la ricezione del numero richiesto di segnali. `Timeout` è una proprietà con limite minimo, il che significa che il timeout non si verifica prima del tempo specificato, ma può verificarsi poco dopo. Il tempo massimo che puoi specificare è 43200 secondi (12 ore).
- `Count`(opzionale) — Il numero di segnali di successo che CloudFormation devono essere ricevuti prima di impostare lo stato di quella condizione di attesa su `CREATE_COMPLETE` e riprendere la creazione dello stack. Se non specificato, il valore predefinito è 1.

In genere, si desidera che una condizione di attesa inizi immediatamente dopo la creazione di una risorsa specifica. A tale scopo, è necessario aggiungere l'`DependsOn` attributo a una condizione di attesa. Quando aggiungi un `DependsOn` attributo a una condizione di attesa, CloudFormation crea prima la risorsa nell'`DependsOn` attributo, quindi crea la condizione di attesa. Per ulteriori informazioni, consulta [Attributo DependsOn](#).

L'esempio seguente dimostra una condizione di attesa che:

- Inizia dopo la corretta creazione della risorsa `MyEC2Instance`
- Utilizza la `MyWaitHandle` risorsa come `WaitConditionHandle`
- Ha un timeout di 4500 secondi
- Ha il valore predefinito `Count` di 1 (poiché non è specificata alcuna `Count` proprietà)

MyWaitCondition:Type: `AWS::CloudFormation::WaitCondition`DependsOn: *MyEC2Instance*

Properties:

Handle: *!Ref MyWaitHandle*Timeout: *'4500'*

3. Invio di un segnale

Per segnalare l'esito positivo o negativo CloudFormation, in genere si esegue un codice o uno script. Ad esempio, un'applicazione in esecuzione su un' EC2 istanza potrebbe eseguire alcune attività di configurazione aggiuntive e quindi inviare un segnale CloudFormation a per indicare il completamento.

Il segnale deve essere inviato all'URL predefinito generato dal gestore della condizione di attesa. L'URL predefinito viene utilizzato per segnalare l'esito positivo o negativo.

Per inviare un segnale

1. Per recuperare l'URL predefinito all'interno del modello, utilizzate la funzione Ref intrinseca con il nome logico del gestore della condizione di attesa.

Come illustrato nell'esempio seguente, il modello può dichiarare un' EC2 istanza Amazon e passare l'URL predefinito alle EC2 istanze utilizzando la proprietà Amazon. EC2 UserData Ciò consente agli script o alle applicazioni in esecuzione su tali istanze di segnalare l'esito positivo o negativo di CloudFormation

MyEC2Instance:Type: `AWS::EC2::Instance`

Properties:

InstanceType: *t2.micro* # Example instance typeImageId: *ami-055e3d4f0bbeb5878* # Change this as needed (Amazon Linux 2023 in us-west-2)

UserData:

Fn::Base64:

Fn::Join:

- ""

- *"SignalURL="*- { "Ref": *"MyWaitHandle"* }

Ciò si traduce in un UserData output simile a:

```
SignalURL=https://amzn-s3-demo-bucket.s3.amazonaws.com/...
```

Nota: negli strumenti AWS Management Console e nella riga di comando, l'URL predefinito viene visualizzato come ID fisico della risorsa wait condition handle.

2. (Facoltativo) Per rilevare quando lo stack entra nella condizione di attesa, puoi utilizzare uno dei seguenti metodi:
 - Se crei lo stack con le notifiche abilitate, CloudFormation pubblica una notifica per ogni evento dello stack per l'argomento specificato. Se tu o l'applicazione effettua la sottoscrizione a tale argomento, puoi monitorare le notifiche relative all'evento di reazione degli handle delle condizioni di attesa e recuperare l'URL prefirato dal messaggio di notifica.
 - Puoi anche monitorare gli eventi dello stack utilizzando il AWS Management Console AWS CLI, il o un SDK.
3. Per inviare un segnale, invia un messaggio di richiesta HTTP utilizzando l'URL prefirato. Il metodo della richiesta deve essere PUT e l'intestazione Content-Type deve essere una stringa vuota o deve essere omessa. Il messaggio di richiesta deve essere una struttura JSON con il formato specificato nel [Sintassi del segnale di condizione di attesa](#).

È necessario inviare il numero di segnali di successo specificati dalla Count proprietà per CloudFormation continuare la creazione dello stack. Se il valore della proprietà Count è maggiore di 1, il valore UniqueId per ogni segnale deve essere univoco per tutti i segnali inviati a una determinata condizione di attesa. Il valore UniqueId è una stringa alfanumerica arbitraria.

Un comando curl è un modo per inviare un segnale. L'esempio seguente mostra una riga di comando curl che segnala l'operazione riuscita a una condizione di attesa.

```
$ curl -T /tmp/a \
  "https://amzn-s3-demo-bucket.s3.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-
  west-2%3A034017226601%3Astack%2Fstack-gosar-20110427004224-test-stack-with-
  WaitCondition--VEYW%2Fe498ce60-70a1-11e0-81a7-5081d0136786%2FmyWaitConditionHandle?
  Expires=1303976584&AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=ik1twT6hpS4cgNAw7wy0oRejVo
  %3D"
```

dove il file `/tmp/a` contiene la seguente struttura JSON:

```
{
  "Status" : "SUCCESS",
```



```

    "Reason" : "Configuration Complete",
    "UniqueId" : "ID1234",
    "Data" : "Application has completed configuration."
  }

```

Questo esempio illustra una riga di comando `curl` che invia lo stesso segnale di operazione riuscita, ma che invia la struttura JSON come parametro alla riga di comando.

```

$ curl -X PUT \
  -H 'Content-Type:' --data-binary '{"Status" : "SUCCESS", "Reason" : "Configuration Complete", "UniqueId" : "ID1234", "Data" : "Application has completed configuration."}' \
  "https://amzn-s3-demo-bucket.s3.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-west-2%3A034017226601%3Astack%2Fstack-gosar-20110427004224-test-stack-with-WaitCondition--VEYW%2Fe498ce60-70a1-11e0-81a7-5081d0136786%2FmyWaitConditionHandle?Expires=1303976584&AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=ik1twT6hpS4cgNAw7wy0oRejVo%3D"

```

Sintassi del segnale di condizione di attesa

Quando invii segnali all'URL generato dal gestore della condizione di attesa, devi utilizzare il seguente formato JSON:

```

{
  "Status" : "StatusValue",
  "UniqueId" : "Some UniqueId",
  "Data" : "Some Data",
  "Reason" : "Some Reason"
}

```

Proprietà

Il `Status` campo deve avere uno dei seguenti valori:

- SUCCESS
- FAILURE

Il `UniqueId` campo identifica il segnale per CloudFormation. Se la `Count` proprietà della condizione di attesa è maggiore di 1, il `UniqueId` valore deve essere unico per tutti i segnali inviati per una

particolare condizione di attesa; in caso contrario, CloudFormation considererà il segnale una ritrasmissione del segnale inviato in precedenza con lo stesso UniqueId e lo ignorerà.

Il Data campo può contenere tutte le informazioni che desideri inviare con il segnale. È possibile accedere al Data valore utilizzando la GetAtt funzione [Fn::](#) all'interno del modello.

Il Reason campo è una stringa senza altre restrizioni sul suo contenuto oltre alla conformità JSON.

Accesso ai dati del segnale

Per accedere ai dati inviati da segnali validi, puoi creare un valore di output per la condizione di attesa nel tuo CloudFormation modello. Per esempio:

Outputs:

WaitConditionData:

Description: *The data passed back as part of signalling the WaitCondition*

Value: *!GetAtt MyWaitCondition.Data*

È quindi possibile visualizzare questi dati utilizzando il [describe-stacks](#) comando o la scheda Output della CloudFormation console.

La Fn::GetAtt funzione restituisce UniqueId e Data come name/value coppia all'interno di una struttura JSON. Per esempio:

```
{"Signal1": "Application has completed configuration."}
```

Crea configurazioni di risorse riutilizzabili che possono essere incluse nei modelli con moduli CloudFormation

I moduli sono un modo per creare pacchetti di configurazioni delle risorse per l'inclusione su modelli di stack, in modo trasparente, gestibile e ripetibile. I moduli possono incapsulare configurazioni di servizio comuni e best practice come blocchi predefiniti modulari e personalizzabili da includere nei modelli di stack. I moduli consentono di includere configurazioni delle risorse che incorporano best practice, conoscenza esperta del settore e linee guida accettate (per ambiti quali sicurezza, conformità, governance e normative di settore) nei modelli, senza dover acquisire una conoscenza approfondita delle complessità dell'implementazione delle risorse.

Ad esempio, un esperto del settore nelle reti potrebbe creare un modulo contenente gruppi di sicurezza incorporati e regole di ingresso/uscita che rispettino le linee guida di sicurezza. Puoi quindi

includere quel modulo nel tuo modello per fornire un'infrastruttura di rete sicura nello stack, senza dover perdere tempo a capire come funzionano le sottoreti VPCs, i gruppi di sicurezza e i gateway. E poiché i moduli hanno più versioni, se le linee guida di sicurezza cambiano nel tempo, l'autore del modulo può creare una nuova versione del modulo che incorpora tali modifiche.

Le caratteristiche dell'utilizzo dei moduli nei modelli includono:

- **Prevedibilità:** un modulo deve rispettare lo schema che registra nel CloudFormation registro, in modo da sapere in quali risorse può risolversi una volta incluso nel modello.
- **Riusabilità:** puoi utilizzare lo stesso modulo su più modelli e account.
- **Tracciabilità:** CloudFormation conserva la conoscenza di quali risorse di uno stack sono state fornite da un modulo, consentendoti di comprendere facilmente l'origine delle modifiche alle risorse.
- **Gestibilità:** dopo aver registrato un modulo, è possibile gestirlo tramite il CloudFormation registro, compresi il controllo delle versioni e la disponibilità dell'account e a livello regionale.

Un modulo può contenere:

- Una o più risorse di cui eseguire il provisioning dal modulo, insieme a tutti i dati associati, come output o condizioni.
- Qualsiasi parametro del modulo, che consente di specificare valori personalizzati ogni volta che viene utilizzato il modulo.

Per informazioni sullo sviluppo di moduli, consulta [Developing modules](#) nella CloudFormation CLI User Guide.

Argomenti

- [Considerazioni su quando utilizzare i moduli](#)
- [Comprendere il controllo delle versioni dei moduli](#)
- [Usa i moduli del registro CloudFormation privato](#)
- [Usa i parametri per specificare i valori del modulo](#)
- [Risorse del modulo di riferimento nei CloudFormation modelli](#)

Considerazioni su quando utilizzare i moduli

- L'utilizzo dei moduli non comporta costi supplementari. Si paga solo per le risorse che i moduli risolvono negli stack.
- CloudFormation le quote, come il numero massimo di risorse consentite in uno stack o la dimensione massima del corpo del modello, si applicano al modello elaborato indipendentemente dal fatto che le risorse incluse in quel modello provengano da moduli o meno. Per ulteriori informazioni, consulta [Comprendi le CloudFormation quote](#).
- I tag specificati a livello di stack vengono assegnati alle singole risorse derivate dal modulo.
- Gli script di supporto specificati a livello di modulo non si propagano alle singole risorse contenute nel modulo durante l'elaborazione del modello. CloudFormation
- Gli output specificati nel modulo vengono propagati agli output a livello di modello.

Ad ogni output verrà assegnato un ID logico che è una concatenazione del nome logico del modulo e del nome di output così come definito nel modulo. Per ulteriori informazioni, consulta [Ottieni gli output esportati da uno stack distribuito CloudFormation](#).

- I parametri specificati nel modulo non vengono propagati ai parametri a livello di modello.

Tuttavia, è possibile creare parametri a livello di modello che fanno riferimento ai parametri a livello di modulo. Per ulteriori informazioni, consulta [Usa i parametri per specificare i valori del modulo](#).

Comprendere il controllo delle versioni dei moduli

Il CloudFormation registro funge da archivio in cui è possibile registrare e gestire i moduli da utilizzare all'interno della propria regione Account AWS . Puoi registrare moduli da varie fonti, tra cui editori di terze parti AWS, e le tue estensioni personalizzate, all'interno del tuo account e della tua regione. Per ulteriori informazioni, consulta [Gestione delle estensioni con il CloudFormation registro](#).

I moduli possono avere diverse versioni, quindi puoi specificare quale versione di un modulo desideri utilizzare. Questa funzionalità di controllo delle versioni è particolarmente utile quando è necessario aggiornare o modificare un modulo senza interrompere gli stack esistenti che dipendono da esso.

Tenete a mente le seguenti considerazioni quando utilizzate più versioni di un modulo:

- Durante le operazioni di stack, CloudFormation utilizza qualsiasi versione del modulo attualmente registrata come versione predefinita nella regione Account AWS e nella regione in cui viene eseguita l'operazione di stack. Sono inclusi i moduli che sono nidificati in altri moduli.

Pertanto, tieni presente che se hai diverse versioni dello stesso modulo registrate come versione predefinita in account o regioni diversi, l'utilizzo dello stesso modello può generare risultati diversi.

- Durante le operazioni di stack, CloudFormation utilizza qualsiasi versione della risorsa attualmente registrata come versione predefinita nella regione Account AWS e nella regione in cui viene eseguita l'operazione di stack. Ciò include le risorse generate includendo i moduli.
- La modifica della versione predefinita di un modulo non inizia alcuna operazione di aggiornamento stack. Tuttavia, la prossima volta che eseguirete un'operazione di stack con qualsiasi modello contenente quel modulo, ad esempio un aggiornamento dello stack, CloudFormation utilizzerà la nuova versione predefinita nell'operazione.

L'unica eccezione a ciò è l'esecuzione di un aggiornamento dello stack con l'opzione `usePreviousTemplate` specificata, come descritto di seguito.

- Per le operazioni di aggiornamento dello stack, se specificate l'opzione `UsePreviousTemplate`, CloudFormation utilizza il modello elaborato in precedenza per l'aggiornamento dello stack e non rielabora il modulo per eventuali modifiche che potreste avervi apportato.
- Per garantire risultati uniformi, se includi moduli in un modello di stack da utilizzare con set di stack, dovresti assicurarti che la stessa versione del modulo sia impostata come versione predefinita in tutti gli account e le regioni in cui intendi distribuire le tue istanze stack. Sono inclusi i moduli che sono nidificati in altri moduli. Per ulteriori informazioni, consulta [Gestione degli stack tra account e regioni con StackSets](#).

Requisiti per l'attivazione di moduli pubblici di terze parti

Per attivare correttamente un modulo pubblico di terze parti nel tuo account e nella tua regione, deve essere vero quanto segue per ogni estensione pubblica di terze parti (risorsa o modulo) inclusa nel modulo:

- Attivazione dell'estensione: l'estensione deve essere attivata nell'account e nella regione in cui desideri utilizzarla. Per ulteriori informazioni, consulta [Usa estensioni pubbliche di terze parti dal CloudFormation registro](#).
- Registrazione di un alias: se l'estensione del modulo utilizza un alias di tipo, l'estensione deve essere registrata nell'account e nella regione utilizzando lo stesso alias di nome. Per ulteriori informazioni, consulta [Usa gli alias per fare riferimento alle estensioni](#).
- Compatibilità delle versioni: la versione dell'estensione attualmente attivata deve essere una delle versioni principali supportate di tale estensione specificate nel modulo.

Se non sono attivate le estensioni pubbliche e le versioni di estensione di terze parti corrette, l'operazione CloudFormation avrà esito negativo con un errore che elenca le estensioni e le versioni che devono essere attivate prima che il modulo possa essere attivato correttamente.

Usa i moduli del registro CloudFormation privato

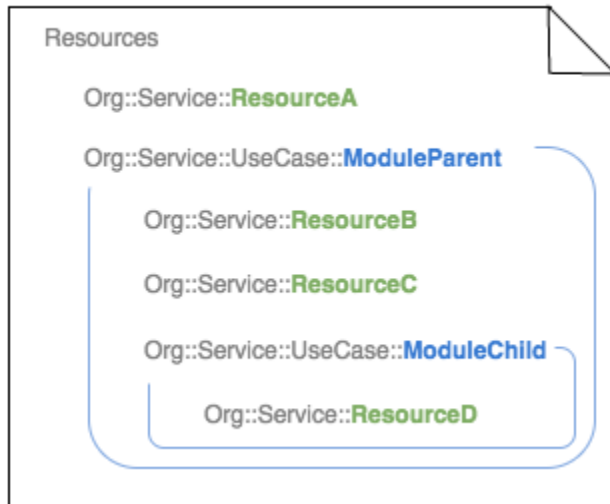
Questo argomento spiega come utilizzare i moduli nei CloudFormation modelli. Pensa ai moduli come a pacchetti di risorse predefiniti che puoi aggiungere ai tuoi modelli.

Per utilizzare un modulo, i passaggi sono i seguenti:

- **Registrazione del modulo:** i moduli vengono registrati nel CloudFormation registro come estensioni private. Assicurati che sia registrato nella regione Account AWS e nella regione in cui lavori. Per ulteriori informazioni, consulta [CloudFormation concetti di registro](#).
- **Includilo nel tuo modello:** aggiungi il modulo alla [Resources](#) sezione del CloudFormation modello, proprio come faresti con altre risorse. Dovrai inoltre fornire tutte le proprietà richieste per il modulo.
- **Crea o aggiorna lo stack:** quando avvii un'operazione di stack, CloudFormation genera un modello elaborato che risolve tutti i moduli inclusi nelle risorse appropriate.
- **Anteprima delle modifiche:** prima di apportare modifiche, puoi utilizzare un set di modifiche per vedere quali risorse verranno aggiunte o modificate. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Considera il seguente esempio: disponi di un modello che contiene sia risorse che moduli. Il modello contiene una singola risorsa e un modulo `ModuleParent`. `ResourceA` Quel modulo contiene due risorse `ResourceB` e `ResourceC`, oltre a un modulo annidato, `ModuleChild`. `ModuleChild` contiene una singola risorsa, `ResourceD`. Se crei uno stack da questo modello, CloudFormation elabora il modello e risolve i moduli nelle risorse appropriate. Lo stack risultante ha quattro risorse: `ResourceA`, `ResourceB`, `ResourceC` e `ResourceD`.

Template



Processed Template



CloudFormation tiene traccia di quali risorse in uno stack sono state create dai moduli. È possibile visualizzare queste informazioni nelle schede Events (Eventi), Resources (Risorse) e Drifts (Derive) per un determinato stack e sono incluse anche nelle anteprime del set di modifiche.

I moduli sono distinguibili dalle risorse di un modello perché adottano la seguente convenzione di denominazione in quattro parti, in contrasto con la classica convenzione in tre parti utilizzata dalle risorse:

```
organization::service::use-case::MODULE
```

Usa i parametri per specificare i valori del modulo

In CloudFormation, puoi utilizzare i parametri dei modelli per personalizzare gli stack fornendo valori di input durante la creazione o l'aggiornamento dello stack. Questi parametri consentono di modificare alcuni aspetti dello stack in base alle proprie esigenze. Per ulteriori informazioni sulla definizione dei parametri del modello, vedere [CloudFormation Parameters sintassi del modello](#).

Analogamente, i moduli possono avere anche dei parametri. Questi parametri del modulo consentono di inserire valori personalizzati nel modulo dal modello (o da un altro modulo) che lo utilizza. Il modulo può quindi utilizzare questi valori personalizzati per impostare i valori delle proprietà per le risorse che contiene.

È inoltre possibile definire parametri del modello che impostano le proprietà del modulo, in modo da poter immettere valori che vengono passati al modulo al momento dell'operazione di stack.

Se un modulo contiene un modulo annidato con i propri parametri di modulo, è possibile:

- Specificare i valori dei parametri del modulo nidificato direttamente nel modulo padre.
- Definire i parametri del modulo corrispondenti nel modulo padre che consentono al modello (o modulo) di impostare i parametri del modulo nidificato in cui è contenuto il modulo padre.

Utilizzo dei parametri modello per specificare i valori dei parametri del modulo

Nell'esempio seguente viene illustrato come definire i parametri del modello che trasferiscono i valori a un modulo.

Questo modello contiene la `My::S3::SampleBucket::MODULE` definizione di un parametro del modello che consente all'utente di specificare un nome di bucket S3 durante l'operazione di stack. `BucketName`

```
# Template containing My::S3::SampleBucket::MODULE
Parameters:
  BucketName:
    Description: Name for your sample bucket
    Type: String
Resources:
  MyBucket:
    Type: 'My::S3::SampleBucket::MODULE'
    Properties:
      BucketName: !Ref BucketName
```

Specifica delle proprietà sulle risorse in un modulo figlio dal modulo padre

Nell'esempio seguente viene illustrato come specificare i valori dei parametri in un modulo nidificato all'interno di un altro modulo.

Questo primo modulo, `My::S3::SampleBucketPrivate::MODULE`, sarà il modulo secondario. Definisce due parametri: `BucketName` e `AccessControl`. I valori specificati per questi parametri vengono utilizzati per specificare le proprietà `BucketName` e `AccessControl` della risorsa `AWS::S3::Bucket` contenuta nel modulo. Di seguito è riportato il frammento del modello per `My::S3::SampleBucketPrivate::MODULE`.

```
# My::S3::SampleBucketPrivate::MODULE
AWSTemplateFormatVersion: 2010-09-09
Description: A sample S3 Bucket with Versioning and DeletionPolicy.
Parameters:
```



```
BucketName:
  Description: Name for the bucket
  Type: String
AccessControl:
  Description: AccessControl for the bucket
  Type: String
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: !Ref BucketName
      AccessControl: !Ref AccessControl
      DeletionPolicy: Retain
      VersioningConfiguration:
        Status: Enabled
```

Successivamente, il modulo precedente è nidificato all'interno di un modulo padre, `My::S3::SampleBucket::MODULE`. Il modulo padre, `My::S3::SampleBucket::MODULE`, imposta i parametri del modulo figlio nei seguenti modi:

- Imposta il `AccessControl` parametro to. `My::S3::SampleBucketPrivate::MODULE Private`
- Per `BucketName`, definisce un parametro modulo, che consentirà di specificare il nome del bucket nel modello (o modulo) che contiene `My::S3::SampleBucket::MODULE`.

```
# My::S3::SampleBucket::MODULE
AWSTemplateFormatVersion: 2010-09-09
Description: A sample S3 Bucket. With Private AccessControl.
Parameters:
  BucketName:
    Description: Name for your sample bucket
    Type: String
Resources:
  MyBucket:
    Type: 'My::S3::SampleBucketPrivate::MODULE'
    Properties:
      BucketName: !Ref BucketName
      AccessControl: Private
```

Specifica dei vincoli per i parametri del modulo

I parametri del modulo non supportano l'applicazione dei vincoli. Per eseguire il controllo dei vincoli su un parametro del modulo, create un parametro di modello con i vincoli desiderati. Quindi, fate riferimento a quel parametro del modello nel parametro del modulo. Per ulteriori informazioni sulla definizione dei parametri del modello, consulta [CloudFormation Parameters sintassi del modello](#).

Risorse del modulo di riferimento nei CloudFormation modelli

Nei CloudFormation modelli, spesso è necessario impostare le proprietà di una risorsa in base al nome o alla proprietà di un'altra risorsa. Per ulteriori informazioni, consulta [Risorse di riferimento](#).

Per fare riferimento a una risorsa contenuta in un modulo del CloudFormation modello, è necessario combinare due nomi logici:

- Il nome logico che hai dato al modulo stesso quando lo hai incluso nel modello.
- Il nome logico della risorsa specifica all'interno di quel modulo.

È possibile combinare questi due nomi logici con o senza utilizzare un punto (.) tra di loro. Ad esempio, se il nome logico del modulo è `MyModule` e il nome logico della risorsa è `MyBucket`, è possibile fare riferimento a tale risorsa come a uno dei due `MyModule.MyBucket` termini `MyModuleMyBucket`.

Per trovare i nomi logici delle risorse all'interno di un modulo, è possibile consultare lo schema del modulo, disponibile nel CloudFormation registro o utilizzando [DescribeType](#) operazione. Lo schema elenca tutte le risorse e i relativi nomi logici che fanno parte del modulo.

Una volta ottenuto il nome logico completo, è possibile utilizzare CloudFormation funzioni come `GetAtt` e accedere `Ref` ai valori delle proprietà sulle risorse del modulo.

Ad esempio, avete un `My::S3::SampleBucket::MODULE` modulo che contiene una `AWS::S3::Bucket` risorsa con il nome logico `S3Bucket`. Per fare riferimento al nome di questo bucket utilizzando la `Ref` funzione, combinate il nome del modulo nel modello (`MyBucket`) con il nome logico della risorsa nel modulo (`S3Bucket`). Il nome logico completo è `MyBucket.S3Bucket` o `MyBucketS3Bucket`.

Modello di esempio

Il modello di esempio seguente crea un bucket S3 utilizzando il `My::S3::SampleBucket::MODULE` modulo. Inoltre, crea una coda Amazon SQS e ne imposta il nome in modo che sia lo stesso del

nome del bucket del modulo. Inoltre, il modello restituisce l'Amazon Resource Name (ARN) del bucket S3 creato.

```
# Template that uses My::S3::SampleBucket::MODULE
Parameters:
  BucketName:
    Description: Name for your sample bucket
    Type: String
Resources:
  MyBucket:
    Type: My::S3::SampleBucket::MODULE
    Properties:
      BucketName: !Ref BucketName
  exampleQueue:
    Type: AWS::SQS::Queue
    Properties:
      QueueName: !Ref MyBucket.S3Bucket
Outputs:
  BucketArn:
    Value: !GetAtt MyBucket.S3Bucket.Arn
```

Gestione AWS delle risorse come singola unità con AWS CloudFormation pile

Uno stack è una raccolta di AWS risorse che puoi gestire come singola unità. In altre parole, è possibile creare, aggiornare ed eliminare una raccolta di risorse creando, aggiornando ed eliminando pile.

La creazione di uno stack comporta l'implementazione di un CloudFormation modello che specifica le risorse e le relative configurazioni, che quindi effettua il provisioning e la configurazione.

CloudFormation

L'aggiornamento di uno stack comporta la modifica del modello o dei parametri. CloudFormation confronta le modifiche inviate con lo stato corrente dello stack e aggiorna solo le risorse modificate. CloudFormation potrebbe interrompere le risorse o sostituire le risorse aggiornate, a seconda delle proprietà aggiornate. Per ulteriori informazioni sui comportamenti di aggiornamento delle risorse, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

CloudFormation fornisce due metodi per aggiornare gli stack:

- **Set di modifiche:** con i set di modifiche, puoi visualizzare in anteprima le modifiche che CloudFormation verranno apportate allo stack e quindi decidere se applicare tali modifiche. I set di modifiche sono documenti in formato JSON che riepilogano le modifiche CloudFormation che verranno apportate a uno stack. Utilizzate i set di modifiche quando volete assicurarvi che CloudFormation non vengano apportate modifiche involontarie o quando volete prendere in considerazione diverse opzioni. Ad esempio, puoi utilizzare un set di modifiche per verificare che CloudFormation non sostituisca le istanze del database dello stack durante un aggiornamento.
- **Aggiornamento diretto:** quando aggiorni direttamente uno stack, invii le modifiche e le distribuisce CloudFormation immediatamente. Esegui un aggiornamento diretto quando vuoi una distribuzione rapida degli aggiornamenti.

L'eliminazione di uno stack comporta l'eliminazione delle risorse ad esso associate. Ad esempio, uno stack può includere tutte le risorse necessarie per l'esecuzione di un'applicazione Web, ad esempio un server Web, un database e le regole di rete. Se l'applicazione Web non è più necessaria, puoi eliminare lo stack. Verranno eliminate anche tutte le relative risorse correlate.

 Note

Ti verrà addebitato il costo delle risorse dello stack per l'intero intervallo in cui tali risorse risultano operative (anche se hai eliminato lo stack).

CloudFormation assicura che tutte le risorse dello stack vengano create o eliminate in modo appropriato. Poiché CloudFormation considera le risorse dello stack come una singola unità, devono essere create o eliminate per consentire la creazione o l'eliminazione dello stack. Se una risorsa non può essere creata, CloudFormation esegue il rollback dello stack ed elimina automaticamente le risorse create. Se una risorsa non può essere eliminata, tutte le risorse rimanenti vengono conservate finché lo stack non viene eliminato.

Argomenti

- [Interfacce per la gestione degli stack](#)
- [Crea uno stack dalla console CloudFormation](#)
- [Visualizza le informazioni sullo stack dalla console CloudFormation](#)
- [Aggiorna il modello dello stack](#)
- [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#)
- [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#)
- [Aggiorna direttamente gli stack](#)
- [Annullare un aggiornamento dello stack](#)
- [Eliminare uno stack dalla console CloudFormation](#)
- [Monitora l'avanzamento dello stack](#)
- [Riduci il tuo CloudFormation stack in caso di violazione degli allarmi con i trigger di rollback](#)
- [Rileva le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento della deriva](#)
- [Importazione di AWS risorse in una CloudFormation pila](#)
- [Rifattorizzazione degli stack](#)
- [Supporto per tipi di risorse](#)
- [Usa i link di creazione rapida per creare pile CloudFormation](#)
- [Esempi di comandi di funzionamento CloudFormation dello stack per e AWS CLI PowerShell](#)

Interfacce per la gestione degli stack

Puoi gestire i tuoi CloudFormation stack utilizzando le seguenti interfacce:

- **CloudFormation console:** fornisce un'interfaccia web che puoi utilizzare per accedere agli stack. Puoi accedere alla CloudFormation console accedendo a AWS Management Console, utilizzando la casella di ricerca sulla barra di navigazione per cercare e CloudFormation quindi scegliendo CloudFormation tra i risultati della ricerca.
- **AWS Command Line Interface**— Fornisce comandi per un'ampia gamma di AWS servizi CloudFormation, inclusi ed è supportato su Windows, Mac e Linux. Per informazioni sui CloudFormation comandi, consulta [cloudformation](#) nel AWS CLI Command Reference.
- **AWS Strumenti per PowerShell**— Un set di PowerShell moduli basati sulle funzionalità esposte da SDK per .NET. Gli strumenti PowerShell consentono di eseguire operazioni tramite script sulle AWS risorse provenienti da PowerShell riga di comando. È possibile trovare i cmdlet per CloudFormation nella Guida ai [AWS Strumenti per PowerShell cmdlet](#).
- **API di query:** forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. Se si effettuano chiamate API nell'applicazione, è necessario scrivere il codice per gestire dettagli di basso livello, come la generazione dell'hash per firmare la richiesta. Per ulteriori informazioni sulle azioni API per CloudFormation, consulta [Azioni](#) nell'AWS CloudFormation API Reference.
- **AWS SDKs**— Fornisce informazioni specifiche per la lingua APIs e si occupa di molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta [Tools to Build on AWS](#).
- **AWS Cloud Development Kit (AWS CDK)**— AWS CDK È un framework di sviluppo software open source che consente di definire l' AWS infrastruttura utilizzando linguaggi di programmazione familiari come Python TypeScript, Java e .NET. Con CDK, è possibile modellare le risorse applicative e quindi eseguirne il provisioning utilizzando CloudFormation direttamente l'ambiente di sviluppo integrato (IDE). Per ulteriori informazioni, consulta [AWS Cloud Development Kit \(AWS CDK\)](#).

Crea uno stack dalla console CloudFormation

Puoi creare un modello di stack e quindi utilizzarlo per creare uno stack utilizzando la CloudFormation console o uno strumento da riga di comando. La console fornisce un'interfaccia guidata con opzioni predefinite, che semplifica il processo di creazione dello stack.

Argomenti

- [Creazione di uno stack](#)
- [Configurare le opzioni dello stack](#)
- [Visualizza l'anteprima della configurazione del tuo stack](#)

Creazione di uno stack

Segui i passaggi di questa sezione per distribuire il modello e creare uno stack.

Prerequisiti

- Devi aver creato un modello di stack. Per ulteriori informazioni, consulta [Lavorare con i CloudFormation modelli](#).

Per creare uno stack (console)

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli in cui Regione AWS creare lo stack.
3. Nella pagina Pile, scegli Crea pila in alto a destra, quindi scegli Con nuove risorse (standard).

In alternativa, puoi scegliere l'opzione Con risorse esistenti (importa risorse) per importare AWS le risorse esistenti descritte nel tuo modello. Per ulteriori informazioni su questa opzione, consulta [Importazione di AWS risorse in una CloudFormation pila](#).

4. Nella pagina Crea stack, esegui una delle seguenti operazioni:
 - Per utilizzare un modello esistente, in Prerequisito - Prepara modello, scegli Scegli un modello esistente. Quindi, in Specificare modello, scegli l'URL di Amazon S3 o Carica un file modello in base alla posizione del modello.
 - Se scegli l'URL di Amazon S3, fornisci un URL per il file modello in un bucket S3.

Se il modello include stack annidati (ad esempio, pile descritte in altri documenti modello situati nelle sottodirectory), assicurati che il bucket S3 contenga i file e le directory necessari.

Se disponi di un modello proveniente da un bucket abilitato al controllo delle versioni, puoi specificare una versione specifica del modello aggiungendolo all'URL. ?

versionId=*version-id* Per ulteriori informazioni sui bucket abilitati alla versione,

consulta [Working with objects in a versioning-enabled bucket nella Amazon Simple Storage Service User Guide](#).

L'URL deve puntare a un modello con dimensioni massime di 1 MB, archiviato in un bucket S3 per cui disponi delle autorizzazioni in lettura. La lunghezza massima dell'URL è 1024 caratteri. Alcune risorse potrebbero richiedere che il bucket si trovi nella stessa Regione dello stack.

- Se scegli Carica un file modello, scegli Scegli file per scegliere un file modello dal tuo computer locale. La dimensione del file modello deve essere pari o inferiore a 1 MB.

Dopo aver scelto il modello, CloudFormation carica il file e visualizza l'URL S3. CloudFormation lo carica in un bucket Amazon S3 nel tuo Account AWS. Se hai già un bucket S3 creato da CloudFormation nel tuo Account AWS, CloudFormation aggiunge il modello a quel bucket. Se non disponi già di un bucket creato, CloudFormation viene creato un bucket unico per ogni regione in cui carichi un file modello.

Di seguito sono riportate le considerazioni relative all'utilizzo dei bucket S3 creati da: CloudFormation

- I bucket sono accessibili a chiunque disponga delle autorizzazioni Amazon S3. Account AWS
- CloudFormation crea i bucket con la crittografia lato server abilitata per impostazione predefinita, crittografando così tutti gli oggetti memorizzati nel bucket.

Puoi gestire direttamente le opzioni di crittografia per i bucket che hai CloudFormation creato, ad esempio, utilizzando la console Amazon S3 <https://console.aws.amazon.com/s3/> all'indirizzo o il AWS CLI. Per ulteriori informazioni, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

- Puoi utilizzare il tuo bucket e gestirne le autorizzazioni caricando manualmente i modelli su Amazon S3. Quando crei o aggiorni uno stack, specifica l'URL Amazon S3 di un file del modello.
- Se non hai un modello pronto, puoi scegliere Build from Infrastructure Composer per creare un modello con Infrastructure Composer. Per ulteriori informazioni, consulta [Infrastructure Composer](#).

5. Scegli Avanti per continuare e convalidare il modello.

Prima di continuare, CloudFormation convalida il modello per rilevare errori sintattici e alcuni errori semantici, come le dipendenze circolari. Durante la convalida, verifica CloudFormation innanzitutto se il modello è JSON valido. In caso contrario, CloudFormation verifica se il modello è YAML valido. Se entrambi i controlli falliscono, CloudFormation restituisce un errore di convalida del modello.

6. Nella pagina Specify stack details (Specifica dettagli stack), digitare il nome dello stack in Stack name (Nome stack).

Il nome dello stack è un identificatore che ti aiuta a trovare un determinato stack da un elenco di stack. Il nome di uno stack può contenere solo caratteri alfanumerici (con distinzione tra lettere maiuscole e minuscole) e trattini. Deve iniziare con un carattere alfabetico e non può avere una lunghezza superiore a 128 caratteri.

7. Nella sezione Parametri, specificate i valori per i parametri definiti nel modello.
8. Scegliete Avanti per continuare a creare lo stack.
9. (Facoltativo) Nella pagina Configura le opzioni dello stack, modificate le opzioni dello stack predefinite. Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#).
10. Se il modello contiene risorse IAM, per Capacità, scegli Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
11. Seleziona Successivo per continuare.
12. Nella pagina Rivedi e crea, esamina i dettagli del tuo stack.

Per modificare uno qualsiasi dei valori prima di avviare lo stack, scegli Modifica nella sezione contenente l'impostazione che desideri modificare.

13. (Facoltativo) È possibile creare un set di modifiche per visualizzare in anteprima la configurazione dello stack prima di crearlo. Nella pagina Rivedi e crea, scegli Crea set di modifiche e segui le istruzioni. Per ulteriori informazioni, consulta [Visualizza l'anteprima della configurazione del tuo stack](#).
14. Scegli Invia per avviare lo stack.

CloudFormation procederà quindi alla creazione di tutte le risorse definite nel modello.

Puoi monitorare l'avanzamento e lo stato della creazione dello stack nella scheda Eventi per il tuo nuovo stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Per creare uno stack utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi:

- [create-stack](#) (AWS CLI)
- [New-CFNStack](#) (AWS Tools for Windows PowerShell)

Per esempi di utilizzo della riga di comando per creare uno stack, consulta. [Esempi di comandi di funzionamento CloudFormation dello stack per e AWS CLI PowerShell](#)

Configurare le opzioni dello stack

Nella pagina Configura le opzioni dello stack, puoi configurare opzioni per i tuoi CloudFormation stack come tag, notifica degli eventi dello stack o una politica dello stack.

È possibile specificare le seguenti opzioni di stack:

Tag

Puoi aggiungere fino a 50 coppie di chiavi di tag allo stack e a qualsiasi risorsa che supporti l'etichettatura per. CloudFormation Un tag è una chiave e un valore definiti dal cliente che possono essere assegnati alle AWS risorse per scopi quali il monitoraggio dei costi.

Una Key (Chiave) è costituita da caratteri alfanumerici o spazi. Le chiavi di tag possono contenere fino a 127 caratteri.

Un Value (Valore) è costituito da caratteri alfanumerici o spazi. I valori possono contenere fino a 255 caratteri.

Dopo la creazione dello stack, l'aggiunta, l'aggiornamento o la rimozione di tag a livello di stack avvierà un aggiornamento dello stack. Tutte le risorse che supportano la propagazione dei tag a livello di stack verranno aggiornate di conseguenza.

Autorizzazioni

Un ruolo di servizio IAM esistente che può assumere. CloudFormation Invece di utilizzare le credenziali dell'account, CloudFormation utilizza le credenziali del ruolo per creare lo stack. Per ulteriori informazioni, consulta [AWS CloudFormation ruolo di servizio](#).

Opzioni di errore degli stack

Specifica le opzioni di errore del provisioning per tutte le implementazioni di stack e le operazioni del set di modifica. Per ulteriori informazioni, consulta [Scegli come gestire gli errori durante il provisioning delle risorse](#).

L'opzione Roll back all stack resources (Effettua il ripristino dello stato precedente di tutte le risorse della pila) ripristinerà tutte le risorse specificate nel modello quando lo stato dello stack è CREATE_FAILED o UPDATE_FAILED.

Nel caso di operazioni di creazione, l'opzione Preserve successfully provisioned resources (Mantieni le risorse con il provisioning riuscito) mantiene lo stato delle risorse in cui l'operazione è riuscita, mentre le risorse in cui l'operazione non è riuscita continuano a presentare lo stato di esito negativo fino all'aggiornamento successivo.

Nel caso di operazioni di aggiornamento e modifica del set, l'opzione Preserve successfully provisioned resources (Mantieni le risorse con il provisioning riuscito) mantiene lo stato delle risorse in cui l'operazione è riuscita, mentre per le risorse in cui l'operazione non è riuscita ripristina l'ultimo stato stabile noto. Le risorse non riuscite presenteranno lo stato UPDATE_FAILED. Le risorse per le quali non è disponibile un ultimo stato stabile noto verranno eliminate in occasione della successiva operazione stack.

È anche possibile impostare le seguenti opzioni avanzate per la creazione dello stack:

Stack policy (Policy dello stack)

Definisce le risorse che si desidera proteggere da aggiornamenti involontari durante un aggiornamento dello stack. Per impostazione predefinita, durante un aggiornamento dello stack possono essere aggiornate tutte le risorse.

È possibile inserire la policy di stack direttamente come JSON o caricare un file in formato JSON che contenga la policy dello stack. Per ulteriori informazioni, consulta [Impedire gli aggiornamenti delle risorse stack](#).

Configurazione di rollback

Puoi CloudFormation monitorare lo stato dello stack durante la creazione e l'aggiornamento dello stack e ripristinare tale operazione se lo stack supera la soglia di uno degli allarmi che hai specificato. Specificate gli allarmi da monitorare CloudWatch . CloudFormation Se uno qualsiasi degli allarmi diventa attivo durante l'operazione ALARM dello stack o il periodo di monitoraggio,

ripristina l'intera CloudFormation operazione dello stack. Per ulteriori informazioni, consulta [Riduci il tuo CloudFormation stack in caso di violazione degli allarmi con i trigger di rollback](#).

Notification options (Opzioni di notifica)

È possibile specificare un argomento Amazon Simple Notification Service nuovo o esistente a cui vengono inviate le notifiche sugli eventi di stack.

Se si crea un argomento Amazon SNS, è necessario specificare un nome e un indirizzo e-mail a cui devono essere inviate le notifiche degli eventi di stack.

Opzioni di creazione dello stack

Le seguenti opzioni sono incluse nella creazione dello stack, ma non sono disponibili come parte aggiornamenti di stack.

Timeout

Specifica la quantità di tempo, in minuti, da dedicare prima di scadere le CloudFormation operazioni di creazione dello stack. Se non CloudFormation riesce a creare l'intero stack entro il tempo assegnato, fallisce la creazione dello stack a causa del timeout e ripristina lo stack.

Per impostazione predefinita, non è previsto alcun timeout per la creazione dello stack. Tuttavia, per la natura del servizio che implementano, alcune singole risorse possono avere un proprio timeout. Ad esempio, se una singola risorsa nello stack produce un timeout, anche la creazione dello stack viene arrestata, anche se il timeout specificato per la creazione dello stack non è ancora stato raggiunto.

Termination protection (Protezione da cessazione)

Impedisce che uno stack venga eliminato per errore. Se un utente tenta di eliminare uno stack con protezione da cessazione abilitata, l'eliminazione ha esito negativo e lo stack, incluso lo stato, rimane invariato. Per ulteriori informazioni, consulta [Proteggi CloudFormation gli stack dall'eliminazione](#).

Per impostazione predefinita, la protezione da cessazione è Disabled (Disabilitato).

Visualizza l'anteprima della configurazione del tuo stack

Per vedere in anteprima come verrà configurato uno CloudFormation stack prima di crearlo, create un set di modifiche. Questa funzionalità consente di esaminare varie configurazioni e di apportare correzioni e modifiche allo stack prima di eseguire il set di modifiche. Per ulteriori informazioni sui set di modifiche, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Creazione di un set di modifiche per un nuovo stack

Per creare un set di modifiche per un nuovo stack, selezionare il modello di stack e specificare la configurazione dello stack come si farebbe per la creazione di un nuovo stack, quindi scegliere per creare un nuovo set di modifiche piuttosto che un nuovo stack.

Per creare un set di modifiche per un nuovo stack

1. Nella pagina Rivedi e crea, scegli Crea set di modifiche.
2. Nella finestra di dialogo Crea set di modifiche, inserite un nome per il set di modifiche e, se lo desiderate, una descrizione. Selezionare Create change set (Crea set di modifiche).

Quando create un set di modifiche per un nuovo stack, CloudFormation effettua le seguenti operazioni:

- Avvia un nuovo stack con lo stato `REVIEW_IN_PROGRESS`.
- Crea un set di modifiche per il nuovo stack che riflette la configurazione dello stack specificata nei passaggi precedenti.

CloudFormation visualizza la pagina Change sets per lo stack proposto. Durante la CloudFormation creazione del set di modifiche, il relativo stato è `CREATE_IN_PROGRESS`, e il relativo stato di esecuzione è `UNAVAILABLE`. Una volta CloudFormation completata con successo la creazione del set di modifiche, imposta lo stato del set di modifiche su `CREATE_COMPLETE` e il relativo stato di esecuzione è `AVAILABLE`. Lo stato dello stack viene aggiornato a `REVIEW_IN_PROGRESS`. A questo punto, è possibile eseguire il set di modifiche per completare la creazione del nuovo stack.

Nel riquadro Modifiche, CloudFormation visualizza la configurazione proposta dello stack.

Se CloudFormation non riesce a creare il set di modifiche, imposta lo stato del set di modifiche su `CREATE_FAILED`. Correggere gli errori visualizzati nel campo Status reason (Stato motivo), quindi creare un nuovo set di modifiche. In questa fase è possibile provare varie configurazioni e apportare correzioni e modifiche allo stack prima di eseguire il successivo set di modifiche.

3. Per completare la creazione di un nuovo stack in base al set di modifiche, scegliere Execute (Esegui), specificare la configurazione di ripristino dello stato precedente, quindi scegliere Execute change set (Esegui set di modifiche).

Visualizza le informazioni sullo stack dalla console CloudFormation

Dopo aver creato uno CloudFormation stack, puoi utilizzarlo AWS Management Console per visualizzarne i dati e le risorse.

Per visualizzare le informazioni sullo stack CloudFormation

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS dove si trova lo stack.
3. Nella pagina Stacks, scegli il nome dello stack. CloudFormation visualizza i dettagli dello stack per lo stack selezionato.

Note

Se lo stack è stato eliminato, puoi trovarlo utilizzando l'opzione Filter status. Per ulteriori informazioni, consulta [Visualizza gli stack eliminati dalla console CloudFormation](#).

Puoi visualizzare le seguenti informazioni stack:

Info stack

Visualizza le informazioni generali sullo stack e sulla relativa configurazione:

Panoramica

Visualizza il nome dello stack, l'ID dello stack, lo stack principale e il [ruolo IAM](#), insieme a informazioni sullo stato come lo stato dello stack, lo stato della deriva e la protezione dalla terminazione.

Tag

Visualizza i tag che sono associati allo stack.

Stack policy (Policy dello stack)

Descrive le risorse dello stack che sono protette dagli aggiornamenti dello stack. Per poter aggiornare queste risorse, devono essere esplicitamente consentite durante un aggiornamento dello stack. Per ulteriori informazioni, consulta [Impedire gli aggiornamenti delle risorse stack](#).

Configurazione di rollback

Visualizza tutti gli CloudWatch allarmi che hai specificato e che devono CloudFormation essere monitorati durante l'operazione dello stack o il periodo di monitoraggio specificato. Se uno qualsiasi degli allarmi diventa attivo durante l'operazione ALARM dello stack o il periodo di monitoraggio, ripristina l'intera operazione CloudFormation dello stack. Per ulteriori informazioni, consulta [Riduci il tuo CloudFormation stack in caso di violazione degli allarmi con i trigger di rollback](#).

Notification options (Opzioni di notifica)

Visualizza l'argomento Amazon Simple Notification Service in cui vengono inviate le notifiche relative agli eventi dello stack, se specificato.

Eventi

Visualizza le operazioni che vengono registrate al momento della creazione, aggiornamento o eliminazione dello stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

A tutti gli eventi che vengono attivati da una determinata operazione stack viene assegnata lo stesso token richiesta client, che puoi utilizzare per monitorare le operazioni. Le operazioni di stack avviate dalla console utilizzano il formato token Console - StackOperation -ID, che consente di identificare facilmente l'operazione dello stack. Ad esempio, se crei uno stack utilizzando la console, a ogni evento stack risultante verrà assegnato lo stesso token nel formato seguente: Console-CreateStack-7f59c3cf-00d2-40c7-b2ff-e75db0987002.

Risorse

Visualizza le risorse che fanno parte dello stack.

Output

Visualizza gli output che sono stati dichiarati nel modello di stack. Per ulteriori informazioni, consulta [Ottieni gli output esportati da uno stack distribuito CloudFormation](#).

Parametri

Visualizza i parametri dello stack e i relativi valori.

Per gli stack che contengono i parametri di Systems Manager, la colonna Valore risolto mostra i valori utilizzati nella definizione dello stack per i parametri di Systems Manager. Per ulteriori informazioni, consulta [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#).

Modello

Visualizza il modello dello stack.

Per gli stack che contengono macro, scegliete Visualizza modello originale per visualizzare il modello inviato dall'utente o Visualizza modello elaborato per visualizzare il modello dopo aver CloudFormation elaborato le macro di riferimento. CloudFormation utilizza il modello elaborato per creare o aggiornare lo stack.

Set di modifiche

Visualizza i set di modifiche dello stack.

Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).

Sincronizzazione Git

Visualizza la dashboard di sincronizzazione Git dello stack.

Per ulteriori informazioni, consulta [Pannello di controllo dello stato di sincronizzazione Git](#).

Aggiorna il modello dello stack

Per modificare le risorse o le proprietà di uno CloudFormation stack, devi aggiornare il modello dello stack. Inizia con il modello esistente per quello stack e apporta le tue modifiche. Se il modello è archiviato in un sistema di controllo del codice sorgente, usane una copia come punto di partenza. Altrimenti, puoi ottenere una copia del modello da CloudFormation.

Se desideri modificare solo i parametri o le impostazioni dello stack (come l'argomento Amazon SNS dello stack), puoi riutilizzare il modello esistente senza ottenerne una copia.

Puoi aggiornare un modello di CloudFormation stack utilizzando un editor di testo o [Infrastructure Composer](#)

Per aggiornare un modello di stack esistente utilizzando Infrastructure Composer

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation).
2. Nella pagina Stacks, scegli il nome dello stack da aggiornare.
3. Scegli la scheda Modello, quindi scegli Visualizza in Infrastructure Composer.

CloudFormation apre il modello in Infrastructure Composer.

4. Aggiorna il modello utilizzando uno dei seguenti metodi:
 - Interfaccia Canvas: qui puoi trascinare e rilasciare dal pallette Risorse. Configura le risorse facendo doppio clic su una scheda per aprire il pannello delle proprietà delle risorse. Connect le risorse in base alle esigenze. Per istruzioni dettagliate sull'uso dell'interfaccia Canvas, vedi [Come comporre in AWS Infrastructure Composer](#).
 - Interfaccia modello: passa dall'interfaccia Canvas all'interfaccia Template. Effettua aggiornamenti in linea al codice del modello. Passa dai formati JSON a YAML in base alle esigenze.
5. Scegli Convalida per verificare eventuali errori di sintassi nel modello.
6. Quando sei pronto per esportare le modifiche in CloudFormation, scegli Aggiorna modello.

Per aggiornare un modello di stack esistente utilizzando il AWS CLI

1. Per ottenere il modello per lo stack che desideri aggiornare, usa il comando CLI [get-template](#).
2. Copiare il modello, incollarlo in un file di testo, modificarlo e salvarlo. Copiare solo il modello. Nel comando il modello è racchiuso tra virgolette, ma le virgolette non vanno copiate. Il modello vero e proprio inizia con una parentesi graffa aperta e termina con la parentesi graffa finale chiusa. Specificare le modifiche alle risorse dello stack in questo file.

Tieni presente i seguenti punti quando apporti modifiche al modello:

- Non puoi aggiungere, modificare o eliminare un parametro utilizzato da una risorsa che non supporta gli aggiornamenti.
- Per la maggior parte delle risorse, modificare il nome logico equivale a eliminare la risorsa sostituendola con una nuova. È necessario aggiornare anche tutte le altre risorse che dipendono dalla risorsa rinominata e questo potrebbe comportarne la sostituzione. Per altre risorse, l'avvio di un aggiornamento richiede l'aggiornamento di una proprietà (non solo del nome logico).
- Alcune risorse potrebbero avere dei vincoli sui valori che è possibile impostare per determinate proprietà. Ad esempio, le modifiche alla `AllocatedStorage` proprietà per un'istanza di database RDS devono essere maggiori del valore corrente. Se l'aggiornamento viola queste regole, quella parte avrà esito negativo.
- L'aggiornamento di una risorsa può influire anche su altre che vi fanno riferimento. Se si utilizzano funzioni come [La funzione Ref](#) o [La funzione Fn::GetAtt](#) per impostare una proprietà basata

su un'altra risorsa, CloudFormation aggiornerà anche la risorsa di riferimento quando quella di riferimento cambia.

- Per informazioni sugli effetti dell'aggiornamento di particolari proprietà delle risorse, consultate il riferimento ai [tipi di AWS risorse e proprietà](#). Per ogni proprietà, l'effetti di un aggiornamento sarà uno dei seguenti:
 - Aggiornamento richiesto: [nessuna interruzione](#)
 - Aggiornamento richiesto: [alcune interruzioni](#)
 - Aggiornamento richiesto: [sostituzione](#)
- È possibile verificare la sintassi JSON o YAML del modello utilizzando il comando [validate-template](#) CLI o specificando il modello sulla console. La console esegue la convalida automaticamente. Tuttavia, questi metodi verificano solo la sintassi del modello e non convalidano che i valori delle proprietà specificati per una risorsa siano validi per quella risorsa. [Per convalidare più complesse o per verificare le migliori pratiche, puoi anche utilizzare strumenti aggiuntivi come CloudFormation Linter \(cfn-lint\) e Rain \(rain fmt\)](#). CloudFormation

Note

A volte CloudFormation non consente alcune modifiche che tenti di apportare e ti dirà che la modifica non è consentita. Tuttavia, questo messaggio potrebbe apparire in modo asincrono, poiché per impostazione predefinita le risorse vengono create e aggiornate da CloudFormation in un ordine non deterministico.

Comprendi i comportamenti di aggiornamento delle risorse dello stack

Quando invii un aggiornamento, AWS CloudFormation aggiorna le risorse in base alle differenze tra ciò che invii e il modello corrente dello stack. Le risorse non interessate da modifiche vengono eseguite senza interruzioni durante il processo di aggiornamento. Per le risorse aggiornate, AWS CloudFormation utilizza uno dei seguenti comportamenti di aggiornamento:

Aggiornamento senza interruzioni

AWS CloudFormation aggiorna la risorsa senza interrompere il funzionamento della risorsa e senza modificare l'ID fisico della risorsa. Ad esempio, se aggiorni determinate proprietà di una [AWS::CloudTrail::Trail](#) risorsa, AWS CloudFormation aggiorna la traccia senza interruzioni.

Aggiornamenti con alcune interruzioni

AWS CloudFormation aggiorna la risorsa con alcune interruzioni. Ad esempio, se aggiorni determinate proprietà su una [AWS::EC2::Instance](#) risorsa, l'istanza potrebbe subire delle interruzioni AWS CloudFormation e Amazon EC2 riconfigurarla.

Sostituzione

AWS CloudFormation ricrea la risorsa durante un aggiornamento, che genera anche un nuovo ID fisico. AWS CloudFormation in genere crea prima la risorsa sostitutiva, modifica i riferimenti da altre risorse dipendenti in modo che puntino alla risorsa sostitutiva e quindi elimina la vecchia risorsa. Ad esempio, se aggiorni la AvailabilityZone proprietà di un tipo di [AWS::EC2::Instance](#) risorsa, AWS CloudFormation crea una nuova risorsa e sostituisce la risorsa EC2 Instance corrente con quella nuova.

Se aggiungi o rimuovi una proprietà che richiede una sostituzione, verrà attivato anche un aggiornamento. L'aggiornamento verrà eseguito anche se il valore reale della proprietà non cambia.

Il metodo AWS CloudFormation utilizzato dipende dalla proprietà aggiornata per un determinato tipo di risorsa. Il comportamento di aggiornamento per ogni proprietà è descritto nel [riferimento ai tipi di AWS risorse e proprietà](#).

A seconda del comportamento di aggiornamento, puoi decidere quando modificare le risorse per ridurre l'impatto di tali modifiche sulla tua applicazione. Più in particolare, puoi pianificare quando le risorse devono essere sostituite durante un aggiornamento. Ad esempio, se aggiorni la Port proprietà di un tipo di DBInstance risorsa [AWS::RDS::](#), AWS CloudFormation sostituisce l'istanza DB creando una nuova istanza DB con l'impostazione della porta aggiornata ed elimina la vecchia istanza DB. Prima dell'aggiornamento, potresti pianificare le seguenti operazioni in preparazione della sostituzione del database:

- Esegui uno snapshot del database corrente.
- Prepara una strategia per il modo in cui le applicazioni che utilizzano quella istanza database gestiranno un'interruzione durante la sostituzione dell'istanza database.
- Verificare che le applicazioni che utilizzano quella istanza database considerino l'impostazione di porta aggiornata e di altri aggiornamenti che potrebbero essere stati eseguiti.
- Utilizza la snapshot DB per ripristinare i database sulla nuova istanza database.

Questo esempio non è esaustivo, ma offre un'idea di cosa pianificare quando una risorsa viene sostituita durante un aggiornamento.

Note

Se il modello include uno o più stack [annidati](#), [avvia AWS CloudFormation anche un aggiornamento per ogni stack](#) annidato. Ciò è necessario per determinare se gli stack nidificati sono stati modificati. AWS CloudFormation aggiorna solo le risorse negli stack nidificati che presentano modifiche specificate nei modelli corrispondenti.

Aggiorna CloudFormation gli stack utilizzando i set di modifiche

Quando devi aggiornare uno stack, comprendere come le modifiche interesseranno le risorse in esecuzione prima di implementarle può aiutarti a aggiornare gli stack in sicurezza. I set di modifiche consentono di visualizzare in anteprima come le modifiche proposte a uno stack potrebbero influire sulle risorse in esecuzione, incluso l'impatto sulle proprietà e sugli attributi delle risorse. Se le modifiche elimineranno o sostituiranno risorse critiche, CloudFormation apporta le modifiche allo stack solo quando decidete di eseguire il set di modifiche, consentendovi di decidere se procedere con le modifiche proposte o esplorare altre modifiche creando un altro set di modifiche. È possibile creare e gestire i set di modifiche utilizzando la CloudFormation console o AWS CLI l' CloudFormation API.

Argomenti

- [Creare un set di modifiche per uno CloudFormation stack](#)
- [Visualizzare un set di modifiche per uno CloudFormation stack](#)
- [Esegui un set di modifiche per uno CloudFormation stack](#)
- [Eliminare un set di modifiche per uno CloudFormation stack](#)
- [Esempi di set di modifiche per le CloudFormation pile](#)
- [Set di modifiche per stack nidificati](#)

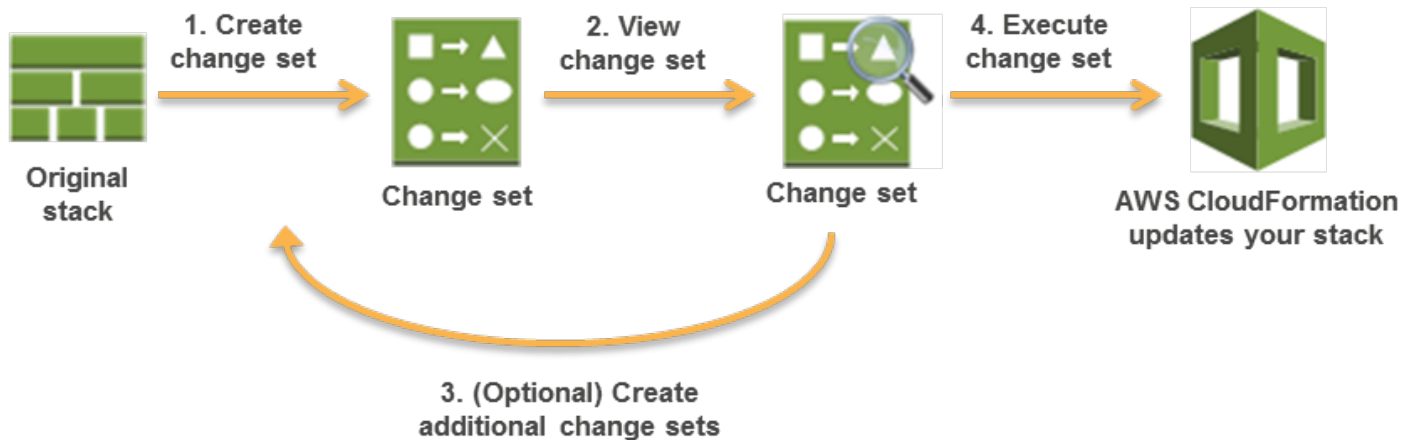
Important

I set di modifiche non indicano se CloudFormation aggiornerà correttamente uno stack. Ad esempio, un set di modifiche non verifica se supererai la quota di un account, se

stai aggiornando una risorsa che non supporta gli aggiornamenti o se non disponi di autorizzazioni sufficienti per modificare una risorsa, il che può causare il fallimento di un aggiornamento dello stack. Se un aggiornamento ha esito negativo, CloudFormation tenta di eseguire il rollback delle risorse allo stato originale.

Panoramica sui set di modifiche

Il seguente diagramma riepiloga come utilizzare i set di modifiche per aggiornare uno stack:



1. Creare un set di modifiche inviando le modifiche per lo stack che si desidera aggiornare. È possibile inviare un modello di stack modificato o valori dei parametri di input modificati. CloudFormation confronta lo stack con le modifiche che hai inviato per generare il set di modifiche; a questo punto non apporta modifiche allo stack.
2. Visualizzare il set di modifiche per vedere quali impostazioni di stack e risorse cambieranno. Ad esempio, puoi vedere quali risorse CloudFormation verranno aggiunte, modificate o eliminate. Inoltre, è possibile visualizzare un before-and-after confronto tra le proprietà e gli attributi delle risorse, ad esempio i tag, che CloudFormation verranno modificati.
3. Facoltativo: se si intende considerare altre modifiche prima di decidere quali modifiche apportare, creare ulteriori set di modifiche. La creazione di più set di modifiche consente di comprendere e valutare in che modo le diverse modifiche influiranno sulle risorse e sulle proprietà. Puoi creare tutti i set di modifiche necessari.
4. Eseguire il set di modifiche che contiene le modifiche da applicare allo stack. CloudFormation aggiorna lo stack con tali modifiche.

 Note

Dopo aver eseguito una modifica, CloudFormation rimuove tutti i set di modifiche associati allo stack perché non sono applicabili allo stack aggiornato.

Puoi eliminare i set di modifiche per evitare l'esecuzione di un set di modifiche che non deve essere applicato.

Creare un set di modifiche per uno CloudFormation stack

Per creare un set di modifiche per uno stack in esecuzione, invia le modifiche che desideri apportare fornendo un modello modificato, nuovi valori dei parametri di input o entrambi. CloudFormation genera un set di modifiche confrontando lo stack con le modifiche inviate.

È possibile modificare un modello prima di creare il set di modifiche o durante la creazione del set di modifiche.

Create a change set (console)

Per creare un set di modifiche

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Stacks, scegli lo stack in esecuzione per cui desideri creare un set di modifiche.
4. Nel riquadro dei dettagli dello stack, scegli Azioni dello stack, quindi scegli Crea un set di modifiche.
5. Nella *stack-name* pagina Crea set di modifiche per, esegui una delle seguenti operazioni per modificare i valori dei parametri di input, specificare la posizione di un modello aggiornato o modificare il modello:

Attività	Azione
Per modificare i valori dei parametri di input	Scegliete Usa modello esistente, quindi scegliete Avanti per procedere all'immissione o alla modifica dei valori dei parametri di input.

Attività	Azione
Per specificare la posizione di un modello aggiornato	Se hai modificato il modello, scegli Sostituisci modello esistente, quindi esegui una delle seguenti operazioni: - Per un modello archiviato in un bucket Amazon S3, seleziona re URL Amazon S3. Inserire o incollare l'URL per il modello, quindi selezionare Next (Avanti). Se hai un modello in un bucket abilitato al controllo delle versioni, puoi specificare una versione specifica del modello ?versionId= version-id aggiungendola all'URL. Per ulteriori informazioni, consulta Lavorare con oggetti in un bucket abilitato al rilascio di versioni nella Guida per l'utente di Amazon Simple Storage Service. - Per un modello memorizzato localmente nel computer, scegliere Upload a template file (Carica un file modello). Scegliere Choose File (Scegli file) per accedere al file e selezionarlo, quindi selezionare Next (Avanti).
Per modificare il modello	Se non hai modificato il modello, scegli Modifica modello in Infrastructure Composer, quindi scegli Modifica in Infrastructure Composer. Sei stato reindirizzato a AWS Infrastructure Composer. Dopo aver modificato il modello, scegli Crea set di modifiche, quindi Conferma e continua per tornare CloudFormation alla pagina Crea set di modifiche per la stack-name pagina, quindi scegli Avanti.

- Nella pagina Specificare i dettagli dello stack, specificate un nome per il set di modifiche e, facoltativamente, specificate una descrizione del set di modifiche per identificarne lo scopo nella sezione Panoramica. Se il modello contiene parametri, nella pagina Specify stack details (Specifica dettagli stack) immettere o modificare i valori dei parametri di input applicabili, quindi selezionare Next (Avanti).

Se state riutilizzando il modello dello stack, CloudFormation compila ogni parametro con il valore corrente nello stack, ad eccezione dei parametri dichiarati con l'attributo. NoEcho Per utilizzare i valori esistenti per quei parametri, selezionare Use existing value (Usa valore esistente).

Per ulteriori informazioni sull'utilizzo per NoEcho mascherare informazioni riservate e sull'utilizzo di parametri dinamici per gestire i segreti, consulta le best practice. [Non incorporare le credenziali nei modelli](#)

7. Nella pagina Configura le opzioni dello stack, aggiorna i tag dello stack, il ruolo del servizio IAM, la politica dello stack, la configurazione del rollback, l'argomento di notifica di Amazon SNS (se applicabile) o i set di modifiche.

 Note

I set di modifiche per gli stack nidificati sono Enabled (Attivati) per impostazione predefinita, il che crea set di modifiche per tutti gli stack nidificati specificati nel modello. Per creare un set di modifiche esclusivamente per lo stack corrente, scegliere Disabled (Disabilitati). Per ulteriori informazioni sui set di modifiche per gli stack annidati, consulta [Set di modifiche per stack nidificati](#)

8. Se il modello include risorse IAM, per Capabilities, scegli Riconosco che CloudFormation potrebbe creare risorse IAM. Le risorse IAM possono modificare le autorizzazioni nell'account AWS esamina queste risorse per assicurarti che vengano consentite solo le operazioni desiderate. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
9. Seleziona Successivo per continuare.
10. Nella **stack-name** pagina Revisione, esamina le modifiche per questo set di modifiche.
11. Scegli Invia.

Si viene reindirizzati alla scheda Changes (Modifiche) dei dettagli del set di modifiche. Durante CloudFormation la generazione del set di modifiche, lo stato del set di modifiche è CREATE_PENDING. Dopo aver creato il set di modifiche, CloudFormation imposta lo stato su CREATE_COMPLETE. Nella sezione Modifiche, CloudFormation elenca tutte le modifiche che apporterà allo stack. Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).

Scegli Visualizza dettagli nella colonna Modifiche a livello di proprietà per visualizzare le modifiche apportate a livello di proprietà.

Se CloudFormation non riesce a creare il set di modifiche (FAILED stato dei report), correggete l'errore visualizzato nel campo Stato, quindi ricreate il set di modifiche.

12. Dopo aver verificato che le modifiche appaiano corrette, scegliete Esegui set di modifiche

Create a change set for nested stacks (console)

Per creare un set di modifiche per gli stack annidati

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Stacks, seleziona lo stack in esecuzione per cui desideri creare un set di modifiche.
4. Nel riquadro dei dettagli dello stack, scegli Azioni dello stack, quindi scegli Crea un set di modifiche.
5. Nella *stack-name* pagina Crea set di modifiche per, esegui una delle seguenti operazioni per modificare i valori dei parametri di input, specificare la posizione di un modello aggiornato o modificare il modello:

Attività	Azione
Per modificare i valori dei parametri di input	Scegliete Usa modello esistente, quindi scegliete Avanti per procedere all'immissione o alla modifica dei valori dei parametri di input.
Per specificare la posizione di un modello aggiornato	Se hai modificato il modello, scegli Sostituisci modello esistente, quindi esegui una delle seguenti operazioni: • Per un modello archiviato in un bucket Amazon S3, seleziona re URL Amazon S3. Inserire o incollare l'URL per il modello, quindi selezionare Next (Avanti). Se hai un modello in un bucket abilitato al controllo delle versioni, puoi specificare una versione specifica del modello ?versionId= <i>version-id</i> aggiungendola all'URL. Per ulteriori informazioni, consulta Lavorare con oggetti in un bucket abilitato al rilascio di versioni nella Guida per l'utente di Amazon Simple Storage Service. • Per un modello memorizzato localmente nel computer, scegliere Upload a template file (Carica un file modello).

Attività	Azione
	Scegliere Choose File (Scegli file) per accedere al file e selezionarlo, quindi selezionare Next (Avanti).
Per modificare il modello	Se non hai modificato il modello, scegli Modifica modello in Infrastructure Composer, quindi scegli Modifica in Infrastructure Composer. Sei stato reindirizzato a AWS Infrastructure Composer. Dopo aver modificato il modello, scegli Crea set di modifiche, quindi Conferma e continua per tornare CloudFormation alla pagina Crea set di modifiche per la stack-name pagina, quindi scegli Avanti.

6. Nella pagina Specificare i dettagli dello stack, specificate un nome per il set di modifiche e, facoltativamente, specificate una descrizione del set di modifiche per identificarne lo scopo nella sezione Panoramica. Se il modello contiene parametri, nella pagina Specify stack details (Specifica dettagli stack) immettere o modificare i valori dei parametri di input applicabili, quindi selezionare Next (Avanti).

Se state riutilizzando il modello dello stack, CloudFormation compila ogni parametro con il valore corrente nello stack, ad eccezione dei parametri dichiarati con l'attributo. NoEcho Per utilizzare i valori esistenti per quei parametri, selezionare Use existing value (Usa valore esistente).

Per ulteriori informazioni sull'utilizzo per NoEcho mascherare informazioni riservate e sull'utilizzo di parametri dinamici per la gestione dei segreti, consulta le best practice. [Non incorporare le credenziali nei modelli](#)

7. Nella pagina Configura le opzioni dello stack, aggiorna i tag dello stack, il ruolo del servizio IAM, la politica dello stack, la configurazione del rollback, l'argomento di notifica di Amazon SNS (se applicabile) o i set di modifiche. Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#).

Note

I set di modifiche per gli stack nidificati sono Enabled (Attivati) per impostazione predefinita, il che crea set di modifiche per tutti gli stack nidificati specificati nel modello. Per ulteriori informazioni sui set di modifiche per gli stack annidati, consulta [Set di modifiche per stack nidificati](#)

8. Se il modello include risorse IAM, per Capabilities, scegli Riconosco che CloudFormation potrebbe creare risorse IAM. Le risorse IAM possono modificare le autorizzazioni nell'account AWS esamina queste risorse per assicurarti che vengano consentite solo le operazioni desiderate. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
9. Seleziona Successivo per continuare.
10. Nella *stack-name* pagina Revisione, esamina le modifiche per questo set di modifiche.
11. Scegli Invia.

 Note

CloudFormation i set di modifiche a livello di proprietà non risolvono i riferimenti incrociati quando si creano set di modifiche per pile nidificate. I set di modifiche possono contrassegnare le risorse in uno stack secondario per la sostituzione condizionale se fanno riferimento all'output di uno stack principale e lo stack principale è stato modificato

Si viene reindirizzati alla scheda Changes (Modifiche) dei dettagli del set di modifiche. Durante la CloudFormation generazione del set di modifiche, lo stato del set di modifiche è. CREATE_PENDING Dopo aver creato il set di modifiche, CloudFormation imposta lo stato su CREATE_COMPLETE. Nella sezione Modifiche, CloudFormation elenca tutte le modifiche che apporterà allo stack. Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).

Se CloudFormation non riesce a creare il set di modifiche (riporta FAILED lo stato), correggete l'errore visualizzato nel campo Stato, quindi ricreate il set di modifiche.

12. Dopo aver verificato che le modifiche appaiano corrette, scegliete Esegui set di modifiche

Per creare un set di modifiche (AWS CLI)

- Utilizza il comando [create-change-set](#).

Le modifiche vengono inviate come opzioni di comando. È possibile specificare i nuovi valori dei parametri, un modello modificato o entrambi. Ad esempio, il comando seguente crea un set di modifiche denominato SampleChangeSet per lo stack MyStack. Il set di modifiche utilizza l'attuale modello di stack, ma con un valore diverso per il parametro Purpose:

```
aws cloudformation create-change-set --stack-name MyStack \  
  --change-set-name SampleChangeSet --use-previous-template \  
  --parameters \  
    ParameterKey="InstanceType",UsePreviousValue=true  
    ParameterKey="KeyPairName",UsePreviousValue=true  
    ParameterKey="Purpose",ParameterValue="production"
```

Visualizzare un set di modifiche per uno CloudFormation stack

Dopo aver creato un set di modifiche, è possibile visualizzare le modifiche proposte prima della loro esecuzione. Puoi utilizzare la CloudFormation console o l' AWS CLI CloudFormation API per visualizzare i set di modifiche. La console CloudFormation fornisce un riepilogo delle modifiche e un elenco dettagliato delle modifiche in formato JSON. L' AWS CloudFormation API AWS CLI and restituisce un elenco dettagliato delle modifiche in formato JSON.

View a change set (console)

Per visualizzare un set di modifiche

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Pile, scegli il nome dello stack che contiene il set di modifiche che desideri visualizzare.
4. Nel riquadro di navigazione, selezionare Change Sets (Set di modifiche) per visualizzare un elenco del set di modifiche dello stack.
5. Selezionare il nome del set di modifiche che si desidera visualizzare.

La CloudFormation console indirizza l'utente alla pagina dei dettagli del set di modifiche, dove è possibile visualizzare l'ora di creazione del set di modifiche, il relativo stato, l'input utilizzato per generare il set di modifiche e un riepilogo delle modifiche.

Nella sezione Changes (Modifiche) ogni riga rappresenta una risorsa che CloudFormation aggiungerà, modificherà o rimuoverà.

- Aggiungi: CloudFormation crea una risorsa quando aggiungi una risorsa al modello dello stack.

- **Modifica:** CloudFormation modifica una risorsa quando si modificano le proprietà di una risorsa nel modello dello stack.
- **Rimuovi:** CloudFormation elimina una risorsa quando elimini una risorsa dal modello dello stack.

 Note

Una modifica può causare l'interruzione o la sostituzione (nuova creazione) della risorsa. Per ulteriori informazioni sui comportamenti di aggiornamento delle risorse, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

Per concentrarsi sulle modifiche specifiche, utilizzare la visualizzazione filtro. Ad esempio, il filtro per un determinato tipo di risorsa, ad esempio `AWS::EC2::Instance`. Per filtrare una risorsa specifica, specificare l'ID logico o fisico, ad esempio `myWebServer` o `i-123abcd4`.

6. Nella sezione Modifiche, scegli Visualizza dettagli nella colonna Modifiche a livello di proprietà per visualizzare le modifiche al valore delle proprietà apportate alla risorsa.
7. La CloudFormation console indirizza l'utente alla pagina delle modifiche a livello di proprietà per una risorsa, in cui è possibile visualizzare la configurazione del modello della risorsa prima di eseguire un set di modifiche e l'aspetto della configurazione del modello dopo l'esecuzione del set di modifiche.

La tabella della sezione Modifiche a livello di proprietà mostra i valori Path, Change type, Before e After per le proprietà interessate. Nella tabella, scegli la casella di controllo per ogni modifica che desideri evidenziare nelle viste Prima e Dopo del modello per vedere quali modifiche verranno apportate a livello di proprietà.

- **Aggiungi:** le proprietà aggiunte sono evidenziate in verde.
- **Modifica:** le proprietà modificate sono evidenziate in blu.
- **Rimuovi:** le proprietà rimosse sono evidenziate in rosso.

View a change set for nested stack (console)

Per visualizzare un set di modifiche per gli stack nidificati (console)

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.

2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Pile, scegli il nome dello stack che contiene il set di modifiche che desideri visualizzare.
4. Nel pannello di navigazione, scegli Cambia set per visualizzare un elenco dei set di modifiche dello stack.
5. Selezionare il nome del set di modifiche che si desidera visualizzare.

La CloudFormation console indirizza l'utente alla pagina dei dettagli del set di modifiche, dove è possibile visualizzare l'ora di creazione del set di modifiche, il relativo stato, l'input utilizzato per generare il set di modifiche e un riepilogo delle modifiche.

Nella sezione Changes (Modifiche), ogni riga rappresenta una risorsa che CloudFormation consente di aggiungere, modificare, rimuovere o visualizzare lo stato di dinamica.

- **Aggiungi:** CloudFormation crea una risorsa quando aggiungi una risorsa al modello dello stack.
- **Modifica:** CloudFormation modifica una risorsa quando si modificano le proprietà di una risorsa nel modello dello stack.
- **Rimuovi:** CloudFormation elimina una risorsa quando elimini una risorsa dal modello dello stack.
- **Dinamico:** non è CloudFormation possibile determinare l'esatta azione di modifica delle risorse dal modello dello stack annidato.

Note

Una modifica può causare l'interruzione o la sostituzione (nuova creazione) della risorsa. Per ulteriori informazioni sui comportamenti di aggiornamento delle risorse, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

Per concentrarsi sulle modifiche specifiche, utilizzare la visualizzazione filtro. Ad esempio, il filtro per un determinato tipo di risorsa, ad esempio **AWS::CloudFormation::Stack**. Per filtrare una risorsa specifica, specificare l'ID logico o fisico, ad esempio **DeadLetterQueue** o **NestedStack**.

6. Nella sezione Modificazioni scegliere Visualizza set di modifiche nidificato del set di modifiche nidificato che si desidera visualizzare.

La CloudFormation console indirizza l'utente alla pagina dei dettagli del set di modifiche nidificato. È possibile scegliere [Vai al set di modifiche root](#) per visualizzare il set di modifiche root oppure scegliere [Visualizza set di modifiche padre](#) per visualizzare il set di modifiche padre. Per ulteriori informazioni, consultare [Set di modifiche per stack nidificati](#).

 Note

CloudFormation i set di modifiche a livello di proprietà non risolvono i riferimenti incrociati quando si creano set di modifiche per pile nidificate. I set di modifiche possono contrassegnare le risorse in uno stack secondario per la sostituzione condizionale se fanno riferimento all'output di uno stack principale e lo stack principale è stato modificato

Per visualizzare un set di modifiche (AWS CLI)

1. Per ottenere l'ID del set di modifiche, esegui il [change-sets](#) comando.

Specificate il nome dello stack contenente il set di modifiche che desiderate visualizzare, come illustrato nell'esempio seguente:

```
aws cloudformation list-change-sets --stack-name MyStack
```

CloudFormation restituisce un elenco di set di modifiche, simile al seguente:

```
{
  "Summaries": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
      "Status": "CREATE_COMPLETE",
      "ChangeSetName": "SampleChangeSet",
      "CreationTime": "2020-11-18T20:44:05.889Z",
      "StackName": "MyStack",
      "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000"
    },
    {
```

```

    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
    "Status": "CREATE_COMPLETE",
    "ChangeSetName": "SampleChangeSet-conditional",
    "CreationTime": "2020-11-18T21:15:56.398Z",
    "StackName": "MyStack",
    "ChangeSetId": "arn:aws:cloudformation:us-
east-1:123456789012:changeSet/SampleChangeSet-conditional/1a2345b6-0000-00a0-
a123-00abc0abc000"
  },
  {
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
    "Status": "CREATE_COMPLETE",
    "ChangeSetName": "SampleChangeSet-replacement",
    "CreationTime": "2020-11-18T21:03:37.706Z",
    "StackName": "MyStack",
    "ChangeSetId": "arn:aws:cloudformation:us-
east-1:123456789012:changeSet/SampleChangeSet-replacement/1a2345b6-0000-00a0-
a123-00abc0abc000"
  }
]
}

```

2. Eseguire [describe-change-set](#) comando, specificando l'ID del set di modifiche che si desidera visualizzare. Per esempio:

```

aws cloudformation describe-change-set \
  --change-set-name arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000

```

CloudFormation restituisce informazioni sul set di modifiche specificato.

```

{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "Status": "CREATE_COMPLETE",
  "ChangeSetName": "SampleChangeSet-direct",
  "Parameters": [
    {
      "ParameterValue": "testing",
      "ParameterKey": "Purpose"
    }
  ],

```



```
{
  "ParameterValue": "ellioty-useast1",
  "ParameterKey": "KeyPairName"
},
{
  "ParameterValue": "t2.micro",
  "ParameterKey": "InstanceType"
}
],
"Changes": [
  {
    "ResourceChange": {
      "ResourceType": "AWS::EC2::Instance",
      "PhysicalResourceId": "i-1abc23d4",
      "Details": [
        {
          "ChangeSource": "DirectModification",
          "Evaluation": "Static",
          "Target": {
            "Attribute": "Tags",
            "RequiresRecreation": "Never"
          }
        }
      ],
      "Action": "Modify",
      "Scope": [
        "Tags"
      ],
      "LogicalResourceId": "MyEC2Instance",
      "Replacement": "False"
    },
    "Type": "Resource"
  }
],
"CreationTime": "2020-11-18T23:35:25.813Z",
"Capabilities": [],
"StackName": "MyStack",
"NotificationARNs": [],
"ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet-direct/9edde307-960d-4e6e-ad66-b09ea2f20255"
}
```

Utilizzare `--include-property-values` con `describe-change-set` per elencare le modifiche a livello di proprietà.

La chiave `Changes` elenca le modifiche apportate alle risorse. Se dovessi eseguire questo set di modifiche, CloudFormation aggiornerebbe i tag dell'`i-1abc23d4` EC2 istanza. Per una descrizione di ogni campo, consulta il tipo di [Change](#) dati nell'AWS CloudFormation API Reference.

Per ulteriori esempi di set di modifiche, consulta [Esempi di set di modifiche per le CloudFormation pile](#).

Per visualizzare le modifiche a livello di proprietà in un set di modifiche ()AWS CLI

- Il comando seguente elenca le modifiche a livello di proprietà relative a un set di modifiche per una `AWS::EC2::NetworkInterface` risorsa che rimuoverà la `Ipv4Prefixes` proprietà, modifica le modifiche `Description` relative alla risorsa e aggiunge un: `Tag`

```
aws cloudformation describe-change-set --include-property-values \  
--change-set-name arn:aws:cloudformation:us-east-1:123456789012:changeSet/  
ExampleChangeSet/9f7b541b-126b-44f7-998e-932174557841
```

Di seguito è riportato un output di esempio.

```
"ChangeSetName": "ExampleChangeSet",  
  "ChangeSetId": "arn:aws:cloudformation:us-east-1:803642222207:changeSet/  
ExampleChangeSet/9f7b541b-126b-44f7-998e-932174557841",  
  "StackId": "arn:aws:cloudformation:us-east-1:803642222207:stack/ExampleStack/  
ab664180-f686-11ee-9e29-12cd92393671",  
  "StackName": "ExampleStack",  
  "Description": null,  
  "Parameters": null,  
  "CreationTime": "2024-04-09T18:04:59.935000+00:00",  
  "ExecutionStatus": "AVAILABLE",  
  "Status": "CREATE_COMPLETE",  
  "StatusReason": null,  
  "NotificationARNs": [],  
  "RollbackConfiguration": {  
    "RollbackTriggers": []  
  },  
  "Capabilities": [],
```

```

    "Tags": null,
    "ParentChangeSetId": null,
    "IncludeNestedStacks": true,
    "RootChangeSetId": null,
    "OnStackFailure": null,
  {
    "Changes": [
      {
        "Type": "Resource",
        "ResourceChange": {
          "Action": "Modify",
          "LogicalResourceId":
"EC2NetworkInterface00eni067fd35b649a05b7100Tpyls",
          "PhysicalResourceId": "eni-067fd35b649a05b71",
          "ResourceType": "AWS::EC2::NetworkInterface",
          "Replacement": "False",
          "Scope": [
            "Properties",
            "Tags"
          ],
          "Details": [
            {
              "Target": {
                "Attribute": "Properties",
                "Name": "Ipv4Prefixes",
                "RequiresRecreation": "Never",
                "Path": "/Properties/Ipv4Prefixes",
                "BeforeValue": "[]",
                "AttributeChangeType": "Remove"
              },
              "Evaluation": "Static",
              "ChangeSource": "DirectModification"
            },
            {
              "Target": {
                "Attribute": "Properties",
                "Name": "Description",
                "RequiresRecreation": "Never",
                "Path": "/Properties/Description",
                "BeforeValue": "",
                "AfterValue": "Description",
                "AttributeChangeType": "Modify"
              },
              "Evaluation": "Static",

```

```

        "ChangeSource": "DirectModification"
    },
    {
        "Target": {
            "Attribute": "Tags",
            "RequiresRecreation": "Never",
            "Path": "/Properties/Tags/0",
            "AfterValue": "{\"Key\":\"Test\",\"Value\":\"Test\"}",
            "AttributeChangeType": "Add"
        },
        "Evaluation": "Static",
        "ChangeSource": "DirectModification"
    }
],
    "BeforeContext": "{\"Properties\":{\"Description\":\"\",
    \"PrivateIpAddress\":\"172.31.76.2\", \"PrivateIpAddresses\": [{\"PrivateIpAddress
    \": \"172.31.76.2\", \"Primary\": \"true\"}], \"SecondaryPrivateIpAddressCount\": \"0\",
    \"Ipv6PrefixCount\": \"0\", \"Ipv4Prefixes\": [], \"Ipv4PrefixCount\": \"0\", \"GroupSet
    \": [\"sg-05a45689b1059e82d\"], \"Ipv6Prefixes\": [], \"SubnetId\": \"subnet-455e8969\",
    \"SourceDestCheck\": \"true\", \"InterfaceType\": \"interface\", \"Tags\": []},
    \"UpdateReplacePolicy\": \"Retain\", \"DeletionPolicy\": \"Retain\"}",
    "AfterContext": "{\"Properties\":{\"Description\":\"Description\",
    \"PrivateIpAddress\":\"172.31.76.2\", \"PrivateIpAddresses\": [{\"PrivateIpAddress
    \": \"172.31.76.2\", \"Primary\": \"true\"}], \"SecondaryPrivateIpAddressCount
    \": \"0\", \"Ipv6PrefixCount\": \"0\", \"Ipv4PrefixCount\": \"0\", \"GroupSet\":
    [\"sg-05a45689b1059e82d\"], \"Ipv6Prefixes\": [], \"SubnetId\": \"subnet-455e8969\",
    \"SourceDestCheck\": \"true\", \"InterfaceType\": \"interface\", \"Tags\": [{\"Value\":
    \"Test\", \"Key\": \"Test\"}]}, \"UpdateReplacePolicy\": \"Retain\", \"DeletionPolicy\":
    \"Retain\"}"
    }
}
],
    "ChangeSetName": "ExampleChangeSet",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
    ExampleChangeSet/9f7b541b-126b-44f7-998e-932174557841",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/ExampleStack/
    ab664180-f686-11ee-9e29-12cd92393671",

```

Esegui un set di modifiche per uno CloudFormation stack

Per eseguire le modifiche descritte in un set di modifiche allo stack, esegui il set di modifiche.

 Important

Dopo aver eseguito un set di modifiche, CloudFormation elimina tutti i set di modifiche aggiuntivi associati allo stack perché non sono più validi per lo stack aggiornato. Se l'aggiornamento ha esito negativo, devi creare un nuovo set di modifiche.

Policy stack ed esecuzione di un set di modifiche

Se si esegue un set di modifiche su uno stack che dispone di una policy stack associata, CloudFormation applica la policy quando aggiorna lo stack. Non è possibile specificare una policy di stack temporanea che sovrascrive la policy esistente quando esegui un set di modifiche. Per aggiornare una risorsa protetta, devi aggiornare la policy stack o utilizzare il metodo aggiornamento diretto. Per ulteriori informazioni, consulta [Aggiorna direttamente gli stack](#).

Execute a change set (console)

Per eseguire un set di modifiche

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Stack, scegli il nome dello stack che desideri aggiornare.
4. Nel riquadro di navigazione, scegli Modifica set per visualizzare un elenco dei set di modifiche dello stack.
5. Selezionare il nome del set di modifiche che si desidera eseguire.
6. Nella pagina dei dettagli del set di modifiche, scegli Esegui set di modifiche.

CloudFormation inizia immediatamente ad aggiornare lo stack. La CloudFormation console ti indirizza alla scheda Eventi, dove puoi monitorare lo stato di avanzamento dell'aggiornamento dello stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Execute a change set for nested stacks (console)

Per eseguire un set di modifiche per gli stack annidati

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS

3. Nella pagina Stack, scegli il nome dello stack che desideri aggiornare. È necessario scegliere il nome dello stack associato al set di modifiche root.
4. Nel riquadro di navigazione, scegli Modifica set per visualizzare un elenco dei set di modifiche dello stack.
5. Scegliere il nome del set di modifiche root che si desidera eseguire.
6. Nella pagina dei dettagli del set di modifiche, scegli Esegui set di modifiche.

 Note

CloudFormation esegue le modifiche descritte nel set di modifiche principale e nei set di modifiche nidificati, se durante il processo è stata selezionata l'opzione Enabled for change set for nested stack. [Creare un set di modifiche per uno CloudFormation stack](#)

CloudFormation avvia immediatamente l'aggiornamento dello stack. La CloudFormation console ti indirizza alla scheda Eventi, dove puoi monitorare lo stato di avanzamento dell'aggiornamento dello stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Per eseguire un set di modifiche (AWS CLI)

- Eseguire [execute-change-set](#) comando.

Specificare l'ID set di modifiche che ha il set di modifiche che si desidera eseguire, come nell'esempio seguente:

```
aws cloudformation execute-change-set \  
  --change-set-name \  
    arn:aws:cloudformation:us-east-1:123456789012:changeSet/  
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000
```

Il comando dell'esempio esegue un set di modifiche con l'ID `arn:aws:cloudformation:us-east-1:123456789012:changeSet/SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000`.

Dopo aver eseguito il comando, CloudFormation inizia l'aggiornamento dello stack. Per visualizzare l'avanzamento dello stack, usa il comando [describe-stacks](#).

Eliminare un set di modifiche per uno CloudFormation stack

L'eliminazione di un set di modifiche lo rimuove dall'elenco dei set di modifiche per lo stack.

L'eliminazione di un set di modifiche impedisce a un utente di eseguire accidentalmente un set di modifiche che non dovrebbe essere applicato. A meno che non li elimini, CloudFormation conserva tutti i set di modifiche finché non aggiorni lo stack.

Delete a change set

Per eliminare un set di modifiche (console)

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Pile, seleziona il nome dello stack che contiene il set di modifiche che desideri eliminare.
4. Nel pannello di navigazione, scegli Cambia set per visualizzare un elenco dei set di modifiche dello stack.
5. Selezionare il nome del set di modifiche che si desidera eliminare.
6. Nella pagina dei dettagli del set di modifiche, scegli Elimina set di modifiche.

CloudFormation inizia immediatamente a eliminare il set di modifiche dall'elenco dei set di modifiche dello stack e verrai reindirizzato alla pagina Pile.

Delete a change set for nested stacks (console)

Per eliminare un set di modifiche per gli stack annidati

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Stacks, selezionate il nome dello stack associato al root change set.
4. Nel riquadro di navigazione, scegli Cambia set per visualizzare un elenco dei set di modifiche dello stack.

5. Selezionare il nome del set di modifiche che si desidera eliminare.
6. Nella pagina dei dettagli del set di modifiche, scegliere Delete (Elimina). Scegliendo Elimina set di modifiche, eliminerai l'intera gerarchia dei set di modifiche annidati.

 Note

L'operazione di eliminazione per i set di modifiche per gli stack nidificati è asincrona e mostrerà uno stato DELETE_PENDING seguito da uno stato DELETE_IN_PROGRESS. Al termine dell'operazione di eliminazione del set di modifiche, i set di modifiche verranno rimossi dall'elenco. Anche gli stack nidificati nello stato REVIEW_IN_PROGRESS verranno eliminati se sono stati creati durante la creazione dei set di modifiche.

CloudFormation inizia immediatamente a eliminare il set di modifiche dall'elenco dei set di modifiche dello stack.

 Note

Se disponi di stack nidificati bloccati in un'operazione in corso, consulta la sezione relativa alla risoluzione degli errori in [Errore di rollback degli stack annidati](#).

Per eliminare un set di modifiche (AWS CLI)

- Eseguire il comando [delete-change-set](#), specificando l'ID del set di modifiche che si desidera eliminare, come nell'esempio seguente:

```
aws cloudformation delete-change-set \  
  --change-set-name \  
    arn:aws:cloudformation:us-east-1:123456789012:changeSet/  
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000
```

Esempi di set di modifiche per le CloudFormation pile

Questa sezione fornisce esempi dei set di modifiche che si CloudFormation potrebbero creare per le modifiche più comuni allo stack. Mostrano come modificare un modello direttamente,

modificare un parametro di input singolo. pianificare per la ricreazione di risorse (sostituzioni), che impedisce di perdere i dati per i quali non è stato eseguito il backup o interrompere le applicazioni che sono in esecuzione nello stack; , nonché aggiungere e rimuovere le risorse. Per illustrare il modo in cui funzionano i set di modifiche, ti mostreremo le modifiche inviate e parleremo dei set di modifiche risultanti. Poiché ogni esempio si basa su e presuppone che l'esempio precedente sia stato compreso, ti consigliamo di leggerli in ordine. Per una descrizione di ogni campo in un set di modifiche, consulta il tipo di dati [Change](#) (Modifica) nella Documentazione di riferimento all'API di AWS CloudFormation .

È possibile utilizzare la [console](#) o il AWS CLI funzionamento dell' CloudFormation [DescribeChangeSet](#)API per visualizzare i dettagli dei set di modifiche.

Abbiamo generato ciascuno dei seguenti set di modifiche da uno stack con il seguente [modello di esempio](#):

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "A sample EC2 instance template for testing change sets.",
  "Parameters" : {
    "Purpose" : {
      "Type" : "String",
      "Default" : "testing",
      "AllowedValues" : ["testing", "production"],
      "Description" : "The purpose of this instance."
    },
    "KeyPairName" : {
      "Type": "AWS::EC2::KeyPair::KeyName",
      "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the
instance"
    },
    "InstanceType" : {
      "Type" : "String",
      "Default" : "t2.micro",
      "AllowedValues" : ["t2.micro", "t2.small", "t2.medium"],
      "Description" : "The EC2 instance type."
    }
  },
  "Resources" : {
    "MyEC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "KeyName" : { "Ref" : "KeyPairName" },
```

```

    "InstanceType" : { "Ref" : "InstanceType" },
    "ImageId" : "ami-8fcee4e5",
    "Tags" : [
      {
        "Key" : "Purpose",
        "Value" : { "Ref" : "Purpose" }
      }
    ]
  }
}
}
}
}
}

```

Modifica diretta di un modello

Quando si modificano direttamente le risorse nel modello dello stack per generare un set di modifiche, CloudFormation classifica la modifica come diretta, anziché come modifica iniziata da un valore di parametro aggiornato. I seguenti set di modifiche, che hanno aggiunto un nuovo tag all'istanza `i-1abc23d4`, è un esempio di modifica diretta. Tutti gli altri valori di input, ad esempio i valori dei parametri e le capacità, sono invariati, perciò ci concentreremo sulla struttura `Changes`.

```

{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "Status": "CREATE_COMPLETE",
  "ChangeSetName": "SampleChangeSet-direct",
  "Parameters": [
    {
      "ParameterValue": "testing",
      "ParameterKey": "Purpose"
    },
    {
      "ParameterValue": "MyKeyName",
      "ParameterKey": "KeyPairName"
    },
    {
      "ParameterValue": "t2.micro",
      "ParameterKey": "InstanceType"
    }
  ],
  "Changes": [
    {
      "ResourceChange": {

```

```

    "ResourceType": "AWS::EC2::Instance",
    "PhysicalResourceId": "i-1abc23d4",
    "Details": [
      {
        "ChangeSource": "DirectModification",
        "Evaluation": "Static",
        "Target": {
          "Attribute": "Tags",
          "RequiresRecreation": "Never"
        }
      }
    ],
    "Action": "Modify",
    "Scope": [
      "Tags"
    ],
    "LogicalResourceId": "MyEC2Instance",
    "Replacement": "False"
  },
  "Type": "Resource"
}
],
"CreationTime": "2020-11-18T23:35:25.813Z",
"Capabilities": [],
"StackName": "MyStack",
"NotificationARNs": [],
"ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet-direct/1a2345b6-0000-00a0-a123-00abc0abc000"
}

```

Nella struttura `Changes`, c'è solo una struttura `ResourceChange`. Questa struttura descrive informazioni come il tipo di risorsa che CloudFormation verrà modificato, l'azione che CloudFormation verrà intrapresa, l'ID della risorsa, l'ambito della modifica e se la modifica richiede una sostituzione (dove CloudFormation crea una nuova risorsa e quindi elimina quella precedente). Nell'esempio, il set di modifiche indica che CloudFormation modificherà l'attributo `Tags` dell'istanza `i-1abc23d4` EC2 e non richiede la sostituzione dell'istanza.

Nella `Details` struttura, CloudFormation etichetta questa modifica come una modifica diretta che non richiederà mai la ricreazione (sostituzione) dell'istanza. Puoi eseguire questa modifica con sicurezza, sapendo che CloudFormation non sostituirà l'istanza.

CloudFormation mostra questa modifica come `Static` valutazione. Una valutazione statica significa che CloudFormation può determinare il valore del tag prima di eseguire il set di modifiche. In alcuni casi, CloudFormation può determinare un valore solo dopo aver eseguito un set di modifiche. CloudFormation etichetta tali modifiche come `Dynamic` valutazioni. Ad esempio, se si fa riferimento a una risorsa aggiornata sostituita in modo condizionale, non è CloudFormation possibile determinare se il riferimento alla risorsa aggiornata cambierà.

Modifica del valore di un parametro di input.

Quando modificate il valore di un parametro di input, CloudFormation genera due modifiche per ogni risorsa che utilizza il valore del parametro aggiornato. In questo esempio, desideriamo evidenziare come appariranno tali modifiche e su quali informazioni dovresti concentrarti. L'esempio seguente è stato generato modificando solo il valore del parametro di input `Purpose`.

Il `Purpose` parametro specifica un valore chiave del tag per l' EC2 istanza. In questo esempio, il valore di parametro è stato modificato da `testing` a `production`. Il nuovo valore viene illustrato nella struttura `Parameters`.

```
{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "Status": "CREATE_COMPLETE",
  "ChangeSetName": "SampleChangeSet",
  "Parameters": [
    {
      "ParameterValue": "production",
      "ParameterKey": "Purpose"
    },
    {
      "ParameterValue": "MyKeyName",
      "ParameterKey": "KeyPairName"
    },
    {
      "ParameterValue": "t2.micro",
      "ParameterKey": "InstanceType"
    }
  ],
  "Changes": [
    {
      "ResourceChange": {
        "ResourceType": "AWS::EC2::Instance",
        "PhysicalResourceId": "i-1abc23d4",
```

```

        "Details": [
            {
                "ChangeSource": "DirectModification",
                "Evaluation": "Dynamic",
                "Target": {
                    "Attribute": "Tags",
                    "RequiresRecreation": "Never"
                }
            },
            {
                "CausingEntity": "Purpose",
                "ChangeSource": "ParameterReference",
                "Evaluation": "Static",
                "Target": {
                    "Attribute": "Tags",
                    "RequiresRecreation": "Never"
                }
            }
        ],
        "Action": "Modify",
        "Scope": [
            "Tags"
        ],
        "LogicalResourceId": "MyEC2Instance",
        "Replacement": "False"
    },
    "Type": "Resource"
}
],
"CreationTime": "2020-11-18T23:59:18.447Z",
"Capabilities": [],
"StackName": "MyStack",
"NotificationARNs": [],
"ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000"
}

```

La Changes struttura funziona in modo simile a quello illustrato nell'[Modifica diretta di un modello](#) esempio. Esiste solo una ResourceChange struttura, che descrive una modifica all'Tagsattributo dell'i-1abc23d4 EC2 istanza.

Tuttavia, nella struttura Details, il set di modifiche mostra due modifiche per l'attributo Tags, anche se solo un singolo valore di parametro è stato modificato. Le risorse che referenziano un valore di

parametro modificato (tramite la funzione intrinseca `Ref`) risultano sempre in due modifiche: una con una valutazione `Dynamic` e un'altra con una valutazione `Static`. Puoi visualizzare questi tipi di modifiche visualizzando i campi riportati di seguito:

- Per la modifica della valutazione `Static`, visualizza il campo `ChangeSource`. In questo esempio, il campo `ChangeSource` equivale a `ParameterReference`, il che significa che questa modifica è il risultato del valore di riferimento di un parametro aggiornato. Il set di modifiche deve contenere una modifica di valutazione `Dynamic` simile.
- Puoi trovare la valutazione `Dynamic` corrispondente confrontando la struttura `Target` per entrambe le modifiche, che conterranno le stesse informazioni. In questo esempio, le strutture `Target` per entrambe le modifiche contengono gli stessi valori per i campi `Attribute` e `RequireRecreation`.

Per questi tipi di modifiche, concentrarsi sulla valutazione statica, che offre le informazioni più dettagliate sulla modifica. In questo esempio, la valutazione statica mostra che la modifica è il risultato di una modifica del valore di riferimento di un parametro (`ParameterReference`). L'esatto parametro che è stato modificato è indicato dal campo `CauseEntity` (il parametro `Purpose`).

Determinazione del valore del campo sostitutivo

Il `Replacement` campo in una `ResourceChange` struttura indica se CloudFormation ricreerà la risorsa. La pianificazione per la ricreazione di risorse (sostituzioni) impedisce di perdere i dati per i quali non è stato eseguito il backup o interrompere le applicazioni che sono in esecuzione nello stack.

Il valore nel campo `Replacement` varia a seconda che una modifica richieda una sostituzione o meno, come indicato dal campo `RequiresRecreation` nella struttura `Target` di una modifica. Ad esempio, se il campo `RequiresRecreation` è `Never`, il campo `Replacement` è `False`. Tuttavia, se sono presenti più modifiche su una singola risorsa e ogni modifica ha un valore diverso per il `RequiresRecreation` campo, CloudFormation aggiorna la risorsa utilizzando il comportamento più intrusivo. In altre parole, se solo una delle molte modifiche richiede una sostituzione, CloudFormation deve sostituire la risorsa e, di conseguenza, impostare il campo `Replacement` su `True`.

Il seguente set di modifiche è stato generato modificando i valori di ogni parametro (`PurposeInstanceType`, `eKeyPairName`), tutti utilizzati dall' EC2 istanza. Con queste modifiche, CloudFormation sarà necessario sostituire l'istanza perché il `Replacement` campo è uguale a `True`.

```
{
```

```

    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
    "Status": "CREATE_COMPLETE",
    "ChangeSetName": "SampleChangeSet-multiple",
    "Parameters": [
      {
        "ParameterValue": "production",
        "ParameterKey": "Purpose"
      },
      {
        "ParameterValue": "MyNewKeyName",
        "ParameterKey": "KeyPairName"
      },
      {
        "ParameterValue": "t2.small",
        "ParameterKey": "InstanceType"
      }
    ],
    "Changes": [
      {
        "ResourceChange": {
          "ResourceType": "AWS::EC2::Instance",
          "PhysicalResourceId": "i-7bef86f8",
          "Details": [
            {
              "ChangeSource": "DirectModification",
              "Evaluation": "Dynamic",
              "Target": {
                "Attribute": "Properties",
                "Name": "KeyName",
                "RequiresRecreation": "Always"
              }
            },
            {
              "ChangeSource": "DirectModification",
              "Evaluation": "Dynamic",
              "Target": {
                "Attribute": "Properties",
                "Name": "InstanceType",
                "RequiresRecreation": "Conditionally"
              }
            }
          ],
          {
            "ChangeSource": "DirectModification",

```

```
        "Evaluation": "Dynamic",
        "Target": {
            "Attribute": "Tags",
            "RequiresRecreation": "Never"
        }
    },
    {
        "CausingEntity": "KeyPairName",
        "ChangeSource": "ParameterReference",
        "Evaluation": "Static",
        "Target": {
            "Attribute": "Properties",
            "Name": "KeyName",
            "RequiresRecreation": "Always"
        }
    },
    {
        "CausingEntity": "InstanceType",
        "ChangeSource": "ParameterReference",
        "Evaluation": "Static",
        "Target": {
            "Attribute": "Properties",
            "Name": "InstanceType",
            "RequiresRecreation": "Conditionally"
        }
    },
    {
        "CausingEntity": "Purpose",
        "ChangeSource": "ParameterReference",
        "Evaluation": "Static",
        "Target": {
            "Attribute": "Tags",
            "RequiresRecreation": "Never"
        }
    }
],
"Action": "Modify",
"Scope": [
    "Tags",
    "Properties"
],
"LogicalResourceId": "MyEC2Instance",
"Replacement": "True"
},
```



```

        "Type": "Resource"
    },
    ],
    "CreationTime": "2020-11-18T00:39:35.974Z",
    "Capabilities": [],
    "StackName": "MyStack",
    "NotificationARNs": [],
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet-multiple/1a2345b6-0000-00a0-a123-00abc0abc000"
}

```

Identificare la modifica che richiede che la risorsa venga sostituita visualizzando ogni modifica (le valutazioni statiche nella struttura `Details`). In questo esempio, ogni modifica ha un valore diverso per il `RequireRecreation` campo, ma la modifica alla `KeyName` proprietà ha il comportamento di aggiornamento più intrusivo, che richiede sempre una ricreazione. CloudFormation sostituirà l'istanza perché il nome della chiave è stato modificato.

Se il nome della chiave è invariato, la modifica alla proprietà `InstanceType` comporterebbe l'aggiornamento più intrusivo (`Conditionally`), in modo che il campo `Replacement` sia `Conditionally`. Per trovare le condizioni in cui CloudFormation sostituisce l'istanza, visualizza il comportamento di aggiornamento per la `InstanceType` proprietà del tipo di [AWS::EC2::Instance](#) risorsa.

Aggiunta e rimozione di risorse

L'esempio seguente è stato generato inviando un modello modificato che rimuove l' EC2 istanza e aggiunge un gruppo Auto Scaling e una configurazione di avvio.

```

{
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
    "Status": "CREATE_COMPLETE",
    "ChangeSetName": "SampleChangeSet-addremove",
    "Parameters": [
        {
            "ParameterValue": "testing",
            "ParameterKey": "Purpose"
        },
        {
            "ParameterValue": "MyKeyName",
            "ParameterKey": "KeyPairName"
        }
    ],
}

```

```

    {
      "ParameterValue": "t2.micro",
      "ParameterKey": "InstanceType"
    }
  ],
  "Changes": [
    {
      "ResourceChange": {
        "Action": "Add",
        "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
        "Scope": [],
        "Details": [],
        "LogicalResourceId": "AutoScalingGroup"
      },
      "Type": "Resource"
    },
    {
      "ResourceChange": {
        "Action": "Add",
        "ResourceType": "AWS::AutoScaling::LaunchConfiguration",
        "Scope": [],
        "Details": [],
        "LogicalResourceId": "LaunchConfig"
      },
      "Type": "Resource"
    },
    {
      "ResourceChange": {
        "ResourceType": "AWS::EC2::Instance",
        "PhysicalResourceId": "i-1abc23d4",
        "Details": [],
        "Action": "Remove",
        "Scope": [],
        "LogicalResourceId": "MyEC2Instance"
      },
      "Type": "Resource"
    }
  ],
  "CreationTime": "2020-11-18T01:44:08.444Z",
  "Capabilities": [],
  "StackName": "MyStack",
  "NotificationARNs": [],
  "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet-addremove/1a2345b6-0000-00a0-a123-00abc0abc000"

```

```
}
```

Nella struttura `Changes`, ci sono tre strutture `ResourceChange`, una per ciascuna risorsa. Per ogni risorsa, il `Action` campo indica se CloudFormation aggiunge o rimuove la risorsa. I campi `Scope` e `Details` sono vuoti perché si applicano solo alle risorse modificate.

Per le nuove risorse, non è CloudFormation possibile determinare il valore di alcuni campi finché non si esegue il set di modifiche. Ad esempio, CloudFormation non fornisce la configurazione fisica IDs del gruppo Auto Scaling e avvia perché non esistono ancora. CloudFormation crea le nuove risorse quando si esegue il set di modifiche.

Visualizzazione delle modifiche a livello di proprietà

L'esempio seguente mostra le modifiche a livello di Tag proprietà alla proprietà di un'istanza Amazon EC2 . Il tag `Value` e `Key` verrà modificato in. `Test`

```
"ChangeSetName": "SampleChangeSet",
  "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet/38d91d27-798d-4736-9bf1-fb7c46207807",
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
SampleEc2Template/68edcdc0-f6b6-11ee-966c-126d572cdd11",
  "StackName": "SampleEc2Template",
  "Description": "A sample EC2 instance template for testing change sets.",
  "Parameters": [
    {
      "ParameterKey": "KeyPairName",
      "ParameterValue": "BatchTest"
    },
    {
      "ParameterKey": "Purpose",
      "ParameterValue": "testing"
    },
    {
      "ParameterKey": "InstanceType",
      "ParameterValue": "t2.micro"
    }
  ],
  "CreationTime": "2024-04-09T21:29:10.759000+00:00",
  "ExecutionStatus": "AVAILABLE",
  "Status": "CREATE_COMPLETE",
  "StatusReason": null,
  "NotificationARNs": [],
```

```

    "RollbackConfiguration": {
:....skipping...
    {
        "Changes": [
            {
                "Type": "Resource",
                "ResourceChange": {
                    "Action": "Modify",
                    "LogicalResourceId": "MyEC2Instance",
                    "PhysicalResourceId": "i-0cc7856a36315e62b",
                    "ResourceType": "AWS::EC2::Instance",
                    "Replacement": "False",
                    "Scope": [
                        "Tags"
                    ],
                    "Details": [
                        {
                            "Target": {
                                "Attribute": "Tags",
                                "RequiresRecreation": "Never",
                                "Path": "/Properties/Tags/0/Value",
                                "BeforeValue": "testing",
                                "AfterValue": "Test",
                                "AttributeChangeType": "Modify"
                            },
                            "Evaluation": "Static",
                            "ChangeSource": "DirectModification"
                        },
                        {
                            "Target": {
                                "Attribute": "Tags",
                                "RequiresRecreation": "Never",
                                "Path": "/Properties/Tags/0/Key",
                                "BeforeValue": "Purpose",
                                "AfterValue": "Test",
                                "AttributeChangeType": "Modify"
                            },
                            "Evaluation": "Static",
                            "ChangeSource": "DirectModification"
                        }
                    ],
                    "BeforeContext": "{\\"Properties\\":{\\"KeyName\\":\\"BatchTest\\",\\"ImageId\\":\\"ami-8fcee4e5\\",\\"InstanceType\\":\\"t2.micro\\",\\"Tags\\":[{\\"Value\\":\\"testing\\",\\"Key\\":\\"Purpose\\"}]}}",

```

```
    "AfterContext": "{\n  \"Properties\": {\n    \"KeyName\": \"BatchTest\",\n    \"ImageId\": \"ami-8fcee4e5\",\n    \"InstanceType\": \"t2.micro\",\n    \"Tags\": [\n      {\n        \"Value\": \"Test\",\n        \"Key\": \"Test\"\n      }\n    ]\n  }\n}"
```

La `Details` struttura mostra i valori per `Key` e `Value` prima dell'esecuzione del set di modifiche e quali saranno dopo l'esecuzione del set di modifiche.

Set di modifiche per stack nidificati

Con i set di modifiche per gli stack nidificati è possibile visualizzare in anteprima le modifiche alle risorse dell'applicazione e dell'infrastruttura nell'intera gerarchia dello stack nidificato e procedere con gli aggiornamenti dopo aver confermato che tutte le modifiche sono come previsto.

Per ulteriori dettagli sui set di modifiche per gli stack nidificati, vedere le sezioni seguenti:

Argomenti

- [Panoramica dei set di modifiche e degli stack nidificati](#)
- [Gestione dei set di modifiche per stack nidificati \(console\)](#)
- [Gestione dei set di modifiche per stack nidificati \(AWS CLI\)](#)

Panoramica dei set di modifiche e degli stack nidificati

I set di modifiche per gli stack nidificati uniscono le seguenti funzionalità per espandere l'ambito di visualizzazione in anteprima delle modifiche all'intera gerarchia dello stack:

- Un set di modifiche è una CloudFormation funzionalità che offre un'anteprima dell'impatto delle modifiche proposte a uno stack sulle risorse esistenti o appena create. Dopo aver creato un set di modifiche, CloudFormation fornisce un elenco di modifiche proposte confrontando lo stack con le modifiche alle risorse inviate. Per ulteriori informazioni sui set di modifiche, vedere [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).
- Uno stack annidato è uno stack creato come parte di un altro stack. Ad esempio, è possibile che si disponga di risorse correlate alla rete e alla sicurezza in uno stack nidificato e risorse dell'applicazione in un altro. Il partizionamento dei modelli applicativi in questo modo aiuta con la manutenibilità e il riutilizzo del codice. Per ulteriori informazioni sugli stack nidificati, consulta [Dividi un modello in pezzi riutilizzabili usando pile annidate](#)

Gestione dei set di modifiche per stack nidificati (console)

- Creare un set di modifiche – Crea un set di modifiche inviando le modifiche da qualsiasi livello della gerarchia dello stack. È possibile inviare un modello di stack modificato o valori di parametro di input modificati e CloudFormation confronta gli stack nidificati con le modifiche inviate per generare un set di modifiche. I set di modifiche per gli stack nidificati sono abilitati per impostazione predefinita nella console CloudFormation. Per ulteriori informazioni, consulta [Creare un set di modifiche per uno CloudFormation stack](#).

▼ Change sets

Change sets for nested stacks

Creates change sets for all nested stacks specified in your template. [Learn more](#) 

☒ Enabled

Creates a change set for all nested stacks specified in the template.

☐ Disabled

Create a change set only on the target stack.

Note

Un set di modifiche root è il set di modifiche associato allo stack da cui viene creata l'intera gerarchia dei set di modifiche. È necessario eseguire o eliminare i set di modifiche per gli stack nidificati dal set di modifiche root. Per ulteriori informazioni, consulta [Esecuzione di operazioni di stack su stack annidati](#).

- Visualizza il set di modifiche – Visualizza le modifiche alle risorse all'interno degli stack nidificati prima di eseguirle. È possibile visualizzare le modifiche proposte nella sezione Modifiche del set di modifiche esplorando lo stack corrente e i relativi set di modifiche nidificati. Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).
- Eseguire il set di modifiche – Eseguire le modifiche descritte nel set di modifiche relativo allo stack corrente e ai relativi discendenti. L'operazione di esecuzione deve essere eseguita dal set di modifiche root. Per ulteriori informazioni, consulta [Esegui un set di modifiche per uno CloudFormation stack](#).
- Elimina il set di modifiche – Rimuove i set di modifiche dallo stack corrente. L'eliminazione di un set di modifiche consente di impedire all'utente o a un altro utente di avviare accidentalmente un set di modifiche che non deve essere applicato. L'operazione di eliminazione deve essere eseguita dal set di modifiche root. Per ulteriori informazioni, consulta [Eliminare un set di modifiche per uno CloudFormation stack](#).

Gestione dei set di modifiche per stack nidificati (AWS CLI)

create-change-set

- [create-change-set](#): per impostazione predefinita, i set di modifiche per gli stack nidificati non sono abilitati per la AWS CLI. Per creare un set di modifiche per l'intera gerarchia degli stack, specificate l'opzione. `--include-nested-stacks` Per ulteriori informazioni, consulta [Creare un set di modifiche per uno CloudFormation stack](#).

L' AWS CLI esempio seguente crea un set di modifiche per lo stack principale specificato.

```
aws cloudformation create-change-set \  
  --stack-name my-root-stack \  
  --change-set-name my-root-stack-change-set \  
  --template-body file://template.yaml \  
  --capabilities CAPABILITY_IAM \  
  --include-nested-stacks
```

Di seguito è riportato un output di esempio.

```
{  
  "Id": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-root-stack-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",  
  "StackId": "arn:aws:cloudformation:us-west-2:123456789012:Stack/my-root-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204"  
}
```

describe-change-set

- [describe-change-set](#)— Restituisce un elenco di modifiche che CloudFormation verranno apportate se si esegue il set di modifiche. Se il set di modifiche specificato contiene set di modifiche secondarie che appartengono a stack nidificati, ChangeSetId restituirà informazioni su tale set di modifiche. Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).

L' AWS CLI esempio seguente descrive il set di modifiche per lo stack principale specificato.

```
aws cloudformation describe-change-set \  
  --change-set-name my-root-stack-change-set \  
  --stack-name my-root-stack
```

```
--stack-name my-root-stack
```

Di seguito è riportato un output di esempio.

```
{
  "Changes": [
    {
      "Type": "Resource",
      "ResourceChange": {
        "Action": "Modify",
        "LogicalResourceId": "ChildStack",
        "PhysicalResourceId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/my-nested-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99205",
        "ResourceType": "AWS::CloudFormation::Stack",
        "Replacement": "False",
        "ChangeSetId": "arn:aws:cloudformation:us-
west-2:123456789012:changeSet/my-nested-stack-change-set/4eca1a01-e285-
xmpl-8026-9a1967bfb4b0",
        "Scope": [
          "Properties"
        ],
        "Details": [
          {
            "Target": {
              "Attribute": "Properties",
              "RequiresRecreation": "Never"
            },
            "Evaluation": "Dynamic",
            "ChangeSource": "Automatic"
          }
        ]
      }
    }
  ],
  "ChangeSetName": "my-root-stack-change-set",
  "ChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-root-
stack-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",
  "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-root-stack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
  "StackName": "my-root-stack",
  "IncludeNestedStacks": true,
  "ParentChangeSetId": null,
  "RootChangeSetId": null,
}
```



```

    "Description": null,
    "Parameters": null,
    "CreationTime": "2020-11-18T05:20:56.651Z",
    "ExecutionStatus": "AVAILABLE",
    "Status": "CREATE_COMPLETE",
    "StatusReason": null,
    "NotificationARNs": [

    ],
    "RollbackConfiguration": {

    },
    "Capabilities": [
        "CAPABILITY_IAM"
    ],
    "Tags": null
}

```

L' AWS CLI esempio seguente descrive il set di modifiche per lo stack annidato specificato.

```

aws cloudformation describe-change-set \
  --change-set-name my-nested-stack-change-set \
  --stack-name my-nested-stack

```

Di seguito è riportato un output di esempio.

```

{
  "Changes": [
    {
      "Type": "Resource",
      "ResourceChange": {
        "Action": "Modify",
        "LogicalResourceId": "function",
        "PhysicalResourceId": "my-function",
        "ResourceType": "AWS::Lambda::Function",
        "Replacement": "False",
        "ChangeSetId": null,
        "Scope": [
          "Properties"
        ],
        "Details": [
          {
            "Target": {

```

```

        "Attribute": "Properties",
        "Name": "Timeout",
        "RequiresRecreation": "Never"
    },
    "Evaluation": "Static",
    "ChangeSource": "DirectModification"
}
    ]
}
    ],
    "ChangeSetName": "my-nested-stack-change-set",
    "ChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-nested-stack-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-nested-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99205",
    "ParentChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-root-stack-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",
    "RootChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-root-stack-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",
    "IncludeNestedStacks": true,
    "StackName": "my-nested-stack",
    "Description": null,
    "Parameters": null,
    "CreationTime": "2020-11-18T05:20:56.651Z",
    "ExecutionStatus": "UNAVAILABLE",
    "Status": "CREATE_COMPLETE",
    "StatusReason": "Executable from root change set",
    "NotificationARNs": [

    ],
    "RollbackConfiguration": {

    },
    "Capabilities": [
        "CAPABILITY_IAM"
    ],
    "Tags": null
}

```

execute-change-set

- [execute-change-set](#) – Crea o aggiorna uno stack utilizzando le informazioni fornite in input al momento della creazione del set di modifiche specificato. Per creare un set di modifiche per l'intera gerarchia dello stack, è necessario specificare l'--include-nested-stacksoptione durante l'operazione. create-change-set Per ulteriori informazioni, consulta [Esegui un set di modifiche per uno CloudFormation stack](#).

Note

execute-change-set deve essere eseguito dal set di modifiche root e applicherà il set di modifiche all'intera gerarchia di stack.

L' AWS CLI esempio seguente esegue un set di modifiche per lo stack principale specificato.

```
aws cloudformation execute-change-set \  
  --stack-name my-root-stack \  
  --change-set-name my-root-stack-change-set
```

delete-change-set

- [delete-change-set](#) – Elimina il set di modifiche specificato. L'eliminazione dei set di modifiche garantisce che nessuno esegua il set di modifiche errato. L'eliminazione dei set di modifiche è asincrona per i set di modifiche creati con l'opzione. --include-nested-stacks Per ulteriori informazioni, consulta [Eliminare un set di modifiche per uno CloudFormation stack](#).

Note

delete-change-set deve essere eseguito dal set di modifiche root ed eliminerà l'intera gerarchia dei set di modifiche. Anche gli stack nidificati nello stato REVIEW_IN_PROGRESS verranno eliminati se sono stati creati durante l'operazione create-change-set.

L' AWS CLI esempio seguente elimina il set di modifiche per lo stack principale specificato.

```
aws cloudformation delete-change-set \  
  --stack-name my-root-stack \  
  --change-set-name my-root-stack-change-set
```

Aggiorna direttamente gli stack

Quando desideri distribuire rapidamente gli aggiornamenti per il tuo stack, esegui un aggiornamento diretto. Con un aggiornamento diretto, invii un modello o dei parametri di input che specificano gli aggiornamenti alle risorse nello stack e li distribuisce CloudFormation immediatamente. Se desideri utilizzare un modello per effettuare gli aggiornamenti, puoi modificare il modello corrente e archiviarlo localmente o in un bucket Amazon S3.

Per le proprietà di risorsa che non supportano gli aggiornamenti, devi mantenere i valori correnti. Per visualizzare in anteprima le modifiche che CloudFormation verranno apportate al tuo stack prima di aggiornarlo, usa i set di modifiche. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

Durante l'aggiornamento di uno stack, CloudFormation potrebbe interrompere le risorse o sostituire le risorse aggiornate, a seconda delle proprietà aggiornate. Per ulteriori informazioni sui comportamenti di aggiornamento delle risorse, consulta [Comprendi i comportamenti di aggiornamento delle risorse dello stack](#).

Per aggiornare uno stack (console)

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation).
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Nella pagina Stacks, seleziona lo stack in esecuzione che desideri aggiornare.
4. Nel riquadro dettagli dello stack, scegliere Update (Aggiorna).
5. Se non hai modificato il modello dello stack, seleziona Usa modello esistente, quindi scegli Avanti.

Se hai modificato il modello, seleziona Sostituisci modello esistente e specifica la posizione del modello aggiornato nella sezione Specificare il modello:

- Per un modello memorizzato localmente nel computer, selezionare Upload a template file (Carica un file modello). Selezionare Choose File (Scegli file) per accedere al file e selezionarlo, quindi selezionare Next (Avanti).

 Note

Se carichi un file modello locale, lo CloudFormation carica in un bucket Amazon Simple Storage Service (Amazon S3) nel tuo Account AWS. Se non disponi già di un bucket S3 creato da CloudFormation, verrà creato un bucket unico per ogni regione in cui carichi un file modello. Se hai già un bucket S3 creato da CloudFormation nel tuo Account AWS, CloudFormation aggiunge il modello a quel bucket.

Considerazioni da tenere a mente sui bucket S3 creati da CloudFormation

- I bucket sono accessibili a chiunque disponga delle autorizzazioni Amazon S3. Account AWS
- CloudFormation crea i bucket con la crittografia lato server abilitata per impostazione predefinita, crittografando così tutti gli oggetti memorizzati nel bucket.

Puoi gestire direttamente le opzioni di crittografia per i bucket che hai CloudFormation creato; ad esempio, utilizzando la console Amazon S3 <https://console.aws.amazon.com/s3/> all'indirizzo o il AWS CLI. Per ulteriori informazioni, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

- Puoi utilizzare il tuo bucket e gestirne le autorizzazioni caricando manualmente i modelli su Amazon S3. Quando crei o aggiorni uno stack, specifica l'URL Amazon S3 di un file del modello.

- Per un modello archiviato in un bucket Amazon S3, selezionare URL Amazon S3. Inserire o incollare l'URL per il modello, quindi selezionare Next (Avanti).

Se hai un modello in un bucket abilitato al rilascio di versioni, puoi specificare una versione specifica del modello aggiungendolo all'URL. ?versionId=**version-id** Per ulteriori informazioni, consulta [Lavorare con oggetti in un bucket abilitato al rilascio di versioni nella Guida](#) per l'utente di Amazon Simple Storage Service.

Se vengono rilevati problemi di sintassi, la console fornisce messaggi di errore che aiutano a correggere il modello.

6. Se il modello contiene parametri, nella pagina Specify stack details (Specifica dettagli stack) immettere o modificare i valori di parametro, quindi selezionare Next (Avanti).

CloudFormation popola ogni parametro con il valore attualmente impostato nello stack, ad eccezione dei parametri dichiarati con l'**NoEcho** attributo; tuttavia, puoi comunque utilizzare i valori correnti selezionando Usa valore esistente.

Per ulteriori informazioni sull'utilizzo per NoEcho mascherare informazioni riservate, oltre all'utilizzo di parametri dinamici per la gestione dei segreti, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

7. Nella pagina Configure stack options (Configura opzioni stack), puoi aggiornare i tag e le autorizzazioni applicati allo stack, e modificare le opzioni avanzate quali la policy dello stack, la configurazione di rollback o l'aggiornamento nell'argomento di notifica Amazon SNS. Per ulteriori informazioni su queste opzioni, consulta [Configurare le opzioni dello stack](#).
8. Se il modello contiene risorse IAM, per Capacità, scegli Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
9. Seleziona Successivo per continuare.
10. Esaminare le informazioni stack e le modifiche inviate.

Verificare di aver inviato le informazioni corrette, come i valori dei parametri o l'URL del modello corretti.

Nella sezione Change set preview, verifica che CloudFormation apporteranno tutte le modifiche che ti aspetti. Ad esempio, puoi verificare che CloudFormation aggiunga, rimuova e modifichi le risorse che intendevi aggiungere, rimuovere o modificare. CloudFormation genera questa anteprima creando un set di modifiche per lo stack. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

11. Una volta completate le modifiche, seleziona Update stack (Aggiorna stack).

Note

A questo punto, è possibile visualizzare il set di modifiche per rivedere gli aggiornamenti proposti più accuratamente. A tale scopo, scegliete Visualizza set di modifiche anziché Aggiorna stack. CloudFormation visualizza il set di modifiche generato in base agli aggiornamenti. Quando si è pronti per eseguire l'aggiornamento dello stack, selezionare Execute (Esegui).

CloudFormation visualizza la pagina dei dettagli dello stack per lo stack, con il riquadro Eventi selezionato. Lo stato del tuo stack ora è pari a. UPDATE_IN_PROGRESS Dopo aver CloudFormation completato con successo l'aggiornamento dello stack, imposta lo stato dello stack su. UPDATE_COMPLETE

Se l'aggiornamento dello stack fallisce CloudFormation, ripristina automaticamente le modifiche e imposta lo stato dello stack su. UPDATE_ROLLBACK_COMPLETE

Note

Puoi annullare un aggiornamento mentre è nello UPDATE_IN_PROGRESS stato. Per ulteriori informazioni, consulta [Annullare un aggiornamento dello stack](#).

Per aggiornare uno stack utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi:

- [update-stack](#) (AWS CLI)
- [Update-CFNStack](#) (AWS Tools for Windows PowerShell)

Per esempi di utilizzo della riga di comando per aggiornare uno stack, consulta. [Esempi di comandi di funzionamento CloudFormation dello stack per e AWS CLI PowerShell](#)

Annullare un aggiornamento dello stack

Dopo che l'aggiornamento dello stack è iniziato, puoi annullare l'aggiornamento dello stack, se lo stack è ancora nello stato UPDATE_IN_PROGRESS. Dopo che un aggiornamento è terminato, non è possibile annullarlo. Puoi tuttavia aggiornare uno stack di nuovo con le impostazioni precedenti.

Se annulli l'aggiornamento dello stack, lo stack viene riportato alla configurazione dello stack che era in uso prima dell'avvio dell'aggiornamento dello stack.

Argomenti

- [Per annullare un aggiornamento dello stack \(console\)](#)
- [Per annullare un aggiornamento dello stack \(\)AWS CLI](#)

Per annullare un aggiornamento dello stack (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS dove si trova lo stack.
3. Nella pagina Stacks, scegli lo stack attualmente in fase di aggiornamento. Il suo stato deve essere. UPDATE_IN_PROGRESS
4. Scegliere Stack actions (Operazioni stack) e quindi Cancel update stack (Annulla aggiornamento stack).
5. Per continuare ad annullare l'aggiornamento, selezionare Cancel update (Annulla aggiornamento). In caso contrario, selezionare Cancel (Annulla) per riprendere l'aggiornamento.

Lo stack procede allo stato UPDATE_ROLLBACK_IN_PROGRESS. Al termine dell'annullamento dell'aggiornamento, lo stack viene impostato UPDATE_ROLLBACK_COMPLETE su.

Per annullare un aggiornamento dello stack (AWS CLI)

Usa il comando [cancel-update-stack](#) per annullare un aggiornamento. Per ulteriori informazioni, consulta [Annulla un aggiornamento dello stack](#).

Eliminare uno stack dalla console CloudFormation

Se non hai più bisogno delle risorse in uno stack, puoi eliminare l'intero stack.

Quando si elimina uno stack, CloudFormation elimina tutte le risorse in esso contenute, a meno che non sia stata utilizzata una politica di eliminazione per conservare risorse specifiche. Per ulteriori informazioni, consulta [Attributo DeletionPolicy](#).

Per eliminare uno stack (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS dove si trova lo stack.
3. Nella pagina Stacks, scegli lo stack che desideri eliminare. Lo stack deve essere attualmente in esecuzione.

4. Scegliere Delete (Elimina).
5. Quando viene richiesta la conferma, selezionare Delete (Elimina).

Note

Una volta iniziata, l'operazione di eliminazione dello stack non può essere interrotta. Lo stack procede allo stato `DELETE_IN_PROGRESS`.

Dopo l'eliminazione dello stack, lo stack sarà nello stato `DELETE_COMPLETE`. Per impostazione predefinita, gli stack nello `DELETE_COMPLETE` stato non vengono visualizzati nella CloudFormation console. Per visualizzare gli stack eliminati, è necessario modificare il filtro di visualizzazione degli stack come descritto in [Visualizza gli stack eliminati dalla console CloudFormation](#).

Per forzare l'eliminazione di uno stack (console)

L'eliminazione di uno stack potrebbe non riuscire perché una risorsa nello stack non riesce a eliminarla. Ad esempio, l'eliminazione di una risorsa da cui dipende anche un altro stack non CloudFormation riuscirà. Tutte le risorse che non sono state eliminate rimarranno finché non sarà possibile eliminare lo stack. Se l'eliminazione fallisce e restituisce uno `DELETE_FAILED` stato, puoi scegliere di riprovare utilizzando uno dei due metodi.

1. Nella pagina Pila della CloudFormation console, scegli lo stack di cui vuoi forzare l'eliminazione.
2. Nel riquadro dei dettagli dello stack, scegli Riprova a eliminare.
3. Scegliete tra le seguenti opzioni:
 - Elimina questa pila ma conserva le risorse: questa opzione consente di selezionare le risorse specifiche che originariamente non sono state eliminate, ma che desideri conservare durante l'eliminazione forzata dello stack.
 - Elimina forzatamente l'intero stack: questa opzione conserva tutte le risorse che non sono state eliminate.
4. Scegli Elimina per iniziare il processo di eliminazione forzata con le tue selezioni.

Per esaminare le risorse conservate (console)

Dopo aver eliminato lo stack, è possibile visualizzare le risorse conservate nella console.

1. Nell'elenco degli stack, scegli lo stato del filtro e seleziona Eliminato.
2. Scegli lo stack eliminato.
3. Scegliere la scheda Resources (Risorse).
4. Tutte le risorse conservate mostrano lo **DELETE_SKIPPED** stato.
5. Scegli la risorsa conservata che desideri esaminare.

Per eliminare uno stack utilizzando la riga di comando

È possibile utilizzare uno dei seguenti comandi:

- [delete-stack](#) (AWS CLI)
- [Remove-CFNStack](#) (AWS Tools for Windows PowerShell)

Per esempi di utilizzo della riga di comando per eliminare uno stack, consulta. [Esempi di comandi di funzionamento CloudFormation dello stack per e AWS CLI PowerShell](#)

Risorse correlate

Per informazioni sulla risoluzione degli errori di eliminazione dello stack, consultate l'argomento [Impossibile eliminare lo stack](#) sulla risoluzione dei problemi.

Per informazioni sulla protezione degli stack dall'eliminazione accidentale degli stack, consulta. [Proteggi CloudFormation gli stack dall'eliminazione](#)

Visualizza gli stack eliminati dalla console CloudFormation

Per impostazione predefinita, la CloudFormation console non mostra pile con uno stato di DELETE_COMPLETE. Per visualizzare le informazioni sugli stack eliminati, è necessario modificare l'impostazione di visualizzazione degli stack.

Per visualizzare gli stack eliminati

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS dove si trova lo stack eliminato.

3. Nella pagina Pile, scegli Eliminato dal menu a discesa Stato del filtro.

CloudFormation elenca tutti i tuoi stack con uno stato di `DELETE_COMPLETE`

Consulta anche

- [Eliminare uno stack dalla console CloudFormation](#)
- [Visualizza le informazioni sullo stack dalla console CloudFormation](#)

Monitora l'avanzamento dello stack

Questa sezione descrive come monitorare una distribuzione dello stack attualmente in corso.

CloudFormation fornisce un elenco cronologico dettagliato degli eventi di distribuzione, che mostra lo stato di avanzamento e gli eventuali problemi riscontrati durante la distribuzione.

Argomenti

- [Visualizza gli CloudFormation eventi dello stack](#)
- [Visualizza la cronologia dell'implementazione di uno CloudFormation stack](#)
- [Comprendi gli CloudFormation eventi di creazione degli stack](#)
- [Monitora lo stato di avanzamento di un aggiornamento dello stack](#)
- [Rollback di un aggiornamento](#)
- [Determinare la causa di un errore dello stack](#)
- [Scegli come gestire gli errori durante il provisioning delle risorse](#)

Visualizza gli CloudFormation eventi dello stack

Gli eventi dello stack consentono di capire quando le risorse vengono create, aggiornate o eliminate e se l'operazione dello stack sta procedendo come previsto. È possibile visualizzare gli eventi dello stack per monitorare l'avanzamento e lo stato dello stack. AWS CloudFormation

Argomenti

- [Visualizza gli eventi dello stack \(console\)](#)
- [Visualizza gli eventi dello stack \(AWS CLI\)](#)
- [Codici di stato dello stack](#)

Visualizza gli eventi dello stack (console)

Per visualizzare gli eventi dello stack

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli lo stack in cui Regione AWS hai creato lo stack.
3. Nella pagina Stacks della CloudFormation console, seleziona il nome dello stack. CloudFormation visualizza i dettagli dello stack per lo stack selezionato.
4. Scegli la scheda Eventi per visualizzare lo stack che gli eventi CloudFormation hanno generato per il tuo stack.

CloudFormation aggiorna automaticamente gli eventi dello stack ogni minuto. Inoltre, CloudFormation visualizza il badge Nuovi eventi disponibili quando si verificano nuovi eventi dello stack. Scegliete l'icona di aggiornamento per caricare questi eventi nell'elenco. La visualizzazione degli eventi di creazione dello stack consente di comprendere la sequenza di eventi che conducono alla creazione (o alla mancata creazione, se si sta eseguendo il debug dello stack).

Durante la creazione, lo stack viene elencato nella pagina Pile con uno stato di.

CREATE_IN_PROGRESS Dopo che lo stack è stato creato con successo, il suo stato diventa.
CREATE_COMPLETE

Per ulteriori informazioni, consulta [Comprendi gli CloudFormation eventi di creazione degli stack](#) e [Monitora lo stato di avanzamento di un aggiornamento dello stack](#).

Visualizza gli eventi dello stack (AWS CLI)

In alternativa, è possibile utilizzare il [describe-stack-events](#) comando durante la creazione dello stack per visualizzare gli eventi man mano che vengono segnalati.

Il describe-stack-events comando seguente descrive gli eventi dello *myteststack* stack.

```
aws cloudformation describe-stack-events --stack-name myteststack
```

Di seguito è riportata una risposta di esempio.

```
{
  "StackEvents": [
    {
```

```

    "StackId": "arn:aws:cloudformation:aws-region:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
    "EventId": "af67ef60-0b8f-11e3-8b8a-500150b352e0",
    "ResourceStatus": "CREATE_COMPLETE",
    "ResourceType": "AWS::CloudFormation::Stack",
    "Timestamp": "2013-08-23T01:02:30.070Z",
    "StackName": "myteststack",
    "PhysicalResourceId": "arn:aws:cloudformation:aws-
region:123456789012:stack/myteststack/a69442d0-0b8f-11e3-8b8a-500150b352e0",
    "LogicalResourceId": "myteststack"
  },
  {
    "StackId": "arn:aws:cloudformation:aws-region:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
    "EventId": "S3Bucket-CREATE_COMPLETE-1377219748025",
    "ResourceStatus": "CREATE_COMPLETE",
    "ResourceType": "AWS::S3::Bucket",
    "Timestamp": "2013-08-23T01:02:28.025Z",
    "StackName": "myteststack",
    "ResourceProperties": "{\"AccessControl\":\"PublicRead\"}",
    "PhysicalResourceId": "myteststack-s3bucket-jssofilzie2w",
    "LogicalResourceId": "S3Bucket"
  },
  {
    "StackId": "arn:aws:cloudformation:aws-region:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
    "EventId": "S3Bucket-CREATE_IN_PROGRESS-1377219746688",
    "ResourceStatus": "CREATE_IN_PROGRESS",
    "ResourceType": "AWS::S3::Bucket",
    "Timestamp": "2013-08-23T01:02:26.688Z",
    "ResourceStatusReason": "Resource creation Initiated",
    "StackName": "myteststack",
    "ResourceProperties": "{\"AccessControl\":\"PublicRead\"}",
    "PhysicalResourceId": "myteststack-s3bucket-jssofilzie2w",
    "LogicalResourceId": "S3Bucket"
  },
  {
    "StackId": "arn:aws:cloudformation:aws-region:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
    "EventId": "S3Bucket-CREATE_IN_PROGRESS-1377219743862",
    "ResourceStatus": "CREATE_IN_PROGRESS",
    "ResourceType": "AWS::S3::Bucket",
    "Timestamp": "2013-08-23T01:02:23.862Z",
    "StackName": "myteststack",

```

```
        "ResourceProperties": "{\"AccessControl\": \"PublicRead\"}\",
        "PhysicalResourceId": null,
        "LogicalResourceId": "S3Bucket"
    },
    {
        "StackId": "arn:aws:cloudformation:aws-region:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
        "EventId": "a69469e0-0b8f-11e3-8b8a-500150b352e0",
        "ResourceStatus": "CREATE_IN_PROGRESS",
        "ResourceType": "AWS::CloudFormation::Stack",
        "Timestamp": "2013-08-23T01:02:15.422Z",
        "ResourceStatusReason": "User Initiated",
        "StackName": "myteststack",
        "PhysicalResourceId": "arn:aws:cloudformation:aws-
region:123456789012:stack/myteststack/a69442d0-0b8f-11e3-8b8a-500150b352e0",
        "LogicalResourceId": "myteststack"
    }
]
}
```

Gli eventi più recenti vengono segnalati per primi. La tabella riportata di seguito descrive i campi restituiti dal comando describe-stack-events:

Campo	Descrizione
EventId	Identificatore di eventi.
StackName	Il nome dello stack a cui corrisponde l'evento.
StackId	L'identificatore dello stack a cui corrisponde l'evento.
LogicalResourceId	L'identificatore logico della risorsa.
PhysicalResourceId	L'identificatore fisico della risorsa.
ResourceProperties	Le proprietà della risorsa.
ResourceType	Il tipo di risorsa.
Timestamp	Ora in cui si è verificato l'evento.

Campo	Descrizione
ResourceStatus	Lo stato della risorsa, che può essere uno dei seguenti codici di stato: CREATE_COMPLETE CREATE_FAILED CREATE_IN_PROGRESS DELETE_COMPLETE DELETE_FAILED DELETE_IN_PROGRESS DELETE_SKIPPED IMPORT_COMPLETE IMPORT_IN_PROGRESS IMPORT_ROLLBACK_COMPLETE IMPORT_ROLLBACK_FAILED IMPORT_ROLLBACK_IN_PROGRESS REVIEW_IN_PROGRESS ROLLBACK_COMPLETE ROLLBACK_FAILED ROLLBACK_IN_PROGRESS UPDATE_COMPLETE UPDATE_COMPLETE_CLEANUP_IN_PROGRESS UPDATE_FAILED UPDATE_IN_PROGRESS UPDATE_ROLLBACK_COMPLETE UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS UPDATE_ROLLBACK_FAILED UPDATE_ROLLBACK_IN_PROGRESS Lo stato DELETE_SKIPPED si applica alle risorse il cui attributo di policy di eliminazione è mantenere.
DetailedStatus	Lo stato dettagliato dello stack. Se CONFIGURATION_COMPLETE presente, la fase di configurazione delle risorse dello stack è completata e la stabilizzazione delle risorse è in corso.
ResourceStatusReason	Ulteriori informazioni sullo stato.

Codici di stato dello stack

Nella tabella seguente vengono descritti i codici di stato dello stack:

Stato dello stack e stato dettagliato opzionale	Descrizione
CREATE_COMPLETE	Creazione di uno o più stack completata.
CREATE_IN_PROGRESS	Creazione di uno o più stack in corso.

Stato dello stack e stato dettagliato opzionale	Descrizione
CREATE_FAILED	Creazione di uno o più stack non riuscita. Visualizzare gli eventi dello stack per vedere gli eventuali messaggi di errore associati. Le possibili ragioni di una creazione non riuscita includono le autorizzazioni insufficienti per lavorare con tutte le risorse dello stack, i valori dei parametri rifiutati da un AWS servizio o un timeout durante la creazione delle risorse.
DELETE_COMPLETE	Eliminazione di uno o più stack completata. Gli stack eliminati vengono conservati e sono visualizzabili per 90 giorni.
DELETE_FAILED	Eliminazione di uno o più stack non riuscita. Poiché l'eliminazione non è riuscita, è possibile che alcune risorse siano ancora in esecuzione; tuttavia, non è possibile utilizzare o aggiornare lo stack. Eliminare nuovamente lo stack o visualizzare gli eventi dello stack per visualizzare gli eventuali messaggi di errore associati.
DELETE_IN_PROGRESS	Rimozione di uno o più stack in corso.
REVIEW_IN_PROGRESS	Creazione di uno o più stack in corso con un StackId previsto ma senza modelli o risorse.  Important Un stack con questo codice di stato conta fino al raggiungimento del massimo numero possibile di stack.

Stato dello stack e stato dettagliato opzionale	Descrizione
ROLLBACK_COMPLETE	Rimozione di uno o più stack completata dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita. Lo stack torna allo stato di funzionamento precedente. Le eventuali risorse che sono state create durante l'operazione di creazione dello stack vengono eliminate. Questo stato esiste solo dopo una creazione stack non riuscita. Indica che tutte le operazioni dallo stack creato parzialmente sono state opportunamente rimosse. In questo stato, è possibile eseguire solo un'operazione di eliminazione.
ROLLBACK_FAILED	Rimozione di uno o più stack non riuscita dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita. Eliminare lo stack o visualizzare gli eventi dello stack per visualizzare gli eventuali messaggi di errore associati.
ROLLBACK_IN_PROGRESS	Rimozione di uno o più stack in corso dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita.
UPDATE_COMPLETE	Aggiornamento di uno o più stack completato.
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS	Rimozione in corso di risorse obsolete per uno o più stack dopo un aggiornamento dello stack completato. Per gli aggiornamenti dello stack che richiedono la sostituzione di risorse, CloudFormation crea prima le nuove risorse e poi elimina le vecchie risorse per ridurre eventuali interruzioni dello stack. In questo stato, lo stack è stato aggiornato ed è utilizzabile, ma le vecchie risorse CloudFormation vengono comunque eliminate.
UPDATE_FAILED	Aggiornamento non completato di uno o più stack. Visualizzare gli eventi dello stack per vedere gli eventuali messaggi di errore associati.

Stato dello stack e stato dettagliato opzionale	Descrizione
UPDATE_IN_PROGRESS	Aggiornamento di uno o più stack in corso.
UPDATE_ROLLBACK_COMPLETE	Restituzione di uno o più stack completata in uno stato attivo precedente dopo un aggiornamento stack non riuscito.
UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS	Rimozione in corso di nuove risorse per uno o più stack dopo un aggiornamento dello stack non riuscito. In questo stato, lo stack è stato ripristinato allo stato di funzionamento precedente ed è utilizzabile, ma CloudFormation sta comunque eliminando tutte le nuove risorse create durante l'aggiornamento dello stack.
UPDATE_ROLLBACK_FAILED	Restituzione di uno o più stack non riuscita in uno stato attivo precedente dopo un aggiornamento stack non riuscito. In questo stato, puoi eliminare lo stack o continuare il rollback . Prima che lo stack possa tornare in uno stato attivo, potrebbe essere necessario risolvere gli errori. In alternativa, puoi contattare Supporto per ripristinare lo stack a uno stato utilizzabile.
UPDATE_ROLLBACK_IN_PROGRESS	Restituzione di uno o più stack in corso allo stato attivo precedente dopo un aggiornamento stack non riuscito.
IMPORT_IN_PROGRESS	L'operazione di importazione è attualmente in corso.
IMPORT_COMPLETE	L'operazione di importazione è stata completata correttamente per tutte le risorse nello stack che supportano <code>resource import</code> .
IMPORT_ROLLBACK_IN_PROGRESS	L'importazione verrà ripristinata alla configurazione del modello precedente.
IMPORT_ROLLBACK_FAILED	L'operazione di rollback di importazione non è riuscita per almeno una risorsa nello stack. I risultati saranno disponibili per le risorse importate CloudFormation con successo.

Stato dello stack e stato dettagliato opzionale	Descrizione
IMPORT_ROLLBACK_COMPLETE	Il rollback dell'importazione alla configurazione del modello precedente è riuscita.

Visualizza la cronologia dell'implementazione di uno CloudFormation stack

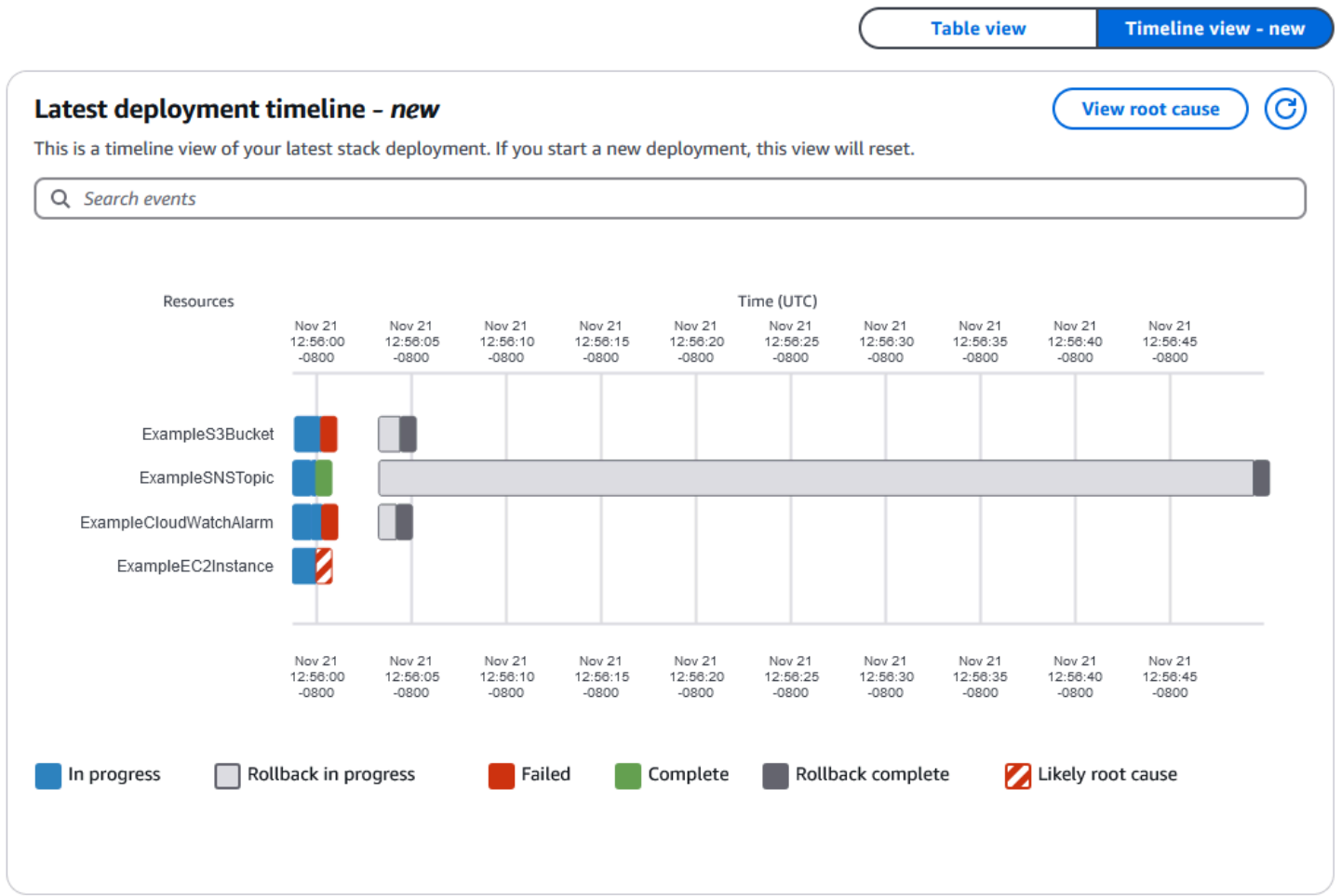
Il grafico della sequenza temporale di implementazione dello stack fornisce una rappresentazione visiva della sequenza temporale di implementazione dello stack. Questa visualizzazione mostra gli stati di distribuzione dello stack e di ciascuna delle relative risorse e le volte in cui ogni stato è cambiato. Gli stati di distribuzione dello stack sono rappresentati da un colore corrispondente.

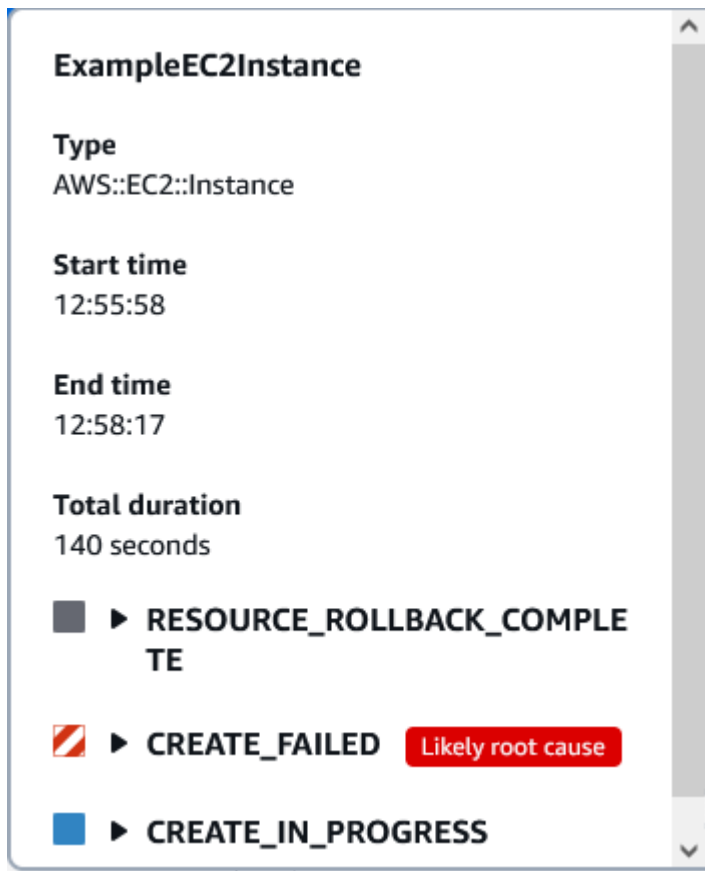
Argomenti

- [Comprensione del grafico della sequenza temporale di distribuzione dello stack](#)
- [Visualizzazione del grafico della sequenza temporale di distribuzione dello stack \(console\)](#)

Comprensione del grafico della sequenza temporale di distribuzione dello stack

L'immagine seguente mostra il grafico della sequenza temporale di una distribuzione dello stack che non è riuscita a causa del mancato avvio di una risorsa di EC2 istanza Amazon.





La scelta di una risorsa mostra il tipo, l'ora di inizio della distribuzione, l'ora di fine della distribuzione e la durata totale della distribuzione. Troverai anche l'ora di inizio, l'ora di fine e la durata di ogni stato di implementazione nei menu a discesa di seguito. Se la risorsa non è stata distribuita, verrà fornito un motivo dell'errore.

Per ulteriori informazioni sugli stati dello stack, consulta. [Codici di stato dello stack](#)

Visualizzazione del grafico della sequenza temporale di distribuzione dello stack (console)

Per visualizzare un grafico della sequenza temporale di distribuzione dello stack:

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli lo stack in cui Regione AWS hai creato lo stack.
3. Nella pagina Stacks della CloudFormation console, scegli il nome dello stack. CloudFormation visualizza i dettagli dello stack per lo stack selezionato.

4. Scegli la scheda Eventi per visualizzare lo stack che gli eventi CloudFormation hanno generato per il tuo stack.
5. Scegli il pulsante Grafico della sequenza temporale per visualizzare il grafico della sequenza temporale del tuo stack.

Comprendi gli CloudFormation eventi di creazione degli stack

Durante la distribuzione dello stack, si verificano diversi eventi per creare, configurare e convalidare le risorse definite nel modello di stack. La comprensione di questi eventi può aiutarvi a ottimizzare il processo di creazione dello stack e a semplificare le implementazioni.

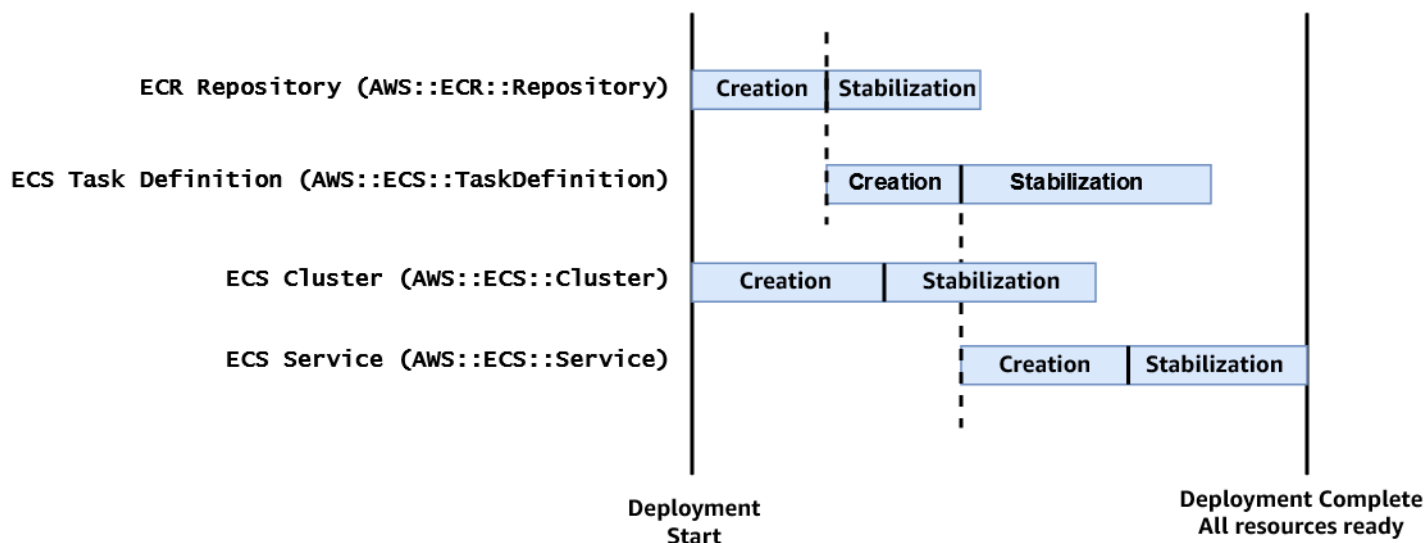
- **Eventi di creazione di risorse:** quando ogni risorsa avvia il processo di creazione, viene impostato uno stato dell'`CREATE_IN_PROGRESS`evento. Questo evento indica che è in corso il provisioning della risorsa.
- **Eventuale controllo di coerenza:** una parte significativa del tempo di creazione dello stack viene impiegata per eseguire un eventuale controllo di coerenza rispetto alle risorse create dallo stack. Durante questa fase, il servizio esegue controlli interni di coerenza, assicurando che la risorsa sia pienamente operativa e soddisfi i criteri di stabilizzazione del servizio definiti da ciascuno. Servizio AWS
- **Evento di completamento della configurazione:** quando ogni risorsa ha terminato l'eventuale fase di controllo della coerenza del provisioning, viene impostato uno stato dettagliato dell'`CONFIGURATION_COMPLETE`evento.
- **Evento completo di creazione della risorsa:** dopo che la risorsa è stata creata e configurata come specificato e la configurazione corrisponde a quella specificata nel modello, viene impostato lo stato dell'`CREATE_COMPLETE`evento.

È possibile sfruttare l'`CONFIGURATION_COMPLETE`evento per semplificare il processo di creazione dello stack in scenari in cui non è richiesto un eventuale controllo della coerenza delle risorse, ad esempio la convalida di una configurazione dello stack di riproduzione o il provisioning tra stack. È possibile utilizzare questo evento in diversi modi. Ad esempio, è possibile utilizzarlo come segnale visivo per evitare di attendere il completamento del controllo di coerenza delle risorse o dello stack. In alternativa, è possibile utilizzarlo per creare un meccanismo automatizzato che utilizza l'integrazione continua e la distribuzione continua (CI/CD) per attivare azioni aggiuntive.

⚠ Important

Sebbene lo sfruttamento dell'`CONFIGURATION_COMPLETE` evento acceleri i tempi di creazione degli stack, dovresti essere consapevole dei suoi compromessi. Innanzitutto, è supportato solo per un sottoinsieme di tipi di risorse che supportano il rilevamento della deriva. Per un elenco dei tipi di risorse che supportano il rilevamento della deriva, consulta [Supporto per tipi di risorse](#). Questo approccio potrebbe non essere adatto a tutti gli scenari, specialmente quando le risorse richiedono eventuali controlli di coerenza approfonditi per garantire la piena disponibilità operativa in tutto l'ambiente cloud (ad esempio, negli ambienti di produzione). Consigliamo di valutare attentamente i requisiti di implementazione e la criticità dei controlli di coerenza per ciascuna risorsa. Utilizzate l'`CONFIGURATION_COMPLETE` evento per ottimizzare la velocità di implementazione senza compromettere l'integrità e l'affidabilità dell'infrastruttura.

Poiché non è garantito che l'`CONFIGURATION_COMPLETE` evento sia impostato, tutti gli scenari che lo utilizzano devono essere preparati per gestire un `CREATE_COMPLETE` evento quando non è stato impostato alcun evento. `CONFIGURATION_COMPLETE`



Quando inizia la distribuzione dello stack, sia le risorse che le `AWS::ECS::Cluster` risorse `AWS::ECR::Repository` avviano il processo di creazione (= `ResourceStatus CREATE_IN_PROGRESS`). Quando il tipo di `AWS::ECR::Repository` risorsa ha avviato l'eventuale controllo di coerenza (`DetailedStatus=CONFIGURATION_COMPLETE`), la `AWS::ECS::TaskDefinition` risorsa può avviare il processo di creazione. Allo stesso modo, una

volta che la `AWS::ECS::TaskDefinition` risorsa inizia l'eventuale controllo di coerenza, avvia il `AWS::ECS::Service` processo di creazione.

Eventi **CREATE_IN_PROGRESS** e **CREATE_COMPLETE**

- [Pila]: `CREATE_IN_PROGRESS`
- [Risorsa]: archivio ECR `CREATE_IN_PROGRESS`
- [Risorsa]: ECS Cluster `CREATE_IN_PROGRESS`
- [Risorsa]: archivio ECR, `CREATE_IN_PROGRESS CONFIGURATION_COMPLETE`
- [Risorsa]: definizione dell'attività ECS `CREATE_IN_PROGRESS`
- [Risorsa]: Cluster ECS, `CREATE_IN_PROGRESS CONFIGURATION_COMPLETE`
- [Risorsa]: definizione delle attività ECS, `CREATE_IN_PROGRESS CONFIGURATION_COMPLETE`
- [Risorsa]: Servizio ECS `CREATE_IN_PROGRESS`
- [Risorsa]: archivio ECR `CREATE_COMPLETE`
- [Risorsa]: ECS Cluster `CREATE_COMPLETE`
- [Risorsa]: Servizio ECS, `CREATE_IN_PROGRESS CONFIGURATION_COMPLETE`
- [Pila]:, `CREATE_IN_PROGRESS CONFIGURATION_COMPLETE`
- [Risorsa]: definizione dell'attività ECS `CREATE_COMPLETE`
- [Risorsa]: Servizio ECS `CREATE_COMPLETE`
- [Pila]: `CREATE_COMPLETE`

Monitora lo stato di avanzamento di un aggiornamento dello stack

Puoi monitorare l'avanzamento dell'aggiornamento di uno stack visualizzandone gli eventi. La scheda Eventi dello stack mostra ogni fase principale della creazione e dell'aggiornamento dello stack, ordinata in base all'ora di ogni evento, con gli ultimi eventi in primo piano. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Argomenti

- [Eventi generati durante un aggiornamento dello stack riuscito](#)
- [Eventi generati quando un aggiornamento delle risorse non va a buon fine](#)

Eventi generati durante un aggiornamento dello stack riuscito

L'inizio del processo di aggiornamento dello stack è contrassegnato da un `UPDATE_IN_PROGRESS` evento per lo stack:

```
2011-09-30 09:35 PDT AWS::CloudFormation::Stack MyStack UPDATE_IN_PROGRESS
```

Seguono gli eventi che contrassegnano l'inizio e il completamento dell'aggiornamento di ciascuna risorsa che è stata modificata nel modello di aggiornamento. Ad esempio, l'aggiornamento di una [AWS::RDS::DBInstance](#) risorsa denominata MyDB comporterebbe le seguenti voci:

```
2011-09-30 09:35 PDT AWS::RDS::DBInstance MyDB UPDATE_COMPLETE  
2011-09-30 09:35 PDT AWS::RDS::DBInstance MyDB UPDATE_IN_PROGRESS
```

L'`UPDATE_IN_PROGRESS` evento viene registrato quando CloudFormation segnala che ha iniziato ad aggiornare la risorsa. L'evento `UPDATE_COMPLETE` viene registrato quando la risorsa viene creata senza errori.

Una volta CloudFormation aggiornato con successo lo stack, verrà visualizzato il seguente evento:

```
2011-09-30 09:35 PDT AWS::CloudFormation::Stack MyStack UPDATE_COMPLETE
```

Important

Durante le operazioni di aggiornamento dello stack, se è CloudFormation necessario sostituire una risorsa esistente, prima crea una nuova risorsa e poi elimina la vecchia risorsa. Tuttavia, potrebbero esserci casi in cui non è CloudFormation possibile eliminare la vecchia risorsa (ad esempio, se l'utente non dispone delle autorizzazioni per eliminare una risorsa di un determinato tipo).

CloudFormation fa tre tentativi di eliminare la vecchia risorsa. Se non CloudFormation riesce a eliminare la vecchia risorsa, rimuove la vecchia risorsa dallo stack e continua ad aggiornare lo stack. Quando l'aggiornamento dello stack è completo, CloudFormation genera un evento `UPDATE_COMPLETE` stack, ma include un evento `StatusReason` che indica che una o più risorse non possono essere eliminate. CloudFormation emette anche un `DELETE_FAILED` evento per la risorsa specifica, con un corrispondente che `StatusReason` fornisce maggiori dettagli sul motivo per cui CloudFormation non è riuscita a eliminare la risorsa.

La vecchia risorsa esiste ancora e continuerà a essere addebitata, ma non è più accessibile tramite CloudFormation. Per eliminare la risorsa precedente, accedere alla risorsa precedente direttamente utilizzando la console o l'API per il servizio sottostante. Questo vale anche per le risorse rimosse dal modello di stack, che quindi verranno eliminate dallo stack durante l'aggiornamento dello stack.

Eventi generati quando un aggiornamento delle risorse non va a buon fine

Se l'aggiornamento di una risorsa fallisce, CloudFormation segnala un `UPDATE_FAILED` evento che include il motivo dell'errore. Ad esempio, se il modello di aggiornamento ha specificato una modifica di proprietà non supportata dalla risorsa, ad esempio la riduzione delle dimensioni di `AllocatedStorage` una [AWS::RDS::DBInstance](#) risorsa, si verificheranno eventi come questi:

```
2011-09-30 09:36 PDT AWS::RDS::DBInstance MyDB UPDATE_FAILED Size cannot be less than
current size; requested: 5; current: 10
2011-09-30 09:35 PDT AWS::RDS::DBInstance MyDB UPDATE_IN_PROGRESS
```

Se l'aggiornamento di una risorsa CloudFormation fallisce, ripristina tutte le risorse che ha aggiornato durante l'aggiornamento alle relative configurazioni precedenti all'aggiornamento. Ecco un esempio di eventi visualizzati durante il rollback di un aggiornamento:

```
2011-09-30 09:38 PDT AWS::CloudFormation::Stack MyStack UPDATE_ROLLBACK_COMPLETE
2011-09-30 09:38 PDT AWS::RDS::DBInstance MyDB UPDATE_COMPLETE
2011-09-30 09:37 PDT AWS::RDS::DBInstance MyDB UPDATE_IN_PROGRESS
2011-09-30 09:37 PDT AWS::CloudFormation::Stack MyStack UPDATE_ROLLBACK_IN_PROGRESS The
following resource(s) failed to update: [MyDB]
```

Rollback di un aggiornamento

A volte, quando CloudFormation tenta di ripristinare un aggiornamento dello stack, non riesce a ripristinare tutte le modifiche apportate durante il processo di aggiornamento. Questo si chiama `UPDATE_ROLLBACK_FAILED` stato. Ad esempio, potresti avere uno stack che inizia a tornare a una vecchia istanza di database che è stata eliminata all'esterno di CloudFormation. Poiché CloudFormation non sa che il database è stato eliminato, presume che l'istanza database sia ancora disponibile e tenta di eseguire il rollback, provocando un errore nel rollback di aggiornamento.

Uno stack nello UPDATE_ROLLBACK_FAILED stato non può essere aggiornato, ma può essere ripristinato a uno stato funzionante (UPDATE_ROLLBACK_COMPLETE). Dopo aver ripristinato le impostazioni originali dello stack, puoi provare ad aggiornarlo nuovamente.

Nella maggior parte dei casi, devi correggere l'errore che causa un guasto durante l'aggiornamento del rollback prima di poter continuare a eseguire il rollback dello stack. In altri casi, puoi continuare a eseguire il rollback dell'aggiornamento senza alcuna modifica, ad esempio quando un'operazione stack scade.

Note

Se utilizzi gli stack nidificati, il rollback dello stack padre cercherà di eseguire il rollback anche su tutti gli stack figlio.

Per continuare il rollback di un aggiornamento (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli Regione AWS dove si trova lo stack.
3. Nella pagina Stack, scegli lo stack che desideri aggiornare, scegli Stack actions, quindi scegli Continua il rollback degli aggiornamenti.

Se nessuna delle soluzioni [Risoluzione degli errori](#) funziona, puoi utilizzare l'opzione avanzata per ignorare le risorse che non CloudFormation possono essere ripristinate correttamente. È necessario [cercare e digitare](#) la logica IDs delle risorse che si desidera ignorare. Specificate solo le risorse che sono state inserite nello UPDATE_FAILED stato durante UpdateRollback e non durante l'aggiornamento successivo.

Warning

CloudFormation imposta lo stato delle risorse specificate su UPDATE_COMPLETE e continua a ripristinare lo stack. Dopo aver completato il rollback, lo stato delle risorse saltate saranno incoerenti con lo stato delle risorse nel modello di stack. Prima di eseguire un altro aggiornamento dello stack, devi aggiornare lo stack o le risorse in modo

che siano coerenti. Altrimenti, i successivi aggiornamenti dello stack potrebbero fallire e lo stack diventerà irrecuperabile.

Specifica il numero minimo di risorse necessarie per eseguire il rollback dello stack. Ad esempio, un aggiornamento della risorsa non riuscito potrebbe causare errori nelle risorse dipendenti. In questo caso, potrebbe non essere necessario ignorare le risorse dipendenti.

Per ignorare le risorse che fanno parte di stack nidificati, utilizzare il formato seguente: *NestedStackName.ResourceLogicalID*. Se desideri specificare l'ID logico di una risorsa stack (Type: `AWS::CloudFormation::Stack`) nell'elenco `ResourcesToSkip`, lo stack corrispondente incorporato deve essere in uno dei seguenti stati: `DELETE_IN_PROGRESS`, `DELETE_COMPLETE` o `DELETE_FAILED`.

Per continuare il rollback di un aggiornamento (AWS CLI)

- Utilizzo dell'[continue-update-rollback](#) comando con la `--stack-name` possibilità di specificare l'ID dello stack di cui si desidera continuare a ripristinare.

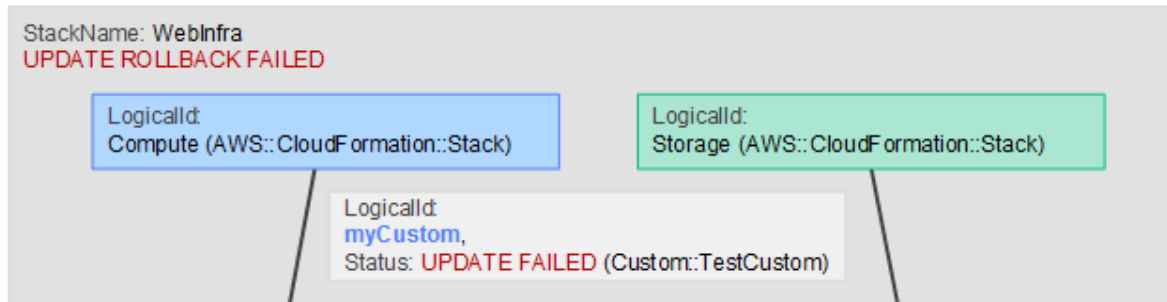
Continua il rollback dopo gli aggiornamenti dello stack annidato non riusciti

Quando sono presenti più stack annidati l'uno nell'altro, potrebbe essere necessario ignorare le risorse su più livelli nidificati per riportare l'intera gerarchia degli stack allo stato operativo.

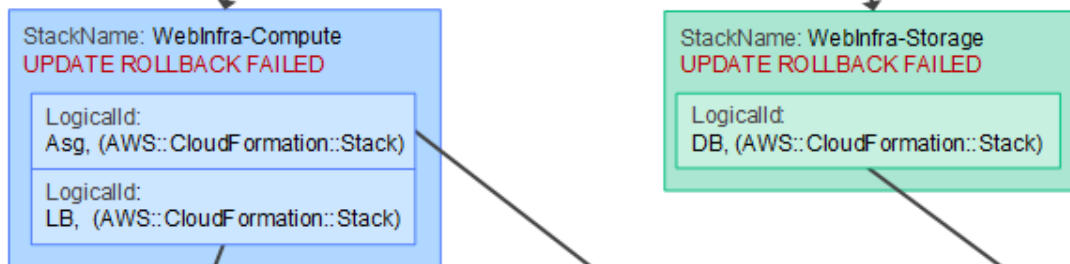
Ad esempio, avete uno stack root chiamato `WebInfra` che contiene due stack più piccoli al suo interno: `and. WebInfra-Compute` e `WebInfra-Storage`. Questi due stack hanno anche i propri stack annidati al loro interno.

Se qualcosa va storto durante un aggiornamento e il processo di aggiornamento fallisce, l'intera gerarchia degli stack potrebbe finire `UPDATE_ROLLBACK_FAILED` nello stato, come illustrato nel diagramma seguente.

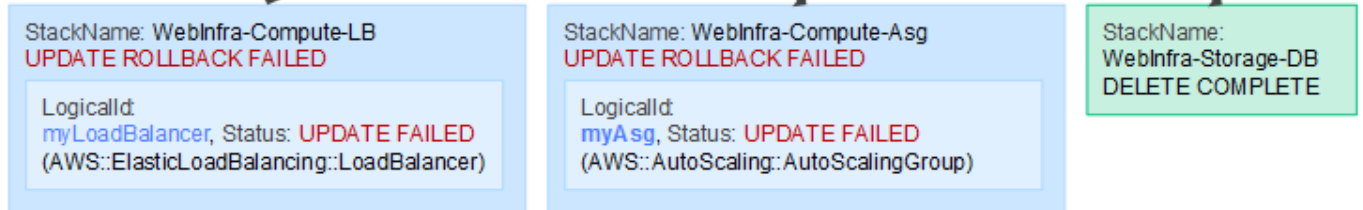
Root



Level 1



Level 2



Note

I nomi di stack in questo esempio vengono troncati per semplicità. I nomi degli stack secondari sono in genere generati CloudFormation e contengono stringhe casuali univoche, pertanto i nomi effettivi potrebbero non essere facili da usare.

Per rendere lo stack principale utilizzabile utilizzando il `continue-update-rollback` comando, è necessario utilizzare l'opzione `--resources-to-skip` per ignorare le risorse per le quali non è stato possibile eseguire il rollback.

L'continue-update-rollbackesempio seguente riprende un'operazione di rollback da un aggiornamento dello stack precedentemente non riuscito. In questo esempio, l'`--resources-to-skip` opzione include i seguenti elementi:

- *myCustom*
- *WebInfra-Compute-Asg.myAsg*
- *WebInfra-Compute-LB.myLoadBalancer*
- *WebInfra-Storage.DB*

Per le risorse dello stack principale, è sufficiente fornire l'ID logico, *myCustom* ad esempio. Tuttavia, per le risorse contenute negli stack nidificati, è necessario fornire sia il nome dello stack nidificato che il relativo ID logico, separati da un punto. Ad esempio *WebInfra-Compute-Asg.myAsg*.

```
aws cloudformation continue-update-rollback --stack-name WebInfra \
  --resources-to-skip myCustom WebInfra-Compute-Asg.myAsg WebInfra-Compute-
  LB.myLoadBalancer WebInfra-Storage.DB
```

Per trovare il nome dello stack di uno stack nidificato

Puoi individuarlo nell'ID dello stack secondario o nell'Amazon Resource Name (ARN).

Il seguente esempio di ARN fa riferimento a uno stack denominato. WebInfra-Storage-Z2VKC706XKXT

```
arn:aws:cloudformation:us-east-1:123456789012:stack/WebInfra-Storage-Z2VKC706XKXT/
ea9e7f90-54f7-11e6-a032-028f3d2330bd
```

Per trovare l'ID logico di uno stack annidato

Puoi trovare l'ID logico dello stack figlio nella definizione del modello del padre. Nel diagramma, lo stack LogicalId WebInfra-Storage-DB secondario si trova DB nello stack principale. WebInfra-Storage

Nella CloudFormation console, puoi anche trovare l'ID logico nella colonna ID logico per la risorsa dello stack nella scheda Risorse o nella scheda Eventi. Per ulteriori informazioni, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Determinare la causa di un errore dello stack

Se la creazione dello stack fallisce, CloudFormation può aiutarti a determinare l'evento che è probabilmente la causa principale dell'errore dello stack. A seconda dello scenario e delle autorizzazioni di cui disponi, AWS CloudTrail gli eventi potrebbero essere in grado di fornire ulteriori dettagli sulla causa principale nel caso in cui il motivo dello Status fornito in Events non sia chiaro.

Per determinare la causa principale di un errore dello stack

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella pagina Stacks, scegli lo stack fallito.
3. Scegli la scheda Eventi.
4. Scegli Rileva la causa principale. CloudFormation analizzerà l'errore e indicherà l'evento che è la probabile causa dell'errore aggiungendo l'etichetta Likely root cause allo stato dell'evento specifico. Vedi il motivo dello stato per ulteriori spiegazioni sullo stato nella CloudFormation console.
5. Scegli lo stato dell'errore con l'etichetta Probabile causa principale per saperne di più sulla causa dell'errore. A seconda dello scenario e delle autorizzazioni di cui disponi, potresti essere in grado di esaminare un CloudTrail evento dettagliato. Questi sono i seguenti potenziali risultati della scelta dello Status
 - CloudTrail gli eventi relativi a questo problema sono disponibili e possono contribuire alla risoluzione. Visualizza CloudTrail gli eventi.
 - Non siamo riusciti a trovare alcun CloudTrail evento relativo a questo problema che possa contribuire alla risoluzione.
 - Le tue attuali autorizzazioni non consentono l'accesso alla visualizzazione CloudTrail degli eventi. [Ulteriori informazioni](#).
 - Durante il processo di verifica degli CloudTrail eventi disponibili, ricontrolla tra qualche minuto.
 - Si è verificato un errore durante il recupero degli CloudTrail eventi. Per l'ispezione manuale, visita la CloudTrail console.
6. Se il motivo fornito in Status reason non è chiaro e la causa principale mostra un collegamento alla CloudTrail console, apri il link per visualizzare l'evento e trovare una causa principale dettagliata.

Per ulteriori informazioni sugli CloudTrail eventi, consulta [Comprendere CloudTrail gli eventi](#) e [il contenuto dei CloudTrail record](#).

Per ulteriori informazioni sulla cronologia CloudTrail degli eventi, consulta [Lavorare con la cronologia CloudTrail degli eventi](#).

 Note

Gli stack annidati non supportano Detect root cause.

Scegli come gestire gli errori durante il provisioning delle risorse

Se l'operazione dello stack fallisce, non è necessario ripristinare le risorse già fornite con successo e ricominciare da capo ogni volta. È invece possibile risolvere i problemi relativi alle risorse con UPDATE_FAILED stato CREATE_FAILED o e quindi riprendere il provisioning dal punto in cui si è verificato il problema.

A tale scopo, è necessario abilitare l'opzione Preserve Provisioned Resources con successo. Questa opzione è disponibile per tutte le distribuzioni in stack e le operazioni relative ai set di modifiche.

- Per la creazione dello stack, se scegliete l'opzione Preserve con successo il provisioning delle risorse, CloudFormation mantiene lo stato delle risorse che sono state create con successo e lascia quelle fallite in uno stato di errore fino all'esecuzione della successiva operazione di aggiornamento.
- Durante le operazioni di aggiornamento e modifica del set, la scelta di Conservare correttamente le risorse distribuite consente di preservare lo stato delle risorse riuscite, ripristinando al contempo l'ultimo stato stabile noto delle risorse con problemi. Le risorse non riuscite presenteranno lo stato UPDATE_FAILED. Le risorse per le quali non è disponibile un ultimo stato stabile noto verranno eliminate in occasione della successiva operazione stack.

Argomenti

- [Panoramica delle opzioni di errore degli stack](#)
- [Condizioni richieste per sospendere il rollback dello stack](#)
- [Mantieni risorse con provisioning effettuato correttamente \(console\)](#)
- [Mantieni risorse con provisioning effettuato correttamente \(AWS CLI\)](#)

Panoramica delle opzioni di errore degli stack

Prima di eseguire un'operazione dalla CloudFormation console, dall'API o AWS CLI, specificate il comportamento in caso di errore delle risorse assegnate. Quindi, procedi con il processo di implementazione delle risorse senza altre modifiche. In caso di guasto operativo, CloudFormation si arresta al primo errore in ogni percorso di provisioning indipendente. CloudFormation identifica le dipendenze tra le risorse per parallelizzare le azioni di approvvigionamento indipendenti. Quindi procede al provisioning delle risorse su ogni percorso di provisioning indipendente fino a quando non si verifica un errore. Un errore in un percorso non influisce sugli altri percorsi di provisioning. CloudFormation continuerà a fornire le risorse fino al completamento o si interromperà in caso di errore diverso.

Risolvi eventuali problemi per continuare il processo di distribuzione. CloudFormation esegue gli aggiornamenti necessari prima di riprovare le azioni di provisioning su risorse che non è stato possibile fornire correttamente in precedenza. Puoi risolvere i problemi inviando un'operazione Retry (Riprova), Update (Aggiorna) o Rollback. Ad esempio, se stai effettuando il provisioning di un' EC2 istanza Amazon e l' EC2 istanza si guasta durante un'operazione di creazione, potresti voler esaminare l'errore, anziché ripristinare immediatamente la risorsa guasta. Puoi rivedere le verifiche dello stato del sistema e dello stato delle istanze, quindi seleziona l'operazione Retry (Riprova) operazione una volta risolti i problemi.

Quando un'operazione di stack ha esito negativo e hai specificato `Preserve successfully provisioned resources` (Mantieni le risorse con provisioning effettuato correttamente) dal menu `Stack failure options` (Opzioni di errore dello stack), puoi selezionare le seguenti opzioni.

- **Retry (Riprova):** riprova l'operazione di provisioning sulle risorse non riuscite e continua il provisioning del modello fino al completamento dell'operazione di stack o al successivo errore. Seleziona questa opzione se il provisioning della risorsa non è riuscito a causa di un problema che non richiede modifiche al modello, ad esempio un'autorizzazione AWS Identity and Access Management (IAM).
- **Update (Aggiorna):** le risorse con provisioning effettuato correttamente vengono aggiornate in base agli aggiornamenti dei modelli. Le risorse che non sono state create o aggiornate verranno riprovate. Seleziona questa opzione se il provisioning della risorsa non è riuscito a causa di errori del modello e questo è stato modificato. Quando aggiorni uno stack con stato `FAILED`, devi selezionare `Preserve successfully provisioned resources` (Mantieni risorse con provisioning effettuato correttamente) per `Stack failure options` (Opzioni di errore dello stack) per continuare ad aggiornare lo stack.
- **Ripristina:** CloudFormation ripristina lo stack all'ultimo stato stabile conosciuto.

Condizioni richieste per sospendere il rollback dello stack

Per CloudFormation evitare che le risorse create correttamente vengano ripristinate ed eliminate automaticamente, devono essere soddisfatte le seguenti condizioni.

1. Quando si crea o si aggiorna lo stack, è necessario scegliere l'opzione Conserva le risorse assegnate correttamente. Ciò indica di CloudFormation non eliminare le risorse che sono state create correttamente, anche se l'operazione complessiva dello stack fallisce.
2. L'operazione stack deve essere fallita, il che significa che lo stato dello stack è o.
`CREATE_FAILED` `UPDATE_FAILED`

Note

I tipi di aggiornamento non modificabili non sono supportati.

Mantieni risorse con provisioning effettuato correttamente (console)

Create stack

Per mantenere le risorse con provisioning effettuato correttamente durante un'operazione di creazione dello stack

1. [Accedi a AWS Management Console e apri la AWS CloudFormation console all'indirizzo `https://console.aws.amazon.com/cloudformazione`.](https://console.aws.amazon.com/cloudformazione)
2. Dalla pagina Stacks, scegli Crea stack in alto a destra, quindi scegli Con nuove risorse (standard).
3. Per Prerequisito - Prepara modello, scegli Scegli un modello esistente.
4. In Specify template (Specifica modello), scegliere di specificare l'URL per il bucket S3 che contiene il modello di stack oppure caricare un file modello di stack. Quindi, seleziona Next (Successivo).
5. Nella pagina Specify stack details (Specifica dettagli stack), immetti il nome dello stack nella casella Stack name (Nome stack).
6. Nella sezione Parameters (Parametri), specifica i parametri definiti nel modello di stack.

È possibile utilizzare o modificare qualsiasi parametro con i valori predefiniti.
7. Una volta definiti i valori dei parametri, seleziona Next (Avanti).

8. Nella pagina Configure stack options (Configura opzioni stack), puoi impostare ulteriori opzioni per lo stack.
9. Per Stack failure options (Opzioni di errore dello stack), seleziona Preserve successfully provisioned resources (Mantieni risorse con provisioning effettuato correttamente).
10. Una volta definite le opzioni di stack, seleziona Next (Avanti).
11. Rivedi lo stack nella pagina Review (Rivedi) e seleziona Create stack (Crea stack).

Results (Risultati): risorse che non sono riuscite a creare la transizione dello stato dello stack in CREATE_FAILED per impedire il rollback dello stack quando l'operazione di stack riscontra un errore. Le risorse con provisioning effettuato correttamente presentano lo stato CREATE_COMPLETE. Puoi monitorare lo stack nella scheda Stack events (Eventi stack).

Update stack

Per mantenere le risorse con provisioning effettuato correttamente durante un'operazione di aggiornamento dello stack

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Seleziona lo stack che desideri aggiornare, quindi seleziona Update (Aggiorna).
3. Nella pagina Update stack (Aggiorna stack), scegli un modello di stack utilizzando una delle opzioni seguenti:
 - Usa il modello esistente
 - Replace current template (Sostituisci modello corrente)
 - Modifica modello in Infrastructure Composer

Accetta le impostazioni desiderate e seleziona Next (Avanti).

4. Nella pagina Specify stack details (Specifica dettagli stack), specifica i parametri definiti nel modello di stack.

È possibile utilizzare o modificare qualsiasi parametro con i valori predefiniti.

5. Una volta definiti i valori dei parametri, seleziona Next (Avanti).
6. Nella pagina Configure stack options (Configura opzioni stack), puoi impostare ulteriori opzioni per lo stack.

7. Per Behavior on provisioning failure (Comportamento con errore di provisioning), seleziona Preserve successfully provisioned resources (Mantieni risorse con provisioning effettuato correttamente).
8. Una volta definite le opzioni di stack, seleziona Next (Avanti).
9. Rivedi lo stack nella pagina Review (Rivedi) e seleziona Update stack (Aggiorna stack).

Risultati: le risorse che non sono riuscite ad aggiornare la transizione dello stato dello stack in UPDATE_FAILED ed eseguire il rollback all'ultimo stato stabile noto. Le risorse senza un ultimo stato stabile noto verranno eliminate CloudFormation alla successiva operazione di stack. Le risorse di cui è stato eseguito il provisioning presentano lo stato CREATE_COMPLETE o UPDATE_COMPLETE. Puoi monitorare lo stack nella scheda Stack events (Eventi stack).

Change set

Note

Puoi avviare un set di modifiche per uno stack con stato CREATE_FAILED o UPDATE_FAILED, ma non per uno stato UPDATE_ROLLBACK_FAILED.

Per mantenere le risorse con provisioning effettuato correttamente durante un'operazione di modifica del set

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Seleziona lo stack che contiene il set di modifiche che desideri avviare, quindi scegli la scheda Change sets (Set di modifiche).
3. Seleziona il set di modifiche, quindi scegli Execute (Esegui).
4. Per Execute change set (Esegui set di modifiche), seleziona l'opzione Preserve successfully provisioned resources (Mantieni risorse con provisioning effettuato correttamente).
5. Seleziona Execute change set (Esegui set di modifiche).

Risultati: le risorse che non sono riuscite ad aggiornare la transizione dello stato dello stack in UPDATE_FAILED ed eseguire il rollback all'ultimo stato stabile noto. Le risorse senza un ultimo stato stabile noto verranno eliminate CloudFormation alla successiva operazione di

stack. Le risorse di cui è stato eseguito il provisioning presentano lo stato `CREATE_COMPLETE` o `UPDATE_COMPLETE`. Puoi monitorare lo stack nella scheda Stack events (Eventi stack).

Mantieni risorse con provisioning effettuato correttamente (AWS CLI)

Create stack

Per mantenere le risorse con provisioning effettuato correttamente durante un'operazione di creazione dello stack

Specifica l'opzione `--disable-rollback` o l'enumerazione on-failure `DO_NOTHING` durante un'operazione [create-stack](#).

1. Fornisci un nome e un modello di stack per il comando `create-stack` con l'opzione `--disable-rollback`.

```
aws cloudformation create-stack --stack-name myteststack \  
  --template-body file://template.yaml \  
  --disable-rollback
```

Questo comando restituisce il seguente output.

```
{  
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"  
}
```

2. Descrivi lo stato dello stack usando il `describe-stacks` comando.

```
aws cloudformation describe-stacks --stack-name myteststack
```

Questo comando restituisce il seguente output.

```
{  
  "Stacks": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",  
      "Description": "AWS CloudFormation Sample Template",  
      "Tags": [],  
    }  
  ]  
}
```

```

        "Outputs": [],
        "StackStatusReason": "The following resource(s) failed to create:
[MyBucket]",
        "CreationTime": "2013-08-23T01:02:15.422Z",
        "Capabilities": [],
        "StackName": "myteststack",
        "StackStatus": "CREATE_FAILED",
        "DisableRollback": true
    }
]
}

```

Update stack

Per preservare le risorse fornite correttamente durante un'operazione di aggiornamento dello stack

1. Fornisci un nome e un modello di stack esistenti per il comando `update-stack` con l'opzione `--disable-rollback`.

```

aws cloudformation update-stack --stack-name myteststack \
  --template-url https://s3.amazonaws.com/amzn-s3-demo-bucket/updated.template
  --disable-rollback

```

Questo comando restituisce il seguente output.

```

{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"
}

```

2. Descrivi lo stato dello stack utilizzando il `describe-stacks` comando or. `describe-stack-events`

```

aws cloudformation describe-stacks --stack-name myteststack

```

Questo comando restituisce il seguente output.

```

{
  "Stacks": [
    {

```

```

        "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
        "Description": "AWS CloudFormation Sample Template",
        "Tags": [],
        "Outputs": [],
        "CreationTime": "2013-08-23T01:02:15.422Z",
        "Capabilities": [],
        "StackName": "myteststack",
        "StackStatus": "UPDATE_COMPLETE",
        "DisableRollback": true
    }
]
}

```

Change set

Note

Puoi avviare un set di modifiche per uno stack con stato `CREATE_FAILED` o `UPDATE_FAILED`, ma non per uno stato `UPDATE_ROLLBACK_FAILED`.

Per mantenere le risorse con provisioning effettuato correttamente durante un'operazione di modifica del set

Specificate l'`--disable-rollback` opzione durante un'[execute-change-set](#) operazione.

1. Fornisci un nome e un modello di stack per il comando `execute-change-set` con l'opzione `--disable-rollback`.

```

aws cloudformation execute-change-set --stack-name myteststack \
  --change-set-name my-change-set --template-body file://template.yaml

```

Questo comando restituisce il seguente output.

```

{
  "Id": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/my-change-set/
bc9555ba-a949-xmpl-bfb8-f41d04ec5784",
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"
}

```

```
}
```

2. Avvia il set di modifiche con l'opzione `--disable-rollback`.

```
aws cloudformation execute-change-set --stack-name myteststack \  
  --change-set-name my-change-set --disable-rollback
```

3. Determina lo stato dello stack utilizzando il `describe-stack-events` comando `describe-stacks` o.

```
aws cloudformation describe-stack-events --stack-name myteststack
```

Questo comando restituisce il seguente output.

```
{  
  "StackEvents": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",  
      "EventId": "49c966a0-7b74-11ea-8071-024244bb0672",  
      "StackName": "myteststack",  
      "LogicalResourceId": " MyBucket",  
      "PhysicalResourceId": "myteststack-MyBucket-abcdefghijkl1",  
      "ResourceType": "AWS::S3::Bucket",  
      "Timestamp": "2020-04-10T21:43:17.015Z",  
      "ResourceStatus": "UPDATE_FAILED"  
      "ResourceStatusReason": "User XYZ is not allowed to perform  
S3::UpdateBucket on MyBucket"  
    }  
  ]  
}
```

4. Correggi gli errori di autorizzazione e riprova l'operazione.

```
aws cloudformation update-stack --stack-name myteststack \  
  --use-previous-template --disable-rollback
```

Questo comando restituisce il seguente output.

```
{  
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"
```



```
}
```

5. Descrivi lo stato dello stack usando il comando `describe-stacks` o `describe-stack-events`.

```
aws cloudformation describe-stacks --stack-name myteststack
```

Questo comando restituisce il seguente output.

```
{
  "Stacks": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
      "Description": "AWS CloudFormation Sample Template",
      "Tags": [],
      "Outputs": [],
      "CreationTime": "2013-08-23T01:02:15.422Z",
      "Capabilities": [],
      "StackName": "myteststack",
      "StackStatus": "UPDATE_COMPLETE",
      "DisableRollback": true
    }
  ]
}
```

Ripristino di una pila

È possibile utilizzare il comando [rollback-stack](#) per riportare uno stack con stato `CREATE_FAILED` o all'ultimo `UPDATE_FAILED` stato stabile.

Il `rollback-stack` comando seguente ripristina lo stack specificato.

```
aws cloudformation rollback-stack --stack-name myteststack
```

Questo comando restituisce il seguente output.

```
{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"
}
```

 Note

L'operazione rollback-stack eliminerà uno stack se non contiene un ultimo stato stabile noto.

Riduci il tuo CloudFormation stack in caso di violazione degli allarmi con i trigger di rollback

Con i trigger di rollback, puoi AWS CloudFormation monitorare lo stato dell'applicazione durante la creazione e l'aggiornamento dello stack e ripristinare tale operazione se l'applicazione supera la soglia degli allarmi che hai specificato. Per ogni trigger di rollback creato, specificate l'allarme da monitorare. CloudWatch CloudFormation CloudFormation monitora gli allarmi specificati durante l'operazione di creazione o aggiornamento dello stack e per il periodo di tempo specificato dopo che tutte le risorse sono state distribuite. Se uno qualsiasi degli allarmi viene attivato durante l'operazione ALARM dello stack o il periodo di monitoraggio, ripristina l'intera operazione dello stack CloudFormation .

Puoi impostare un tempo di monitoraggio compreso tra il valore predefinito 0 e 180 minuti. Durante questo periodo di tempo, CloudFormation monitora tutti i trigger di rollback dopo l'operazione di creazione o aggiornamento dello stack e distribuisce tutte le risorse necessarie. Se uno qualsiasi degli allarmi viene attivato durante l'operazione ALARM dello stack o durante questo periodo di monitoraggio, ripristina l'intera operazione dello CloudFormation stack. Quindi, per le operazioni di aggiornamento, se il periodo di monitoraggio scade senza che venga emesso alcun allarme, CloudFormation procede ALARM allo smaltimento delle vecchie risorse come al solito. Se imposti un periodo di monitoraggio ma non specifichi alcun trigger di rollback, attende CloudFormation comunque il periodo di tempo specificato prima di ripulire le vecchie risorse per le operazioni di aggiornamento. Puoi utilizzare questo periodo di monitoraggio per eseguire eventuali operazioni di convalida dello stack e annullare manualmente la creazione o l'aggiornamento dello stack in base alle esigenze. Se imposti un tempo di monitoraggio di 0 minuti, CloudFormation monitora comunque i trigger di rollback durante le operazioni di creazione e aggiornamento dello stack ed esegue il rollback dell'operazione se un allarme entra nello stato ALARM. Quindi, per le operazioni di aggiornamento senza che sia stata violata la soglia di alcun allarme, inizia a eliminare le risorse obsolete subito dopo il termine dell'operazione.

Per impostazione predefinita, ripristina le operazioni dello stack CloudFormation solo se un allarme passa allo stato e non allo ALARM stato. `INSUFFICIENT_DATA` Per CloudFormation ripristinare l'operazione dello stack se anche un allarme passa allo `INSUFFICIENT_DATA` stato attuale, modifica

L' CloudWatch avviso in modo da trattare i dati mancanti come. `breaching` Per ulteriori informazioni, consulta [Configurazione del modo in cui gli CloudWatch allarmi trattano i dati mancanti](#) nella Amazon CloudWatch User Guide.

CloudFormation non monitora i trigger di rollback quando ripristina uno stack durante un'operazione di aggiornamento.

Puoi aggiungere un massimo di 5 trigger di rollback. Per aggiungere un trigger di rollback, specifica l'Amazon Resource Name (ARN) dell' CloudWatch allarme. Attualmente, si possono utilizzare i tipi `AWS::CloudWatch::Alarm` e `AWS::CloudWatch::CompositeAlarm` come trigger di rollback. Per ulteriori informazioni sugli CloudWatch allarmi, consulta [Using CloudWatch alarms](#) in Amazon CloudWatch User Guide.

Se manca un determinato CloudWatch allarme, l'intera operazione dello stack fallisce e viene ripristinata.

Tieni presente che l'accesso a CloudWatch richiede credenziali. Tali credenziali devono disporre delle autorizzazioni per accedere alle AWS risorse, ad esempio per recuperare i dati CloudWatch metrici relativi alle risorse. Per ulteriori informazioni, consulta la sezione [Autenticazione e controllo degli accessi CloudWatch](#) nella Amazon CloudWatch User Guide.

Aggiungi trigger di rollback durante la creazione o l'aggiornamento dello stack

Per aggiungere trigger di rollback durante la creazione o l'aggiornamento dello stack (console)

1. Quando crei o aggiorni uno stack, nella pagina Configura le opzioni dello stack, in Opzioni avanzate, espandi la sezione Configurazione del rollback.
2. Immetti un tempo di monitoraggio compreso tra 0 180 minuti. Il valore predefinito è 0.
3. Specificate l'ARN dell' CloudWatch allarme o dell'allarme composito che desiderate utilizzare come trigger di rollback e scegliete Aggiungi ARN di allarme CloudWatch .

Ad esempio, quanto segue è un ARN per un CloudWatch allarme o un allarme composito,.

```
arn:aws:cloudwatch:us-east-1:123456789012:alarm:MyAlarmName
```

4. Scegli Avanti e controlla i dettagli del tuo stack.
5. Quando sei pronto, scegli Invia per creare o aggiornare lo stack.

Per aggiungere trigger di rollback durante la creazione o l'aggiornamento dello stack (AWS CLI)

Utilizzo dell'[create-stack](#) o [update-stack](#) comando con l'opzione. `--rollback-configuration`

Ad esempio, il `update-stack` comando seguente viene impostato *MyCompositeAlarm* come trigger di rollback con un periodo di monitoraggio di 5 minuti:

```
aws cloudformation update-stack --stack-name MyStack \
  --use-previous-template \
  --rollback-configuration \
  "RollbackTriggers=[{Arn=arn:aws:cloudwatch:us-
east-1:123456789012:alarm:MyCompositeAlarm,Type=AWS::CloudWatch::CompositeAlarm}],MonitoringTim
```

Aggiungere i trigger di rollback a un set di modifiche

Per aggiungere i trigger di rollback a un set di modifiche (console)

1. Quando si crea un set di modifiche, nella pagina Configura le opzioni dello stack, in Opzioni avanzate, espandi la sezione Configurazione del rollback.
2. Immetti un tempo di monitoraggio compreso tra 0 180 minuti. Il valore predefinito è 5.
3. Specificate l'ARN dell' CloudWatch allarme o dell'allarme composito che desiderate utilizzare come trigger di rollback e scegliete Aggiungi ARN di allarme CloudWatch .

Ad esempio, quanto segue è un ARN per un CloudWatch allarme o un allarme composito,.
`arn:aws:cloudwatch:us-east-1:123456789012:alarm:MyAlarmName`

4. Scegliete Avanti e controllate i dettagli del set di modifiche.
5. Quando sei pronto, scegli Crea set di modifiche per creare il set di modifiche.

Per aggiungere i trigger di rollback a un set di modifiche (AWS CLI)

Utilizzo dell'[create-change-set](#) comando con l'opzione. `--rollback-configuration`

Visualizza i trigger di rollback per uno stack

Per visualizzare trigger di rollback per uno stack, vai alla sezione Rollback configuration (Configurazione rollback).

1. Nella pagina Pile, scegli lo stack che desideri visualizzare dall'elenco a sinistra.
2. Nella scheda Informazioni sullo stack, espandi la sezione di configurazione del rollback per visualizzare i trigger di rollback.

Visualizza i trigger di rollback per un set di modifiche

Per visualizzare trigger di rollback per un set di modifiche, vai alla sezione Rollback configuration (Configurazione rollback).

1. Nella pagina Pile, scegli lo stack che desideri visualizzare dall'elenco a sinistra.
2. Scegli la scheda Change sets, quindi scegli il set di modifiche che desideri visualizzare.
3. Scegliete la scheda Input e visualizzate la sezione di configurazione del rollback.

Rileva le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento della deriva

Anche se gestisci le tue risorse tramite CloudFormation, gli utenti possono modificare tali risorse all'esterno di CloudFormation. Gli utenti possono modificare le risorse direttamente utilizzando il servizio sottostante che ha creato la risorsa. Ad esempio, puoi utilizzare la EC2 console Amazon per aggiornare un'istanza del server creata come parte di uno CloudFormation stack. Alcune modifiche potrebbero essere accidentali mentre altre potrebbero essere apportate intenzionalmente per rispondere a eventi operativi prioritari. In ogni caso, le modifiche apportate all'esterno di CloudFormation possono complicare le operazioni di aggiornamento o eliminazione dello stack. È possibile utilizzare il rilevamento delle deviazioni per identificare le risorse dello stack a cui sono state apportate modifiche alla configurazione al di fuori della gestione di CloudFormation. Puoi quindi intraprendere un'azione correttiva per risincronizzare le risorse di stack con le relative definizioni nel modello di stack, ad esempio aggiornando direttamente le risorse deviate affinché corrispondano alla propria definizione di modello. La risoluzione della deviazione consente di assicurare la coerenza della configurazione e la riuscita delle operazioni di stack.

Argomenti

- [Cos'è una deviazione?](#)
- [Codici di stato del rilevamento della deviazione](#)
- [Considerazioni sul rilevamento della deviazione](#)
- [Rileva la deriva su un'intera CloudFormation pila](#)
- [Rilevamento della deviazione su singole risorse di stack](#)
- [Risoluzione della deviazione con un'operazione di importazione](#)

Cos'è una deviazione?

Il rilevamento della deviazione consente di stabilire se la configurazione effettiva di uno stack differisce, o risulta deviata, da quella prevista. Utilizzalo CloudFormation per rilevare la deriva su un intero stack o su singole risorse all'interno dello stack. Una risorsa è considerata come deviata se uno qualsiasi dei relativi valori di proprietà effettivi differisce dai valori di proprietà previsti. Ciò include l'eventuale eliminazione della proprietà o della risorsa. Uno stack è considerato come deviato se una o più delle relative risorse risultano deviate.

Per determinare se una risorsa è andata alla deriva, CloudFormation determina i valori delle proprietà della risorsa previsti, come definiti nel modello dello stack, e tutti i valori specificati come parametri del modello. CloudFormation quindi confronta i valori previsti con i valori effettivi di tali proprietà delle risorse così come sono attualmente presenti nello stack. Una risorsa è considerata deviata se una o più delle relative proprietà sono state eliminate o se il valore delle stesse è stato modificato.

CloudFormation genera informazioni dettagliate su ogni risorsa dello stack che è andata alla deriva.

CloudFormation rileva la deriva su quelle AWS risorse che supportano il rilevamento della deriva. Alle risorse che non supportano il rilevamento delle deviazioni viene assegnato lo stato di deviazione NOT_CHECKED. Per un elenco di AWS risorse che supportano il rilevamento della deriva, vedere.

[Supporto per tipi di risorse](#)

Inoltre, CloudFormation supporta il rilevamento della deriva su tipi di risorse private che sono disponibili, ovvero il cui tipo di approvvigionamento è o. FULLY_MUTABLE IMMUTABLE Per eseguire un rilevamento della deviazione su una risorsa di un tipo di risorsa privata, è necessario che per la versione predefinita del tipo di risorsa registrata nell'account sia possibile effettuare il provisioning. Per ulteriori informazioni sul tipo di fornitura delle risorse, consulta il *ProvisioningType* parametro dell'[DescribeType](#) operazione nell'AWS CloudFormation API Reference e del [DescribeType](#) comando nel Command Reference.AWS CLI Per ulteriori informazioni sulle risorse private, vedere [Gestione delle estensioni con il CloudFormation registro](#).

Puoi eseguire il rilevamento della deviazione su stack il cui stato è: CREATE_COMPLETE, UPDATE_COMPLETE, UPDATE_ROLLBACK_COMPLETE o UPDATE_ROLLBACK_FAILED.

Quando rileva una deriva su una pila, CloudFormation non rileva la deriva su nessuna pila annidata che appartiene a quella pila. Per ulteriori informazioni, consulta [Dividi un modello in pezzi riutilizzabili usando pile annidate](#). È invece possibile avviare un'operazione di rilevamento della deviazione direttamente sullo stack nidificato.

 Note

CloudFormation determina la deriva solo per i valori delle proprietà che sono impostati in modo esplicito, tramite il modello di stack o specificando i parametri del modello. Ciò non include i valori predefiniti delle proprietà di risorsa. Per tenere CloudFormation traccia della proprietà di una risorsa allo scopo di determinare la deriva, impostate esplicitamente il valore della proprietà, anche se la state impostando sul valore predefinito.

Codici di stato del rilevamento della deviazione

Le tabelle di questa sezione descrivono i vari tipi di stato utilizzati con il rilevamento della deviazione:

- Lo stato dell'operazione di rilevamento della deviazione descrive lo stato corrente dell'operazione.
- Drift status (Stato di deviazione)

Per i set di stack, questo descrive lo stato di deviazione del set di stack nel suo complesso, in base allo stato di deviazione delle istanze dello stack che lo appartengono.

Per le istanze dello stack, questo descrive lo stato di deviazione dell'istanza dello stack, in base allo stato di deviazione dello stack associato.

Lo stato di deviazione dello stack descrive lo stato di deviazione dell'intero stack, in base allo stato di deviazione delle relative risorse.

- Lo stato di deviazione di risorsa descrive lo stato di deviazione di una singola risorsa.

La tabella seguente elenca i codici di stato CloudFormation assegnati alle operazioni di rilevamento della deriva dello stack.

Stato dell'operazione di rilevamento della deviazione	Descrizione
DETECTION_COMPLETE	L'operazione di rilevamento della deviazione di stack è stata completata con successo per tutte le risorse nello stack che supportano il rilevamento della deviazione.
DETECTION_FAILED	L'operazione di rilevamento della deviazione di stack non è riuscita per almeno una risorsa nello stack. I risultati saranno

Stato dell'operazione di rilevamento della deviazione	Descrizione
	disponibili per le risorse sulle quali il rilevamento della deriva è CloudFormation stato completato con successo.
DETECTION_IN_PROGRESS	L'operazione di rilevamento della deviazione di stack è attualmente in corso.

La tabella seguente elenca i codici di stato di deriva assegnati agli CloudFormation stack.

Drift status (Stato di deviazione)	Descrizione
DRIFTED	Per gli stack: lo stack differisce, o risulta deviato, dalla configurazione di modello prevista. Uno stack è considerato come deviato se una o più delle relative risorse risultano deviate. Per le istanze dello stack: un'istanza dello stack è considerata deviate se lo stack ad esso associato è stato deviato. Per i set di stack: un set di stack è considerato deviato se una o più istanze di stack sono state deviate.
NOT_CHECKED	CloudFormation non ha verificato se lo stack, lo stack set o l'istanza dello stack differiscono dalla configurazione del modello prevista.
IN_SYNC	La configurazione corrente di ogni risorsa supportata corrisponde alla configurazione di modello prevista. Uno stack, un set di stack o un'istanza di stack senza risorse che supportano il rilevamento della deviazione avrà anche lo stato IN_SYNC.

La tabella seguente elenca i codici di stato di drift assegnati alle risorse dello stack CloudFormation .

Stato di deviazione di risorsa	Descrizione
DELETED	La risorsa differisce dalla relativa configurazione di modello prevista in quanto la risorsa è stata eliminata.
MODIFIED	La risorsa differisce, o risulta deviata, dalla relativa configurazione di modello prevista.
NOT_CHECKED	CloudFormation non ha verificato se la risorsa differisce dalla configurazione del modello prevista.
IN_SYNC	La configurazione corrente della risorsa corrisponde alla configurazione di modello prevista.

La tabella seguente elenca i codici di stato del tipo di differenza CloudFormation assegnati alle proprietà delle risorse che differiscono dalla configurazione prevista del modello.

Tipi di differenza di proprietà	Descrizione
ADD	Un valore è stato aggiunto a una proprietà della risorsa che è un tipo di dati a matrice o elenco.
REMOVE	La proprietà è stata rimossa dalla configurazione di risorsa corrente.
NOT_EQUAL	Il valore di proprietà corrente differisce dal relativo valore previsto come definito nel modello di stack.

Considerazioni sul rilevamento della deviazione

Per eseguire con successo il rilevamento della deviazione su uno stack, un utente deve disporre delle autorizzazioni seguenti:

- Autorizzazione di lettura per ogni risorsa che supporta il rilevamento della rilevazione inclusa nello stack. Ad esempio, se lo stack include una risorsa `AWS::EC2::Instance`, devi disporre dell'autorizzazione `ec2:DescribeInstances` per eseguire il rilevamento della deviazione sullo stack.

- `cloudformation:DetectStackDrift`
- `cloudformation:DetectStackResourceDrift`
- `cloudformation:BatchDescribeTypeConfigurations`

Per ulteriori informazioni sull'impostazione delle autorizzazioni in, vedere. CloudFormation [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#)

In alcuni casi estremi, CloudFormation potrebbe non essere possibile restituire sempre risultati di deriva accurati. Devi essere consapevole dell'esistenza di questi casi limite per interpretare in modo appropriato i risultati del rilevamento della deviazione.

- In alcuni casi, gli oggetti contenuti in matrici di proprietà sono segnalati come deviazione, quando in realtà sono valori predefiniti forniti alla proprietà dal servizio sottostante responsabile della risorsa.
- Alcune risorse hanno relazioni di collegamento con risorse correlate; una risorsa può quindi effettivamente collegare o rimuovere valori di proprietà per un'altra risorsa, definiti nello stesso modello o in un altro modello. Ad esempio, le risorse `AWS::EC2::SecurityGroupEgress` e `AWS::EC2::SecurityGroupIngress` possono essere utilizzate per collegare e rimuovere valori dalle risorse `AWS::EC2::SecurityGroup`. In questi casi, CloudFormation analizza il modello di pila per gli allegati prima di eseguire il confronto della deriva. Tuttavia, non è CloudFormation possibile eseguire questa analisi tra pile e pertanto potrebbe non restituire risultati di deriva accurati se le risorse collegate risiedono in pile diverse.

Le risorse che supportano il rilevamento della deviazione e consentono o necessitano collegamenti da altre risorse includono:

Tipo di risorsa	Tipo di risorsa di collegamento
<code>AWS::SNS::Topic</code>	<code>AWS::SNS::Subscription</code>
<code>AWS::IAM::User</code>	<code>AWS::IAM::UserToGroupAddition</code>
<code>AWS::IAM::Group</code>	<code>AWS::IAM::ManagedPolicy</code>
<code>AWS::IAM::Role</code>	<code>AWS::IAM::Policy</code>
<code>AWS::IAM::User</code>	<code>AWS::IAM::RolePolicy</code>

Tipo di risorsa	Tipo di risorsa di collegamento
<code>AWS::ElasticLoadBalancingV2::Listener</code>	<code>AWS::ElasticLoadBalancingV2::ListenerCertificate</code>
<code>AWS::EC2::SecurityGroup</code>	<code>AWS::EC2::SecurityGroupEgress</code> <code>AWS::EC2::SecurityGroupIngress</code>

- CloudFormation non esegue il rilevamento della deriva sulla proprietà di alcuna risorsa. `KMSKeyId` Poiché AWS KMS le chiavi possono essere referenziate da più alias, non è CloudFormation possibile garantire risultati di deriva costantemente accurati per questa proprietà.
- Nel modello di stack è possibile specificare alcune proprietà delle risorse che, per loro stessa natura, CloudFormation non possono essere confrontate con le proprietà delle risorse dello stack risultanti. Queste proprietà non possono quindi essere incluse nei risultati del rilevamento della deviazione. Tali proprietà rientrano in due categorie generali:
 - Valori delle proprietà che CloudFormation non possono essere mappati al valore iniziale delle proprietà della risorsa nel modello dello stack.

Ad esempio, CloudFormation non può mappare il codice sorgente di una funzione Lambda al tipo di `Code` proprietà della `AWS::Lambda::Function` risorsa e quindi non CloudFormation può includerlo nei risultati del rilevamento della deriva.

- Valori di proprietà che il servizio responsabile della risorsa non restituisce.

Esistono alcuni valori di proprietà che, per concezione, non vengono mai restituiti dal servizio a cui la risorsa appartiene. Questi valori contengono in genere informazioni riservate, come password o altri dati sensibili che non devono essere esposti. Ad esempio, il servizio IAM non restituirà mai il valore della `Password` proprietà del tipo di `AWS::IAM::User LoginProfile` proprietà e pertanto non CloudFormation potrà includerlo nei risultati del rilevamento delle deviazioni.

- Gli oggetti in un array: possono essere in realtà impostazioni predefinite del servizio, non una deviazione aggiunta manualmente.
- Se riscontri falsi positivi, inviaci i tuoi commenti utilizzando il link di feedback nella CloudFormation console oppure contattaci tramite [AWS re:Post](#).
- Alcune proprietà possono avere valori di input uguali ma non identici. Per evitare falsi positivi, è necessario assicurarsi che la configurazione prevista corrisponda alla configurazione effettiva.

- Ad esempio, la configurazione prevista della proprietà della risorsa può essere 1.024 MB, mentre la configurazione effettiva della stessa proprietà può essere 1 GB. 1.024 MB e 1 GB sono valori uguali ma non identici.

Quando su questa proprietà della risorsa viene eseguito il rilevamento delle deviazioni, verranno segnalate le deviazioni.

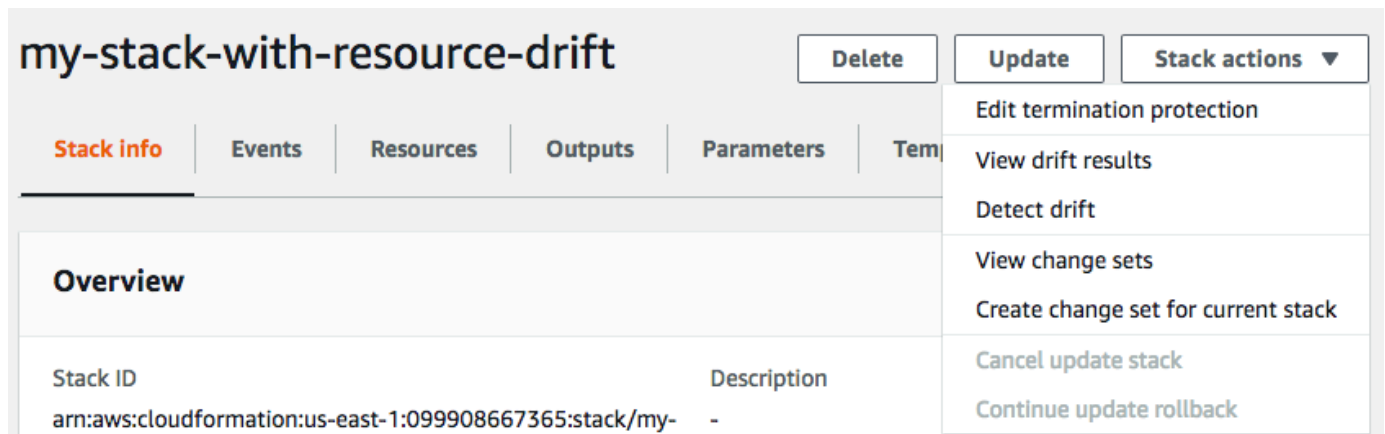
Per evitare questo falso positivo, modifica la configurazione prevista della proprietà della risorsa a 1.024 MB, quindi esegui il rilevamento delle deviazioni.

Rileva la deriva su un'intera CloudFormation pila

L'esecuzione di un'operazione di rilevamento della deviazione su uno stack determina se lo stack risulta deviato dalla relativa configurazione di modello prevista e restituisce informazioni dettagliate sullo stato di deviazione di ogni risorsa nello stack che supporta il rilevamento della deviazione.

Per rilevare la deriva su un'intera pila utilizzando il AWS Management Console

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Dagli elenchi di stack, selezionare lo stack su cui eseguire il rilevamento delle deviazioni. Nel riquadro dei dettagli dello stack, scegliere Stack actions (Operazioni stack), quindi scegliere Detect drift (Rileva deviazioni).



CloudFormation visualizza una barra informativa che indica che il rilevamento della deriva è stato avviato per lo stack selezionato.

3. Attendere il CloudFormation completamento dell'operazione di rilevamento della deriva. Al termine dell'operazione di rilevamento della deriva, CloudFormation aggiorna lo stato di Drift e

l'ora di verifica dell'ultima deriva per lo stack. Questi campi sono elencati nella sezione Overview (Panoramica) del riquadro Stack info (Info stack) della pagina dei dettagli dello stack.

L'operazione di rilevamento della deviazione può durare vari minuti, a seconda del numero di risorse incluse nello stack. È possibile eseguire una sola operazione di rilevamento della deriva su un determinato stack alla volta. CloudFormation continua l'operazione di rilevamento della deriva anche dopo aver chiuso la barra delle informazioni.

4. Esaminare i risultati del rilevamento della deviazione per lo stack e le relative risorse. Con lo stack selezionato, dal menu Stack actions (Operazioni stack), selezionare View drift results (Visualizza risultati deviazione).

CloudFormation elenca lo stato generale della deriva dello stack, oltre all'ultima volta in cui è stato avviato il rilevamento della deriva sullo stack o su una delle sue singole risorse. Uno stack è considerato come deviato se una o più delle relative risorse risultano deviate.

CloudFormation > Stacks: my-stack-with-resource-drift > Drifts

Drifts

[Refresh](#) [Detect stack drift](#)

Stack drift status

Drift detection enables you to detect whether a stack's actual configuration differs, or has drifted, from its template configuration. [Learn more.](#)

Drift status	Last drift check time
DRIFTED	Fri, 24 May 2019 16:08:12 GMT

Nella sezione Resource drift status, CloudFormation elenca ogni risorsa dello stack, il relativo stato di deriva e l'ultima volta in cui è stato avviato il rilevamento della deriva sulla risorsa. L'ID logico e l'ID fisico di ogni risorsa sono visualizzati per consentirti di identificarla. Inoltre, per le risorse con stato MODIFICATO, visualizza i dettagli sulla deriva delle risorse. CloudFormation

È possibile ordinare le risorse in base al loro stato deviazione, utilizzando la colonna Drift (Deviazione).

- Per visualizzare i dettagli su una risorsa modificata
 - Con le risorse modificate selezionate, selezionare View drift details (Visualizza dettagli deviazione).

CloudFormation visualizza la pagina di dettaglio della deriva per quella risorsa. Questa pagina elenca i valori di proprietà previsti e correnti della risorsa e le differenze tra gli stessi.

Per evidenziare una differenza, nella sezione Differences (Differenze) selezionare il nome della proprietà.

- Le proprietà aggiunte vengono evidenziate in verde nella colonna Current (Corrente) della sezione Details (Dettagli).
- Le proprietà eliminate vengono evidenziate in rosso nella colonna Expected (Previsti) della sezione Details (Dettagli).
- Le proprietà il cui valore è stato modificato sono evidenziate in giallo nelle colonne Expected (Previsti) e Current (Correnti).

Differences (4)

< 1 >

☒	Property	Change	Expected value	Current value
☒	AttributeDefinitions.1	ADD	-	{"AttributeName": "stuff", "AttributeType": "S"}
☒	ProvisionedThroughput.ReadCapacityUnits	NOT_EQUAL	5	6
☒	ProvisionedThroughput.WriteCapacityUnits	NOT_EQUAL	5	4
☒	Tags	REMOVE	[{"Key": "test", "Value": "test"}]	-

Details

Expected

Actual

```
{
  "AttributeDefinitions": [
    {
      "AttributeName": "Name",
      "AttributeType": "S"
    },
  ],
  "KeySchema": [
    {
      "AttributeName": "Name",
      "KeyType": "HASH"
    }
  ],
  "ProvisionedThroughput": {
    "ReadCapacityUnits": 5,
    "WriteCapacityUnits": 5
  },
  "Tags": [
    {
      "Key": "test",
      "Value": "test"
    }
  ]
}
```

```
{
  "AttributeDefinitions": [
    {
      "AttributeName": "Name",
      "AttributeType": "S"
    },
    {
      "AttributeName": "stuff",
      "AttributeType": "S"
    }
  ],
  "KeySchema": [
    {
      "AttributeName": "Name",
      "KeyType": "HASH"
    }
  ],
  "ProvisionedThroughput": {
    "ReadCapacityUnits": 6,
    "WriteCapacityUnits": 4
  }
}
```

Per rilevare la deriva su un'intera pila utilizzando il AWS CLI

Important

Controlla l'ora di verifica dell'ultima deriva per lo stack e conferma che sia precedente al timestamp mostrato nei risultati della deriva delle risorse per evitare l'uso di dati non aggiornati.

Per rilevare la deriva su un intero stack utilizzando il, utilizzate i seguenti comandi: AWS CLI AWS CLI

- `detect-stack-drift` per avviare un'operazione di rilevamento della deviazione su uno stack.
 - `describe-stack-drift-detection-status` per monitorare lo stato dell'operazione di rilevamento della deviazione di stack.
 - `describe-stack-resource-drifts` per esaminare i dettagli dell'operazione di rilevamento della deviazione di stack.
1. Utilizzare `detect-stack-drift` per rilevare la deviazione su un intero stack. Specificare il nome o l'ARN dello stack. È inoltre possibile specificare la logica IDs di qualsiasi risorsa specifica che si desidera utilizzare come filtri per questa operazione di rilevamento della deriva.

```
aws cloudformation detect-stack-drift --stack-name my-stack-with-resource-drift
```

Output:

```
{  
  "StackDriftDetectionId": "624af370-311a-11e8-b6b7-500cexample"  
}
```

2. Poiché le operazioni di rilevamento della deviazione di stack possono durare parecchio tempo, utilizzare `describe-stack-drift-detection-status` per monitorare lo stato dell'operazione di rilevamento. Questo comando utilizza l'ID rilevamento della deviazione di stack restituito dal comando `detect-stack-drift`.

Nell'esempio seguente, abbiamo passato come parametro a `describe-stack-drift-detection-status` l'ID rilevamento della deviazione di stack restituito dall'esempio `detect-stack-drift` precedente. Il parametro restituisce i dettagli dell'operazione che mostrano che l'operazione di rilevamento

della deviazione è stata completata, che una singola risorsa di stack risulta deviata e che di conseguenza l'intero stack è considerato come deviato.

```
aws cloudformation describe-stack-drift-detection-status --stack-drift-detection-id 624af370-311a-11e8-b6b7-500cexample
```

Output:

```
{
  "StackId": "arn:aws:cloudformation:us-east-1:099908667365:stack/my-stack-with-resource-drift/489e5570-df85-11e7-a7d9-50example",
  "StackDriftDetectionId": "624af370-311a-11e8-b6b7-500cexample",
  "StackDriftStatus": "DRIFTED",
  "Timestamp": "2018-03-26T17:23:22.279Z",
  "DetectionStatus": "DETECTION_COMPLETE",
  "DriftedStackResourceCount": 1
}
```

3. Al termine dell'operazione di rilevamento della deviazione di stack, utilizzare il comando `describe-stack-resource-drifts` per esaminare i risultati, inclusi i valori di proprietà correnti e previsti per le risorse deviate.

L'esempio seguente utilizza l'`--stack-resource-drift-status-filters` opzione per richiedere informazioni sulla deriva dello stack per quelle risorse che sono state modificate o eliminate. La richiesta restituisce informazioni sulla risorsa che è stata modificata, tra cui dettagli su due proprietà della stessa i cui valori sono stati modificati. Nessuna risorsa è stata eliminata.

```
aws cloudformation describe-stack-resource-drifts --stack-name my-stack-with-resource-drift --stack-resource-drift-status-filters MODIFIED DELETED
```

Output:

```
{
  "StackResourceDrifts": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:099908667365:stack/my-stack-with-resource-drift/489e5570-df85-11e7-a7d9-50example",
      "ActualProperties": "{\"ReceiveMessageWaitTimeSeconds\":0, \"DelaySeconds\":120, \"RedrivePolicy\":{\"deadLetterTargetArn\":\"arn:aws:sqs:us-east-1:099908667365:my-stack-with-resource-drift-DLQ-1BCY7HHD5QIM3\"},
```



```

    \"maxReceiveCount\":12},\"MessageRetentionPeriod\":345600,\"MaximumMessageSize
    \":262144,\"VisibilityTimeout\":60,\"QueueName\":\"my-stack-with-resource-drift-
    Queue-494PBHC076H4\"}],
    \"ResourceType\": \"AWS::SQS::Queue\",
    \"Timestamp\": \"2018-03-26T17:23:34.489Z\",
    \"PhysicalResourceId\": \"https://sqs.us-
    east-1.amazonaws.com/099908667365/my-stack-with-resource-drift-
    Queue-494PBHC076H4\",
    \"StackResourceDriftStatus\": \"MODIFIED\",
    \"ExpectedProperties\": \"{\\\"ReceiveMessageWaitTimeSeconds\\\":0,
    \\\"DelaySeconds\\\":20,\\\"RedrivePolicy\\\":{\\\"deadLetterTargetArn\\\":\\\"arn:aws:sqs:us-
    east-1:099908667365:my-stack-with-resource-drift-DLQ-1BCY7HHD5QIM3\\\",
    \\\"maxReceiveCount\\\":10},\\\"MessageRetentionPeriod\\\":345600,\\\"MaximumMessageSize
    \":262144,\\\"VisibilityTimeout\\\":60,\\\"QueueName\\\":\\\"my-stack-with-resource-drift-
    Queue-494PBHC076H4\\\"}\",
    \"PropertyDifferences\": [
      {
        \"PropertyPath\": \"/DelaySeconds\",
        \"ActualValue\": \"120\",
        \"ExpectedValue\": \"20\",
        \"DifferenceType\": \"NOT_EQUAL\"
      },
      {
        \"PropertyPath\": \"/RedrivePolicy/maxReceiveCount\",
        \"ActualValue\": \"12\",
        \"ExpectedValue\": \"10\",
        \"DifferenceType\": \"NOT_EQUAL\"
      }
    ],
    \"LogicalResourceId\": \"Queue\"
  }
]
}

```

Rilevamento della deviazione su singole risorse di stack

Puoi rilevare la deviazione su specifiche risorse di uno stack anziché sull'intero stack. Ciò è particolarmente utile quando è necessario determinare soltanto se specifiche risorse corrispondono di nuovo alle relative configurazioni di modello previste.

Quando si esegue il rilevamento della deriva su una risorsa, aggiorna CloudFormation anche lo stato generale della deriva dello stack e l'ora dell'ultima verifica della deriva, se applicabile. Ad esempio,

supponiamo che uno stack abbia uno stato di deriva pari a. `IN_SYNC` È stato CloudFormation eseguito il rilevamento della deriva su una o più risorse contenute in quella pila e si CloudFormation rileva che una o più di tali risorse si sono spostate. CloudFormation aggiorna lo stato di deriva dello stack a. `DRIFTED` Al contrario, supponiamo di avere uno stack con uno stato di deriva `DRIFTED` dovuto a una singola risorsa alla deriva. Se reimpostate la risorsa ai valori di proprietà previsti e quindi rilevate nuovamente la deriva sulla risorsa, CloudFormation aggiornerà sia lo stato di deriva della risorsa che lo stato di deriva dello stack `IN_SYNC` senza che sia necessario rilevare nuovamente la deriva sull'intero stack.

Per rilevare la deriva su una singola risorsa utilizzando AWS Management Console

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Dall'elenco di stack, selezionare lo stack che contiene la risorsa. CloudFormation mostra i dettagli stack per quello stack.
3. Nel riquadro di spostamento a sinistra, in Stack, scegliere Azioni stack, quindi scegliere Rileva deriva.
4. In Resource drift status (Stato deviazione risorsa), scegliere la risorsa e quindi selezionare Detect drift for resource (Rileva deviazione per risorsa).

CloudFormation esegue il rilevamento della deriva sulla risorsa selezionata. In caso di successo, CloudFormation aggiorna lo stato di deriva della risorsa e lo stato generale della deriva dello stack, se necessario. CloudFormation aggiorna anche il timestamp dell'ultima volta che il rilevamento della deriva è stato eseguito sulla risorsa e sullo stack nel suo insieme. Se la risorsa è stata modificata, CloudFormation visualizza informazioni dettagliate sulla deriva sui valori delle proprietà attesi e correnti della risorsa.

5. Esaminare i risultati del rilevamento della deviazione per la risorsa.
 - Per visualizzare i dettagli su una risorsa modificata
 - Con le risorse modificate selezionate, selezionare View drift details (Visualizza dettagli deviazione).

CloudFormation visualizza i dettagli sulla deriva per quella risorsa, inclusi i valori delle proprietà attesi e correnti della risorsa e le eventuali differenze tra le due.

Per evidenziare una differenza, nella sezione Differences (Differenze) selezionare il nome della proprietà.

- Le proprietà aggiunte vengono evidenziate in verde nella colonna Current (Corrente) della sezione Details (Dettagli).
- Le proprietà eliminate vengono evidenziate in rosso nella colonna Expected (Previsti) della sezione Details (Dettagli).
- Le proprietà il cui valore è stato modificato sono evidenziate in giallo nelle colonne Expected (Previsti) e Current (Correnti).

Differences (4)

< 1 >

☒	Property	Change	Expected value	Current value
☒	AttributeDefinitions.1	ADD	-	{"AttributeName": "stuff", "AttributeType": "S"}
☒	ProvisionedThroughput.ReadCapacityUnits	NOT_EQUAL	5	6
☒	ProvisionedThroughput.WriteCapacityUnits	NOT_EQUAL	5	4
☒	Tags	REMOVE	[{"Key": "test", "Value": "test"}]	-

Details

Expected

Actual

```
{
  "AttributeDefinitions": [
    {
      "AttributeName": "Name",
      "AttributeType": "S"
    },
  ],
  "KeySchema": [
    {
      "AttributeName": "Name",
      "KeyType": "HASH"
    }
  ],
  "ProvisionedThroughput": {
    "ReadCapacityUnits": 5,
    "WriteCapacityUnits": 5
  },
  "Tags": [
    {
      "Key": "test",
      "Value": "test"
    }
  ]
}
```

```
{
  "AttributeDefinitions": [
    {
      "AttributeName": "Name",
      "AttributeType": "S"
    },
    {
      "AttributeName": "stuff",
      "AttributeType": "S"
    }
  ],
  "KeySchema": [
    {
      "AttributeName": "Name",
      "KeyType": "HASH"
    }
  ],
  "ProvisionedThroughput": {
    "ReadCapacityUnits": 6,
    "WriteCapacityUnits": 4
  }
}
```

Per rilevare la deriva su una singola risorsa utilizzando AWS CLI

Important

Esamina l'ora di controllo dell'ultima deriva per la risorsa dello stack e conferma che sia precedente al timestamp mostrato nei risultati della deriva delle risorse per evitare l'uso di dati obsoleti.

Per rilevare la deriva su una singola risorsa utilizzando il, usa il comando `AWS CLI detect-stack-resource-drift`. Specificare l'ID logico della risorsa, nonché lo stack che la contiene.

L'esempio seguente esegue un'operazione di rilevamento della deriva su una specifica risorsa dello stack, `my-drifted-resource`. La risposta restituisce informazioni che confermano che la risorsa è stata modificata, tra cui dettagli su due proprietà della stessa i cui valori sono stati modificati.

```
aws cloudformation detect-stack-resource-drift \
  --stack-name my-stack-with-resource-drift \
  --logical-resource-id my-drifted-resource
```

Output:

```
{
  "StackResourceDrift": {
    "StackId": "arn:aws:cloudformation:us-east-1:099908667365:stack/my-stack-with-resource-drift/489e5570-df85-11e7-a7d9-50example",
    "ActualProperties": "{\"ReceiveMessageWaitTimeSeconds\":0,\"DelaySeconds\":120,\"RedrivePolicy\":{\"deadLetterTargetArn\":\"arn:aws:sqs:us-east-1:099908667365:my-stack-with-resource-drift-DLQ-1BCY7HHD5QIM3\",\"maxReceiveCount\":12},\"MessageRetentionPeriod\":345600,\"MaximumMessageSize\":262144,\"VisibilityTimeout\":60,\"QueueName\":\"my-stack-with-resource-drift-Queue-494PBHC076H4\"}",
    "ResourceType": "AWS::SQS::Queue",
    "Timestamp": "2018-03-26T18:54:28.462Z",
    "PhysicalResourceId": "https://sqs.us-east-1.amazonaws.com/099908667365/my-stack-with-resource-drift-Queue-494PBHC076H4",
    "StackResourceDriftStatus": "MODIFIED",
    "ExpectedProperties": "{\"ReceiveMessageWaitTimeSeconds\":0,\"DelaySeconds\":20,\"RedrivePolicy\":{\"deadLetterTargetArn\":\"arn:aws:sqs:us-
```

```

east-1:099908667365:my-stack-with-resource-drift-DLQ-1BCY7HHD5QIM3\",
\"maxReceiveCount\":10},\"MessageRetentionPeriod\":345600,\"MaximumMessageSize
\":262144,\"VisibilityTimeout\":60,\"QueueName\":\"my-stack-with-resource-drift-
Queue-494PBHC076H4\"}],
  \"PropertyDifferences\": [
    {
      \"PropertyPath\": \"/DelaySeconds\",
      \"ActualValue\": \"120\",
      \"ExpectedValue\": \"20\",
      \"DifferenceType\": \"NOT_EQUAL\"
    },
    {
      \"PropertyPath\": \"/RedrivePolicy/maxReceiveCount\",
      \"ActualValue\": \"12\",
      \"ExpectedValue\": \"10\",
      \"DifferenceType\": \"NOT_EQUAL\"
    }
  ],
  \"LogicalResourceId\": \"my-drifted-resource\"
}
}

```

Risoluzione della deviazione con un'operazione di importazione

Ci possono essere casi in cui la configurazione di una risorsa ha deviato dalla configurazione prevista e si desidera accettare la nuova configurazione come configurazione prevista. Nella maggior parte dei casi, è possibile risolvere i risultati della deviazione aggiornando la definizione della risorsa nel modello di stack con una nuova configurazione e quindi eseguire un aggiornamento dello stack. Tuttavia, se la nuova configurazione aggiorna una proprietà della risorsa che richiede la sostituzione, la risorsa verrà ricreata durante l'aggiornamento dello stack. Se si desidera mantenere la risorsa esistente, è possibile utilizzare la caratteristica di importazione delle risorse per aggiornare la risorsa e risolvere i risultati della deviazione senza causare la sostituzione della risorsa.

La risoluzione della deviazione per una risorsa tramite un'operazione di importazione consiste nelle fasi di base riportate di seguito.

- [Aggiungi un DeletionPolicy attributo, impostato su Retain, alla risorsa](#). In questo modo la risorsa esistente viene mantenuta anziché eliminata quando viene rimossa dallo stack.
- [Rimuovere la risorsa dal modello ed eseguire un'operazione di aggiornamento dello stack](#). Questa operazione rimuove la risorsa dallo stack, ma non la elimina.

- [Descrivere lo stato effettivo della risorsa nel modello di stack e quindi importare nuovamente la risorsa esistente nello stack](#). Questa operazione aggiunge nuovamente la risorsa nello stack e risolve le differenze di proprietà che causavano i risultati di deviazione.

Per ulteriori informazioni sull'importazione di risorse, vedere [Importazione AWS manuale delle risorse in uno CloudFormation stack](#). Per un elenco di risorse che supportano l'importazione, vedere [Supporto per tipi di risorse](#).

In questo esempio, viene utilizzato il modello seguente, denominato `templateToImport.json`.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "BillingMode": "PROVISIONED",
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    },
    "GamesTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
```

```

        "TableName": "Games",
        "AttributeDefinitions": [
            {
                "AttributeName": "key",
                "AttributeType": "S"
            }
        ],
        "KeySchema": [
            {
                "AttributeName": "key",
                "KeyType": "HASH"
            }
        ],
        "BillingMode": "PROVISIONED",
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 1
        }
    }
}

```

Example YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Import test
Resources:
  ServiceTable:
    Type: 'AWS::DynamoDB::Table'
    Properties:
      TableName: Service
      AttributeDefinitions:
        - AttributeName: key
          AttributeType: S
      KeySchema:
        - AttributeName: key
          KeyType: HASH
      BillingMode: PROVISIONED
      ProvisionedThroughput:
        ReadCapacityUnits: 5
        WriteCapacityUnits: 1
  GamesTable:

```

```

Type: 'AWS::DynamoDB::Table'
Properties:
  TableName: Games
  AttributeDefinitions:
    - AttributeName: key
      AttributeType: S
  KeySchema:
    - AttributeName: key
      KeyType: HASH
  BillingMode: PROVISIONED
  ProvisionedThroughput:
    ReadCapacityUnits: 5
    WriteCapacityUnits: 1

```

In questo esempio, supponiamo che un utente abbia modificato una risorsa esterna a CloudFormation. Dopo aver eseguito il rilevamento della deviazione, abbiamo scoperto che è GamesTable stato modificato da BillingMode in PAY_PER_REQUEST. Per ulteriori informazioni sul rilevamento della deriva, vedere [Rileva le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento della deriva](#).

Differences (3)					< 1 >
☒	Property	Change	Expected value	Current value	
☒	BillingMode	NOT_EQUAL	PROVISIONED	PAY_PER_REQUEST	
☒	ProvisionedThroughput.ReadCapacityUnits	NOT_EQUAL	5	0	
☒	ProvisionedThroughput.WriteCapacityUnits	NOT_EQUAL	1	0	
Details					
Expected			Actual		
<pre> { "AttributeDefinitions": [{ "AttributeName": "key", "AttributeType": "S" }], "BillingMode": "PROVISIONED", "KeySchema": [{ "AttributeName": "key", "KeyType": "HASH" }], "ProvisionedThroughput": { "ReadCapacityUnits": 5, "WriteCapacityUnits": 1 }, "TableName": "Games" } </pre>			<pre> { "AttributeDefinitions": [{ "AttributeName": "key", "AttributeType": "S" }], "BillingMode": "PAY_PER_REQUEST", "KeySchema": [{ "AttributeName": "key", "KeyType": "HASH" }], "ProvisionedThroughput": { "ReadCapacityUnits": 0, "WriteCapacityUnits": 0 }, "TableName": "Games" } </pre>		

Il nostro stack è ora obsoleto, le nostre risorse sono attive, ma vogliamo preservare la configurazione delle risorse desiderata. Possiamo farlo risolvendo la deviazione attraverso un'operazione di importazione, senza interrompere i servizi.

Risolvi la deriva con un'operazione di importazione utilizzando la console CloudFormation

Fase 1: Aggiornare lo stack con la policy di eliminazione Retain

Per aggiornare lo stack utilizzando un attributo **DeletionPolicy** con l'opzione **Retain**

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella pagina Stacks (stack) scegliere lo stack che ha deviato.
3. Scegliere Update (Aggiorna), quindi Replace current template (Sostituisci modello corrente) dal riquadro dei dettagli dello stack.
4. Nella pagina Specify template (Specifica modello) fornire il modello aggiornato contenente l'attributo DeletionPolicy con l'opzione Retain utilizzando uno dei seguenti metodi:
 - Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il modello.

Quindi, seleziona Next (Successivo).

5. Esaminare la pagina Specify stack details (Specifica dettagli stack) e scegliere Next (Avanti).
6. Esaminare la pagina Configure stack options (Configura opzioni stack) e scegliere Next (Avanti).
7. Nella **stack-name** pagina di revisione, scegli Update stack.

Risultati: nella pagina Events (Eventi) dello stack, lo stato è UPDATE_COMPLETE.

Per risolvere il problema della deriva derivante da un'operazione di importazione, senza interrompere i servizi, specificate a Retain [DeletionPolicy](#) per le risorse che desiderate rimuovere dallo stack. Nell'esempio seguente, abbiamo aggiunto un [DeletionPolicy](#) attributo, set to Retain, alla risorsa GameTable

Example JSON

```
"GameTable": {
  "Type": "AWS::DynamoDB::Table",
  "DeletionPolicy": "Retain",
  "Properties": {
```

```
"TableName": "Games",
```

Example YAML

```
GamesTable:
  Type: 'AWS::DynamoDB::Table'
  DeletionPolicy: Retain
  Properties:
    TableName: Games
```

Fase 2: Rimozione delle risorse deviate, dei parametri correlati e degli output

Per rimuovere le risorse deviate, i parametri correlati e gli output

1. Scegliere Update (Aggiorna), quindi Replace current template (Sostituisci modello corrente) dal riquadro dei dettagli dello stack.
2. Nella pagina Specify template (Specifica modello) fornire al modello aggiornato le risorse, i parametri correlati e gli output rimossi dal modello di stack utilizzando uno dei seguenti metodi:
 - Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il modello.

Quindi, seleziona Next (Successivo).

3. Esaminare la pagina Specify stack details (Specifica dettagli stack) e scegliere Next (Avanti).
4. Esaminare la pagina Configure stack options (Configura opzioni stack) e scegliere Next (Avanti).
5. Nella *stack-name* pagina Revisione, scegli Aggiorna stack.

Risultati: Logical ID (ID logico) GamesTable ha lo stato DELETE_SKIPPED nella pagina Events (Eventi) dello stack.

Attendi il CloudFormation completamento dell'operazione di aggiornamento dello stack. Al termine dell'operazione di aggiornamento dello stack, rimuovere la risorsa, i parametri correlati e gli output dal modello di stack. Quindi, importare il modello aggiornato. Dopo aver completato queste operazioni, il modello di esempio sarà simile al seguente.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "BillingMode": "PROVISIONED",
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    }
  }
}
```

Example YAML

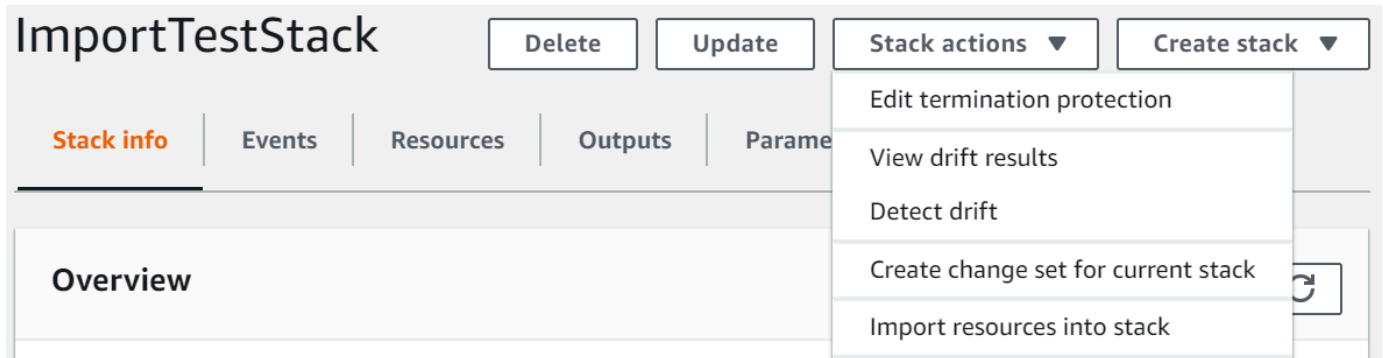
```
AWSTemplateFormatVersion: 2010-09-09
Description: Import test
Resources:
  ServiceTable:
    Type: 'AWS::DynamoDB::Table'
    Properties:
      TableName: Service
      AttributeDefinitions:
        - AttributeName: key
```

```
AttributeType: S
KeySchema:
  - AttributeName: key
    KeyType: HASH
BillingMode: PROVISIONED
ProvisionedThroughput:
  ReadCapacityUnits: 5
  WriteCapacityUnits: 1
```

Fase 3. Aggiornamento del modello in modo che corrisponda allo stato attivo delle risorse

Per aggiornare il modello in modo che corrisponda allo stato attivo delle risorse

1. Per importare il modello aggiornato, scegliere **Stack actions** (Operazioni stack) e quindi scegliere **Import resources into stack** (Importa risorse nello stack).



2. Esaminare la pagina **Import overview** (Panoramica importazione) per un elenco di elementi da fornire durante questa operazione, quindi scegliere **Next** (Avanti).
3. Nella pagina **Specify model** (Specifica modello), fornire il modello aggiornato utilizzando uno dei metodi descritti di seguito.
 - Scegliere **Amazon S3 URL** (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere **Upload a template file** (Carica un file modello), quindi cercare il modello.

Quindi, seleziona **Next** (Successivo).

4. Nella pagina **Identify resources** (Identifica risorse), identifica ogni risorsa di destinazione. Per ulteriori informazioni, consulta [Identificatori di risorse](#).

- a. In Identifier property (Proprietà identificatore), scegliere il tipo di identificatore di risorsa. Ad esempio, la proprietà `TableName` identificherà la risorsa `AWS::DynamoDB::Table`.
 - b. In Identifier value (Valore identificatore), immettere il valore effettivo della proprietà. Nel modello di esempio, `TableName` per la risorsa `GameTable` è `Games`.
 - c. Scegli Next (Successivo).
5. Esaminare la pagina Specify stack details (Specifica dettagli stack) e scegliere Next (Avanti).
 6. Nella pagina Import overview (Panoramica importazione) esaminare le risorse importate, quindi scegliere Import resources (Importa risorse). Questa operazione importerà il tipo di risorsa `AWS::DynamoDB::Table` nello stack.

Risultati: in questo esempio, è stata risolta la deviazione delle risorse attraverso un'operazione di importazione, senza interrompere i servizi. Puoi controllare lo stato di avanzamento di un'azione di importazione nella CloudFormation console nella scheda Eventi. Le risorse importate avranno uno stato `IMPORT_COMPLETE` seguito da uno stato `CREATE_COMPLETE` con `Resource import complete` (Importazione risorse completata) come motivo dello stato.

Attendi il CloudFormation completamento dell'operazione di aggiornamento dello stack. Al termine dell'operazione di aggiornamento dello stack, aggiornare il modello in modo che corrisponda allo stato effettivo di deviazione delle risorse. Ad esempio, `BillingMode` verrà impostato su `PAY_PER_REQUEST` e `ReadCapacityUnits` e `WriteCapacityUnits` saranno impostati su `0`.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
```

```

        {
            "AttributeName": "key",
            "KeyType": "HASH"
        }
    ],
    "BillingMode": "PROVISIONED",
    "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
    }
}
},
"GamesTable": {
    "Type": "AWS::DynamoDB::Table",
    "DeletionPolicy": "Retain",
    "Properties": {
        "TableName": "Games",
        "AttributeDefinitions": [
            {
                "AttributeName": "key",
                "AttributeType": "S"
            }
        ],
        "KeySchema": [
            {
                "AttributeName": "key",
                "KeyType": "HASH"
            }
        ],
        "BillingMode": "PAY_PER_REQUEST",
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 0,
            "WriteCapacityUnits": 0
        }
    }
}
}
}
}
}

```

Example YAML

```

AWSTemplateFormatVersion: 2010-09-09
Description: Import test

```

```
Resources:
  ServiceTable:
    Type: 'AWS::DynamoDB::Table'
    Properties:
      TableName: Service
      AttributeDefinitions:
        - AttributeName: key
          AttributeType: S
      KeySchema:
        - AttributeName: key
          KeyType: HASH
      BillingMode: PROVISIONED
      ProvisionedThroughput:
        ReadCapacityUnits: 5
        WriteCapacityUnits: 1
  GamesTable:
    Type: 'AWS::DynamoDB::Table'
    DeletionPolicy: Retain
    Properties:
      TableName: Games
      AttributeDefinitions:
        - AttributeName: key
          AttributeType: S
      KeySchema:
        - AttributeName: key
          KeyType: HASH
      BillingMode: PAY_PER_REQUEST
      ProvisionedThroughput:
        ReadCapacityUnits: 0
        WriteCapacityUnits: 0
```

Importazione di AWS risorse in una CloudFormation pila

Puoi importare risorse esistenti in uno stack. CloudFormation. Ciò è utile se si desidera iniziare a utilizzare CloudFormation per gestire risorse create all'esterno di CloudFormation, senza doverle eliminare e ricreare.

CloudFormation offre le seguenti opzioni per importare risorse esistenti in uno stack:

- [laC generator](#) è uno strumento che analizza automaticamente le risorse esistenti e genera un CloudFormation modello basato sul loro stato attuale. Questo modello può quindi essere utilizzato per importare tali risorse in uno stack.
- L'[importazione delle risorse](#) è un processo manuale in cui si descrivono le risorse esistenti nel CloudFormation modello e quindi le si importa in uno stack. Questo approccio richiede di specificare manualmente le proprietà e le configurazioni delle risorse nel modello.
- L'[importazione automatica](#) è un processo automatico in cui si descrivono le risorse esistenti nel CloudFormation modello e si CloudFormation importano quelle con nomi personalizzati corrispondenti in una pila.
- Il [refactoring dello stack](#) è una funzionalità che semplifica la riorganizzazione delle risorse negli CloudFormation stack preservando al contempo le proprietà e i dati delle risorse esistenti. Con il refactoring degli stack, puoi spostare le risorse tra gli stack, dividere gli stack monolitici in componenti più piccoli o consolidare più stack in uno solo.

Oltre a CloudFormation gestire le risorse esistenti, la funzionalità di importazione delle risorse può essere utile nei seguenti scenari:

- Spostamento delle risorse tra gli stack: è possibile importare risorse da uno stack all'altro, in modo da riorganizzare l'infrastruttura in base alle esigenze.
- Annidamento degli stack esistenti: è possibile importare uno stack esistente come stack annidato all'interno di un altro stack, abilitando progetti di infrastruttura modulari e riutilizzabili.

CloudFormation supporta l'importazione di un'ampia gamma di risorse. Per ulteriori informazioni, consulta [Supporto per tipi di risorse](#).

Argomenti

- [Importazione AWS manuale delle risorse in uno CloudFormation stack](#)
- [Importa AWS automaticamente le risorse in uno CloudFormation stack](#)
- [Ripristino di un'operazione di importazione](#)

Importazione AWS manuale delle risorse in uno CloudFormation stack

Con l'importazione delle risorse, puoi importare AWS le risorse esistenti in uno stack nuovo o esistente. CloudFormation Durante un'operazione di importazione, si crea un set di modifiche

che importa le risorse esistenti in uno stack o crea un nuovo stack dalle risorse esistenti. Durante l'importazione è possibile fornire quanto segue.

- Un modello che descrive l'intero stack, incluse le risorse dello stack originali e quelle in fase di importazione. Ogni risorsa da importare deve avere un [DeletionPolicy](#) attributo.
- Identificatori per le risorse che stai importando che CloudFormation possono essere utilizzati per mappare la logica IDs del modello con le risorse esistenti.

Note

CloudFormation supporta solo un livello di nidificazione utilizzando l'importazione di risorse. Ciò significa che non è possibile importare uno stack in uno stack figlio o importare uno stack con figli.

Argomenti

- [Identificatori di risorse](#)
- [Convalida dell'importazione delle risorse](#)
- [Codici di stato dell'importazione delle risorse](#)
- [Considerazioni durante un'operazione di importazione](#)
- [Risorse aggiuntive](#)
- [Creazione di uno stack da risorse esistenti](#)
- [Importazione di risorse esistenti in uno stack](#)
- [Spostamento di risorse tra stack](#)
- [Nidificazione di uno stack esistente](#)

Identificatori di risorse

Fornisci due valori per identificare ogni risorsa che stai importando.

- Una proprietà identificatore. Si tratta di una proprietà di risorsa che può essere utilizzata per identificare ogni tipo di risorsa. Ad esempio, una risorsa AWS::S3::Bucket può essere identificata utilizzando il suo BucketName.

La proprietà della risorsa utilizzata per identificare la risorsa che stai importando varia a seconda del tipo di risorsa. Puoi trovare la proprietà della risorsa nella CloudFormation console. Dopo aver creato un modello che include la risorsa da importare, puoi avviare il processo di importazione, in cui troverai le proprietà degli identificatori per le risorse che stai importando. Per alcuni tipi di risorse, potrebbero esserci diversi modi per identificarli ed è possibile selezionare la proprietà da utilizzare negli elenchi a discesa.

In alternativa, puoi ottenere le proprietà dell'identificatore per le risorse che stai importando chiamando il comando [get-template-summary](#) CLI e specificando l'URL S3 del modello di stack come valore per l'opzione. `--template-url`

- Un valore identificativo. Questo è il valore effettivo della proprietà della risorsa. Ad esempio, il valore effettivo per la proprietà `BucketName` potrebbe essere `MyS3Bucket`.

È possibile ottenere il valore della proprietà identificatore dalla console di servizio per la risorsa.

Convalida dell'importazione delle risorse

Durante un'operazione di importazione, CloudFormation esegue le seguenti convalide.

- La risorsa da importare esiste.
- Le proprietà e i valori di configurazione per ogni risorsa da importare aderiscono allo schema del tipo di risorsa, che definisce le proprietà accettate, le proprietà richieste e i valori delle proprietà supportate.
- Le proprietà richieste sono specificate nel modello. Le proprietà obbligatorie per ogni tipo di risorsa sono descritte nel [riferimento ai tipi di AWS risorse e proprietà](#).
- La risorsa da importare non appartiene a un altro stack nella stessa Regione.

CloudFormation non verifica che la configurazione del modello corrisponda alla configurazione effettiva delle proprietà delle risorse.

Important

Verifica che le risorse e le rispettive proprietà definite nel modello corrispondano alla configurazione prevista per l'importazione delle risorse per evitare modifiche impreviste.

Codici di stato dell'importazione delle risorse

Questa tabella descrive i vari tipi di stato utilizzati con la funzionalità di importazione delle risorse.

Stato dell'operazione di importazione	Descrizione
IMPORT_IN_PROGRESS	L'operazione di importazione è in corso.
IMPORT_COMPLETE	L'operazione di importazione è stata completata per tutte le risorse nello stack.
IMPORT_ROLLBACK_IN_PROGRESS	L'operazione di importazione di rollback sta eseguendo il rollback della configurazione del modello precedente.
IMPORT_ROLLBACK_FAILED	L'operazione di rollback dell'importazione ha avuto esito negativo.
IMPORT_ROLLBACK_COMPLETE	È stato eseguito il rollback dell'importazione alla configurazione del modello precedente.

Considerazioni durante un'operazione di importazione

- Al termine dell'importazione e prima di eseguire operazioni di stack successive, si consiglia di eseguire il rilevamento della deviazione sulle risorse importate. Il rilevamento della deviazione garantisce che la configurazione del modello corrisponda alla configurazione effettiva. Per ulteriori informazioni, consulta [Rileva la deriva su un'intera CloudFormation pila](#).
- Le operazioni di importazione non consentono nuove creazioni di risorse, eliminazioni di risorse o modifiche alle configurazioni di proprietà.
- Ogni risorsa da importare deve avere un attributo `DeletionPolicy` affinché l'operazione di importazione abbia esito positivo. È possibile impostare `DeletionPolicy` su qualsiasi valore possibile. Solo le risorse che stai importando richiedono un `DeletionPolicy`. Le risorse che fanno già parte dello stack non richiedono un `DeletionPolicy`.
- Non è possibile importare la stessa risorsa in più stack.
- È possibile utilizzare la condizione della policy IAM `cloudformation:ImportResourceTypes` per controllare i tipi di risorse con cui gli utenti possono lavorare durante un'operazione di

importazione. Per ulteriori informazioni, consulta [Chiavi relative alle condizioni politiche per CloudFormation](#).

- I limiti CloudFormation dello stack si applicano all'importazione di risorse. Per ulteriori informazioni sui limiti, vedere. [Comprendi le CloudFormation quote](#)

Risorse aggiuntive

Per risolvere la deriva dello stack con l'importazione di risorse, vedere. [Risoluzione della deviazione con un'operazione di importazione](#)

Creazione di uno stack da risorse esistenti

In questo argomento viene illustrato come creare uno stack a partire da AWS risorse esistenti descrivendole in un modello. Per cercare invece le risorse esistenti e generare automaticamente un modello da utilizzare per importare risorse esistenti CloudFormation o replicare le risorse in un nuovo account, consulta. [Genera modelli da risorse esistenti con il generatore IaC](#)

Prerequisiti

Prima di iniziare, devi disporre di quanto segue:

- Un modello che descrive tutte le risorse che desideri inserire nel nuovo stack. Salva il modello localmente o in un bucket Amazon S3.
- Per ogni risorsa che desideri importare, includi quanto segue:
 - le proprietà e i valori delle proprietà che definiscono la configurazione corrente della risorsa.
 - l'identificatore univoco della risorsa, ad esempio il nome della risorsa. Per ulteriori informazioni, consulta [Identificatori di risorse](#).
 - l'[DeletionPolicy](#) attributo.

Argomenti

- [Modello di esempio](#)
- [Crea uno stack a partire dalle risorse esistenti utilizzando il AWS Management Console](#)
- [Creazione di uno stack da risorse esistenti utilizzando l' AWS CLI](#)

Modello di esempio

In questa procedura dettagliata, supponiamo che tu stia utilizzando il seguente modello di esempio, chiamato `TemplateToImport.json`, che specifica due tabelle DynamoDB che sono state create all'esterno di. CloudFormation `ServiceTable` e `GamesTable` sono gli obiettivi dell'importazione.

Note

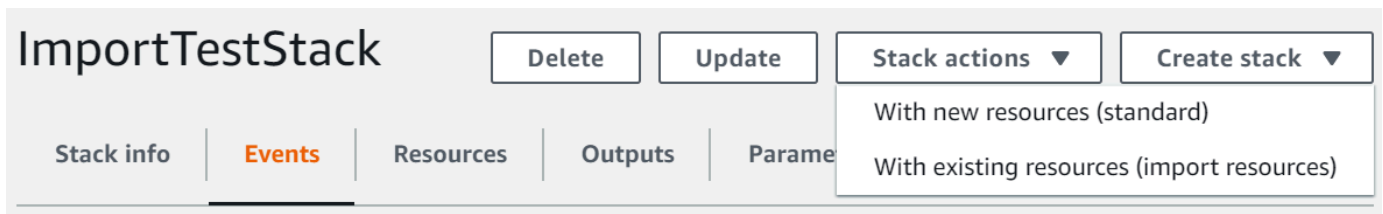
Questo modello è inteso solo come esempio. Per utilizzarlo per scopi di test, sostituisci le risorse di esempio con le risorse del tuo account.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "DeletionPolicy": "Retain",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    },
    "GamesTable": {
      "Type": "AWS::DynamoDB::Table",
      "DeletionPolicy": "Retain",
```

```
"Properties": {
  "TableName": "Games",
  "AttributeDefinitions": [
    {
      "AttributeName": "key",
      "AttributeType": "S"
    }
  ],
  "KeySchema": [
    {
      "AttributeName": "key",
      "KeyType": "HASH"
    }
  ],
  "ProvisionedThroughput": {
    "ReadCapacityUnits": 5,
    "WriteCapacityUnits": 1
  }
}
```

Crea uno stack a partire dalle risorse esistenti utilizzando il AWS Management Console

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella pagina Stacks (Stack), scegliere Create stack (Crea stack), quindi scegliere With existing resources (import resources) (Con risorse esistenti (risorse di importazione)).



3. Leggere la pagina Import overview (Panoramica importazione) per un elenco di elementi da fornire durante questa operazione. Quindi, seleziona Next (Successivo).
4. Nella pagina Specify model (Specifica modello), fornire il modello utilizzando uno dei metodi descritti di seguito, quindi scegliere Next (Successivo).

- Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il modello.
5. Nella pagina Identify resources (Identifica risorse), identifica ogni risorsa di destinazione. Per ulteriori informazioni, consulta [Identificatori di risorse](#).
- a. In Identifier property (Proprietà identificatore), scegliere il tipo di identificatore di risorsa. Ad esempio, la risorsa AWS::DynamoDB::Table può essere identificata utilizzando la proprietà TableName.
 - b. In Identifier value (Valore identificatore), digitare il valore effettivo della proprietà. Ad esempio, il TableName per la risorsa GamesTable nel modello di esempio è *Games*.
 - c. Scegli Next (Successivo).
6. Nella pagina Specify stack details (Specifica dettagli stack), modificare i parametri, quindi scegliere Next (Successivo). Questo crea automaticamente un set di modifiche.

 Important

L'operazione di importazione ha esito negativo se si modificano i parametri esistenti che iniziano un'operazione di creazione, aggiornamento o eliminazione.

7. Nella *stack-name* pagina Revisione, conferma che vengano importate le risorse corrette, quindi scegli Importa risorse. In questo modo si esegue automaticamente il set di modifiche creato nell'ultimo passaggio.

Per il nuovo stack viene visualizzato il riquadro Events (Eventi) della pagina Stack details (Dettagli stack).

ImportTestStack

Delete

Update

Stack actions

Create stack

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Events

Q Search events

Timestamp	Logical ID	Status	Status reason
2019-10-24 15:52:49 UTC-0700	ImportTestStack	IMPORT_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_IN_PROGRESS	Apply stack-level tags to imported resource if applicable.
2019-10-24 15:52:46 UTC-0700	SampleIamUser	IMPORT_COMPLETE	Resource import completed.
2019-10-24 15:52:45 UTC-0700	SampleIamUser	IMPORT_IN_PROGRESS	Resource import started.
2019-10-24 15:52:43 UTC-0700	ImportTestStack	IMPORT_IN_PROGRESS	User Initiated
2019-10-24 15:52:01 UTC-0700	ImportTestStack	REVIEW_IN_PROGRESS	User Initiated

8. (Facoltativo) Eseguire il rilevamento della deviazione nello stack per assicurarsi che il modello e la configurazione effettiva delle risorse importate corrispondano. Per ulteriori informazioni sul rilevamento della deriva, vedere [Rileva la deriva su un'intera CloudFormation pila](#)
9. (Facoltativo) Se le risorse importate non corrispondono alle configurazioni dei modelli previste, correggi le configurazioni dei modelli o aggiorna direttamente le risorse. In questa spiegazione passo per passo, vengono corrette le configurazioni dei modelli in modo che corrispondano alle configurazioni effettive.
 - a. [Ripristinare l'operazione di importazione](#) per le risorse interessate.
 - b. Aggiungere nuovamente le destinazioni di importazione al modello, assicurandosi che le configurazioni del modello corrispondano alle configurazioni effettive.
 - c. Ripeti i passaggi 2-8 utilizzando il modello modificato per importare nuovamente le risorse.

Creazione di uno stack da risorse esistenti utilizzando l' AWS CLI

1. Per scoprire quali proprietà identificano ogni tipo di risorsa nel modello, esegui il `get-template-summary` comando, specificando l'URL S3 del modello. Ad esempio, la risorsa `AWS::DynamoDB::Table` può essere identificata utilizzando la proprietà `TableName`. Per la risorsa `GameTable` nel modello di esempio, il valore di `TableName` è `Games`. Avrai bisogno di queste informazioni nel passaggio successivo.

```
aws cloudformation get-template-summary \
  --template-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/
  TemplateToImport.json
```


Per ulteriori informazioni, consulta [Identificatori di risorse](#).

2. Componi un elenco delle risorse effettive del tuo modello e dei relativi identificatori univoci nel seguente formato di stringa JSON.

```
[{"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"GamesTable","ResourceIdentifier":{"TableName":"Games"}}, {"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"ServiceTable","ResourceIdentifier":{"TableName":"Service"}}]
```

In alternativa, puoi specificare i parametri formattati JSON in un file di configurazione.

Ad esempio, per importare ServiceTable e GamesTable, è possibile creare un *ResourcesToImport.txt* file che contenga la seguente configurazione.

```
[
  {
    "ResourceType":"AWS::DynamoDB::Table",
    "LogicalResourceId":"GamesTable",
    "ResourceIdentifier":{"
      "TableName":"Games"
    }
  },
  {
    "ResourceType":"AWS::DynamoDB::Table",
    "LogicalResourceId":"ServiceTable",
    "ResourceIdentifier":{"
      "TableName":"Service"
    }
  }
]
```

3. Per creare un set di modifiche, utilizzate il create-change-set comando seguente e sostituite il testo segnaposto. Per l'opzione `--change-set-type`, specifica il valore di **IMPORT**. Per l'opzione `--resources-to-import`, sostituite la stringa JSON di esempio con la stringa JSON effettiva che avete appena creato.

```
aws cloudformation create-change-set \
  --stack-name TargetStack --change-set-name ImportChangeSet \
  --change-set-type IMPORT \
```

```
--template-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/  
TemplateToImport.json \  
--resources-to-  
import '["ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"GamesTable","ResourceIdentifi  
{"TableName":"Games"}},  
{"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"ServiceTable","ResourceIdentifi  
{"TableName":"Service"}}]'
```

Note

`--resources-to-import` non supporta YAML in linea. I requisiti per l'escape tra virgolette nella stringa JSON variano a seconda del terminale. Per ulteriori informazioni, consulta [Uso delle virgolette all'interno delle stringhe](#) nella Guida per l'utente AWS Command Line Interface.

In alternativa, è possibile utilizzare l'URL di un file come input per l'`--resources-to-import` opzione, come illustrato nell'esempio seguente.

```
--resources-to-import file:///ResourcesToImport.txt
```

4. Esaminare il set di modifiche per assicurarsi che vengano importate le risorse corrette.

```
aws cloudformation describe-change-set \  
--change-set-name ImportChangeSet --stack-name TargetStack
```

5. Per avviare il set di modifiche e importare le risorse, utilizzate il `execute-change-set` comando seguente e sostituite il testo segnaposto. Al completamento dell'operazione (`IMPORT_COMPLETE`), le risorse vengono importate correttamente.

```
aws cloudformation execute-change-set \  
--change-set-name ImportChangeSet --stack-name TargetStack
```

6. (Facoltativo) Eseguire il rilevamento della deviazione sullo stack `IMPORT_COMPLETE` per assicurarsi che il modello e la configurazione effettiva delle risorse importate corrispondano. Per ulteriori informazioni sul rilevamento della deriva, vedere [Rilevamento della deviazione su singole risorse di stack](#)
 - a. Eseguire il rilevamento della deriva sullo stack specificato.

```
aws cloudformation detect-stack-drift --stack-name TargetStack
```

In caso di successo, questo comando restituisce il seguente output di esempio.

```
{ "Stack-Drift-Detection-Id" : "624af370-311a-11e8-b6b7-500cexample" }
```

- b. Visualizza lo stato di avanzamento di un'operazione di rilevamento della deriva per l'ID di rilevamento della deriva dello stack specificato.

```
aws cloudformation describe-stack-drift-detection-status \  
--stack-drift-detection-id 624af370-311a-11e8-b6b7-500cexample
```

- c. Visualizza le informazioni sulla deriva per le risorse per le quali è stata verificata la deriva nello stack specificato.

```
aws cloudformation describe-stack-resource-drifts --stack-name TargetStack
```

7. (Facoltativo) Se le risorse importate non corrispondono alle configurazioni dei modelli previste, correggi le configurazioni dei modelli o aggiorna direttamente le risorse. In questa spiegazione passo per passo, vengono corrette le configurazioni dei modelli in modo che corrispondano alle configurazioni effettive.
 - a. [Ripristinare l'operazione di importazione](#) per le risorse interessate.
 - b. Aggiungere nuovamente le destinazioni di importazione al modello, assicurandosi che le configurazioni del modello corrispondano alle configurazioni effettive.
 - c. Ripeti i passaggi da 3 a 6 utilizzando il modello modificato per importare nuovamente le risorse.

Importazione di risorse esistenti in uno stack

Questo argomento mostra come importare AWS risorse esistenti in uno stack esistente descrivendole in un modello. Per cercare invece le risorse esistenti e generare automaticamente un modello da utilizzare per importare risorse esistenti CloudFormation o replicare le risorse in un nuovo account, consulta. [Genera modelli da risorse esistenti con il generatore IaC](#)

Prerequisiti

Prima di iniziare, devi disporre di quanto segue:

- Un modello che descrive l'intero stack, incluse le risorse che fanno già parte dello stack e le risorse da importare. Salva il modello localmente o in un bucket Amazon S3.

Per ottenere una copia del modello di uno stack in esecuzione

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation/>.
 2. Dall'elenco degli stack, scegli lo stack da cui vuoi recuperare il modello.
 3. Nel riquadro dei dettagli dello stack, scegli la scheda Modello, quindi scegli Copia negli appunti.
 4. Incolla il codice in un editor di testo per iniziare ad aggiungere altre risorse al modello.
- Per ogni risorsa che desideri importare, includi quanto segue:
 - le proprietà e i valori delle proprietà che definiscono la configurazione corrente della risorsa.
 - l'identificatore univoco della risorsa, ad esempio il nome della risorsa. Per ulteriori informazioni, consulta [Identificatori di risorse](#).
 - l'[DeletionPolicy](#) attributo.

Argomenti

- [Modello di esempio](#)
- [Importa una risorsa esistente in uno stack utilizzando il AWS Management Console](#)
- [Importa una risorsa esistente in uno stack utilizzando il AWS CLI](#)

Modello di esempio

In questa procedura dettagliata, supponiamo che tu stia utilizzando il seguente modello di esempio, chiamato `TemplateToImport.json`, che specifica due tabelle DynamoDB. `ServiceTable` è attualmente parte dello stack ed `GameTable` è la tabella che desideri importare.

Note

Questo modello è inteso solo come esempio. Per utilizzarlo per scopi di test, sostituisci le risorse di esempio con le risorse del tuo account.

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Description": "Import test",
```

```
"Resources": {
  "ServiceTable": {
    "Type": "AWS::DynamoDB::Table",
    "Properties": {
      "TableName": "Service",
      "AttributeDefinitions": [
        {
          "AttributeName": "key",
          "AttributeType": "S"
        }
      ],
      "KeySchema": [
        {
          "AttributeName": "key",
          "KeyType": "HASH"
        }
      ],
      "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
      }
    }
  },
  "GamesTable": {
    "Type": "AWS::DynamoDB::Table",
    "DeletionPolicy": "Retain",
    "Properties": {
      "TableName": "Games",
      "AttributeDefinitions": [
        {
          "AttributeName": "key",
          "AttributeType": "S"
        }
      ],
      "KeySchema": [
        {
          "AttributeName": "key",
          "KeyType": "HASH"
        }
      ],
      "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
      }
    }
  }
}
```

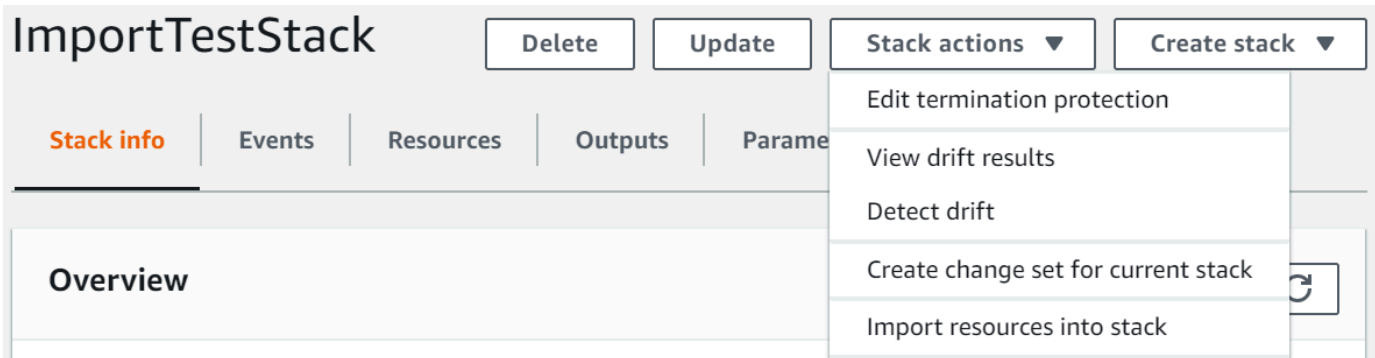
```
}  
  }  
}  
}
```

Importa una risorsa esistente in uno stack utilizzando il AWS Management Console

Note

La CloudFormation console non supporta l'uso della funzione intrinseca `Fn::Transform` durante l'importazione di risorse. È possibile utilizzare il AWS CLI per importare risorse che utilizzano la funzione. `Fn::Transform`

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella pagina Stacks (Stack), scegliere lo stack in cui importare le risorse.
3. Scegliere Stack actions (Operazioni stack), quindi scegliere Import resources into stack (Importa risorse nello stack).



4. Rivedere la pagina Import overview (Panoramica importazione), quindi scegliere Next (Successivo).
5. Nella pagina Specify model (Specifica modello), fornire il modello aggiornato utilizzando uno dei metodi descritti di seguito, quindi scegliere Next (Successivo).
 - Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il modello.
6. Nella pagina Identify resources (Identifica risorse), identifica ogni risorsa di destinazione. Per ulteriori informazioni, consulta [Identificatori di risorse](#).

- a. In Identifier property (Proprietà identificatore), scegliere il tipo di identificatore di risorsa. Ad esempio, la risorsa `AWS::DynamoDB::Table` può essere identificata utilizzando la proprietà `TableName`.
 - b. In Identifier value (Valore identificatore), digitare il valore effettivo della proprietà. Ad esempio, il `TableName` per la risorsa `GameTable` nel modello di esempio è *Games*.
 - c. Scegli Next (Successivo).
7. Nella pagina Specify stack details (Specifica dettagli stack), aggiornare i parametri, quindi scegliere Next (Successivo). Questo crea automaticamente un set di modifiche.

Note

L'operazione di importazione ha esito negativo se si modificano i parametri esistenti che iniziano un'operazione di creazione, aggiornamento o eliminazione.

8. Nella *stack-name* pagina Revisione, esamina le risorse da importare, quindi scegli Importa risorse. In questo modo si esegue automaticamente il set di modifiche creato nell'ultimo passaggio. Tutti i tag a livello di stack vengono applicati alle risorse importate in questo momento. Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#).

Viene visualizzata la pagina Events (Eventi) per lo stack.

ImportTestStack

Delete

Update

Stack actions

Create stack

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Events

Q Search events

Timestamp	Logical ID	Status	Status reason
2019-10-24 15:52:49 UTC-0700	ImportTestStack	IMPORT_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_IN_PROGRESS	Apply stack-level tags to imported resource if applicable.
2019-10-24 15:52:46 UTC-0700	SampleIamUser	IMPORT_COMPLETE	Resource import completed.
2019-10-24 15:52:45 UTC-0700	SampleIamUser	IMPORT_IN_PROGRESS	Resource import started.
2019-10-24 15:52:43 UTC-0700	ImportTestStack	IMPORT_IN_PROGRESS	User Initiated
2019-10-24 15:52:01 UTC-0700	ImportTestStack	REVIEW_IN_PROGRESS	User Initiated

9. (Facoltativo) Eseguire il rilevamento della deviazione nello stack per assicurarsi che il modello e la configurazione effettiva delle risorse importate corrispondano. Per ulteriori informazioni sul rilevamento della deriva, consulta [Rileva la deriva su un'intera CloudFormation pila](#)

10. (Facoltativo) Se le risorse importate non corrispondono alle configurazioni dei modelli previste, correggi le configurazioni dei modelli o aggiorna direttamente le risorse. Per ulteriori informazioni sull'importazione di risorse che derivano dalla deriva, vedere. [Risoluzione della deviazione con un'operazione di importazione](#)

Importa una risorsa esistente in uno stack utilizzando il AWS CLI

1. Per scoprire quali proprietà identificano ogni tipo di risorsa nel modello, esegui il `get-template-summary` comando, specificando l'URL S3 del modello. Ad esempio, la risorsa `AWS::DynamoDB::Table` può essere identificata utilizzando la proprietà `TableName`. Per la risorsa `GamesTable` nel modello di esempio, il valore di `TableName` è `Games`. Avrai bisogno di queste informazioni nel passaggio successivo.

```
aws cloudformation get-template-summary \
  --template-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/
  TemplateToImport.json
```

Per ulteriori informazioni, consulta [Identificatori di risorse](#).

2. Componi un elenco di risorse effettive da importare e i relativi identificatori univoci nel seguente formato di stringa JSON.

```
[{"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"GamesTable","ResourceIdentifier":
{"TableName":"Games"}]}
```

In alternativa, puoi specificare i parametri formattati JSON in un file di configurazione.

Ad esempio, per importare `GamesTable`, è possibile creare un *ResourcesToImport.txt* file che contenga la seguente configurazione.

```
[
  {
    "ResourceType":"AWS::DynamoDB::Table",
    "LogicalResourceId":"GamesTable",
    "ResourceIdentifier": {
      "TableName":"Games"
    }
  }
]
```


3. Per creare un set di modifiche, utilizzate il `create-change-set` comando seguente e sostituite il testo segnaposto. Per l'opzione `--change-set-type`, specifica il valore di **IMPORT**. Per l'opzione `--resources-to-import`, sostituite la stringa JSON di esempio con la stringa JSON effettiva che avete appena creato.

```
aws cloudformation create-change-set \  
  --stack-name TargetStack --change-set-name ImportChangeSet \  
  --change-set-type IMPORT \  
  --template-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/  
TemplateToImport.json \  
  --resources-to-  
import '["ResourceType":"AWS::DynamoDB::Table", "LogicalResourceId":"GamesTable", "ResourceI  
{"TableName":"Games"}"]'
```

Note

`--resources-to-import` non supporta YAML in linea. I requisiti per l'escape tra virgolette nella stringa JSON variano a seconda del terminale. Per ulteriori informazioni, consulta [Uso delle virgolette all'interno delle stringhe](#) nella Guida per l'utente AWS Command Line Interface.

In alternativa, è possibile utilizzare l'URL di un file come input per l'opzione `--resources-to-import`, come illustrato nell'esempio seguente.

```
--resources-to-import file:///ResourcesToImport.txt
```

4. Esaminare il set di modifiche per assicurarsi che vengano importate le risorse corrette.

```
aws cloudformation describe-change-set \  
  --change-set-name ImportChangeSet --stack-name TargetStack
```

5. Per avviare il set di modifiche e importare le risorse, utilizzate il `execute-change-set` comando seguente e sostituite il testo segnaposto. Tutti i tag a livello di stack vengono applicati alle risorse importate in questo momento. Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#). Al completamento dell'operazione (`IMPORT_COMPLETE`), le risorse vengono importate correttamente.

```
aws cloudformation execute-change-set \  
  --change-set-name ImportChangeSet --stack-name TargetStack
```

```
--change-set-name ImportChangeSet --stack-name TargetStack
```

6. (Facoltativo) Eseguire il rilevamento della deviazione sullo stack `IMPORT_COMPLETE` per assicurarsi che il modello e la configurazione effettiva delle risorse importate corrispondano. Per ulteriori informazioni sul rilevamento della deriva, vedere. [Rileva la deriva su un'intera CloudFormation pila](#)

- a. Eseguire il rilevamento della deriva sullo stack specificato.

```
aws cloudformation detect-stack-drift --stack-name TargetStack
```

In caso di successo, questo comando restituisce il seguente output di esempio.

```
{ "Stack-Drift-Detection-Id" : "624af370-311a-11e8-b6b7-500cexample" }
```

- b. Visualizza lo stato di avanzamento di un'operazione di rilevamento della deriva per l'ID di rilevamento della deriva dello stack specificato.

```
aws cloudformation describe-stack-drift-detection-status \  
  --stack-drift-detection-id 624af370-311a-11e8-b6b7-500cexample
```

- c. Visualizza le informazioni sulla deriva per le risorse per le quali è stata verificata la deriva nello stack specificato.

```
aws cloudformation describe-stack-resource-drifts --stack-name TargetStack
```

7. (Facoltativo) Se le risorse importate non corrispondono alle configurazioni dei modelli previste, correggi le configurazioni dei modelli o aggiorna direttamente le risorse. Per ulteriori informazioni sull'importazione di risorse alla deriva, vedere. [Risoluzione della deviazione con un'operazione di importazione](#)

Spostamento di risorse tra stack

Utilizzando la funzionalità `resource import`, è possibile spostare le risorse tra stack o eseguirne il refactoring. Prima di tutto è necessario aggiungere una policy di eliminazione `Retain` alla risorsa da spostare per fare in modo che la risorsa venga mantenuta quando viene rimossa dallo stack di origine e importata nello stack di destinazione.

Se non conosci l'importazione, ti consigliamo di rivedere prima le informazioni introduttive nell'argomento. [Importazione di AWS risorse in una CloudFormation pila](#)

 Important

Non tutte le risorse supportano le operazioni di importazione. Consulta [Risorse che supportano le operazioni di importazione](#) prima di rimuovere una risorsa dallo stack. Se rimuovi una risorsa che non supporta le operazioni di importazione dallo stack, non potrai importarla in un altro stack o riportarla nello stack di origine.

Effettua il refactoring di uno stack utilizzando il AWS Management Console

1. Nel modello di origine, specificate a Retain [DeletionPolicy](#) per la risorsa che desiderate spostare.

Nel seguente modello di origine di esempio, Games è la destinazione di questo refactoring.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
```

```
        "WriteCapacityUnits": 1
      }
    },
    "GamesTable": {
      "Type": "AWS::DynamoDB::Table",
      "DeletionPolicy": "Retain",
      "Properties": {
        "TableName": "Games",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    }
  }
}
```

2. Apri la CloudFormation console per eseguire un aggiornamento dello stack per applicare la politica di eliminazione.
 - a. Nella pagina Stacks (Stack) con lo stack selezionato, scegliere Update (Aggiorna).
 - b. In Prepare template (Prepara modello), scegliere Replace current template (Sostituisci modello corrente).
 - c. In Specify template (Specifica modello), fornire il modello di origine aggiornato con l'attributo DeletionPolicy su GamesTable, quindi scegliere Next (Successivo).
 - Scegliere Amazon URL S3 (URL Amazon S3), quindi specificare l'URL per il modello di origine aggiornato nella casella di testo.

- Scegliere Upload a template file (Carica un file modello), quindi cercare il file modello di origine aggiornato.
 - d. Nella pagina Specify stack details (Specifica dettagli stack), non sono necessarie modifiche. Scegli Next (Successivo).
 - e. Nella pagina Configure stack options (Configura opzioni stack) non sono necessarie modifiche. Scegli Next (Successivo).
 - f. Nella **SourceStackName** pagina Revisione, rivedi le modifiche. Se il modello contiene risorse IAM, selezionare **I acknowledge that this template may create IAM resources** (Acconsento che questo modello possa creare risorse IAM) per specificare che si desidera utilizzare risorse IAM nel modello. Per ulteriori informazioni sull'utilizzo delle risorse IAM nei modelli, consulta [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#). Quindi, aggiornare lo stack di origine creando un set di modifiche o aggiornare direttamente lo stack di origine.
3. Rimuovi la risorsa , i parametri correlati e gli output dal modello di origine, quindi aggiungili al modello di destinazione.

Il modello di origine ora è simile al seguente.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ]
      }
    }
  }
}
```

```

    ],
    "ProvisionedThroughput": {
      "ReadCapacityUnits": 5,
      "WriteCapacityUnits": 1
    }
  }
}
}
}
}

```

Il seguente modello di destinazione di esempio ha attualmente la risorsa `PlayersTable` e ora contiene anche `GamesTable`.

Example JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "PlayersTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Players",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    },
    "GamesTable": {
      "Type": "AWS::DynamoDB::Table",

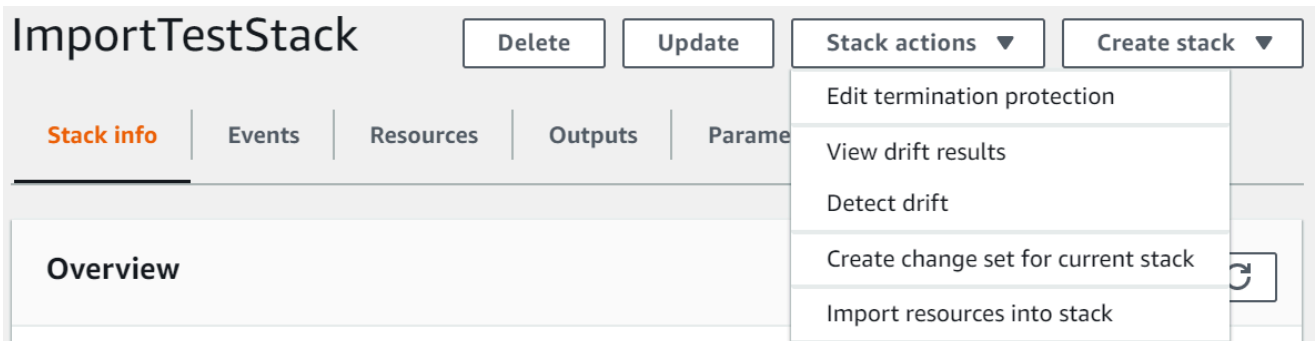
```

```

        "DeletionPolicy": "Retain",
        "Properties": {
            "TableName": "Games",
            "AttributeDefinitions": [
                {
                    "AttributeName": "key",
                    "AttributeType": "S"
                }
            ],
            "KeySchema": [
                {
                    "AttributeName": "key",
                    "KeyType": "HASH"
                }
            ],
            "ProvisionedThroughput": {
                "ReadCapacityUnits": 5,
                "WriteCapacityUnits": 1
            }
        }
    }
}

```

4. Ripeti i passaggi 2-3 per aggiornare nuovamente lo stack di origine, questa volta per eliminare la risorsa di destinazione dallo stack.
5. Eseguire un'operazione di importazione per aggiungere GamesTable allo stack di destinazione.
 - a. Nella pagina Stacks (Stack) con lo stack padre selezionato, scegliere Stack actions (Operazioni stack), quindi scegliere Import resources into stack (Importa risorse nello stack).



- b. Leggere la pagina Import overview (Panoramica importazione) per un elenco di elementi da fornire durante questa operazione. Quindi, seleziona Next (Successivo).

- c. Nella pagina Specify template (Specifica modello) completa una delle seguenti operazioni, quindi scegli Next (Avanti).
 - Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare un URL nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare un file da caricare.
 - d. Nella pagina Identify resources (Identifica risorse), identificare la risorsa che si sta spostando (in questo esempio `GameTable`). Per ulteriori informazioni, consulta [Identificatori di risorse](#).
 1. In Identifier property (Proprietà identificatore), scegliere il tipo di identificatore di risorsa. Ad esempio, una risorsa `AWS::DynamoDB::Table` può essere identificata utilizzando la proprietà `TableName`.
 2. In Identifier value (Valore identificatore), digitare il valore effettivo della proprietà. Ad esempio, *GameTables*.
 3. Scegli Next (Successivo).
 - e. Nella pagina Specify stack details (Specifica dettagli stack), modificare i parametri, quindi scegliere Next (Successivo). Questo crea automaticamente un set di modifiche.
-
- Important
- L'operazione di importazione ha esito negativo se si modificano i parametri esistenti che iniziano un'operazione di creazione, aggiornamento o eliminazione.
- f. Nella *TargetStackName* pagina Revisione, conferma che sia stata importata la risorsa corretta, quindi scegli Importa risorse. In questo modo il set di modifiche creato nell'ultima fase viene avviato automaticamente. Tutti i [tag a livello di stack](#) vengono applicati alle risorse importate in questo momento.
 - g. Per lo stack padre viene visualizzato il riquadro Events (Eventi) della pagina Stack details (Dettagli stack).

ImportTestStack

Delete

Update

Stack actions

Create stack

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Events

Search events

Timestamp	Logical ID	Status	Status reason
2019-10-24 15:52:49 UTC-0700	ImportTestStack	IMPORT_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SampleIamUser	UPDATE_IN_PROGRESS	Apply stack-level tags to imported resource if applicable.
2019-10-24 15:52:46 UTC-0700	SampleIamUser	IMPORT_COMPLETE	Resource import completed.
2019-10-24 15:52:45 UTC-0700	SampleIamUser	IMPORT_IN_PROGRESS	Resource import started.
2019-10-24 15:52:43 UTC-0700	ImportTestStack	IMPORT_IN_PROGRESS	User Initiated
2019-10-24 15:52:01 UTC-0700	ImportTestStack	REVIEW_IN_PROGRESS	User Initiated

Note

Non è necessario eseguire il rilevamento della deviazione nello stack padre dopo questa operazione di importazione perché la risorsa `AWS::CloudFormation::Stack` è già gestita da CloudFormation.

Effettua il refactoring di uno stack utilizzando il AWS CLI

1. Nel modello di origine, specificate a Retain [DeletionPolicy](#) per la risorsa che desiderate spostare.

Nel seguente modello di origine di esempio, `GameTable` è la destinazione di questo refactoring.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
```

```

        "AttributeType": "S"
    },
    ],
    "KeySchema": [
        {
            "AttributeName": "key",
            "KeyType": "HASH"
        }
    ],
    "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
    }
}

},
"GamesTable": {
    "Type": "AWS::DynamoDB::Table",
    "DeletionPolicy": "Retain",
    "Properties": {
        "TableName": "Games",
        "AttributeDefinitions": [
            {
                "AttributeName": "key",
                "AttributeType": "S"
            }
        ],
        "KeySchema": [
            {
                "AttributeName": "key",
                "KeyType": "HASH"
            }
        ],
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 1
        }
    }
}

}

}

```

2. Aggiornare lo stack di origine per applicare la policy di eliminazione alla risorsa.

```
aws cloudformation update-stack --stack-name SourceStackName
```

3. Rimuovi la risorsa , i parametri correlati e gli output dal modello di origine, quindi aggiungili al modello di destinazione.

Il modello di origine ora è simile al seguente.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    }
  }
}
```

Il seguente modello di destinazione di esempio ha attualmente la risorsa `PlayersTable` e ora contiene anche `GamesTable`.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "PlayersTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Players",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
          "ReadCapacityUnits": 5,
          "WriteCapacityUnits": 1
        }
      }
    },
    "GamesTable": {
      "Type": "AWS::DynamoDB::Table",
      "DeletionPolicy": "Retain",
      "Properties": {
        "TableName": "Games",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ]
      }
    }
  }
}
```

```

        }
      ],
      "ProvisionedThroughput": {
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
      }
    }
  }
}

```

4. Aggiornare lo stack di origine per eliminare la risorsa `GamesTable` e i relativi parametri e output dallo stack.

```
aws cloudformation update-stack --stack-name SourceStackName
```

5. Componi un elenco di risorse effettive da importare e i relativi identificatori univoci nel seguente formato di stringa JSON. Per ulteriori informazioni, consulta [Identificatori di risorse](#).

```
[{"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"GamesTable","ResourceIdentifier":{
{"TableName":"Games"}}}]
```

In alternativa, puoi specificare i parametri formattati JSON in un file di configurazione.

Ad esempio, per importare `GamesTable`, è possibile creare un *ResourcesToImport.txt* file che contenga la seguente configurazione.

```
[
  {
    "ResourceType":"AWS::DynamoDB::Table",
    "LogicalResourceId":"GamesTable",
    "ResourceIdentifier": {
      "TableName":"Games"
    }
  }
]
```

6. Per creare un set di modifiche, utilizzate il `create-change-set` comando seguente e sostituite il testo segnaposto. Per l'opzione `--change-set-type`, specifica il valore di **IMPORT**. Per l'opzione `--resources-to-import`, sostituite la stringa JSON di esempio con la stringa JSON effettiva che avete appena creato.

```
aws cloudformation create-change-set \  
  --stack-name TargetStackName --change-set-name ImportChangeSet \  
  --change-set-type IMPORT \  
  --template-body file://TemplateToImport.json \  
  --resources-to-import  
  "'[{"ResourceType":"AWS::DynamoDB::Table","LogicalResourceId":"GamesTable","ResourceIdentifiers":{"TableName":"Games"}}]'"
```

Note

--resources-to-import non supporta YAML in linea. I requisiti per l'escape tra virgolette nella stringa JSON variano a seconda del terminale. Per ulteriori informazioni, consulta [Uso delle virgolette all'interno delle stringhe](#) nella Guida per l'utente AWS Command Line Interface.

In alternativa, è possibile utilizzare l'URL di un file come input per l'--resources-to-import opzione, come illustrato nell'esempio seguente.

```
--resources-to-import file://ResourcesToImport.txt
```

7. Esaminare il set di modifiche per assicurarsi che la risorsa corretta venga importata nello stack di destinazione.

```
aws cloudformation describe-change-set \  
  --change-set-name ImportChangeSet
```

8. Per avviare il set di modifiche e importare la risorsa, utilizzate il execute-change-set comando seguente e sostituite il testo segnaposto. Tutti i tag a livello di stack vengono applicati alle risorse importate in questo momento. Al completamento dell'operazione (IMPORT_COMPLETE), la risorsa viene importata correttamente.

```
aws cloudformation execute-change-set \  
  --change-set-name ImportChangeSet --stack-name TargetStackName
```

 Note

Non è necessario eseguire il rilevamento della deviazione nello stack di destinazione dopo questa operazione di importazione perché la risorsa è già gestita da CloudFormation.

Nidificazione di uno stack esistente

Utilizzare la funzione `resource import` per nidificare uno stack esistente all'interno di un altro stack esistente. Gli stack nidificati sono componenti comuni che l'utente dichiara e vi fa riferimento all'interno di altri modelli. In questo modo, è possibile evitare di copiare e incollare le stesse configurazioni nei modelli e semplificare gli aggiornamenti dello stack. Se si dispone di un modello per un componente comune, è possibile utilizzare la risorsa `AWS::CloudFormation::Stack` per fare riferimento a questo modello da un altro modello. Per ulteriori informazioni sugli stack nidificati, consulta [Dividi un modello in pezzi riutilizzabili usando pile annidate](#).

AWS CloudFormation supporta solo un livello di nidificazione. `resource import` Ciò significa che non è possibile importare uno stack in uno stack figlio o importare uno stack con figli.

Se non conosci l'importazione, ti consigliamo di leggere prima le informazioni introduttive contenute nell'argomento. [Importazione AWS manuale delle risorse in uno CloudFormation stack](#)

Convalida dell'importazione dello stack nidificato

Durante un'operazione di importazione di stack annidati, AWS CloudFormation esegue le seguenti convalide.

- La definizione `AWS::CloudFormation::Stack` nidificata nel modello di stack padre corrisponde al modello dello stack nidificato effettivo.
- I tag per la definizione `AWS::CloudFormation::Stack` nidificata nel modello di stack padre corrispondono ai tag per la risorsa stack nidificata effettiva.

Nidificazione di uno stack esistente utilizzando la AWS Management Console

1. Aggiungi la `AWS::CloudFormation::Stack` risorsa al modello dello stack principale con un. Retain [DeletionPolicy](#) Nell'esempio seguente, il modello dello stack principale, `MyNestedStack` è la destinazione dell'importazione.

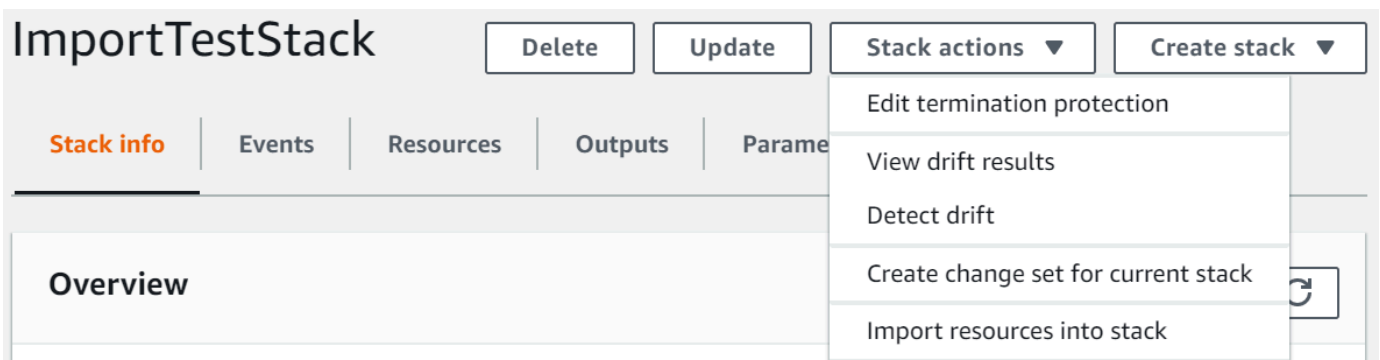
JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "ServiceTable":{
      "Type":"AWS::DynamoDB::Table",
      "Properties":{
        "TableName":"Service",
        "AttributeDefinitions":[
          {
            "AttributeName":"key",
            "AttributeType":"S"
          }
        ],
        "KeySchema":[
          {
            "AttributeName":"key",
            "KeyType":"HASH"
          }
        ],
        "ProvisionedThroughput":{
          "ReadCapacityUnits":5,
          "WriteCapacityUnits":1
        }
      }
    },
    "MyNestedStack" : {
      "Type" : "AWS::CloudFormation::Stack",
      "DeletionPolicy": "Retain",
      "Properties" : {
        "TemplateURL" : "https://s3.amazonaws.com/cloudformation-templates-us-east-2/EC2ChooseAMI.template",
        "Parameters" : {
          "InstanceType" : "t1.micro",
          "KeyName" : "mykey"
        }
      }
    }
  }
}
```


YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  ServiceTable:
    Type: 'AWS::DynamoDB::Table'
    Properties:
      TableName: Service
      AttributeDefinitions:
        - AttributeName: key
          AttributeType: S
      KeySchema:
        - AttributeName: key
          KeyType: HASH
      ProvisionedThroughput:
        ReadCapacityUnits: 5
        WriteCapacityUnits: 1
  MyNestedStack:
    Type: 'AWS::CloudFormation::Stack'
    DeletionPolicy: Retain
    Properties:
      TemplateURL: >-
        https://s3.amazonaws.com/cloudformation-templates-us-east-2/
        EC2ChooseAMI.template
      Parameters:
        InstanceType: t1.micro
        KeyName: mykey
```

2. Apri la AWS CloudFormation console.
3. Nella pagina Stacks (Stack) con lo stack padre selezionato, scegliere Stack actions (Operazioni stack), quindi scegliere Import resources into stack (Importa risorse nello stack).



4. Leggere la pagina Import overview (Panoramica importazione) per un elenco di elementi da fornire durante questa operazione. Quindi, seleziona Next (Successivo).
5. Nella pagina Specify model (Specifica modello), fornire il modello padre aggiornato utilizzando uno dei metodi descritti di seguito, quindi scegliere Next (Successivo).
 - Scegliere Amazon S3 URL (URL Amazon S3), quindi specificare l'URL per il tuo modello nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il modello.
6. Nella pagina Identify resources (Identifica risorse), identifica la risorsa `AWS::CloudFormation::Stack`.
 - a. In Identifier property (Proprietà identificatore), scegliere il tipo di identificatore di risorsa. Ad esempio, una risorsa `AWS::CloudFormation::Stack` può essere identificata utilizzando la proprietà `StackId`.
 - b. In Valore identificatore, digita l'ARN dello stack che stai importando. Ad esempio, *`arn:aws:cloudformation:us-west-2:12345678910:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10`*.

Resources to import (1)

The following logical IDs are new to your template. Provide the identifier values for the resource you are importing.

NestedStack

`AWS::CloudFormation::Stack`

Identifier property

StackId

Identifier value

Enter StackId

- c. Scegli Next (Successivo).
7. Nella pagina Specify stack details (Specifica dettagli stack), modificare i parametri, quindi scegliere Next (Successivo). Questo crea automaticamente un set di modifiche.

Important

L'operazione di importazione ha esito negativo se si modificano i parametri esistenti che iniziano un'operazione di creazione, aggiornamento o eliminazione.

8. Nella **MyParentStack** pagina Revisione, conferma che sia stata importata la risorsa corretta, quindi scegli Importa risorse. In questo modo si esegue automaticamente il set di modifiche creato nell'ultimo passaggio. Tutti i tag a livello di stack vengono applicati alle risorse importate in questo momento.
9. Per lo stack padre viene visualizzato il riquadro Events (Eventi) della pagina Stack details (Dettagli stack).

ImportTestStack Delete Update Stack actions ▼ Create stack ▼

Stack info **Events** Resources Outputs Parameters Template Change sets

Events

🔍 Search events

Timestamp	Logical ID	Status	Status reason
2019-10-24 15:52:49 UTC-0700	ImportTestStack	🟢 IMPORT_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SamplelamUser	🟢 UPDATE_COMPLETE	-
2019-10-24 15:52:47 UTC-0700	SamplelamUser	🔄 UPDATE_IN_PROGRESS	Apply stack-level tags to imported resource if applicable.
2019-10-24 15:52:46 UTC-0700	SamplelamUser	🟢 IMPORT_COMPLETE	Resource import completed.
2019-10-24 15:52:45 UTC-0700	SamplelamUser	🔄 IMPORT_IN_PROGRESS	Resource import started.
2019-10-24 15:52:43 UTC-0700	ImportTestStack	🔄 IMPORT_IN_PROGRESS	User Initiated
2019-10-24 15:52:01 UTC-0700	ImportTestStack	🔄 REVIEW_IN_PROGRESS	User Initiated

Note

Non è necessario eseguire il rilevamento della deviazione nello stack padre dopo questa operazione di importazione perché la risorsa `AWS::CloudFormation::Stack` era già gestita da AWS CloudFormation.

Nidificazione di uno stack esistente utilizzando la AWS CLI

1. Aggiungi la `AWS::CloudFormation::Stack` risorsa al modello dello stack principale con un. Retain [DeletionPolicy](#) Nel seguente modello padre di esempio, MyNestedStack è la destinazione dell'importazione.

JSON

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
    "ServiceTable":{
      "Type":"AWS::DynamoDB::Table",
```

```

        "Properties":{
            "TableName":"Service",
            "AttributeDefinitions":[
                {
                    "AttributeName":"key",
                    "AttributeType":"S"
                }
            ],
            "KeySchema":[
                {
                    "AttributeName":"key",
                    "KeyType":"HASH"
                }
            ],
            "ProvisionedThroughput":{
                "ReadCapacityUnits":5,
                "WriteCapacityUnits":1
            }
        },
        "MyNestedStack" : {
            "Type" : "AWS::CloudFormation::Stack",
            "DeletionPolicy": "Retain",
            "Properties" : {
                "TemplateURL" : "https://s3.amazonaws.com/cloudformation-templates-us-east-2/EC2ChooseAMI.template",
                "Parameters" : {
                    "InstanceType" : "t1.micro",
                    "KeyName" : "mykey"
                }
            }
        }
    }
}

```

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Resources:
  ServiceTable:
    Type: 'AWS::DynamoDB::Table'
    Properties:
      TableName: Service

```

```

AttributeDefinitions:
  - AttributeName: key
    AttributeType: S
KeySchema:
  - AttributeName: key
    KeyType: HASH
ProvisionedThroughput:
  ReadCapacityUnits: 5
  WriteCapacityUnits: 1
MyNestedStack:
  Type: 'AWS::CloudFormation::Stack'
  DeletionPolicy: Retain
  Properties:
    TemplateURL: >-
      https://s3.amazonaws.com/cloudformation-templates-us-east-2/
EC2ChooseAMI.template
    Parameters:
      InstanceType: t1.micro
      KeyName: mykey

```

2. Componi una stringa JSON come mostrato nell'esempio seguente, con queste modifiche:

- Sostituisci *MyNestedStack* con l'ID logico della risorsa di destinazione come specificato nel modello.
- Sostituisci *arn:aws:cloudformation:us-west-2:12345678910:stack/mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10* con l'ARN dello stack che desideri importare.

```

[{"ResourceType":"AWS::CloudFormation::Stack","LogicalResourceId":"MyNestedStack","Resource
{"StackId":"arn:aws:cloudformation:us-east-2:123456789012:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10"}]}]

```

In alternativa, è possibile specificare i parametri in un file di configurazione.

Ad esempio, per importare *MyNestedStack*, è possibile creare un *ResourcesToImport.txt* file contenente la seguente configurazione.

JSON

```

[
{

```

```

    "ResourceType": "AWS::CloudFormation::Stack",
    "LogicalResourceId": "MyNestedStack",
    "ResourceIdentifier": {
        "StackId": "arn:aws:cloudformation:us-west-2:12345678910:stack/
mystack/5b918d10-cd98-11ea-90d5-0a9cd3354c10"
    }
}
]

```

YAML

```

ResourceType: 'AWS::CloudFormation::Stack'
LogicalResourceId: MyNestedStack
ResourceIdentifier:
  StackId: >-
    arn:aws:cloudformation:us-west-2:12345678910:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10

```

3. Per creare un set di modifiche, utilizzate il create-change-set comando seguente e sostituite il testo segnaposto. Per l'opzione --change-set-type, specifica il valore di **IMPORT**. Per l'--resources-to-import opzione, sostituite la stringa JSON di esempio con la stringa JSON effettiva che avete appena creato.

```

aws cloudformation create-change-set \
  --stack-name MyParentStack --change-set-name ImportChangeSet \
  --change-set-type IMPORT \
  --template-body file://TemplateToImport.json \
  --resources-to-
import '[{"ResourceType": "AWS::CloudFormation::Stack", "LogicalResourceId": "MyNestedStack",
{"StackId": "arn:aws:cloudformation:us-west-2:12345678910:stack/mystack/5b918d10-
cd98-11ea-90d5-0a9cd3354c10"}}]'

```

Note

--resources-to-import non supporta YAML in linea. I requisiti per l'escape tra virgolette nella stringa JSON variano a seconda del terminale. Per ulteriori informazioni, consulta [Uso delle virgolette all'interno delle stringhe](#) nella Guida per l'utente AWS Command Line Interface

In alternativa, è possibile utilizzare l'URL di un file come input per l'`--resources-to-import` opzione, come illustrato nell'esempio seguente.

```
--resources-to-import file:///ResourcesToImport.txt
```

In caso di successo, questo comando restituisce il seguente output di esempio.

```
{
  "Id": "arn:aws:cloudformation:us-west-2:12345678910:changeSet/
  ImportChangeSet/8ad75b3f-665f-46f6-a200-0b4727a9442e",
  "StackId": "arn:aws:cloudformation:us-west-2:12345678910:stack/
  MyParentStack/4e345b70-1281-11ef-b027-027366d8e82b"
}
```

4. Esaminare il set di modifiche per assicurarsi che venga importato lo stack corretto.

```
aws cloudformation describe-change-set --change-set-name ImportChangeSet
```

5. Per avviare il set di modifiche e importare lo stack nello stack principale di origine, utilizzate il `execute-change-set` comando seguente e sostituite il testo segnaposto. Tutti i [tag a livello di stack](#) vengono applicati alle risorse importate in questo momento. Al completamento dell'operazione di importazione (`IMPORT_COMPLETE`), lo stack viene nidificato correttamente.

```
aws cloudformation execute-change-set --change-set-name ImportChangeSet
```

Note

Non è necessario eseguire il rilevamento della deviazione nello stack padre dopo questa operazione di importazione perché la risorsa `AWS::CloudFormation::Stack` è già gestita da AWS CloudFormation.

Importa AWS automaticamente le risorse in uno CloudFormation stack

Ora puoi importare automaticamente risorse denominate durante la creazione o l'aggiornamento degli stack. CloudFormation Una risorsa denominata è una risorsa con un nome personalizzato. Per ulteriori informazioni, vedere [Tipo di nome](#) nel riferimento del CloudFormation modello.

Quando avvii l'importazione automatica, CloudFormation verifica le risorse esistenti che corrispondono al modello e le importa durante la distribuzione. Per gli stack annidati, create il set di modifiche dallo stack principale.

Al termine dell'importazione e prima di eseguire operazioni di stack successive, si consiglia di eseguire il rilevamento della deviazione sulle risorse importate. Il rilevamento della deviazione garantisce che la configurazione del modello corrisponda alla configurazione effettiva. Per ulteriori informazioni, consulta [Rileva la deriva su un'intera CloudFormation pila](#).

Per importare una risorsa, devono soddisfare i seguenti requisiti:

- La risorsa deve avere un nome statico personalizzato definito nel modello. Nomi dinamici (usando Ref (o altre funzioni) non sono attualmente supportate.
- La risorsa deve avere un valore DeletionPolicy di Retain o RetainExceptOnCreate.
- La risorsa non deve già appartenere a un altro CloudFormation stack.
- Il tipo di risorsa deve supportare le operazioni di CloudFormation importazione. Per ulteriori informazioni, consulta [Supporto per tipi di risorse](#).
- L'ID principale per il tipo di risorsa deve essere nel modello. Le proprietà primarie IDs con sola lettura non sono supportate. Per scoprire qual è l'ID principale di un tipo, cerca la `primaryIdentifier` proprietà nello schema delle risorse. Per ulteriori informazioni sulla proprietà, vedere [PrimaryIdentifier](#).

Example Esempio di importazione automatica

L'esempio seguente utilizza un set di modifiche `CreateChangeSet` per creare uno stack chiamato `my-stack` base a un file modello e importa `template.yaml` automaticamente le risorse corrispondenti.

```
aws cloudformation create-change-set \  
  --stack-name my-stack \  
  --change-set-name CreateChangeSet \  
  --change-set-type CREATE \  
  --template-body file://template.yaml \  
  --import-existing-resources
```

Risoluzione dei problemi

Se l'importazione automatica fallisce, procedi come segue per risolvere il problema:

- Verifica che il nome della risorsa nel modello corrisponda esattamente al nome della risorsa
- Verifica che la risorsa non sia già gestita da un altro stack
- Assicurati che il tipo di risorsa supporti le operazioni di importazione
- Verifica che il modello includa tutte le proprietà richieste per il tipo di risorsa

Ripristino di un'operazione di importazione

Per ripristinare un'operazione di importazione, specificare una policy di eliminazione `Retain` per la risorsa che si desidera rimuovere dal modello per assicurarsi che venga mantenuta quando viene eliminata dallo stack.

Ripristino di un'operazione di importazione utilizzando la AWS Management Console

1. Specificate a `Retain` [DeletionPolicy](#) per le risorse che desiderate rimuovere dal vostro stack. Nel modello di esempio seguente, `GameTable` è la destinazione di questa operazione di inversione.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ],
        "ProvisionedThroughput": {
```

```
        "ReadCapacityUnits": 5,  
        "WriteCapacityUnits": 1  
    }  
}  
  
},  
"GamesTable": {  
    "Type": "AWS::DynamoDB::Table",  
    "DeletionPolicy": "Retain",  
    "Properties": {  
        "TableName": "Games",  
        "AttributeDefinitions": [  
            {  
                "AttributeName": "key",  
                "AttributeType": "S"  
            }  
        ],  
        "KeySchema": [  
            {  
                "AttributeName": "key",  
                "KeyType": "HASH"  
            }  
        ],  
        "ProvisionedThroughput": {  
            "ReadCapacityUnits": 5,  
            "WriteCapacityUnits": 1  
        }  
    }  
}  
  
}
```

2. Apri la CloudFormation console per eseguire un aggiornamento dello stack per applicare la politica di eliminazione.
 - a. Nella pagina Stacks (Stack) con lo stack selezionato, scegliere Update (Aggiorna), quindi scegliere Update stack (Aggiorna stack) (standard).
 - b. In Prepare template (Prepara modello), scegliere Replace current template (Sostituisci modello corrente).
 - c. In Specify template (Specifica modello), fornire il modello di origine aggiornato con l'attributo DeletionPolicy su GameTable, quindi scegliere Next (Successivo).

- Scegliere Amazon URL S3 (URL Amazon S3), quindi specificare l'URL per il modello di origine aggiornato nella casella di testo.
 - Scegliere Upload a template file (Carica un file modello), quindi cercare il file modello di origine aggiornato.
- d. Nella pagina Specify stack details (Specifica dettagli stack), non sono necessarie modifiche. Scegli Next (Successivo).
- e. Nella pagina Configure stack options (Configura opzioni stack) non sono necessarie modifiche. Scegli Next (Successivo).
- f. Nella *MyStack* pagina Revisione, rivedi le modifiche. Se il modello contiene risorse IAM, selezionare ☒ acknowledge that this template may create IAM resources (Acconsento che questo modello possa creare risorse IAM) per specificare che si desidera utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#). Quindi, aggiornare lo stack di origine creando un set di modifiche o aggiornare direttamente lo stack di origine.
3. Rimuovere la risorsa, i parametri correlati e gli output dal modello dello stack. In questo esempio, il modello ora è simile al seguente.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "TableName": "Service",
        "AttributeDefinitions": [
          {
            "AttributeName": "key",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "key",
            "KeyType": "HASH"
          }
        ]
      }
    }
  }
}
```

```

    ],
    "ProvisionedThroughput":{
      "ReadCapacityUnits":5,
      "WriteCapacityUnits":1
    }
  }
}
}
}

```

4. Ripetere il passaggio 2 per eliminare la risorsa (GameTable) e i relativi parametri e output dallo stack.

Ripristino di un'operazione di importazione utilizzando la AWS CLI

1. Specificate a Retain [DeletionPolicy](#) per le risorse che desiderate rimuovere dal vostro stack. Nel modello di esempio seguente, GameTable è la destinazione di questa operazione di inversione.

Example JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Resources": {
    "ServiceTable":{
      "Type":"AWS::DynamoDB::Table",
      "Properties":{
        "TableName":"Service",
        "AttributeDefinitions":[
          {
            "AttributeName":"key",
            "AttributeType":"S"
          }
        ],
        "KeySchema":[
          {
            "AttributeName":"key",
            "KeyType":"HASH"
          }
        ],
        "ProvisionedThroughput":{

```

```
        "ReadCapacityUnits": 5,
        "WriteCapacityUnits": 1
    }
},
"GamesTable": {
    "Type": "AWS::DynamoDB::Table",
    ""DeletionPolicy": "Retain",
    "Properties": {
        "TableName": "Games",
        "AttributeDefinitions": [
            {
                "AttributeName": "key",
                "AttributeType": "S"
            }
        ],
        "KeySchema": [
            {
                "AttributeName": "key",
                "KeyType": "HASH"
            }
        ],
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 1
        }
    }
}
}
```

2. Aggiornare lo stack per applicare la policy di eliminazione alla risorsa.

```
aws cloudformation update-stack --stack-name MyStack
```

3. Rimuovere la risorsa, i parametri correlati e gli output dal modello dello stack. In questo esempio, il modello ora è simile al seguente.

Example JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Import test",
  "Parameters": {
    "BucketName": {
      "Type": "Text",
      "Default": "test-bucket",
      "ConstraintDescription": "Bucket name must be 3-63 characters long."
    },
    "Region": {
      "Type": "Text",
      "Default": "us-east-1",
      "ConstraintDescription": "Region must be a valid AWS region."
    }
  },
  "Resources": {
    "Bucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {
        "BucketName": "test-bucket",
        "Region": "us-east-1"
      }
    }
  }
}
```

```
"Resources": {
  "ServiceTable":{
    "Type":"AWS::DynamoDB::Table",
    "Properties":{
      "TableName":"Service",
      "AttributeDefinitions":[
        {
          "AttributeName":"key",
          "AttributeType":"S"
        }
      ],
      "KeySchema":[
        {
          "AttributeName":"key",
          "KeyType":"HASH"
        }
      ],
      "ProvisionedThroughput":{
        "ReadCapacityUnits":5,
        "WriteCapacityUnits":1
      }
    }
  }
}
```

4. Aggiornare lo stack per eliminare la risorsa (GameTable) e i relativi parametri e output dallo stack.

```
aws cloudformation update-stack --stack-name MyStack
```

Rifattorizzazione degli stack

Il refactoring dello stack semplifica la riorganizzazione delle risorse negli stack preservando al contempo le proprietà e i dati delle risorse esistenti. CloudFormation Con il refactoring dello stack, puoi spostare le risorse tra gli stack, dividere gli stack monolitici in componenti più piccoli o consolidare più stack in uno solo.

Come funziona lo stack refactoring

Prendi in considerazione i passaggi seguenti quando pianifichi il refactor dello stack:

1. Valuta la tua infrastruttura attuale: esamina gli CloudFormation stack e le risorse esistenti per identificare le opportunità di refactoring degli stack.
2. Pianifica il refactoring: definisci come devono essere organizzate le risorse. Considerate le vostre dipendenze, le convenzioni di denominazione e i limiti operativi. Questi possono influire sulla convalida successiva CloudFormation .

Determina il numero di stack di destinazione in cui rifattorizzerai le risorse. Puoi spostare le risorse tra almeno 2 pile e un massimo di 5 pile. Le risorse possono essere spostate tra pile annidate.

3. Aggiorna i modelli: modifica i CloudFormation modelli in modo che riflettano la modifica pianificata, ad esempio spostando le definizioni delle risorse tra i modelli. È possibile rinominare il codice logico IDs durante il refactoring.
4. Crea il refactor dello stack: fornisci un elenco di nomi e modelli dello stack che desideri rifattorizzare.
5. Esamina l'impatto del refactoring sulla tua infrastruttura e risolvi eventuali conflitti: CloudFormation convalida i modelli forniti e verifica le dipendenze tra gli stack, i tipi di risorse con problemi di aggiornamento dei tag e i conflitti tra gli ID logici delle risorse.

Se la convalida ha esito positivo, CloudFormation genererà un'anteprima delle azioni di rifattore che avverranno dopo l'esecuzione del refactor.

Se la convalida fallisce, puoi riprovare dopo aver risolto i problemi rilevati. In caso di conflitti, sarà necessario fornire una mappatura degli ID logici delle risorse che mostri l'origine e la destinazione della risorsa in conflitto.

6. Esegui il refactoring: dopo aver verificato che le modifiche siano in linea con il modo in cui desideri rifattorizzare gli stack, esegui lo stack refactor.
7. Monitora: controlla lo stato dello stack refactor `ExecutionStatus` per assicurarti che abbia esito positivo.

Limitazioni dello stack refactoring

Considerate le seguenti limitazioni quando pianificate il refactoring dello stack:

- Le operazioni di rifattorizzazione non consentono la creazione di nuove risorse, l'eliminazione di risorse o la modifica delle configurazioni delle risorse.

- Non è possibile modificare o aggiungere nuovi parametri, condizioni o mappature durante un refactoring dello stack. Una possibile soluzione alternativa consiste nell'aggiornare lo stack prima di eseguire il refactoring.
- Non puoi rifattorizzare la stessa risorsa in più stack.
- Non è possibile rifattorizzare una risorsa in un nuovo stack se quello stack utilizza determinati pseudo parametri (Esempio:). `AWS::StackName`
- CloudFormation non supporta pile vuote. Prima di creare un refactor dello stack che rimuova tutte le risorse esistenti da uno stack, è necessario aggiungere una risorsa a quello stack. Questa risorsa può essere semplice, ad esempio un tipo di risorsa. `waitCondition`
- Stack refactor non supporta gli stack che contengono policy di stack, incluse le policy che consentono la modifica delle risorse.
- Le seguenti risorse non sono disponibili:
 - `AWS::ACMPCA::Certificate`
 - `AWS::ACMPCA::CertificateAuthority`
 - `AWS::ACMPCA::CertificateAuthorityActivation`
 - `AWS::ApiGateway::BasePathMapping`
 - `AWS::ApiGateway::Method`
 - `AWS::AppConfig::ConfigurationProfile`
 - `AWS::AppConfig::Deployment`
 - `AWS::AppConfig::Environment`
 - `AWS::AppConfig::Extension`
 - `AWS::AppConfig::ExtensionAssociation`
 - `AWS::AppStream::DirectoryConfig`
 - `AWS::AppStream::StackFleetAssociation`
 - `AWS::AppStream::StackUserAssociation`
 - `AWS::AppStream::User`
 - `AWS::BackupGateway::Hypervisor`
 - `AWS::CodePipeline::CustomActionType`
 - `AWS::Cognito::UserPoolRiskConfigurationAttachment`
 - `AWS::Cognito::UserPoolUICustomizationAttachment`
 - `AWS::Cognito::UserPoolUserToGroupAttachment`

- `AWS::Config::ConfigRule`
- `AWS::DataBrew::Dataset`
- `AWS::DataBrew::Job`
- `AWS::DataBrew::Project`
- `AWS::DataBrew::Recipe`
- `AWS::DataBrew::Ruleset`
- `AWS::DataBrew::Schedule`
- `AWS::DataZone::DataSource`
- `AWS::DataZone::Environment`
- `AWS::DataZone::EnvironmentBlueprintConfiguration`
- `AWS::DataZone::EnvironmentProfile`
- `AWS::DataZone::Project`
- `AWS::DataZone::SubscriptionTarget`
- `AWS::DynamoDB::GlobalTable`
- `AWS::EC2::LaunchTemplate`
- `AWS::EC2::SpotFleet`
- `AWS::EC2::VolumeAttachment`
- `AWS::EC2::VPCDHCPOptionsAssociation`
- `AWS::ElasticBeanstalk::ConfigurationTemplate`
- `AWS::FIS::ExperimentTemplate`
- `AWS::Glue::Schema`
- `AWS::GuardDuty::IPSet`
- `AWS::GuardDuty::PublishingDestination`
- `AWS::GuardDuty::ThreatIntelSet`
- `AWS::ImageBuilder::Component`
- `AWS::IoT FleetWise::Campaign`
- `AWS::IoTWireless::WirelessDeviceImportTask`
- `AWS::Lambda::EventInvokeConfig`
- `AWS::Lex::BotVersion`
- `AWS::M2::Application`

- `AWS::Maester::DocumentType`
- `AWS::MediaTailor::Channel`
- `AWS::MSK::Configuration`
- `AWS::MSK::ServerlessCluster`
- `AWS::NeptuneGraph::PrivateGraphEndpoint`
- `AWS::Omics::AnnotationStore`
- `AWS::Omics::ReferenceStore`
- `AWS::Omics::SequenceStore`
- `AWS::OpenSearchServerless::Collection`
- `AWS::Panorama::PackageVersion`
- `AWS::PCACConnectorAD::Connector`
- `AWS::PCACConnectorAD::DirectoryRegistration`
- `AWS::PCACConnectorAD::Template`
- `AWS::PCACConnectorAD::TemplateGroupAccessControlEntry`
- `AWS::QuickSight::Theme`
- `AWS::RefactorSpaces::Environment`
- `AWS::RefactorSpaces::Route`
- `AWS::RefactorSpaces::Service`
- `AWS::RoboMaker::RobotApplication`
- `AWS::RoboMaker::SimulationApplication`
- `AWS::SageMaker::InferenceComponen`
- `AWS::ServiceCatalog::PortfolioPrincipalAssociation`
- `AWS::ServiceCatalog::PortfolioProductAssociation`
- `AWS::ServiceCatalog::PortfolioShare`
- `AWS::ServiceCatalog::TagOptionAssociation`
- `AWS::ServiceCatalogAppRegistry::AttributeGroupAssociation`
- `AWS::ServiceCatalogAppRegistry::ResourceAssociation`
- `AWS::StepFunctions::StateMachineVersion`
- `AWS::Synthetics::Canary`
- `AWS::VoiceID::Domain`

- `AWS::WAFv2::IPSet`
- `AWS::WAFv2::RegexPatternSet`
- `AWS::WAFv2::RuleGroup`
- `AWS::WAFv2::WebACL`

Rifattorizzazione di uno stack utilizzando il AWS Command Line Interface

I seguenti comandi vengono utilizzati per il refactoring dello stack:

- [create-stack-refactor](#)
- [describe-stack-refactor](#)
- [execute-stack-refactor](#)
- [list-stack-refactors](#)
- [list-stack-refactor-actions](#)

Di seguito è riportato un esempio di come rifattorizzare uno stack utilizzando (AWS Command Line Interface CLI).

1. Per iniziare, avrai bisogno del CloudFormation modello che desideri rifattorizzare. Il comando seguente recupera il modello:

```
aws cloudformation get-template --stack-name ExampleStack1
```

Una volta ottenuto il modello, utilizzate l'ambiente di sviluppo integrato (IDE) di vostra scelta per aggiornarlo in modo da utilizzare la struttura e l'organizzazione delle risorse desiderate.

2. Crea lo stack refactor usando il `create-stack-refactor` comando e fornisci il nome dello stack e i modelli per ogni stack coinvolto nel refactoring:

```
aws cloudformation create-stack-refactor \  
  --stack-definitions \  
    StackName=MySns,TemplateBody@=file://afterSns.yaml \  
    StackName=MyLambdaSubscription,TemplateBody@=file://afterLambda.yaml \  
  --enable-stack-creation \  
  --resource-mappings file://refactor.json
```

Il `--resource-mappings` parametro è facoltativo, ma sarà necessario se viene rilevato un conflitto durante la convalida del modello. Oltre a fornire gli `Destination stack Source` and, dovrai fornire anche il `LogicalResourceId`. Di seguito è riportato un esempio del file `refactor.json`.

```
[
  {
    "Source": {
      "StackName": "MySns",
      "LogicalResourceId": "MyFunction"
    },
    "Destination": {
      "StackName": "MyLambdaSubscription",
      "LogicalResourceId": "Function"
    }
  }
]
```

3. Dopo aver creato il refactor, CloudFormation genera un'anteprima della modifica del refactor, che consente di visualizzare in anteprima l'impatto che le modifiche proposte avranno sull'infrastruttura. In questo esempio, il file `StackRefactorId` creato è `stack-refactor-1ab2-c34d-5ef6`. Utilizzate il seguente comando per visualizzare in anteprima le modifiche:

```
aws cloudformation list-stack-refactor-actions \
  --stack-refactor-id stack-refactor-1ab2-c34d-5ef6
```

4. Dopo aver esaminato e confermato le modifiche, utilizzate il `execute-stack-refactor` comando per completare il processo di refactoring:

```
aws cloudformation execute-stack-refactor \
  --stack-refactor-id stack-refactor-1ab2-c34d-5ef6
```

5. Dopo l'esecuzione di `execute-stack-refactor`, è possibile monitorare lo stato dell'operazione utilizzando il seguente comando:

```
aws cloudformation describe-stack-refactor \
  --stack-refactor-id stack-refactor-1ab2-c34d-5ef6
```

CloudFormation aggiornerà automaticamente la Status fine ExecutionStatus dell'operazione di refactor.

Supporto per tipi di risorse

La tabella seguente elenca i tipi di AWS risorse che attualmente supportano le operazioni di importazione, rilevamento della deriva e generazione di infrastrutture come codice (IaC). Il nome di ogni tipo di risorsa rimanda all'argomento di riferimento corrispondente nella [AWS CloudFormation Template Reference](#) Guide.

Una risorsa che supporta l'importazione di risorse potrebbe supportare anche l'importazione automatica. Per ulteriori informazioni, consulta [Importazione di AWS risorse in una CloudFormation pila](#).

Questo non è un elenco esaustivo di AWS risorse. Se un tipo di risorsa specifico non è elencato, probabilmente significa che non è accessibile tramite AWS Cloud Control API. Per ulteriori informazioni, consulta [Tipi di risorse che supportano l'API Cloud Control](#) nella Guida per l'utente dell'API Cloud Control. Ogni AWS servizio determina in modo indipendente quali tipi di risorse rendere accessibili tramite l'API Cloud Control.

CloudFormation supporta anche operazioni di importazione e rilevamento della deriva per i tipi di risorse private che sono disponibili (quelle con tipi di provisioning di uno o più). FULLY_MUTABLE IMMUTABLE Per importare o eseguire il rilevamento della deriva su un tipo di risorsa privata, devi prima registrare la versione predefinita di quel tipo di risorsa nel tuo account e assicurarti che sia disponibile. Per ulteriori informazioni, consulta [Usa estensioni private di terze parti che sono state condivise con te](#).

Tieni presente che il generatore IaC supporta solo AWS risorse compatibili con l'API Cloud Control nella tua regione.

Per accedere in modo programmatico alle informazioni sui tipi di risorse fornibili pubbliche e private, puoi utilizzare AWS Cloud Control API. Per ulteriori informazioni, consulta [Determinare se un tipo di risorsa supporta l'API Cloud Control nella Guida per l'utente dell'API Cloud Control](#).

Per iniziare a usare l'importazione, il rilevamento delle derive o il generatore IaC, ecco alcuni argomenti utili da esaminare:

- [Importazione di AWS risorse in una CloudFormation pila](#)

- [Rileva le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento della deriva](#)
- [Genera modelli da risorse esistenti con il generatore IaC](#)

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IaC
AWS::ACMPCA::Certificate	 Sì	 No	 No
AWS::ACMPCA::CertificateAuthority	 Sì	 Sì	 Sì
AWS::ACMPCA::CertificateAuthorityActivation	 Sì	 No	 No
AWS::ACMPCA::Permission	 Sì	 Sì	 No
AWS::APS::RuleGroupsNamespace	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::APS::Scraper</u>	 Sì	 Sì	 No
<u>AWS::APS::Workspace</u>	 Sì	 Sì	 Sì
<u>AWS::ARCZonalShift::AutoshiftObserve rNotificationStatus</u>	 Sì	 Sì	 No
<u>AWS::ARCZonalShift::ZonalAutoshiftCo nfiguration</u>	 Sì	 Sì	 No
<u>AWS::AccessAnalyzer::Analyzer</u>	 Sì	 Sì	 Sì
<u>AWS::AmazonMQ::Configuration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Amplify::App	 Sì	 Sì	 Sì
AWS::Amplify::Branch	 Sì	 Sì	 Sì
AWS::Amplify::Domain	 Sì	 Sì	 Sì
AWS::AmplifyUIBuilder::Component	 Sì	 Sì	 Sì
AWS::AmplifyUIBuilder::Form	 Sì	 Sì	 Sì
AWS::AmplifyUIBuilder::Theme	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGateway::Account</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::ApiKey</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGateway::Authorizer</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::BasePathMapping</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::BasePathMappingV2</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::ClientCertificate</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGateway::Deployment</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGateway::DocumentationPart</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::DocumentationVersion</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGateway::DomainName</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::DomainNameAccessAssociation</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::DomainNameV2</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGateway::GatewayResponse</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::Method</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::Model</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::RequestValidator</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::Resource</u>	 Sì	 Sì	 No
<u>AWS::ApiGateway::RestApi</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGateway::Stage</u>	 Sì	 No	 Sì
<u>AWS::ApiGateway::UsagePlan</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGateway::UsagePlanKey</u>	 Sì	 No	 Sì
<u>AWS::ApiGateway::VpcLink</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::Api</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGatewayV2::ApiMapping</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGatewayV2::Authorizer</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::Deployment</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGatewayV2::DomainName</u>	 Sì	 Sì	 Sì
<u>AWS::ApiGatewayV2::Integration</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::IntegrationRespon se</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::Model</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApiGatewayV2::Route</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::RouteResponse</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::RoutingRule</u>	 Sì	 Sì	 No
<u>AWS::ApiGatewayV2::VpcLink</u>	 Sì	 Sì	 Sì
<u>AWS::AppConfig::Application</u>	 Sì	 Sì	 Sì
<u>AWS::AppConfig::ConfigurationProfile</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppConfig::Deployment</u>	 Sì	 Sì	 No
<u>AWS::AppConfig::DeploymentStrategy</u>	 Sì	 Sì	 No
<u>AWS::AppConfig::Environment</u>	 Sì	 Sì	 No
<u>AWS::AppConfig::Extension</u>	 Sì	 Sì	 No
<u>AWS::AppConfig::ExtensionAssociation</u>	 Sì	 Sì	 No
<u>AWS::AppConfig::HostedConfigurationVersion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppFlow::Connector</u>	 Sì	 Sì	 Sì
<u>AWS::AppFlow::ConnectorProfile</u>	 Sì	 Sì	 Sì
<u>AWS::AppFlow::Flow</u>	 Sì	 Sì	 Sì
<u>AWS::AppIntegrations::Application</u>	 Sì	 Sì	 No
<u>AWS::AppIntegrations::DataIntegratio n</u>	 Sì	 Sì	 Sì
<u>AWS::AppIntegrations::EventIntegrati on</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppRunner::AutoScalingConfigura tion</u>	 Sì	 Sì	 No
<u>AWS::AppRunner::ObservabilityConfigu ration</u>	 Sì	 Sì	 No
<u>AWS::AppRunner::Service</u>	 Sì	 Sì	 No
<u>AWS::AppRunner::VpcConnector</u>	 Sì	 Sì	 No
<u>AWS::AppRunner::VpcIngressConnection</u>	 Sì	 Sì	 No
<u>AWS::AppStream::AppBlock</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppStream::AppBlockBuilder</u>	 Sì	 Sì	 No
<u>AWS::AppStream::Application</u>	 Sì	 Sì	 No
<u>AWS::AppStream::ApplicationEntitleme ntAssociation</u>	 Sì	 Sì	 No
<u>AWS::AppStream::ApplicationFleetAsso ciation</u>	 Sì	 Sì	 No
<u>AWS::AppStream::DirectoryConfig</u>	 Sì	 Sì	 Sì
<u>AWS::AppStream::Entitlement</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppStream::ImageBuilder</u>	 Sì	 Sì	 Sì
<u>AWS::AppSync::Api</u>	 Sì	 Sì	 No
<u>AWS::AppSync::ChannelNamespace</u>	 Sì	 Sì	 No
<u>AWS::AppSync::DataSource</u>	 Sì	 Sì	 No
<u>AWS::AppSync::DomainName</u>	 Sì	 Sì	 Sì
<u>AWS::AppSync::DomainNameApiAssociati on</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AppSync::FunctionConfiguration</u>	 Sì	 Sì	 No
<u>AWS::AppSync::GraphQLApi</u>	 Sì	 Sì	 No
<u>AWS::AppSync::Resolver</u>	 Sì	 Sì	 No
<u>AWS::AppSync::SourceApiAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::ApplicationAutoScaling::ScalableTarget</u>	 Sì	 Sì	 Sì
<u>AWS::ApplicationAutoScaling::ScalingPolicy</u>	 Sì	 No	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ApplicationInsights::Applicatio n</u>	 Sì	 Sì	 No
<u>AWS::ApplicationSignals::Discovery</u>	 Sì	 Sì	 No
<u>AWS::ApplicationSignals::ServiceLeve lObjective</u>	 Sì	 Sì	 No
<u>AWS::Athena::CapacityReservation</u>	 Sì	 Sì	 Sì
<u>AWS::Athena::DataCatalog</u>	 Sì	 Sì	 Sì
<u>AWS::Athena::NamedQuery</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Athena::PreparedStatement</u>	 Sì	 Sì	 Sì
<u>AWS::Athena::WorkGroup</u>	 Sì	 Sì	 Sì
<u>AWS::AuditManager::Assessment</u>	 Sì	 No	 No
<u>AWS::AutoScaling::AutoScalingGroup</u>	 Sì	 No	 Sì
<u>AWS::AutoScaling::LaunchConfiguratio n</u>	 Sì	 Sì	 Sì
<u>AWS::AutoScaling::LifecycleHook</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::AutoScaling::ScalingPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::AutoScaling::ScheduledAction</u>	 Sì	 Sì	 Sì
<u>AWS::AutoScaling::WarmPool</u>	 Sì	 Sì	 No
<u>AWS::B2BI::Capability</u>	 Sì	 Sì	 No
<u>AWS::B2BI::Partnership</u>	 Sì	 Sì	 No
<u>AWS::B2BI::Profile</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::B2BI::Transformer</u>	 Sì	 Sì	 No
<u>AWS::Backup::BackupPlan</u>	 Sì	 Sì	 No
<u>AWS::Backup::BackupSelection</u>	 Sì	 No	 Sì
<u>AWS::Backup::BackupVault</u>	 Sì	 Sì	 No
<u>AWS::Backup::Framework</u>	 Sì	 Sì	 Sì
<u>AWS::Backup::LogicallyAirGappedBackupVault</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Backup::ReportPlan</u>	 Sì	 Sì	 Sì
<u>AWS::Backup::RestoreTestingPlan</u>	 Sì	 Sì	 No
<u>AWS::Backup::RestoreTestingSelection</u>	 Sì	 Sì	 No
<u>AWS::BackupGateway::Hypervisor</u>	 Sì	 Sì	 No
<u>AWS::Batch::ComputeEnvironment</u>	 Sì	 Sì	 Sì
<u>AWS::Batch::ConsumableResource</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Batch::JobDefinition</u>	 Sì	 Sì	 No
<u>AWS::Batch::JobQueue</u>	 Sì	 Sì	 Sì
<u>AWS::Batch::SchedulingPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::Bedrock::Agent</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::AgentAlias</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::ApplicationInferenceProfile</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Bedrock::Blueprint	 Sì	 Sì	 No
AWS::Bedrock::DataAutomationProject	 Sì	 Sì	 No
AWS::Bedrock::DataSource	 Sì	 Sì	 No
AWS::Bedrock::Flow	 Sì	 Sì	 No
AWS::Bedrock::FlowAlias	 Sì	 Sì	 No
AWS::Bedrock::FlowVersion	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Bedrock::Guardrail</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::GuardrailVersion</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::IntelligentPromptRoute r</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::KnowledgeBase</u>	 Sì	 No	 No
<u>AWS::Bedrock::Prompt</u>	 Sì	 Sì	 No
<u>AWS::Bedrock::PromptVersion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Budgets::BudgetsAction</u>	 Sì	 Sì	 Sì
<u>AWS::CE::AnomalyMonitor</u>	 Sì	 Sì	 No
<u>AWS::CE::AnomalySubscription</u>	 Sì	 Sì	 No
<u>AWS::CE::CostCategory</u>	 Sì	 Sì	 Sì
<u>AWS::Cassandra::Keyspace</u>	 Sì	 Sì	 No
<u>AWS::Cassandra::Table</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Cassandra::Type</u>	 Sì	 Sì	 No
<u>AWS::CertificateManager::Account</u>	 Sì	 Sì	 No
<u>AWS::Chatbot::CustomAction</u>	 Sì	 Sì	 No
<u>AWS::Chatbot::MicrosoftTeamsChannelC onfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::Chatbot::SlackChannelConfigurat ion</u>	 Sì	 Sì	 Sì
<u>AWS::CleanRooms::AnalysisTemplate</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CleanRooms::Collaboration</u>	 Sì	 Sì	 Sì
<u>AWS::CleanRooms::ConfiguredTable</u>	 Sì	 Sì	 Sì
<u>AWS::CleanRooms::ConfiguredTableAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::CleanRooms::IdMappingTable</u>	 Sì	 Sì	 No
<u>AWS::CleanRooms::IdNamespaceAssociation</u>	 Sì	 Sì	 No
<u>AWS::CleanRooms::Membership</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CleanRooms::PrivacyBudgetTemplate</u>	 Sì	 Sì	 No
<u>AWS::CleanRoomsML::TrainingDataset</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::GuardHook</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::HookDefaultVersion</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFormation::HookTypeConfig</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFormation::HookVersion</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudFormation::LambdaHook</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::ModuleDefaultVersion</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::ModuleVersion</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::PublicTypeVersion</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::Publisher</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::ResourceDefaultVersion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudFormation::ResourceVersion</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::Stack</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::StackSet</u>	 Sì	 Sì	 No
<u>AWS::CloudFormation::TypeActivation</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::AnycastIpList</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::CachePolicy</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudFront::CloudFrontOriginAccessIdentity</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::ConnectionGroup</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::ContinuousDeploymentPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::Distribution</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::DistributionTenant</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::Function</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudFront::KeyGroup</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::KeyValueStore</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::MonitoringSubscript ion</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::OriginAccessControl</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::OriginRequestPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::PublicKey</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudFront::RealtimeLogConfig</u>	 Sì	 Sì	 Sì
<u>AWS::CloudFront::ResponseHeadersPolicy</u>	 Sì	 Sì	 No
<u>AWS::CloudFront::VpcOrigin</u>	 Sì	 Sì	 No
<u>AWS::CloudTrail::Channel</u>	 Sì	 Sì	 No
<u>AWS::CloudTrail::Dashboard</u>	 Sì	 Sì	 No
<u>AWS::CloudTrail::EventDataStore</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CloudTrail::ResourcePolicy</u>	 Sì	 Sì	 No
<u>AWS::CloudTrail::Trail</u>	 Sì	 Sì	 Sì
<u>AWS::CloudWatch::Alarm</u>	 Sì	 Sì	 Sì
<u>AWS::CloudWatch::CompositeAlarm</u>	 Sì	 Sì	 Sì
<u>AWS::CloudWatch::Dashboard</u>	 Sì	 Sì	 No
<u>AWS::CloudWatch::MetricStream</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CodeArtifact::Domain</u>	 Sì	 Sì	 Sì
<u>AWS::CodeArtifact::PackageGroup</u>	 Sì	 Sì	 No
<u>AWS::CodeArtifact::Repository</u>	 Sì	 Sì	 Sì
<u>AWS::CodeBuild::Fleet</u>	 Sì	 Sì	 No
<u>AWS::CodeConnections::Connection</u>	 Sì	 Sì	 No
<u>AWS::CodeDeploy::Application</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CodeDeploy::DeploymentConfig</u>	 Sì	 Sì	 No
<u>AWS::CodeGuruProfiler::ProfilingGroup</u>	 Sì	 Sì	 Sì
<u>AWS::CodeGuruReviewer::RepositoryAssociation</u>	 Sì	 Sì	 No
<u>AWS::CodePipeline::CustomActionType</u>	 Sì	 Sì	 No
<u>AWS::CodePipeline::Pipeline</u>	 Sì	 Sì	 No
<u>AWS::CodeStarConnections::Connection</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::CodeStarConnections::RepositoryLink	 Sì	 Sì	 No
AWS::CodeStarConnections::SyncConfiguration	 Sì	 Sì	 No
AWS::CodeStarNotifications::NotificationRule	 Sì	 Sì	 Sì
AWS::Cognito::IdentityPool	 Sì	 Sì	 No
AWS::Cognito::IdentityPoolPrincipalTag	 Sì	 Sì	 Sì
AWS::Cognito::IdentityPoolRoleAttachment	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Cognito::LogDeliveryConfigurati on</u>	 Sì	 No	 No
<u>AWS::Cognito::ManagedLoginBranding</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPool</u>	 Sì	 No	 No
<u>AWS::Cognito::UserPoolClient</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolDomain</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolGroup</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Cognito::UserPoolIdentityProvider</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolResourceServer</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolRiskConfigurationAttachment</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolUICustomizationAttachment</u>	 Sì	 Sì	 No
<u>AWS::Cognito::UserPoolUser</u>	 Sì	 No	 No
<u>AWS::Cognito::UserPoolUserToGroupAttachment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Comprehend::DocumentClassifier</u>	 Sì	 Sì	 Sì
<u>AWS::Comprehend::Flywheel</u>	 Sì	 Sì	 Sì
<u>AWS::Config::AggregationAuthorizatio n</u>	 Sì	 Sì	 Sì
<u>AWS::Config::ConfigRule</u>	 Sì	 Sì	 Sì
<u>AWS::Config::ConfigurationAggregator</u>	 Sì	 Sì	 Sì
<u>AWS::Config::ConformancePack</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Config::OrganizationConformancePack	 Sì	 Sì	 Sì
AWS::Config::StoredQuery	 Sì	 Sì	 Sì
AWS::Connect::AgentStatus	 Sì	 Sì	 No
AWS::Connect::ApprovedOrigin	 Sì	 Sì	 Sì
AWS::Connect::ContactFlow	 Sì	 Sì	 Sì
AWS::Connect::ContactFlowModule	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Connect::ContactFlowVersion</u>	 Sì	 Sì	 No
<u>AWS::Connect::EmailAddress</u>	 Sì	 Sì	 No
<u>AWS::Connect::EvaluationForm</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::HoursOfOperation</u>	 Sì	 Sì	 No
<u>AWS::Connect::Instance</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::InstanceStorageConfig</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Connect::IntegrationAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::PhoneNumber</u>	 Sì	 Sì	 No
<u>AWS::Connect::PredefinedAttribute</u>	 Sì	 Sì	 No
<u>AWS::Connect::Prompt</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::Queue</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::QuickConnect</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Connect::RoutingProfile	 Sì	 Sì	 Sì
AWS::Connect::Rule	 Sì	 Sì	 No
AWS::Connect::SecurityKey	 Sì	 Sì	 Sì
AWS::Connect::SecurityProfile	 Sì	 Sì	 Sì
AWS::Connect::TaskTemplate	 Sì	 Sì	 No
AWS::Connect::TrafficDistributionGroup	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Connect::User</u>	 Sì	 Sì	 No
<u>AWS::Connect::UserHierarchyGroup</u>	 Sì	 Sì	 No
<u>AWS::Connect::UserHierarchyStructure</u>	 Sì	 Sì	 No
<u>AWS::Connect::View</u>	 Sì	 Sì	 Sì
<u>AWS::Connect::ViewVersion</u>	 Sì	 Sì	 Sì
<u>AWS::ConnectCampaigns::Campaign</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ConnectCampaignsV2::Campaign</u>	 Sì	 Sì	 No
<u>AWS::ControlTower::EnabledBaseline</u>	 Sì	 Sì	 No
<u>AWS::ControlTower::EnabledControl</u>	 Sì	 Sì	 Sì
<u>AWS::ControlTower::LandingZone</u>	 Sì	 Sì	 No
<u>AWS::CustomerProfiles::CalculatedAttributeDefinition</u>	 Sì	 Sì	 Sì
<u>AWS::CustomerProfiles::Domain</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::CustomerProfiles::EventStream</u>	 Sì	 Sì	 Sì
<u>AWS::CustomerProfiles::EventTrigger</u>	 Sì	 Sì	 No
<u>AWS::CustomerProfiles::Integration</u>	 Sì	 Sì	 Sì
<u>AWS::CustomerProfiles::ObjectType</u>	 Sì	 Sì	 Sì
<u>AWS::CustomerProfiles::SegmentDefini tion</u>	 Sì	 Sì	 No
<u>AWS::DMS::DataMigration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DMS::DataProvider</u>	 Sì	 Sì	 No
<u>AWS::DMS::InstanceProfile</u>	 Sì	 Sì	 No
<u>AWS::DMS::MigrationProject</u>	 Sì	 Sì	 No
<u>AWS::DMS::ReplicationConfig</u>	 Sì	 Sì	 Sì
<u>AWS::DSQL::Cluster</u>	 Sì	 Sì	 No
<u>AWS::DataBrew::Dataset</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataBrew::Job</u>	 Sì	 Sì	 Sì
<u>AWS::DataBrew::Project</u>	 Sì	 Sì	 Sì
<u>AWS::DataBrew::Recipe</u>	 Sì	 Sì	 Sì
<u>AWS::DataBrew::Ruleset</u>	 Sì	 Sì	 Sì
<u>AWS::DataBrew::Schedule</u>	 Sì	 Sì	 Sì
<u>AWS::DataPipeline::Pipeline</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataSync::Agent</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationAzureBlob</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationEFS</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationFSxLustre</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationFSxONTAP</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationFSxOpenZFS</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataSync::LocationFSxWindows</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationHDFS</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationNFS</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationObjectStorage</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationS3</u>	 Sì	 Sì	 Sì
<u>AWS::DataSync::LocationSMB</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataSync::Task</u>	 Sì	 Sì	 Sì
<u>AWS::DataZone::Connection</u>	 Sì	 Sì	 No
<u>AWS::DataZone::DataSource</u>	 Sì	 Sì	 No
<u>AWS::DataZone::Domain</u>	 Sì	 Sì	 No
<u>AWS::DataZone::DomainUnit</u>	 Sì	 Sì	 No
<u>AWS::DataZone::Environment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataZone::EnvironmentActions</u>	 Sì	 Sì	 No
<u>AWS::DataZone::EnvironmentBlueprintConfiguration</u>	 Sì	 Sì	 No
<u>AWS::DataZone::EnvironmentProfile</u>	 Sì	 Sì	 No
<u>AWS::DataZone::GroupProfile</u>	 Sì	 Sì	 No
<u>AWS::DataZone::Owner</u>	 Sì	 Sì	 No
<u>AWS::DataZone::Project</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DataZone::ProjectMembership</u>	 Sì	 Sì	 No
<u>AWS::DataZone::ProjectProfile</u>	 Sì	 Sì	 No
<u>AWS::DataZone::SubscriptionTarget</u>	 Sì	 Sì	 No
<u>AWS::DataZone::UserProfile</u>	 Sì	 Sì	 No
<u>AWS::Deadline::Farm</u>	 Sì	 Sì	 No
<u>AWS::Deadline::Fleet</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Deadline::LicenseEndpoint</u>	 Sì	 Sì	 No
<u>AWS::Deadline::Limit</u>	 Sì	 Sì	 No
<u>AWS::Deadline::MeteredProduct</u>	 Sì	 Sì	 No
<u>AWS::Deadline::Monitor</u>	 Sì	 Sì	 No
<u>AWS::Deadline::Queue</u>	 Sì	 Sì	 No
<u>AWS::Deadline::QueueEnvironment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Deadline::QueueFleetAssociation</u>	 Sì	 Sì	 No
<u>AWS::Deadline::QueueLimitAssociation</u>	 Sì	 Sì	 No
<u>AWS::Deadline::StorageProfile</u>	 Sì	 Sì	 No
<u>AWS::Detective::Graph</u>	 Sì	 Sì	 Sì
<u>AWS::Detective::MemberInvitation</u>	 Sì	 Sì	 Sì
<u>AWS::Detective::OrganizationAdmin</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DevOpsGuru::LogAnomalyDetectionIntegration</u>	 Sì	 Sì	 Sì
<u>AWS::DevOpsGuru::NotificationChannel</u>	 Sì	 Sì	 Sì
<u>AWS::DevOpsGuru::ResourceCollection</u>	 Sì	 Sì	 Sì
<u>AWS::DeviceFarm::DevicePool</u>	 Sì	 Sì	 No
<u>AWS::DeviceFarm::InstanceProfile</u>	 Sì	 Sì	 No
<u>AWS::DeviceFarm::NetworkProfile</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DeviceFarm::Project</u>	 Sì	 Sì	 No
<u>AWS::DeviceFarm::TestGridProject</u>	 Sì	 Sì	 No
<u>AWS::DeviceFarm::VPCEConfiguration</u>	 Sì	 Sì	 No
<u>AWS::DirectoryService::SimpleAD</u>	 Sì	 Sì	 Sì
<u>AWS::DocDBElastic::Cluster</u>	 Sì	 Sì	 Sì
<u>AWS::DynamoDB::GlobalTable</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::DynamoDB::Table</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::CapacityReservation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::CapacityReservationFleet</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::CarrierGateway</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::CustomerGateway</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::DHCPOptions</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::EC2Fleet</u>	 Sì	 Sì	 No
<u>AWS::EC2::EIP</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::EIPAssociation</u>	 Sì	 No	 Sì
<u>AWS::EC2::EgressOnlyInternetGateway</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::EnclaveCertificateIamRoleA ssociation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::FlowLog</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::GatewayRouteTableAssociation</u>	 Sì	 Sì	 No
<u>AWS::EC2::Host</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAM</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAMAllocation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAMPool</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAMPoolCidr</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::IPAMResourceDiscovery</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAMResourceDiscoveryAssoc iation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::IPAMScope</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::Instance</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::InstanceConnectEndpoint</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::InternetGateway</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::KeyPair</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::LaunchTemplate</u>	 Sì	 Sì	 No
<u>AWS::EC2::LocalGatewayRoute</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::LocalGatewayRouteTable</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::LocalGatewayRouteTableVPCAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::NatGateway</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::NetworkAcl</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::NetworkInsightsAccessScope</u>	 Sì	 Sì	 No
<u>AWS::EC2::NetworkInsightsAccessScope Analysis</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::NetworkInsightsAnalysis</u>	 Sì	 Sì	 No
<u>AWS::EC2::NetworkInsightsPath</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::NetworkInterface</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::NetworkInterfaceAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::NetworkPerformanceMetricSubscription</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::PlacementGroup</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::PrefixList</u>	 Sì	 Sì	 No
<u>AWS::EC2::Route</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::RouteServer</u>	 Sì	 Sì	 No
<u>AWS::EC2::RouteServerAssociation</u>	 Sì	 Sì	 No
<u>AWS::EC2::RouteServerEndpoint</u>	 Sì	 Sì	 No
<u>AWS::EC2::RouteServerPeer</u>	 Sì	 Sì	 No
<u>AWS::EC2::RouteServerPropagation</u>	 Sì	 Sì	 No
<u>AWS::EC2::RouteTable</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::SecurityGroup</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::SecurityGroupEgress</u>	 Sì	 Sì	 No
<u>AWS::EC2::SecurityGroupIngress</u>	 Sì	 Sì	 No
<u>AWS::EC2::SecurityGroupVpcAssociatio n</u>	 Sì	 Sì	 No
<u>AWS::EC2::SnapshotBlockPublicAccess</u>	 Sì	 Sì	 No
<u>AWS::EC2::SpotFleet</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::Subnet</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::SubnetCidrBlock</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::SubnetNetworkAclAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::SubnetRouteTableAssociation</u>	 Sì	 No	 Sì
<u>AWS::EC2::TrafficMirrorFilter</u>	 Sì	 Sì	 No
<u>AWS::EC2::TrafficMirrorFilterRule</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::TransitGateway</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayConnect</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayMulticastDomain</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayMulticastDomainAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayMulticastGroupMember</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::TransitGatewayMulticastGroupSource</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayPeeringAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayRoute</u>	 Sì	 Sì	 No
<u>AWS::EC2::TransitGatewayRouteTable</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::TransitGatewayRouteTableAssociation</u>	 Sì	 Sì	 No
<u>AWS::EC2::TransitGatewayRouteTablePropagation</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::EC2::TransitGatewayVpcAttachment	 Sì	 Sì	 Sì
AWS::EC2::VPC	 Sì	 Sì	 Sì
AWS::EC2::VPCLockPublicAccessExclusion	 Sì	 Sì	 No
AWS::EC2::VPCLockPublicAccessOptions	 Sì	 Sì	 No
AWS::EC2::VPCCIDRBlock	 Sì	 Sì	 No
AWS::EC2::VPCDHCPOptionsAssociation	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::EC2::VPCEndpoint	 Sì	 Sì	 Sì
AWS::EC2::VPCEndpointConnectionNotif ication	 Sì	 Sì	 Sì
AWS::EC2::VPCEndpointService	 Sì	 Sì	 Sì
AWS::EC2::VPCEndpointServicePermissi ons	 Sì	 Sì	 No
AWS::EC2::VPCGatewayAttachment	 Sì	 Sì	 No
AWS::EC2::VPCPeeringConnection	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::EC2::VPNConnection	 Sì	 Sì	 Sì
AWS::EC2::VPNConnectionRoute	 Sì	 Sì	 Sì
AWS::EC2::VPNGateway	 Sì	 Sì	 Sì
AWS::EC2::VerifiedAccessEndpoint	 Sì	 Sì	 Sì
AWS::EC2::VerifiedAccessGroup	 Sì	 Sì	 Sì
AWS::EC2::VerifiedAccessInstance	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EC2::VerifiedAccessTrustProvider</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::Volume</u>	 Sì	 Sì	 Sì
<u>AWS::EC2::VolumeAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::ECR::PullThroughCacheRule</u>	 Sì	 Sì	 Sì
<u>AWS::ECR::RegistryPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::ECR::RegistryScanningConfiguration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ECR::ReplicationConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::ECR::Repository</u>	 Sì	 Sì	 Sì
<u>AWS::ECR::RepositoryCreationTemplate</u>	 Sì	 Sì	 No
<u>AWS::ECS::CapacityProvider</u>	 Sì	 Sì	 No
<u>AWS::ECS::Cluster</u>	 Sì	 No	 Sì
<u>AWS::ECS::ClusterCapacityProviderAss ociations</u>	 Sì	 No	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ECS::PrimaryTaskSet</u>	 Sì	 Sì	 No
<u>AWS::ECS::Service</u>	 Sì	 Sì	 Sì
<u>AWS::ECS::TaskDefinition</u>	 Sì	 Sì	 Sì
<u>AWS::ECS::TaskSet</u>	 Sì	 Sì	 No
<u>AWS::EFS::AccessPoint</u>	 Sì	 Sì	 Sì
<u>AWS::EFS::FileSystem</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EFS::MountTarget</u>	 Sì	 Sì	 Sì
<u>AWS::EKS::AccessEntry</u>	 Sì	 Sì	 No
<u>AWS::EKS::Addon</u>	 Sì	 Sì	 Sì
<u>AWS::EKS::Cluster</u>	 Sì	 No	 Sì
<u>AWS::EKS::FargateProfile</u>	 Sì	 Sì	 Sì
<u>AWS::EKS::IdentityProviderConfig</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EKS::Nodegroup</u>	 Sì	 No	 Sì
<u>AWS::EKS::PodIdentityAssociation</u>	 Sì	 Sì	 No
<u>AWS::EMR::SecurityConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::EMR::Step</u>	 Sì	 No	 No
<u>AWS::EMR::Studio</u>	 Sì	 Sì	 Sì
<u>AWS::EMR::StudioSessionMapping</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EMR::WALWorkspace</u>	 Sì	 Sì	 No
<u>AWS::EMRContainers::VirtualCluster</u>	 Sì	 Sì	 No
<u>AWS::EMRServerless::Application</u>	 Sì	 Sì	 Sì
<u>AWS::EVS::Environment</u>	 Sì	 Sì	 No
<u>AWS::ElastiCache::GlobalReplicationGroup</u>	 Sì	 Sì	 No
<u>AWS::ElastiCache::ParameterGroup</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ElastiCache::ServerlessCache</u>	 Sì	 Sì	 No
<u>AWS::ElastiCache::SubnetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::ElastiCache::User</u>	 Sì	 Sì	 Sì
<u>AWS::ElastiCache::UserGroup</u>	 Sì	 Sì	 Sì
<u>AWS::ElasticBeanstalk::Application</u>	 Sì	 Sì	 Sì
<u>AWS::ElasticBeanstalk::ApplicationVersion</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ElasticBeanstalk::Configuration Template</u>	 Sì	 Sì	 Sì
<u>AWS::ElasticBeanstalk::Environment</u>	 Sì	 No	 No
<u>AWS::ElasticLoadBalancingV2::Listene r</u>	 Sì	 Sì	 Sì
<u>AWS::ElasticLoadBalancingV2::Listene rRule</u>	 Sì	 No	 Sì
<u>AWS::ElasticLoadBalancingV2::LoadBal ancer</u>	 Sì	 Sì	 Sì
<u>AWS::ElasticLoadBalancingV2::TargetG roup</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ElasticLoadBalancingV2::TrustStore</u>	 Sì	 Sì	 No
<u>AWS::ElasticLoadBalancingV2::TrustStoreRevocation</u>	 Sì	 Sì	 No
<u>AWS::EntityResolution::IdMappingWorkflow</u>	 Sì	 Sì	 Sì
<u>AWS::EntityResolution::IdNamespace</u>	 Sì	 Sì	 No
<u>AWS::EntityResolution::MatchingWorkflow</u>	 Sì	 Sì	 Sì
<u>AWS::EntityResolution::PolicyStatement</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::EntityResolution::SchemaMapping</u>	 Sì	 Sì	 Sì
<u>AWS::EventSchemas::Discoverer</u>	 Sì	 Sì	 No
<u>AWS::EventSchemas::Registry</u>	 Sì	 Sì	 No
<u>AWS::EventSchemas::RegistryPolicy</u>	 Sì	 Sì	 No
<u>AWS::EventSchemas::Schema</u>	 Sì	 Sì	 No
<u>AWS::Events::ApiDestination</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Events::Archive</u>	 Sì	 Sì	 Sì
<u>AWS::Events::Connection</u>	 Sì	 Sì	 No
<u>AWS::Events::Endpoint</u>	 Sì	 Sì	 Sì
<u>AWS::Events::EventBus</u>	 Sì	 Sì	 Sì
<u>AWS::Events::Rule</u>	 Sì	 Sì	 Sì
<u>AWS::Evidently::Experiment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Evidently::Feature</u>	 Sì	 No	 No
<u>AWS::Evidently::Launch</u>	 Sì	 Sì	 No
<u>AWS::Evidently::Project</u>	 Sì	 Sì	 No
<u>AWS::Evidently::Segment</u>	 Sì	 Sì	 No
<u>AWS::FIS::ExperimentTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::FIS::TargetAccountConfiguration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::FMS::NotificationChannel</u>	 Sì	 Sì	 No
<u>AWS::FMS::Policy</u>	 Sì	 No	 No
<u>AWS::FMS::ResourceSet</u>	 Sì	 Sì	 No
<u>AWS::FSx::DataRepositoryAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::FSx::S3AccessPointAttachment</u>	 Sì	 Sì	 No
<u>AWS::FinSpace::Environment</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Forecast::Dataset</u>	 Sì	 Sì	 No
<u>AWS::Forecast::DatasetGroup</u>	 Sì	 Sì	 No
<u>AWS::FraudDetector::Detector</u>	 Sì	 Sì	 Sì
<u>AWS::FraudDetector::EntityType</u>	 Sì	 Sì	 Sì
<u>AWS::FraudDetector::EventType</u>	 Sì	 Sì	 Sì
<u>AWS::FraudDetector::Label</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::FraudDetector::List</u>	 Sì	 Sì	 Sì
<u>AWS::FraudDetector::Outcome</u>	 Sì	 Sì	 Sì
<u>AWS::FraudDetector::Variable</u>	 Sì	 Sì	 Sì
<u>AWS::GameLift::Alias</u>	 Sì	 Sì	 Sì
<u>AWS::GameLift::Build</u>	 Sì	 Sì	 Sì
<u>AWS::GameLift::ContainerFleet</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::GameLift::ContainerGroupDefinit ion</u>	 Sì	 Sì	 No
<u>AWS::GameLift::Fleet</u>	 Sì	 Sì	 Sì
<u>AWS::GameLift::GameServerGroup</u>	 Sì	 Sì	 No
<u>AWS::GameLift::GameSessionQueue</u>	 Sì	 Sì	 No
<u>AWS::GameLift::Location</u>	 Sì	 Sì	 No
<u>AWS::GameLift::MatchmakingConfigurat ion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::GameLift::MatchmakingRuleSet</u>	 Sì	 Sì	 No
<u>AWS::GameLift::Script</u>	 Sì	 Sì	 No
<u>AWS::GameLiftStreams::Application</u>	 Sì	 Sì	 No
<u>AWS::GameLiftStreams::StreamGroup</u>	 Sì	 Sì	 No
<u>AWS::GlobalAccelerator::Accelerator</u>	 Sì	 Sì	 Sì
<u>AWS::GlobalAccelerator::CrossAccount Attachment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::GlobalAccelerator::EndpointGroup</u>	 Sì	 Sì	 Sì
<u>AWS::GlobalAccelerator::Listener</u>	 Sì	 Sì	 Sì
<u>AWS::Glue::Crawler</u>	 Sì	 Sì	 No
<u>AWS::Glue::Database</u>	 Sì	 Sì	 No
<u>AWS::Glue::Job</u>	 Sì	 Sì	 No
<u>AWS::Glue::Registry</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Glue::Schema</u>	 Sì	 Sì	 Sì
<u>AWS::Glue::SchemaVersion</u>	 Sì	 Sì	 Sì
<u>AWS::Glue::SchemaVersionMetadata</u>	 Sì	 Sì	 Sì
<u>AWS::Glue::Trigger</u>	 Sì	 Sì	 No
<u>AWS::Glue::UsageProfile</u>	 Sì	 Sì	 No
<u>AWS::Grafana::Workspace</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::GreengrassV2::ComponentVersion	 Sì	 Sì	 No
AWS::GreengrassV2::Deployment	 Sì	 Sì	 Sì
AWS::GroundStation::Config	 Sì	 Sì	 Sì
AWS::GroundStation::DataflowEndpoint Group	 Sì	 Sì	 Sì
AWS::GroundStation::MissionProfile	 Sì	 Sì	 Sì
AWS::GuardDuty::Detector	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::GuardDuty::Filter</u>	 Sì	 Sì	 No
<u>AWS::GuardDuty::IPSet</u>	 Sì	 Sì	 No
<u>AWS::GuardDuty::MalwareProtectionPla n</u>	 Sì	 Sì	 No
<u>AWS::GuardDuty::Master</u>	 Sì	 Sì	 No
<u>AWS::GuardDuty::Member</u>	 Sì	 Sì	 No
<u>AWS::GuardDuty::PublishingDestinatio n</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::GuardDuty::ThreatIntelSet	 Sì	 Sì	 No
AWS::HealthImaging::Datastore	 Sì	 Sì	 Sì
AWS::HealthLake::FHIRDatastore	 Sì	 Sì	 Sì
AWS::IAM::Group	 Sì	 Sì	 Sì
AWS::IAM::GroupPolicy	 Sì	 Sì	 No
AWS::IAM::InstanceProfile	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::IAM::ManagedPolicy	 Sì	 Sì	 Sì
AWS::IAM::OIDCProvider	 Sì	 Sì	 Sì
AWS::IAM::Role	 Sì	 Sì	 Sì
AWS::IAM::RolePolicy	 Sì	 Sì	 No
AWS::IAM::SAMLProvider	 Sì	 Sì	 Sì
AWS::IAM::ServerCertificate	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IAM::ServiceLinkedRole</u>	 Sì	 Sì	 No
<u>AWS::IAM::User</u>	 Sì	 Sì	 Sì
<u>AWS::IAM::UserPolicy</u>	 Sì	 Sì	 No
<u>AWS::IAM::VirtualMFADevice</u>	 Sì	 Sì	 No
<u>AWS::IVS::Channel</u>	 Sì	 Sì	 Sì
<u>AWS::IVS::EncoderConfiguration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IVS::IngestConfiguration</u>	 Sì	 Sì	 No
<u>AWS::IVS::PlaybackKeyPair</u>	 Sì	 Sì	 Sì
<u>AWS::IVS::PlaybackRestrictionPolicy</u>	 Sì	 Sì	 No
<u>AWS::IVS::PublicKey</u>	 Sì	 Sì	 No
<u>AWS::IVS::RecordingConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::IVS::Stage</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IVS::StorageConfiguration</u>	 Sì	 Sì	 No
<u>AWS::IVS::StreamKey</u>	 Sì	 Sì	 No
<u>AWS::IVSChat::LoggingConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::IVSChat::Room</u>	 Sì	 Sì	 Sì
<u>AWS::IdentityStore::Group</u>	 Sì	 Sì	 Sì
<u>AWS::IdentityStore::GroupMembership</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ImageBuilder::Component</u>	 Sì	 Sì	 Sì
<u>AWS::ImageBuilder::ContainerRecipe</u>	 Sì	 Sì	 No
<u>AWS::ImageBuilder::DistributionConfi guration</u>	 Sì	 Sì	 Sì
<u>AWS::ImageBuilder::Image</u>	 Sì	 Sì	 Sì
<u>AWS::ImageBuilder::ImagePipeline</u>	 Sì	 Sì	 Sì
<u>AWS::ImageBuilder::ImageRecipe</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ImageBuilder::InfrastructureCon figuration</u>	 Sì	 Sì	 Sì
<u>AWS::ImageBuilder::LifecyclePolicy</u>	 Sì	 Sì	 No
<u>AWS::ImageBuilder::Workflow</u>	 Sì	 Sì	 No
<u>AWS::Inspector::AssessmentTarget</u>	 Sì	 Sì	 Sì
<u>AWS::Inspector::AssessmentTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::Inspector::ResourceGroup</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::InspectorV2::CisScanConfigurati on</u>	 Sì	 Sì	 No
<u>AWS::InspectorV2::Filter</u>	 Sì	 Sì	 No
<u>AWS::InternetMonitor::Monitor</u>	 Sì	 Sì	 Sì
<u>AWS::Invoicing::InvoiceUnit</u>	 Sì	 Sì	 No
<u>AWS::IoT::AccountAuditConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::Authorizer</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT::BillingGroup</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::CACertificate</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::Certificate</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::CertificateProvider</u>	 Sì	 Sì	 No
<u>AWS::IoT::Command</u>	 Sì	 Sì	 No
<u>AWS::IoT::CustomMetric</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT::Dimension</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::DomainConfiguration</u>	 Sì	 Sì	 No
<u>AWS::IoT::FleetMetric</u>	 Sì	 Sì	 No
<u>AWS::IoT::JobTemplate</u>	 Sì	 Sì	 No
<u>AWS::IoT::Logging</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::MitigationAction</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT::Policy</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::ProvisioningTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::ResourceSpecificLogging</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::RoleAlias</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::ScheduledAudit</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::SecurityProfile</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT::SoftwarePackage</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::SoftwarePackageVersion</u>	 Sì	 Sì	 No
<u>AWS::IoT::Thing</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::ThingGroup</u>	 Sì	 Sì	 Sì
<u>AWS::IoT::ThingType</u>	 Sì	 Sì	 No
<u>AWS::IoT::TopicRule</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT::TopicRuleDestination</u>	 Sì	 Sì	 Sì
<u>AWS::IoTAnalytics::Channel</u>	 Sì	 Sì	 Sì
<u>AWS::IoTAnalytics::Dataset</u>	 Sì	 Sì	 Sì
<u>AWS::IoTAnalytics::Datastore</u>	 Sì	 Sì	 Sì
<u>AWS::IoTAnalytics::Pipeline</u>	 Sì	 Sì	 Sì
<u>AWS::IoTCoreDeviceAdvisor::SuiteDefi nition</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoTEvents::AlarmModel</u>	 Sì	 Sì	 Sì
<u>AWS::IoTEvents::DetectorModel</u>	 Sì	 Sì	 Sì
<u>AWS::IoTEvents::Input</u>	 Sì	 Sì	 Sì
<u>AWS::IoTFleetHub::Application</u>	 Sì	 Sì	 Sì
<u>AWS::IoTSiteWise::AccessPolicy</u>	 Sì	 Sì	 No
<u>AWS::IoTSiteWise::Asset</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoTSiteWise::AssetModel</u>	 Sì	 Sì	 Sì
<u>AWS::IoTSiteWise::Dashboard</u>	 Sì	 Sì	 No
<u>AWS::IoTSiteWise::Dataset</u>	 Sì	 Sì	 No
<u>AWS::IoTSiteWise::Gateway</u>	 Sì	 Sì	 Sì
<u>AWS::IoTSiteWise::Portal</u>	 Sì	 Sì	 No
<u>AWS::IoTSiteWise::Project</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoT TwinMaker::ComponentType</u>	 Sì	 Sì	 Sì
<u>AWS::IoT TwinMaker::Entity</u>	 Sì	 Sì	 Sì
<u>AWS::IoT TwinMaker::Scene</u>	 Sì	 Sì	 Sì
<u>AWS::IoT TwinMaker::SyncJob</u>	 Sì	 Sì	 Sì
<u>AWS::IoT TwinMaker::Workspace</u>	 Sì	 Sì	 Sì
<u>AWS::IoT Wireless::Destination</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoTWireless::DeviceProfile</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::FuotaTask</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::MulticastGroup</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::NetworkAnalyzerCon figuration</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::ServiceProfile</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::TaskDefinition</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::IoTWireless::WirelessDevice</u>	 Sì	 Sì	 Sì
<u>AWS::IoTWireless::WirelessGateway</u>	 Sì	 Sì	 Sì
<u>AWS::KMS::Alias</u>	 Sì	 No	 Sì
<u>AWS::KMS::Key</u>	 Sì	 No	 Sì
<u>AWS::KMS::ReplicaKey</u>	 Sì	 No	 Sì
<u>AWS::KafkaConnect::Connector</u>	 Sì	 No	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::KafkaConnect::CustomPlugin</u>	 Sì	 Sì	 No
<u>AWS::KafkaConnect::WorkerConfigurati on</u>	 Sì	 Sì	 No
<u>AWS::Kendra::DataSource</u>	 Sì	 Sì	 Sì
<u>AWS::Kendra::Faq</u>	 Sì	 Sì	 Sì
<u>AWS::Kendra::Index</u>	 Sì	 Sì	 Sì
<u>AWS::KendraRanking::ExecutionPlan</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Kinesis::ResourcePolicy</u>	 Sì	 Sì	 No
<u>AWS::Kinesis::Stream</u>	 Sì	 Sì	 Sì
<u>AWS::KinesisAnalyticsV2::Application</u>	 Sì	 Sì	 No
<u>AWS::KinesisFirehose::DeliveryStream</u>	 Sì	 No	 No
<u>AWS::KinesisVideo::SignalingChannel</u>	 Sì	 Sì	 No
<u>AWS::KinesisVideo::Stream</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::LakeFormation::DataCellsFilter</u>	 Sì	 Sì	 No
<u>AWS::LakeFormation::PrincipalPermissions</u>	 Sì	 Sì	 No
<u>AWS::LakeFormation::Tag</u>	 Sì	 Sì	 No
<u>AWS::LakeFormation::TagAssociation</u>	 Sì	 Sì	 No
<u>AWS::Lambda::Alias</u>	 Sì	 Sì	 No
<u>AWS::Lambda::CodeSigningConfig</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Lambda::EventInvokeConfig</u>	 Sì	 Sì	 No
<u>AWS::Lambda::EventSourceMapping</u>	 Sì	 Sì	 Sì
<u>AWS::Lambda::Function</u>	 Sì	 Sì	 Sì
<u>AWS::Lambda::LayerVersion</u>	 Sì	 Sì	 No
<u>AWS::Lambda::LayerVersionPermission</u>	 Sì	 Sì	 Sì
<u>AWS::Lambda::Permission</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Lambda::Url	 Sì	 Sì	 Sì
AWS::Lambda::Version	 Sì	 Sì	 Sì
AWS::LaunchWizard::Deployment	 Sì	 Sì	 No
AWS::Lex::Bot	 Sì	 Sì	 No
AWS::Lex::BotAlias	 Sì	 Sì	 No
AWS::Lex::BotVersion	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Lex::ResourcePolicy</u>	 Sì	 Sì	 No
<u>AWS::LicenseManager::Grant</u>	 Sì	 Sì	 No
<u>AWS::LicenseManager::License</u>	 Sì	 Sì	 No
<u>AWS::Lightsail::Alarm</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::Bucket</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::Certificate</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Lightsail::Container</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::Database</u>	 Sì	 Sì	 No
<u>AWS::Lightsail::Disk</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::Instance</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::InstanceSnapshot</u>	 Sì	 Sì	 No
<u>AWS::Lightsail::LoadBalancer</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Lightsail::LoadBalancerTlsCertificate</u>	 Sì	 Sì	 Sì
<u>AWS::Lightsail::StaticIp</u>	 Sì	 Sì	 Sì
<u>AWS::Location::APIKey</u>	 Sì	 Sì	 No
<u>AWS::Location::GeofenceCollection</u>	 Sì	 Sì	 Sì
<u>AWS::Location::Map</u>	 Sì	 Sì	 Sì
<u>AWS::Location::PlaceIndex</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Location::RouteCalculator</u>	 Sì	 Sì	 Sì
<u>AWS::Location::Tracker</u>	 Sì	 Sì	 Sì
<u>AWS::Location::TrackerConsumer</u>	 Sì	 Sì	 Sì
<u>AWS::Logs::AccountPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::Logs::Delivery</u>	 Sì	 Sì	 No
<u>AWS::Logs::DeliveryDestination</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Logs::DeliverySource</u>	 Sì	 Sì	 No
<u>AWS::Logs::Destination</u>	 Sì	 Sì	 Sì
<u>AWS::Logs::Integration</u>	 Sì	 Sì	 No
<u>AWS::Logs::LogAnomalyDetector</u>	 Sì	 Sì	 No
<u>AWS::Logs::LogGroup</u>	 Sì	 Sì	 Sì
<u>AWS::Logs::LogStream</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::Logs::MetricFilter	 Sì	 Sì	 Sì
AWS::Logs::QueryDefinition	 Sì	 Sì	 No
AWS::Logs::ResourcePolicy	 Sì	 Sì	 Sì
AWS::Logs::SubscriptionFilter	 Sì	 Sì	 Sì
AWS::Logs::Transformer	 Sì	 Sì	 No
AWS::LookoutMetrics::Alert	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::LookoutMetrics::AnomalyDetector</u>	 Sì	 Sì	 No
<u>AWS::LookoutVision::Project</u>	 Sì	 Sì	 Sì
<u>AWS::M2::Application</u>	 Sì	 Sì	 No
<u>AWS::M2::Deployment</u>	 Sì	 Sì	 No
<u>AWS::M2::Environment</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::BatchScramSecret</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MSK::Cluster</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::ClusterPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::Configuration</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::Replicator</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::ServerlessCluster</u>	 Sì	 Sì	 Sì
<u>AWS::MSK::VpcConnection</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MWAA::Environment</u>	 Sì	 Sì	 No
<u>AWS::Macie::AllowList</u>	 Sì	 Sì	 No
<u>AWS::Macie::CustomDataIdentifier</u>	 Sì	 Sì	 No
<u>AWS::Macie::FindingsFilter</u>	 Sì	 Sì	 No
<u>AWS::Macie::Session</u>	 Sì	 Sì	 Sì
<u>AWS::MediaConnect::Bridge</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaConnect::BridgeOutput</u>	 Sì	 Sì	 No
<u>AWS::MediaConnect::BridgeSource</u>	 Sì	 Sì	 No
<u>AWS::MediaConnect::Flow</u>	 Sì	 Sì	 No
<u>AWS::MediaConnect::FlowEntitlement</u>	 Sì	 Sì	 No
<u>AWS::MediaConnect::FlowOutput</u>	 Sì	 Sì	 No
<u>AWS::MediaConnect::FlowSource</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaConnect::FlowVpcInterface</u>	 Sì	 Sì	 Sì
<u>AWS::MediaConnect::Gateway</u>	 Sì	 Sì	 Sì
<u>AWS::MediaLive::ChannelPlacementGroup</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::CloudWatchAlarmTemplate</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::CloudWatchAlarmTemplateGroup</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::Cluster</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaLive::EventBridgeRuleTemplate</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::EventBridgeRuleTemplateGroup</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::Multiplex</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::Multiplexprogram</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::Network</u>	 Sì	 Sì	 No
<u>AWS::MediaLive::SdiSource</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaLive::SignalMap</u>	 Sì	 Sì	 No
<u>AWS::MediaPackage::Asset</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackage::Channel</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackage::OriginEndpoint</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackage::PackagingConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackage::PackagingGroup</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaPackageV2::Channel</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackageV2::ChannelGroup</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackageV2::ChannelPolicy</u>	 Sì	 Sì	 No
<u>AWS::MediaPackageV2::OriginEndpoint</u>	 Sì	 Sì	 Sì
<u>AWS::MediaPackageV2::OriginEndpointPolicy</u>	 Sì	 Sì	 No
<u>AWS::MediaTailor::Channel</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MediaTailor::ChannelPolicy</u>	 Sì	 Sì	 No
<u>AWS::MediaTailor::LiveSource</u>	 Sì	 Sì	 Sì
<u>AWS::MediaTailor::PlaybackConfigurat ion</u>	 Sì	 Sì	 No
<u>AWS::MediaTailor::SourceLocation</u>	 Sì	 Sì	 Sì
<u>AWS::MediaTailor::VodSource</u>	 Sì	 Sì	 Sì
<u>AWS::MemoryDB::ACL</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::MemoryDB::Cluster</u>	 Sì	 Sì	 Sì
<u>AWS::MemoryDB::MultiRegionCluster</u>	 Sì	 Sì	 No
<u>AWS::MemoryDB::ParameterGroup</u>	 Sì	 Sì	 Sì
<u>AWS::MemoryDB::SubnetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::MemoryDB::User</u>	 Sì	 Sì	 Sì
<u>AWS::Neptune::DBCluster</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Neptune::DBClusterParameterGroup</u>	 Sì	 Sì	 No
<u>AWS::Neptune::DBInstance</u>	 Sì	 Sì	 No
<u>AWS::Neptune::DBParameterGroup</u>	 Sì	 Sì	 No
<u>AWS::Neptune::DBSubnetGroup</u>	 Sì	 Sì	 No
<u>AWS::NeptuneGraph::Graph</u>	 Sì	 Sì	 No
<u>AWS::NeptuneGraph::PrivateGraphEndpoint</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::NetworkFirewall::Firewall</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkFirewall::FirewallPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkFirewall::LoggingConfigu ration</u>	 Sì	 Sì	 No
<u>AWS::NetworkFirewall::RuleGroup</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkFirewall::TLSInspectionC onfiguration</u>	 Sì	 Sì	 No
<u>AWS::NetworkFirewall::VpcEndpointAss ociation</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::NetworkManager::ConnectAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::ConnectPeer</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::CoreNetwork</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::CustomerGatewayAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::Device</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::DirectConnectGatewayAttachment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::NetworkManager::GlobalNetwork</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::Link</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::LinkAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::Site</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::SiteToSiteVpnAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::TransitGatewayPeering</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::NetworkManager::TransitGatewayRegistration</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::TransitGatewayRouteTableAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::NetworkManager::VpcAttachment</u>	 Sì	 Sì	 Sì
<u>AWS::OSIS::Pipeline</u>	 Sì	 Sì	 Sì
<u>AWS::Oam::Link</u>	 Sì	 Sì	 Sì
<u>AWS::Oam::Sink</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Omics::AnnotationStore</u>	 Sì	 Sì	 Sì
<u>AWS::Omics::ReferenceStore</u>	 Sì	 Sì	 Sì
<u>AWS::Omics::RunGroup</u>	 Sì	 Sì	 Sì
<u>AWS::Omics::SequenceStore</u>	 Sì	 Sì	 Sì
<u>AWS::Omics::VariantStore</u>	 Sì	 Sì	 Sì
<u>AWS::Omics::Workflow</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Omics::WorkflowVersion</u>	 Sì	 Sì	 No
<u>AWS::OpenSearchServerless::AccessPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::OpenSearchServerless::Collection</u>	 Sì	 Sì	 No
<u>AWS::OpenSearchServerless::Index</u>	 Sì	 Sì	 No
<u>AWS::OpenSearchServerless::LifecyclePolicy</u>	 Sì	 Sì	 No
<u>AWS::OpenSearchServerless::SecurityConfig</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::OpenSearchServerless::SecurityPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::OpenSearchServerless::VpcEndpoint</u>	 Sì	 Sì	 Sì
<u>AWS::OpenSearchService::Application</u>	 Sì	 Sì	 No
<u>AWS::OpenSearchService::Domain</u>	 Sì	 Sì	 No
<u>AWS::Organizations::Account</u>	 Sì	 Sì	 Sì
<u>AWS::Organizations::Organization</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Organizations::OrganizationalUnit</u>	 Sì	 Sì	 Sì
<u>AWS::Organizations::Policy</u>	 Sì	 Sì	 Sì
<u>AWS::Organizations::ResourcePolicy</u>	 Sì	 Sì	 Sì
<u>AWS::PCAConectorAD::Connector</u>	 Sì	 Sì	 Sì
<u>AWS::PCAConectorAD::DirectoryRegistration</u>	 Sì	 Sì	 Sì
<u>AWS::PCAConectorAD::ServicePrincipalName</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::PCAConnectorAD::Template</u>	 Sì	 Sì	 Sì
<u>AWS::PCAConnectorAD::TemplateGroupAccessControlEntry</u>	 Sì	 Sì	 Sì
<u>AWS::PCAConnectorSCEP::Challenge</u>	 Sì	 Sì	 No
<u>AWS::PCAConnectorSCEP::Connector</u>	 Sì	 Sì	 No
<u>AWS::PCS::Cluster</u>	 Sì	 Sì	 No
<u>AWS::PCS::ComputeNodeGroup</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::PCS::Queue</u>	 Sì	 Sì	 No
<u>AWS::Panorama::ApplicationInstance</u>	 Sì	 Sì	 Sì
<u>AWS::Panorama::Package</u>	 Sì	 Sì	 Sì
<u>AWS::Panorama::PackageVersion</u>	 Sì	 Sì	 No
<u>AWS::PaymentCryptography::Alias</u>	 Sì	 Sì	 No
<u>AWS::PaymentCryptography::Key</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Personalize::Dataset</u>	 Sì	 Sì	 Sì
<u>AWS::Personalize::DatasetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::Personalize::Schema</u>	 Sì	 Sì	 Sì
<u>AWS::Personalize::Solution</u>	 Sì	 Sì	 No
<u>AWS::Pinpoint::InAppTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::Pipes::Pipe</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Proton::EnvironmentAccountConne ction</u>	 Sì	 Sì	 Sì
<u>AWS::Proton::EnvironmentTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::Proton::ServiceTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::QBusiness::Application</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::DataAccessor</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::DataSource</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::QBusiness::Index</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::Permission</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::Plugin</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::Retriever</u>	 Sì	 Sì	 No
<u>AWS::QBusiness::WebExperience</u>	 Sì	 Sì	 No
<u>AWS::QLDB::Stream</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::QuickSight::Analysis</u>	 Sì	 Sì	 No
<u>AWS::QuickSight::CustomPermissions</u>	 Sì	 Sì	 No
<u>AWS::QuickSight::Dashboard</u>	 Sì	 Sì	 No
<u>AWS::QuickSight::DataSet</u>	 Sì	 Sì	 Sì
<u>AWS::QuickSight::DataSource</u>	 Sì	 Sì	 Sì
<u>AWS::QuickSight::Folder</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::QuickSight::RefreshSchedule</u>	 Sì	 Sì	 Sì
<u>AWS::QuickSight::Template</u>	 Sì	 Sì	 No
<u>AWS::QuickSight::Theme</u>	 Sì	 Sì	 No
<u>AWS::QuickSight::Topic</u>	 Sì	 Sì	 Sì
<u>AWS::QuickSight::VPCConnection</u>	 Sì	 Sì	 Sì
<u>AWS::RAM::Permission</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::RAM::ResourceShare</u>	 Sì	 Sì	 No
<u>AWS::RDS::CustomDBEngineVersion</u>	 Sì	 Sì	 No
<u>AWS::RDS::DBCluster</u>	 Sì	 Sì	 Sì
<u>AWS::RDS::DBClusterParameterGroup</u>	 Sì	 Sì	 No
<u>AWS::RDS::DBInstance</u>	 Sì	 No	 Sì
<u>AWS::RDS::DBParameterGroup</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::RDS::DBProxy</u>	 Sì	 Sì	 Sì
<u>AWS::RDS::DBProxyEndpoint</u>	 Sì	 Sì	 Sì
<u>AWS::RDS::DBProxyTargetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::RDS::DBShardGroup</u>	 Sì	 Sì	 No
<u>AWS::RDS::DBSubnetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::RDS::EventSubscription</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::RDS::GlobalCluster	 Sì	 Sì	 Sì
AWS::RDS::Integration	 Sì	 Sì	 No
AWS::RDS::OptionGroup	 Sì	 Sì	 Sì
AWS::RUM::AppMonitor	 Sì	 Sì	 Sì
AWS::Rbin::Rule	 Sì	 Sì	 No
AWS::Redshift::Cluster	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Redshift::ClusterParameterGroup</u>	 Sì	 Sì	 No
<u>AWS::Redshift::ClusterSubnetGroup</u>	 Sì	 Sì	 No
<u>AWS::Redshift::EndpointAccess</u>	 Sì	 Sì	 Sì
<u>AWS::Redshift::EndpointAuthorization</u>	 Sì	 Sì	 Sì
<u>AWS::Redshift::EventSubscription</u>	 Sì	 Sì	 No
<u>AWS::Redshift::Integration</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Redshift::ScheduledAction</u>	 Sì	 Sì	 Sì
<u>AWS::RedshiftServerless::Namespace</u>	 Sì	 Sì	 No
<u>AWS::RedshiftServerless::Snapshot</u>	 Sì	 Sì	 No
<u>AWS::RedshiftServerless::Workgroup</u>	 Sì	 Sì	 No
<u>AWS::RefactorSpaces::Application</u>	 Sì	 Sì	 Sì
<u>AWS::RefactorSpaces::Environment</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::RefactorSpaces::Route</u>	 Sì	 Sì	 Sì
<u>AWS::RefactorSpaces::Service</u>	 Sì	 Sì	 Sì
<u>AWS::Rekognition::Collection</u>	 Sì	 Sì	 Sì
<u>AWS::Rekognition::Project</u>	 Sì	 Sì	 Sì
<u>AWS::Rekognition::StreamProcessor</u>	 Sì	 Sì	 Sì
<u>AWS::ResilienceHub::App</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ResilienceHub::ResiliencyPolicy</u>	 Sì	 Sì	 Sì
<u>AWS::ResourceExplorer2::DefaultViewAssociation</u>	 Sì	 Sì	 No
<u>AWS::ResourceExplorer2::Index</u>	 Sì	 Sì	 Sì
<u>AWS::ResourceExplorer2::View</u>	 Sì	 Sì	 Sì
<u>AWS::ResourceGroups::Group</u>	 Sì	 Sì	 Sì
<u>AWS::ResourceGroups::TagSyncTask</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::RoboMaker::Fleet</u>	 Sì	 Sì	 No
<u>AWS::RoboMaker::Robot</u>	 Sì	 Sì	 No
<u>AWS::RoboMaker::RobotApplication</u>	 Sì	 Sì	 No
<u>AWS::RoboMaker::RobotApplicationVersion</u>	 Sì	 Sì	 No
<u>AWS::RoboMaker::SimulationApplication</u>	 Sì	 Sì	 No
<u>AWS::RoboMaker::SimulationApplicationVersion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
AWS::RolesAnywhere::CRL	 Sì	 Sì	 Sì
AWS::RolesAnywhere::Profile	 Sì	 Sì	 Sì
AWS::RolesAnywhere::TrustAnchor	 Sì	 Sì	 No
AWS::Route53::CidrCollection	 Sì	 Sì	 Sì
AWS::Route53::DNSSEC	 Sì	 Sì	 Sì
AWS::Route53::HealthCheck	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Route53::HostedZone</u>	 Sì	 Sì	 Sì
<u>AWS::Route53::KeySigningKey</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Profiles::Profile</u>	 Sì	 Sì	 No
<u>AWS::Route53Profiles::ProfileAssocia tion</u>	 Sì	 Sì	 No
<u>AWS::Route53Profiles::ProfileResourc eAssociation</u>	 Sì	 Sì	 No
<u>AWS::Route53RecoveryControl::Cluster</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Route53RecoveryControl::ControlPanel</u>	 Sì	 Sì	 Sì
<u>AWS::Route53RecoveryControl::RoutingControl</u>	 Sì	 Sì	 Sì
<u>AWS::Route53RecoveryControl::SafetyRule</u>	 Sì	 Sì	 Sì
<u>AWS::Route53RecoveryReadiness::Cell</u>	 Sì	 Sì	 Sì
<u>AWS::Route53RecoveryReadiness::ReadinessCheck</u>	 Sì	 Sì	 Sì
<u>AWS::Route53RecoveryReadiness::RecoveryGroup</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Route53RecoveryReadiness::ResourceSet</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::FirewallDomainList</u>	 Sì	 Sì	 No
<u>AWS::Route53Resolver::FirewallRuleGroup</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::FirewallRuleGroupAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::OutpostResolver</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::ResolverConfig</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Route53Resolver::ResolverDNSSEC Config</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::ResolverEndpoi nt</u>	 Sì	 Sì	 No
<u>AWS::Route53Resolver::ResolverQueryL oggingConfig</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::ResolverQueryL oggingConfigAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::Route53Resolver::ResolverRule</u>	 Sì	 Sì	 No
<u>AWS::Route53Resolver::ResolverRuleAs sociation</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::S3::AccessGrant</u>	 Sì	 Sì	 No
<u>AWS::S3::AccessGrantsInstance</u>	 Sì	 Sì	 No
<u>AWS::S3::AccessGrantsLocation</u>	 Sì	 Sì	 No
<u>AWS::S3::AccessPoint</u>	 Sì	 Sì	 Sì
<u>AWS::S3::Bucket</u>	 Sì	 Sì	 Sì
<u>AWS::S3::BucketPolicy</u>	 Sì	 No	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::S3::MultiRegionAccessPoint</u>	 Sì	 Sì	 Sì
<u>AWS::S3::MultiRegionAccessPointPolicy</u>	 Sì	 No	 No
<u>AWS::S3::StorageLens</u>	 Sì	 Sì	 Sì
<u>AWS::S3::StorageLensGroup</u>	 Sì	 Sì	 No
<u>AWS::S3Express::AccessPoint</u>	 Sì	 Sì	 No
<u>AWS::S3Express::BucketPolicy</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::S3Express::DirectoryBucket</u>	 Sì	 Sì	 No
<u>AWS::S3ObjectLambda::AccessPoint</u>	 Sì	 Sì	 Sì
<u>AWS::S3ObjectLambda::AccessPointPolicy</u>	 Sì	 Sì	 No
<u>AWS::S3Outposts::AccessPoint</u>	 Sì	 Sì	 Sì
<u>AWS::S3Outposts::Bucket</u>	 Sì	 Sì	 Sì
<u>AWS::S3Outposts::BucketPolicy</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::S3Outposts::Endpoint</u>	 Sì	 Sì	 Sì
<u>AWS::S3Tables::Namespace</u>	 Sì	 Sì	 No
<u>AWS::S3Tables::TableBucket</u>	 Sì	 Sì	 No
<u>AWS::S3Tables::TableBucketPolicy</u>	 Sì	 Sì	 No
<u>AWS::SES::ConfigurationSet</u>	 Sì	 Sì	 No
<u>AWS::SES::ConfigurationSetEventDesti nation</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SES::ContactList</u>	 Sì	 Sì	 No
<u>AWS::SES::DedicatedIpPool</u>	 Sì	 Sì	 Sì
<u>AWS::SES::EmailIdentity</u>	 Sì	 Sì	 Sì
<u>AWS::SES::MailManagerAddonInstance</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerAddonSubscripti on</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerAddressList</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SES::MailManagerArchive</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerIngressPoint</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerRelay</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerRuleSet</u>	 Sì	 Sì	 No
<u>AWS::SES::MailManagerTrafficPolicy</u>	 Sì	 Sì	 No
<u>AWS::SES::Template</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SES::VdmAttributes</u>	 Sì	 Sì	 No
<u>AWS::SNS::Subscription</u>	 Sì	 Sì	 No
<u>AWS::SNS::Topic</u>	 Sì	 Sì	 Sì
<u>AWS::SNS::TopicInlinePolicy</u>	 Sì	 Sì	 No
<u>AWS::SQS::Queue</u>	 Sì	 Sì	 Sì
<u>AWS::SQS::QueueInlinePolicy</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SSM::Association</u>	 Sì	 Sì	 Sì
<u>AWS::SSM::Document</u>	 Sì	 No	 No
<u>AWS::SSM::Parameter</u>	 Sì	 Sì	 No
<u>AWS::SSM::PatchBaseline</u>	 Sì	 Sì	 No
<u>AWS::SSM::ResourceDataSync</u>	 Sì	 Sì	 No
<u>AWS::SSM::ResourcePolicy</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SSMContacts::Contact</u>	 Sì	 Sì	 Sì
<u>AWS::SSMContacts::ContactChannel</u>	 Sì	 Sì	 Sì
<u>AWS::SSMContacts::Plan</u>	 Sì	 Sì	 No
<u>AWS::SSMContacts::Rotation</u>	 Sì	 Sì	 No
<u>AWS::SSMGuiConnect::Preferences</u>	 Sì	 Sì	 No
<u>AWS::SSMIncidents::ReplicationSet</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SSMIncidents::ResponsePlan</u>	 Sì	 Sì	 Sì
<u>AWS::SSMQuickSetup::ConfigurationManager</u>	 Sì	 Sì	 No
<u>AWS::SSO::Application</u>	 Sì	 Sì	 No
<u>AWS::SSO::ApplicationAssignment</u>	 Sì	 Sì	 No
<u>AWS::SSO::Assignment</u>	 Sì	 Sì	 No
<u>AWS::SSO::Instance</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SSO::InstanceAccessControlAttributeConfiguration</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::App</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::AppImageConfig</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::Cluster</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::DataQualityJobDefinition</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::Device</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SageMaker::DeviceFleet</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::Domain</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::Endpoint</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::FeatureGroup</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::Image</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::ImageVersion</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SageMaker::InferenceComponent</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::InferenceExperiment</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::MlflowTrackingServer</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::ModelBiasJobDefinit ion</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::ModelCard</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::ModelExplainabilityJ obDefinition</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SageMaker::ModelPackage</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::ModelPackageGroup</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::ModelQualityJobDefinition</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::MonitoringSchedule</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::PartnerApp</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::Pipeline</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SageMaker::Project</u>	 Sì	 Sì	 Sì
<u>AWS::SageMaker::Space</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::StudioLifecycleConfig</u>	 Sì	 Sì	 No
<u>AWS::SageMaker::UserProfile</u>	 Sì	 Sì	 No
<u>AWS::Scheduler::Schedule</u>	 Sì	 Sì	 Sì
<u>AWS::Scheduler::ScheduleGroup</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SecretsManager::ResourcePolicy</u>	 Sì	 No	 No
<u>AWS::SecretsManager::RotationSchedule</u>	 Sì	 Sì	 No
<u>AWS::SecretsManager::Secret</u>	 Sì	 Sì	 Sì
<u>AWS::SecretsManager::SecretTargetAttachment</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::AggregatorV2</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::AutomationRule</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SecurityHub::AutomationRuleV2</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::ConfigurationPolicy</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::DelegatedAdmin</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::FindingAggregator</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::Hub</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::HubV2</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SecurityHub::Insight</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::OrganizationConfig uration</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::PolicyAssociation</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::ProductSubscriptio n</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::SecurityControl</u>	 Sì	 Sì	 No
<u>AWS::SecurityHub::Standard</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SecurityLake::AwsLogSource</u>	 Sì	 Sì	 No
<u>AWS::SecurityLake::DataLake</u>	 Sì	 Sì	 No
<u>AWS::SecurityLake::Subscriber</u>	 Sì	 Sì	 No
<u>AWS::SecurityLake::SubscriberNotific ation</u>	 Sì	 Sì	 No
<u>AWS::ServiceCatalog::CloudFormationP rovisionedProduct</u>	 Sì	 No	 No
<u>AWS::ServiceCatalog::ServiceAction</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::ServiceCatalog::ServiceActionAs sociation</u>	 Sì	 Sì	 No
<u>AWS::ServiceCatalogAppRegistry::Appl ication</u>	 Sì	 Sì	 Sì
<u>AWS::ServiceCatalogAppRegistry::Attr ibuteGroup</u>	 Sì	 Sì	 Sì
<u>AWS::ServiceCatalogAppRegistry::Attr ibuteGroupAssociation</u>	 Sì	 Sì	 No
<u>AWS::ServiceCatalogAppRegistry::Reso urceAssociation</u>	 Sì	 No	 No
<u>AWS::Shield::DRTAccess</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Shield::ProactiveEngagement</u>	 Sì	 Sì	 No
<u>AWS::Shield::Protection</u>	 Sì	 Sì	 No
<u>AWS::Shield::ProtectionGroup</u>	 Sì	 Sì	 No
<u>AWS::Signer::ProfilePermission</u>	 Sì	 Sì	 No
<u>AWS::Signer::SigningProfile</u>	 Sì	 Sì	 Sì
<u>AWS::SimSpaceWeaver::Simulation</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::StepFunctions::Activity</u>	 Sì	 Sì	 No
<u>AWS::StepFunctions::StateMachine</u>	 Sì	 Sì	 Sì
<u>AWS::StepFunctions::StateMachineAlias</u>	 Sì	 Sì	 Sì
<u>AWS::StepFunctions::StateMachineVersion</u>	 Sì	 Sì	 Sì
<u>AWS::SupportApp::AccountAlias</u>	 Sì	 Sì	 Sì
<u>AWS::SupportApp::SlackChannelConfiguration</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::SupportApp::SlackWorkspaceConfi guration</u>	 Sì	 Sì	 Sì
<u>AWS::Synthetics::Canary</u>	 Sì	 Sì	 Sì
<u>AWS::Synthetics::Group</u>	 Sì	 Sì	 Sì
<u>AWS::SystemsManagerSAP::Application</u>	 Sì	 Sì	 No
<u>AWS::Timestream::Database</u>	 Sì	 Sì	 Sì
<u>AWS::Timestream::InfluxDBInstance</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Timestream::ScheduledQuery</u>	 Sì	 Sì	 No
<u>AWS::Timestream::Table</u>	 Sì	 Sì	 Sì
<u>AWS::Transfer::Agreement</u>	 Sì	 Sì	 Sì
<u>AWS::Transfer::Certificate</u>	 Sì	 Sì	 Sì
<u>AWS::Transfer::Connector</u>	 Sì	 Sì	 Sì
<u>AWS::Transfer::Profile</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Transfer::Server</u>	 Sì	 Sì	 No
<u>AWS::Transfer::User</u>	 Sì	 Sì	 No
<u>AWS::Transfer::WebApp</u>	 Sì	 Sì	 No
<u>AWS::Transfer::Workflow</u>	 Sì	 Sì	 Sì
<u>AWS::VerifiedPermissions::IdentitySource</u>	 Sì	 Sì	 Sì
<u>AWS::VerifiedPermissions::Policy</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::VerifiedPermissions::PolicyStore</u>	 Sì	 Sì	 Sì
<u>AWS::VerifiedPermissions::PolicyTemplate</u>	 Sì	 Sì	 Sì
<u>AWS::VoiceID::Domain</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::AccessLogSubscription</u>	 Sì	 Sì	 Sì
<u>AWS::VpcLattice::AuthPolicy</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::Listener</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::VpcLattice::ResourceConfigurati on</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::ResourceGateway</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::ResourcePolicy</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::Rule</u>	 Sì	 Sì	 Sì
<u>AWS::VpcLattice::Service</u>	 Sì	 Sì	 Sì
<u>AWS::VpcLattice::ServiceNetwork</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::VpcLattice::ServiceNetworkResourceAssociation</u>	 Sì	 Sì	 No
<u>AWS::VpcLattice::ServiceNetworkServiceAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::VpcLattice::ServiceNetworkVpcAssociation</u>	 Sì	 Sì	 Sì
<u>AWS::VpcLattice::TargetGroup</u>	 Sì	 Sì	 Sì
<u>AWS::WAFv2::IPSet</u>	 Sì	 Sì	 Sì
<u>AWS::WAFv2::LoggingConfiguration</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::WAFv2::RegexPatternSet</u>	 Sì	 Sì	 Sì
<u>AWS::WAFv2::RuleGroup</u>	 Sì	 Sì	 Sì
<u>AWS::WAFv2::WebACL</u>	 Sì	 Sì	 Sì
<u>AWS::WAFv2::WebACLAssociation</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::AIAgent</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::AIAgentVersion</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Wisdom::AIGuardrail</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::AIGuardrailVersion</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::AIPrompt</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::AIPromptVersion</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::Assistant</u>	 Sì	 Sì	 Sì
<u>AWS::Wisdom::AssistantAssociation</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::Wisdom::KnowledgeBase</u>	 Sì	 Sì	 Sì
<u>AWS::Wisdom::MessageTemplate</u>	 Sì	 Sì	 No
<u>AWS::Wisdom::MessageTemplateVersion</u>	 Sì	 Sì	 No
<u>AWS::WorkSpaces::ConnectionAlias</u>	 Sì	 Sì	 No
<u>AWS::WorkSpaces::WorkspacesPool</u>	 Sì	 Sì	 No
<u>AWS::WorkSpacesThinClient::Environment</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::WorkSpacesWeb::BrowserSettings</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::DataProtectionSettings</u>	 Sì	 Sì	 No
<u>AWS::WorkSpacesWeb::IdentityProvider</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::IpAccessSettings</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::NetworkSettings</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::Portal</u>	 Sì	 Sì	 Sì

Risorsa	Importa	Rilevamen to delle deviazioni	generatore IAC
<u>AWS::WorkSpacesWeb::TrustStore</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::UserAccessLoggingSettings</u>	 Sì	 Sì	 Sì
<u>AWS::WorkSpacesWeb::UserSettings</u>	 Sì	 Sì	 Sì
<u>AWS::XRay::Group</u>	 Sì	 Sì	 Sì
<u>AWS::XRay::ResourcePolicy</u>	 Sì	 Sì	 Sì
<u>AWS::XRay::SamplingRule</u>	 Sì	 Sì	 No

Risorsa	Importa	Rilevamento delle deviazioni	generatore IAC
AWS::XRay::TransactionSearchConfig	 Sì	 Sì	 No

Usa i link di creazione rapida per creare pile CloudFormation

I link di creazione rapida forniscono un metodo semplificato per avviare gli CloudFormation stack direttamente dalla console. URLs CloudFormation Specificando l'URL del modello, il nome dello stack e i parametri del modello come parametri di query URL, puoi precompilare un'unica pagina Create stack e accelerare la creazione dello stack. Ciò semplifica il processo di creazione degli stack riducendo sia il numero di pagine della procedura guidata sia la quantità di input richiesto dall'utente. Inoltre, ottimizza il riutilizzo dei modelli, in quanto è possibile crearne di multipli URLs che specificano valori diversi per lo stesso modello.

Formato URL

Il link di creazione rapida segue questo formato URL:

```
https://region-code.console.aws.amazon.com/cloudformation/home?region=region-code#/stacks/create/review
?templateURL=TemplateURL
&stackName=StackName
&param_parameterName=parameterValue
```

CloudFormation supporta i seguenti parametri di query URL:

URL del modello

Obbligatorio. Il `templateURL` parametro specifica l'URL del modello di stack situato in un bucket Amazon S3. Per evitare problemi di accesso con un URL S3 predefinito, assicurati di codificare l'URL.

Formati URL S3 supportati:

- `https://s3.region-code.amazonaws.com/bucket-name/template-name`
- `https://bucket-name.s3.region-code.amazonaws.com/template-name`
- `https://s3-region-code.amazonaws.com/bucket-name/template-name`(formato precedente)

Stack name (Nome stack)

Facoltativo. Utilizzate il `stackName` parametro per specificare il nome dello CloudFormation stack da creare. Il nome di uno stack può contenere solo caratteri alfanumerici (con distinzione tra lettere maiuscole e minuscole) e trattini. Deve iniziare con un carattere alfabetico e non può avere una lunghezza superiore a 128 caratteri.

Parametri del modello

Facoltativo. Per i parametri del modello di stack che non sono di tipo di NoEcho parametro, utilizzate il formato `param_parameterName` nella stringa di query URL. Il parametro URL deve includere il prefisso `param_` e il segmento nome del parametro deve corrispondere esattamente al nome del parametro nel modello. Ad esempio: `param_DBName`.

CloudFormation ignora i parametri che non esistono nel modello e tutti i parametri definiti con le relative NoEcho proprietà impostate su `true` types (in genere, nomi utente e password). I parametri URL sostituiscono i valori predefiniti specificati nel modello. Puoi includere il numero di parametri necessari.

Important

Anziché incorporare informazioni sensibili direttamente nei CloudFormation modelli, si consiglia di utilizzare parametri dinamici nel modello dello stack per fare riferimento a informazioni riservate archiviate e gestite all'esterno CloudFormation, ad esempio nel Parameter Store o. AWS Systems Manager AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

Tutti i nomi di parametro query fanno distinzione tra maiuscole e minuscole. Gli utenti possono sovrascrivere tali valori nella console prima di creare lo stack.

Esempio

L'esempio seguente si basa sul modello di esempio di [WordPress base a istanza singola](#). La stringa di query include il parametro `templateURL` e i parametri `stackName` `DBName` `InstanceType` e `KeyName`.

Il seguente URL ha interruzioni di riga aggiunte per chiarezza.

```
https://us-east-2.console.aws.amazon.com/cloudformation/home?region=us-east-2#/stacks/
create/review
    ?templateURL=https://s3.us-east-2.amazonaws.com/cloudformation-templates-us-east-2/
WordPress_Single_Instance.template
    &stackName=MyWPBlog
    &param_DBName=mywpblog
    &param_InstanceType=t2.medium
```

Il seguente URL include gli stessi parametri dell'esempio precedente, ma le interruzioni di riga vengono rimosse. Questo è il formato URL effettivo.

```
https://us-east-2.console.aws.amazon.com/cloudformation/home?
region=us-east-2#/stacks/create/review?templateURL=https://
s3.us-east-2.amazonaws.com/cloudformation-templates-us-east-2/
WordPress_Single_Instance.template&stackName=MyWPBlog&param_DBName=mywpblog&param_InstanceType=
```

Creazione di uno stack utilizzando un link di creazione rapida

Quando apri un link di creazione rapida, vieni indirizzato alla console. CloudFormation La console si apre direttamente alla pagina Quick create stack, con i valori forniti utilizzati automaticamente per i parametri.

Per creare uno stack utilizzando un collegamento di creazione rapida (console)

1. Nella pagina Quick create stack, per Template, Template URL, verifica che l'URL del modello sia corretto.
2. Espandi la sezione Visualizza modello per verificare il modello.
3. Per il nome dello stack, verifica il nome dello stack precompilato.
4. Esamina la sezione Parametri. Verificate che i valori dei parametri precompilati siano corretti. Inserisci tutti i parametri obbligatori che non sono stati specificati nell'URL. Se necessario, modificate i valori precompilati.

5. Successivamente, puoi configurare le seguenti impostazioni:

- Tag: organizza le risorse con coppie chiave-valore.
- Autorizzazioni: scegli il ruolo del servizio IAM per le operazioni di stack.
- Opzioni di errore dello stack: scegli di eseguire il rollback (impostazione predefinita) o preservare le risorse.
- Stack policy: controlla le autorizzazioni di aggiornamento delle risorse.
- Configurazione del rollback: configura CloudWatch il rollback basato sugli allarmi.
- Opzioni di notifica: configura le notifiche di Amazon SNS per gli eventi dello stack.
- Opzioni di creazione dello stack: definisci il tempo massimo per la creazione dello stack e abilita la protezione dalla terminazione per prevenire eliminazioni accidentali.

Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#).

6. Per Capabilities, completa tutti i riconoscimenti richiesti. Ad esempio, se il modello contiene risorse IAM, seleziona Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
7. (Facoltativo) È possibile creare un set di modifiche per visualizzare in anteprima la configurazione dello stack prima di crearlo. Scegliete Crea set di modifiche e seguite le istruzioni. Per ulteriori informazioni, consulta [Visualizza l'anteprima della configurazione del tuo stack](#).
8. Quando sei pronto, scegli Crea stack per avviare lo stack, quindi monitora l'avanzamento della creazione dello stack nella scheda Eventi. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Esempi di comandi di funzionamento CloudFormation dello stack per e AWS CLI PowerShell

I seguenti esempi da riga di comando mostrano come eseguire CloudFormation azioni individuali con and. AWS CLI PowerShell Questi esempi includono solo le azioni più comunemente utilizzate. Per un elenco completo, vedere [cloudformation](#) nel AWS CLI Command Reference.

Gli esempi di questa guida utilizzano la convenzione di una barra rovesciata (\) per indicare che una lunga riga di comando continua sulla riga successiva.

Argomenti

- [Annulla un aggiornamento dello stack](#)
- [Rollback di un aggiornamento](#)
- [Creare uno stack](#)
- [Crea una pila che includa le trasformazioni](#)
- [Eliminazione di uno stack](#)
- [Descrivi gli eventi dello stack](#)
- [Descrivi una risorsa stack](#)
- [Descrivi le risorse dello stack](#)
- [Descrivi gli stack](#)
- [Procurati un modello](#)
- [Elenca le risorse dello stack](#)
- [Elenca pile](#)
- [Aggiornare uno stack](#)
- [Convalida il modello](#)
- [Carica gli artefatti locali in un bucket S3 con AWS CLI](#)

Annulla un aggiornamento dello stack

Utilizzate il [cancel-update-stack](#) comando di comando per annullare un aggiornamento dello stack. Per ulteriori informazioni, consulta [Annullare un aggiornamento dello stack](#).

CLI

AWS CLI

Per annullare un aggiornamento dello stack in corso

Il `cancel-update-stack` comando seguente annulla un aggiornamento dello stack nello stack: `myteststack`

```
aws cloudformation cancel-update-stack --stack-name myteststack
```

- Per i dettagli sull'API, consulta Command [CancelUpdateStack](#) Reference AWS CLI .

PowerShell

Strumenti per PowerShell V4

Esempio 1: annulla un aggiornamento sullo stack specificato.

```
Stop-CFNUpdateStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [CancelUpdateStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: annulla un aggiornamento sullo stack specificato.

```
Stop-CFNUpdateStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [CancelUpdateStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Rollback di un aggiornamento

Utilizzare il [continue-update-rollback](#) comando per continuare a ripristinare un aggiornamento. Per ulteriori informazioni, consulta [Rollback di un aggiornamento](#).

CLI

AWS CLI

Per riprovare a eseguire un aggiornamento, eseguire il rollback

L'`continue-update-rollback` esempio seguente riprende un'operazione di rollback da un aggiornamento dello stack precedentemente non riuscito.

```
aws cloudformation continue-update-rollback \  
  --stack-name my-stack
```

Questo comando non produce alcun output.

- Per i dettagli sull'API, vedere [ContinueUpdateRollback](#) in Command Reference.AWS CLI

PowerShell

Strumenti per PowerShell V4

Esempio 1: continua il rollback dello stack denominato, che dovrebbe trovarsi nello stato 'UPDATE_ROLLBACK_FAILED'. Se il rollback continuato ha esito positivo, lo stack entrerà nello stato 'UPDATE_ROLLBACK_COMPLETE'.

```
Resume-CFNUpdateRollback -StackName "myStack"
```

- Per i dettagli sull'API, vedere in Cmdlet Reference (V4). [ContinueUpdateRollbackAWS](#)
Strumenti per PowerShell

Strumenti per V5 PowerShell

Esempio 1: continua il rollback dello stack denominato, che dovrebbe trovarsi nello stato 'UPDATE_ROLLBACK_FAILED'. Se il rollback continuato ha esito positivo, lo stack entrerà nello stato 'UPDATE_ROLLBACK_COMPLETE'.

```
Resume-CFNUpdateRollback -StackName "myStack"
```

- Per i dettagli sull'API, vedere in Cmdlet Reference (V5). [ContinueUpdateRollbackAWS](#)
Strumenti per PowerShell

Creare uno stack

Utilizzare il [create-stack](#) comando per creare uno stack. Devi fornire il nome dello stack, la posizione di un modello valido e i parametri di input. I nomi delle chiavi dei parametri distinguono tra maiuscole e minuscole. Se digiti erroneamente il nome della chiave di un parametro, CloudFormation non crea lo stack e segnala che il modello non contiene quel parametro.

Gli esempi seguenti mostrano come creare un nuovo stack con il nome, il modello e i parametri di input specificati.

CLI

AWS CLI

Per creare uno stack AWS CloudFormation

Il `create-stacks` comando seguente crea uno stack con il nome `myteststack` utilizzando il `sampletemplate.json` modello:

```
aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json --parameters ParameterKey=KeyPairName,ParameterValue=TestKey  
ParameterKey=SubnetIDs,ParameterValue=SubnetID1\\,SubnetID2
```

Output:

```
{  
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"  
}
```

Per ulteriori informazioni, consulta [Stacks](#) nella Guida per l'AWS CloudFormation utente.

- Per i dettagli sull'API, consulta [CreateStack AWS CLI Command Reference](#).

PowerShell

Strumenti per PowerShell V4

Esempio 1: crea un nuovo stack con il nome specificato. Il modello viene analizzato a partire dal contenuto fornito con parametri di personalizzazione (" e PK1 'PK2' rappresentano i nomi dei parametri dichiarati nel contenuto del modello, " e PV1 'PV2' rappresentano i valori di tali parametri. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, non verrà ripristinato.

```
New-CFNStack -StackName "myStack" `  
    -TemplateBody "{TEMPLATE CONTENT HERE}" `  
    -Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },  
    @{ ParameterKey="PK2"; ParameterValue="PV2" } ) `  
    -DisableRollback $true
```

Esempio 2: crea un nuovo stack con il nome specificato. Il modello viene analizzato a partire dal contenuto fornito con parametri di personalizzazione (" e PK1 'PK2' rappresentano i nomi dei parametri dichiarati nel contenuto del modello, " e PV1 'PV2' rappresentano i valori di tali parametri. I parametri di personalizzazione possono anche essere specificati utilizzando «Key»

e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato.

```
$p1 = New-Object -Type Amazon.CloudFormation.Model.Parameter
$p1.ParameterKey = "PK1"
$p1.ParameterValue = "PV1"

$p2 = New-Object -Type Amazon.CloudFormation.Model.Parameter
$p2.ParameterKey = "PK2"
$p2.ParameterValue = "PV2"

New-CFNStack -StackName "myStack" `
    -TemplateBody "{TEMPLATE CONTENT HERE}" `
    -Parameter @( $p1, $p2 ) `
    -OnFailure "ROLLBACK"
```

Esempio 3: crea un nuovo stack con il nome specificato. Il modello è ottenuto dall'URL di Amazon S3 con parametri di personalizzazione ('PK1' rappresenta il nome di un parametro dichiarato nel contenuto del modello, 'PV1' rappresenta il valore del parametro. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato (come specificare - DisableRollback \$false).

```
New-CFNStack -StackName "myStack" `
    -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
    -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 4: crea un nuovo stack con il nome specificato. Il modello è ottenuto dall'URL di Amazon S3 con parametri di personalizzazione ('PK1' rappresenta il nome di un parametro dichiarato nel contenuto del modello, 'PV1' rappresenta il valore del parametro. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato (come specificare - DisableRollback \$false). La notifica specificata AENs riceverà gli eventi pubblicati relativi allo stack.

```
New-CFNStack -StackName "myStack" `
    -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
    -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" }
```



```
-NotificationARN @( "arn1", "arn2" )
```

- Per i dettagli sull'API, vedere [CreateStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: crea un nuovo stack con il nome specificato. Il modello viene analizzato a partire dal contenuto fornito con parametri di personalizzazione (" e PK1 'PK2' rappresentano i nomi dei parametri dichiarati nel contenuto del modello, " e PV1 'PV2' rappresentano i valori di tali parametri. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, non verrà ripristinato.

```
New-CFNStack -StackName "myStack" `
    -TemplateBody "{TEMPLATE CONTENT HERE}" `
    -Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
    @{ ParameterKey="PK2"; ParameterValue="PV2" } ) `
    -DisableRollback $true
```

Esempio 2: crea un nuovo stack con il nome specificato. Il modello viene analizzato a partire dal contenuto fornito con parametri di personalizzazione (" e PK1 'PK2' rappresentano i nomi dei parametri dichiarati nel contenuto del modello, " e PV1 'PV2' rappresentano i valori di tali parametri. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato.

```
$p1 = New-Object -Type Amazon.CloudFormation.Model.Parameter
$p1.ParameterKey = "PK1"
$p1.ParameterValue = "PV1"

$p2 = New-Object -Type Amazon.CloudFormation.Model.Parameter
$p2.ParameterKey = "PK2"
$p2.ParameterValue = "PV2"

New-CFNStack -StackName "myStack" `
    -TemplateBody "{TEMPLATE CONTENT HERE}" `
    -Parameter @( $p1, $p2 ) `
    -OnFailure "ROLLBACK"
```

Esempio 3: crea un nuovo stack con il nome specificato. Il modello è ottenuto dall'URL di Amazon S3 con parametri di personalizzazione ('PK1' rappresenta il nome di un parametro dichiarato nel contenuto del modello, 'PV1' rappresenta il valore del parametro. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato (come specificare - DisableRollback \$false).

```
New-CFNStack -StackName "myStack" `
              -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
              -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 4: crea un nuovo stack con il nome specificato. Il modello è ottenuto dall'URL di Amazon S3 con parametri di personalizzazione ('PK1' rappresenta il nome di un parametro dichiarato nel contenuto del modello, 'PV1' rappresenta il valore del parametro. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «» e «ParameterKey». ParameterValue Se la creazione dello stack fallisce, verrà ripristinato (come specificare - DisableRollback \$false). La notifica specificata AENs riceverà gli eventi pubblicati relativi allo stack.

```
New-CFNStack -StackName "myStack" `
              -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
              -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" } `
              -NotificationARN @( "arn1", "arn2" )
```

- Per i dettagli sull'API, vedere [CreateStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Note

Puoi utilizzare l' AWS CLI `--template-url` opzione per specificare una posizione del file modello in Amazon S3 o. AWS Systems Manager
Per Amazon S3, l'URL deve iniziare con. `https://` I siti Web statici S3 non URLs sono supportati.

```
--template-url https://s3.region-code.amazonaws.com/bucket-name/template-name
```

Per AWS Systems Manager, utilizza il seguente formato:

```
--template-url "ssm-doc://arn:aws:ssm:region-code:account-id:document/document-name"
```

Crea una pila che includa le trasformazioni

Usa il [deploy](#) comando per creare uno stack che includa le trasformazioni. Quando create uno stack da un modello che include trasformazioni, dovete utilizzare un set di modifiche. Il `deploy` comando combina due passaggi (creazione di un set di modifiche ed esecuzione dello stesso) in un unico comando.

AWS CLI

Il `deploy` comando seguente crea uno stack con il nome, il modello e i parametri di input specificati.

```
aws cloudformation deploy --stack-name myteststack \  
  --template /path_to_template/my-template.json \  
  --parameter-overrides Key1=Value1 Key2=Value2
```

Eliminazione di uno stack

Utilizzate il [delete-stack](#) comando per eliminare uno stack. Per ulteriori informazioni, consulta [Eliminazione di uno stack](#).

CLI

AWS CLI

Per eliminare una pila

L'`delete-stack` esempio seguente elimina lo stack specificato.

```
aws cloudformation delete-stack \  
  --stack-name my-stack
```

Questo comando non produce alcun output.

- Per i dettagli sull'API, vedere [DeleteStack](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: elimina lo stack specificato.

```
Remove-CFNStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DeleteStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: elimina lo stack specificato.

```
Remove-CFNStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DeleteStack](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Se l'eliminazione fallisce e restituisce uno DELETE_FAILED stato, puoi scegliere di eliminare lo stack con la forza utilizzando l'opzione. `--deletion-mode` Questi sono i seguenti valori che possono essere usati con `deletion-mode`:

- STANDARD: elimina lo stack normalmente. Questa è la modalità di eliminazione predefinita.
- FORCE_DELETE_STACK: elimina lo stack e salta tutte le risorse che non riescono a eliminare.

AWS CLI

La seguente forza di `delete-stack` comando elimina lo *myteststack* stack utilizzando il valore con il parametro: `FORCE_DELETE_STACK` `deletion-mode`

```
aws cloudformation delete-stack --stack-name myteststack \  
--deletion-mode FORCE_DELETE_STACK
```

Questo comando non produce alcun output.

Dopo l'uso `FORCE_DELETE_STACK`, è possibile utilizzare il `list-stack-resources` comando per elencare le risorse che sono state ignorate durante il processo di eliminazione dello stack. Le risorse conservate mostreranno lo stato `DELETE_SKIPPED`. Per ulteriori informazioni, consulta [Elenca le risorse dello stack](#).

Descrivi gli eventi dello stack

Usa il [describe-stack-events](#) comando per descrivere gli eventi dello stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

CLI

AWS CLI

Per descrivere gli eventi dello stack

L'`describe-stack-events` esempio seguente visualizza i 2 eventi più recenti per lo stack specificato.

```
aws cloudformation describe-stack-events \
  --stack-name my-stack \
  --max-items 2

{
  "StackEvents": [
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "EventId": "4e1516d0-e4d6-xmpl-b94f-0a51958a168c",
      "StackName": "my-stack",
      "LogicalResourceId": "my-stack",
      "PhysicalResourceId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "ResourceType": "AWS::CloudFormation::Stack",
      "Timestamp": "2019-10-02T05:34:29.556Z",
      "ResourceStatus": "UPDATE_COMPLETE"
    },
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "EventId": "4dd3c810-e4d6-xmpl-bade-0aaf8b31ab7a",
      "StackName": "my-stack",
```

```

        "LogicalResourceId": "my-stack",
        "PhysicalResourceId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
        "ResourceType": "AWS::CloudFormation::Stack",
        "Timestamp": "2019-10-02T05:34:29.127Z",
        "ResourceStatus": "UPDATE_COMPLETE_CLEANUP_IN_PROGRESS"
    },
    "NextToken": "eyJ0ZXh0VG9XMPLiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}

```

- Per i dettagli sull'API, vedere [DescribeStackEvents](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce tutti gli eventi relativi allo stack per lo stack specificato.

```
Get-CFNStackEvent -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DescribeStackEvents](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce tutti gli eventi relativi allo stack per lo stack specificato.

```
Get-CFNStackEvent -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DescribeStackEvents](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Descrivi una risorsa stack

CLI

AWS CLI

Per ottenere informazioni su una risorsa dello stack

L'output seguente visualizza i dettagli della risorsa denominata `MyFunction` nello stack specificato.

```
aws cloudformation describe-stack-resource \  
  --stack-name MyStack \  
  --logical-resource-id MyFunction
```

Output:

```
{  
  "StackResourceDetail": {  
    "StackName": "MyStack",  
    "StackId": "arn:aws:cloudformation:us-east-2:123456789012:stack/MyStack/  
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",  
    "LogicalResourceId": "MyFunction",  
    "PhysicalResourceId": "my-function-SEZV4XMPL4S5",  
    "ResourceType": "AWS::Lambda::Function",  
    "LastUpdatedTimestamp": "2019-10-02T05:34:27.989Z",  
    "ResourceStatus": "UPDATE_COMPLETE",  
    "Metadata": "{}",  
    "DriftInformation": {  
      "StackResourceDriftStatus": "IN_SYNC"  
    }  
  }  
}
```

- Per i dettagli sull'API, vedere [DescribeStackResource](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce la descrizione di una risorsa identificata nel modello associato allo stack specificato dall'ID logico «`MyDBInstance`».

```
Get-CFNStackResource -StackName "myStack" -LogicalResourceId "MyDBInstance"
```

- Per i dettagli sull'API, vedere [DescribeStackResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce la descrizione di una risorsa identificata nel modello associato allo stack specificato dall'ID logico «MyDBInstance».

```
Get-CFNStackResource -StackName "myStack" -LogicalResourceId "MyDBInstance"
```

- Per i dettagli sull'API, vedere [DescribeStackResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Descrivi le risorse dello stack

CLI

AWS CLI

Per ottenere informazioni su una risorsa dello stack

L'`describe-stack-resources` esempio seguente visualizza i dettagli delle risorse nello stack specificato.

```
aws cloudformation describe-stack-resources \
  --stack-name my-stack
```

Output:

```
{
  "StackResources": [
    {
      "StackName": "my-stack",
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "LogicalResourceId": "bucket",
      "PhysicalResourceId": "my-stack-bucket-1vc62xmplgguf",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2019-10-02T04:34:11.345Z",
      "ResourceStatus": "CREATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    }
  ]
}
```



```

    },
    {
      "StackName": "my-stack",
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "LogicalResourceId": "function",
      "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
      "ResourceType": "AWS::Lambda::Function",
      "Timestamp": "2019-10-02T05:34:27.989Z",
      "ResourceStatus": "UPDATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    },
    {
      "StackName": "my-stack",
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
      "LogicalResourceId": "functionRole",
      "PhysicalResourceId": "my-functionRole-HIZXMPLE0M9E",
      "ResourceType": "AWS::IAM::Role",
      "Timestamp": "2019-10-02T04:34:06.350Z",
      "ResourceStatus": "CREATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    }
  ]
}

```

- Per i dettagli sull'API, vedere [DescribeStackResources](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce le descrizioni AWS delle risorse per un massimo di 100 risorse associate allo stack specificato. Per ottenere i dettagli di tutte le risorse associate a uno stack, usa `Get-CFNStackResourceSummary`, che supporta anche la paginazione manuale dei risultati.

```
Get-CFNStackResourceList -StackName "myStack"
```

Esempio 2: restituisce la descrizione dell' EC2 istanza Amazon identificata nel modello associato allo stack specificato dall'ID logico «Ec2Instance».

```
Get-CFNStackResourceList -StackName "myStack" -LogicalResourceId "Ec2Instance"
```

Esempio 3: restituisce la descrizione di un massimo di 100 risorse associate allo stack contenente un' EC2 istanza Amazon identificata dall'ID di istanza «i-123456». Per ottenere i dettagli di tutte le risorse associate a uno stack, usa Get- CFNStackResourceSummary, che supporta anche la paginazione manuale dei risultati.

```
Get-CFNStackResourceList -PhysicalResourceId "i-123456"
```

Esempio 4: restituisce la descrizione dell' EC2 istanza Amazon identificata dall'ID logico «Ec2Instance» nel modello per uno stack. Lo stack viene identificato utilizzando l'ID della risorsa fisica di una risorsa che contiene, in questo caso anche un' EC2 istanza Amazon con ID di istanza «i-123456». È inoltre possibile utilizzare una risorsa fisica diversa per identificare lo stack in base al contenuto del modello, ad esempio un bucket Amazon S3.

```
Get-CFNStackResourceList -PhysicalResourceId "i-123456" -LogicalResourceId  
"Ec2Instance"
```

- Per i dettagli sull'API, vedere [DescribeStackResources](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce le descrizioni AWS delle risorse per un massimo di 100 risorse associate allo stack specificato. Per ottenere i dettagli di tutte le risorse associate a uno stack, usa Get- CFNStackResourceSummary, che supporta anche la paginazione manuale dei risultati.

```
Get-CFNStackResourceList -StackName "myStack"
```

Esempio 2: restituisce la descrizione dell' EC2 istanza Amazon identificata nel modello associato allo stack specificato dall'ID logico «Ec2Instance».

```
Get-CFNStackResourceList -StackName "myStack" -LogicalResourceId "Ec2Instance"
```

Esempio 3: restituisce la descrizione di un massimo di 100 risorse associate allo stack contenente un' EC2 istanza Amazon identificata dall'ID di istanza «i-123456». Per ottenere i dettagli di tutte le risorse associate a uno stack, usa `Get-CFNStackResourceSummary`, che supporta anche la paginazione manuale dei risultati.

```
Get-CFNStackResourceList -PhysicalResourceId "i-123456"
```

Esempio 4: restituisce la descrizione dell' EC2 istanza Amazon identificata dall'ID logico «Ec2Instance» nel modello per uno stack. Lo stack viene identificato utilizzando l'ID della risorsa fisica di una risorsa che contiene, in questo caso anche un' EC2 istanza Amazon con ID di istanza «i-123456». È inoltre possibile utilizzare una risorsa fisica diversa per identificare lo stack in base al contenuto del modello, ad esempio un bucket Amazon S3.

```
Get-CFNStackResourceList -PhysicalResourceId "i-123456" -LogicalResourceId  
"Ec2Instance"
```

- Per i dettagli sull'API, vedere [DescribeStackResources](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Descrivi gli stack

CLI

AWS CLI

Per descrivere le pile AWS CloudFormation

Il `describe-stacks` comando seguente mostra informazioni di riepilogo per lo `myteststack` stack:

```
aws cloudformation describe-stacks --stack-name myteststack
```

Output:

```
{  
  "Stacks": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
```

```
    "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample
template showing how to create a publicly accessible S3 bucket. **WARNING** This
template creates an S3 bucket. You will be billed for the AWS resources used if
you create a stack from this template.",
    "Tags": [],
    "Outputs": [
        {
            "Description": "Name of S3 bucket to hold website content",
            "OutputKey": "BucketName",
            "OutputValue": "myteststack-s3bucket-jssofilzie2w"
        }
    ],
    "StackStatusReason": null,
    "CreationTime": "2013-08-23T01:02:15.422Z",
    "Capabilities": [],
    "StackName": "myteststack",
    "StackStatus": "CREATE_COMPLETE",
    "DisableRollback": false
}
]
```

Per ulteriori informazioni, consulta Stacks nella Guida per l'AWS CloudFormation utente.

- Per i dettagli sull'API, consulta [DescribeStacks AWS CLI Command Reference](#).

Go

SDK per Go V2

Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
import (
    "context"
    "log"

    "github.com/aws/aws-sdk-go-v2/aws"
```

```
"github.com/aws/aws-sdk-go-v2/service/cloudformation"
)

// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
    CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
// structured format.
func (actor CloudFormationActions) GetOutputs(ctx context.Context, stackName
    string) StackOutputs {
    output, err := actor.CfnClient.DescribeStacks(ctx,
        &cloudformation.DescribeStacksInput{
            StackName: aws.String(stackName),
        })
    if err != nil || len(output.Stacks) == 0 {
        log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
            stackName, err)
    }
    stackOutputs := StackOutputs{}
    for _, out := range output.Stacks[0].Outputs {
        stackOutputs[*out.OutputKey] = *out.OutputValue
    }
    return stackOutputs
}
```

- Per i dettagli sull'API, consulta la [DescribeStacks](#) sezione AWS SDK per Go API Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce una raccolta di istanze Stack che descrivono tutti gli stack dell'utente.

```
Get-CFNStack
```

Esempio 2: restituisce un'istanza Stack che descrive lo stack specificato

```
Get-CFNStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DescribeStacks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce una raccolta di istanze Stack che descrivono tutti gli stack dell'utente.

```
Get-CFNStack
```

Esempio 2: restituisce un'istanza Stack che descrive lo stack specificato

```
Get-CFNStack -StackName "myStack"
```

- Per i dettagli sull'API, vedere [DescribeStacks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per impostazione predefinita, il `describe-stacks` comando restituisce i valori dei parametri. Per evitare che vengano restituiti valori di parametri sensibili come le password, includi una `NoEcho` proprietà impostata su `TRUE` nei tuoi CloudFormation modelli.

Important

L'utilizzo dell'attributo `NoEcho` non maschera le informazioni memorizzate nei seguenti elementi:

- La sezione dei Metadata modelli. CloudFormation non trasforma, modifica o oscura le informazioni incluse nella Metadata sezione. Per ulteriori informazioni, vedere [Metadati](#).
- Sezione dei modelli Outputs. Per ulteriori informazioni, consulta [Output](#).
- Attributo Metadata di una definizione di risorsa. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Si consiglia vivamente di non utilizzare questi meccanismi per includere informazioni sensibili, come password o segreti.

⚠ Important

Anziché incorporare informazioni riservate direttamente nei CloudFormation modelli, consigliamo di utilizzare parametri dinamici nel modello di pila per fare riferimento a informazioni sensibili archiviate e gestite all'esterno CloudFormation, ad esempio nel AWS Systems Manager Parameter Store o. AWS Secrets Manager

Per ulteriori informazioni, consulta la best practice [Non incorporare le credenziali nei modelli](#).

Procurati un modello

CLI

AWS CLI

Per visualizzare il corpo del modello per una AWS CloudFormation pila

Il `get-template` comando seguente mostra il modello per lo `myteststack` stack:

```
aws cloudformation get-template --stack-name myteststack
```

Output:

```
{
  "TemplateBody": {
    "AWSTemplateFormatVersion": "2010-09-09",
    "Outputs": {
      "BucketName": {
        "Description": "Name of S3 bucket to hold website content",
        "Value": {
          "Ref": "S3Bucket"
        }
      }
    },
    "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample template showing how to create a publicly accessible S3 bucket. **WARNING** This template creates an S3 bucket. You will be billed for the AWS resources used if you create a stack from this template.",
    "Resources": {
      "S3Bucket": {
        "Type": "AWS::S3::Bucket",
```

```
        "Properties": {  
            "AccessControl": "PublicRead"  
        }  
    }  
}
```

- Per i dettagli sull'API, vedere [GetTemplate](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce il modello associato allo stack specificato.

```
Get-CFNTemplate -StackName "myStack"
```

- Per i dettagli sull'API, vedere [GetTemplate](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce il modello associato allo stack specificato.

```
Get-CFNTemplate -StackName "myStack"
```

- Per i dettagli sull'API, vedere [GetTemplate](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Elenca le risorse dello stack

CLI

AWS CLI

Per elencare le risorse in una pila

Il comando seguente visualizza l'elenco delle risorse nello stack specificato.

```
aws cloudformation list-stack-resources \
```



```
--stack-name my-stack
```

Output:

```
{
  "StackResourceSummaries": [
    {
      "LogicalResourceId": "bucket",
      "PhysicalResourceId": "my-stack-bucket-1vc62xmplgguf",
      "ResourceType": "AWS::S3::Bucket",
      "LastUpdatedTimestamp": "2019-10-02T04:34:11.345Z",
      "ResourceStatus": "CREATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    },
    {
      "LogicalResourceId": "function",
      "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
      "ResourceType": "AWS::Lambda::Function",
      "LastUpdatedTimestamp": "2019-10-02T05:34:27.989Z",
      "ResourceStatus": "UPDATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    },
    {
      "LogicalResourceId": "functionRole",
      "PhysicalResourceId": "my-functionRole-HIZXMPLE0M9E",
      "ResourceType": "AWS::IAM::Role",
      "LastUpdatedTimestamp": "2019-10-02T04:34:06.350Z",
      "ResourceStatus": "CREATE_COMPLETE",
      "DriftInformation": {
        "StackResourceDriftStatus": "IN_SYNC"
      }
    }
  ]
}
```

- Per i dettagli sull'API, vedere [ListStackResources](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce le descrizioni di tutte le risorse associate allo stack specificato.

```
Get-CFNStackResourceSummary -StackName "myStack"
```

- Per i dettagli sull'API, vedere [ListStackResources](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce le descrizioni di tutte le risorse associate allo stack specificato.

```
Get-CFNStackResourceSummary -StackName "myStack"
```

- Per i dettagli sull'API, vedere [ListStackResources](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Elenco pile

Usa il [list-stacks](#) comando per elencare le pile. Per elencare solo le pile con i codici di stato specificati, includi l'--stack-status-filter opzione. È possibile specificare uno o più codici di stato dello stack per l'--stack-status-filter opzione. Per ulteriori informazioni, consulta [Codici di stato dello stack](#).

CLI

AWS CLI

Per elencare le pile AWS CloudFormation

Il list-stacks comando seguente mostra un riepilogo di tutti gli stack con uno stato di: CREATE_COMPLETE

```
aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE
```

Output:

```
[
```

```
{
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
  "TemplateDescription": "AWS CloudFormation Sample Template S3_Bucket:
Sample template showing how to create a publicly accessible S3 bucket.
**WARNING** This template creates an S3 bucket. You will be billed for the AWS
resources used if you create a stack from this template.",
  "StackStatusReason": null,
  "CreationTime": "2013-08-26T03:27:10.190Z",
  "StackName": "myteststack",
  "StackStatus": "CREATE_COMPLETE"
}
```

- Per i dettagli sull'API, vedere [ListStacks](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce informazioni di riepilogo per tutti gli stack.

```
Get-CFNStackSummary
```

Esempio 2: restituisce informazioni di riepilogo per tutti gli stack attualmente in fase di creazione.

```
Get-CFNStackSummary -StackStatusFilter "CREATE_IN_PROGRESS"
```

Esempio 3: restituisce informazioni di riepilogo per tutti gli stack attualmente in fase di creazione o aggiornamento.

```
Get-CFNStackSummary -StackStatusFilter @("CREATE_IN_PROGRESS",
"UPDATE_IN_PROGRESS")
```

- Per i dettagli sull'API, vedere [ListStacks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce informazioni di riepilogo per tutti gli stack.

```
Get-CFNStackSummary
```

Esempio 2: restituisce informazioni di riepilogo per tutti gli stack attualmente in fase di creazione.

```
Get-CFNStackSummary -StackStatusFilter "CREATE_IN_PROGRESS"
```

Esempio 3: restituisce informazioni di riepilogo per tutti gli stack attualmente in fase di creazione o aggiornamento.

```
Get-CFNStackSummary -StackStatusFilter @("CREATE_IN_PROGRESS",  
"UPDATE_IN_PROGRESS")
```

- Per i dettagli sull'API, vedere [ListStacks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Aggiornare uno stack

Utilizzare il comando [update-stack](#) per aggiornare direttamente uno stack. È possibile specificare lo stack e i valori e le funzionalità dei parametri che si desidera aggiornare; inoltre, se si sceglie di utilizzare un modello aggiornato, è possibile specificare il nome del modello. Per ulteriori informazioni, consulta [Aggiorna direttamente gli stack](#).

CLI

AWS CLI

Per aggiornare gli stack AWS CloudFormation

Il `update-stack` comando seguente aggiorna il modello e i parametri di input per lo `mystack` stack:

```
aws cloudformation update-stack --stack-name mystack --  
template-url https://s3.amazonaws.com/sample/updated.template --  
parameters ParameterKey=KeyPairName,ParameterValue=SampleKeyPair  
ParameterKey=SubnetIDs,ParameterValue=SampleSubnetID1\\,SampleSubnetID2
```

Il `update-stack` comando seguente aggiorna solo il valore del `SubnetIDs` parametro per lo `mystack` stack. Se non si specifica un valore di parametro, viene utilizzato il valore predefinito specificato nel modello:

```
aws cloudformation update-stack --stack-name mystack --  
template-url https://s3.amazonaws.com/sample/updated.template  
--parameters ParameterKey=KeyPairName,UsePreviousValue=true  
ParameterKey=SubnetIDs,ParameterValue=SampleSubnetID1\\,UpdatedSampleSubnetID2
```

Il `update-stack` comando seguente aggiunge due argomenti di notifica dello stack allo `mystack` stack:

```
aws cloudformation update-stack --stack-name mystack --use-previous-template --  
notification-arns "arn:aws:sns:us-east-1:123456789012:mytopic1" "arn:aws:sns:us-east-1:123456789012:mytopic2"
```

Per ulteriori informazioni, consulta [gli aggiornamenti AWS CloudFormation dello stack nella Guida](#) per l'AWS CloudFormation utente.

- Per i dettagli sull'API, consulta [UpdateStack AWS CLI](#) Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' rappresenta il nome di un parametro dichiarato nel modello e 'PV1' ne rappresenta il valore. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `  
    -TemplateBody "{Template Content Here}" `  
    -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 2: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, " e PV1 'PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `
```

```
-TemplateBody "{Template Content Here}" `
-Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
@{ ParameterKey="PK2"; ParameterValue="PV2" } )
```

Esempio 3: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' rappresenta il nome di un parametro dichiarato nel modello e 'PV2' ne rappresenta il valore. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" -TemplateBody "{Template Content Here}" -
Parameters @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 4: aggiorna lo stack 'MyStack' con il modello specificato, ottenuto da Amazon S3, e i parametri di personalizzazione. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, " e 'PV1PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `
-TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
-Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
@{ ParameterKey="PK2"; ParameterValue="PV2" } )
```

Esempio 5: aggiorna lo stack 'MyStack', che in questo esempio si presume contenga risorse IAM, con il modello specificato, ottenuto da Amazon S3, e i parametri di personalizzazione. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, mentre " e 'PV1PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue». Gli stack contenenti risorse IAM richiedono di specificare il parametro -Capabilities «CAPABILITY_IAM», altrimenti l'aggiornamento avrà esito negativo con un errore "InsufficientCapabilities".

```
Update-CFNStack -StackName "myStack" `
-TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
-Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
@{ ParameterKey="PK2"; ParameterValue="PV2" } ) `
-Capabilities "CAPABILITY_IAM"
```

- Per i dettagli sull'API, vedere [UpdateStack](#) in Cmdlet Reference (V4).AWS Strumenti per PowerShell

Strumenti per V5 PowerShell

Esempio 1: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' rappresenta il nome di un parametro dichiarato nel modello e 'PV1' ne rappresenta il valore. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `
                -TemplateBody "{Template Content Here}" `
                -Parameter @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 2: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, " e PV1 'PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `
                -TemplateBody "{Template Content Here}" `
                -Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
                             @{ ParameterKey="PK2"; ParameterValue="PV2" } )
```

Esempio 3: aggiorna lo stack 'MyStack' con il modello e i parametri di personalizzazione specificati. 'PK1' rappresenta il nome di un parametro dichiarato nel modello e 'PV2' ne rappresenta il valore. I parametri di personalizzazione possono essere specificati anche utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" -TemplateBody "{Template Content Here}" -
Parameters @{ ParameterKey="PK1"; ParameterValue="PV1" }
```

Esempio 4: aggiorna lo stack 'MyStack' con il modello specificato, ottenuto da Amazon S3, e i parametri di personalizzazione. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, " e 'PV1PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue».

```
Update-CFNStack -StackName "myStack" `
```

```
-TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
    -Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
    @{ ParameterKey="PK2"; ParameterValue="PV2" } )
```

Esempio 5: aggiorna lo stack 'MyStack', che in questo esempio si presume contenga risorse IAM, con il modello specificato, ottenuto da Amazon S3, e i parametri di personalizzazione. 'PK1' e 'PK2' rappresentano i nomi dei parametri dichiarati nel modello, mentre " e 'PV1PV2' rappresentano i valori richiesti. I parametri di personalizzazione possono anche essere specificati utilizzando «Key» e «Value» anziché «ParameterKey» e «ParameterValue». Gli stack contenenti risorse IAM richiedono di specificare il parametro -Capabilities «CAPABILITY_IAM», altrimenti l'aggiornamento avrà esito negativo con un errore "InsufficientCapabilities".

```
Update-CFNStack -StackName "myStack" `
    -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template `
    -Parameter @( @{ ParameterKey="PK1"; ParameterValue="PV1" },
    @{ ParameterKey="PK2"; ParameterValue="PV2" } ) `
    -Capabilities "CAPABILITY_IAM"
```

- Per i dettagli sull'API, vedere [UpdateStack](#) in Cmdlet Reference (V5). AWS Strumenti per PowerShell

Note

Per rimuovere tutte le notifiche, specificare [] per l'opzione. --notification-arns

Convalida il modello

Usa il [validate-template](#) comando per verificare la presenza di errori di sintassi nel file modello.

Durante la convalida, verifica CloudFormation innanzitutto se il modello è JSON valido. Se non lo è, CloudFormation verifica se il modello è in un formato YAML valido. Se entrambi i controlli falliscono, CloudFormation restituisce un errore di convalida del modello.

CLI

AWS CLI

Per convalidare un modello AWS CloudFormation

Il `validate-template` comando seguente convalida il `sampletemplate.json` modello:

```
aws cloudformation validate-template --template-body file://sampletemplate.json
```

Output:

```
{
  "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample template
showing how to create a publicly accessible S3 bucket. **WARNING** This template
creates an S3 bucket. You will be billed for the AWS resources used if you
create a stack from this template.",
  "Parameters": [],
  "Capabilities": []
}
```

Per ulteriori informazioni, vedere *Working with AWS CloudFormation Templates* nella Guida per l'AWS CloudFormation utente.

- Per i dettagli sull'API, consulta [ValidateTemplate AWS CLI](#) Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: convalida il contenuto del modello specificato. L'output descrive in dettaglio le funzionalità, la descrizione e i parametri del modello.

```
Test-CFNTemplate -TemplateBody "{TEMPLATE CONTENT HERE}"
```

Esempio 2: convalida il modello specificato a cui si accede tramite un URL Amazon S3. L'output descrive in dettaglio le funzionalità, la descrizione e i parametri del modello.

```
Test-CFNTemplate -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/
templatefile.template
```

- Per i dettagli sull'API, vedere [ValidateTemplate](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: convalida il contenuto del modello specificato. L'output descrive in dettaglio le funzionalità, la descrizione e i parametri del modello.

```
Test-CFNTemplate -TemplateBody "{TEMPLATE CONTENT HERE}"
```

Esempio 2: convalida il modello specificato a cui si accede tramite un URL Amazon S3. L'output descrive in dettaglio le funzionalità, la descrizione e i parametri del modello.

```
Test-CFNTemplate -TemplateURL https://s3.amazonaws.com/amzn-s3-demo-bucket/  
templatefile.template
```

- Per i dettagli sull'API, vedere [ValidateTemplate](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Di seguito è riportato un esempio di risposta che produce un errore di convalida.

```
{  
  "ResponseMetadata": {  
    "RequestId": "4ae33ec0-1988-11e3-818b-e15a6df955cd"  
  },  
  "Errors": [  
    {  
      "Message": "Template format error: JSON not well-formed. (line 11, column  
8)",  
      "Code": "ValidationError",  
      "Type": "Sender"  
    }  
  ],  
  "Capabilities": [],  
  "Parameters": []  
}  
A client error (ValidationError) occurred: Template format error: JSON not well-formed.  
(line 11, column 8)
```

 Note

Il comando `validate-template` è progettato per controllare solo la sintassi del modello. Non garantisce che i valori delle proprietà specificati per una risorsa siano validi per tale risorsa. Né determina il numero di risorse presenti quando verrà creato lo stack. Per verificare la validità operativa, devi tentare di creare lo stack. Non esiste una sandbox o un'area di test per gli AWS CloudFormation stack, quindi ti verranno addebitate le risorse create durante i test.

Carica gli artefatti locali in un bucket S3 con AWS CLI

Puoi utilizzarlo AWS CLI per caricare artefatti locali a cui fa riferimento un CloudFormation modello in un bucket Amazon S3. Gli artefatti locali sono file a cui fai riferimento nel tuo modello. Invece di caricare manualmente i file in un bucket S3 e quindi aggiungere le relative posizioni al modello, puoi specificare gli artefatti locali nel modello e utilizzare il comando per caricarli rapidamente. [package](#)

Un artefatto locale è un percorso a un file o a una cartella che il comando `package` carica in Amazon S3. Ad esempio, un artefatto può essere un percorso locale al codice sorgente della AWS Lambda funzione o un file OpenAPI dell'API REST di Amazon API Gateway.

Quando si utilizza il comando: `package`

- Se specifichi un file, il comando lo carica direttamente nel bucket S3.
- Se si specifica una cartella, il comando crea un `.zip` file per la cartella e quindi carica il `.zip` file.
- Se non specifichi un percorso, il comando crea un `.zip` file per la directory di lavoro e lo carica.

È possibile specificare un percorso assoluto o relativo, in cui il percorso è relativo alla posizione del modello.

Dopo aver caricato gli artefatti, il comando restituisce una copia del modello, sostituendo i riferimenti ad artefatti locali con la posizione S3 in cui il comando ha caricato gli artefatti. È quindi possibile utilizzare il modello restituito per creare o aggiornare uno stack.

 Note

Puoi utilizzare artefatti locali solo per le proprietà di risorsa supportate dal comando `package`. Per ulteriori informazioni su questo comando e un elenco delle proprietà delle risorse supportate, consultate la [package](#) documentazione nel [AWS CLI Command Reference](#).

Prerequisiti

Prima di iniziare, devi disporre di un bucket Amazon S3 esistente.

Package e distribuzione di un modello con artefatti locali

Il seguente modello specifica l'artefatto locale per il codice sorgente della funzione Lambda. Il codice sorgente è memorizzato nella cartella. `/home/user/code/lambdafunction`

Modello originale

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Transform": "AWS::Serverless-2016-10-31",
  "Resources": {
    "MyFunction": {
      "Type": "AWS::Serverless::Function",
      "Properties": {
        "Handler": "index.handler",
        "Runtime": "nodejs18.x",
        "CodeUri": "/home/user/code/lambdafunction"
      }
    }
  }
}
```

Il [package](#) comando seguente crea e carica un `.zip` file della cartella del codice sorgente della funzione nella radice del bucket specificato.

```
aws cloudformation package \
  --s3-bucket amzn-s3-demo-bucket \
  --template /path_to_template/template.json \
  --output-template-file packaged-template.json \
```

```
--output json
```

Il comando genera un nuovo modello nel percorso specificato da `--output-template-file`. Sostituisce il riferimento all'artefatto con la posizione Amazon S3, come illustrato di seguito. Il `.zip` file viene denominato utilizzando il MD5 checksum del contenuto della cartella, anziché utilizzando il nome della cartella stessa.

Modello risultante

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Transform": "AWS::Serverless-2016-10-31",
  "Resources": {
    "MyFunction": {
      "Type": "AWS::Serverless::Function",
      "Properties": {
        "Handler": "index.handler",
        "Runtime": "nodejs18.x",
        "CodeUri": "s3://amzn-s3-demo-bucket/md5_checksum"
      }
    }
  }
}
```

Dopo aver impacchettato gli elementi del modello, distribuisce il modello elaborato utilizzando il comando. [deploy](#)

```
aws cloudformation deploy \
  --template-file packaged-template.json \
  --stack-name stack-name
```

Quando distribuisce modelli di dimensioni superiori a 51.200 byte, usa il `deploy` comando con l' `--s3-bucket` opzione per caricare il modello su S3, come nell'esempio seguente.

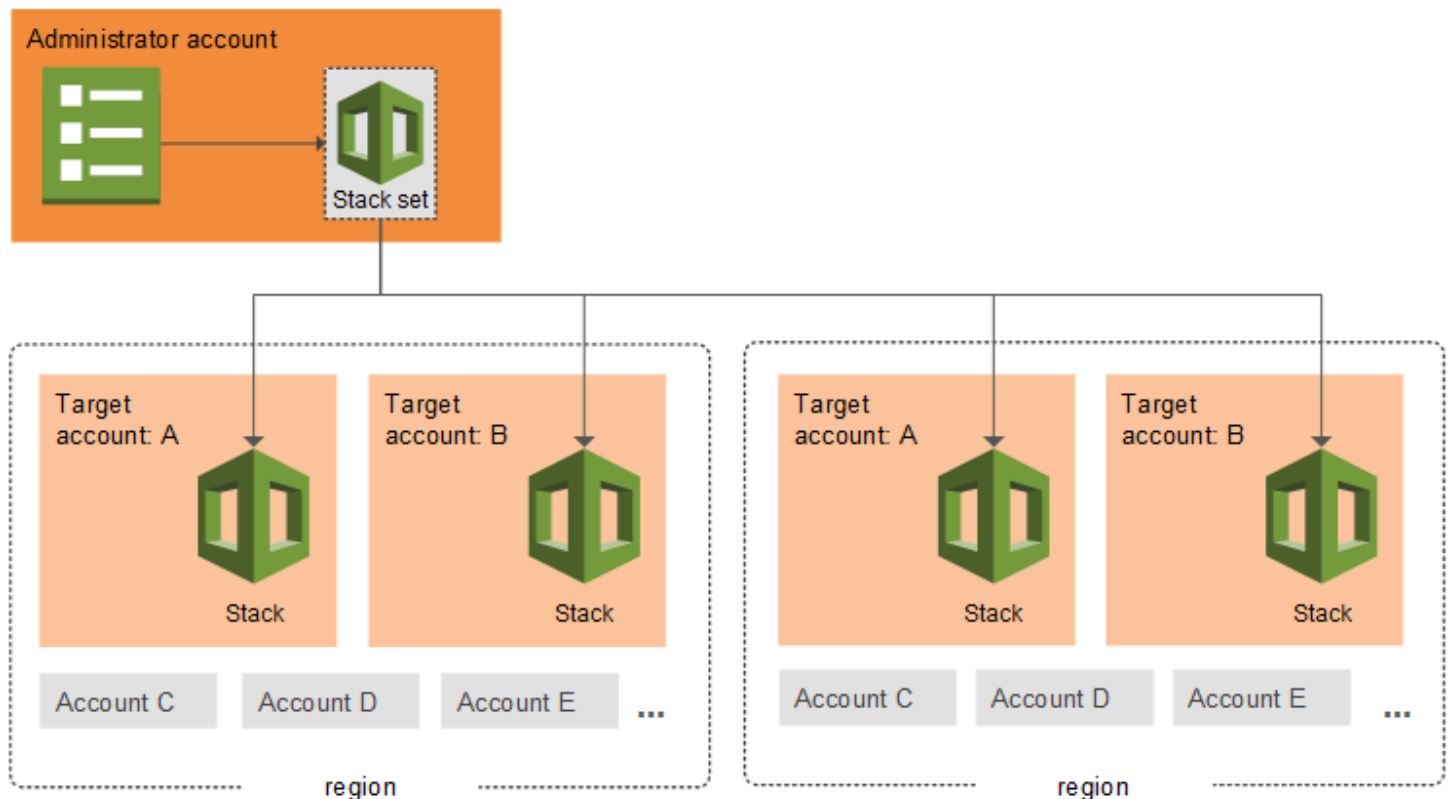
```
aws cloudformation deploy \
  --template-file packaged-template.json \
  --stack-name stack-name \
  --s3-bucket amzn-s3-demo-bucket
```

 Note

Per un altro esempio di utilizzo del package comando per caricare artefatti locali, vedi. [Dividi un modello in pezzi riutilizzabili usando pile annidate](#)

Gestione degli stack tra account e regioni con StackSets

AWS CloudFormation StackSets estende la funzionalità degli stack consentendoti di creare, aggiornare o eliminare gli stack su più account e Regioni AWS con un'unica operazione. Utilizzando un account amministratore, è possibile definire e gestire un CloudFormation modello e utilizzare il modello come base per il provisioning degli stack in account di destinazione selezionati tra quelli specificati. Regioni AWS



Questa sezione consente di iniziare a utilizzare StackSets e risponde a domande comuni su come utilizzare e risolvere i problemi di StackSet creazione, aggiornamento ed eliminazione.

Argomenti

- [StackSets concetti](#)
- [Prerequisiti per l'utilizzo AWS CloudFormation StackSets](#)
- [Inizia a StackSets usare un modello di esempio](#)
- [Crea AWS CloudFormation StackSets con autorizzazioni autogestite](#)
- [Crea AWS CloudFormation StackSets con autorizzazioni gestite dal servizio](#)
- [Abilita o disabilita le distribuzioni automatiche per in StackSets AWS Organizations](#)

- [Aggiornamento AWS CloudFormation StackSets](#)
- [Aggiungi pile a CloudFormation StackSets](#)
- [Sostituisci i valori dei parametri sugli stack all'interno del tuo CloudFormation StackSet](#)
- [Elimina pile da AWS CloudFormation StackSets](#)
- [Eliminare AWS CloudFormation StackSets](#)
- [Impedisci le StackSets implementazioni fallite utilizzando le porte dell'account di destinazione](#)
- [Scegli la modalità Concurrency per AWS CloudFormation StackSets](#)
- [Esecuzione del rilevamento della deriva su CloudFormation StackSets](#)
- [Importa pile in AWS CloudFormation StackSets](#)
- [Procedure consigliate per l'utilizzo AWS CloudFormation StackSets](#)
- [AWS CloudFormation StackSets modelli di esempio](#)
- [Risoluzione dei problemi AWS CloudFormation StackSets](#)

StackSets concetti

Quando usi StackSets, lavori con StackSetsistanze e pile in pila.

Argomenti

- [Account amministratore e target](#)
- [AWS CloudFormation StackSets](#)
- [Modelli di autorizzazione per StackSets](#)
- [Istanze di stack](#)
- [StackSet operazioni](#)
- [StackSet opzioni operative](#)
- [Tag](#)
- [StackSets codici di stato](#)
- [Codici di stato delle istanze di stack](#)

Account amministratore e target

Un account amministratore è l'account Account AWS in cui crei. StackSets Per StackSets le autorizzazioni gestite dal servizio, l'account amministratore è l'account di gestione dell'organizzazione

o un account amministratore delegato. Puoi gestirlo StackSet accedendo all'account AWS amministratore che ha creato il StackSet

Un account di destinazione è l'account in cui crei, aggiorni o elimini uno o più stack nel tuo StackSet. Prima di poter utilizzare StackSet a per creare stack in un account di destinazione, imposta una relazione di fiducia tra l'amministratore e gli account di destinazione.

AWS CloudFormation StackSets

A StackSetti consente di creare pile in Account AWS più regioni utilizzando un unico CloudFormation modello. StackSetIl CloudFormation modello di A definisce tutte le risorse in ogni pila. Durante la creazione StackSet, specificate il modello da utilizzare, oltre ai parametri e alle funzionalità richiesti dal modello.

Dopo aver definito un StackSet, puoi creare, aggiornare o eliminare gli stack negli account di destinazione e Regioni AWS specificare. Quando crei, aggiorni o elimini stack, puoi anche specificare le preferenze operative. Ad esempio, includere l'ordine delle Regioni in cui desideri eseguire l'operazione, la soglia di tolleranza di errore prima dell'interruzione delle operazioni di stack e il numero di account che eseguono operazioni di stack contemporaneamente.

A StackSet è una risorsa regionale. Se ne crei una StackSet in una Regione AWS, puoi visualizzarla o modificarla solo quando visualizzi quella regione.

Modelli di autorizzazione per StackSets

È possibile creare StackSets utilizzando autorizzazioni autogestite o autorizzazioni gestite dal servizio.

Con le autorizzazioni gestite automaticamente, crei i ruoli IAM necessari per la distribuzione su più account e regioni. StackSets Questi ruoli sono necessari per stabilire una relazione di fiducia tra l'account che amministri e l' StackSet account su cui stai distribuendo le istanze dello stack. Utilizzando questo modello di autorizzazioni, StackSets puoi eseguire il deployment su qualsiasi dispositivo Account AWS in cui disponi delle autorizzazioni per creare un ruolo IAM.

Con le autorizzazioni gestite dal servizio è possibile distribuire le istanze dello stack agli account gestiti da AWS Organizations. Utilizzando questo modello di autorizzazioni, non è necessario creare i ruoli IAM necessari; StackSets crea i ruoli IAM per tuo conto. Con questo modello puoi anche attivare le implementazioni automatiche negli account che aggiungerai all'organizzazione in futuro.

AWS Organizations si integra CloudFormation e ti aiuta a gestire e governare centralmente il tuo ambiente man mano che ridimensioni e fai crescere le tue risorse. AWS

- Account di gestione: è l'account utilizzato per creare l'organizzazione. Per ulteriori informazioni, vedere [Terminologia e concetti](#) per. AWS Organizations
- Amministratore delegato: un AWS servizio compatibile può registrare un account AWS membro nell'organizzazione come amministratore degli account dell'organizzazione in quel servizio. Per ulteriori informazioni, consulta [AWS i servizi con AWS Organizations cui è possibile utilizzare](#).

Per ulteriori informazioni sulla creazione e la gestione StackSets con autorizzazioni gestite dal servizio, consulta i seguenti argomenti:

- [Attiva l'accesso affidabile per StackSets con AWS Organizations](#)
- [Registrare un account membro amministratore delegato](#)
- [Crea AWS CloudFormation StackSets con autorizzazioni gestite dal servizio](#)

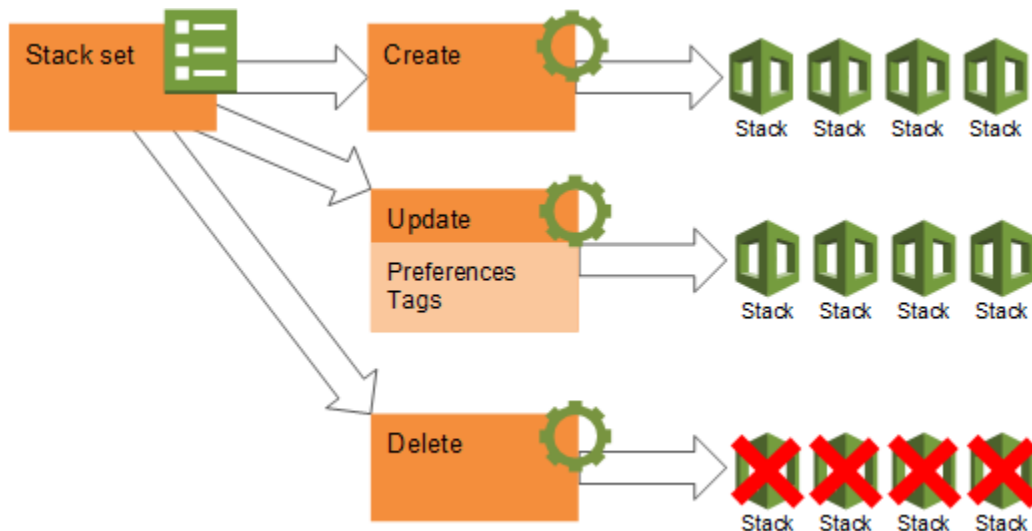
Istanze di stack

Un'istanza di stack è un riferimento a uno stack in un account target all'interno di una Regione.

Un'istanza di stack può esistere senza uno stack. Ad esempio, se non è possibile creare lo stack, l'istanza di stack indica il motivo per cui la creazione dello stack non ha avuto esito positivo.

Un'istanza stack si associa a una sola istanza. StackSet

La figura seguente mostra le relazioni logiche tra StackSets le operazioni di stack e gli stack. Quando si aggiorna a StackSet, tutte le istanze dello stack associate si aggiornano in tutti gli account e le regioni.



StackSet operazioni

È possibile eseguire le seguenti operazioni su StackSets.

Crea StackSet

La creazione di un nuovo StackSet include la specificazione di un CloudFormation modello da utilizzare per creare gli stack, la specificazione degli account di destinazione in cui si desidera creare gli stack e l'identificazione degli stack Regioni AWS in cui si desidera distribuire gli stack negli account di destinazione. A StackSet garantisce la distribuzione coerente delle stesse risorse dello stack, con le stesse impostazioni, su tutti gli account di destinazione specificati all'interno delle regioni scelte.

Aggiorna StackSet

Quando aggiorni un StackSet, inserisci le modifiche agli stack del tuo StackSet. Puoi aggiornare un StackSet in uno dei seguenti modi. Gli aggiornamenti dei modelli influiscono sempre su tutti gli stack; non è possibile aggiornare il modello in modo selettivo per alcuni stack degli stack StackSet, ma non per altri.

- Modifica le impostazioni esistenti nel modello o aggiungi nuove risorse, ad esempio aggiornando le impostazioni dei parametri per un servizio specifico o aggiungendo nuove EC2 istanze Amazon.
- Sostituisci il modello con un modello diverso.
- Aggiungi stack in account target esistenti o aggiuntivi, in Regioni esistenti o aggiuntive.

Eliminazione degli stack

L'eliminazione di uno stack comporta anche l'eliminazione di tutte le risorse a esso associate dagli account target specificati all'interno delle Regioni selezionate. Puoi eliminare stack nei modi seguenti.

- Eliminare stack da alcuni account target e conservare altri stack in esecuzione in altri account target.
- Eliminare stack da alcune Regioni e lasciare stack in esecuzione in altre Regioni.
- Elimina gli stack dal tuo StackSet, ma salvali in modo che continuino a funzionare indipendentemente StackSet dal tuo scegliendo l'opzione Retain Stacks. Potrai quindi gestire gli stack conservati all'esterno del tuo alloggio. StackSet CloudFormation
- Elimina tutte le pile che hai StackSet, preparandoti a eliminare tutte le tue pile. StackSet

Elimina StackSet

Puoi eliminare il tuo StackSet solo quando non contiene istanze dello stack.

StackSet opzioni operative

Le opzioni descritte in questa sezione aiutano a controllare il tempo e il numero di errori consentiti per eseguire StackSet operazioni di successo e impediscono la perdita di risorse dello stack.

Numero massimo di account simultanei

Questa impostazione, disponibile nei flussi di lavoro di creazione, aggiornamento ed eliminazione, consente di specificare il numero massimo o la percentuale massima di account di destinazione in cui viene eseguita un'operazione simultaneamente. Un numero o una percentuale inferiore indica che un'operazione viene eseguita in un minor numero di account di destinazione contemporaneamente. Le operazioni vengono eseguite in una Regione alla volta, nell'ordine specificato nella casella Deployment order (Ordine di implementazione). Ad esempio, se implementi stack in 10 account target in due Regioni e imposti Maximum concurrent accounts (Numero massimo di account simultanei) su 50 e By percentage (In base alla percentuale), gli stack verranno implementati in cinque account nella prima Regione, quindi nei successivi cinque account nella prima Regione, prima di passare alla Regione successiva e iniziare l'implementazione nei primi cinque account di destinazione.

Quando si sceglie Per percentuale, se la percentuale specificata non rappresenta un numero intero degli account specificati, viene CloudFormation arrotondata per difetto. Ad esempio, se stai

distribuendo pile su 10 account di destinazione e hai impostato il numero massimo di account simultanei su 25 e Per percentuale, CloudFormation arrotonda per difetto la distribuzione da 2,5 pile contemporaneamente (che non sarebbe possibile) alla distribuzione simultanea di due pile.

Tieni presente che questa impostazione consente di specificare il valore massimo per le operazioni. Per distribuzioni di grandi dimensioni, in determinate circostanze il numero effettivo di account simultanei potrebbe essere inferiore per via del throttling.

Il numero massimo di account simultanei può dipendere dal valore della tolleranza agli errori a seconda della modalità Concurrency utilizzata. Se la modalità Concurrency Mode è impostata su Strict Failure Tolerance, il numero massimo di conti concorrenti può essere al massimo uno in più rispetto all'impostazione Tolleranza di errore.

Modalità di simultaneità

Questa impostazione, disponibile nei flussi di lavoro di creazione, aggiornamento ed eliminazione, consente di scegliere il comportamento del livello di concorrenza durante le operazioni. StackSet Per ulteriori informazioni, consulta [Scegli la modalità Concurrency per AWS CloudFormation StackSets](#).

Tolleranza di errore

Questa impostazione, disponibile nei flussi di lavoro di creazione, aggiornamento ed eliminazione, consente di specificare il numero o la percentuale massima di errori delle operazioni di stack che possono verificarsi, per regione, oltre i quali interrompe automaticamente un'operazione. CloudFormation Se il numero o la percentuale sono di piccola entità, l'operazione viene eseguita su un numero inferiore di stack, ma è possibile avviare più rapidamente la risoluzione dei problemi relativi alle operazioni non riuscite. Ad esempio, se aggiorni 10 stack in 10 account target in tre Regioni e imposti Failure tolerance (Tolleranza di errore) su 20 e By percentage (In base alla percentuale), potranno verificarsi massimo due aggiornamenti di stack non riusciti in una Regione perché l'operazione continui. Se un terzo stack nella stessa regione fallisce, CloudFormation interrompe l'operazione. Se è impossibile aggiornare uno stack nella prima Regione, l'operazione di aggiornamento prosegue in quella Regione, quindi passa alla Regione successiva. Se due stack non possono essere aggiornati nella seconda regione, la tolleranza di errore raggiunge il 20%; se un terzo stack nella regione fallisce, CloudFormation interrompe l'operazione di aggiornamento e non passa alle regioni successive.

Quando scegli Per percentuale, se la percentuale specificata non rappresenta un numero intero degli stack all'interno di ciascuna regione, CloudFormation viene arrotondata per difetto. Ad esempio, se stai distribuendo pile su 10 account di destinazione in tre regioni e imposti

la tolleranza di errore su 25 e per percentuale, CloudFormation arrotonda per difetto da una tolleranza di errore di 2,5 pile (che non sarebbe possibile) a una tolleranza di fallimento di due pile per regione.

Conservazione degli stack

Questa impostazione, disponibile nei flussi di lavoro di eliminazione degli stack, consente di mantenere attivi gli stack e le relative risorse anche dopo aver rimosso gli stack da un. StackSet. Quando mantieni gli stack, AWS CloudFormation lascia intatti gli stack nei singoli account e nelle singole Regioni. Gli stack si dissociano da StackSet, ma salvano lo stack e le relative risorse. Una volta completata un'operazione di eliminazione degli stack, puoi gestire gli stack conservati nell' CloudFormation account di destinazione (non nell'account amministratore) che ha creato gli stack.

Simultaneità Regione

Questa impostazione, disponibile nei flussi di lavoro di creazione, aggiornamento ed eliminazione, consente di scegliere la modalità di distribuzione nelle regioni. StackSets

Sequenziale: distribuisce StackSets l'operazione in una regione alla volta, come specificato nella casella d'ordine Distribuzione regionale, purché gli errori di distribuzione di una regione non superino la tolleranza di errore specificata. La distribuzione sequenziale è la selezione predefinita.

Parallelo: distribuisce StackSets le operazioni in tutte le regioni specificate contemporaneamente, purché gli errori di distribuzione di una regione non superino la tolleranza di errore specificata.

Tag

È possibile aggiungere tag durante le operazioni StackSet di creazione e aggiornamento specificando coppie di chiavi e valori. I tag sono utili per ordinare e filtrare le StackSet risorse per la fatturazione e l'allocazione dei costi. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta [Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione dei costi nella AWS Guida per l'utente](#). AWS Billing and Cost Management. Dopo aver specificato la coppia chiave-valore, scegliere + per salvare il tag. Puoi eliminare i tag non più utilizzati scegliendo la X rossa a destra di un tag.

I tag che applichi StackSets si applicano a tutti gli stack e alle risorse create dagli stack. Puoi anche aggiungere tag solo a livello di pila in CloudFormation, ma tali tag potrebbero non essere visualizzati in. StackSets

Sebbene StackSets non aggiunga alcun tag definito dal sistema, non dovresti iniziare i nomi chiave di nessun tag con la stringa. aws :

StackSets codici di stato

AWS CloudFormation StackSets genera codici di stato per StackSet le operazioni.

La tabella seguente descrive i codici di stato per StackSet le operazioni.

RUNNING

L'operazione è attualmente in corso.

SUCCEEDED

L'operazione è terminata senza che sia stata superata la tolleranza di errore per l'operazione.

FAILED

Il numero di stack in cui non è stato possibile completare l'operazione ha superato la tolleranza di errore definita dall'utente. Il valore della tolleranza di errore che hai impostato per un'operazione viene applicato per ciascuna Regione durante le operazioni di creazione e aggiornamento degli stack. Se il numero di stack non riusciti all'interno di una Regione supera la tolleranza di errore, lo stato dell'operazione nella Regione cambia in FAILED. Lo stato dell'operazione nel suo complesso è inoltre impostato su e CloudFormation annulla l'operazione in tutte le regioni rimanenti. FAILED

QUEUED

[Service-managed permissions] Per le implementazioni automatiche che richiedono una sequenza di operazioni, l'operazione viene messa in coda per l'esecuzione. Per esempio:

- Lo spostamento di un account da un'unità organizzativa (OU) a un'altra attiva una distribuzione automatica. OU1 OU2 StackSets esegue un'operazione di eliminazione per rimuovere l'istanza dello stack dall'OU1account di destinazione nella regione di destinazione e mette in coda un'operazione di creazione per aggiungere un'istanza dello stack all'OU2account di destinazione nella regione di destinazione.
- L'aggiunta di un account AccountA a un'unità organizzativa attiva una distribuzione automatica. StackSets esegue un'operazione di creazione per aggiungere un'istanza dello stack AccountA nella regione di destinazione. Se si aggiunge un altro account AccountB all'unità organizzativa durante l'esecuzione di questa operazione di creazione, mette in StackSets coda una seconda operazione di creazione. Una volta completata la prima operazione di creazione, StackSets esegue la seconda operazione di creazione a cui aggiungere un'istanza dello stack AccountB nella regione di destinazione.

STOPPING

L'operazione è in fase di arresto su richiesta dell'utente.

STOPPED

L'operazione è stata interrotta su richiesta dell'utente.

Codici di stato delle istanze di stack

AWS CloudFormation StackSets genera codici di stato per le istanze dello stack.

La tabella seguente descrive i codici di stato per le istanze dello stack all'interno. StackSets

CURRENT

Lo stack è aggiornato con. StackSet

OUTDATED

Lo stack non è aggiornato con il StackSet per uno dei seguenti motivi.

- Un'operazione [CreateStackSet](#) o [UpdateStackSet](#) sullo stack associato ha avuto esito negativo.
- La stack faceva parte di un'operazione [CreateStackSet](#) o [UpdateStackSet](#) che ha avuto esito negativo o è stata interrotta prima della creazione o dell'aggiornamento dello stack.

INOPERABLE

Un'operazione [DeleteStackInstances](#) non è andata a buon fine e ha lasciato lo stack in uno stato instabile. Gli stack in questo stato vengono esclusi da ulteriori operazioni [UpdateStackSet](#). Per eliminare l'istanza di stack, potresti dover eseguire un'operazione [DeleteStackInstances](#) impostando `RetainStacks` su `true`, quindi eliminare lo stack manualmente.

CANCELLED

L'operazione nell'account e nella Regione specificati è stata annullata. Ciò accade perché un utente ha interrotto l' StackSet operazione o perché StackSet le operazioni superano la tolleranza di errore.

FAILED

L'operazione nell'account e nella Regione specificati non è riuscita. Se l' StackSet operazione fallisce in un numero sufficiente di account all'interno di una regione, la tolleranza di errore per l'intera StackSet operazione potrebbe essere superata.

FAILED_IMPORT

L'importazione dell'istanza dello stack nell'account e nella regione specificati non è riuscita e ha lasciato lo stack in uno stato instabile. Una volta risolti i problemi che hanno causato l'errore, è possibile ritentare l'operazione di importazione. Se un numero sufficiente di StackSet operazioni non riesce in un numero sufficiente di account all'interno di una regione, la tolleranza di errore per l'intera StackSet operazione potrebbe essere superata.

PENDING

L'operazione nell'account e nella Regione specificati deve ancora essere avviata.

RUNNING

L'operazione nell'account e nella Regione specificati è attualmente in corso.

SKIPPED_SUSPENDED_ACCOUNT

L'operazione nell'account e nella Regione specificati è stata ignorata perché l'account era sospeso al momento dell'operazione.

SUCCEEDED

L'operazione nell'account e nella Regione specificati è stata completata correttamente.

Prerequisiti per l'utilizzo AWS CloudFormation StackSets

StackSets estendi la funzionalità degli stack, in modo da poter creare, aggiornare o eliminare gli stack su più account e regioni con un'unica operazione.

Poiché StackSets esegui operazioni di stack su più account, prima di poter creare il primo StackSet account sono necessarie le autorizzazioni necessarie definite nel tuo Account AWS

È possibile eseguire la gestione StackSets utilizzando autorizzazioni autogestite o gestite dal servizio.

- Per la gestione automatica StackSets, devi creare e gestire i ruoli IAM in ogni account di destinazione e. Regione AWS Per ulteriori informazioni, consulta [Concedere autorizzazioni gestite dal cliente](#).
- Per quanto riguarda la gestione dei servizi StackSets, non è necessario creare e gestire manualmente i ruoli IAM in ogni account; AWS gestisce la creazione dei ruoli e le autorizzazioni per te. Per ulteriori informazioni, consulta [Attiva l'accesso affidabile](#).

 Note

L'attivazione dell'accesso affidabile con AWS Organizations for AWS CloudFormation StackSets non è attualmente supportata nelle regioni di Cina, Pechino e Ningxia.

Argomenti

- [Preparati a eseguire StackSet operazioni Regioni AWS disattivate per impostazione predefinita](#)
- [Concedere autorizzazioni gestite dal cliente](#)
- [Attiva l'accesso affidabile per StackSets con AWS Organizations](#)

Preparati a eseguire StackSet operazioni Regioni AWS disattivate per impostazione predefinita

Regioni AWS introdotte dopo il 20 marzo 2019, ad esempio Asia Pacifico (Hong Kong), sono disabilitate per impostazione predefinita. Occorre abilitare queste Regioni per gli account prima di poterli utilizzare. Per ulteriori informazioni, consulta [Abilita o disabilita Regioni AWS nel tuo account](#) nella Guida Gestione dell'account AWS di riferimento.

Per creare un account amministratore StackSet di un account (se si utilizzano autorizzazioni autogestite) o un account di gestione dell'organizzazione (se si utilizzano le autorizzazioni gestite dal servizio) in una regione disabilitata per impostazione predefinita, è necessario innanzitutto abilitare tale regione per l'account amministratore o di gestione.

Per creare o AWS CloudFormation aggiornare correttamente un'istanza dello stack:

- L'account di destinazione deve risiedere in una Regione attualmente abilitata per tale account di destinazione.
- L'account StackSet amministratore o l'account di gestione dell'organizzazione devono avere la stessa regione abilitata dell'account di destinazione.

 Important

Tieni presente che durante StackSet le operazioni, gli account amministratore e di destinazione si scambiano i metadati relativi agli account stessi, oltre alle istanze StackSet e alle StackSet istanze coinvolte.

Inoltre, se disabiliti una regione che contiene un account in cui risiedono StackSet le istanze, sei responsabile dell'eliminazione di tali istanze o risorse, se lo desideri. Inoltre, tenere presente che i metadati relativi all'account di destinazione nella Regione disabilitata verranno conservati nell'account amministratore.

Concedere autorizzazioni gestite dal cliente

Questo argomento fornisce istruzioni su come creare i ruoli di servizio IAM necessari per la distribuzione su più account e Regioni AWS con StackSets autorizzazioni autogestite. Questi ruoli sono necessari per stabilire una relazione di fiducia tra l'account StackSet da cui amministri e l'account su cui stai distribuendo le istanze dello stack. Utilizzando questo modello di autorizzazioni, StackSets puoi eseguire il deployment su qualsiasi dispositivo Account AWS in cui disponi delle autorizzazioni per creare un ruolo IAM.

Per utilizzare le autorizzazioni gestite dal servizio, consulta invece. [Attiva l'accesso affidabile](#)

Argomenti

- [Panoramica delle autorizzazioni gestite automaticamente](#)
- [Concedi a tutti gli utenti dell'account amministratore le autorizzazioni per gestire gli stack in tutti gli account di destinazione](#)
- [Imposta le opzioni di autorizzazione avanzate per le operazioni StackSet](#)
- [Configurazione di chiavi globali per mitigare i problemi di "confused deputy"](#)

Panoramica delle autorizzazioni gestite automaticamente

Prima di creare un account StackSet con autorizzazioni autogestite, devi aver creato i ruoli di servizio IAM in ogni account.

I passaggi di base sono:

1. Determina qual Account AWS è l'account amministratore.

StackSets vengono creati in questo account amministratore. Un account di destinazione è l'account in cui si creano singoli stack che appartengono a un StackSet.

2. Determina come desideri strutturare le autorizzazioni per. StackSet

La configurazione delle autorizzazioni più semplice (e più permissiva) consiste nel concedere a tutti gli utenti e i gruppi dell'account amministratore la possibilità di creare e aggiornare tutti i file StackSets gestiti tramite tale account. Per ottenere un controllo più accurato, puoi configurare le autorizzazioni per specificare:

- Quali utenti e gruppi possono eseguire StackSet operazioni in quali account di destinazione.
- Quali risorse gli utenti e i gruppi possono includere nei propri StackSets.
- Quali StackSet operazioni possono eseguire utenti e gruppi specifici.

3. Crea i ruoli di servizio IAM necessari negli account amministratore e di destinazione per definire le autorizzazioni desiderate.

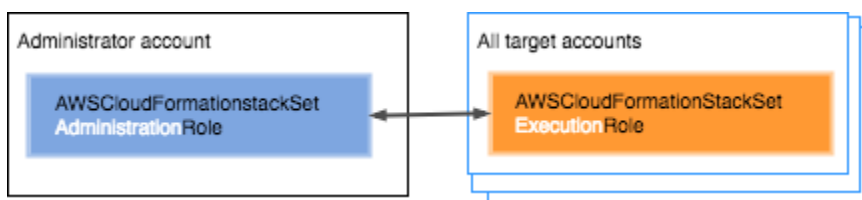
Nello specifico, i due ruoli richiesti sono:

- **AWSCloudFormationStackSetAdministrationRole**— Questo ruolo viene distribuito all'account amministratore.
- **AWSCloudFormationStackSetExecutionRole**— Questo ruolo viene distribuito a tutti gli account in cui si creano istanze stack.

Concedi a tutti gli utenti dell'account amministratore le autorizzazioni per gestire gli stack in tutti gli account di destinazione

Questa sezione mostra come impostare le autorizzazioni per consentire a tutti gli utenti e i gruppi dell'account amministratore di eseguire StackSet operazioni in tutti gli account di destinazione. Ti guida nella creazione dei ruoli di servizio IAM richiesti negli account amministratore e di destinazione. Tutti gli utenti dell'account amministratore possono quindi creare, aggiornare o eliminare qualsiasi stack in uno qualsiasi degli account di destinazione.

Strutturando le autorizzazioni in questo modo, gli utenti non assegnano un ruolo di amministrazione durante la creazione o l'aggiornamento di un StackSet



Administrator account

Nell'account amministratore, crea un ruolo IAM denominato `AWSCloudFormationStackSetAdministrationRole`.

Puoi farlo creando uno stack dal CloudFormation modello disponibile in <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/AWSCloudFormationStackSetAdministrationRole.yml>.

Example Esempio di politica delle autorizzazioni

Il ruolo di amministrazione creato dal modello precedente include la seguente politica di autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AWSCloudFormationStackSetExecutionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Example Esempio di politica di fiducia 1

Il modello precedente include anche la seguente politica di fiducia che concede al servizio l'autorizzazione a utilizzare il ruolo di amministrazione e le autorizzazioni associate al ruolo.

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

```
}  
]  
}
```

Example Esempio di politica di fiducia 2

Per distribuire le istanze dello stack in un account di destinazione che risiede in una regione disattivata per impostazione predefinita, devi includere anche il responsabile del servizio regionale per quella regione. Ogni Regione disabilitata per impostazione predefinita avrà un proprio principale del servizio regionale.

L'esempio seguente di politica di fiducia concede al servizio l'autorizzazione a utilizzare il ruolo di amministrazione nella regione Asia Pacifico (Hong Kong) (ap-east-1), una regione disabilitata per impostazione predefinita.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": [  
          "cloudformation.amazonaws.com",  
          "cloudformation.ap-east-1.amazonaws.com"  
        ]  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

Per ulteriori informazioni, consulta [Preparati a eseguire StackSet operazioni Regioni AWS disattivate per impostazione predefinita](#). Per un elenco dei codici regionali, consulta [Endpoint regionali](#) nella Riferimenti generali di AWS Guida.

Target accounts

In ogni account di destinazione, crea un ruolo di servizio denominato `AWSCloudFormationStackSetExecutionRole` che consideri attendibile l'account amministratore. Il ruolo deve avere questo nome esatto. [Puoi farlo creando uno stack dal CloudFormation modello disponibile in .yaml](#). <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us->

[east-1/ AWSCloudFormationStackSetExecutionRole](#) Quando si utilizza questo modello, viene richiesto di fornire l'ID dell'account amministratore con cui l'account di destinazione deve avere una relazione di fiducia.

 Important

Questo modello concede l'accesso di amministratore. Dopo aver utilizzato il modello per creare un ruolo di esecuzione dell'account di destinazione, è necessario definire l'ambito delle autorizzazioni contenute nella dichiarazione politica in base ai tipi di risorse che si stanno creando utilizzando StackSets

Il ruolo del servizio dell'account di destinazione richiede le autorizzazioni per eseguire tutte le operazioni specificate CloudFormation nel modello. Ad esempio, se il modello crea un bucket S3, è necessario disporre delle autorizzazioni per creare nuovi oggetti per S3. L'account di destinazione richiede sempre le autorizzazioni CloudFormation complete, che includono le autorizzazioni per creare, aggiornare, eliminare e descrivere gli stack.

Example Esempio di politica delle autorizzazioni 1

Il ruolo creato da questo modello abilita la seguente policy su un account di destinazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Example Esempio di politica di autorizzazione 2

L'esempio seguente mostra una dichiarazione politica con le autorizzazioni minime StackSets per funzionare. Per creare pile negli account di destinazione che utilizzano risorse di servizi diversi da CloudFormation, è necessario aggiungere tali azioni e risorse di servizio all'AWSCloudFormationStackSetExecutionRole informativa relativa a ciascun account di destinazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempio di politica di fiducia

La seguente relazione di trust viene creata dal modello. L'ID dell'account amministratore viene visualizzato come *admin_account_id*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::admin_account_id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

È possibile configurare la relazione di trust di un ruolo di esecuzione dell'account di destinazione esistente per stabilire una relazione di trust con un determinato ruolo nell'account amministratore. Se elimini il ruolo nell'account amministratore e ne crei uno nuovo per sostituirlo, devi configurare le relazioni di fiducia dell'account di destinazione con il nuovo ruolo dell'account amministratore, rappresentato *admin_account_id* nell'esempio precedente.

Imposta le opzioni di autorizzazione avanzate per le operazioni StackSet

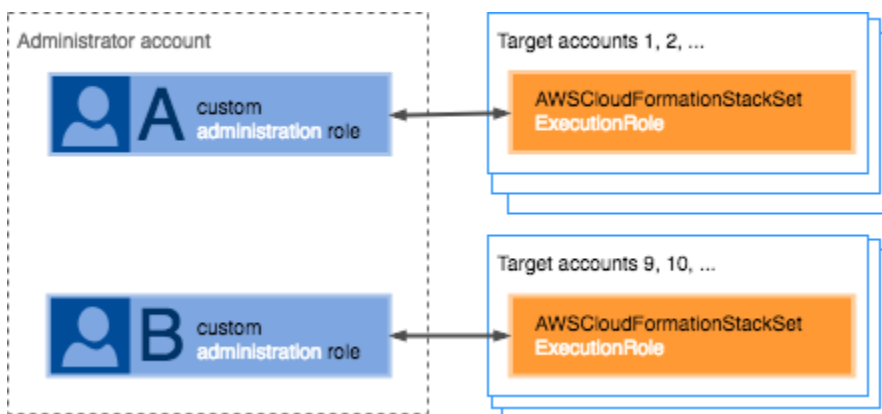
Se hai bisogno di un controllo più preciso su StackSets ciò che utenti e gruppi creano tramite un singolo account amministratore, puoi utilizzare i ruoli IAM per specificare:

- Quali utenti e gruppi possono eseguire StackSet operazioni in quali account di destinazione.
- Quali risorse gli utenti e i gruppi possono includere nei propri StackSets.
- Quali StackSet operazioni possono eseguire utenti e gruppi specifici.

Controlla quali utenti possono eseguire StackSet operazioni su account di destinazione specifici

Utilizza ruoli amministrativi personalizzati per controllare quali utenti e gruppi possono eseguire StackSet operazioni in quali account di destinazione. Potresti voler controllare quali utenti dell'account amministratore possono eseguire StackSet operazioni in quali account di destinazione. A tale scopo, si crea una relazione di fiducia tra ciascun account di destinazione e uno specifico ruolo di amministrazione personalizzato, anziché creare il ruolo di `AWSCloudFormationStackSetAdministrationRole` nell'account amministratore stesso. Si attivano quindi utenti e gruppi specifici per utilizzare il ruolo di amministrazione personalizzato quando si eseguono StackSet operazioni in un account di destinazione specifico.

Ad esempio, è possibile creare Ruolo A e Ruolo B all'interno dell'account amministratore. È possibile assegnare a Ruolo A le autorizzazioni per accedere all'account di destinazione 1 tramite l'account 8. È possibile assegnare a Ruolo B le autorizzazioni per accedere all'account di destinazione 9 tramite l'account 16.



L'impostazione delle autorizzazioni necessarie implica la definizione di un ruolo di amministrazione personalizzato, la creazione di un ruolo di servizio per l'account di destinazione e la concessione agli utenti dell'autorizzazione a passare il ruolo di amministrazione personalizzato durante l'esecuzione StackSet delle operazioni.

In generale, ecco come funziona una volta ottenute le autorizzazioni necessarie: quando si crea un ruolo di amministrazione personalizzato StackSet, l'utente deve specificare un ruolo di amministrazione personalizzato. L'utente deve disporre dell'autorizzazione per trasferire il ruolo a CloudFormation. Inoltre, il ruolo di amministrazione personalizzato deve avere una relazione di fiducia

con gli account di destinazione specificati per. StackSet CloudFormation crea StackSet e associa il ruolo di amministrazione personalizzato. Quando aggiorna un StackSet, l'utente deve specificare esplicitamente un ruolo di amministrazione personalizzato, anche se si tratta dello stesso ruolo di amministrazione personalizzato utilizzato in precedenza. StackSet CloudFormation utilizza quel ruolo per aggiornare lo stack, in base ai requisiti di cui sopra.

Administrator account

Example Esempio di politica delle autorizzazioni

Per ognuno StackSet, crea un ruolo di amministrazione personalizzato con le autorizzazioni per assumere il ruolo di esecuzione dell'account di destinazione.

Il nome del ruolo di esecuzione dell'account di destinazione deve essere lo stesso in ogni account di destinazione. Se il nome del ruolo è `AWSCloudFormationStackSetExecutionRole`, lo StackSet utilizza automaticamente durante la creazione di un StackSet. Se si specifica un nome di ruolo personalizzato, gli utenti devono fornire il nome del ruolo di esecuzione durante la creazione di un StackSet.

Crea un [ruolo di servizio IAM](#) con un nome personalizzato e la seguente politica di autorizzazioni. Negli esempi seguenti, *custom_execution_role* si riferisce al ruolo di esecuzione negli account di destinazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::target_account_id:role/custom_execution_role"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Per specificare più conti in un unico rendiconto, separali con virgole.

```
"Resource": [
```

```

    "arn:aws:iam::target_account_id_1:role/custom_execution_role",
    "arn:aws:iam::target_account_id_2:role/custom_execution_role"
  ]

```

È possibile specificare tutti gli account di destinazione utilizzando un carattere jolly (*) anziché un ID account.

```

"Resource": [
  "arn:aws:iam::*:role/custom_execution_role"
]

```

Example Esempio di politica di fiducia 1

È necessario fornire una policy di fiducia per il ruolo di servizio per definire quali dirigenti IAM possono assumere il ruolo.

```

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

```

Example Esempio di politica di fiducia 2

Per distribuire le istanze dello stack in un account di destinazione che risiede in una regione disattivata per impostazione predefinita, devi includere anche il responsabile del servizio regionale per quella regione. Ogni Regione disabilitata per impostazione predefinita avrà un proprio principale del servizio regionale.

L'esempio seguente di politica di fiducia concede al servizio l'autorizzazione a utilizzare il ruolo di amministrazione nella regione Asia Pacifico (Hong Kong) (ap-east-1), una regione disabilitata per impostazione predefinita.

```

{

```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "cloudformation.amazonaws.com",
        "cloudformation.ap-east-1.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }
]
```

Per ulteriori informazioni, consulta [Preparati a eseguire StackSet operazioni Regioni AWS disattivate per impostazione predefinita](#). Per un elenco dei codici regionali, consulta [Endpoint regionali](#) nella Guida di riferimento AWS generale.

Example Esempio di politica di passaggio del ruolo

È inoltre necessaria una politica di autorizzazioni IAM per gli utenti IAM che consenta all'utente di passare il ruolo di amministrazione personalizzato durante l'esecuzione StackSet delle operazioni. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un servizio AWS](#).

Nell'esempio seguente, *customized_admin_role* si riferisce al ruolo di amministrazione che l'utente deve assegnare.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/customized_admin_role"
    }
  ]
}
```

Target accounts

In ogni account di destinazione, crea un ruolo di servizio che si affidi al ruolo di amministrazione personalizzato che desideri utilizzare con questo account.

Il ruolo dell'account di destinazione richiede le autorizzazioni per eseguire tutte le operazioni specificate CloudFormation nel modello. Ad esempio, se il modello crea un bucket S3, è necessario disporre delle autorizzazioni per creare nuovi oggetti in S3. Il tuo account di destinazione necessita sempre di CloudFormation autorizzazioni complete, che includono le autorizzazioni per creare, aggiornare, eliminare e descrivere gli stack.

Il nome del ruolo dell'account di destinazione deve essere lo stesso in ogni account di destinazione. Se il nome del ruolo è `AWSCloudFormationStackSetExecutionRole`, lo `StackSets` utilizza automaticamente durante la creazione di un `StackSet`. Se si specifica un nome di ruolo personalizzato, gli utenti devono fornire il nome del ruolo di esecuzione durante la creazione di un `StackSet`.

Example Esempio di politica delle autorizzazioni

L'esempio seguente mostra una dichiarazione politica con le autorizzazioni minime `StackSets` per funzionare. Per creare pile negli account di destinazione che utilizzano risorse di servizi diversi da CloudFormation, è necessario aggiungere tali azioni e risorse di servizio alla politica delle autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempio di politica di fiducia

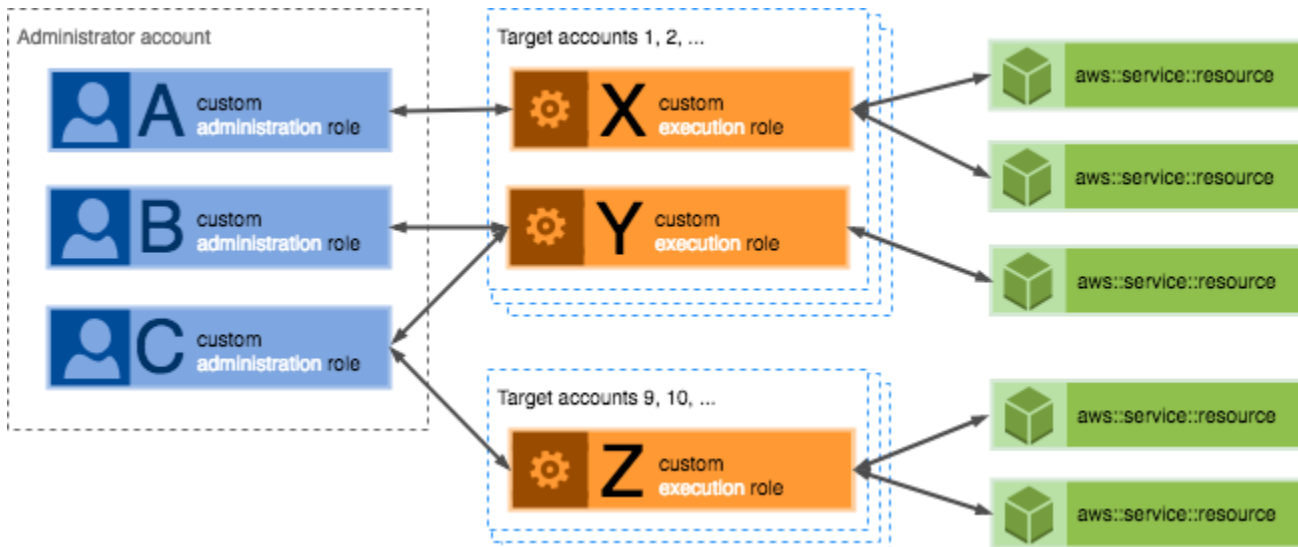
È necessario fornire la seguente politica di fiducia quando si crea il ruolo per definire la relazione di fiducia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::admin_account_id:role/customized_admin_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Controlla le risorse che gli utenti possono includere in specifiche StackSets

Utilizza ruoli di esecuzione personalizzati per controllare quali risorse dello stack utenti e gruppi possono includere nei propri StackSets. Ad esempio, potresti voler creare un gruppo che possa includere solo risorse relative ad Amazon S3 nel pacchetto creato, mentre un altro team può includere solo risorse DynamoDB. StackSets A tale scopo, si crea una relazione di fiducia tra il ruolo di amministrazione personalizzato per ogni gruppo e un ruolo di esecuzione personalizzato per ogni set di risorse. Il ruolo di esecuzione personalizzato definisce in quali risorse dello stack possono essere incluse. StackSets Il ruolo di amministrazione personalizzato risiede nell'account amministratore, mentre il ruolo di esecuzione personalizzato risiede in ogni account di destinazione in cui si desidera creare StackSets utilizzando le risorse definite. È quindi possibile attivare utenti e gruppi specifici per utilizzare il ruolo di amministrazione personalizzato durante l'esecuzione StackSets delle operazioni.

Ad esempio, è possibile creare ruoli amministrativi personalizzati A, B e C nell'account amministratore. Gli utenti e i gruppi autorizzati a utilizzare il ruolo A possono creare risorse StackSets contenenti lo stack specificamente elencate nel ruolo di esecuzione personalizzato X, ma non quelle nei ruoli Y o Z o risorse non incluse in alcun ruolo di esecuzione.



Quando aggiorna un StackSet, l'utente deve specificare esplicitamente un ruolo di amministrazione personalizzato, anche se si tratta dello stesso ruolo di amministrazione personalizzato utilizzato StackSet in precedenza. CloudFormation esegue l'aggiornamento utilizzando il ruolo di amministrazione personalizzato specificato, purché l'utente disponga delle autorizzazioni per eseguire operazioni su tale ruolo. StackSet

Analogamente, l'utente può specificare anche un ruolo di esecuzione personalizzato. Se specificano un ruolo di esecuzione personalizzato, CloudFormation utilizza tale ruolo per aggiornare lo stack, in base ai requisiti di cui sopra. Se l'utente non specifica un ruolo di esecuzione personalizzato, CloudFormation esegue l'aggiornamento utilizzando il ruolo di esecuzione personalizzato precedentemente associato a StackSet, purché l'utente disponga delle autorizzazioni per eseguire operazioni su tale ruolo. StackSet

Administrator account

Crea un ruolo di amministrazione personalizzato nel tuo account amministratore, come descritto in [Controlla quali utenti possono eseguire StackSet operazioni su account di destinazione specifici](#). Includi una relazione di fiducia tra il ruolo di amministrazione personalizzato e i ruoli di esecuzione personalizzati che desideri venga utilizzato.

Example Esempio di politica delle autorizzazioni

L'esempio seguente è una politica di autorizzazioni per entrambi gli account AWS CloudFormation StackSet Execution Role definiti per l'account di destinazione, oltre a un ruolo di esecuzione personalizzato.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Stmt1487980684000",
    "Effect": "Allow",
    "Action": [
      "sts:AssumeRole"
    ],
    "Resource": [
      "arn:aws:iam::*:role/AWSCloudFormationStackSetExecutionRole",
      "arn:aws:iam::*:role/custom_execution_role"
    ]
  }
]
```

Target accounts

Negli account di destinazione in cui desideri creare i tuoi StackSets, crea un ruolo di esecuzione personalizzato che conceda le autorizzazioni ai servizi e alle risorse che desideri che utenti e gruppi possano includere in. StackSets

Example Esempio di politica delle autorizzazioni

L'esempio seguente fornisce le autorizzazioni minime per StackSets, oltre all'autorizzazione per creare tabelle Amazon DynamoDB.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:createTable"
      ],
      "Resource": "*"
    }
  ]
}
```



```
}  
]  
}
```

Example Esempio di politica di fiducia

È necessario fornire la seguente politica di fiducia quando si crea il ruolo per definire la relazione di fiducia.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::admin_account_id:role/customized_admin_role"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

Imposta le autorizzazioni per operazioni specifiche StackSet

Inoltre, è possibile impostare le autorizzazioni in base alle quali utenti e gruppi possono eseguire StackSet operazioni specifiche, come la creazione, l'aggiornamento o l'eliminazione StackSets di istanze o lo stack di istanze. Per ulteriori informazioni, consulta [Operazioni, risorse e chiavi di condizione per CloudFormation](#) nella Documentazione di riferimento per l'autorizzazione al servizio.

Configurazione di chiavi globali per mitigare i problemi di "confused deputy"

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Inoltre AWS, l'impersonificazione tra servizi può portare al confuso problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Ti consigliamo di utilizzare [aws:SourceArn](#) le chiavi di contesto della condizione [aws:SourceAccount](#) globale nelle politiche delle risorse per limitare le autorizzazioni che AWS CloudFormation StackSets forniscono un altro servizio alla risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:cloudformation::123456789012:*`. Quando possibile, usa `aws:SourceArn`, perché è più specifico. Utilizza `aws:SourceAccount` solo quando non è possibile determinare il modello ARN o ARN corretto.

Quando StackSets assume il ruolo di amministratore nel tuo account amministratore, StackSets inserisce l'ID dell'account amministratore e StackSets Amazon Resource Name (ARN). Per questo motivo, puoi definire le condizioni per le [chiavi globali](#) `aws:SourceAccount` e `aws:SourceArn` nelle relazioni di trust per prevenire [problemi di "confused deputy"](#). L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition StackSets per evitare il confuso problema del vice.

Administrator account

Example Chiavi globali per `aws:SourceAccount` e `aws:SourceArn`

Durante l'utilizzo StackSets, definite le chiavi globali `aws:SourceAccount` e `aws:SourceArn` la vostra politica di `AWSCloudFormationStackSetAdministrationRole` fiducia per evitare problemi confusi tra i vicepresidenti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

```

    },
    "StringLike": {
      "aws:SourceArn": "arn:aws:cloudformation:*:111122223333:stackset/*"
    }
  }
}
]
}

```

Example StackSets ARNs

Specificate il vostro associato StackSets ARNs per un controllo più preciso.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": [
            "arn:aws:cloudformation:STACKSETS-REGION:111122223333:stackset/STACK-SET-ID-1",
            "arn:aws:cloudformation:STACKSETS-REGION:111122223333:stackset/STACK-SET-ID-2"
          ]
        }
      }
    }
  ]
}

```

Attiva l'accesso affidabile per StackSets con AWS Organizations

Questo argomento fornisce istruzioni su come attivare l'accesso affidabile con AWS Organizations, necessario per la distribuzione su più account e Regioni AWS l'utilizzo delle autorizzazioni gestite

dal StackSets servizio. Per utilizzare le autorizzazioni gestite automaticamente, consulta invece.

[Concedere autorizzazioni gestite dal cliente](#)

Prima di creare un account StackSet con autorizzazioni gestite dal servizio, devi prima completare le seguenti attività:

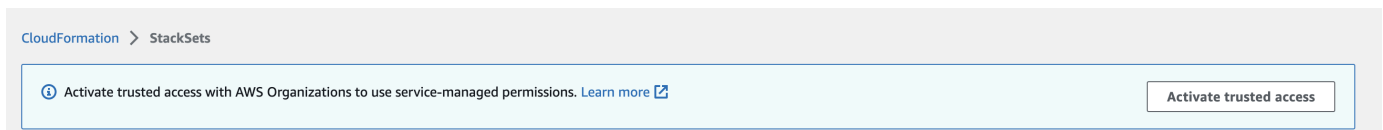
- [Abilita tutte le funzionalità](#) in. AWS Organizations Con solo le funzionalità di fatturazione consolidate abilitate, non puoi crearne una StackSet con autorizzazioni gestite dal servizio.
- Attiva l'accesso affidabile con. AWS Organizations Questa azione consente di CloudFormation creare un ruolo collegato al servizio nell'account di gestione. Dopo l'attivazione dell'accesso affidabile, quando si CloudFormation crea un ruolo StackSet con autorizzazioni gestite dal servizio, viene creato sia il ruolo collegato al servizio necessario sia un ruolo di servizio denominato `stacksets-exec-*` negli account di destinazione (membri).

Con l'accesso affidabile attivato, l'account di gestione e gli account amministratore delegato possono creare e gestire servizi gestiti per la propria organizzazione. StackSets

Per attivare l'accesso affidabile, devi essere un utente amministratore nell'account di gestione. Un utente amministratore è un utente con autorizzazioni complete per il tuo Account AWS. Per ulteriori informazioni, consulta [Crea un utente amministratore](#) nella Guida Gestione dell'account AWS di riferimento. Per consigli su come proteggere la sicurezza dell'account di gestione, consulta [le migliori pratiche per l'account di gestione](#) nella Guida per l'AWS Organizations utente.

Per attivare l'accesso affidabile

1. Accedi AWS come amministratore dell'account di gestione e apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Dal pannello di navigazione, scegli StackSets. Se l'accesso attendibile è disabilitato, viene visualizzato un banner che richiede di abilitarlo.



3. Scegli Attiva accesso attendibile.

L'accesso attendibile è abilitato quando viene visualizzato il seguente banner.



 Note

L'opzione Attiva accesso delle organizzazioni è uguale all'opzione Abilita accesso delle organizzazioni e Disattiva accesso delle organizzazioni è uguale a Disabilita accesso delle organizzazioni. Questi termini sono stati aggiornati in base alle linee guida di marketing.

Per disattivare l'accesso attendibile

Vedi [AWS CloudFormation StackSets e AWS Organizations](#) nella Guida AWS Organizations per l'utente.

Prima di poter disattivare l'accesso affidabile con AWS Organizations, è necessario annullare la registrazione di tutti gli amministratori delegati. Per ulteriori informazioni, consulta [Registrazione di un amministratore delegato](#).

 Note

Per informazioni sull'utilizzo delle operazioni API anziché della console per attivare o disattivare l'accesso affidabile, consulta:

- [ActivateOrganizationsAccess](#)
- [DeactivateOrganizationsAccess](#)
- [DescribeOrganizationsAccess](#)

Ruoli collegati ai servizi

L'account di gestione utilizza il ruolo collegato al `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` servizio. È possibile modificare o eliminare questo ruolo solo se l'accesso attendibile con AWS Organizations è disattivato.

Ogni account di destinazione utilizza un ruolo collegato al `AWSServiceRoleForCloudFormationStackSetsOrgMembers` servizio. È possibile modificare o eliminare questo ruolo solo a due condizioni: se l'accesso affidabile con AWS Organizations è disattivato o se l'account viene rimosso dall'organizzazione o dall'unità organizzativa (OU) di destinazione.

Per ulteriori informazioni, vedere [AWS CloudFormation StackSets e AWS Organizations](#) nella Guida per l'AWS Organizations utente.

Registrare un account membro amministratore delegato

Oltre all'account di gestione dell'organizzazione, gli account dei membri con autorizzazioni di amministratore delegato possono creare e gestire StackSets con autorizzazioni gestite dal servizio per l'organizzazione. StackSets con autorizzazioni gestite dal servizio vengono creati nell'account di gestione, inclusi quelli creati da amministratori delegati. StackSets Per essere registrato come amministratore delegato per l'organizzazione, l'account membro deve trovarsi nell'organizzazione. Per ulteriori informazioni sull'adesione a un'organizzazione, vedi [Invitare](#) un utente a entrare a far parte dell'organizzazione. Account AWS

L'organizzazione può avere fino a cinque amministratori delegati registrati contemporaneamente. Gli amministratori delegati possono scegliere di eseguire l'implementazione su tutti gli account dell'organizzazione o su account specifici. OUs L'accesso affidabile con AWS Organizations deve essere attivato prima che gli amministratori delegati possano effettuare la distribuzione sugli account gestiti da Organizations. Per ulteriori informazioni, consulta [Attiva l'accesso affidabile per StackSets con AWS Organizations](#).

Important

Tieni presente quanto segue:

- Gli amministratori delegati dispongono delle autorizzazioni complete per la distribuzione negli account dell'organizzazione. L'account di gestione non può limitare le autorizzazioni degli amministratori delegati per la distribuzione a operazioni specifiche OUs o per l'esecuzione di operazioni specifiche. StackSet
- Assicurati che gli amministratori delegati dispongano delle `organizations:ListDelegatedAdministrators` autorizzazioni necessarie per evitare potenziali errori.

Puoi registrare amministratori delegati per la tua organizzazione nelle seguenti regioni: Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Tokyo), Canada (Centrale), Europa (Francoforte), Europa (Irlanda), Europa (Londra), Europa (Parigi), Europa (Stoccolma), Israele (Tel

Aviv), Sud America (San Paolo), (Stati Uniti orientali) e (Stati Uniti occidentali). AWS GovCloud AWS GovCloud

È possibile registrare e annullare la registrazione degli amministratori delegati utilizzando la [AWS CloudFormation console AWS CLI](#), oppure [AWS SDKs](#).

Per registrare un amministratore delegato (console)

1. Accedere AWS come amministratore dell'account di gestione e aprire la console all'indirizzo. AWS CloudFormation <https://console.aws.amazon.com/cloudformation/>
2. Dal pannello di navigazione, scegli StackSets.
3. In Amministratori delegati, seleziona Registra amministratore delegato.
4. Nella finestra di dialogo Registra amministratore delegato, seleziona Registra amministratore delegato.

Il messaggio di esito positivo indica che l'account membro è stato correttamente registrato come amministratore delegato.

Per annullare la registrazione di un amministratore delegato (console)

1. Accedi AWS come amministratore dell'account di gestione e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/>.
2. Dal pannello di navigazione, scegli StackSets.
3. In Amministratori delegati, seleziona l'account per cui desideri annullare la registrazione, quindi scegli Annulla registrazione.

Il messaggio di esito positivo indica che la registrazione dell'account membro come amministratore delegato è stata correttamente annullata.

Potrai registrare nuovamente questo account in qualsiasi momento.

Per registrare un amministratore delegato ()AWS CLI

1. Aprire il. AWS CLI
2. Esegui il comando `register-delegated-administrator`.

```
$ aws organizations register-delegated-administrator \
```

```
--service-principal=member.org.stacksets.cloudformation.amazonaws.com \  
--account-id="memberAccountId"
```

3. Esegui il comando `list-delegated-administrators` per verificare che l'account membro specificato sia stato registrato correttamente come amministratore delegato.

```
$ aws organizations list-delegated-administrators \  
--service-principal=member.org.stacksets.cloudformation.amazonaws.com
```

Per annullare la registrazione di un amministratore delegato ()AWS CLI

1. Aprire il. AWS CLI
2. Esegui il comando `deregister-delegated-administrator`.

```
$ aws organizations deregister-delegated-administrator \  
--service-principal=member.org.stacksets.cloudformation.amazonaws.com \  
--account-id="memberAccountId"
```

3. Esegui il comando `list-delegated-administrators` per verificare che la registrazione dell'account membro specificato come amministratore delegato sia stata correttamente annullata.

```
$ aws organizations list-delegated-administrators \  
--service-principal=member.org.stacksets.cloudformation.amazonaws.com
```

Potrai registrare nuovamente questo account in qualsiasi momento.

Inizia a StackSets usare un modello di esempio

Questo tutorial ti aiuterà a iniziare a StackSets utilizzare il. AWS Management Console Ti guida nella creazione di StackSet un modello di esempio. Imparerai come distribuire gli stack in più regioni, monitorare StackSet le operazioni e visualizzare i risultati.

In questo tutorial, ne creerai una StackSet che abiliti AWS Config Account AWS nella tua regione () degli Stati Uniti occidentali (Oregonus-west-2) e negli Stati Uniti orientali (Virginia settentrionale) (). us-east-1 Con StackSets, puoi creare, aggiornare o eliminare pile su più account e regioni con un'unica operazione, rendendola la soluzione ideale per la gestione dell'infrastruttura su larga scala. Sebbene questo tutorial utilizzi un unico account per semplicità, dimostra efficacemente le funzionalità multiregionali di. StackSets

Il modello di esempio è disponibile nel seguente bucket S3: Enable .yaml. <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/AWSConfig>

Note

StackSets è gratuito, ma ti verranno addebitate le AWS risorse che crei con esso, come AWS Config in questo tutorial. Per ulteriori informazioni, consulta [Prezzi di AWS Config](#).

Argomenti

- [Prerequisiti](#)
- [Crea un modello StackSet con un esempio dalla console](#)
- [Monitora StackSet la creazione](#)
- [Visualizza i risultati StackSet](#)
- [Aggiorna il tuo StackSet](#)
- [Aggiungi pile al tuo StackSet](#)
- [Eliminazione](#)
- [Passaggi successivi](#)

Prerequisiti

Prima di iniziare questo tutorial, assicurati di aver completato i seguenti prerequisiti:

- È necessario aver configurato i ruoli IAM richiesti per le autorizzazioni autogestite. Per creare StackSet e distribuire gli stack all'interno di un singolo account, devi avere i seguenti ruoli nel tuo account:
 - `AWSCloudFormationStackSetAdministrationRole`
 - `AWSCloudFormationStackSetExecutionRole`

Per istruzioni dettagliate sulla configurazione di questi ruoli, consulta. [Concedere autorizzazioni gestite dal cliente](#)

Crea un modello StackSet con un esempio dalla console

Per creare un file StackSet che abiliti AWS Config

1. Apri la [CloudFormation console](#).
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il modulo StackSet da Regione AWS cui vuoi gestire.

Puoi scegliere qualsiasi regione che supporti StackSets. La regione selezionata non influisce sulle regioni in cui puoi effettuare la distribuzione con il tuo StackSet.
3. Dal riquadro di navigazione, scegli StackSets.
4. Nella parte superiore della StackSetspagina, scegli Crea StackSet.
5. In Autorizzazioni, scegli Autorizzazioni self-service e scegli i ruoli IAM che hai creato nei prerequisiti.
 - Per il ruolo di amministratore IAM, scegli. `AWSCloudFormationStackSetAdministrationRole`
 - Per il nome del ruolo di esecuzione IAM, scegli `AWSCloudFormationStackSetExecutionRole`.
6. In Prerequisite - Prepare template (Prerequisito - Prepara modello), scegliere Use a sample template (Utilizza un modello di esempio).
7. In Seleziona un modello di esempio, scegli Abilita AWS Config modello. Quindi, seleziona Next (Successivo).

Questo modello crea le risorse necessarie da abilitare AWS Config nel tuo account, tra cui un registratore di configurazione e un canale di distribuzione.
8. Nella pagina Specificare StackSet i dettagli, per StackSet nome, immetteremy-awsconfig-stackset.
9. Per la StackSet descrizione, immettere**A StackSet that enables Config across multiple Regions.**
10. In Parametri, AWS Config configurate le impostazioni come segue:
 - a. Per Supporta tutti i tipi di risorse, mantieni il valore predefinito, true, per registrare tutti i tipi di risorse supportati.
 - b. Per Include tipi di risorse globali, mantieni il valore predefinito, false, per escludere risorse globali come i ruoli IAM.
 - c. Lascia l'opzione Elenco dei tipi di risorse se non tutti i tipi di risorse sono supportati impostata su<All>.

- d. Per L'area contenente la risorsa ruolo collegata al servizio Config, sostituire < > con.
DeployToAnyRegion us-west-2

Ciò significa che il ruolo collegato al servizio denominato **AWSServiceRoleForConfig** verrà creato solo se uno stack viene distribuito nella regione Stati Uniti occidentali (Oregon). Sceglierei le regioni di distribuzione più avanti in questa procedura.

- e. Per la frequenza di registrazione del registratore Configuration, scegli Registrazione GIORNALIERA.

11. Seleziona Successivo per continuare.

12. Nella pagina Configura StackSet opzioni, scegli Aggiungi nuovo tag e aggiungi un tag specificando una coppia chiave/valore:

- a. In Chiave, inserire **Stage**.
- b. In Valore, specifica **Test**.

I tag a cui ti applichi StackSets vengono applicati alle risorse create dai tuoi stack.

13. Per la configurazione di Execution, scegli Active per abilitare CloudFormation la gestione ottimizzata delle operazioni:

- Le operazioni non in conflitto vengono eseguite contemporaneamente per tempi di implementazione più rapidi.
- Le operazioni in conflitto vengono automaticamente messe in coda ed elaborate nell'ordine in cui sono state richieste.

Mentre le operazioni sono in esecuzione o in CloudFormation coda, mette in coda tutte le operazioni in entrata anche se non sono in conflitto. Non è possibile modificare le impostazioni di esecuzione durante questo periodo.

14. Scegli Next (Successivo).

15. Nella pagina Imposta opzioni di distribuzione, per Aggiungi stack a StackSet, scegli Distribuisci nuovi stack.

16. Per Accounts (Account), scegliere Deploy stacks in accounts (Distribuisci stack in account).

17. Nella casella di testo, inserisci il tuo ID. Account AWS

18. Per Specificare le regioni, seleziona le seguenti regioni in questo ordine:

1. Regione Stati Uniti occidentali (Oregon) (us-west-2)

2. Regione Stati Uniti orientali (Virginia settentrionale) () us-east-1

Utilizzate la freccia rivolta verso l'alto accanto alla regione Stati Uniti occidentali (Oregon) per spostarla come prima voce nell'elenco, se necessario. L'ordine delle regioni determina l'ordine di distribuzione.

19. Per le opzioni di distribuzione, configura le seguenti impostazioni:

- a. Per Maximum concurrent accounts (Numero massimo di account simultanei), mantieni i valori predefiniti di Number (Numero) e 1.

Per le distribuzioni con più account, questa impostazione significa che lo stack CloudFormation viene distribuito in un solo account alla volta.

- b. Per Failure tolerance (Tolleranza di errore), mantenere i valori predefiniti di Number (Numero) e 0.

Ciò significa che un massimo di distribuzioni pari a zero stack possono fallire in una delle regioni specificate prima CloudFormation di interrompere la distribuzione nella regione corrente e annullare le distribuzioni nelle regioni rimanenti.

- c. Per la concorrenza regionale, scegli Sequenziale (impostazione predefinita).

Questa impostazione garantisce il CloudFormation completamento delle distribuzioni in una regione prima di passare alla successiva.

- d. Per la modalità Concurrency, mantieni l'impostazione predefinita di Strict failure tolerance.

Per le implementazioni con più account, ciò riduce il livello di concorrenza degli account in caso di errori, rimanendo entro la tolleranza di errore +1.

20. Scegli Next (Successivo).

21. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.

22. Quando sei pronto per creare il tuo StackSet, scegli Invia.

Monitora StackSet la creazione

Dopo aver scelto Invia, CloudFormation inizia a creare i tuoi stack StackSet e a distribuirli nelle regioni specificate nel tuo account. La pagina dei StackSet dettagli si apre automaticamente, in cui è possibile monitorare lo stato di avanzamento dell'operazione.

Per monitorare la StackSet creazione

1. Nella pagina dei StackSet dettagli, per impostazione predefinita, viene visualizzata la scheda Operazioni, che mostra l'operazione corrente in corso.
2. Lo stato dell'operazione dovrebbe essere RUNNING iniziale. CloudFormation crea stack nelle regioni specificate in base alle opzioni di distribuzione configurate.
3. Per visualizzare ulteriori dettagli sull'operazione, seleziona l'ID dell'operazione nell'elenco.
4. Nella pagina dei dettagli dell'operazione, è possibile visualizzare lo stato delle istanze dello stack create in ciascuna regione.
5. Attendi che lo stato dell'operazione cambi a SUCCEEDED, il che indica che tutte StackSet le relative istanze dello stack sono state create correttamente.

Visualizza i risultati StackSet

Una volta completata la StackSet creazione, puoi visualizzare le istanze dello stack distribuite e verificare che siano AWS Config state abilitate nel tuo account nelle regioni specificate.

Per visualizzare i risultati StackSet

1. Nella pagina dei StackSet dettagli, scegli la scheda Stack instances.
2. Dovresti vedere un elenco di istanze stack create nel tuo account nelle regioni specificate. Ogni istanza dello stack deve avere uno stato pari a SUCCEEDED, a indicare che è stata distribuita con successo.
3. Per verificare che AWS Config sia abilitata nel tuo account, puoi controllare la AWS Config console in ciascuna delle regioni distribuite.

Aggiorna il tuo StackSet

Dopo aver creato il tuo StackSet, potresti volerlo aggiornare per modificare i valori dei parametri o aggiungere altre regioni. Questa sezione mostra come aggiornare il parametro della frequenza di AWS Config registrazione.

Per aggiornare il StackSet

1. Nella StackSet pagina, seleziona il tuo **my-awsconfig-stackset**.
2. Dopo aver StackSet selezionato, scegli Modifica StackSet dettagli dal menu Azioni.

3. Nella pagina Scegli un modello, per Prerequisito - Prepara modello, scegli Usa il modello corrente.
4. Scegli Next (Successivo).
5. Nella pagina Specificare StackSet i dettagli, in Parametri, trova la frequenza di registrazione del registratore di configurazione e modificala da GIORNALIERA a CONTINUA.
6. Scegli Next (Successivo).
7. Nella pagina Configura StackSet le opzioni, lascia le impostazioni invariate e scegli Avanti.
8. Nella pagina Imposta le opzioni di distribuzione, specifica l'ID del tuo account e le stesse regioni che hai utilizzato durante la creazione di StackSet.
9. Per le opzioni di distribuzione, mantieni le stesse impostazioni di prima.
10. Scegli Next (Successivo).
11. Nella pagina Revisione, rivedi le modifiche e scegli Invia.
12. CloudFormation inizia ad aggiornare il tuo StackSet. È possibile monitorare lo stato di avanzamento nella scheda Operazioni della pagina dei StackSet dettagli.

Aggiungi pile al tuo StackSet

Puoi aggiungere altri stack ai tuoi StackSet distribuendoli in altre regioni. Questa sezione mostra come aggiungere pile a una nuova regione.

Per aggiungere pile al tuo StackSet

1. Nella StackSetspagina, seleziona il tuo **my-awsconfig-stackset**.
2. Con quello StackSet selezionato, scegli Aggiungi pile a StackSet dal menu Azioni.
3. Nella pagina Imposta le opzioni di distribuzione, per Aggiungi stack a StackSet, scegli Distribuisci nuovi stack.
4. Per gli account, scegli Distribuisci gli stack negli account e inserisci l'ID del tuo account.
5. Per Specificare le regioni, selezionare una nuova regione, ad esempio Europa (Irlanda) eu-west-1 ().
6. Per le opzioni di distribuzione, mantieni le stesse impostazioni di prima.
7. Scegli Next (Successivo).
8. Nella pagina Specify Overrides, lascia i valori delle proprietà come specificato e scegli Avanti.
9. Nella pagina Review (Rivedi), rivedere le selezioni e scegliere Submit (Invia).

10. CloudFormation inizia a creare nuovi stack nella regione specificata. È possibile monitorare l'avanzamento nella scheda Operazioni della pagina dei StackSet dettagli.

Eliminazione

Per evitare di incorrere in addebiti per AWS Config risorse indesiderate, dovresti effettuare la pulizia eliminando gli stack dal tuo account StackSet, eliminando quelli StackSet stessi e rimuovendo i ruoli IAM che hai creato per questo tutorial. Poiché tutte le risorse sono distribuite all'interno del tuo account, la pulizia è semplice.

Per eliminare gli stack dal tuo StackSet

1. Nella StackSetspagina, seleziona il tuo **my-awsconfig-stackset**.
2. Una volta StackSet selezionato, scegli Elimina pile StackSet dal menu Azioni.
3. Nella pagina Imposta le opzioni di distribuzione, per Account, scegli Distribuisci gli stack negli account e inserisci l'ID del tuo account.
4. Per Specificare le regioni, seleziona tutte le regioni in cui hai distribuito gli stack.
5. Per le opzioni di distribuzione, mantieni le impostazioni predefinite.
6. Assicuratevi che Retain stacks non sia attivato, in modo che gli stack e le relative risorse vengano eliminati.
7. Scegli Next (Successivo).
8. Nella pagina Review (Rivedi), rivedere le selezioni e scegliere Submit (Invia).
9. CloudFormation inizia a eliminare gli stack dal tuo StackSet. È possibile monitorare l'avanzamento nella scheda Operazioni della pagina dei StackSet dettagli.

Per eliminare i tuoi StackSet

1. Dopo che tutti gli stack sono stati eliminati, nella StackSetspagina, seleziona il tuo **my-awsconfig-stackset**.
2. Una volta StackSet selezionato, scegli Elimina StackSet dal menu Azioni.
3. Quando viene richiesto di confermare, scegliete Elimina.

Per eliminare i ruoli del servizio IAM

Poiché l'hai distribuito solo sul tuo account, devi solo eliminare i ruoli IAM da questo singolo account, rendendo la pulizia molto più semplice rispetto alle distribuzioni con più account.

1. Apri la [console IAM](#).
2. Nel riquadro di navigazione scegliere Roles (Ruoli).
3. Nella casella di ricerca, inserisci **AWSCloudFormationStackSet** per trovare i ruoli che hai creato per questo tutorial.
4. Seleziona la casella di controllo accanto a. **AWSCloudFormationStackSetAdministrationRole**
5. Scegli Elimina nella parte superiore della pagina.
6. Nella finestra di dialogo di conferma, inserisci **delete** e scegli Elimina.
7. Ripeti la stessa procedura per eliminare il **AWSCloudFormationStackSetExecutionRole**.

Dopo aver eliminato il StackSet, un bucket Amazon S3 rimarrà in Regione AWS ciascuno a causa dell'attributo **DeletionPolicy** sulla risorsa. **AWS::S3::Bucket** In questo modo vengono preservati i dati della cronologia. AWS Config Se non hai più bisogno di questi dati, puoi tranquillamente eliminare il bucket manualmente. Prima di poter eliminare un bucket, è necessario prima svuotarlo. Lo svuotamento di un bucket comporta l'eliminazione di tutti gli oggetti in esso contenuti.

Per svuotare ed eliminare i bucket Amazon S3

1. Apri la [console Amazon S3](#).
2. Nel riquadro di navigazione sul lato sinistro della console scegliere Bucket.
3. Nell'elenco dei bucket, vedrai i bucket creati a tale scopo StackSet in ogni regione in cui hai distribuito. Seleziona l'opzione accanto al nome del bucket creato a tale scopo StackSet, quindi scegli Empty.
4. Nella pagina Svuota il bucket, conferma che desideri svuotare il bucket digitando **permanently delete** nel campo di testo, quindi scegli Svuota.
5. Monitorare l'avanzamento del processo di svuotamento del bucket nella pagina Svuota bucket: stato.
6. Per tornare all'elenco dei bucket, scegliere Exit (Esci).
7. Seleziona l'opzione accanto al nome del bucket, quindi scegli Elimina.

8. Quando viene richiesta la conferma, digita il nome del bucket, quindi scegli Elimina bucket.
9. Monitora l'avanzamento del processo di eliminazione del bucket dall'elenco dei bucket. Quando Amazon S3 completa l'eliminazione del bucket, lo rimuove dall'elenco.
10. Ripeti questo processo per ogni bucket creato da nelle diverse regioni. StackSet

Passaggi successivi

Complimenti! Hai creato con successo un modello StackSet utilizzando un modello di esempio, distribuito gli stack in più regioni del tuo account, aggiornato StackSet, aggiunto altri stack e ripulito le tue risorse. Concentrandoti sulla distribuzione con un solo account, hai semplificato il processo di pulizia, pur continuando ad apprendere le principali funzionalità multiregionali di StackSets

Per saperne di più StackSets, esplora i seguenti argomenti:

- [Sostituisci i valori dei parametri sugli stack all'interno del tuo CloudFormation StackSet](#)— Scopri come sovrascrivere i valori dei parametri per account e regioni specifici.
- [Crea AWS CloudFormation StackSets con autorizzazioni gestite dal servizio](#)— Esplora la creazione di implementazioni StackSets per più account con AWS Organizations

Crea AWS CloudFormation StackSets con autorizzazioni autogestite

Questo argomento descrive come creare StackSets con autorizzazioni autogestite per distribuire stack in tutte le regioni. Account AWS

Note

Prima di continuare, crea i ruoli di servizio IAM necessari StackSets per stabilire una relazione di fiducia tra l'account da cui amministri e l'account su cui stai StackSet distribuendo gli stack. Per ulteriori informazioni, consulta [Concedere autorizzazioni gestite dal cliente](#).

Argomenti

- [Crea un account StackSet con autorizzazioni autogestite \(console\)](#)
- [Crea un file StackSet con autorizzazioni gestite automaticamente \(AWS CLI\)](#)

Crea un account StackSet con autorizzazioni autogestite (console)

Per creare un StackSet

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il modulo da Regione AWS cui vuoi gestire. StackSet
3. Dal pannello di navigazione, scegli StackSets.
4. Nella parte superiore della StackSetspagina, scegli Crea StackSet.
5. In Autorizzazioni, scegli Autorizzazioni self-service e scegli i ruoli IAM che hai creato.
6. In Prerequisito: prepara il modello, scegli Il modello è pronto.
7. In Specify template (Specifica modello), scegliere di specificare l'URL per il bucket S3 che contiene il modello di stack oppure caricare un file modello di stack. Quindi, seleziona Next (Successivo).
8. Nella pagina Specificate StackSet i dettagli, fornite un nome per il StackSet, specificate eventuali parametri e quindi scegliete Avanti.
9. Seleziona Successivo per continuare.
10. Nella pagina Configura StackSet opzioni, in Tag, specifica i tag da applicare alle risorse dello stack. Per ulteriori informazioni sull'utilizzo dei tag AWS, consulta [Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione dei costi nella Guida](#) per l'AWS Billing and Cost Management utente.
11. Per la configurazione di Execution, scegli Active per abilitare CloudFormation la gestione ottimizzata delle operazioni:
 - Le operazioni non in conflitto vengono eseguite contemporaneamente per tempi di implementazione più rapidi.
 - Le operazioni in conflitto vengono automaticamente messe in coda ed elaborate nell'ordine in cui sono state richieste.

Mentre le operazioni sono in esecuzione o in CloudFormation coda, mette in coda tutte le operazioni in entrata anche se non sono in conflitto. Non è possibile modificare le impostazioni di esecuzione durante questo periodo.

12. Se il modello contiene risorse IAM, per Capacità, scegli Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
13. Scegli Next (Successivo).
14. Nella pagina Imposta le opzioni di distribuzione, per Aggiungi stack a StackSet, scegli Distribuisci nuovi stack.
15. Per Accounts (Account), scegliere Deploy stacks in accounts (Distribuisci stack in account). Incolla i Account AWS numeri di destinazione nella casella di testo, separando più numeri con virgole.

 Note

Puoi includere l'ID del tuo account amministratore se desideri distribuire gli stack anche in quell'account.

16. In Specificare le regioni, scegli le regioni in cui desideri distribuire gli stack.
17. Per le opzioni di distribuzione, procedi come segue:
 - Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.
 - Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
 - Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
 - Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.
 - Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.
18. Scegli Next (Successivo).
19. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.
20. Quando sei pronto per creare il tuo StackSet, scegli Invia.

CloudFormation inizia a creare il tuo StackSet. Visualizza l'avanzamento e lo stato della creazione degli stack StackSet nella pagina dei StackSet dettagli che si apre quando scegli Invia.

Crea un file StackSet con autorizzazioni gestite automaticamente (AWS CLI)

Segui la procedura descritta in questa sezione per utilizzare: AWS CLI

- Crea il StackSet contenitore.
- Distribuisci istanze stack.

Per creare un StackSet

1. Usa il [create-stack-set](#) comando per creare un nuovo StackSet nome *my-stackset*. L'esempio seguente utilizza un modello memorizzato in un bucket S3 e include un parametro che imposta a *KeyPairName* con il valore. *TestKey*

```
aws cloudformation create-stack-set \  
  --stack-set-name my-stackset \  
  --template-url https://s3.region-code.amazonaws.com/amzn-s3-demo-bucket/  
MyApp.template \  
  --parameters ParameterKey=KeyPairName,ParameterValue=TestKey
```

2. Al termine del create-stack-set comando, esegui il [list-stack-sets](#) comando per verificare che il tuo sia StackSet stato creato. Dovresti vedere il tuo nuovo StackSet nei risultati.

```
aws cloudformation list-stack-sets
```

3. Usa il [create-stack-instances](#) comando per distribuire gli stack all'interno del tuo StackSet. L'esempio seguente distribuisce gli stack in due Account AWS (*account_ID_1* e *account_ID_2*) in due regioni (e). *us-west-2* *us-east-1*

Imposta l'elaborazione simultanea degli account e altre preferenze di distribuzione utilizzando l'opzione. `--operation-preferences` Questo esempio utilizza impostazioni basate sul conteggio. Nota che non `MaxConcurrentCount` deve superare `FailureToleranceCount + 1`. Per le impostazioni basate sulla percentuale, usa `FailureTolerancePercentage` o invece. `MaxConcurrentPercentage`

```
aws cloudformation create-stack-instances \  
  --stack-set-name my-stackset \  
  --accounts account_ID_1 account_ID_2 \  
  --regions us-west-2 us-east-1 \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per ulteriori informazioni, consulta [CreateStackInstances](#) nella documentazione di riferimento dell'API AWS CloudFormation .

4. Usa il [describe-stack-set-operation](#) comando per verificare che gli stack siano stati creati correttamente. Per l' `--operation-id` opzione, specificate l'ID dell'operazione che è stato restituito come parte dell'`create-stack-instances` output.

```
aws cloudformation describe-stack-set-operation \  
  --stack-set-name my-stackset \  
  --operation-id operation_ID
```

Crea AWS CloudFormation StackSets con autorizzazioni gestite dal servizio

Con le autorizzazioni gestite dal servizio, puoi distribuire stack su account gestiti da regioni specifiche. AWS Organizations Con questo modello, non è necessario creare i ruoli IAM necessari; CloudFormation crea i ruoli IAM per tuo conto. Per ulteriori informazioni, consulta [Attiva l'accesso affidabile](#).

Argomenti

- [Considerazioni](#)
- [Crea un account StackSet con autorizzazioni gestite dal servizio \(console\)](#)
- [Crea un file StackSet con autorizzazioni gestite dal servizio \(AWS CLI\)](#)

Considerazioni

Prima di creare un account StackSet con autorizzazioni gestite dal servizio, considera quanto segue:

- StackSets le autorizzazioni con gestione del servizio vengono create nell'account di gestione, incluse quelle create dagli amministratori StackSets delegati.

- **StackSet** È possibile scegliere come target l'intera organizzazione (inclusi tutti gli account) o unità organizzative specifiche (). OUs Se il tuo StackSet obiettivo è un'unità organizzativa principale, sarà indirizzata anche a qualsiasi bambino OUs. Se i tuoi StackSet obiettivi sono specifici OUs, per impostazione predefinita OUs sono inclusi tutti gli account inclusi in tali obiettivi. Tuttavia, puoi scegliere come target account specifici utilizzando le opzioni di filtro degli account.
- Più unità StackSets possono avere come target la stessa organizzazione o unità organizzativa.
- Non StackSet puoi scegliere come target account esterni all'organizzazione.
- Non StackSet puoi distribuire stack annidati.
- CloudFormation non distribuisce gli stack nell'account di gestione dell'organizzazione, anche se l'account di gestione si trova all'interno dell'organizzazione o in un'unità organizzativa dell'organizzazione.
- La distribuzione automatica è impostata al StackSet livello. Non è possibile modificare le distribuzioni automatiche in modo selettivo per OUs account o regioni.
- Le autorizzazioni dell'entità principale IAM (utente, ruolo o gruppo) che utilizzi per accedere all'account di gestione determinano se sei autorizzato a eseguire la distribuzione con. StackSets Per una policy IAM di esempio che concede le autorizzazioni per la distribuzione a un'organizzazione, consulta [Limita le operazioni relative ai set di stack in base alla regione e ai tipi di risorse](#).
- Gli amministratori delegati dispongono delle autorizzazioni complete per la distribuzione negli account dell'organizzazione. L'account di gestione non può limitare le autorizzazioni degli amministratori delegati per la distribuzione a operazioni specifiche OUs o per eseguire operazioni specifiche. StackSet

Crea un account StackSet con autorizzazioni gestite dal servizio (console)

Per creare un StackSet

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il modulo da Regione AWS cui vuoi gestire. StackSet
3. Dal pannello di navigazione, scegli StackSets.
4. Nella parte superiore della StackSetspagina, scegli Crea StackSet.

5. In Permissions (Autorizzazioni) scegliere Service-managed permissions (Autorizzazioni gestite dal servizio).

 Note

Se l'accesso affidabile con AWS Organizations è disabilitato, viene visualizzato un banner. È necessario un accesso affidabile per creare o aggiornare un file StackSet con autorizzazioni gestite dal servizio. Solo l'amministratore nell'account di gestione dell'organizzazione dispone delle autorizzazioni per [Attiva l'accesso affidabile per StackSets con AWS Organizations](#).

6. In Prerequisito: prepara il modello, scegli Il modello è pronto.
7. In Specify template (Specifica modello), scegliere di specificare l'URL per il bucket S3 che contiene il modello di stack oppure caricare un file modello di stack. Quindi, seleziona Next (Successivo).
8. Nella pagina Specificate StackSet i dettagli, fornite un nome per il StackSet, specificate eventuali parametri e quindi scegliete Avanti.
9. Nella pagina Configura StackSet opzioni, in Tag, specifica i tag da applicare alle risorse dello stack. Per ulteriori informazioni sull'utilizzo dei tag AWS, consulta [Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione dei costi nella Guida](#) per l'AWS Billing and Cost Management utente.
10. Per la configurazione di Execution, scegli Active per abilitare CloudFormation la gestione ottimizzata delle operazioni:
 - Le operazioni non in conflitto vengono eseguite contemporaneamente per tempi di implementazione più rapidi.
 - Le operazioni in conflitto vengono automaticamente messe in coda ed elaborate nell'ordine in cui sono state richieste.

Mentre le operazioni sono in esecuzione o in CloudFormation coda, mette in coda tutte le operazioni in entrata anche se non sono in conflitto. Non è possibile modificare le impostazioni di esecuzione durante questo periodo.

11. Se il modello contiene risorse IAM, per Capacità, scegli Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
12. Scegli Avanti per procedere e attivare l'accesso attendibile, se non è già attivato.

13. Nella pagina Imposta opzioni di distribuzione, in Obiettivi di distribuzione, esegui una delle seguenti operazioni:

- Per eseguire la distribuzione su tutti gli account dell'organizzazione, scegli Distribuisci nell'organizzazione.
- Per eseguire la distribuzione su tutti gli account in modo specifico OUs, scegli Distribuisci su unità organizzative (). OUs Scegliere Add an OU (Aggiungi un'unità organizzativa) e quindi incollare l'ID dell'unità organizzativa di destinazione nella casella di testo. Ripetere per ogni nuova unità organizzativa di destinazione.

Se hai scelto Distribuisci su unità organizzative (OUs), per il tipo di filtro Account, puoi impostare gli obiettivi di distribuzione in modo che siano account individuali specifici scegliendo una delle seguenti opzioni e fornendo i numeri di account.

- Nessuno (impostazione predefinita): distribuisce gli stack su tutti gli account specificati. OUs
 - Intersezione: distribuisce gli stack su singoli account specifici all'interno di quelli selezionati. OUs
 - Differenza: distribuisce gli stack su tutti gli account selezionati OUs ad eccezione di account specifici.
 - Union: distribuisce gli stack negli account individuali specificati OUs più altri.
14. In Distribuzione automatica, scegli se eseguire la distribuzione automatica sugli account aggiunti all'organizzazione di destinazione o OUs in futuro. Per ulteriori informazioni, consulta [Abilita o disabilita le distribuzioni automatiche per in StackSets AWS Organizations](#).
15. Se è stata abilitata la distribuzione automatica, in Account removal behavior (Comportamento rimozione account) scegliere se le risorse dello stack vengono mantenute o eliminate quando un account viene rimosso da un'organizzazione o da un'unità organizzativa di destinazione.

 Note

Selezionando gli stack Retain, gli stack vengono rimossi dagli stack StackSet, ma gli stack e le risorse associate vengono mantenuti. Le risorse rimangono nello stato attuale, ma non faranno più parte di. StackSet

16. In Specificare le regioni, scegli le regioni in cui desideri distribuire gli stack.

17. Per le opzioni di distribuzione, procedi come segue:

- Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.
- Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
- Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
- Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.
 - Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.

18. Seleziona Successivo per continuare.

19. Nella pagina Revisione, verifica di eseguire StackSet la distribuzione negli account corretti nelle regioni corrette, quindi scegli Crea. StackSet

Si apre la pagina dei StackSet dettagli. Puoi visualizzare l'avanzamento e lo stato della creazione degli stack nel tuo StackSet.

Crea un file StackSet con autorizzazioni gestite dal servizio (AWS CLI)

Segui i passaggi descritti in questa sezione per utilizzare: AWS CLI

- Crea il StackSet contenitore.
- Distribuisci istanze stack.

Note

Quando agisci come amministratore delegato, devi includere `--call-as DELEGATED_ADMIN` nel comando.

Deploy to your organization

Per creare un StackSet

1. Usa il [create-stack-set](#) comando per creare un nuovo StackSet nome *my-stackset*. L'esempio seguente utilizza un modello archiviato in un bucket S3, abilita le distribuzioni automatiche e conserva gli stack quando gli account vengono rimossi. Per ulteriori informazioni, consulta [Abilita o disabilita le distribuzioni automatiche per in StackSets AWS Organizations](#).

```
aws cloudformation create-stack-set \  
  --stack-set-name my-stackset \  
  --template-url https://s3.region-code.amazonaws.com/amzn-s3-demo-bucket/MyApp.template \  
  --permission-model SERVICE_MANAGED \  
  --auto-deployment Enabled=true,RetainStacksOnAccountRemoval=true
```

2. Usa il [list-stack-sets](#) comando per confermare che il tuo è stato creato. StackSet Il tuo nuovo StackSet è elencato nei risultati.

```
aws cloudformation list-stack-sets
```

- Se imposti l'--call-asopzione su DELEGATED_ADMIN mentre hai effettuato l'accesso al tuo account membro, list-stack-sets restituisce tutti i dati StackSets con autorizzazioni gestite dal servizio nell'account di gestione dell'organizzazione.
 - Se imposti l'--call-asopzione su SELF mentre hai effettuato l'accesso al tuo Account AWS, list-stack-sets restituisce tutti i resi StackSets autogestiti nel tuo. Account AWS
 - Se imposti l'--call-asopzione su SELF mentre sei connesso all'account di gestione dell'organizzazione, list-stack-sets restituisce tutto StackSets nell'account di gestione dell'organizzazione.
3. Usa il [create-stack-instances](#) comando per aggiungere pile al tuo StackSet. Per l'--deployment-targetsopzione, specifica l'ID root dell'organizzazione da distribuire a tutti gli account dell'organizzazione.

Imposta l'elaborazione simultanea degli account e altre preferenze di distribuzione utilizzando l'--operation-preferencesopzione. Questo esempio utilizza impostazioni basate sul conteggio. Nota che non MaxConcurrentCount deve superare FailureToleranceCount

+ 1. Per le impostazioni basate sulla percentuale, usa `FailureTolerancePercentage` o invece. `MaxConcurrentPercentage`

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets OrganizationalUnitIds=r-a1b2c3d4e5 \  
  --regions us-west-2 us-east-1 \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per ulteriori informazioni, consulta [CreateStackInstances](#) nella documentazione di riferimento dell'API AWS CloudFormation .

4. Utilizzando il comando `operation-id` che è stato restituito come parte dell'`create-stack-instances` output, utilizzate il [describe-stack-set-operation](#) comando seguente per verificare che gli stack siano stati creati correttamente.

```
aws cloudformation describe-stack-set-operation \  
  --stack-set-name my-stackset \  
  --operation-id operation_ID
```

Deploy to organizational units (OUs)

Per creare un StackSet

1. Usa il [create-stack-set](#) comando per creare un nuovo StackSet nome *my-stackset*. L'esempio seguente utilizza un modello memorizzato in un bucket S3 e include un parametro che imposta a *KeyPairName* con il valore *TestKey*

```
aws cloudformation create-stack-set \  
  --stack-set-name my-stackset \  
  --template-url https://s3.region-code.amazonaws.com/amzn-s3-demo-bucket/MyApp.template \  
  --permission-model SERVICE_MANAGED \  
  --parameters ParameterKey=KeyPairName,ParameterValue=TestKey
```

2. Usa il [list-stack-sets](#) comando per confermare che il tuo StackSet è stato creato. Il tuo nuovo StackSet è elencato nei risultati.

```
aws cloudformation list-stack-sets
```

- Se imposti l'`--call-as` opzione su `DELEGATED_ADMIN` mentre hai effettuato l'accesso al tuo account membro, `list-stack-sets` restituisce tutti i dati `StackSets` con autorizzazioni gestite dal servizio nell'account di gestione dell'organizzazione.
 - Se imposti l'`--call-as` opzione su `SELF` mentre hai effettuato l'accesso al tuo Account AWS, `list-stack-sets` restituisce tutti i `StackSets` autogestiti nel tuo Account AWS.
 - Se imposti l'`--call-as` opzione su `SELF` mentre sei connesso all'account di gestione dell'organizzazione, `list-stack-sets` restituisce tutto `StackSets` nell'account di gestione dell'organizzazione.
3. Usa il [create-stack-instances](#) comando per aggiungere pile al tuo `StackSet`. Per l'`--deployment-targets` opzione, specifica l'unità organizzativa su IDs cui eseguire la distribuzione.

Imposta l'elaborazione simultanea degli account e altre preferenze di distribuzione utilizzando l'`--operation-preferences` opzione. Questo esempio utilizza impostazioni basate sul conteggio. Nota che non `MaxConcurrentCount` deve superare `FailureToleranceCount` + 1. Per le impostazioni basate sulla percentuale, usa `FailureTolerancePercentage` o invece. `MaxConcurrentPercentage`

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets OrganizationalUnitIds=ou-rcuk-1x5j1lwo,ou-rcuk-slr5lh0a \  
  --regions us-west-2 us-east-1 \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per ulteriori informazioni, consulta [CreateStackInstances](#) nella documentazione di riferimento dell'API AWS CloudFormation .

4. Utilizzando il comando `operation-id` che è stato restituito come parte dell'`create-stack-instances` output, utilizzate il [describe-stack-set-operation](#) comando seguente per verificare che gli stack siano stati creati correttamente.

```
aws cloudformation describe-stack-set-operation \  
  --stack-set-name my-stackset \  
  --operation-id operation_ID
```

Deploy to specific accounts in OUs

Puoi scegliere come target unità organizzative specifiche (OUs) e utilizzare il filtro degli account per controllare con precisione quali account ricevono le distribuzioni in stack. Per impostazione predefinita, gli stack vengono distribuiti su tutti gli account specificati OUs se non viene specificato alcun filtro degli account.

In AWS CLI, si specifica il filtraggio degli account con l'opzione. `--deployment-targets` Per ulteriori informazioni, consulta [DeploymentTargets](#).

Dopo aver creato il StackSet contenitore con il `create-stack-set` comando, utilizzate uno dei seguenti esempi per distribuire gli stack su account specifici.

Scegli come target account specifici in un'unità organizzativa

L'esempio seguente distribuisce gli stack solo negli account A1 e A2 in OU1

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets  
  OrganizationalUnitIds=OU1,Accounts=A1,A2,AccountFilterType=INTERSECTION \  
  --regions us-west-2 us-east-1
```

Escludere gli account da un'unità organizzativa

L'esempio seguente distribuisce gli stack su tutti gli account OU1 ad eccezione degli account A1 e A2.

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets  
  OrganizationalUnitIds=OU1,Accounts=A1,A2,AccountFilterType=DIFFERENCE \  
  --regions us-west-2 us-east-1
```

Includi account aggiuntivi

L'esempio seguente distribuisce gli stack su tutti gli account OU1 più un account A4 aggiuntivo da un'altra unità organizzativa.

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets OrganizationalUnitIds=OU1,Accounts=A4,AccountFilterType=UNION  
  \  
  --regions us-west-2 us-east-1
```

Abilita o disabilita le distribuzioni automatiche per in StackSets AWS Organizations

CloudFormation puoi distribuire automaticamente stack aggiuntivi a nuovi AWS Organizations account quando vengono aggiunti all'organizzazione o alle unità organizzative di destinazione (). OUs Puoi abilitare le distribuzioni automatiche e scegliere se eliminare o conservare gli stack e le risorse associate quando gli account vengono rimossi da Target. OUs Queste impostazioni possono essere modificate in qualsiasi momento, ad esempio utilizzando le autorizzazioni gestite dal StackSets servizio.

Come funzionano le distribuzioni automatiche

Quando le distribuzioni automatiche sono abilitate, vengono attivate quando gli account vengono aggiunti a un'organizzazione o unità organizzativa di destinazione, rimossi da un'organizzazione o unità organizzativa di destinazione o spostati da una destinazione all'altra. OUs

Ad esempio, si consideri StackSet1 che gli obiettivi si trovano OU1 nella us-east-1 regione e StackSet2 che gli obiettivi si trovano OU2 nella regione. us-east-1 OU1contieneAccountA.

Se si passa AccountA da OU1 a OU2 con le distribuzioni automatiche abilitate, esegue CloudFormation automaticamente un'operazione di eliminazione per rimuovere lo StackSet1 stack AccountA e mette in coda un'operazione di creazione che aggiunge lo stack. StackSet2 AccountA

Considerazioni

Di seguito sono riportate le considerazioni relative all'utilizzo delle distribuzioni automatiche:

- La funzionalità di distribuzione automatica è abilitata a livello. StackSet Non è possibile modificare le distribuzioni automatiche in modo selettivo per OUs account o regioni.
- I valori dei parametri sostituiti si applicano solo agli account attualmente presenti nell'obiettivo e ai relativi figli. OUs OUs Gli account aggiunti alla destinazione OUs e ai relativi figli OUs in futuro utilizzeranno i valori StackSet predefiniti e non i valori sostituiti.
- Se scegli come target account specifici e abiliti le distribuzioni automatiche, StackSet continuerai a utilizzare il filtro a livello di account definito nell'ultima distribuzione, eseguendo anche la distribuzione su nuovi account aggiunti all'interno dell'organizzazione distribuita. Per impedire le distribuzioni ai nuovi account aggiunti, disabilita le distribuzioni automatiche.

Abilita o disabilita le distribuzioni automatiche (console)

Per abilitare o disabilitare le distribuzioni automatiche

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformazione](https://console.aws.amazon.com/cloudformazione).
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
3. Dal riquadro di navigazione, scegli StackSets.
4. Nella StackSetspagina, seleziona l'opzione accanto al nome del file StackSet da aggiornare.
5. Scegli Modifica distribuzione automatica dal menu Azioni nell'angolo in alto a destra.
6. Nella finestra di dialogo che si apre, procedi come segue:
 - a. Per la distribuzione automatica, scegli Attivato o Disattivato.
 - b. Per il comportamento di rimozione dell'account, scegli Elimina pile o Conserva pile. Le risorse conservate rimangono nello stato attuale, ma non faranno più parte di. StackSet
7. Scegli Save (Salva).

Abilita o disabilita le distribuzioni automatiche (AWS CLI)

Per abilitare o disabilitare le distribuzioni automatiche

1. Utilizzare il comando [update-stack-set](#) con l'opzione `--auto-deployment`.

Il comando seguente abilita le distribuzioni automatiche.

```
aws cloudformation update-stack-set --stack-set-name my-stackset \  
  --use-previous-template --auto-deployment  
  Enabled=true,RetainStacksOnAccountRemoval=true
```

In alternativa, per disabilitare le distribuzioni automatiche, specificate `Enabled=false` come valore per l'`--auto-deployment`opzione, come nell'esempio seguente.

```
aws cloudformation update-stack-set --stack-set-name my-stackset \  
  --use-previous-template --auto-deployment Enabled=false
```

- Utilizzando l'ID dell'operazione restituito come parte dell'update-stack-setoutput, esegui [describe-stack-set-operation](#) per verificare che l'aggiornamento sia StackSet stato eseguito correttamente.

```
aws cloudformation describe-stack-set-operation --operation-id operation_ID
```

Aggiornamento AWS CloudFormation StackSets

Puoi aggiornare il tuo StackSet utilizzando la CloudFormation console o il AWS CLI.

Per aggiungere e rimuovere account e regioni da a StackSet, vedi [Aggiungi pile a StackSets](#) e [Elimina pile da StackSets](#). Per sovrascrivere i valori dei parametri per uno stack, vedi. [Sostituisci i parametri sugli stack](#)

Argomenti

- [Aggiorna la tua StackSet \(console\)](#)
- [Aggiorna il tuo StackSet \(AWS CLI\)](#)

Aggiorna la tua StackSet (console)

Per aggiornare un StackSet

- Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
- Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
- Dal pannello di navigazione, scegli StackSets.
- Nella StackSetspagina, seleziona StackSet quello che desideri aggiornare.
- Con l' StackSet opzione selezionata, scegli Modifica StackSet dettagli dal menu Azioni.
- Nella pagina Scegli un modello, aggiorna la sezione Autorizzazioni secondo necessità o vai al passaggio successivo.
- Per Prerequisito: prepara il modello, scegli Usa il modello corrente per utilizzare il modello corrente o Sostituisci il modello corrente per specificare un URL S3 con un altro modello o caricare un nuovo modello.
- Scegli Next (Successivo).

9. Nella pagina Specificare StackSet i dettagli, per la StackSet descrizione, aggiorna la descrizione in base alle esigenze StackSet .
10. Per Parametri, aggiorna i valori dei parametri in base alle esigenze.
11. Scegli Next (Successivo).
12. Nella pagina Configura StackSet opzioni, per Tag, modificate i tag in base alle esigenze. Puoi aggiungere, aggiornare o eliminare i tag. Per ulteriori informazioni sull'utilizzo dei tag AWS, consulta [Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione dei costi AWS](#) nella Guida per l'AWS Billing and Cost Management utente.
13. Per la configurazione di esecuzione, è possibile aggiornare la configurazione di esecuzione in base alle esigenze.

 Note

Ricorda che non puoi modificare le impostazioni di esecuzione quando le operazioni sono in esecuzione o in coda.

14. Se il modello contiene risorse IAM, per Capabilities, scegli Riconosco che questo modello può creare risorse IAM per specificare che desideri utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).
15. Scegli Next (Successivo).
16. Nella pagina Imposta le opzioni di distribuzione, fornisci gli account e le regioni per l'aggiornamento.

CloudFormation distribuirà gli aggiornamenti dello stack negli account specificati all'interno della prima regione, quindi passerà alla successiva e così via, purché gli errori di distribuzione in una regione non superino una tolleranza di errore specificata.

- a. [Autorizzazioni gestite automaticamente] Per Account e sedi di distribuzione, scegli Distribuisci stack negli account. Incolla l'account di destinazione IDs che hai usato per creare il tuo StackSet nella casella di testo, separando più numeri con virgole.

[Autorizzazioni gestite dal servizio] Effettua una delle seguenti operazioni:

- Scegli Distribuisci in unità organizzative (). OUs Inserisci l'obiettivo OUs che hai usato per creare il tuo StackSet.
- Scegliere Deploy to accounts (Distribuisci agli account). Incolla l'unità organizzativa IDs o l'account di destinazione IDs che hai usato per creare il tuo StackSet.

- b. Per Specificare le regioni, specifica l'ordine in cui CloudFormation desideri distribuire gli aggiornamenti.
 - c. Per le opzioni di distribuzione, procedi come segue:
 - Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.
 - Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
 - Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
 - Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.
 - Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.
 - d. Seleziona Successivo per continuare.
17. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.
18. Quando sei pronto per procedere, scegli Invia.

CloudFormation inizia ad applicare gli aggiornamenti al tuo StackSet e visualizza la scheda Operazioni della pagina dei StackSet dettagli. È possibile visualizzare l'avanzamento e lo stato delle operazioni di aggiornamento nella scheda Operations (Operazioni).

Aggiorna il tuo StackSet (AWS CLI)

Note

Quando agisci come amministratore delegato, devi includere `--call-as DELEGATED_ADMIN` nel comando.

1. Per aggiornare un StackSet

Usa il [update-stack-set](#) comando per apportare modifiche al tuo StackSet.

Nei seguenti esempi, stiamo StackSet aggiornando l'`--parameters` opzione utilizzando. In particolare, modifichiamo la frequenza di consegna delle istantanee predefinita per la configurazione del canale di consegna da `TwentyFour_Hours` a `Twelve_Hours`. Poiché stiamo ancora utilizzando il modello corrente, aggiungiamo l'`--use-previous-template` opzione.

Imposta l'elaborazione simultanea degli account e altre preferenze di distribuzione utilizzando l'`--operation-preferences` opzione. Questi esempi utilizzano impostazioni basate sul conteggio. Nota che non `MaxConcurrentCount` deve superare `FailureToleranceCount + 1`. Per le impostazioni basate sulla percentuale, usa `FailureTolerancePercentage` o invece `MaxConcurrentPercentage`.

[Autorizzazioni gestite automaticamente] Per l'`--accounts` opzione, fornisci l'account a IDs cui desideri indirizzare l'aggiornamento.

```
aws cloudformation update-stack-set --stack-set-name my-stackset \  
  --use-previous-template \  
  --parameters ParameterKey=MaximumExecutionFrequency,ParameterValue=Twelve_Hours \  
  --accounts account_ID_1 account_ID_2 \  
  --regions us-west-2 us-east-1 \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

[Autorizzazioni gestite dal servizio] Per `--deployment-targets` questa opzione, fornisci l'ID radice dell'organizzazione o l'unità organizzativa (OU) a IDs cui desideri indirizzare l'aggiornamento.

```
aws cloudformation update-stack-set --stack-set-name my-stackset \  
  --use-previous-template \  
  --parameters ParameterKey=MaximumExecutionFrequency,ParameterValue=Twelve_Hours \  
  --deployment-targets OrganizationalUnitIds=ou-rcuk-1x5j1lwo,ou-rcuk-slr5lh0a \  
  --regions us-west-2 us-east-1 \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per ulteriori informazioni, consulta [UpdateStackSet](#) nella documentazione di riferimento dell'API AWS CloudFormation .

2. Verifica che l'aggiornamento sia StackSet stato eseguito correttamente eseguendo il `describe-stack-set-operation` comando per mostrare lo stato e i risultati dell'operazione di aggiornamento. Per `--operation-id`, utilizzare l'ID dell'operazione restituito dal comando `update-stack-set`.

```
aws cloudformation describe-stack-set-operation \  
  --operation-id operation_ID
```

Aggiungi pile a CloudFormation StackSets

Quando crei un StackSet, puoi creare gli stack necessari a tale scopo. StackSet CloudFormation consente inoltre di aggiungere altri stack, per account e regioni aggiuntivi, in qualsiasi momento dopo la StackSet creazione di. Puoi aggiungere pile utilizzando la CloudFormation console o il. AWS CLI

Argomenti

- [Aggiungi pile a StackSet \(console\)](#)
- [Aggiungi pile a \(\) StackSet AWS CLI](#)

Aggiungi pile a StackSet (console)

Per aggiungere pile a StackSet

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
3. Dal pannello di navigazione, scegli StackSets. Nella StackSets pagina, seleziona quello StackSet che hai creato.
4. Con l' StackSet opzione selezionata, scegli Aggiungi pile a StackSet dal menu Azioni.
5. Nella pagina Imposta opzioni di distribuzione, procedi come segue:
 - a. Per Aggiungi stack a StackSet, scegli Distribuisci nuovi stack.
 - b. Quindi, procedi come segue in base alla tua configurazione delle autorizzazioni StackSet:
 - [Autorizzazioni autogestite] Per Account, sedi di distribuzione, scegli Distribuisci pile negli account. Incollare i numeri di account target nella casella di testo, separando più numeri con virgole.

- [Autorizzazioni gestite dal servizio] Per gli obiettivi di distribuzione, esegui una delle seguenti operazioni:
 - Scegliere Deploy to organization (Distribuisci all'organizzazione per eseguire la distribuzione a tutti gli account dell'organizzazione).
 - Scegli Distribuisci alle unità organizzative (OUs) per eseguire la distribuzione su tutti gli account in modo specifico. OUs Scegliere Add another OU (Aggiungi altra unità organizzativa) e quindi incollare l'ID dell'unità organizzativa di destinazione nella casella di testo. Ripetere l'operazione per ogni nuova unità organizzativa di destinazione. CloudFormation si rivolge anche a qualsiasi figlio OUs dei bersagli selezionati.

 Note

Se aggiungi un'unità organizzativa StackSet già scelta come destinazione, CloudFormation crea nuovi stack in tutti gli account dell'unità organizzativa che non dispongono già degli stack dell'unità organizzativa StackSet (ad esempio, account che sono stati aggiunti all'unità organizzativa dopo la creazione e con le StackSet distribuzioni automatiche disattivate).

- c. Per Specificare le regioni, specifica Regioni AWS a quali eseguire la distribuzione negli account di destinazione specificati nel passaggio precedente. Per impostazione predefinita, CloudFormation distribuirà gli stack negli account specificati all'interno della prima regione, quindi passerà alla successiva e così via, a condizione che gli errori di distribuzione di una regione non superino una tolleranza di errore specificata.
- d. Per le opzioni di distribuzione, procedi come segue:
 - Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.
 - Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
 - Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
 - Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.

- Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.
- e. Scegli Next (Successivo).
6. Nella pagina Specify overrides (Specifica sostituzioni), lasciare i valori delle proprietà specificati. Non verrà sostituito alcune valore delle proprietà per gli stack che verranno creati. Scegli Next (Successivo).
 7. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.
 8. Quando sei pronto per procedere, scegli Invia.

CloudFormation inizia a creare i tuoi stack. Visualizza l'avanzamento e lo stato della creazione degli stack StackSet nella pagina dei StackSet dettagli che si apre quando scegli Invia. Al termine, i nuovi stack dovrebbero essere elencati nella scheda Istanze dello stack.

Aggiungi pile a () StackSet AWS CLI

Note

Quando agisci come amministratore delegato, devi includerlo `--call-as DELEGATED_ADMIN` nel comando.

Per aggiungere pile a un file StackSet con autorizzazioni gestite automaticamente

Utilizza il comando della CLI `create-stack-instances`. Per l' `--account` opzione, fornisci gli account IDs per i quali desideri creare pile.

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
--accounts account_id --regions eu-west-1 us-west-2
```

Per aggiungere stack a uno StackSet con autorizzazioni gestite dal servizio

Utilizza il comando della CLI `create-stack-instances`. Come `--deployment-targets` opzione, fornisci l'ID dell'organizzazione (root) o l'unità organizzativa IDs per cui desideri creare gli stack. Ad esempio, i comandi destinati ad account specifici, vedi [Crea un file StackSet con autorizzazioni gestite dal servizio \(\)AWS CLI](#).

```
aws cloudformation create-stack-instances --stack-set-name my-stackset \  
  --deployment-targets OrganizationalUnitIds=ou-rcuk-r1qi0wl7 --regions eu-west-1 us-  
west-2
```

Note

Se aggiungi un'unità organizzativa StackSet già scelta come destinazione, CloudFormation crea nuovi stack in tutti gli account dell'unità organizzativa che non dispongono già degli stack dell'unità organizzativa StackSet (ad esempio, account che sono stati aggiunti all'unità organizzativa dopo la creazione e con le StackSet distribuzioni automatiche disattivate).

Sostituisci i valori dei parametri sugli stack all'interno del tuo CloudFormation StackSet

In alcuni casi, potresti volere che gli stack in determinate regioni o account abbiano valori di proprietà diversi da quelli specificati nelle stesse aree. StackSet Ad esempio, potresti specificare un valore diverso per un determinato parametro in base al fatto che un account venga utilizzato per lo sviluppo o la produzione. In queste situazioni, CloudFormation consente di sovrascrivere i valori dei parametri negli stack per account e regione. È possibile sovrascrivere i valori dei parametri del modello quando si creano gli stack per la prima volta e i valori dei parametri per gli stack esistenti. È possibile riportare i parametri precedentemente sovrascritti negli stack solo ai valori specificati in. StackSet

Le sostituzioni dei valori dei parametri si applicano agli stack negli account e nelle regioni selezionati. Durante StackSet gli aggiornamenti, tutti i valori dei parametri sostituiti per uno stack non vengono aggiornati, ma mantengono il valore sovrascritto.

È possibile sovrascrivere solo i valori dei parametri specificati in StackSet; per aggiungere o eliminare un parametro stesso, è necessario aggiornare il modello. StackSet Se aggiungete un parametro a un StackSet modello, prima di poter sovrascrivere il valore di quel parametro in uno stack, dovete prima aggiornare tutti gli stack con il nuovo parametro e il nuovo valore specificati in. StackSet Una volta che tutti gli stack sono stati aggiornati con il nuovo parametro, potete sovrascrivere il valore del parametro nei singoli stack, se lo desiderate.

Per informazioni su come sovrascrivere i valori StackSet dei parametri durante la creazione di pile, consulta. [Aggiungi pile a StackSets](#)

Argomenti

- [Sostituisci i parametri negli stack \(console\)](#)
- [Sostituisci i parametri sugli stack \(\)AWS CLI](#)

Sostituisci i parametri negli stack (console)

Per sovrascrivere i parametri per pile specifiche

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformazione.](https://console.aws.amazon.com/cloudformazione)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
3. Dal pannello di navigazione, scegli StackSets. Nella StackSets pagina, seleziona il tuo StackSet.
4. Una volta StackSet selezionati, scegliete Ignora StackSet parametri dal menu Azioni.
5. Nella pagina Imposta le opzioni di distribuzione, fornisci gli account e le regioni per gli stack per i quali creerai le sostituzioni.

Per impostazione predefinita, CloudFormation distribuirà gli stack negli account specificati all'interno della prima regione, quindi passerà alla successiva e così via, a condizione che gli errori di distribuzione in una regione non superino una tolleranza di errore specificata.

- a. [Autorizzazioni gestite automaticamente] Per le sedi di distribuzione, scegli Distribuisci stack negli account. Incolla alcuni o tutti gli account di destinazione IDs che hai usato per creare il tuo. StackSet

[Autorizzazioni gestite dal servizio] Effettua una delle seguenti operazioni:

- Scegli Distribuisci in unità organizzative (). OUs Inserisci uno o più obiettivi OUs che hai usato per creare il tuo StackSet. I valori dei parametri sostituiti si applicano solo agli account attualmente presenti nell'obiettivo OUs e ai relativi figli. OUs Gli account aggiunti alla destinazione OUs e ai relativi figli OUs in futuro utilizzeranno i valori StackSet predefiniti e non i valori sostituiti.
 - Scegliere Deploy to accounts (Distribuisci agli account). Incolla alcune o tutte le unità organizzative IDs o l'account di destinazione IDs che hai usato per creare il tuo. StackSet
- b. Per Specificare le regioni, aggiungi una o più delle regioni in cui hai distribuito gli stack a tale scopo. StackSet

Se si aggiungono più Regioni, l'ordine delle Regioni in Specify regions (Specifica Regioni) determina l'ordine di distribuzione.

c. Per le opzioni di distribuzione, procedi come segue:

- Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.
- Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
- Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
- Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.
 - Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.

d. Scegli Next (Successivo).

6. Nella pagina Specificare le sostituzioni, selezionate le caselle di controllo relative ai parametri da sostituire, quindi scegliete Sostituisci valore dal menu Modifica valore di sostituzione StackSet.
7. Nella pagina Sostituisci i valori StackSet dei parametri, apporta le modifiche, quindi scegli Salva modifiche.

Note

Per reimpostare i parametri sostituiti all'utilizzo del valore specificato in StackSet, seleziona tutti i parametri e scegli Imposta su StackSet valore dal menu Modifica valore sostitutivo. In questo modo vengono rimossi tutti i valori sovrascritti una volta aggiornati gli stack.

8. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.
9. Quando sei pronto per procedere, scegli Invia.

CloudFormation inizia ad aggiornare i tuoi stack. Visualizza l'avanzamento e lo stato degli stack nella pagina dei StackSet dettagli che si apre quando scegli Invia.

Sostituisci i parametri sugli stack ()AWS CLI

Note

Quando agisci come amministratore delegato, devi includerlo `--call-as DELEGATED_ADMIN` nel comando.

Per sovrascrivere i parametri per pile specifiche

1. Utilizzate il [update-stack-instances](#) AWS CLI comando e specificate l'`--parameter-overrides` opzione.

[Autorizzazioni gestite automaticamente] Per l'`--accounts` opzione, fornite l'account IDs per il quale desiderate sovrascrivere i valori dei parametri sugli stack.

```
aws cloudformation update-stack-instances --stack-set-name my-stackset \  
  --parameter-overrides ParameterKey=Subnets,ParameterValue=subnet-1baa3351\  
  \,subnet-27b86940 \  
  --accounts account_id --regions us-east-1
```

[Autorizzazioni gestite dal servizio] Per l'`--deployment-targets` opzione, fornisci l'ID radice, l'unità organizzativa o l' AWS Organizations account dell'organizzazione IDs per cui desideri IDs sovrascrivere i parametri sugli stack. In questo esempio, sostituiamo i valori dei parametri per gli stack in tutti gli account dell'unità organizzativa con l'ID. *ou-rcuk-1x5j1lwo*

I valori dei parametri sostituiti si applicano solo agli account che si trovano attualmente nell'unità organizzativa di destinazione e nella relativa unità figlio. OUs Gli account aggiunti all'unità organizzativa di destinazione e alla relativa unità secondaria OUs in futuro utilizzeranno i valori StackSet predefiniti e non i valori sostituiti.

```
aws cloudformation update-stack-instances --stack-set-name my-stackset \  
  --parameter-overrides ParameterKey=Subnets,ParameterValue=subnet-1baa3351\  
  \,subnet-27b86940 \  
  --deployment-targets OrganizationalUnitIds=ou-rcuk-1x5j1lwo \  
  --accounts account_id --regions us-east-1
```

```
--regions us-east-1
```

2. Verifica che i valori dei parametri siano stati sovrascritti correttamente negli stack eseguendo il `describe-stack-set-operation` comando per mostrare lo stato e i risultati dell'operazione di aggiornamento. Per `--operation-id`, utilizzare l'ID dell'operazione restituito dal comando `update-stack-instances`.

```
aws cloudformation describe-stack-set-operation --operation-id operation_ID
```

Elimina pile da AWS CloudFormation StackSets

Puoi eliminare gli stack StackSets utilizzando la CloudFormation console o il AWS CLI

Argomenti

- [Elimina gli stack dalla tua \(console\) StackSet](#)
- [Elimina gli stack dal tuo \(\) StackSet AWS CLI](#)

Note

L'eliminazione degli stack da un'unità organizzativa (OU) di primo livello rimuove tale unità organizzativa come destinazione. StackSet

Elimina gli stack dalla tua (console) StackSet

Per eliminare gli stack

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
3. Dal pannello di navigazione, scegli StackSets. Nella StackSets pagina, seleziona StackSet.
4. Una volta StackSet selezionato, scegli Elimina pile StackSet dal menu Azioni.
5. Nella pagina Imposta le opzioni di distribuzione, scegli innanzitutto gli account e le regioni in cui desideri eliminare gli stack.

- a. [Autorizzazioni gestite automaticamente] Per gli account, scegli Distribuisci gli stack negli account o Distribuisci gli stack nelle unità organizzative.

Se scegli Distribuisci gli stack negli account, incolla i numeri di account di destinazione nella casella di testo Numeri di account, separando più numeri con virgole.

Se scegli Distribuisci gli stack nelle unità organizzative, incolla un ID OU di destinazione nella casella di testo Numeri dell'organizzazione per scegliere come target tutti gli account che fanno parte dell'organizzazione specificata.

- b. [Autorizzazioni gestite dal servizio] Per le unità organizzative (OUs), specificare l'unità organizzativa di destinazione. IDs

 Important

CloudFormation eliminerà gli stack sia dalla destinazione OUs specificata che dal relativo elemento secondario. OUs

Per il tipo di filtro Account, puoi definire a quali account verranno eliminati gli stack scegliendo una delle seguenti opzioni e fornendo i numeri di account.

- Nessuno (impostazione predefinita): elimina gli stack da tutti gli account nel periodo specificato. OUs
- Intersezione: elimina le pile solo da singoli account specifici all'interno di quello selezionato. OUs
- Differenza: elimina le pile da tutti gli account selezionati OUs ad eccezione di account specifici.
- Union: elimina gli stack dagli account individuali specificati OUs più altri.

- c. Per Specificare le regioni, scegli le regioni da cui desideri eliminare gli stack all'interno degli account di destinazione.
6. Per le opzioni di distribuzione, procedi come segue:
 - Per Numero massimo di account simultanei, specifica quanti account vengono elaborati contemporaneamente.

- Per Tolleranza agli errori, specifica il numero massimo di errori di account consentiti per regione. L'operazione si interromperà e non passerà ad altre regioni una volta raggiunto questo limite.
 - Per gli stack Retain, attiva questa opzione per salvare gli stack e le risorse associate quando li rimuovi dal tuo StackSet. Le risorse rimangono nello stato attuale ma non fanno più parte di StackSet.
 - Per la concorrenza regionale, scegli come elaborare le regioni: sequenziali (una regione alla volta) o parallele (più regioni contemporaneamente).
 - Per la modalità Concurrency, scegliete come si comporta la concorrenza durante l'esecuzione dell'operazione.
 - Rigorosa tolleranza agli errori: riduce il livello di concorrenza dell'account in caso di errori, rimanendo entro la tolleranza di errore +1.
 - Tolleranza morbida agli errori: mantiene il livello di concorrenza specificato (il valore di Maximum Concurrent Account) indipendentemente dagli errori.
7. Scegli Next (Successivo).
 8. Nella pagina Review (Esamina), esaminare le proprie opzioni. Per apportare modifiche, scegli Modifica nella sezione correlata.
 9. Quando sei pronto a rimuovere gli stack dal tuo StackSet, scegli Invia.

Al termine dell'eliminazione dello stack, puoi verificare che gli stack siano stati eliminati dalla tua pagina di StackSet dettaglio, StackSet nella scheda Istanze dello stack.

Elimina gli stack dal tuo () StackSet AWS CLI

Note

Quando agisci come amministratore delegato, devi includere `--call-as DELEGATED_ADMIN` nel comando.

Usa il `delete-stack-instances` comando con il tuo StackSet nome.

In questi esempi, utilizziamo l'`--no-retain-stacks` opzione perché non conserviamo alcuna pila. Usa `--retain-stacks` invece di `--no-retain-stacks` se vuoi conservare gli stack e le relative risorse.

Per `--regions`, specifica da Regioni AWS cosa vuoi eliminare gli stack, ad esempio, `us-west-2` e `us-east-1`

Imposta l'elaborazione simultanea dell'account e altre preferenze utilizzando l'`--operation-preferences` opzione. Questi esempi utilizzano impostazioni basate sul conteggio. Nota che non `MaxConcurrentCount` deve superare `FailureToleranceCount + 1`. Per le impostazioni basate sulla percentuale, usa `FailureTolerancePercentage` o invece. `MaxConcurrentPercentage`

Per eliminare gli stack (autorizzazioni autogestite)

Per l'`--accounts` opzione, specifica l'account da IDs cui eliminare gli stack.

```
aws cloudformation delete-stack-instances --stack-set-name my-stackset \  
  --accounts account_ID_1 account_ID_2 \  
  --regions us-west-2 us-east-1 \  
  --no-retain-stacks \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per eliminare gli stack (autorizzazioni gestite dal servizio)

Per `--deployment-targets`, specifica l'ID radice dell'organizzazione o l'unità organizzativa (OU) da cui eliminare IDs gli stack.

Important

CloudFormation eliminerà gli stack sia dalla destinazione specificata che dal relativo elemento OUs secondario. OUs

```
aws cloudformation delete-stack-instances --stack-set-name my-stackset \  
  --deployment-targets OrganizationalUnitIds=ou-rcuk-1x5jlwo,ou-rcuk-slr5lh0a \  
  --regions us-west-2 us-east-1 \  
  --no-retain-stacks \  
  --operation-preferences MaxConcurrentCount=1,FailureToleranceCount=0
```

Per ulteriori informazioni, consulta [DeleteStackInstances](#) nella documentazione di riferimento dell'API AWS CloudFormation .

Facoltativamente, al termine dell'eliminazione degli stack, verifica che gli stack siano stati eliminati dal tuo StackSet eseguendo il `describe-stack-set-operation` comando per mostrare lo stato e i risultati

dell'operazione di eliminazione degli stack. Per `--operation-id`, utilizzare l'ID dell'operazione restituito dal comando `delete-stack-instances`.

```
aws cloudformation describe-stack-set-operation --stack-set-name my-stackset \  
--operation-id ddf16f54-ad62-4d9b-b0ab-3ed8e9example
```

Eliminare AWS CloudFormation StackSets

Per eliminare un StackSet, devi prima eliminare tutti gli stack in. StackSet Per informazioni su come eliminare tutte le pile, vedere. [Elimina pile da StackSets](#)

Argomenti

- [Eliminare una StackSet \(console\)](#)
- [Eliminare un StackSet \(\)AWS CLI](#)
- [Eliminare ruoli dei servizi \(opzionale\)](#)

Eliminare una StackSet (console)

Per eliminare un StackSet

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il file in cui Regione AWS hai creato. StackSet
3. Nella StackSetspagina, seleziona il StackSet.
4. Una volta StackSet selezionato, scegliete Elimina StackSet dal menu Azioni.
5. Quando ti viene richiesto di confermare che desideri eliminare il StackSet, scegli Elimina StackSet.

Eliminare un StackSet ()AWS CLI

Note

Quando agisci come amministratore delegato, devi includerlo `--call-as DELEGATED_ADMIN` nel comando.

Per eliminare un StackSet

1. Utilizza il seguente comando `delete-stack-set`. Quando viene richiesto di confermare, digitare **y**, quindi premere Enter (Invio).

```
aws cloudformation delete-stack-set --stack-set-name my-stackset
```

2. Verificare che sia StackSet stato eliminato eseguendo il `list-stack-sets` comando. I risultati del `list-stack-sets` comando dovrebbero mostrare lo stack con uno stato pari DELETED a.

```
aws cloudformation list-stack-sets
```

Eliminare ruoli dei servizi (opzionale)

Se non hai più bisogno dei ruoli di servizio IAM CloudFormation necessari per eseguire StackSet le operazioni, ti consigliamo di eliminare i ruoli.

Per la gestione automatica StackSets, i ruoli che hai creato. Per ulteriori informazioni su questi ruoli, consulta [Concedere autorizzazioni gestite dal cliente](#).

Per i ruoli gestiti dal servizio StackSets, i ruoli per cui sono stati creati automaticamente StackSets hanno il suffisso `CloudFormationStackSetsOrgAdmin` nell'account di gestione dell'organizzazione e `CloudFormationStackSetsOrgMember` in ogni account di destinazione. Per ulteriori informazioni, consulta [Ruoli collegati ai servizi](#).

Per eliminare un ruolo di servizio (console)

1. Accedi AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Dal pannello di navigazione, scegli Ruoli, quindi compila la casella di controllo accanto al ruolo che desideri eliminare.
3. Nel menu Role actions (Operazioni per ruolo) nella parte superiore della pagina, selezionare Delete role (Elimina ruolo).
4. Nella finestra di dialogo di conferma, scegliere Yes, Delete (Sì, elimina). Se sei sicuro, puoi procedere con l'eliminazione anche se l'ultimo accesso ai dati del servizio è ancora in fase di caricamento.

Per eliminare un ruolo di servizio (AWS CLI)

- Utilizza il seguente comando `delete-role`. Quando viene richiesto di confermare, digita **y**, digita e premi **Enter**.

```
aws iam delete-role --role-name role name
```

Per ulteriori informazioni sull'eliminazione dei ruoli, consulta [Eliminare ruoli o profili di istanza nella Guida](#) per l'utente IAM.

Impedisci le StackSets implementazioni fallite utilizzando le porte dell'account di destinazione

Un account gate è una funzionalità opzionale che consente di verificare che un account di destinazione soddisfi determinati requisiti prima di CloudFormation iniziare StackSets le operazioni su quell'account. Questa verifica viene eseguita tramite una AWS Lambda funzione che funge da controllo preliminare.

Un esempio comune di account gate è la verifica che non vi siano CloudWatch allarmi attivi o irrisolti sull'account di destinazione. CloudFormation richiama la funzione Lambda ogni volta che si avviano operazioni di stack nell'account di destinazione e continua solo se la funzione restituisce un codice. **SUCCEEDED** Se la funzione Lambda restituisce uno stato di **FAILED**, CloudFormation non continua con l'operazione richiesta. Se non hai configurato una funzione Lambda con controllo dell'account CloudFormation, salta il controllo e continua con l'operazione.

Se l'attività di controllo del tuo account non ha esito positivo, l'operazione non riuscita viene inclusa nel numero o nella percentuale di stack di tolleranza di errore che hai specificato. Per ulteriori informazioni sulla tolleranza di errore, consulta [StackSet opzioni operative](#).

L'account gating è disponibile solo per le operazioni. StackSets Questa funzionalità non è disponibile per altre CloudFormation operazioni al di fuori di StackSets.

Requisiti

Per il controllo degli account devono essere soddisfatti i seguenti requisiti:

- La funzione Lambda deve avere un nome `AWSCloudFormationStackSetAccountGate` per utilizzare questa funzionalità.

- È `AWSCloudFormationStackSetExecutionRole` necessario disporre delle autorizzazioni per richiamare la funzione Lambda. Senza queste autorizzazioni, CloudFormation salterà il controllo del gating dell'account e procederà con le operazioni sullo stack.
- Affinché l'attività di controllo dell'account funzioni, è necessario aggiungere l'autorizzazione `Lambda InvokeFunction` agli account target. La policy di attendibilità dell'account target deve trovarsi in una relazione di attendibilità con l'account dell'amministratore. Di seguito è riportato un esempio di istruzione di policy che concede autorizzazioni `InvokeFunction` Lambda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": "*"
    }
  ]
}
```

CloudFormation modelli per la creazione di funzioni Lambda

Usa i seguenti modelli di esempio per creare funzioni

`LambdaAWSCloudFormationStackSetAccountGate`. Per creare un nuovo stack utilizzando uno di questi modelli, vedi. [Crea uno stack dalla console CloudFormation](#)

Posizione del modello	Descrizione
https://s3.amazonaws.com/cloudformation-sta-ckset-sample-templates-us-east-1/AccountGateSucceeded.yml	Crea uno stack che implementa una funzione di controllo dell'account Lambda che restituisce lo stato <code>SUCCEEDED</code> .
https://s3.amazonaws.com/cloudformation-sta-ckset-sample-templates-us-east-1/AccountGateFailed.yml	Crea uno stack che implementa una funzione di controllo dell'account Lambda che restituisce lo stato <code>FAILED</code> .

Scegli la modalità Concurrency per AWS CloudFormation StackSets

La modalità di concorrenza è un parametro [StackSetOperationPreferences](#) che consente di scegliere il comportamento del livello di concorrenza durante le operazioni. StackSet Puoi scegliere tra le seguenti modalità:

- **Tolleranza rigorosa ai guasti:** questa opzione riduce dinamicamente il livello di simultaneità per garantire che il numero di account non riusciti non superi mai il valore della tolleranza ai guasti +1. La simultaneità effettiva iniziale viene impostata sul valore più basso tra quello degli account simultanei massimi e quello della tolleranza ai guasti +1. La simultaneità effettiva viene quindi ridotta proporzionalmente in base al numero di errori. Questo è il comportamento che segue di default.
- **Tolleranza flessibile ai guasti:** questa opzione disaccoppia la tolleranza ai guasti dalla simultaneità effettiva. Ciò consente l'esecuzione StackSet delle operazioni al livello di concorrenza impostato dal valore Maximum concurrent accounts, indipendentemente dal numero di errori.

La tolleranza rigorosa ai guasti riduce la velocità di implementazione in caso di errori StackSet operativi, poiché la concorrenza diminuisce per ogni errore. Soft Failure Tolerance dà priorità alla velocità di implementazione sfruttando al contempo le funzionalità di sicurezza. CloudFormation Ciò consente di esaminare e risolvere gli errori StackSet operativi per problemi comuni, come quelli relativi alle risorse esistenti, alle quote di servizio e alle autorizzazioni.

Per ulteriori informazioni sugli errori delle operazioni di StackSets stack, vedere. [Motivi comuni per operazioni di stack non riuscite](#)

Per ulteriori informazioni sul numero massimo di account simultanei e sulla tolleranza ai guasti, consulta la sezione [StackSet opzioni operative](#).

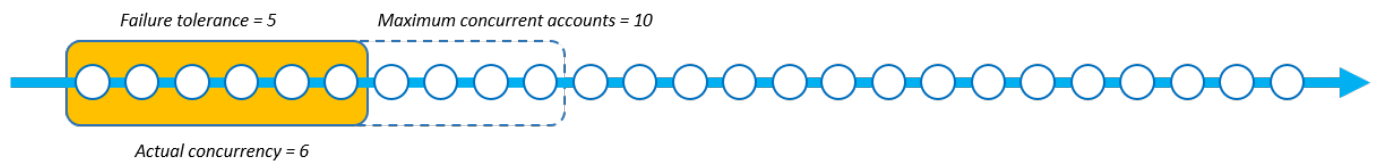
Come funziona ogni modalità di simultaneità

Le immagini seguenti forniscono una rappresentazione visiva del funzionamento di ciascuna modalità Concurrency durante un'operazione. StackSet La stringa di nodi rappresenta una distribuzione su single Regione AWS e ogni nodo è un target Account AWS.

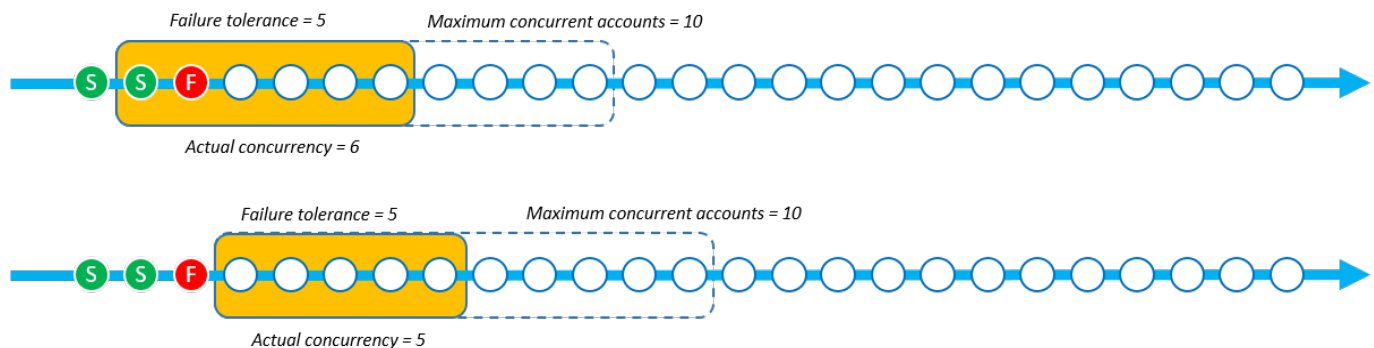
Tolleranza rigorosa ai guasti

Quando un' StackSet operazione che utilizza Strict Failure Tolerance ha il valore di tolleranza di errore impostato su 5 e il valore Maximum concurrent accounts è impostato su 10, la concorrenza effettiva è 6. La simultaneità effettiva è 6 perché il valore di tolleranza ai guasti di $5 + 1$ è inferiore al valore del numero massimo di account simultanei.

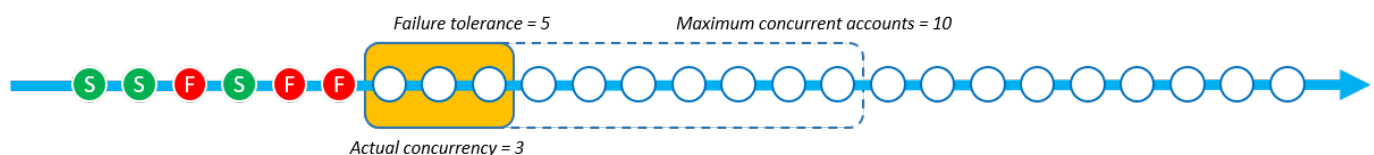
L'immagine seguente mostra l'impatto che il valore di tolleranza di errore ha sul valore Maximum concurrent accounts e l'impatto che entrambi hanno sull'effettiva concomitanza dell'operazione: StackSet



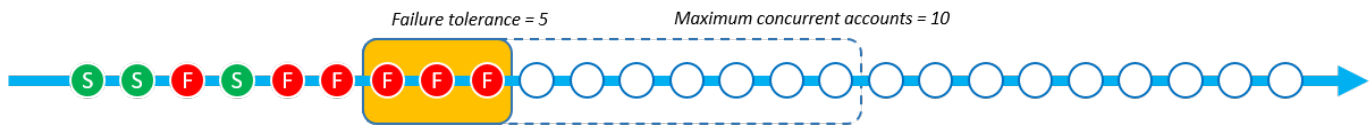
Quando inizia l'implementazione e si verificano istanze di stack non riuscite, la simultaneità effettiva si riduce per offrire un'esperienza di implementazione sicura. La concorrenza effettiva si riduce da 6 a 5 quando StackSets non riesce a distribuire 1 istanza dello stack.



La modalità di tolleranza rigorosa ai guasti riduce la simultaneità effettiva proporzionalmente al numero di istanze di stack non riuscite. Nell'esempio seguente, la concorrenza effettiva si riduce da 5 a 3 quando StackSets non riesce a implementare altre 2 istanze dello stack, portando il totale delle istanze dello stack non riuscite a 3.



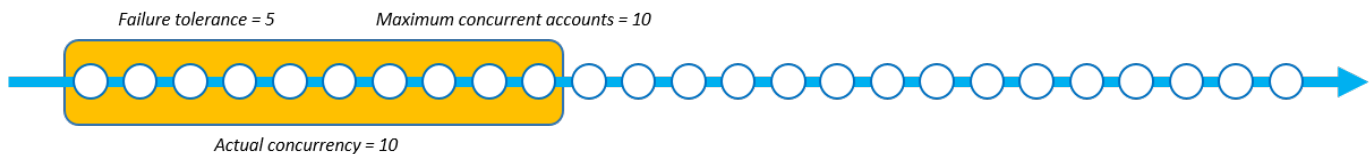
StackSets fallisce l' StackSet operazione quando il numero di istanze dello stack fallite è uguale al valore definito di Failure tolerance +1. Nell'esempio seguente, l'operazione StackSets fallisce quando ci sono 6 istanze di stack fallite e il valore di tolleranza di errore è 5.



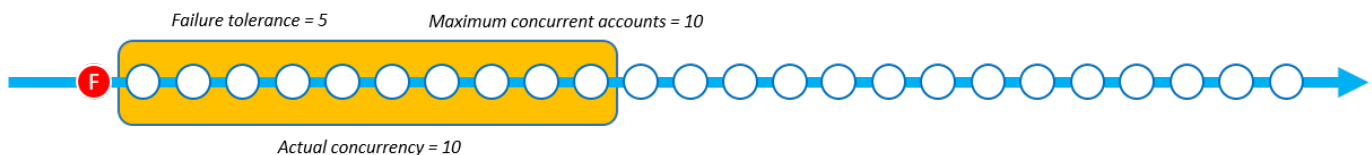
In questo esempio, sono CloudFormation state distribuite 9 istanze dello stack (3 riuscite e 6 non riuscite) prima di interrompere l'operazione. StackSet

Tolleranza flessibile ai guasti

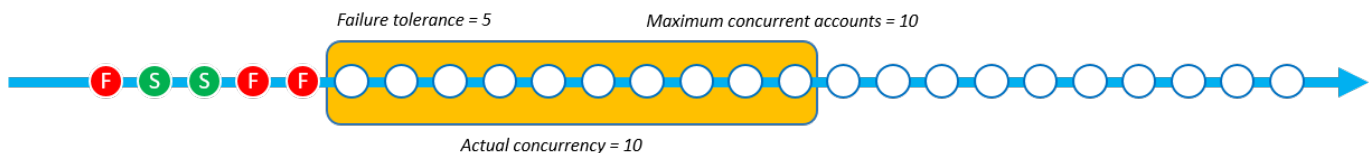
Quando per un' StackSet operazione che utilizza Soft Failure Tolerance il valore di tolleranza di errore è impostato su 5 e il valore Maximum concurrent accounts è impostato su 10, la concorrenza effettiva è 10.



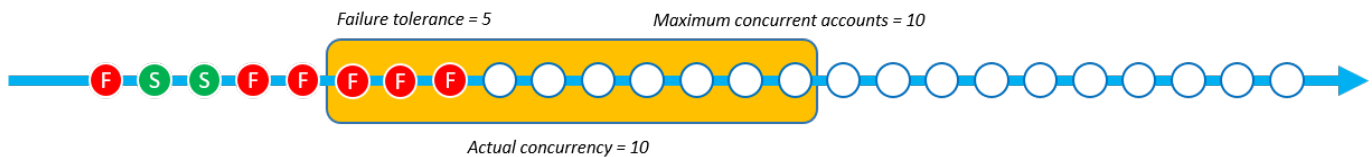
Quando inizia l'implementazione e si verificano istanze di stack non riuscite, la simultaneità effettiva non cambia. Nell'esempio seguente, 1 operazione di stack non è riuscita, ma la simultaneità effettiva rimane a 10.



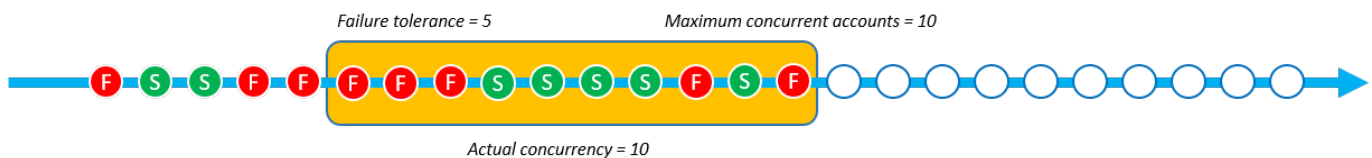
La simultaneità effettiva rimane pari a 10 anche dopo altri 2 errori dell'istanza di stack.



StackSets fallisce l' StackSet operazione quando le istanze dello stack fallite superano il valore di tolleranza di errore. Nell'esempio seguente, l'operazione StackSets fallisce quando ci sono 6 istanze di stack fallite e il numero di tolleranza di errore è 5. Tuttavia, l'operazione non terminerà fino alla fine delle operazioni rimanenti nella coda di simultaneità.



StackSets continua a distribuire istanze stack già presenti nella coda di concorrenza. Ciò significa che il numero delle istanze di stack non riuscite può essere superiore alla tolleranza ai guasti. Nell'esempio seguente, ci sono 8 istanze dello stack fallite perché la coda di concorrenza aveva ancora 7 operazioni da eseguire, anche se l'operazione aveva raggiunto la StackSet tolleranza di errore di 5.



In questo esempio, sono StackSets state distribuite 15 istanze dello stack (7 riuscite e 8 fallite) prima di interrompere l'operazione dello stack.

Scelta tra Tolleranza rigorosa ai guasti e Tolleranza flessibile ai guasti in base alla velocità di implementazione

La scelta tra le modalità Strict failure tolerance e Soft failure tolerance dipende dalla velocità preferita di StackSet implementazione e dal numero consentito di errori di implementazione.

Le tabelle seguenti mostrano come ciascuna modalità di concorrenza gestisce un' StackSet operazione che non riesce durante il tentativo di distribuire un totale di 1000 istanze di stack. In ogni scenario, il valore di tolleranza ai guasti è impostato su 100 istanze di stack e il valore numero massimo di account simultanei è impostato su 250 istanze di stack.

Sebbene StackSets in realtà gli account vengano messi in coda come una finestra scorrevole (vedi [Come funziona ogni modalità di simultaneità](#)), questo esempio mostra l'operazione in batch per dimostrare la velocità di ciascuna modalità.

Tolleranza rigorosa ai guasti

Questo esempio, che utilizza la modalità di tolleranza rigorosa ai guasti, riduce la simultaneità effettiva rispetto al numero di errori che si verificano in ogni batch precedente. Ogni batch presenta

20 istanze non riuscite, il che riduce quindi la concorrenza effettiva del batch successivo di 20 fino a quando l' StackSet operazione non raggiunge il valore di tolleranza di errore di 100.

Nella tabella seguente, la simultaneità effettiva iniziale del primo batch è pari a 101 istanze di stack. La simultaneità effettiva è 101 perché è il valore più basso tra quello del numero massimo di account simultanei (250) e quello della tolleranza ai guasti (100) +1. Ogni batch contiene 20 distribuzioni di istanze di stack non riuscite, il che riduce quindi la simultaneità effettiva di ogni batch successivo di 20 istanze di stack.

Tolleranza rigorosa ai guasti	Batch 1	Batch 2	Batch 3	Batch 4	Batch 5	Batch 6
Conteggio effettivo della simultaneità	101	81	61	41	21	-
Numero di istanze non riuscite	20	20	20	20	20	-
Numero di istanze di stack riuscite	81	61	41	21	1	-

L'operazione che utilizza Strict failure tolerance ha completato 305 implementazioni di istanze stack in 5 batch quando l' StackSet operazione ha raggiunto la tolleranza di errore di 100 istanze stack. L' StackSet operazione distribuisce correttamente 205 istanze dello stack prima che fallisca.

Tolleranza flessibile ai guasti

Questo esempio, che utilizza la modalità di tolleranza flessibile ai guasti, mantiene lo stesso conteggio effettivo di simultaneità definito dal valore numero massimo di account simultanei di 250 istanze di stack, indipendentemente dal numero di istanze non riuscite. Le StackSet operazioni

mantengono la stessa concorrenza effettiva fino a raggiungere il valore di tolleranza di errore di 100 istanze.

Nella tabella seguente, la simultaneità effettiva iniziale del primo batch è pari a 250 istanze di stack. La concorrenza effettiva è 250 perché il valore Massimo di conti concorrenti è impostato su 250 e la modalità Soft failure tolerance consente di StackSets utilizzare questo valore come concorrenza effettiva, indipendentemente dal numero di errori. Anche se in questo esempio sono presenti 50 errori in ciascuno dei batch, la simultaneità effettiva rimane inalterata.

Tolleranza flessibile ai guasti	Batch 1	Batch 2	Batch 3	Batch 4	Batch 5	Batch 6
Conteggio effettivo della simultaneità	250	250	-	-	-	-
Numero di istanze non riuscite	50	50	-	-	-	-
Numero di istanze di stack riuscite	200	200	-	-	-	-

Utilizzando lo stesso valore numero massimo di account simultanei e tolleranza ai guasti, l'operazione che utilizza la modalità di tolleranza flessibile ai guasti ha completato 500 implementazioni di istanze di stack in 2 batch. L' StackSet operazione distribuisce correttamente 400 istanze dello stack prima che fallisca.

Scelta della modalità Concurrency (console)

Durante la creazione o l'aggiornamento di un StackSet file, nella pagina Imposta opzioni di distribuzione, per la modalità Concurrency, scegli Strict failure tolerance o Soft failure tolerance.

Scelta della modalità Concurrency ()AWS CLI

È possibile utilizzare il ConcurrencyMode parametro con i seguenti StackSets comandi:

- [create-stack-instances](#)
- [delete-stack-instances](#)
- [detect-stack-set-drift](#)
- [import-stacks-to-stack-set](#)
- [update-stack-instances](#)
- [update-stack-set](#)

Questi comandi hanno un parametro esistente chiamato `--operation-preferences` che può utilizzare l'impostazione ConcurrencyMode. ConcurrencyMode può essere impostata su uno dei seguenti valori:

- STRICT_FAILURE_TOLERANCE
- SOFT_FAILURE_TOLERANCE

L'esempio seguente crea un'istanza stack utilizzando

STRICT_FAILURE_TOLERANCEConcurrencyMode, con un FailureToleranceCount set su 10 e un MaxConcurrentCount set su 5.

```
aws cloudformation create-stack-instances \  
  --stack-set-name example-stackset \  
  --accounts 123456789012 \  
  --regions eu-west-1 \  
  --operation-preferences  
ConcurrencyMode=STRICT_FAILURE_TOLERANCE,FailureToleranceCount=10,MaxConcurrentCount=5
```

Note

Per procedure dettagliate per la creazione e l'aggiornamento di un StackSet, consultate i seguenti argomenti:

- [Crea StackSets \(autorizzazioni autogestite\)](#)
- [Crea StackSets \(autorizzazioni gestite dal servizio\)](#)

- [Aggiorna StackSets](#)

Esecuzione del rilevamento della deriva su CloudFormation StackSets

Anche se gestisci gli stack e le risorse in essi contenute CloudFormation, gli utenti possono modificare tali risorse al di fuori di CloudFormation. Gli utenti possono modificare le risorse direttamente utilizzando il servizio sottostante che ha creato la risorsa. Eseguendo il rilevamento della deriva su un StackSet, è possibile determinare se alcune delle istanze dello stack appartenenti allo stack StackSet differiscono, o si sono discostate, dalla configurazione prevista.

Argomenti

- [Come esegue il rilevamento della deriva su CloudFormation un StackSet](#)
- [Rileva la deriva su una \(console\) StackSet](#)
- [Rileva la deriva su un StackSet \(AWS CLI\)](#)
- [Interruzione del rilevamento della deriva su un StackSet](#)

Come esegue il rilevamento della deriva su CloudFormation un StackSet

Quando CloudFormation esegue il rilevamento della deriva su un StackSet, esegue il rilevamento della deriva sullo stack associato a ciascuna istanza dello stack in un StackSet. A tale scopo, CloudFormation confronta lo stato corrente di ogni risorsa nello stack con lo stato previsto di tale risorsa, come definito nel modello dello stack e qualsiasi parametro di input specificato. Se lo stato corrente di una risorsa varia dallo stato previsto, tale risorsa viene considerata deviata. Se una o più risorse in uno stack sono deviate, lo stack stesso è considerato deviato e anche le istanze dello stack a cui lo stack è associato vengono considerate deviate. Se una o più istanze dello stack in uno sono andate alla deriva, si considera che la stessa istanza StackSet abbia subito una deriva. StackSet

Il rilevamento delle deviazioni identifica le modifiche non gestite, ovvero le modifiche apportate agli stack esterni a CloudFormation. Le modifiche apportate direttamente a uno stack, anziché a un StackSet a livello locale, non sono considerate deviazioni. Ad esempio, supponiamo di avere uno stack associato a un'istanza dello stack di un StackSet. Se si utilizza CloudFormation per aggiornare lo stack per utilizzare un modello diverso, ciò non viene considerato deriva, anche se quello stack ora ha un modello diverso da qualsiasi altro stack appartenente a un StackSet. Questo

perché lo stack corrisponde ancora al modello previsto e alla configurazione dei parametri in CloudFormation.

Per informazioni dettagliate su come CloudFormation esegue il rilevamento della deriva su uno stack, consulta [Rileva le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento della deriva](#)

Poiché CloudFormation esegue il rilevamento della deriva su ogni pila singolarmente, tiene conto di tutti i valori dei parametri sostituiti per determinare se una pila ha subito una deriva. Per ulteriori informazioni sull'override dei parametri del modello nelle istanze dello stack, consulta [Sostituisci i valori dei parametri sugli stack all'interno del tuo CloudFormation StackSet](#).

Se esegui il rilevamento della deriva [direttamente su uno stack associato a un'istanza dello stack](#), tali risultati non sono disponibili nella pagina della console. StackSets

Rileva la deriva su una (console) StackSet

Per rilevare la deriva su un StackSet

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella StackSetspagina, seleziona quello StackSet su cui desideri eseguire il rilevamento della deriva.
3. Dal menu Actions (Operazioni), selezionare Detect drifts (Rileva deviazioni).

CloudFormation visualizza una barra informativa che indica che il rilevamento della deriva è stato avviato per il selezionato. StackSet

4. Facoltativo: per monitorare lo stato di avanzamento dell'operazione di rilevamento della deviazione:
 - a. Seleziona il StackSet nome per visualizzare la pagina dei dettagli dello Stackset.
 - b. Selezionare la scheda Operations (Operazioni), selezionare l'operazione di rilevamento della deviazione e quindi selezionare View drift details (Visualizza dettagli deviazione).

CloudFormation visualizza la finestra di dialogo dei dettagli dell'operazione.

5. Attendere il CloudFormation completamento dell'operazione di rilevamento della deriva. Al termine dell'operazione di rilevamento della deriva, CloudFormation aggiorna Drift status e Last drift check time per il tuo. StackSet Questi campi sono elencati nella scheda Panoramica della pagina dei StackSet dettagli del selezionato. StackSet

L'operazione di rilevamento della deriva può richiedere del tempo, a seconda del numero di istanze dello stack incluse e del StackSet numero di risorse incluse in. StackSet È possibile eseguire una sola operazione di rilevamento della deriva su una determinata StackSet operazione alla volta. CloudFormation continua l'operazione di rilevamento della deriva anche dopo aver chiuso la barra delle informazioni.

6. Per esaminare i risultati del rilevamento della deriva per le istanze dello stack in a StackSet, seleziona la scheda Istanze dello stack.

La colonna Stack name (Nome stack) elenca il nome dello stack associato a ogni istanza dello stack e la colonna di Drift status (Stato deviazione) elenca lo stato della deviazione di tale stack. Uno stack è considerato come deviato se una o più delle relative risorse risultano deviate.

7. Per esaminare i risultati del rilevamento della deviazione per lo stack associato a un'istanza dello stack specifica:
 - a. Scegli la scheda Operazioni.
 - b. Seleziona l'operazione di deviazione per la quale desideri visualizzare i risultati del rilevamento della deviazione. Un pannello di suddivisione mostrerà lo stato e il motivo dell'istanza dello stack per l'operazione selezionata. Per un'operazione di deviazione, la colonna del motivo dello stato mostra lo stato di deviazione di un'istanza stack.
 - c. Scegli l'istanza dello stack per cui desideri visualizzare i dettagli della deviazione, quindi seleziona Visualizza deviazioni delle risorse. Nella tabella Stato deviazione risorse sulla pagina Deviazione delle risorse elenca ogni risorsa di stack, il relativo stato di deviazione e l'ultima volta in cui è stato iniziato il rilevamento sulla risorsa. L'ID logico e l'ID fisico di ogni risorsa sono visualizzati per consentirti di identificarla.
8. È possibile ordinare le risorse in base al loro stato deviazione, utilizzando la colonna Drift (Deviazione).

Per visualizzare i dettagli su una risorsa modificata:

- Con la risorsa selezionata, scegli Visualizza dettagli deviazione.

CloudFormation visualizza la pagina di dettaglio della deriva per quella particolare risorsa. Questa pagina elenca le differenze tra le risorse. Elenca anche i valori delle proprietà previsti e correnti della risorsa.

 Note

Se lo stack appartiene a una Regione e a un account diversi da quelli a cui sei attualmente connesso, il pulsante Rileva deviazione sarà disabilitato e non potrai visualizzare i dettagli.

Rileva la deriva su un StackSet (AWS CLI)

Per rilevare la deriva su un'intera pila utilizzando il AWS CLI, utilizzate la seguente procedura:

Per rilevare la deriva su un StackSet

1. Utilizzate il [detect-stack-set-drift](#) comando per rilevare la deriva su un'intera istanza dello stack StackSet e sulle relative istanze dello stack associate.

L'esempio seguente avvia il rilevamento della deriva su. StackSet `stack-set-drift-example`

```
aws cloudformation detect-stack-set-drift \  
  --stack-set-name stack-set-drift-example
```

Output:

```
{  
  "OperationId": "c36e44aa-3a83-411a-b503-cb611example"  
}
```

2. Poiché le operazioni di rilevamento della StackSet deriva possono essere operazioni di lunga durata, utilizzate il [describe-stack-set-operation](#) comando per monitorare lo stato dell'operazione. Questo comando accetta l'ID dell' StackSet operazione restituito dal comando. `detect-stack-set-drift`

Negli esempi seguenti viene utilizzato l'ID dell'operazione dell'esempio precedente per restituire informazioni sull'operazione di rilevamento della StackSet deriva. In questo esempio, l'operazione è ancora in esecuzione. Delle sette istanze dello stack associate a questa istanza StackSet, è già stato rilevato che un'istanza dello stack è andata alla deriva, due istanze sono sincronizzate e il rilevamento della deriva per le restanti quattro istanze dello stack è ancora

in corso. Poiché un'istanza è andata alla deriva, lo stato di deriva dell'istanza stessa è ora lo stesso. StackSet DRIFTED

```
aws cloudformation describe-stack-set-operation \  
  --stack-set-name stack-set-drift-example \  
  --operation-id c36e44aa-3a83-411a-b503-cb611example
```

Output:

```
{  
  "StackSetOperation": {  
    "Status": "RUNNING",  
    "AdministrationRoleARN": "arn:aws:iam::123456789012:role/  
AWSCloudFormationStackSetAdministrationRole",  
    "OperationPreferences": {  
      "RegionOrder": []  
    },  
    "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole",  
    "StackSetDriftDetectionDetails": {  
      "DriftedStackInstancesCount": 1,  
      "TotalStackInstancesCount": 7,  
      "LastDriftCheckTimestamp": "2019-12-04T20:34:28.543Z",  
      "InSyncStackInstancesCount": 2,  
      "InProgressStackInstancesCount": 4,  
      "DriftStatus": "DRIFTED",  
      "FailedStackInstancesCount": 0  
    },  
    "Action": "DETECT_DRIFT",  
    "CreationTimestamp": "2019-12-04T20:33:13.673Z",  
    "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-  
a73f-8c22example",  
    "OperationId": "c36e44aa-3a83-411a-b503-cb611example"  
  }  
}
```

Eseguendo lo stesso comando in un secondo momento, questo esempio mostra le informazioni restituite una volta completata l'operazione di rilevamento della deviazione. Due delle sette istanze dello stack totali associate a questa situazione StackSet sono andate alla deriva, rendendo lo stato di drift dell'istanza stessa pari a. StackSet DRIFTED

```
aws cloudformation describe-stack-set-operation \  

```

```
--stack-set-name stack-set-drift-example \  
--operation-id c36e44aa-3a83-411a-b503-cb611example
```

Output:

```
{  
  "StackSetOperation": {  
    "Status": "SUCCEEDED",  
    "AdministrationRoleARN": "arn:aws:iam::123456789012:role/  
AWSCloudFormationStackSetAdministrationRole",  
    "OperationPreferences": {  
      "RegionOrder": []  
    }  
  },  
  "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole",  
  "EndTimestamp": "2019-12-04T20:37:32.829Z",  
  "StackSetDriftDetectionDetails": {  
    "DriftedStackInstancesCount": 2,  
    "TotalStackInstancesCount": 7,  
    "LastDriftCheckTimestamp": "2019-12-04T20:36:55.612Z",  
    "InSyncStackInstancesCount": 5,  
    "InProgressStackInstancesCount": 0,  
    "DriftStatus": "DRIFTED",  
    "FailedStackInstancesCount": 0  
  },  
  "Action": "DETECT_DRIFT",  
  "CreationTimestamp": "2019-12-04T20:33:13.673Z",  
  "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-  
a73f-8c22example",  
  "OperationId": "c36e44aa-3a83-411a-b503-cb611example"  
}
```

- Una volta completata l'operazione di rilevamento della StackSet deriva, utilizzate i comandi, `describe-stack-set`, `list-stack-instances`, `describe-stack-instance`, e `list-stack-instance-resource-drifts` per esaminare i risultati.

Il comando [describe-stack-set](#) include le stesse informazioni dettagliate sulla deviazione restituite dal comando `describe-stack-set-operation`.

```
aws cloudformation describe-stack-set \  
--stack-set-name stack-set-drift-example
```

Output:

```
{
  "StackSet": {
    "Status": "ACTIVE",
    "Description": "Demonstration of drift detection on stack sets.",
    "Parameters": [],
    "Tags": [
      {
        "Value": "Drift detection",
        "Key": "Feature"
      }
    ],
    "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole",
    "Capabilities": [],
    "AdministrationRoleARN": "arn:aws:iam::123456789012:role/AWSCloudFormationStackSetAdministrationRole",
    "StackSetDriftDetectionDetails": {
      "DriftedStackInstancesCount": 2,
      "TotalStackInstancesCount": 7,
      "LastDriftCheckTimestamp": "2019-12-04T20:36:55.612Z",
      "InProgressStackInstancesCount": 0,
      "DriftStatus": "DRIFTED",
      "DriftDetectionStatus": "COMPLETED",
      "InSyncStackInstancesCount": 5,
      "FailedStackInstancesCount": 0
    },
    "StackSetARN": "arn:aws:cloudformation:us-east-1:123456789012:stackset/stack-set-drift-example:bd1f4017-d4f9-432e-a73f-8c22example",
    "TemplateBody": [details omitted],
    "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-a73f-8c22ebexample",
    "StackSetName": "stack-set-drift-example"
  }
}
```

È possibile utilizzare il [list-stack-instances](#) comando per restituire informazioni di riepilogo sulle istanze dello stack associate a a StackSet, incluso lo stato di deriva di ciascuna istanza dello stack.

In questo esempio, l'esecuzione `list-stack-instances` sull'esempio `StackSet` con il filtro `drift status` impostato su `DRIFTED` consente di identificare quali due istanze dello stack hanno uno stato di drift pari a `DRIFTED`

```
aws cloudformation list-stack-instances \  
  --stack-set-name stack-set-drift-example \  
  --filters Name=DRIFT_STATUS,Values=DRIFTED
```

Output:

```
{  
  "Summaries": [  
    {  
      "StackId": "arn:aws:cloudformation:eu-west-1:123456789012:stack/  
StackSet-stack-set-drift-example-b0fb6083-60c0-4e39-  
af15-2f071e0db90c/0e4f0940-16d4-11ea-93d8-0641cexample",  
      "Status": "CURRENT",  
      "Account": "012345678910",  
      "Region": "eu-west-1",  
      "LastDriftCheckTimestamp": "2019-12-04T20:37:32.687Z",  
      "DriftStatus": "DRIFTED",  
      "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-  
a73f-8c22eexample",  
      "LastOperationId": "c36e44aa-3a83-411a-b503-cb611example"  
    },  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/  
StackSet-stack-set-drift-example-b7fde68e-e541-44c2-b33d-  
ef2e2988071a/008e6030-16d4-11ea-8090-12f89example",  
      "Status": "CURRENT",  
      "Account": "123456789012",  
      "Region": "us-east-1",  
      "LastDriftCheckTimestamp": "2019-12-04T20:34:28.275Z",  
      "DriftStatus": "DRIFTED",  
      "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-  
a73f-8c22eexample",  
      "LastOperationId": "c36e44aa-3a83-411a-b503-cb611example"  
    },  
    [additional stack instances omitted]
```

```
]
}
```

Il comando [describe-stack-instance](#) restituisce anche queste informazioni, ma per una singola istanza di stack, come nell'esempio riportato di seguito.

```
aws cloudformation describe-stack-instance \
  --stack-set-name stack-set-drift-example \
  --stack-instance-account 012345678910 --stack-instance-region us-east-1
```

Output:

```
{
  "StackInstance": {
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/StackSet-stack-set-drift-example-b7fde68e-e541-44c2-b33d-ef2e2988071a/008e6030-16d4-11ea-8090-12f89example",
    "Status": "CURRENT",
    "Account": "123456789012",
    "Region": "us-east-1",
    "ParameterOverrides": [],
    "DriftStatus": "DRIFTED",
    "LastDriftCheckTimestamp": "2019-12-04T20:34:28.275Z",
    "StackSetId": "stack-set-drift-example:bd1f4017-d4f9-432e-a73f-8c22eexample",
    "LastOperationId": "c36e44aa-3a83-411a-b503-cb611example"
  }
}
```

4. Dopo aver identificato quali istanze dello stack sono andate alla deriva, puoi utilizzare le informazioni sulle istanze dello stack restituite dai comandi `aws cloudformation list-stack-instances` o `aws cloudformation describe-stack-instance` per eseguire il comando `aws cloudformation list-stack-instance-resource-drifts`. Questo comando restituisce informazioni dettagliate su quali risorse nello stack sono state deviate per una determinata operazione di deviazione.

L'esempio seguente utilizza il parametro `--stack-instance-resource-drift-statuses` per richiedere le informazioni sulla deviazione dello stack per le risorse che sono state modificate o eliminate nell'esempio dell'operazione di deviazione precedente. La richiesta restituisce informazioni sulla risorsa che è stata modificata, tra cui dettagli su due proprietà della stessa i cui valori sono stati modificati. Nessuna risorsa è stata eliminata.

```
aws cloudformation list-stack-instance-resource-drifts \
  --stack-set-name my-stack-set-with-resource-drift \
  --stack-instance-account 123456789012 \
  --stack-instance-region us-east-1 \
  --operation-id c36e44aa-3a83-411a-b503-cb611example \
  --stack-instance-resource-drift-statuses MODIFIED DELETED
```

Output:

```
{
  "Summaries": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/my-stack-set-with-resource-drift/489e5570-df85-11e7-a7d9-50example",
      "ResourceType": "AWS::SQS::Queue",
      "Timestamp": "2018-03-26T17:23:34.489Z",
      "PhysicalResourceId": "https://sqs.us-east-1.amazonaws.com/123456789012/my-stack-with-resource-drift-Queue-494PBHC076H4",
      "StackResourceDriftStatus": "MODIFIED",
      "PropertyDifferences": [
        {
          "PropertyPath": "/DelaySeconds",
          "ActualValue": "120",
          "ExpectedValue": "20",
          "DifferenceType": "NOT_EQUAL"
        },
        {
          "PropertyPath": "/RedrivePolicy/maxReceiveCount",
          "ActualValue": "12",
          "ExpectedValue": "10",
          "DifferenceType": "NOT_EQUAL"
        }
      ],
      "LogicalResourceId": "Queue"
    }
  ]
}
```

Interruzione del rilevamento della deriva su un StackSet

Poiché il rilevamento della deriva su a StackSet può essere un'operazione di lunga durata, in alcuni casi si desidera interrompere un'operazione di rilevamento della deriva attualmente in esecuzione su un. StackSet

Per interrompere il rilevamento della deriva su una (console) StackSet

1. Apri la AWS CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Nella StackSetspagina, seleziona il nome di. StackSet

CloudFormation visualizza la pagina dei StackSets dettagli per il selezionato StackSet.

3. Nella pagina dei StackSets dettagli, selezionare la scheda Operazioni, quindi selezionare l'operazione di rilevamento della deriva.
4. Selezionare Stop operation (Interrompi operazione).

Per interrompere il rilevamento della deriva su () StackSet AWS CLI

- Utilizza il comando [stop-stack-set-operation](#). È necessario fornire sia il StackSet nome che l'ID dell'operazione di rilevamento StackSet della deriva.

```
aws cloudformation stop-stack-set-operation \  
  --stack-set-name stack-set-drift-example \  
  --operation-id 624af370-311a-11e8-b6b7-500cexample
```

Importa pile in AWS CloudFormation StackSets

Un'operazione di importazione degli stack può importare gli stack esistenti in nuovi o esistenti StackSets, in modo da poter migrare gli stack esistenti verso un'unica operazione. StackSet

In caso di gestione automatica StackSets, l'operazione di importazione può importare pile nell'account amministratore o in diversi account di destinazione e. Regioni AWS Per i servizi gestiti StackSets, l'operazione di importazione può importare qualsiasi stack nello stesso AWS Organizations account di gestione.

Di seguito sono riportate le considerazioni e le limitazioni relative all'importazione degli stack in: StackSets

- L'operazione di importazione può importare fino a 10 stack utilizzando lo stack in linea IDs o fino a 200 stack utilizzando un oggetto Amazon S3.
- La proprietà NoEcho non è supportata. Gli stack che contengono NoEcho non verranno importati in nuovi file tramite l'importazione. StackSets StackSet
- Gli stack possono appartenere solo a uno. StackSet
- È possibile implementare i tag dello stack StackSet specificando i tag in modo esplicito come parametri nell'operazione di importazione dello stack.
- Le sostituzioni dei parametri personalizzati di uno stack non sono interessate durante l'operazione di importazione.
- Le StackSets quote e le istanze dello stack si applicano all'importazione degli stack. Per ulteriori informazioni sulle quote, consulta [Comprendi le CloudFormation quote](#).

Argomenti

- [Importazione di stack autogestita per AWS CloudFormation StackSets](#)
- [Importazione di stack gestita dal servizio per AWS CloudFormation StackSets](#)
- [Ripristina le importazioni di stack in AWS CloudFormation StackSets](#)

Importazione di stack autogestita per AWS CloudFormation StackSets

L'operazione di importazione degli CloudFormation stack consente di importare gli stack esistenti in stack nuovi o esistenti StackSets, in modo da poter migrare gli stack esistenti verso un'unica operazione. StackSet L'importazione di stack, consente di evitare tempi di inattività e interruzioni senza dover eliminare e ricreare tali risorse. Una volta importato lo stack in a StackSet, lo stack originale diventerà un'istanza dello stack set specificato.

Considerazioni per le importazioni di stack autogestite

- L'operazione di importazione dello stack richiede un account amministratore in cui si crea un StackSet account di destinazione che contenga uno stack.
- L'account di destinazione deve disporre delle autorizzazioni per utilizzare l'operazione `GetTemplate` con l'input di ID stack o ARN. Per questo motivo, al tuo account amministratore devono essere concesse le autorizzazioni `AWSCloudFormationStackSetAdministrationRole` o `AWSCloudFormationStackSetsExecutionRole` le autorizzazioni.

Argomenti

- [Importa uno stack esistente in uno nuovo StackSet \(console\)](#)
- [Importa uno stack esistente in uno esistente StackSet \(console\)](#)
- [Importa uno stack in a StackSet \(AWS CLI\)](#)

Importa uno stack esistente in uno nuovo StackSet (console)

Prima di iniziare, identifica lo stack che desideri importare.

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Dal pannello di navigazione, scegli. StackSets
3. Nella parte superiore della StackSetspagina, scegli Crea StackSet.
4. Nella pagina Scegli un modello, specifica un modello con una delle seguenti opzioni e scegli Avanti.
 - Scegli Amazon S3 URL (URL Amazon S3) e specifica l'URL per il modello nella casella di testo.
 - Scegli Upload a template file (Carica un file modello) e cerca il modello.
 - Scegli From stack ID (Da ID stack) e immetti l'ID stack.
5. Nella pagina Specificare StackSet i dettagli, inserisci il nome di un StackSet file che desideri creare e scegli Avanti.

(Facoltativo) Inserite una descrizione di StackSet.

6. Nella pagina Configura le StackSet opzioni, rivedi le tue scelte e scegli Avanti.
7. Nella pagina Imposta le opzioni di distribuzione, scegli Importa stack in stack set.
8. Immetti l'ID dello stack da importare nel campo Stacks to import (Stack da importare). Ad esempio, *arn:aws:cloudformation:us-east-1:123456789012:stack/StackToImport/f449b250-b969-11e0-a185-5081d0136786*.

(Facoltativo) Scegli Aggiungi un altro stack ID e inserisci l'ID dello stack di un altro stack che desideri importare. Puoi aggiungere fino a 10 stack per operazione di importazione di stack.

9. Esamina le opzioni di distribuzione e scegli Avanti.
10. Nella pagina Revisione, esamina le tue scelte e StackSet le tue proprietà. Quando sei pronto per importare lo stack nel tuo StackSet, scegli Invia.

Risultati: lo stack importato è ora un'istanza dello stack specificato. StackSet Per ulteriori informazioni sullo stato di importazione dello stack, consulta. [StackSets codici di stato](#)

Importa uno stack esistente in uno esistente StackSet (console)

Prima di iniziare, identifica lo stack che desideri importare.

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Dal pannello di navigazione, scegli. StackSets
3. Nella StackSetspagina, scegli StackSet quello in cui vuoi importare uno stack.
4. Con quello StackSet selezionato, scegli Aggiungi pile a StackSet dal menu Azioni.
5. Nella pagina Imposta le opzioni di distribuzione, scegli Importa pile nello stack set e inserisci l'ID dello stack che desideri importare nel campo Pile da importare. Ad esempio, *arn:aws:cloudformation:us-east-1:123456789012:stack/StackToImport/f449b250-b969-11e0-a185-5081d0136786*.

(Facoltativo) Scegli Aggiungi un altro stack ID e inserisci l'ID dello stack di un altro stack che desideri importare. Puoi aggiungere fino a 10 stack per operazione di importazione di stack.

6. Scegli Next (Successivo).
7. Nella pagina Specificare le eccezioni, rivedi le tue scelte e scegli Avanti.
8. Nella pagina Revisione, esamina le tue scelte e le tue proprietà StackSet. Quando sei pronto per creare il tuo StackSet, scegli Invia.

Risultati: lo stack importato è ora un'istanza dello stack specificato. StackSet Per ulteriori informazioni sullo stato di importazione dello stack, consulta. [StackSets codici di stato](#)

Importa uno stack in a StackSet ()AWS CLI

Per importare uno stack esistente in uno nuovo StackSet

Il `create-stack-set` comando seguente crea uno stack StackSet e importa lo stack specificato. Lo stack da importare è identificato dal relativo ARN. Sostituisci il testo segnaposto con le tue informazioni.

```
aws cloudformation create-stack-set \  
  --stack-set-name MyStackSet \  
  --template-url ...
```

```
--stack-id arn:aws:cloudformation:us-east-1:123456789012:stack/
StackToImport/466df9e0-0dff-08e3-8e2f-5088487c4896 \
--administration-role-arn arn:aws:iam::123456789012:role/
AWSCloudFormationStackSetAdministrationRole \
--execution-role-name AWSCloudFormationStackSetExecutionRole
```

Per importare uno stack esistente in uno esistente StackSet

Il `import-stacks-to-stack-sets` comando seguente importa lo stack specificato in.

MyStackSet StackSet Lo stack da importare è identificato dal relativo ARN. Sostituisci il testo segnaposto con le tue informazioni.

```
aws cloudformation import-stacks-to-stack-set \
--stack-set MyStackSet \
--stack-ids arn:aws:cloudformation:us-east-1:123456789012:stack/StackToImport/
f449b250-b969-11e0-a185-5081d0136786
```

Per specificare più di uno stack, utilizzate il seguente formato per il valore dell'opzione. `--stack-ids`

```
--stack-ids "arn_1" "arn_2"
```

Per clonare lo stack importato in altre regioni e account

Il `create-stack-instances` comando seguente aggiunge istanze dello stack al tuo. StackSet Sostituisci il testo segnaposto con le tue informazioni.

```
aws cloudformation create-stack-instances \
--stack-set-name MyStackSet \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1","region_2"]'
```

Importazione di stack gestita dal servizio per AWS CloudFormation StackSets

L'operazione di importazione degli CloudFormation stack consente di importare gli stack esistenti in stack nuovi o esistenti StackSets, in modo da poter migrare gli stack esistenti verso un'unica operazione. StackSet StackSets estende la funzionalità degli stack, in modo da poter creare, aggiornare o eliminare gli stack su più account e regioni con un'unica operazione.

Considerazioni per le importazioni di stack gestite dal servizio

- L'operazione di importazione dello stack richiede un account di gestione o un account amministratore delegato in cui è possibile gestire gli elementi associati, ad AWS Organizations esempio abilitando l'accesso fiduciario con. StackSets
- Gli account di destinazione devono essere membri dell'account AWS Organizations gestito dall'account di gestione o dell'account amministratore delegato.
- Lo stack di destinazione esiste in uno degli obiettivi. OUs
- L'account di destinazione deve essere membro di AWS Organizations.
- AWS Organizations l'accesso dovrebbe essere nello ACTIVATED stato per le Organizzazioni.
- Gli stack importati devono essere presenti in uno degli account membri e non nell'account di gestione.

Argomenti

- [Importa uno stack gestito dal servizio in una nuova StackSet \(console\)](#)
- [Crea e importa uno stack gestito dai servizi in uno stack esistente \(console\) StackSet](#)
- [Importa uno stack gestito dal servizio in uno stack esistente \(console\) StackSet](#)
- [Importazione di uno stack gestito dal servizio in un \(\) StackSet AWS CLI](#)

Importa uno stack gestito dal servizio in una nuova StackSet (console)

Importa uno stack in uno nuovo utilizzando il StackSet AWS Management Console

Per importare un nuovo stack in un StackSet, identifica uno stack che contiene la risorsa che desideri importare.

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.](https://console.aws.amazon.com/cloudformation)
2. Dal pannello di navigazione, scegli. StackSets
3. Nella parte superiore della StackSetspagina, scegli Crea StackSet.
4. Nella pagina Scegli un modello, procedi come segue:
 - a. Per StackSet il modello di autorizzazione, scegli Autorizzazioni gestite dal servizio.
 - b. Per Prerequisito: prepara il modello, scegli Il modello è pronto e scegli il modello utilizzando una delle seguenti opzioni:

- Per l'URL di Amazon S3, inserisci il tuo URL Amazon S3 nel campo URL Amazon S3.
- Per caricare un file modello, scegli un CloudFormation modello sul tuo computer locale.

Accetta le impostazioni desiderate e scegli Next (Avanti).

5. Nella pagina Specificare StackSet i dettagli, procedi come segue:

- a. Immettete un StackSet nome nella casella del StackSet nome.
- b. (Facoltativo) Inserisci una descrizione nella sezione della StackSet descrizione.

Nella pagina Configura le StackSet opzioni, rivedi le tue scelte e scegli Avanti.

6. Nella pagina Imposta opzioni di distribuzione, procedi come segue:

- a. Per Aggiungi pile allo stack set, scegli Importa pile allo stack set.
- b. Per Stacks to import (Stack da importare), scegli il metodo di importazione dello stack.
 - i. Per Stack ID (ID stack), immetti l'ID stack.
 - ii. Per Stack URL, inserisci l'URL di Amazon S3.

7. In Associa unità organizzative, procedi come segue:

- a. Scegli Associa all'organizzazione per utilizzare l'unità organizzativa root.
- b. Scegli Associa alle unità organizzative (OUs) per inserire l'unità organizzativa principale IDs per gli stack da importare. Ad esempio, se Stack 1 e Stack 2 sono sotto OU1 e Stack 3 è sotto OU2, immetti OU1 e OU2.

Accetta le impostazioni desiderate e scegli Next (Avanti).

8. Rivedi le impostazioni nella pagina Review (Rivedi) e scegli Submit (Invia).

Crea e importa uno stack gestito dai servizi in uno stack esistente (console) StackSet

Per importare uno stack esistente in uno nuovo StackSet, identifica uno stack che contiene la risorsa che desideri importare.

Per creare StackSet e importare uno stack

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Dal pannello di navigazione, scegli. StackSets
3. Nella parte superiore della StackSetspagina, scegli Crea StackSet.
4. Nella pagina Scegli un modello, procedi come segue:
 - a. Per StackSet il modello di autorizzazione, scegli Autorizzazioni gestite dal servizio.
 - b. Per Prerequisito: prepara il modello, scegli Il modello è pronto e scegli il modello utilizzando una delle seguenti opzioni:
 - Per l'URL di Amazon S3, inserisci il tuo URL Amazon S3 nel campo URL Amazon S3.
 - Per caricare un file modello, scegli un CloudFormation modello sul tuo computer locale.

Accetta le impostazioni desiderate e scegli Next (Avanti).

5. Nella pagina Specificare StackSet i dettagli, procedi come segue:
 - a. Immettete un StackSet nome nella casella del StackSet nome.
 - b. (Facoltativo) Inserisci una descrizione nella sezione della StackSet descrizione.

Nella pagina Configura le StackSet opzioni, rivedi le tue scelte e scegli Avanti.

6. Nella pagina Imposta opzioni di distribuzione, procedi come segue:
 - In Add stacks to stack set (Aggiungi stack a un set di stack), scegli Deploy new stacks (Implementa nuovi stack).
7. Per la sezione Associa unità organizzative, procedi come segue:
 - a. Scegli Associa all'organizzazione per utilizzare l'unità organizzativa root.
 - b. Scegli Associa alle unità organizzative (OUs) per inserire l'unità organizzativa principale IDs per gli stack da importare. Ad esempio, se Stack 1 e Stack 2 sono sotto OU1 e Stack 3 è sotto OU2, immetti OU1 e OU2.
8. Per Specify regions (Specifica Regioni) e Deployment options (Opzioni di implementazione), rivedi le scelte effettuate.

Accetta le impostazioni desiderate e scegli Next (Avanti).

9. Rivedi le impostazioni nella pagina Review (Rivedi) e scegli Submit (Invia).

Importa uno stack gestito dal servizio in uno stack esistente (console) StackSet

Scegli il tuo StackSet e identifica lo stack che desideri importare.

Per importare uno stack in uno esistente StackSet

1. Accedi a AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Dal pannello di navigazione, scegli. StackSets
3. Scegli la pila in cui StackSet vuoi importare una pila, quindi scegli Aggiungi pile StackSet dal menu a discesa Azioni.
4. Nella pagina Imposta le opzioni di distribuzione, procedi come segue:
 - a. Per Aggiungi pile allo stack set, scegli Importa pile allo stack set.
 - b. In Pile da importare, procedi come segue
 - i. Per Stack ID (ID stack), immetti l'ID stack.
 - ii. Per Stack URL, inserisci l'URL di Amazon S3.
 - c. In Associa unità organizzative, procedi come segue:
 - i. Scegli Associa all'organizzazione per utilizzare l'unità organizzativa root.
 - ii. Scegli Associa alle unità organizzative (OUs) per inserire l'unità organizzativa principale IDs per gli stack da importare. Ad esempio, se Stack 1 e Stack 2 sono sotto OU1 e Stack 3 è sotto OU2, immetti OU1 e OU2.

Accetta le impostazioni desiderate e scegli Next (Avanti).

5. Rivedi la pagina Specify stack details (Specifica dettagli stack) e scegli Next (Avanti).
6. Conferma e rivedi la pagina Review (Rivedi) e scegli Submit (Invia).

Importazione di uno stack gestito dal servizio in un () StackSet AWS CLI

Una volta creato StackSet uno, potete importare gli stack passando gli ID dello stack degli stack importati. Puoi inoltre passare l'elenco degli ID delle unità organizzative a cui desideri mapparli.

CloudFormation importerà gli stack forniti dall'utente all'interno di tali stack OUs e li utilizzerà OUs come obiettivi di distribuzione per. StackSet Lo stack IDs presentato nell'input verrà mappato all'unità organizzativa più vicina nell'elenco di ID OU inserito internamente. Se uno stack non appartiene a un ID OU esistente nell'elenco di input, AWS CLI restituirà l'errore. StackNotFoundException

L'operazione `import-stacks-to-stack-set` istanze di stack per gli stack nell'input dell'ID dell'unità organizzativa. AWS CLI Gli esempi seguenti utilizzano l'`import-stacks-to-stack-set` operazione per importare uno stack in un. StackSet

- Per utilizzare l'operazione `import-stacks-to-stack-sets`, specifica `stack-ids` o `stack-ids-url` che desideri importare nel set di stack.

```
aws cloudformation import-stacks-to-stack-set \  
  --stack-set-name ServiceManagedStackSet \  
  --stack-ids "arn:123456789012:us-east-1:Stack1" \  
  --organizational-unit-ids ou-examplerootid111-exampleouid111
```

```
aws cloudformation import-stacks-to-stack-set \  
  --stack-set-name ServiceManagedStackSet \  
  --stack-ids-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/file-  
name.json \  
  --organizational-unit-ids ou-examplerootid111-exampleouid111
```

Note

L'operazione `import-stacks-to-stack-sets` richiede di specificare almeno un ID unità organizzativa (ID UO) in modo che possa associare lo stack importato a quella particolare unità organizzativa. Questa operazione non crea istanze stack per altri account membri nell'area associata. OUs Per aggiornare gli account dei membri associati OUs, usa `create-stack-instances` o `update-stack-instances`

`create-stack-set` crea istanze stack per tutti gli account OUs con un modello fornito dall'utente, dal caricamento diretto o da Amazon S3. AWS CLI Gli esempi seguenti utilizzano l'`create-stack-set` operazione per importare uno stack in uno nuovo. StackSet

- Per utilizzare l'`create-stack-set` operazione, specificate il vostro StackSet nome e importate uno stack in uno appena creato. StackSet

```
aws cloudformation create-stack-set \  
  --template-url https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/file-  
name.json \  
  --permission-model SERVICE_MANAGED \  
  --auto-deployment Enabled=true
```

Ripristina le importazioni di stack in AWS CloudFormation StackSets

Se hai modifiche indesiderate nella tua istanza stack, puoi ripristinare l'importazione dell'istanza stack.

Quando ripristini l'importazione di un'istanza dello stack, CloudFormation elimina l'istanza dello stack ma conserva le risorse dello StackSet stack.

Per annullare un'operazione di importazione dello stack, complete la procedura seguente.

1. Specifica un attributo DeletionPolicy di Retain per ogni risorsa che desideri conservare dopo l'eliminazione dell'istanza di stack. Per ulteriori informazioni, consulta [Ripristino di un'operazione di importazione](#).
2. Elimina le istanze dello stack dal tuo. StackSet Per ulteriori informazioni, consulta [Elimina pile da AWS CloudFormation StackSets](#).
3. Elimina il tuo. StackSet Per ulteriori informazioni, consulta [Eliminare AWS CloudFormation StackSets](#).

Procedure consigliate per l'utilizzo AWS CloudFormation StackSets

Questa sezione descrive le migliori pratiche per definire un StackSet modello, creare o aggiungere pile a un StackSet o aggiornare un. StackSet

Se non lo conosci CloudFormation, consulta l'[CloudFormation migliori pratiche](#) argomento per ulteriori consigli che possono aiutarti a utilizzare in modo CloudFormation più efficace e sicuro.

Argomenti

- [Definizione del modello](#)
- [Creare o aggiungere pile a StackSet](#)
- [Aggiornamento degli stack in un StackSet](#)

Definizione del modello

- Definisci il modello da standardizzare in più account, in diverse Regioni.
- Durante la creazione del modello, accertati che le risorse globali (ad esempio ruoli IAM e bucket Amazon S3) non dispongano di conflitti di denominazione quando vengono create in più Regioni nell'ambito di uno stesso account.
- A StackSet ha un unico modello e set di parametri. Lo stesso stack viene creato in tutti gli account associati a StackSet. Durante la creazione dei modelli, rendili abbastanza dettagliati da consentire un buon equilibrio tra controllo e standardizzazione.
- Ti consigliamo di archiviare il modello in un bucket Amazon S3.

Creare o aggiungere pile a StackSet

- Verifica che l'aggiunta di istanze stack agli stack iniziali StackSet funzioni prima di aggiungere un numero maggiore di istanze stack al tuo. StackSet
- Scegli le opzioni di distribuzione (rollout) più adatte al tuo caso d'uso.
 - Per una distribuzione più restrittiva, imposta Maximum Concurrent Accounts (Numero massimo di account simultanei) su 1 e Failure tolerance (Tolleranza di errore) su 0. Imposta per prima la Regione con l'impatto minore nell'elenco Region Order (Ordine Regioni). Inizia con una Regione.
 - Per una distribuzione più rapida, aumenta i valori di Maximum Concurrent Accounts (Numero massimo di account simultanei) e Failure Tolerance (Tolleranza di errore) in base alle esigenze.
- Le operazioni StackSets dipendono dal numero di istanze dello stack coinvolte e possono richiedere molto tempo.

Aggiornamento degli stack in un StackSet

- Per impostazione predefinita, l'aggiornamento di un aggiornamento StackSet aggiorna tutte le istanze dello stack. Se disponi di 20 account ciascuno in due regioni, avrai a disposizione 40 istanze stack e tutte verranno aggiornate quando aggiorni la. StackSet

Poiché StackSets con un numero elevato di istanze stack, ti consigliamo di testare la versione aggiornata di un modello, di aggiornare selettivamente le istanze dello stack in alcuni account di test prima di aggiornare tutte le istanze dello stack.

- Per avere un controllo più granulare sull'aggiornamento dei singoli stack all'interno del tuo, pianifica di crearne più di uno. StackSet StackSets

- L'aggiornamento di uno StackSet che contiene un numero elevato di stack può richiedere molto tempo. In questa versione, è consentita una sola operazione alla volta su a StackSet. Pianifica gli aggiornamenti in modo da non essere bloccato dall'esecuzione di altre operazioni su StackSet.

AWS CloudFormation StackSets modelli di esempio

Questa sezione include collegamenti ad alcuni CloudFormation modelli di esempio che possono essere utilizzati AWS CloudFormation StackSets in azienda. I modelli elencati in questa sezione abilitano [AWS CloudTrail](#) o [AWS Config](#) e le relative regole.

Important

Come best practice di sicurezza per consentire l' AWS Config accesso a un bucket Amazon S3, consigliamo vivamente di limitare l'accesso nella policy del bucket con la condizione. `AWS:SourceAccount` I nuovi modelli vengono aggiornati per includere `AWS:SourceAccount`. Se la tua policy sui bucket esistente non segue questa best practice di sicurezza, ti consigliamo vivamente di modificarla per includere questa protezione. In questo modo AWS Config viene garantito l'accesso solo per conto degli utenti previsti.

Descrizione	Collegamento S3
Abilita AWS CloudTrail	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/AbilitaAWSCloudtrail .yml
Abilita AWS Config	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/AbilitaAWSConfig .yml
Abilita AWS Config con registrazione centralizzata	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/Abilita .yml AWSConfig ForOrganizations
Abilita le policy predefinite di Amazon Data Lifecycle Manager in un' AWS organizzazione o tra account specifici AWS	• Policy predefinita per le istantanee EBS: .yaml https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/AbilitaAWSConfigForOrganizations .yml

Descrizione	Collegamento S3
	east-1/ DataLifecycleManager EBSSnapshot DefaultPolicy Politica predefinita per EBS-backed — Policy.yaml AMIs https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ DataLifecycleManager AMIDefault https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ConfigRuleEncryptedVolumes.yml
Configura una AWS Config regola per determinare se CloudTrail è abilitata	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ConfigRuleCloudtrailEnabled.yml
Configurare una AWS Config regola per determinare se l'MFA root è abilitata	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ConfigRuleRootAccountMFAEnabled.yml
Configura una AWS Config regola per determinare se EIPs sono allegati	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ConfigRuleEipAttached.yml
Configura una AWS Config regola per determinare se i volumi EBS sono crittografati	https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/ConfigRuleEncryptedVolumes.yml

Risoluzione dei problemi AWS CloudFormation StackSets

Questo argomento contiene alcuni StackSets problemi comuni e le relative soluzioni suggerite.

Argomenti

- [Motivi comuni per operazioni di stack non riuscite](#)
- [Nuovo tentativo di operazioni di creazione o aggiornamento d stack non riuscite](#)

- [L'eliminazione dell'istanza di stack non riesce](#)
- [L'operazione di importazione di stack ha esito negativo](#)
- [Numero di errori delle istanze dello stack per le operazioni StackSets](#)

Motivi comuni per operazioni di stack non riuscite

Problema: un'operazione di stack non è riuscita e lo stato dell'istanza di stack è OUTDATED.

Causa: esistono diverse cause comuni per le operazioni di stack non riuscite.

- Autorizzazioni insufficienti in un account target per la creazione delle risorse specificate nel modello.
- Il CloudFormation modello potrebbe contenere errori. Convalida il modello CloudFormation e correggi gli errori prima di provare a creare il tuo StackSet.
- È possibile che il modello stia provando a creare le risorse globali che devono essere univoche, ma non lo sono, ad esempio i bucket S3.
- Non esiste un numero di account target specificato. Controlla i numeri di account target specificati nella pagina Set deployment options (Imposta opzioni di distribuzione) della procedura guidata.
- L'account amministratore non ha una relazione di trust con l'account target.
- Nell'account target è già presente il numero massimo di una risorsa specificato nel modello. Ad esempio, è possibile che sia stato raggiunto il limite di ruoli IAM consentiti in un account target, ma il modello crea un numero maggiore di ruoli IAM.
- Hai raggiunto il numero massimo di pile consentite in a. StackSet Per il numero massimo di pile per pila StackSet, vedi. [Comprendi le CloudFormation quote](#)

Soluzione: per ulteriori informazioni sulle autorizzazioni richieste agli account di destinazione e amministratore prima di poter creare StackSets, consulta. [Concedi a tutti gli utenti dell'account amministratore le autorizzazioni per gestire gli stack in tutti gli account di destinazione](#)

Nuovo tentativo di operazioni di creazione o aggiornamento d stack non riuscite

Problema: un'operazione di creazione o aggiornamento di stack non è riuscita e lo stato dell'istanza di stack è OUTDATED. Per risolvere il motivo per cui la creazione o l'aggiornamento di uno stack non sono riusciti, apri la CloudFormation console e visualizza gli eventi dello stack, che avrà lo

stato di (in caso di operazioni di creazione non riuscite) o DELETED FAILED (in caso di operazioni di aggiornamento non riuscite). Sfogliare gli eventi di stack e individuare la colonna Status reason (Motivo dello stato). Il valore di Status reason (Motivo dello stato) spiega perché l'operazione dello stack non è riuscita.

Dopo aver corretto la causa alla base dell'errore di creazione dello stack e si è pronti per riprovare, eseguire la procedura riportata di seguito.

Soluzione: eseguire la procedura seguente per riprovare l'operazione di stack.

1. Nella console, seleziona StackSet quello che contiene lo stack in cui l'operazione non è riuscita.
2. Nel menu Azioni, scegli Modifica StackSet dettagli per riprovare a creare o aggiornare gli stack.
3. Nella pagina Specify template (Specifica modello), per utilizzare lo stesso modello CloudFormation, mantenere l'opzione predefinita Use current template (Utilizza modello corrente). Se l'operazione di stack non è riuscita perché il modello richiedeva modifiche e si desidera caricare un modello aggiornato, scegliere invece Upload a template to Amazon S3 (Carica un modello in Amazon S3), quindi selezionare Browse (Sfoglia) per selezionare il modello aggiornato. Dopo aver caricato il modello aggiornato, scegliere Next (Avanti).
4. Nella pagina Specificare i dettagli dello stack, se non state modificando alcun parametro specifico del modello, scegliete Avanti.
5. Nella pagina Set deployment options (Imposta opzioni di distribuzione), se si desidera, modificare le impostazioni predefinite per Maximum concurrent accounts (Numero massimo di account simultanei) e Failure tolerance (Tolleranza ai guasti). Per ulteriori informazioni su queste impostazioni, consultare [StackSet opzioni operative](#).
6. Nella pagina Review (Revisione) rivedere le selezioni e indicare con un segno di spunta di aver preso visione delle funzionalità IAM richieste. Scegli Invia.
7. Se lo stack non viene aggiornato, ripetere questa procedura dopo aver risolto eventuali problemi sottostanti che impediscono di creare lo stack.

L'eliminazione dell'istanza di stack non riesce

Problema: non è stato possibile eliminare uno stack.

Causa: non è possibile eliminare gli stack per cui è stata abilitata la protezione da cessazione.

Soluzione: verificare se per lo stack è stata abilitata la protezione da cessazione. In caso affermativo, disabilitare la protezione da cessazione, quindi eseguire nuovamente l'eliminazione dell'istanza dello stack.

L'operazione di importazione di stack ha esito negativo

Problema: un'operazione di importazione degli stack non riesce a importare gli stack esistenti in nuovi o esistenti. StackSets L'istanza di stack si trova in uno stato INOPERABLE.

Soluzione: ripristinare l'operazione di importazione di stack, completando le seguenti attività.

1. Usa l' `StackSets` opzione `Delete Stacks from` e abilitala `Retain Stacks durante` la configurazione, quindi procedi con l'eliminazione delle istanze dello stack dal tuo `StackSet`. Per ulteriori informazioni, per ulteriori informazioni, vedere. [Elimina pile da AWS CloudFormation StackSets](#)
2. Vedrai che le istanze dello stack `StackSet` vengono aggiornate per rimuovere l'istanza dello `INOPERABLE` stack.
3. Correggi le istanze dello stack in base all'errore di importazione non riuscita e riprova l'operazione di importazione dello stack.

Numero di errori delle istanze dello stack per le operazioni StackSets

Il numero degli errori delle istanze di stack ti avvisa se le istanze di stack non vengono fornite o aggiornate. Queste istanze di stack non sono state implementate a causa di uno o più motivi di seguito indicati:

- Risorse esistenti con una configurazione simile
- Dipendenze mancanti, come i ruoli AWS Identity and Access Management (IAM)
- Altri fattori in conflitto

Per l'implementazione con la massima simultaneità, il numero massimo di simultaneità è maggiore di almeno un'unità rispetto al numero di tolleranze di errori. Ad esempio, se il numero di tolleranze di errori è 9, il numero massimo di simultaneità non può essere superiore a 10. In tal modo, l'operazione restituisce `SUCCEEDED` anche se alcune istanze di stack non vengono aggiornate. Il nuovo numero degli errori delle istanze di stack consente di determinare se l'operazione è riuscita solo in maniera condizionale poiché il numero di tolleranze di errori è impostato per consentire tutti gli errori.

Puoi utilizzare l' AWS Management Console AWS SDK o ottenere il conteggio degli errori e AWS CLI filtrare le istanze dello stack per determinare quali istanze devono essere ridistribuite.

Utilizzo della console

Per visualizzare il numero di istanze di stack non riuscite:

1. [Apri la console e scegli. CloudFormation StackSets](#)
2. Scegli il tuo StackSet, quindi scegli la scheda Operazioni.
3. Scegli uno stato nella colonna Stato per visualizzare i dettagli dello stato. Troverai il numero di istanze di stack non riuscite per un'operazione particolare nei dettagli dello stato.

Per visualizzare l'account, la regione e lo stato delle istanze di stack per l'operazione:

1. Nei dettagli dello stato, scegli il numero di istanze di stack non riuscite. Esempio: Istanze di stack: **<number of failed stack instances>**.
2. Espandi il pannello laterale scegliendo l'intestazione del pannello. I risultati nel pannello laterale sono gli stati delle istanze di stack dopo il completamento dell'operazione selezionata.

Per visualizzare i dettagli dell'istanza di stack corrente per un'operazione:

1. Scegli la scheda Istanze stack.
2. Filtra per ID ultima operazione. I risultati sono gli stati correnti e i relativi motivi dall'ultima operazione di modifica dell'istanza. Puoi utilizzare questo filtro in combinazione con Account AWS , Regione AWS , Stato dettagliato e Stato deviazione per restringere ulteriormente i risultati della ricerca.

Utilizzando il AWS CLI

Per ottenere il numero di istanze di stack non riuscite, richiama `describe-stack-set-operation` o `list-stack-set-operations` e consulta `StatusDetails`.

```
aws cloudformation describe-stack-set-operation --stack-set-name ss1 \  
--operation-id 5550e62f-c822-4331-88fa-21c1d7bafc60
```

```
{
```

```

    "StackSetOperation": {
      "OperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60",
      "StackSetId": "ss1:9101ca57-49fc-4a61-a5a6-4c97b8adb08f",
      "Action": "CREATE",
      "Status": "SUCCEEDED",
      "OperationPreferences": {
        "RegionOrder": [],
        "FailureToleranceCount": 10,
        "MaxConcurrentCount": 10
      },
      "AdministrationRoleARN": "arn:aws:iam::123456789012:role/AWSCloudFormationStackSetAdministrationRole",
      "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole",
      "CreationTimestamp": "2022-10-26T17:18:53.947000+00:00",
      "EndTimestamp": "2022-10-26T17:19:35.304000+00:00",
      "StatusDetails": {
        "FailedStackInstancesCount": 3
      }
    }
  }
}

```

```
aws cloudformation list-stack-set-operations --stack-set-name ss1
```

```

{
  "Summaries": [
    {
      "OperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60",
      "Action": "CREATE",
      "Status": "SUCCEEDED",
      "CreationTimestamp": "2022-10-26T17:18:53.947000+00:00",
      "EndTimestamp": "2022-10-26T17:19:35.304000+00:00",
      "StatusDetails": {
        "FailedStackInstancesCount": 3
      },
      "OperationPreferences": {
        "RegionOrder": [],
        "FailureToleranceCount": 10,
        "MaxConcurrentCount": 10
      }
    }
  ]
}

```

Per ottenere una panoramica cronologica di una particolare operazione, usa `list-stack-set-operation-results` per visualizzare lo stato e il relativo motivo per ogni istanza di stack dopo il completamento dell'operazione. Consulta l'esempio seguente per trovare `Status` e `StatusReason`.

```
aws cloudformation list-stack-set-operation-results --stack-set-name ss1 \
  --operation-id 5550e62f-c822-4331-88fa-21c1d7bafc60 --
  filters Name=OPERATION_RESULT_STATUS,Values=FAILED
```

```
{
  "Summaries": [
    {
      "Account": "123456789012",
      "Region": "us-west-2",
      "Status": "FAILED",
      "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
      "AccountGateResult": {
        "Status": "SKIPPED",
        "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'."
      },
      "OrganizationalUnitId": ""
    },
    {
      "Account": "123456789012",
      "Region": "us-west-1",
      "Status": "FAILED",
      "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
      "AccountGateResult": {
        "Status": "SKIPPED",
        "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'."
      },
      "OrganizationalUnitId": ""
    },
    {
      "Account": "123456789012",
      "Region": "us-east-1",
```

```

        "Status": "FAILED",
        "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
        "AccountGateResult": {
            "Status": "SKIPPED",
            "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'."
        },
        "OrganizationalUnitId": ""
    }
]
}

```

Usa `list-stack-instances` con i filtri `DETAILED_STATUS` e `LAST_OPERATION_ID` per ottenere un elenco di istanze di stack non riuscite nell'ultima operazione che ha tentato l'implementazione dell'istanza di stack. Consulta il contrassegno `--filters` nell'esempio con `DETAILED_STATUS` e `LAST_OPERATION_ID`:

```

aws cloudformation list-stack-instances --stack-set-name ss1 \
  --filters Name=DETAILED_STATUS,Values=FAILED Name=LAST_OPERATION_ID,Values=5550e62f-
c822-4331-88fa-21c1d7bafc60

```

```

{
  "Summaries": [
    {
      "StackSetId": "ss1:9101ca57-49fc-4a61-a5a6-4c97b8adb08f",
      "Region": "us-east-1",
      "Account": "123456789012",
      "Status": "OUTDATED",
      "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
      "StackInstanceStatus": {
        "DetailedStatus": "FAILED"
      },
      "OrganizationalUnitId": "",
      "DriftStatus": "NOT_CHECKED",
      "LastOperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60"
    },
    {

```



```

        "StackSetId": "ss1:9101ca57-49fc-4a61-a5a6-4c97b8adb08f",
        "Region": "us-west-1",
        "Account": "123456789012",
        "Status": "OUTDATED",
        "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
        "StackInstanceStatus": {
            "DetailedStatus": "FAILED"
        },
        "OrganizationalUnitId": "",
        "DriftStatus": "NOT_CHECKED",
        "LastOperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60"
    },
    {
        "StackSetId": "ss1:9101ca57-49fc-4a61-a5a6-4c97b8adb08f",
        "Region": "us-west-2",
        "Account": "123456789012",
        "Status": "OUTDATED",
        "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
        "StackInstanceStatus": {
            "DetailedStatus": "FAILED"
        },
        "OrganizationalUnitId": "",
        "DriftStatus": "NOT_CHECKED",
        "LastOperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60"
    }
]
}

```

Per individuare l'ID dell'ultima operazione per modificare un'istanza di stack, usa `list-stack-instances` o `describe-stack-instance` per ottenere `LastOperationId`:

```

aws cloudformation describe-stack-instance --stack-set-name ss1 \
  --stack-instance-account 123456789012 --stack-instance-region us-east-2

```

```

{
  "StackInstance": {
    "StackSetId": "ss1:9101ca57-49fc-4a61-a5a6-4c97b8adb08f",
    "Region": "us-west-2",
    "Account": "123456789012",

```

```
    "ParameterOverrides": [],
    "Status": "OUTDATED",
    "StackInstanceStatus": {
      "DetailedStatus": "FAILED"
    },
    "StatusReason": "Account 123456789012 should have
'AWSCloudFormationStackSetExecutionRole' role with trust relationship to Role
'AWSCloudFormationStackSetAdministrationRole'.",
    "OrganizationalUnitId": "",
    "DriftStatus": "NOT_CHECKED",
    "LastOperationId": "5550e62f-c822-4331-88fa-21c1d7bafc60"
  }
}
```

Sincronizzazione degli stack con il codice sorgente archiviato in un repository Git con Git sync

Con Git sync, puoi gestire i tuoi CloudFormation stack con il controllo del codice sorgente. Puoi farlo configurando CloudFormation per monitorare un repository Git. Il repository viene monitorato per rilevare eventuali modifiche a due file:

- Un file CloudFormation modello che definisce uno stack
- Un file di implementazione dello stack che contiene i parametri per la configurazione dello stack

Con Git sync, puoi utilizzare le pull request e il monitoraggio delle versioni per configurare, distribuire e aggiornare i tuoi CloudFormation stack da una posizione centralizzata. Quando esegui modifiche al modello o al file di distribuzione, aggiorna CloudFormation automaticamente lo stack. Se utilizzi le richieste pull, CloudFormation puoi lasciare un commento sulla richiesta pull spiegando quali modifiche verranno apportate al tuo stack prima di aggiornarlo effettivamente. Tuttavia, è necessario prima abilitare questa funzionalità.

Git sync fornisce un'interfaccia console che puoi usare per collegarti a un repository, generare un file di distribuzione dello stack, aggiornare un CloudFormation modello e inviare una richiesta pull al tuo repository. La sincronizzazione Git presenta anche una dashboard di stato attraverso la quale puoi monitorare e modificare le implementazioni attive dello stack di sincronizzazione Git, nonché risolvere eventuali problemi. La sincronizzazione Git è accessibile tramite la [CloudFormation console](#) quando [crei uno stack](#). Puoi anche accedere a Git sync usando CodeConnections. Per ulteriori informazioni, consulta [Lavorare con le configurazioni di sincronizzazione per gli archivi collegati](#) nella Guida per l'utente della console Developer Tools.

Git sync supporta [GitHub Enterprise](#), [GitHubGitLab](#), [Bitbucket](#) e repository [GitLab autogestiti](#).

Note

La sincronizzazione Git è disponibile nelle Regioni seguenti: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon), Canada (Centrale), Asia Pacifico (Mumbai), Asia Pacifico (Tokyo), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Europa (Irlanda), Europa (Londra), Europa (Parigi), Europa (Stoccolma), Europa (Francoforte), Europa (Milano) e Sud America (San Paolo).

Per informazioni sull'utilizzo di Git sync con una strategia multi-account, consulta il seguente post sul blog [Use AWS CloudFormation Git sync per configurare le risorse negli account dei clienti](#).

Argomenti

- [Come funziona Git sync con CloudFormation](#)
- [Prerequisiti per sincronizzare gli stack con un repository Git utilizzando Git sync](#)
- [Crea uno stack dal codice sorgente del repository con Git sync](#)
- [Abilita CloudFormation la pubblicazione di un riepilogo delle modifiche allo stack nelle richieste pull](#)
- [Pannello di controllo dello stato di sincronizzazione Git](#)

Come funziona Git sync con CloudFormation

Questo argomento descrive come funziona Git sync e introduce i concetti chiave necessari per utilizzarlo.

Argomenti

- [Come funziona la sincronizzazione Git](#)
- [Commenti sulle richieste pull](#)
- [File di implementazione dello stack](#)
- [CloudFormation file modello](#)
- [Repository delle definizioni dei modelli](#)

Come funziona la sincronizzazione Git

Per utilizzare Git sync, devi prima connettere un provider Git all' CloudFormation utilizzo del [CodeConnections](#) servizio. Nelle procedure di questa guida, la connessione viene creata tramite la CodeConnections console. In alternativa, è possibile creare la connessione con AWS CLI. Puoi utilizzare uno dei seguenti provider Git:

- [GitHub](#)
- [GitHub Impresa](#)
- [GitLab](#)
- [Bitbucket](#)
- [GitLabautogestita](#)

Successivamente, crei un CloudFormation modello che definisca il tuo stack e lo aggiungi al tuo repository. Questo file modello viene monitorato. CloudFormation aggiorna automaticamente lo stack quando vengono apportate modifiche.

Nella CloudFormation console, crei un nuovo stack e scegli Sincronizza da Git per indicare di CloudFormation usare Git sync. Specificherai il repository e il ramo che desideri CloudFormation monitorare e specificherai il CloudFormation modello nel tuo repository che definisce lo stack.

Durante la configurazione, puoi fornire il tuo file di implementazione dello stack dal repository o fare in modo che la sincronizzazione Git ne generi uno per te. Il file di implementazione dello stack contiene parametri e valori che configurano le risorse dello stack. Questo file di distribuzione dello stack viene monitorato. CloudFormation aggiorna automaticamente lo stack quando vengono apportate modifiche allo stack.

Git sync crea una richiesta pull nel tuo repository per sincronizzare lo stack con il file CloudFormation modello e il file di distribuzione dello stack. Il file di implementazione dello stack viene inviato al tuo repository dalla sincronizzazione Git se quest'ultima lo genera al posto tuo.

Quindi unisci la pull request al tuo repository in modo da effettuare il CloudFormation provisioning dello stack, configurarlo con i parametri di distribuzione e iniziare a monitorare il repository per rilevare eventuali modifiche.

Da quel momento in poi, ogni volta che apporti modifiche al tuo file modello o al file di distribuzione dello stack e le esegui nel tuo repository, rileverà automaticamente le modifiche. CloudFormation Se il tuo team utilizza le richieste pull, i membri del team possono quindi rivedere e approvare le modifiche prima che vengano implementate. Una volta accettata la pull request, CloudFormation distribuisce le modifiche.

Puoi monitorare lo stato della configurazione di sincronizzazione Git per lo stack e vedere una cronologia dei commit applicati allo stack nella console. CloudFormation La console fornisce anche strumenti per la riconfigurazione della sincronizzazione Git e la risoluzione dei problemi.

Commenti sulle richieste pull

Puoi scegliere di CloudFormation creare un riepilogo delle modifiche al codice nelle richieste pull tramite il CodeConnections servizio attivando l'opzione Abilita commento sulla pull request nella console. Fornire un riepilogo delle modifiche nelle pull request significa che i membri del team possono facilmente esaminare e comprendere l'impatto delle modifiche proposte prima di unire la pull request. Per ulteriori informazioni, consulta [Abilita CloudFormation la pubblicazione di un riepilogo delle modifiche allo stack nelle richieste pull](#).

File di implementazione dello stack

Un file di distribuzione dello stack è un file in formato standard JSON (JavaScript Object Notation) o YAML che contiene parametri e valori che gestiscono lo stack. CloudFormation Viene monitorato per rilevare eventuali modifiche. Quando viene eseguito il commit delle modifiche al file nel repository, lo stack associato viene aggiornato automaticamente.

Il file di implementazione dello stack contiene una coppia chiave-valore e due dizionari:

- `template-file-path`

Questo è il percorso completo del repository per il file modello. CloudFormation Il file modello dichiara le risorse per lo CloudFormation stack associato a questo file di distribuzione.

- `parameters`

Il dizionario dei parametri contiene coppie chiave-valore che configurano le risorse nello stack. Un file di implementazione dello stack può avere fino a 50 parametri.

- `tags`

Il dizionario dei tag contiene coppie chiave-valore facoltative che puoi utilizzare per identificare e classificare le risorse nello stack. Un file di implementazione dello stack può avere fino a 50 tag.

Puoi fornire il tuo file di implementazione dello stack o fare in modo che la sincronizzazione Git ne crei uno per te e invii automaticamente una richiesta pull al repository. Puoi gestire i parametri e i tag modificando il file di implementazione dello stack ed eseguendo il commit delle modifiche al repository.

Di seguito è riportato l'esempio di un file di implementazione dello stack della sincronizzazione Git:

```
template-file-path: fargate-srvs/my-stack-template.yaml

parameters:
  image: public.ecr.aws/lts/nginx:latest
  task_size: x-small
  max_capacity: 5
  port: 8080
  env: production
tags:
  cost-center: '123456'
  org: 'AWS'
```

CloudFormation file modello

Un file modello contiene una dichiarazione delle AWS risorse che compongono uno CloudFormation stack. Con la sincronizzazione Git, il file di modello a cui il file di implementazione dello stack fa riferimento viene archiviato nel repository Git. Puoi gestire lo stack modificando il file di modello ed eseguendo il commit delle modifiche al repository.

Per ulteriori informazioni, consulta [Lavorare con i CloudFormation modelli](#).

Repository delle definizioni dei modelli

Il repository delle definizioni dei modelli è il repository Git a cui è collegato tramite CloudFormation Git sync. Il repository viene monitorato per rilevare eventuali modifiche al CloudFormation modello e al file di distribuzione dello stack. Quando esegui il commit delle modifiche al file, lo stack associato viene aggiornato automaticamente.

Important

Quando configuri il repository delle definizioni dei modelli nella console della sincronizzazione Git, seleziona il repository e il ramo corretti dalla connessione Git. Git sync monitora solo il repository e il ramo configurati per le modifiche al CloudFormation modello e al file di distribuzione dello stack.

Prerequisiti per sincronizzare gli stack con un repository Git utilizzando Git sync

Prima di sincronizzare uno CloudFormation stack con il tuo repository Git, verifica che siano soddisfatti i seguenti requisiti.

Argomenti

- [Repository Git](#)
- [CloudFormation modello](#)
- [Ruolo IAM](#)
- [Autorizzazioni richieste](#)
- [Policy di attendibilità](#)

Repository Git

È necessario disporre di un repository Git ospitato su una delle seguenti piattaforme:

- [GitHub](#)
- [GitHub Enterprise](#)
- [GitLab](#)
- [Bitbucket](#)
- [GitLabautogestita](#)

Il repository può essere pubblico o privato. Dovrai connettere questo repository Git CloudFormation tramite la [console Connections](#).

CloudFormation modello

Il tuo repository Git deve contenere un [file CloudFormation modello](#) archiviato nel ramo a cui intendi connetterti con Git sync. A questo modello farà riferimento il file di distribuzione dello [stack](#).

Ruolo IAM

La sincronizzazione Git richiede un ruolo IAM. Puoi scegliere di creare un ruolo IAM per il tuo stack quando configuri Git sync, oppure puoi usare un ruolo esistente.

Note

Un ruolo IAM generato automaticamente applica le autorizzazioni solo allo stack per il quale viene generato. Per riutilizzare un ruolo IAM generato automaticamente, devi modificare il ruolo per il nuovo stack.

Autorizzazioni richieste

Il ruolo IAM fornito per la sincronizzazione Git richiede le seguenti autorizzazioni:

- [cloudformation:CreateChangeSet](#)
- [cloudformation>DeleteChangeSet](#)

- [cloudformation:DescribeChangeSet](#)
- [cloudformation:DescribeStackEvents](#)
- [cloudformation:DescribeStacks](#)
- [cloudformation:ExecuteChangeSet](#)
- [cloudformation:ListChangeSets](#)
- [cloudformation:ValidateTemplate](#)
- [events:PutRule](#)
- [events:PutTargets](#)

 Note

Le precedenti autorizzazioni richieste vengono aggiunte automaticamente ai ruoli IAM generati dalla sincronizzazione Git.

Il seguente esempio di ruolo IAM include le autorizzazioni di prerequisito necessarie per la sincronizzazione Git.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SyncToCloudFormation",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate"
      ],
      "Resource": "*"
    },
  ],
}
```

```
{
  "Sid": "PolicyForManagedRules",
  "Effect": "Allow",
  "Action": [
    "events:PutRule",
    "events:PutTargets"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "events:ManagedBy":
["cloudformation.sync.codeconnections.amazonaws.com"]
    }
  },
  {
    "Sid": "PolicyForDescribingRule",
    "Effect": "Allow",
    "Action": "events:DescribeRule",
    "Resource": "*"
  }
}
```

Policy di attendibilità

La seguente policy di attendibilità è necessaria per consentire alla sincronizzazione Git di connettersi al repository Git:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CfnGitSyncTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudformation.sync.codeconnections.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Crea uno stack dal codice sorgente del repository con Git sync

Questo argomento spiega come creare uno CloudFormation stack che si sincronizzi con un repository Git con Git sync.

Important

Prima di continuare, completa tutti i [prerequisiti indicati](#) nella sezione precedente.

Crea uno stack dal codice sorgente del repository

1. [Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformazione.](https://console.aws.amazon.com/cloudformazione)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli in cui Regione AWS creare lo stack.
3. Nella pagina Pile, scegli Crea pila, quindi scegli Con nuove risorse (standard).
4. Nella pagina Create stack (Crea stack), esegui le operazioni seguenti:
 - a. Per Prerequisito: prepara il modello, mantieni selezionata l'opzione Scegli un modello esistente.
 - b. Per Specificare modello, scegli Sincronizza da Git, quindi scegli Avanti.
5. Nella pagina Specificare i dettagli dello stack, in Nome dello stack, digita un nome per lo stack. Il nome dello stack può includere lettere (A-Z o a-z), numeri (0-9) e trattini (-).
6. Per il file di distribuzione Stack, Creazione del file di distribuzione:
 - Se non hai creato un file di distribuzione dello stack e non lo hai aggiunto al tuo repository, scegli Crea il file utilizzando i seguenti parametri e inseriscilo nel mio repository.
 - Se hai un file di distribuzione dello stack nel tuo repository, scegli Sto fornendo il mio file nel mio repository.
7. Per Template definition repository, scegli Scegli un repository Git collegato per scegliere un repository Git già collegato oppure Collega un repository Git per collegarne uno nuovo. CloudFormation Se scegli Collega un repository Git, procedi come segue:
 - a. Per Select repository provider, scegli una delle seguenti opzioni:
 - GitHub

- GitHub Enterprise Server
 - GitLab
 - Bitbucket
 - GitLab autogestito
- b. Per Connessione, scegli una connessione dall'elenco. Se non viene visualizzata alcuna opzione nell'elenco Connessione, scegli aggiungi una nuova connessione per accedere alla [console Connections](#) e creare una connessione al tuo repository.
8. Nell'elenco Repository, seleziona il repository Git che contiene il tuo file di modello dello stack.
9. Nell'elenco Ramo, seleziona il ramo che la sincronizzazione Git deve monitorare.

 Note

Git sync monitora solo il ramo selezionato per le modifiche al CloudFormation modello e ai file di distribuzione dello stack. Per qualsiasi modifica che desideri apportare al tuo stack è necessario eseguire il commit su questo ramo.

10. Specifica il percorso completo per il Percorso del file di distribuzione, incluso il nome del file di implementazione dello stack dalla radice del ramo del repository.

Se CloudFormation sta generando il file per te, è qui che il file verrà salvato nel tuo repository. Se sei tu a fornire il file, questa sarà la sua posizione nel repository.

11. Aggiungi un ruolo IAM. Il ruolo IAM include le autorizzazioni necessarie per CloudFormation sincronizzare lo stack dal tuo repository Git. Puoi scegliere Nuovo ruolo IAM per generare un nuovo ruolo oppure scegliere il ruolo IAM esistente per selezionare un ruolo esistente dal tuo Account AWS. Se scegli di generare un nuovo ruolo, le autorizzazioni necessarie sono già incluse.
12. Abilita o disattiva i commenti sulla pull request:
- Per inserire le informazioni relative ai CloudFormation post change set nelle pull request for stack updates, tieni attivo l'interruttore Enable comment on pull request.
 - Se disattivi questo interruttore, CloudFormation non descriverà le differenze tra la configurazione corrente dello stack e le modifiche proposte nelle richieste pull quando i file del repository vengono aggiornati.
13. Per il Percorso del file modello, specifica il percorso completo dalla radice del repository per il file del modello di stack.

14. (Facoltativo) Per specificare i parametri dello stack, scegliete Aggiungi parametro, fornite una chiave e un valore per ogni parametro, quindi scegliete Avanti. Per ulteriori informazioni, consulta [File di implementazione dello stack](#).

Ad esempio, per specificare un **port=8080** parametro nel file di distribuzione dello stack, procedi come segue:

- a. Scegli Add parameter (Aggiungi parametro).
 - b. In Chiave, inserire **port**.
 - c. In Valore, specifica **8080**.
15. (Facoltativo) Per specificare gli stack tag, scegliete Aggiungi nuovo tag, fornite una chiave e un valore per ogni tag, quindi scegliete Avanti. Per ulteriori informazioni, consulta [File di implementazione dello stack](#).
16. Scegli Avanti per continuare con Configura opzioni dello stack. Per informazioni sulla configurazione delle opzioni dello stack, consulta [Configurare le opzioni dello stack](#).

Una volta completata la configurazione dello stack, scegli Avanti per continuare.

17. Controlla le impostazioni dello stack e verifica quanto segue:
- Il modello di stack è configurato correttamente e impostato su Sincronizza da Git.
 - Il file di implementazione è configurato correttamente.
 - Il repository delle definizioni dei modelli è configurato correttamente e, in particolare, è selezionato il Repository e il Nome ramo corretto.
 - L'anteprima del file di implementazione è corretta e contiene i parametri e i valori previsti.
18. Scegli Invia per creare lo stack.

Dopo aver scelto Invia, viene creata automaticamente una pull request nel tuo repository Git. Devi unire questa pull request nel tuo repository Git per creare il tuo stack. Dopo aver creato lo stack, CloudFormation monitora il tuo repository Git per rilevare eventuali modifiche.

Aggiorna il tuo stack dal tuo repository Git

Per aggiornare lo stack, apporta le modifiche direttamente al file modello o al file di distribuzione dello stack nel tuo repository Git. Dopo aver eseguito il commit delle modifiche nel ramo monitorato, aggiorna CloudFormation automaticamente lo stack. Se utilizzi le richieste pull, una richiesta pull

viene creata automaticamente nel tuo repository Git prima che lo stack venga aggiornato. Devi unire questa pull request nel tuo repository Git per aggiornare lo stack.

Nella CloudFormation console, puoi selezionare lo stack e scegliere la scheda Git sync per visualizzare informazioni sullo stato dello stack e sugli eventi di sincronizzazione. Per ulteriori informazioni, consulta [Pannello di controllo dello stato di sincronizzazione Git](#).

Abilita CloudFormation la pubblicazione di un riepilogo delle modifiche allo stack nelle richieste pull

Questo argomento mostra come CloudFormation abilitare la pubblicazione di un riepilogo delle modifiche allo stack nelle richieste pull nel tuo repository Git.

Abilitando la funzionalità dei commenti sulle richieste pull, si consente di CloudFormation pubblicare un commento che descrive le differenze tra la configurazione corrente dello stack e le modifiche proposte quando i file del repository vengono aggiornati. Questo commento fornisce un riepilogo delle risorse che verranno aggiunte, modificate o eliminate e consente di eseguire una revisione approfondita del codice prima di unire la pull request.

Per abilitare i commenti sulle richieste pull per un nuovo stack (console)

Quando crei lo stack, nella pagina Specify stack details, sotto Template definition repository, assicurati che l'opzione Abilita commento sulla richiesta pull sia attiva. Questa è l'impostazione predefinita per i nuovi stack.

Per abilitare i commenti sulle richieste pull per uno stack esistente (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli lo stack in Regione AWS cui hai creato lo stack.
3. Nella pagina Stacks, scegli lo stack in esecuzione che desideri aggiornare.
4. Scegli la scheda Git sync, quindi scegli Modifica.
5. Nella pagina Modifica impostazioni di sincronizzazione Git, sotto Template definition repository, attiva l'opzione Abilita commento su pull request.
6. Selezionare Update configuration (Aggiorna configurazione).

Pannello di controllo dello stato di sincronizzazione Git

Per visualizzare lo stato di una distribuzione AWS CloudFormation Git sync, seleziona lo stack nella CloudFormation console e scegli la scheda Git sync.

La scheda Sincronizzazione Git è divisa in due pannelli: Stato della sincronizzazione Git ed Eventi di sincronizzazione più recenti.

Stato della sincronizzazione Git

Il pannello superiore fornisce le seguenti informazioni sulla configurazione della sincronizzazione Git per lo stack.

Repository

Un collegamento al repository connesso alla sincronizzazione Git

Provider di repository

Il nome del provider di repository

Ramo

Il nome del ramo monitorato dalla sincronizzazione Git

Percorso del file di distribuzione

Il percorso completo del file di implementazione dello stack per lo stack in questione

Stato di sincronizzazione del repository

Lo stato dell'operazione di sincronizzazione più recente

Messaggio sullo stato della sincronizzazione del repository

Il messaggio relativo all'operazione di sincronizzazione più recente

Stato della sincronizzazione Git

Lo stato della sincronizzazione Git per lo stack in questione

Stato del provisioning

Lo stato dell'operazione di provisioning

Nella sezione in alto a destra del pannello, utilizza i pulsanti seguenti per modificare o aggiornare la sincronizzazione Git:

- **Modifica:** modifica la configurazione della sincronizzazione Git.
- **Riprova l'ultimo commit:** aggiorna lo stack in base al commit più recente al repository.
- **Disconnetti:** disconnetti la sincronizzazione Git dallo stack.
- **Aggiorna:** aggiorna il pannello di stato della sincronizzazione Git.

Eventi di sincronizzazione più recenti

Il pannello Eventi di sincronizzazione più recenti mostra una tabella dei commit che sono stati eseguiti sullo stack.

È possibile ordinare la tabella utilizzando le frecce presenti nell'intestazione di ogni colonna. La tabella può essere ordinata in ordine crescente o decrescente in base ai seguenti parametri:

- Data
- ID commit
- Evento
- Data
- Tipo di evento

Stati dello stack supportati

La sincronizzazione Git può essere configurata per uno stack solo se quest'ultimo si trova in uno dei seguenti stati supportati:

- `CREATE_COMPLETE`
- `UPDATE_COMPLETE`
- `UPDATE_ROLLBACK_COMPLETE`
- `IMPORT_COMPLETE`
- `IMPORT_ROLLBACK_COMPLETE`

La tabella seguente contiene un elenco completo dei codici di stato dello stack con le relative descrizioni:

Stato dello stack e stato dettagliato opzionale	Descrizione
CREATE_COMPLETE	Creazione di uno o più stack completata.
CREATE_IN_PROGRESS	Creazione di uno o più stack in corso.
CREATE_FAILED	Creazione di uno o più stack non riuscita. Visualizzare gli eventi dello stack per vedere gli eventuali messaggi di errore associati. Le possibili ragioni di una creazione non riuscita includono le autorizzazioni insufficienti per lavorare con tutte le risorse dello stack, i valori dei parametri rifiutati da un AWS servizio o un timeout durante la creazione delle risorse.
DELETE_COMPLETE	Eliminazione di uno o più stack completata. Gli stack eliminati vengono conservati e sono visualizzabili per 90 giorni.
DELETE_FAILED	Eliminazione di uno o più stack non riuscita. Poiché l'eliminazione non è riuscita, è possibile che alcune risorse siano ancora in esecuzione; tuttavia, non è possibile utilizzare o aggiornare lo stack. Eliminare nuovamente lo stack o visualizzare gli eventi dello stack per visualizzare gli eventuali messaggi di errore associati.
DELETE_IN_PROGRESS	Rimozione di uno o più stack in corso.
REVIEW_IN_PROGRESS	Creazione di uno o più stack in corso con un StackId previsto ma senza modelli o risorse.  Important Un stack con questo codice di stato conta fino al raggiungimento del massimo numero possibile di stack.
ROLLBACK_COMPLETE	Rimozione di uno o più stack completata dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita. Lo stack torna allo stato di funzionamento

Stato dello stack e stato dettagliato opzionale	Descrizione
	precedente. Le eventuali risorse che sono state create durante l'operazione di creazione dello stack vengono eliminate. Questo stato esiste solo dopo una creazione stack non riuscita. Indica che tutte le operazioni dallo stack creato parzialmente sono state opportunamente rimosse. In questo stato, è possibile eseguire solo un'operazione di eliminazione.
ROLLBACK_FAILED	Rimozione di uno o più stack non riuscita dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita. Eliminare lo stack o visualizzare gli eventi dello stack per visualizzare gli eventuali messaggi di errore associati.
ROLLBACK_IN_PROGRESS	Rimozione di uno o più stack in corso dopo una creazione stack non riuscita o dopo una creazione stack annullata in maniera esplicita.
UPDATE_COMPLETE	Aggiornamento di uno o più stack completato.
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS	Rimozione in corso di risorse obsolete per uno o più stack dopo un aggiornamento dello stack completato. Per gli aggiornamenti dello stack che richiedono la sostituzione di risorse, CloudFormation crea prima le nuove risorse e poi elimina le vecchie risorse per ridurre eventuali interruzioni dello stack. In questo stato, lo stack è stato aggiornato ed è utilizzabile, ma le vecchie risorse CloudFormation vengono comunque eliminate.
UPDATE_FAILED	Aggiornamento non completato di uno o più stack. Visualizzare gli eventi dello stack per vedere gli eventuali messaggi di errore associati.
UPDATE_IN_PROGRESS	Aggiornamento di uno o più stack in corso.

Stato dello stack e stato dettagliato opzionale	Descrizione
UPDATE_ROLLBACK_COMPLETE	Restituzione di uno o più stack completata in uno stato attivo precedente dopo un aggiornamento stack non riuscito.
UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS	Rimozione in corso di nuove risorse per uno o più stack dopo un aggiornamento dello stack non riuscito. In questo stato, lo stack è stato ripristinato allo stato di funzionamento precedente ed è utilizzabile, ma CloudFormation sta comunque eliminando tutte le nuove risorse create durante l'aggiornamento dello stack.
UPDATE_ROLLBACK_FAILED	Restituzione di uno o più stack non riuscita in uno stato attivo precedente dopo un aggiornamento stack non riuscito. In questo stato, puoi eliminare lo stack o continuare il rollback . Prima che lo stack possa tornare in uno stato attivo, potrebbe essere necessario risolvere gli errori. In alternativa, puoi contattare Supporto per ripristinare lo stack a uno stato utilizzabile.
UPDATE_ROLLBACK_IN_PROGRESS	Restituzione di uno o più stack in corso allo stato attivo precedente dopo un aggiornamento stack non riuscito.
IMPORT_IN_PROGRESS	L'operazione di importazione è attualmente in corso.
IMPORT_COMPLETE	L'operazione di importazione è stata completata correttamente per tutte le risorse nello stack che supportano <code>resource import</code> .
IMPORT_ROLLBACK_IN_PROGRESS	L'importazione verrà ripristinata alla configurazione del modello precedente.
IMPORT_ROLLBACK_FAILED	L'operazione di rollback di importazione non è riuscita per almeno una risorsa nello stack. I risultati saranno disponibili per le risorse importate CloudFormation con successo.

Stato dello stack e stato dettagliato opzionale	Descrizione
IMPORT_ROLLBACK_COMPLETE	Il rollback dell'importazione alla configurazione del modello precedente è riuscita.

Gestione delle estensioni con il CloudFormation registro

Il AWS CloudFormation registro funge da hub centralizzato per la gestione delle estensioni che possono essere integrate nei CloudFormation modelli di Account AWS. Le estensioni includono tipi di risorse, moduli e Hooks di editori AWS e di terze parti, oltre alle estensioni personalizzate dell'utente. Il registro semplifica l'individuazione e il provisioning delle estensioni nei CloudFormation modelli nello stesso modo in cui si utilizzano AWS le risorse fornite.

Questa sezione descrive come utilizzare il CloudFormation registro per attivare estensioni di terze parti nel tuo account, tra cui:

- Attivazione di estensioni pubbliche
- Registrazione e attivazione delle estensioni private

Argomenti

- [Documentazione correlata](#)
- [CloudFormation concetti di registro](#)
- [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#)
- [Usa estensioni pubbliche di terze parti dal CloudFormation registro](#)
- [Usa estensioni private di terze parti che sono state condivise con te](#)
- [Modifica i dati di configurazione per le estensioni nel tuo account](#)
- [Registra i tipi di risorse in AWS Config](#)

Documentazione correlata

Se sei uno sviluppatore interessato a creare estensioni personalizzate, consulta la seguente documentazione:

- [Sviluppo di moduli utilizzando la CloudFormation CLI](#) nella Guida per l'utente dell'interfaccia a CloudFormation riga di comando
- [Creazione di tipi di risorse utilizzando la CloudFormation CLI](#) nella Guida per l'utente dell'interfaccia a riga di CloudFormation comando
- [Sviluppo di hook personalizzati utilizzando la CloudFormation CLI](#) nella Guida per AWS CloudFormation l'utente di Hooks

Inoltre, tutti i tipi di AWS risorse disponibili nel CloudFormation registro possono essere utilizzati con AWS Cloud Control API, con i relativi attributi e proprietà definiti in uno schema JSON standard. Per ulteriori informazioni, consulta la Guida per l'utente dell'[API Cloud Control](#). Quando utilizzi l'API Cloud Control per eseguire operazioni CRUDL (Create, Read, Update, Delete, List) sulle AWS risorse, puoi farlo solo sulle tue AWS risorse. Account AWS

CloudFormation concetti di registro

In questo argomento vengono descritti i concetti chiave che consentono di comprendere e iniziare a utilizzare il CloudFormation registro.

Tipi di estensione

Il CloudFormation registro offre i seguenti tipi di estensione:

Ganci

Gli hook sono controlli di convalida che esaminano gli stack o le risorse specifiche prima di CloudFormation crearli, aggiornarli o eliminarli. Gli hook possono essere richiamati anche durante le operazioni di creazione dei set di modifiche. Forniscono un meccanismo per far rispettare gli standard organizzativi e le migliori pratiche convalidando le configurazioni delle risorse rispetto a requisiti specifici. Se un Hook rileva configurazioni non conformi alla sua logica, può emettere un avviso o fallire il processo di provisioning per impedire l'implementazione di risorse non conformi.

[Per ulteriori informazioni, consulta la Guida per l'utente di Hooks.AWS CloudFormation](#)

Per una documentazione specifica sugli Hooks Guard e Lambda, consulta le seguenti sezioni della Guida per l'utente di AWS CloudFormation Hooks:

- [Guard Hooks](#)
- [Ganci Lambda](#)

Modules

I moduli sono configurazioni di risorse riutilizzabili che possono essere incluse in più modelli di stack. CloudFormation Semplificano la creazione e la manutenzione dei CloudFormation modelli incapsulando configurazioni di risorse complesse o utilizzate di frequente in componenti riutilizzabili. Ciò favorisce la coerenza e la standardizzazione tra le implementazioni dell'infrastruttura dell'organizzazione.

Tipi di risorsa

I tipi di risorse consentono di modellare e automatizzare risorse di terze parti o risorse personalizzate che non sono supportate nativamente da CloudFormation. Sviluppando tipi di risorse, è possibile estendere le funzionalità CloudFormation di fornitura e gestione delle risorse da vari servizi di terze parti.

Estensioni pubbliche

Le estensioni pubbliche sono CloudFormation estensioni pubblicate pubblicamente nel registro per essere utilizzate da tutti Account AWS. Ciò include:

- **AWS estensioni:** le estensioni pubblicate da AWS sono sempre pubbliche e attivate per impostazione predefinita, quindi non devi intraprendere alcuna azione prima di utilizzarle nel tuo account. AWS controlla il controllo delle versioni di queste estensioni, quindi utilizzi sempre l'ultima versione disponibile.
- **Estensioni di terze parti:** queste estensioni sono rese disponibili per l'uso generale da parte di editori diversi da AWS. Per utilizzare un'estensione pubblica di terze parti, devi prima attivarla nel tuo account e nella tua regione.

Estensioni attivate

Il CloudFormation registro specifico Account AWS include tre tipi di estensioni attivate:

- **AWS estensioni:** tutte le estensioni AWS pubbliche vengono attivate automaticamente.
- **Attivate da terze parti:** si tratta di copie locali di estensioni pubbliche di terze parti che hai attivato esplicitamente per il tuo account e la tua regione. Quando attivi un'estensione pubblica di terze parti, ne CloudFormation crea una copia locale nel registro del tuo account. Per ulteriori informazioni, consulta [Usa estensioni pubbliche di terze parti dal CloudFormation registro](#).
- **Registrate privatamente:** si tratta di estensioni private che non sono elencate nel CloudFormation registro pubblico. Queste possono essere estensioni che hai creato tu stesso o condivise con te dalla tua organizzazione o da altre terze parti. Per utilizzare l'estensione privata nell'account, devi prima registrarla. La registrazione dell'estensione carica una copia CloudFormation nel registro del tuo account e la attiva. Per ulteriori informazioni, consulta [Usa estensioni private di terze parti che sono state condivise con te](#).

Utilizzare nel proprio account estensioni registrate privatamente ed estensioni pubbliche attivate da editori terzi è come utilizzarle in un ambiente sandbox. Le estensioni sono gestite con il controllo della versione, quindi il loro comportamento di provisioning è legato a una versione specifica. Di conseguenza, queste estensioni funzionano allo stesso modo delle estensioni pubbliche, rispettando le stesse regole specifiche della versione.

Note

Le estensioni registrate privatamente e le estensioni pubbliche di terze parti attivate possono implementare gestori di eventi che vengono eseguiti durante le operazioni di creazione, lettura, aggiornamento, elenco ed eliminazione. L'utilizzo di queste estensioni negli CloudFormation stack può comportare addebiti sul tuo account, oltre a quelli per le risorse create. Per ulteriori informazioni, consulta [Prezzi di AWS CloudFormation](#).

Visualizza le estensioni disponibili e attivate nel CloudFormation registro

Per visualizzare le estensioni disponibili e attivate nel CloudFormation registro, puoi utilizzare il AWS Management Console o il AWS CLI.

Per visualizzare le estensioni disponibili e attivate (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Dal pannello di navigazione, sotto Registro, scegli la categoria di estensione che desideri visualizzare:
 - Public extensions (Estensioni pubbliche) visualizza le estensioni pubbliche disponibili nell'account.
 1. Per Filtro, Tipo di estensione, scegli il tipo di estensione: Tipi di risorse, Moduli o Hooks.
 2. Per Filter, Publisher, scegli un editore: AWS o Terza parte.
 - Activated extensions (Estensioni attivate) visualizza le estensioni pubbliche e private attivate nell'account.

1. Scegli il tipo di estensione: Resource types (Tipo di risorsa), Modules (Moduli) o Hooks (Hook).
2. Utilizza il menu a discesa Filtro per scegliere ulteriormente le estensioni da visualizzare:
 - AWS— elenca le estensioni pubblicate da AWS. Le estensioni pubblicate da AWS sono attivate per impostazione predefinita.
 - Terze parti: elenca tutte le estensioni pubbliche di editori diversi da quelli AWS che hai attivato in questo account.
 - Registered (Registrate): elenca tutte le estensioni private che hai attivato l'account.
 - Publisher: visualizza tutte le estensioni pubbliche che hai pubblicato utilizzando l'account.
4. Cerca o scegli il nome dell'estensione per visualizzarne i dettagli.

Per visualizzare le estensioni disponibili e attivate (AWS CLI)

Utilizzo dell'[list-types](#) comando.

Usa estensioni pubbliche di terze parti dal CloudFormation registro

Per utilizzare un'estensione pubblica di terze parti nel tuo modello, devi prima attivare l'estensione per l'account e la regione in cui desideri utilizzarla. L'attivazione di un'estensione la rende utilizzabile nelle operazioni stack nell'account e nella regione in cui è attivata.

Quando attivi un'estensione pubblica di terze parti, CloudFormation crea una voce nel registro delle estensioni del tuo account per l'estensione attivata come estensione privata. Ciò consente di impostare tutte le proprietà di configurazione incluse nell'estensione. Le proprietà di configurazione definiscono come l'estensione è configurata per una determinata Account AWS regione.

Oltre a impostare le proprietà di configurazione, puoi anche personalizzare l'estensione nei seguenti modi:

- Specificate il ruolo di esecuzione CloudFormation utilizzato per attivare l'estensione, oltre a configurare la registrazione per l'estensione.
- Specifica se l'estensione viene aggiornata automaticamente quando diventa disponibile una nuova versione secondaria o patch.
- Specificate un alias da utilizzare anziché il nome dell'estensione pubblica di terze parti. In questo modo puoi evitare conflitti di denominazione tra le estensioni di terze parti.

Argomenti

- [Configura un ruolo di esecuzione con autorizzazioni IAM e una policy di fiducia per l'accesso alle estensioni pubbliche](#)
- [Utilizza automaticamente nuove versioni delle estensioni](#)
- [Usa gli alias per fare riferimento alle estensioni](#)
- [AWS CLI Comandi di uso comune per lavorare con le estensioni pubbliche](#)
- [Attiva un'estensione pubblica di terze parti nel tuo account](#)
- [Aggiorna un'estensione pubblica di terze parti nel tuo account](#)
- [Disattiva le estensioni pubbliche di terze parti nel tuo account](#)

Configura un ruolo di esecuzione con autorizzazioni IAM e una policy di fiducia per l'accesso alle estensioni pubbliche

Quando attivi un'estensione pubblica dal CloudFormation registro, puoi fornire un ruolo di esecuzione che fornisce CloudFormation le autorizzazioni necessarie per richiamare quell'estensione nella tua regione. Account AWS

Le autorizzazioni richieste per il ruolo di esecuzione sono definite nella sezione del gestore dello schema di estensione. È necessario creare una policy IAM che conceda le autorizzazioni specifiche necessarie all'estensione e collegarla al ruolo di esecuzione.

Oltre alla politica delle autorizzazioni, il ruolo di esecuzione deve avere anche una politica di fiducia che CloudFormation consenta di assumere il ruolo. Segui le indicazioni in [Creare un ruolo utilizzando politiche di fiducia personalizzate](#) nella Guida per l'utente IAM per creare un ruolo con una politica di fiducia personalizzata.

Relazione di attendibilità

Di seguito sono riportati alcuni esempi di policy di fiducia che è possibile utilizzare.

Facoltativamente, è possibile limitare l'ambito dell'autorizzazione per la prevenzione della confusione tra diversi servizi utilizzando una o più chiavi di contesto delle condizioni globali insieme al Condition campo. Per ulteriori informazioni, consulta [Prevenzione del problema "confused deputy" tra servizi](#).

- Imposta il valore `aws:SourceAccount` sull'ID del tuo account.
- Imposta il `aws:SourceArn` valore sull'ARN dell'estensione.

Esempio di politica di fiducia 1

Di seguito è riportato un esempio di politica di fiducia dei ruoli IAM per un'estensione del tipo di risorsa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resources.cloudformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/Organization-Service-Resource/*"
        }
      }
    }
  ]
}
```

Esempio di politica di fiducia 2

Di seguito è riportato un esempio di politica di fiducia dei ruoli IAM per un'estensione Hook.

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

```
    "Condition":{
      "StringEquals":{
        "aws:SourceAccount":"123456789012"
      },
      "StringLike":{
        "aws:SourceArn":"arn:aws:cloudformation:us-
west-2:123456789012:type/hook/Organization-Service-Hook/*"
      }
    }
  ]
}
```

Utilizza automaticamente nuove versioni delle estensioni

Quando attivi un'estensione, puoi anche specificare il tipo di estensione per utilizzare la versione secondaria più recente. Il tipo di estensione aggiorna la versione secondaria, ogni volta che il publisher rilascia una nuova versione sull'estensione attivata.

Ad esempio, la prossima volta che esegui un'operazione di stack, come la creazione o l'aggiornamento di uno stack, utilizzando un modello che include tale estensione, CloudFormation utilizza la nuova versione secondaria.

L'aggiornamento a una nuova versione di estensione, automatico o manuale, non influisce sulle istanze di estensione di cui è già stato eseguito il provisioning negli stack.

CloudFormation considera gli aggiornamenti delle versioni principali delle estensioni come potenzialmente contenenti modifiche sostanziali e pertanto richiede l'aggiornamento manuale a una nuova versione principale di un'estensione.

Le estensioni pubblicate da AWS sono attivate per impostazione predefinita per tutti gli account e le regioni in cui sono disponibili e utilizzano sempre la versione più recente disponibile in ciascuno Regione AWS di essi.

Important

Poiché sei tu a decidere se e quando le estensioni vengono aggiornate all'ultima versione del tuo account, potresti ritrovarti con versioni diverse della stessa estensione distribuite in account e aree geografiche diversi.

Ciò potrebbe portare a risultati imprevisti quando si utilizza lo stesso modello, contenente l'estensione, in tali account e regioni.

Usa gli alias per fare riferimento alle estensioni

Non puoi attivare più di un'estensione con un determinato nome in una determinata Account AWS regione. Poiché diversi editori possono offrire estensioni pubbliche con lo stesso nome di estensione, CloudFormation consente di specificare un alias per qualsiasi estensione pubblica di terze parti attivata.

Se specifichi un alias per l'estensione, CloudFormation considera l'alias come il nome del tipo di estensione all'interno dell'account e della regione. È necessario utilizzare l'alias per fare riferimento all'estensione nei modelli, nelle chiamate API e nella console. CloudFormation

Gli alias dell'estensione devono essere univoci in un determinato account e Regione. Puoi attivare la stessa risorsa pubblica più volte nello stesso account e nella stessa Regione, utilizzando alias di nomi di tipo diverso.

Important

Sebbene gli alias delle estensioni debbano essere univoci solo in un determinato account e regione, consigliamo vivamente agli utenti di non assegnare lo stesso alias a diverse estensioni pubbliche di terze parti tra account e regioni. Ciò potrebbe portare a risultati imprevisti quando si utilizza un modello che contiene l'alias dell'estensione su più account o regioni.

AWS CLI Comandi di uso comune per lavorare con le estensioni pubbliche

I comandi comunemente usati per lavorare con le estensioni pubbliche includono:

- [activate-type](#) per attivare un modulo o un tipo di risorsa pubblico di terze parti nel tuo account.
- [set-type-configuration](#) per specificare i dati di configurazione per un'estensione nel tuo account e per disabilitare e abilitare gli Hooks.
- [list-types](#) per elencare le estensioni presenti nel tuo account.
- [describe-type](#) per restituire informazioni dettagliate su un'estensione specifica o una versione di estensione specifica, inclusi i dati di configurazione correnti.

- [set-type-default-version](#) per specificare quale versione di un'estensione è la versione predefinita.
- [deactivate-type](#) per disattivare un modulo o un tipo di risorsa pubblico di terze parti precedentemente attivato nel tuo account.

Attiva un'estensione pubblica di terze parti nel tuo account

L'argomento seguente mostra come attivare un'estensione pubblica di terze parti nel tuo account, rendendola utilizzabile nell'account e nella regione in cui è stata attivata.

Note

Prima di continuare, conferma di aver creato quella [Ruolo IAM](#) che utilizzerai con questa estensione.

Argomenti

- [Attiva un'estensione pubblica \(console\)](#)
- [Attiva un'estensione pubblica \(\)AWS CLI](#)

Attiva un'estensione pubblica (console)

Segui i passaggi indicati in questa sezione per utilizzare la console per:

- Attiva un'estensione pubblica di terze parti
- Specificate ulteriori dati di configurazione dell'estensione per il vostro account

Per attivare un'estensione pubblica da utilizzare nel tuo account

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Dal pannello di navigazione, sotto Registro, scegli Estensioni pubbliche.
4. Usa il filtro per scegliere il tipo di estensione e scegli Terze parti. (Le estensioni pubblicate da AWS sono attivate per impostazione predefinita).
5. Scegli l'estensione, quindi scegli Attiva.

Se sono disponibili più versioni di un'estensione, puoi utilizzare il menu Versione per scegliere la versione dell'estensione che desideri attivare. Il valore predefinito è la versione più recente.

6. Per Nome estensione, puoi mantenere selezionata l'opzione Usa default oppure scegliere Ignora default e quindi inserire l'alias del tipo di estensione che desideri utilizzare con questa estensione. L'alias deve seguire il formato consigliato per il tipo di estensione. Per ulteriori informazioni, consulta [Usa gli alias per fare riferimento alle estensioni](#).
7. Se l'estensione che stai attivando è un Hook o un tipo di risorsa, per il ruolo di esecuzione ARN, specifica il ruolo CloudFormation IAM da assumere quando richiami l'estensione. Per ulteriori informazioni, consulta [Configura un ruolo di esecuzione con autorizzazioni IAM e una policy di fiducia per l'accesso alle estensioni pubbliche](#).
8. Per Logging config, specificate le informazioni di configurazione della registrazione per un'estensione, se lo desiderate. Per esempio:

```
{
  "logRoleArn": "arn:aws:iam::account:role/rolename",
  "logGroupName": "log-group-name"
}
```

Le informazioni di configurazione della registrazione non sono obbligatorie, ma sono consigliate ai fini del debug. Per utilizzare la configurazione di registrazione con Hooks, aggiungi la stessa politica di fiducia del ruolo di esecuzione specificato, in modo che il ruolo di log possa scrivere i log nel tuo gruppo di log.

logRoleArne i nomi delle logGroupName chiavi fanno distinzione tra maiuscole e minuscole.

9. Per Controllo delle versioni, Aggiornamenti automatici, scegli come ricevere gli aggiornamenti.
 - On (Attivato): effettua automaticamente l'aggiornamento all'ultima versione secondaria. Le versioni principali vengono aggiornate manualmente.
 - Off (Disattivato): non effettua mai automaticamente l'aggiornamento all'ultima versione. Tutte le versioni vengono aggiornate manualmente.

Per ulteriori informazioni, consulta [Utilizza automaticamente nuove versioni delle estensioni](#).

Se l'estensione richiede una configurazione aggiuntiva, hai la possibilità di specificare i dati di configurazione ora o dopo l'attivazione dell'estensione.

⚠ Important

Se l'estensione che stai attivando è un Hook, questo passaggio è obbligatorio. È necessario specificare `ENABLED` per la proprietà `HookInvocationStatus`. Questa operazione abilita le proprietà dell'Hook definite nella `properties` sezione dello schema di Hook. Per ulteriori informazioni, vedere il [riferimento alla sintassi dello schema di configurazione di Hook nella Guida](#) per l'utente di AWS CloudFormation Hooks.

Per specificare i dati di configurazione

1. Per Configurazione, scegli Configura ora, quindi scegli Attiva estensione.

CloudFormation visualizza la pagina Configura estensione. Per visualizzare lo schema di configurazione corrente per l'estensione, assicurati che View configuration schema (Visualizza schema di configurazione) sia attivato.

2. Nella casella di testo Configurazione JSON, inserisci una stringa JSON che rappresenta i dati di configurazione che desideri specificare per questa estensione. Il codice JSON specificato deve essere convalidato rispetto allo schema di configurazione dell'estensione.
3. Scegli Configura estensione.

Se preferisci configurare l'estensione dopo l'attivazione, puoi saltare questo passaggio e fornire i dati di configurazione in un secondo momento.

1. Per Configurazione, scegli Configura in seguito, quindi scegli Attiva estensione.
2. Dopo l'attivazione dell'estensione, puoi configurarla accedendo all'estensione dalla pagina delle estensioni attivate e fornendo i dati di configurazione.

Attiva un'estensione pubblica (AWS CLI)

Segui la procedura descritta in questa sezione per AWS CLI utilizzare:

- Attivare un'estensione pubblica di terze parti
- Specificare ulteriori dati di configurazione dell'estensione per il vostro account

Attiva gli Hooks pubblici

Attivando Hooks nel tuo account, autorizzi un Hook a utilizzare le autorizzazioni definite dal tuo Account AWS CloudFormation rimuove le autorizzazioni non richieste prima di passare le autorizzazioni all'Hook. CloudFormation consiglia ai clienti o agli utenti di Hook di rivedere le autorizzazioni di Hook e di essere consapevoli delle autorizzazioni a cui sono consentiti gli Hook prima di attivare gli Hook nel proprio account.

Per attivare un Hook pubblico da utilizzare nel tuo account (AWS CLI)

1. Ottieni l'ARN per il tuo Hook e salvalo. Puoi ottenere l'ARN di un Hook usando o. AWS Management Console AWS CLI Per ulteriori informazioni, consulta [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#).

```
export HOOK_TYPE_ARN="arn:aws:cloudformation:us-west-2:123456789012:type/hook/  
Organization-Service-Hook/"
```

2. Utilizzo dell'[set-type-configuration](#) comando per specificare i dati di configurazione. Il JSON richiesto `--configuration` deve essere convalidato rispetto allo schema di configurazione di Hook. Per attivare l'Hook per tutte le operazioni sullo stack, è necessario impostare la `HookInvocationStatus` proprietà su `ENABLED` nella sezione `HookConfiguration`

```
aws cloudformation set-type-configuration \  
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":  
  {"HookInvocationStatus": "ENABLED", "FailureMode": "FAIL", "Properties":{}}}}' \  
  --type-arn $HOOK_TYPE_ARN --region us-west-2
```

Per ulteriori informazioni sulle opzioni di `HookConfiguration` configurazione, vedere il [riferimento alla sintassi dello schema di configurazione di Hook](#) nella Guida per l'utente di AWS CloudFormation Hooks.

Attiva moduli pubblici e tipi di risorse

Per attivare un'estensione pubblica da utilizzare nel tuo account (AWS CLI)

- Utilizzo dell'[activate-type](#) comando per attivare l'estensione e specificare se aggiornare automaticamente l'estensione ogni volta che viene pubblicata una nuova versione secondaria dell'estensione.

L'esempio riportato di seguito specifica il nome della risorsa Amazon (ARN) pubblico di un'estensione pubblica da attivare per l'account. Inoltre, specifica che CloudFormation aggiorna l'estensione ogni volta che viene pubblicata una nuova versione secondaria.

```
aws cloudformation activate-type \  
  --public-type-arn public_extension_ARN \  
  --execution-role-arn arn:aws:iam::123456789012:role/my-execution-role \  
  --auto-update true --region us-west-2
```

Questo comando restituisce un ARN dell'estensione attivata.

```
{  
  "Arn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/My-  
Resource-Example"  
}
```

Aggiorna la versione di un'estensione pubblica (AWS CLI)

Utilizzare [activate-type](#) per attivare nuovamente l'estensione.

Utilizzate l'--version-bump opzione per specificare se aggiornare l'estensione alla MAJOR versione più recente o alla versione più recente MINOR.

```
aws cloudformation activate-type --type RESOURCE \  
  --type-name Example::Test::1234567890abcdef0 \  
  --type-name-alias Example::Test::Alias \  
  --version-bump MAJOR --region us-west-2
```

Aggiorna un'estensione pubblica di terze parti nel tuo account

Dopo aver attivato un'estensione pubblica di terze parti, puoi aggiornare la maggior parte dei dettagli dell'estensione dal tuo account.

Per aggiornare un'estensione pubblica nel tuo account (console)

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS

3. Dal pannello di navigazione, sotto Registro, scegli Estensioni attivate.
4. Trova l'estensione che desideri aggiornare e selezionala. Per ulteriori informazioni, consulta [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#).
5. Dal menu Azioni, scegli Modifica, quindi l'opzione di modifica appropriata:
 - Per aggiornare lo schema di configurazione, vedere [Modifica i dati di configurazione per le estensioni nel tuo account](#).
 - Per attivare o disattivare gli aggiornamenti automatici:
 1. Scegli Modifica aggiornamenti automatici.
 2. Scegli Attivato o Disattivato, quindi scegli Salva. Per ulteriori informazioni, consulta [Utilizza automaticamente nuove versioni delle estensioni](#).
 - Per aggiornare il ruolo di esecuzione:
 1. Scegli Modifica ruolo di esecuzione.
 2. Specificate l'ARN del ruolo IAM che desiderate CloudFormation utilizzare quando richiamate questa estensione, quindi scegliete Salva. Per ulteriori informazioni, consulta [Configura un ruolo di esecuzione con autorizzazioni IAM e una policy di fiducia per l'accesso alle estensioni pubbliche](#).
 - Per aggiornare la configurazione di registrazione:
 1. Scegli Modifica configurazione di registrazione.
 2. Modifica la configurazione di registrazione JSON, quindi scegli Salva.

Disattiva le estensioni pubbliche di terze parti nel tuo account

Quando non hai più bisogno di un'estensione pubblica di terze parti attivata, utilizza le seguenti procedure per disattivarla nel tuo account.

Argomenti

- [Disattiva un'estensione pubblica nel tuo account \(console\)](#)
- [Disattiva un'estensione pubblica nel tuo account \(\)AWS CLI](#)
- [Disattiva un Hook nel tuo account \(AWS CLI\)](#)

Disattiva un'estensione pubblica nel tuo account (console)

Per disattivare un'estensione pubblica nel tuo account

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Dal pannello di navigazione, sotto Registro, scegli Estensioni attivate.
4. Trova l'estensione che desideri disattivare e selezionala. Per ulteriori informazioni, consulta [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#).
5. Dal menu Azioni, scegli Disattiva.
6. Seleziona Disattiva.

Disattiva un'estensione pubblica nel tuo account (AWS CLI)

Usa quanto segue [deactivate-type](#) comando.

```
aws cloudformation deactivate-type --type MODULE \  
  --type-name Example::Test::Type::MODULE \  
  --region us-west-2
```

Disattiva un Hook nel tuo account (AWS CLI)

La disabilitazione di un Hook impedisce all'Hook di funzionare Account AWS senza rimuoverlo.

Utilizzo dell'[set-type-configuration](#) comando e specifica HookInvocationStatus come DISABLED disabilitare un Hook.

L'esempio seguente specifica il Regione AWS e l'Amazon Resource Name (ARN) dell'Hook che viene disabilitato.

```
aws cloudformation set-type-configuration \  
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":  
{"HookInvocationStatus": "DISABLED", "FailureMode": "FAIL", "Properties":{}}}}' \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" --  
  region us-west-2
```

Per ulteriori informazioni, consulta [Disabilitare e abilitare gli AWS CloudFormation Hooks](#) nella Guida per l'utente di AWS CloudFormation Hooks.

Usa estensioni private di terze parti che sono state condivise con te

Per utilizzare le estensioni private di terze parti che sono state condivise con te, devi prima registrarle con CloudFormation gli account e le regioni in cui desideri utilizzarle. La registrazione dell'estensione ne carica una copia nel CloudFormation registro del tuo account e la attiva. Una volta registrata un'estensione privata, questa verrà visualizzata nel CloudFormation registro di quella regione Account AWS e potrai utilizzarla nei tuoi modelli di stack.

Argomenti

- [Autorizzazioni IAM per la registrazione di un'estensione privata di terze parti](#)
- [AWS CLI Comandi comunemente usati per lavorare con estensioni private](#)
- [Registra un'estensione privata di terze parti nel tuo account](#)
- [Annulla la registrazione delle estensioni private di terze parti che hai precedentemente registrato nel tuo account](#)

Autorizzazioni IAM per la registrazione di un'estensione privata di terze parti

Come parte della registrazione di un'estensione privata, puoi specificare un bucket Amazon S3 che contenga il pacchetto del progetto di estensione. Questo pacchetto contiene tutti i file sorgente necessari per l'estensione che desideri registrare. L'utente che registra l'estensione deve essere in grado di accedere al pacchetto del progetto nel bucket Amazon S3. A tale scopo, l'utente deve avere [GetObject](#) autorizzazioni per il pacchetto di estensione.

Questo è vero indipendentemente dal fatto che tu stia usando il [register-type](#) comando di AWS CLI, o [submit](#) comando della CloudFormation CLI.

Per ulteriori informazioni, consulta [Actions, Resources and Condition Keys per Amazon S3](#) nel Service Authorization Reference.

AWS CLI Comandi comunemente usati per lavorare con estensioni private

I comandi comunemente usati per lavorare con le estensioni private includono:

- [register-type](#) per registrare un'estensione privata nel tuo account.
- [describe-type-registration](#) per restituire lo stato attuale di una richiesta di registrazione.
- [list-types](#) per elencare le estensioni presenti nel tuo account.

- [describe-type](#) per restituire informazioni dettagliate su un'estensione specifica o una versione di estensione specifica, inclusi i dati di configurazione correnti.
- [set-type-configuration](#) per specificare i dati di configurazione per un'estensione nel tuo account e per disabilitare e abilitare gli Hooks.
- [set-type-default-version](#) per specificare quale versione di un'estensione è la versione predefinita.
- [deregister-type](#) per rimuovere un'estensione o una versione di estensione privata dal tuo account.

Registra un'estensione privata di terze parti nel tuo account

Questo argomento illustra i passaggi per registrare un'estensione privata di terze parti condivisa con te in modo che sia disponibile per l'uso nel tuo account.

Note

Prima di continuare, conferma di avere i requisiti necessari [Autorizzazioni IAM](#) per registrare un'estensione privata.

Per registrare un'estensione privata condivisa con te (AWS CLI)

1. Individua il bucket Amazon S3 che contiene il pacchetto di progetto per l'estensione privata che desideri registrare nel tuo account.
2. Utilizzo dell'[register-type](#) comando per registrare l'estensione privata nel tuo account.

Ad esempio, il comando seguente registra il tipo di `My::Resource::Example` risorsa nel campo specificato Account AWS.

```
aws cloudformation register-type --type RESOURCE \  
  --type-name My::Resource::Example \  
  --schema-handler-package [s3 object path] --region us-west-2
```

`RegisterType` è un'operazione asincrona e restituisce un token di registrazione che è possibile utilizzare per monitorare lo stato di avanzamento della richiesta di registrazione.

```
{  
  "RegistrationToken": "f5525280-104e-4d35-bef5-8f1fexample"  
}
```

Se la tua estensione chiama AWS APIs come parte della sua funzionalità, devi creare un ruolo di esecuzione IAM che includa le autorizzazioni necessarie per chiamarle AWS APIs e fornire tale ruolo di esecuzione nel tuo account. È quindi possibile specificare questo ruolo di esecuzione utilizzando l'`--execution-role-arn` opzione. CloudFormation assume quindi quel ruolo di esecuzione per fornire al tipo di risorsa le credenziali appropriate.

```
--execution-role-arn arn:aws:iam::123456789012:role/MyIAMRole
```

3. (Facoltativo) Utilizzate il token di registrazione con [describe-type-registration](#) comando per tracciare lo stato di avanzamento della richiesta di registrazione.

Quando CloudFormation completa la richiesta di registrazione, imposta lo stato di avanzamento della richiesta su. COMPLETE

Nell'esempio seguente viene utilizzato il token di registrazione restituito dal comando `describe-type-registration` sopra per restituire le informazioni sullo stato della registrazione.

```
aws cloudformation describe-type-registration \  
  --registration-token f5525280-104e-4d35-bef5-8f1fexample \  
  --region us-west-2
```

Questo comando restituisce il seguente output.

```
{  
  "ProgressStatus": "COMPLETE",  
  "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/My-  
Resource-Example",  
  "Description": "Deployment is currently in DEPLOY_STAGE of status COMPLETED; ",  
  "TypeVersionArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/  
My-Resource-Example/00000001"  
}
```

Important

Se l'estensione che stai registrando è un Hook, questo passaggio successivo è necessario. È necessario specificare `ENABLED` per la proprietà `HookInvocationStatus`. Questa operazione abilita le proprietà dell'Hook definite nella `properties` sezione dello schema

di Hook. Per ulteriori informazioni, vedere il [riferimento alla sintassi dello schema di configurazione di Hook nella Guida](#) per l'utente di AWS CloudFormation Hooks.

Per specificare i dati di configurazione per un Hook ()AWS CLI

1. Ottieni l'ARN per il tuo Hook e salvalo. Puoi ottenere l'ARN di un Hook usando o. AWS Management Console AWS CLI Per ulteriori informazioni, consulta [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#).

```
export HOOK_TYPE_ARN="arn:aws:cloudformation:us-west-2:123456789012:type/hook/  
Organization-Service-Hook/"
```

2. Utilizzo dell'[set-type-configuration](#) comando per specificare i dati di configurazione. Il JSON richiesto --configuration deve essere convalidato rispetto allo schema di configurazione di Hook. Per attivare l'Hook, è necessario impostare la HookInvocationStatus proprietà su ENABLED nella HookConfiguration sezione.

```
aws cloudformation set-type-configuration \  
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":  
  {"HookInvocationStatus": "ENABLED", "FailureMode": "FAIL", "Properties":{}}}}' \  
  --type-arn $HOOK_TYPE_ARN --region us-west-2
```

Per ulteriori informazioni, vedere il [riferimento alla sintassi dello schema di configurazione di Hook nella Guida](#) per l'utente di AWS CloudFormation Hooks.

Annulla la registrazione delle estensioni private di terze parti che hai precedentemente registrato nel tuo account

Per rimuovere un'estensione o una versione di estensione privata di terze parti, utilizza il [deregister-type](#) comando.

È possibile annullare la registrazione di una versione specifica dell'estensione o dell'estensione nel suo insieme. Per annullare la registrazione di un'estensione, è necessario annullare singolarmente tutte le versioni registrate di tale estensione. Se un'estensione ha una sola versione registrata, l'annullamento della registrazione di quella versione comporta l'annullamento della registrazione dell'estensione stessa. Non puoi annullare la registrazione della versione predefinita di un'estensione,

a meno che non sia l'unica versione registrata di quell'estensione, nel qual caso viene annullata anche l'estensione stessa.

L'esempio seguente annulla la registrazione di un'estensione. Sostituite i valori di esempio per e. --type --type-name

```
aws cloudformation deregister-type --type MODULE \  
  --type-name My::S3::SampleBucket::MODULE \  
  --region us-west-2
```

Per annullare la registrazione di una versione specifica dell'estensione, specificate l'--version-id opzione nel comando.

Modifica i dati di configurazione per le estensioni nel tuo account

Questo argomento fornisce indicazioni sulla modifica dei dati di configurazione per le estensioni del tuo account all'interno di una regione specifica. Le estensioni possono includere proprietà di configurazione che si applicano a tutte le istanze dell'estensione per un determinato account e regione. Queste sono definite dall'autore dell'estensione nella definizione di configurazione dell'estensione. Se sono presenti proprietà richieste nella definizione di configurazione dell'estensione, è necessario specificare tali proprietà prima di poter utilizzare l'estensione nell'account e nella Regione.

Per ulteriori informazioni su come vengono definite le definizioni di configurazione durante lo sviluppo di un'estensione, consultate la seguente documentazione.

- [Riferimento alla sintassi dello schema di configurazione di Hook](#)
- [Definizione della configurazione di un'estensione a livello di account](#)

Argomenti

- [Autorizzazioni necessarie per utilizzare i riferimenti dinamici](#)
- [Modifica i dati di configurazione per un'estensione \(console\)](#)
- [Modifica i dati di configurazione per un'estensione \(AWS CLI\)](#)

Autorizzazioni necessarie per utilizzare i riferimenti dinamici

Se i dati di configurazione includono riferimenti dinamici ai valori archiviati in AWS Systems Manager o AWS Secrets Manager, qualsiasi ruolo utilizzato per fornire il tipo (ad esempio, durante la creazione o l'aggiornamento di uno stack) deve disporre delle autorizzazioni appropriate per recuperare quel valore. Nello specifico:

- Se i dati di configurazione contengono un parametro memorizzato in AWS Systems Manager Parameter Store, l'utente o il ruolo utilizzato per il provisioning del tipo deve disporre delle autorizzazioni per la chiamata [GetParameter](#).
- Se i dati di configurazione contengono un segreto archiviato in AWS Secrets Manager, l'utente o il ruolo utilizzato per fornire il tipo deve disporre delle autorizzazioni per effettuare la chiamata [GetSecretValue](#).

Per ulteriori informazioni, consulta [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#).

Modifica i dati di configurazione per un'estensione (console)

Segui i passaggi indicati in questa sezione per utilizzare la console per:

- Visualizza i dati di configurazione correnti per un'estensione
- Aggiorna i dati di configurazione dell'estensione per il tuo account

Per visualizzare i dati di configurazione correnti per un'estensione

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Dal pannello di navigazione, sotto Registro, scegli Estensioni attivate.
4. Trova l'estensione che desideri visualizzare. Per ulteriori informazioni, consulta [Visualizza le estensioni disponibili e attivate nel CloudFormation registro](#).
5. Scegli l'estensione per visualizzare i dettagli dell'estensione.
6. Nella pagina dei dettagli dell'estensione, scegli la scheda Configuration (Configurazione).
7. Espandi la scheda Configuration schema (Schema di configurazione) per visualizzare lo schema di configurazione definito per l'estensione.

8. Espandi la scheda Configuration (Configurazione) per visualizzare la configurazione attualmente impostata per l'estensione.

Per aggiornare i dati di configurazione per un'estensione

1. Nella pagina dei dettagli dell'estensione, dalla scheda Configurazione, scegli Modifica configurazione.

In alternativa, da Azioni, scegli Modifica, quindi scegli Modifica configurazione.

CloudFormation visualizza la pagina Configura estensione. Assicurati che View configuration schema ((Visualizza schema di configurazione)) sia attivato per vedere lo schema di definizione della configurazione corrente dell'estensione.

2. Nella casella di testo Configuration JSON (Configurazione JSON), immetti una stringa JSON che rappresenti lo schema di configurazione da impostare per l'estensione. Devi convalidarlo a fronte dello schema definito in Configuration schema (Schema di configurazione).
3. Scegli Configura estensione.

Modifica i dati di configurazione per un'estensione (AWS CLI)

Segui la procedura descritta in questa sezione per AWS CLI utilizzare:

- Visualizzare i dati di configurazione correnti per un'estensione
- Aggiorna i dati di configurazione dell'estensione per il tuo account

Per visualizzare i dati di configurazione correnti per un'estensione

- Utilizzo dell'[describe-type](#) comando per restituire informazioni dettagliate sull'estensione. L'elemento ConfigurationSchema dell'output contiene la definizione di configurazione corrente dell'estensione in una determinata Regione.

In alternativa, utilizzare il [batch-describe-type-configurations](#) comando per restituire i dati di configurazione relativi a più estensioni.

Per aggiornare i dati di configurazione per un'estensione

- Utilizzo dell'[set-type-configuration](#) comando per specificare i dati di configurazione. Il codice JSON richiesto `--configuration` deve essere convalidato rispetto allo schema di configurazione dell'estensione.

Nell'esempio seguente, il `set-type-configuration` comando specifica i dati di configurazione `{"CredentialKey": "testUserCredential"}` per l'opzione. `--configuration`

```
aws cloudformation set-type-configuration --type RESOURCE \  
  --type-name My::Resource::Example \  
  --configuration-alias default \  
  --configuration '{"CredentialKey": "testUserCredential"}' \  
  --region us-west-2
```

Registra i tipi di risorse in AWS Config

Puoi specificare che tenga traccia AWS Config automaticamente dei tipi di risorse private e registri le modifiche a tali risorse come elementi di configurazione. Ciò consente di visualizzare la cronologia di configurazione per questi tipi di risorse private, oltre a scrivere Regole di AWS Config regole per verificare le migliori pratiche di configurazione. AWS Config è necessario per l'estensione Hook.

Per tenere traccia AWS Config automaticamente dei tipi di risorse private:

- Gestisci le risorse tramite CloudFormation. Ciò include l'esecuzione di tutte le operazioni di creazione, aggiornamento ed eliminazione delle risorse tramite CloudFormation.

Note

Se utilizzi un ruolo IAM per eseguire le operazioni sullo stack, tale ruolo IAM deve avere l'autorizzazione a eseguire le seguenti AWS Config azioni:

- [PutResourceConfig](#)
- [DeleteResourceConfig](#)

- Configura AWS Config per registrare tutti i tipi di risorse. Per ulteriori informazioni, consulta [Registrazione delle configurazioni per risorse di terze parti utilizzando la AWS CLI](#) Guida per gli AWS Config sviluppatori.

 Note

AWS Config non supporta la registrazione di risorse private contenenti proprietà definite sia come obbligatorie che di sola scrittura.

In base alla progettazione, le proprietà delle risorse definite come di sola scrittura non vengono restituite nello schema utilizzato per creare l'elemento di configurazione. AWS Config Di conseguenza, se includi una proprietà definita come di sola scrittura e come obbligatoria, la creazione dell'elemento di configurazione avrà esito negativo perché una proprietà obbligatoria non sarà presente. Per visualizzare lo schema che verrà utilizzato per creare l'elemento di configurazione, è possibile esaminare la schema proprietà del [DescribeTypeOperazione](#).

Per ulteriori informazioni, consulta [Elementi della configurazione](#) nella Guida per gli sviluppatori di AWS Config.

Impedire la registrazione di proprietà con dati sensibili in un elemento di configurazione

Il tipo di risorsa può contenere proprietà considerate informazioni riservate, ad esempio password, segreti o altri dati sensibili, che non si desidera registrare come parte dell'elemento di configurazione. Per evitare che una proprietà venga registrata nell'elemento di configurazione, è possibile includere tale proprietà nell'elenco `writeOnlyProperties` nello schema del tipo di risorsa. Le proprietà delle risorse elencate come `writeOnlyProperties` possono essere specificate dall'utente, ma non verranno restituite da una richiesta `read` o `list`.

Per ulteriori informazioni, consulta [writeOnlyProperties](#) nella Guida per l'utente della CloudFormation CLI.

Consegna continua con CodePipeline

La distribuzione continua è un metodo di rilascio in cui le modifiche al codice vengono applicate a una build, testate e preparate per il rilascio in produzione in modo automatico. Con CloudFormation e CodePipeline, puoi utilizzare la distribuzione continua per creare e testare automaticamente le modifiche ai tuoi CloudFormation modelli prima di promuoverli negli stack di produzione. Questo processo di rilascio consente di apportare modifiche all'infrastruttura in modo rapido e affidabile. AWS

Ad esempio, è possibile creare un flusso di elaborazione che crea automaticamente uno stack di test quando viene inviato un modello aggiornato a un repository di codice. Dopo CloudFormation aver creato lo stack di test, puoi testarlo e poi decidere se trasferire le modifiche a uno stack di produzione. Per ulteriori informazioni sui vantaggi della distribuzione continua, consulta [Cos'è la distribuzione continua?](#)

Utilizzalo CodePipeline per creare un flusso di lavoro di distribuzione continua creando una pipeline per gli stack. CloudFormation CodePipeline ha un'integrazione integrata con CloudFormation, quindi puoi specificare azioni CloudFormation specifiche, come la creazione, l'aggiornamento o l'eliminazione di uno stack, all'interno di una pipeline. [Per ulteriori informazioni in merito CodePipeline, consulta la Guida per l'utente.AWS CodePipeline](#)

Argomenti

- [Spiegazione passo per passo: creazione di una pipeline per stack di test e produzione](#)
- [AWS CloudFormation riferimento alle proprietà di configurazione](#)
- [AWS CloudFormation artefatti](#)
- [Utilizzo delle funzioni di sovrascrittura dei parametri con le pipeline CodePipeline](#)

Spiegazione passo per passo: creazione di una pipeline per stack di test e produzione

Immagina un processo di rilascio in cui invii un AWS CloudFormation modello, che CloudFormation poi viene utilizzato per creare automaticamente uno stack di test. Dopo avere esaminato lo stack di test, puoi visualizzare in anteprima gli effetti delle modifiche apportate allo stack e decidere se implementarle. Per realizzare questo flusso di lavoro, puoi CloudFormation creare lo stack di test, eliminare lo stack di test, creare un set di modifiche e quindi eseguire il set di modifiche. Tuttavia ciascuna operazione prevede l'interazione manuale con CloudFormation. In questa procedura

dettagliata, creeremo una CodePipeline pipeline che automatizza molte di queste azioni, aiutandoti a ottenere un flusso di lavoro di distribuzione continua con i tuoi stack. CloudFormation

Prerequisiti

Questa procedura dettagliata presuppone che tu abbia utilizzato CodePipeline e sappia come funzionano pipeline CloudFormation, modelli e stack. AWS CloudFormation [Per ulteriori informazioni in merito CodePipeline, consulta la Guida per l'utente.AWS CodePipeline](#) È inoltre necessario disporre di un bucket Amazon S3 nello stesso in Regione AWS cui si crea la pipeline.

Important

Il WordPress modello di esempio crea un' EC2 istanza che richiede una connessione a Internet. Verifica che la sottorete e il VPC predefiniti consentano il traffico in Internet.

Panoramica della spiegazione passo per passo

Questa procedura dettagliata crea una pipeline per un WordPress sito di esempio in uno stack. La pipeline è suddivisa in tre fasi. Ogni fase deve contenere almeno un'operazione, ovvero un'attività eseguita dalla pipeline sul tuo artefatto (il tuo input). Una fase organizza le operazioni in una pipeline. CodePipeline deve completare tutte le operazioni in una fase prima che la fase elabori nuovi artefatti, ad esempio, se è stato inviato un nuovo input per eseguire nuovamente la pipeline.

Al termine di questa procedura guidata, avrai una pipeline che esegue il flusso di elaborazione seguente:

1. La prima fase della pipeline recupera un elemento sorgente (un CloudFormation modello e i relativi file di configurazione) da un repository.

Preparerai un artefatto che include un WordPress modello di esempio e lo caricherai in un bucket S3.

2. Nella seconda fase la pipeline crea uno stack di test e attende la tua approvazione.

Dopo avere esaminato lo stack di test, puoi scegliere di continuare con la pipeline originale o di creare e inviare un altro artefatto per apportare modifiche. Se approvi, questa fase elimina lo stack di test e la pipeline procede con la fase successiva.

3. Nella terza fase la pipeline crea un set di modifiche su uno stack di produzione e attende la tua approvazione.

Nell'esecuzione iniziale non avrai uno stack di produzione. Il set di modifiche mostra tutte le risorse che verranno create. CloudFormation Se approvi, questa fase esegue il set di modifiche e crea il tuo stack di produzione.

Note

CloudFormation è un servizio gratuito. Tuttavia, ti verranno addebitate le AWS risorse, EC2 ad esempio l'istanza, che includi nel tuo stack alla tariffa corrente per ciascuna di esse. Per ulteriori informazioni sui AWS prezzi, consulta la pagina dei dettagli di ciascun prodotto all'[indirizzo http://aws.amazon.com](http://aws.amazon.com).

Fase 1: modifica dell'artefatto e caricamento in un bucket S3

Prima di creare la pipeline, è necessario configurare l'archivio e i file di origine. CodePipeline copia questi file sorgente nell'[archivio degli artefatti](#) della pipeline e quindi li usa per eseguire azioni nella pipeline, come la creazione di uno stack. CloudFormation

Quando utilizzi Amazon Simple Storage Service (Amazon S3) come repository di origine CodePipeline, è necessario comprimere i file sorgente prima di caricarli in un bucket S3. Il file compresso è un CodePipeline artefatto che può contenere un modello, un file di configurazione del CloudFormation modello o entrambi. Forniamo un artefatto che contiene un modello di esempio e due file di configurazione del WordPress modello. I due file di configurazione specificano i valori dei parametri per il WordPress modello. CodePipeline li usa quando crea gli WordPress stack. Un file contiene i valori dei parametri per uno stack di test, l'altro per uno stack di produzione. Dovrai modificare i file di configurazione, ad esempio, per specificare il nome di una EC2 coppia di chiavi esistente di tua proprietà. Per ulteriori informazioni sugli artefatti, vedi [AWS CloudFormation artefatti](#).

Dopo aver creato il tuo artefatto, potrai caricarlo in un bucket S3.

Per modificare e caricare l'artefatto

1. [Scaricate e aprite l'artefatto di esempio: https://s3.amazonaws.com/cloudformation-examples/user-single-instance.zip.guide/continuous-deployment/wordpress](https://s3.amazonaws.com/cloudformation-examples/user-single-instance.zip.guide/continuous-deployment/wordpress)

L'artefatto contiene tre file:

- Il modello di esempio WordPress : `wordpress-single-instance.yaml`

- Il file di configurazione del modello per lo stack di test: `test-stack-configuration.json`
 - Il file di configurazione del modello per lo stack di produzione: `prod-stack-configuration.json`
2. Estrarre tutti i file e utilizzare un editor di testo per modificare i file di configurazione del modello.

Apri i file di configurazione per vedere che contengono coppie chiave-valore che corrispondono ai parametri del WordPress modello. I file di configurazione specificano i valori dei parametri utilizzati dalla tua pipeline quando crea gli stack di test e di produzione.

Modificare il file `test-stack-configuration.json` per specificare i valori dei parametri per lo stack di test e il file `prod-stack-configuration.json` per lo stack di produzione.

- Cambia i valori `DBPassword` e `DBRootPassword` chiavi in password che puoi usare per accedere al tuo database. WordPress Come definito nel WordPress modello, i valori dei parametri devono contenere solo caratteri alfanumerici.
 - Modifica il valore della `KeyName` chiave con il nome di una EC2 coppia di chiavi esistente nella regione in cui creerai la pipeline.
3. Aggiungere i file di configurazione modificati al file di artefatto originale (`.zip`), sostituendo i file duplicati.

A questo punto hai un artefatto personalizzato che puoi caricare in un bucket S3.

4. [Caricare l'artefatto in un bucket S3 di cui si è proprietari.](#)

Prendere nota della posizione del file. Si dovrà specificare il percorso di questo file quando si creerà la pipeline.

Note sugli artefatti e sul bucket S3:

- Usa un bucket che si trova nella stessa AWS regione in cui creerai la tua pipeline.
- CodePipeline [richiede che il bucket sia abilitato al controllo delle versioni.](#)
- Puoi anche utilizzare servizi che non richiedono di comprimere i file prima di caricarli, ad esempio nel tuo GitHub repository CodeCommit di origine.
- Gli artefatti possono contenere informazioni sensibili, ad esempio password. Limitare l'accesso in modo che solo gli utenti autorizzati possano visualizzare il file. Quando lo fai, assicurati che CodePipeline possa ancora accedere al file. Ad esempio, se carichi l'artefatto su un bucket S3, utilizza le [policy del bucket S3 o le policy utente](#) per limitare l'accesso.

Ora hai un artefatto che CodePipeline può entrare nella tua pipeline. Nel passaggio successivo, specificherai la posizione dell'artefatto e costruirai la pipeline. WordPress

Fase 2: creazione dello stack della pipeline

Per creare la WordPress pipeline, utilizzerai un modello di esempio. CloudFormation Oltre a creare la pipeline, il modello imposta i ruoli di servizio AWS Identity and Access Management (IAM) per CodePipeline e CloudFormation, un bucket S3 per l' CodePipeline artifact store e un argomento Amazon Simple Notification Service (Amazon SNS) a cui la pipeline invia notifiche, ad esempio notifiche sulle recensioni. Il modello di esempio semplifica il provisioning e la configurazione di queste risorse in un unico stack. CloudFormation

Per ulteriori dettagli sulla configurazione della pipeline, vedi [Operazioni della pipeline](#).

Important

Il WordPress modello di esempio crea un' EC2 istanza che richiede una connessione a Internet. Verifica che la sottorete e il VPC predefiniti consentano il traffico in Internet.

Per creare lo stack della pipeline

1. Scaricate il modello di esempio all'indirizzo <https://s3.amazonaws.com/cloudformation-examples/user-guide/continuous-deployment/basic-pipeline.yml>. Salvarlo sul computer.
2. Apri la console all'indirizzo. CloudFormation <https://console.aws.amazon.com/cloudformation/>
3. Scegli una AWS regione che supporti CodePipeline e CloudFormation.

Per ulteriori informazioni, consulta [CodePipeline endpoint e quote](#) e [AWS CloudFormation endpoint e quote](#) in. Riferimenti generali di AWS

4. Seleziona Crea stack.
5. In Specify template (Specifica modello), scegli Upload a template file (Carica un file modello), quindi scegli il modello appena scaricato, `basic-pipeline.yml`.
6. Scegli Next (Successivo).
7. Per Stack name (Nome stack), digitare `sample-WordPress-pipeline`.
8. Nella sezione Parameters (Parametri) specificare i seguenti valori di parametro, quindi selezionare Next (Avanti). Quando impostate i parametri dello stack, se avete mantenuto gli

stessi nomi per il WordPress modello e i relativi file di configurazione, potete utilizzare i valori predefiniti. In caso contrario, specificare i nomi file utilizzati.

PipelineName

Il nome della pipeline, ad esempio `WordPress-test-pipeline`.

S3Bucket

Nome del bucket S3 in cui hai salvato il tuo artefatto (file `.zip`).

SourceS3Key

Nome file dell'artefatto. Se hai salvato l'artefatto in una cartella, includila come parte del nome file, ad esempio `folder/subfolder/wordpress-single-instance.zip`.

E-mail

L'indirizzo e-mail a cui CodePipeline invia la notifica della pipeline, ad esempio.
`myemail@example.com`

9. Per questa procedura guidata, non è necessario aggiungere tag o specificare impostazioni avanzate, quindi selezionare Next (Avanti).
10. Assicurarsi che il nome dello stack e l'URL del modello siano corretti e scegliere Create stack (Crea stack).
11. Per confermare che sei a conoscenza del fatto che CloudFormation potrebbe creare risorse IAM, seleziona la casella di controllo.

La creazione del tuo stack potrebbe richiedere alcuni minuti. AWS CloudFormation È possibile controllare l'avanzamento negli eventi per lo stack. Per ulteriori informazioni, consulta [Monitora l'avanzamento dello stack](#).

Dopo aver creato lo stack, CodePipeline avvia la nuova pipeline. Per visualizzarne lo stato, vedi la [console CodePipeline](#). Dall'elenco delle pipeline, scegli `-test-pipeline`. WordPress

Operazioni della pipeline

Questa sezione spiega le tre fasi della pipeline, utilizzando frammenti del modello di pipeline di esempio. WordPress

Fase 1: origine

La prima fase della pipeline è una fase di origine in cui si specifica la posizione del codice sorgente. Ogni volta che invii una revisione a questa posizione, riesegue la pipeline. CodePipeline

Il codice sorgente si trova in un bucket S3 e viene identificato dal relativo nome file. Questi valori sono stati specificati come valori dei parametri di input al momento della creazione dello stack della pipeline. Per consentire l'utilizzo dell'artefatto di origine nelle fasi successive, il frammento specifica la proprietà `OutputArtifacts` con il nome `TemplateSource`. Per utilizzare questo artefatto nelle fasi successive, è necessario specificare `TemplateSource` come artefatto di input.

```
- Name: S3Source
  Actions:
    - Name: TemplateSource
      ActionTypeId:
        Category: Source
        Owner: AWS
        Provider: S3
        Version: '1'
      Configuration:
        S3Bucket: !Ref 'S3Bucket'
        S3ObjectKey: !Ref 'SourceS3Key'
      OutputArtifacts:
        - Name: TemplateSource
```

Fase 2: TestStage

Nella fase `TestStage` la pipeline crea lo stack di test, attende l'approvazione, quindi elimina lo stack di test.

Per l'operazione `CreateStack`, la pipeline utilizza il file e il WordPress modello di configurazione del test per creare lo stack di test. Entrambi i file sono contenuti nell'artefatto di input `TemplateSource`, che viene introdotto dalla fase di origine. Il frammento utilizza la modalità di operazione `REPLACE_ON_FAILURE`. Se la creazione dello stack non riesce la pipeline lo sostituisce, in questo modo non è più necessario eseguire la pulizia o risolvere i problemi dello stack prima di poter eseguire nuovamente la pipeline. La modalità di operazione è utile per effettuare in modo rapido iterazioni sugli stack di test. Per la `RoleArn` proprietà, il valore è un ruolo AWS CloudFormation di servizio dichiarato altrove nel modello.

L'operazione `ApproveTestStack` sospende la pipeline e invia una notifica all'indirizzo e-mail da te indicato al momento della creazione dello stack della pipeline. Mentre la pipeline è in pausa,

puoi controllare lo stack di WordPress test e le sue risorse. Utilizzare CodePipeline per [approvare o rifiutare](#) questa azione. La proprietà CustomData include una descrizione dell'operazione che stai approvando, che la pipeline aggiunge all'e-mail di notifica.

Dopo aver approvato questa azione, CodePipeline passa all'DeleteTestStackazione ed elimina lo WordPress stack di test e le relative risorse.

```
- Name: TestStage
  Actions:
    - Name: CreateStack
      ActionTypeId:
        Category: Deploy
        Owner: AWS
        Provider: CloudFormation
        Version: '1'
      InputArtifacts:
        - Name: TemplateSource
      Configuration:
        ActionMode: REPLACE_ON_FAILURE
        RoleArn: !GetAtt [CFNRole, Arn]
        StackName: !Ref TestStackName
        TemplateConfiguration: !Sub "TemplateSource::${TestStackConfig}"
        TemplatePath: !Sub "TemplateSource::${TemplateFileName}"
      RunOrder: '1'
    - Name: ApproveTestStack
      ActionTypeId:
        Category: Approval
        Owner: AWS
        Provider: Manual
        Version: '1'
      Configuration:
        NotificationArn: !Ref CodePipelineSNSTopic
        CustomData: !Sub 'Do you want to create a change set against the production
stack and delete the ${TestStackName} stack?'
      RunOrder: '2'
    - Name: DeleteTestStack
      ActionTypeId:
        Category: Deploy
        Owner: AWS
        Provider: CloudFormation
        Version: '1'
      Configuration:
        ActionMode: DELETE_ONLY
```

```
RoleArn: !GetAtt [CFNRole, Arn]
StackName: !Ref TestStackName
RunOrder: '3'
```

Fase 3: ProdStage

La fase ProdStage della pipeline crea un set di modifiche sullo stack di produzione esistente, attende l'approvazione, quindi esegue il set di modifiche.

Un set di modifiche fornisce un'anteprima di tutte le modifiche che AWS CloudFormation verranno apportate allo stack di produzione prima di implementarle. Sulla prima pipeline eseguita non avrai uno stack di produzione in esecuzione. Il set di modifiche mostra le azioni AWS CloudFormation eseguite durante la creazione dello stack di test. Per creare il set di modifiche, l'CreateChangeSet azione utilizza il modello di WordPress esempio e la configurazione del modello di produzione dall'elemento TemplateSource di input.

Analogamente alla fase precedente, l'operazione ApproveChangeSet sospende la pipeline e invia una notifica e-mail. Mentre la pipeline è in pausa, è possibile visualizzare il set di modifiche per verificare tutte le modifiche proposte allo stack di produzione. WordPress CodePipeline Utilizzatelo per [approvare o rifiutare](#) questa azione rispettivamente per continuare o arrestare la pipeline.

Dopo aver approvato questa azione, l'ExecuteChangeSet azione esegue il set di modifiche, in modo da AWS CloudFormation eseguire tutte le azioni descritte nel set di modifiche. Per l'esecuzione iniziale, AWS CloudFormation crea lo stack di WordPress produzione. Con le esecuzioni successive AWS CloudFormation aggiorna lo stack.

```
- Name: ProdStage
  Actions:
    - Name: CreateChangeSet
      ActionTypeId:
        Category: Deploy
        Owner: AWS
        Provider: CloudFormation
        Version: '1'
      InputArtifacts:
        - Name: TemplateSource
      Configuration:
        ActionMode: CHANGE_SET_REPLACE
        RoleArn: !GetAtt [CFNRole, Arn]
        StackName: !Ref ProdStackName
        ChangeSetName: !Ref ChangeSetName
        TemplateConfiguration: !Sub "TemplateSource:${ProdStackConfig}"
```

```
    TemplatePath: !Sub "TemplateSource::${TemplateFileName}"
  RunOrder: '1'
- Name: ApproveChangeSet
  ActionTypeId:
    Category: Approval
    Owner: AWS
    Provider: Manual
    Version: '1'
  Configuration:
    NotificationArn: !Ref CodePipelineSNSTopic
    CustomData: !Sub 'A new change set was created for the ${ProdStackName} stack.
Do you want to implement the changes?'
  RunOrder: '2'
- Name: ExecuteChangeSet
  ActionTypeId:
    Category: Deploy
    Owner: AWS
    Provider: CloudFormation
    Version: '1'
  Configuration:
    ActionMode: CHANGE_SET_EXECUTE
    ChangeSetName: !Ref ChangeSetName
    RoleArn: !GetAtt [CFNRole, Arn]
    StackName: !Ref ProdStackName
  RunOrder: '3'
```

Fase 3: Visualizza lo stack WordPress

Durante CodePipeline la pipeline, viene utilizzato CloudFormation per creare stack di test e produzione. Per vedere lo stato di questi stack e il loro output, usa la console. CloudFormation

Per visualizzare uno stack

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation/>.
2. A seconda che la pipeline sia in fase di test o di produzione, scegliere lo stack Test-MyWordPressSite o Prod-MyWordPressSite.
3. Per controllare lo stato dello stack, visualizzare gli [eventi](#) dello stack.

Se lo stack si trova nello stato non riuscito, visualizzare il motivo per individuare l'errore. Correggere l'errore ed eseguire nuovamente la pipeline. Se lo stack è nello CREATE_COMPLETE stato, visualizza i suoi output per ottenere l'URL del tuo WordPress sito.

Lo hai utilizzato con successo CodePipeline per creare un flusso di lavoro di distribuzione continua per un sito di esempio WordPress . Se invii modifiche al bucket S3, rileva CodePipeline automaticamente una nuova versione e quindi riesegue la pipeline. Questo flusso di elaborazione semplifica l'invio e il test delle modifiche prima di apportare modifiche al sito di produzione.

Fase 4: Eliminazione delle risorse

Per essere sicuro che non ti vengano addebitati servizi indesiderati, elimina le risorse.

Important

Elimina gli stack di test e produzione WordPress prima di eliminare lo stack di pipeline. Lo stack di pipeline contiene un ruolo di servizio necessario per eliminare gli stack. WordPress. Se hai eliminato prima lo stack di pipeline, puoi associare un altro ruolo di servizio Amazon Resource Name (ARN) agli WordPress stack e quindi eliminarli.

Per eliminare oggetti nello store degli artefatti

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli il bucket S3 CodePipeline utilizzato come archivio degli artefatti della tua pipeline.

Il nome del bucket segue il formato: *stackname-artifactstorebucket-id*. Se è stata seguita questa procedura guidata, il nome del bucket potrebbe essere simile all'esempio seguente: sample-WordPress-pipeline-artifactstorebucket-12345abcd12345.

3. Eliminare tutti gli oggetti nel bucket S3 dello store di artefatti.

Quando si elimina lo stack della pipeline nella fase successiva, questo bucket deve essere vuoto. Altrimenti, CloudFormation non sarà possibile eliminare il bucket.

Per eliminare gli stack

1. Dalla CloudFormation console, scegli lo stack che desideri eliminare.

Se gli WordPress stack creati dalla pipeline sono ancora in esecuzione, sceglili prima. Per impostazione predefinita, i nomi degli stack sono Test-MyWordPressSite e Prod-MyWordPressSite.

Se hai già eliminato gli WordPress stack, scegli lo stack. sample-WordPress-pipeline

2. Scegliere Actions (Operazioni), quindi Delete Stack (Elimina stack).
3. Nel messaggio di conferma, scegliere Yes, Delete (Sì, elimina).

CloudFormation elimina lo stack con tutte le risorse dello stack, ad esempio l' EC2 istanza, l'argomento della notifica, il ruolo del servizio e la pipeline.

Ora che hai capito come creare un CloudFormation flusso di lavoro di base CodePipeline, puoi utilizzare il modello e gli artefatti di esempio come punto di partenza per crearne uno personalizzato.

Consulta anche

Le risorse correlate seguenti possono rivelarsi utili durante l'utilizzo di questi parametri.

- Per ulteriori informazioni sui parametri di CloudFormation azione in CodePipeline, consulta il [riferimento alla configurazione dell'azione di AWS CloudFormation distribuzione](#) nella Guida per l'AWS CodePipeline utente.
- Per i valori del modello di esempio per provider di operazioni, ad esempio per il campo Owner o i campi configuration, consulta il [Riferimento per la struttura delle operazioni](#) nella Guida per l'utente di AWS CodePipeline .
- Per scaricare esempi di modelli di stack di pipeline in formato YAML o JSON, consulta [Tutorial: Create a pipeline with the User Guide](#). AWS CloudFormationAWS CodePipeline

AWS CloudFormation riferimento alle proprietà di configurazione

Quando si crea una CodePipeline pipeline, si aggiunge un'Deployazione alla pipeline utilizzando AWS CloudFormation come provider. È quindi necessario specificare l' AWS CloudFormation azione richiamata dalla pipeline e le impostazioni dell'azione. In questo argomento vengono descritte le proprietà di configurazione di AWS CloudFormation . Per specificare le proprietà, puoi utilizzare la CodePipeline console oppure puoi creare un oggetto JSON da utilizzare per l' CodePipeline API o AWS CLI i modelli. AWS CloudFormation

Argomenti

- [Proprietà di configurazione \(console\)](#)
- [Proprietà di configurazione \(oggetto JSON\)](#)
- [Consulta anche](#)

Proprietà di configurazione (console)

La CodePipeline [console](#) mostra le proprietà di configurazione e indica le proprietà richieste in base alla modalità di azione scelta.

Note

Quando crei una pipeline, puoi specificare solo le modalità operazione Create or update a stack (Crea o aggiorna uno stack) o Create or replace a change set (Crea o sostituisci un set di modifiche). Le proprietà nella sezione Advanced (Avanzate) sono disponibili solo quando modifichi una pipeline.

Action mode (Modalità operazione)

L' AWS CloudFormation azione che viene CodePipeline richiamata durante l'elaborazione della fase associata. Scegli una delle seguenti modalità operazione:

- Create or replace a change set (Crea o sostituisci un set di modifiche) crea il set di modifiche, se non esistente, in base al nome dello stack e al modello che invii. Se il set di modifiche esiste, lo AWS CloudFormation elimina e ne crea uno nuovo.
- Create or update a stack (Crea o aggiorna uno stack) crea lo stack se lo stack specificato non esiste. Se lo stack esiste, lo AWS CloudFormation aggiorna. Utilizzate questa azione per aggiornare gli stack esistenti. CodePipeline non sostituirà lo stack.
- Delete a stack (Elimina uno stack) elimina uno stack. Se specifichi uno stack che non esiste, l'operazione viene completata senza l'eliminazione di uno stack.
- Execute a change set (Esegui un set di modifiche) esegue un set di modifiche.
- Replace a failed stack (Sostituisci uno stack non riuscito) crea lo stack se lo stack specificato non esiste. Se lo stack esiste e si trova in uno stato non riuscito (segnalato come ROLLBACK_COMPLETE, ROLLBACK_FAILED, CREATE_FAILED, DELETE_FAILED, o UPDATE_ROLLBACK_FAILED), AWS CloudFormation elimina lo stack e ne crea uno nuovo. Se lo stack non è in uno stato di errore, lo aggiorna. AWS CloudFormation Utilizza questa operazione per sostituire gli stack non riusciti senza effettuarne il ripristino o eseguire la relativa risoluzione di problemi. In genere questa modalità viene selezionata per il testing.

Stack name (Nome stack)

Il nome associato a uno stack esistente o a uno stack che desideri creare. Il nome deve essere univoco nella AWS regione in cui state creando lo stack.

 Note

Il nome di uno stack può contenere solo caratteri alfanumerici (con distinzione tra lettere maiuscole e minuscole) e trattini. Deve iniziare con un carattere alfabetico e non può avere una lunghezza superiore a 128 caratteri.

Change set name (Modifica nome set)

Il nome di un set di modifiche esistente o di uno nuovo che desideri creare per lo stack specificato.

Template (Modello)

La posizione di un file AWS CloudFormation modello, che segue il formato *ArtifactName::TemplateFileName*.

Template configuration (Configurazione modello)

Posizione di un file di configurazione del modello, nel formato *ArtifactName::TemplateConfigurationFileName*. Il file di configurazione del modello può contenere i valori dei parametri del modello, una policy relativa allo stack e i tag. Se includi informazioni sensibili, come le password, limita l'accesso a questo file. Per ulteriori informazioni, consulta [AWS CloudFormation artefatti](#).

Funzionalità

Per gli stack che contengono determinate risorse, riconoscimento esplicito dell' AWS CloudFormation eventuale creazione o aggiornamento di tali risorse. Ad esempio, devi specificare `CAPABILITY_IAM` se il modello dello stack include risorse AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [CreateStack](#) Parametri di richiesta operativa dell'API.

Se il tuo modello di stack include risorse IAM, devi specificare questa proprietà.

Puoi specificare più funzionalità.

Role name (Nome ruolo)

Il nome del ruolo del servizio IAM che AWS CloudFormation assume quando opera su risorse nello stack specificato.

Output file name (Nome file di output)

Nella sezione Avanzate, puoi specificare un nome di file di output, ad esempio `CreateStackOutput.json`, che CodePipeline viene aggiunto all'[artefatto di output](#) dopo che questo ha eseguito l'azione specificata. L'elemento di output contiene un file JSON con il contenuto della sezione del Outputs modello. AWS CloudFormation

Se non si specifica un nome, CodePipeline non genera un artefatto di output.

Parameter overrides (Sostituzioni parametri)

I parametri sono definiti nel modello e consentono di immettere valori personalizzati quando crei o aggiorni uno stack. Puoi specificare un oggetto JSON che sostituisce i valori dei parametri del modello nel file di configurazione del modello. Tutti i nomi dei parametri devono essere presenti nel modello di stack. Per ulteriori informazioni, consulta [CloudFormation Parameters sintassi del modello](#).

Note

L'oggetto JSON che può essere archiviato nella proprietà `ParameterOverrides` deve avere una dimensione massima di 1 kilobyte.

È consigliabile utilizzare il file di configurazione del modello per specificare la maggior parte dei valori dei parametri. Utilizza le sostituzioni dei parametri per specificare solo i valori dei parametri dinamici. I parametri dinamici non sono noti finché non si esegue la pipeline.

L'esempio seguente definisce un valore per il parametro `ParameterName` utilizzando una funzione di sostituzione dei parametri. La funzione recupera un valore da un CodePipeline artefatto di input. Per ulteriori informazioni sulle funzioni di sostituzione dei parametri, consulta [Utilizzo delle funzioni di sovrascrittura dei parametri con le pipeline CodePipeline](#).

```
{
  "ParameterName" : { "Fn::GetParam" : ["ArtifactName", "config-file-name.json",
    "ParamName"]}
}
```

Proprietà di configurazione (oggetto JSON)

Quando specifichi CloudFormation come provider per un'operazione di fase, definisci le seguenti proprietà nella proprietà Configuration. Utilizza l'oggetto JSON per l' CodePipelineAPI o AWS CLI i modelli. AWS CloudFormation Per alcuni esempi, consulta [Spiegazione passo per passo: creazione di una pipeline per stack di test e produzione](#) e [AWS CloudFormation riferimento alle proprietà di configurazione](#).

ActionMode

L' AWS CloudFormation azione che CodePipeline invoca quando elabora la fase associata. Specifica solo una delle seguenti modalità operazione:

- `CHANGE_SET_EXECUTE` esegue un set di modifiche.
- `CHANGE_SET_REPLACE` crea il set di modifiche, se non esiste, in base al nome dello stack e al modello che invii. Se il set di modifiche esiste, lo AWS CloudFormation elimina e ne crea uno nuovo.
- `CREATE_UPDATE` crea lo stack se lo stack specificato non esiste. Se lo stack esiste, AWS CloudFormation lo aggiorna. Utilizzate questa azione per aggiornare gli stack esistenti. CodePipeline non sostituirà lo stack.
- `DELETE_ONLY` elimina uno stack. Se specifichi uno stack che non esiste, l'operazione viene completata senza l'eliminazione di uno stack.
- `REPLACE_ON_FAILURE` crea uno stack se lo stack specificato non esiste. Se lo stack esiste e si trova in uno stato di errore (segnalato come `ROLLBACK_COMPLETE`, `ROLLBACK_FAILED`, `CREATE_FAILED`, `DELETE_FAILED`, o `UPDATE_ROLLBACK_FAILED`), AWS CloudFormation elimina lo stack e quindi ne crea uno nuovo. Se lo stack non è in uno stato di errore, lo aggiorna. AWS CloudFormation Utilizza questa operazione per sostituire automaticamente gli stack non riusciti senza effettuarne il ripristino o eseguire la relativa risoluzione di problemi. In genere questa modalità viene selezionata per il testing.

Questa proprietà è obbligatoria.

Capabilities

Per gli stack che contengono determinate risorse, riconoscimento esplicito che AWS CloudFormation potrebbe creare o aggiornare tali risorse. Ad esempio, devi specificare `CAPABILITY_IAM` se il modello dello stack include risorse AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [CreateStack](#) Parametri di richiesta operativa dell'API.

Questa proprietà è condizionale. Se il tuo modello di stack include risorse IAM, devi specificare questa proprietà.

Puoi specificare più funzionalità. L'esempio seguente aggiunge le `CAPABILITY_AUTO_EXPAND` proprietà `CAPABILITY_IAM` and al modello:

YAML

```
configuration:
  ActionMode: CHANGE_SET_REPLACE
  Capabilities: CAPABILITY_IAM,CAPABILITY_AUTO_EXPAND
  ChangeSetName: pipeline-changeset
  RoleArn: CloudFormation_Role_ARN
  StackName: my-pipeline-stack
  TemplateConfiguration: 'my-pipeline-stack::template-configuration.json'
  TemplatePath: 'my-pipeline-stack::template-export.yml'
```

JSON

```
"configuration": {
  "ActionMode": "CHANGE_SET_REPLACE",
  "Capabilities": "CAPABILITY_IAM,CAPABILITY_AUTO_EXPAND",
  "ChangeSetName": "pipeline-changeset",
  "RoleArn": "CloudFormation_Role_ARN",
  "StackName": "my-pipeline-stack",
  "TemplateConfiguration": "my-pipeline-stack::template-configuration.json",
  "TemplatePath": "my-pipeline-stack::template-export.yml"
}
```

ChangeSetName

Il nome di un set di modifiche esistente o di uno nuovo che desideri creare per lo stack specificato.

Questa proprietà è obbligatoria per le seguenti modalità operazione: `CHANGE_SET_REPLACE` e `CHANGE_SET_EXECUTE`. La proprietà viene ignorata per tutte le altre modalità operazione.

OutputFileName

Un nome per il file di output, ad esempio `CreateStackOutput.json`. CodePipeline aggiunge il file all'elemento [di output dopo aver eseguito l'azione](#) specificata. L'artefatto di output contiene un file JSON con il contenuto della sezione del `Outputs` modello. AWS CloudFormation

Questa proprietà è opzionale. Se non si specifica un nome, CodePipeline non genera un artefatto di output.

ParameterOverrides

I parametri sono definiti nel modello e consentono di immettere valori personalizzati quando crei o aggiorni uno stack. Puoi specificare un oggetto JSON che sostituisce i valori dei parametri del modello nel file di configurazione del modello. Tutti i nomi dei parametri devono essere presenti nel modello di stack. Per ulteriori informazioni, consulta [CloudFormation Parameterssintassi del modello](#).

L'esempio seguente aggiunge le sostituzioni dei parametri KeyName e InstanceType al modello:

YAML

```
configuration:
  ActionMode: CHANGE_SET_REPLACE
  Capabilities: CAPABILITY_NAMED_IAM
  ChangeSetName: pipeline-changeset
  ParameterOverrides: '{"InstanceType": "t2.small","KeyName": "my-keypair"}'
  RoleArn: CloudFormation_Role_ARN
  StackName: my-pipeline-stack
  TemplateConfiguration: 'my-pipeline-stack::template-configuration.json'
  TemplatePath: 'my-pipeline-stack::template-export.yml'
```

JSON

```
"configuration": {
  "ActionMode": "CHANGE_SET_REPLACE",
  "Capabilities": "CAPABILITY_NAMED_IAM",
  "ChangeSetName": "pipeline-changeset",
  "ParameterOverrides": "{\"InstanceType\": \"t2.small\", \"KeyName\": \"my-keypair\"}",
  "RoleArn": "CloudFormation_Role_ARN",
  "StackName": "my-pipeline-stack",
  "TemplateConfiguration": "my-pipeline-stack::template-configuration.json",
  "TemplatePath": "my-pipeline-stack::template-export.yml"
}
```

Note

La dimensione massima per l'oggetto JSON che può essere archiviato nella proprietà `ParameterOverrides` è di 1 kilobyte.

È consigliabile utilizzare il file di configurazione del modello per specificare la maggior parte dei valori dei parametri. Utilizza le sostituzioni dei parametri per specificare solo i valori dei parametri dinamici. I valori dei parametri dinamici non sono noti finché non si esegue la pipeline.

L'esempio seguente definisce un valore per il parametro `ParameterName` utilizzando una funzione di sostituzione dei parametri. La funzione recupera un valore da un `CodePipeline` artefatto di input. Per ulteriori informazioni sulle funzioni di sostituzione dei parametri, consulta [Utilizzo delle funzioni di sovrascrittura dei parametri con le pipeline CodePipeline](#).

```
{
  "ParameterName" : { "Fn::GetParam" : ["ArtifactName", "config-file-name.json",
    "ParamName"]}
}
```

Questa proprietà è opzionale.

RoleArn

Il ruolo del servizio Amazon Resource Name (ARN) del servizio IAM che AWS CloudFormation assume quando opera su risorse in uno stack.

Questa proprietà è obbligatoria per le seguenti modalità operazione: `CREATE_UPDATE`, `REPLACE_ON_FAILURE`, `DELETE_ONLY` e `CHANGE_SET_REPLACE`. `RoleArn` non viene applicata durante l'esecuzione di un set di modifiche. Se non lo utilizzi `CodePipeline` per creare il set di modifiche, assicurati che al set o allo stack di modifiche sia associato un ruolo.

StackName

Il nome di uno stack esistente o che desideri creare.

Questa proprietà è obbligatoria per tutte le altre modalità operazione.

TemplateConfiguration

`TemplateConfiguration` è il file di configurazione del modello. Includi il file in un artefatto di input per questa operazione. Il nome del file di configurazione del modello segue questo formato:

Artifactname::TemplateConfigurationFileName

Artifactname è il nome dell'artefatto di input così come appare in. CodePipeline Ad esempio, una fase di origine con il nome di artefatto di SourceArtifact e un nome file di test-configuration.json crea un nome TemplateConfiguration come mostrato in questo esempio:

```
"TemplateConfiguration": "SourceArtifact::test-configuration.json"
```

Il file di configurazione del modello può contenere i valori dei parametri del modello e una policy relativa allo stack. Se includi informazioni sensibili, come le password, limita l'accesso a questo file. Per un esempio di file di configurazione del modello, consulta [AWS CloudFormation artefatti](#).

Questa proprietà è opzionale.

TemplatePath

TemplatePath rappresenta il file AWS CloudFormation modello. Includi il file in un artefatto di input per questa operazione. Il nome del file segue questo formato:

Artifactname::TemplateFileName

Artifactname è il nome dell'artefatto di input così come appare in. CodePipeline Ad esempio, una fase di origine con il nome di artefatto di SourceArtifact e un nome file di template.yaml crea un nome TemplatePath come mostrato in questo esempio:

```
"TemplatePath": "SourceArtifact::template.yaml"
```

Questa proprietà è obbligatoria per le seguenti modalità operazione: CREATE_UPDATE, REPLACE_ON_FAILURE e CHANGE_SET_REPLACE. La proprietà viene ignorata per tutte le altre modalità operazione.

Consulta anche

Le risorse correlate seguenti possono rivelarsi utili durante l'utilizzo di questi parametri.

- Per ulteriori informazioni sui parametri di CloudFormation azione in CodePipeline, vedere il [riferimento alla configurazione dell'azione di AWS CloudFormation distribuzione](#) nella Guida per l'AWS CodePipeline utente.

- Per i valori del modello di esempio per provider di operazioni, ad esempio per il campo Owner o i campi configuration, consulta il [Riferimento per la struttura delle operazioni](#) nella Guida per l'utente di AWS CodePipeline .
- Per scaricare esempi di modelli di stack di pipeline in formato YAML o JSON, consulta [Tutorial: Create a pipeline with the User Guide](#). AWS CloudFormationAWS CodePipeline

AWS CloudFormation artefatti

CodePipeline esegue attività sugli artefatti come esegue una pipeline. CodePipeline Infatti AWS CloudFormation, gli artefatti possono includere un file modello di stack, un file di configurazione del modello o entrambi. CodePipeline utilizza questi artefatti per lavorare con AWS CloudFormation pile e set di modifiche.

Se utilizzi Amazon Simple Storage Service (Amazon S3) come repository di origine, devi comprimere i file del modello e della configurazione del modello in un singolo file prima di caricarli su un bucket S3. Per altri archivi, ad esempio GitHub and AWS CodeCommit, carica gli artefatti senza comprimerli. Per ulteriori informazioni, consulta [Creare una pipeline, fasi e azioni](#) nella Guida per l'utente.AWS CodePipeline

Puoi aggiungere tutti i file di cui hai bisogno al repository. Ad esempio, puoi includere due diverse configurazioni per lo stesso modello: una per la configurazione di test e l'altra per la configurazione di produzione.

Questo argomento descrive ogni tipo di artefatto.

Argomenti

- [File del modello dello stack](#)
- [File di configurazione del modello](#)
- [Consulta anche](#)

File del modello dello stack

Un file modello di stack definisce le risorse per il provisioning e la AWS CloudFormation configurazione. Questi file sono gli stessi file modello utilizzati quando si creano o si aggiornano gli stack utilizzando. AWS CloudFormation Puoi utilizzare i modelli in formato JSON o YAML. Per ulteriori informazioni sui modelli, consulta [CloudFormation sezioni modello](#).

File di configurazione del modello

Un file di configurazione del modello è un file di testo in formato JSON che può specificare i valori di parametro del modello, una [policy dello stack](#) e tag. Utilizza questi file di configurazione per specificare i valori del parametro o una policy dello stack per uno stack. Tutti i valori dei parametri specificati devono essere dichiarati nel modello associato.

Se includi informazioni sensibili, come le password, limita l'accesso a questo file. Ad esempio, se carichi l'artefatto su un bucket S3, utilizza le [policy del bucket S3 o le policy utente](#) per limitare l'accesso.

Per creare un file di configurazione, utilizza il seguente formato:

```
{
  "Parameters" : {
    "NameOfTemplateParameter" : "ValueOfParameter",
    ...
  },
  "Tags" : {
    "TagKey" : "TagValue",
    ...
  },
  "StackPolicy" : {
    "Statement" : [
      StackPolicyStatement
    ]
  }
}
```

L'esempio seguente specifica TestEC2Key per il parametro KeyName, aggiunge un tag Department il cui valore è Marketing e aggiunge una policy dello stack che consente tutte le operazioni di aggiornamento tranne per un aggiornamento che elimina una risorsa.

```
{
  "Parameters" : {
    "KeyName" : "TestEC2Key"
  },
  "Tags" : {
    "Department" : "Marketing"
  },
  "StackPolicy" : {
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "NotAction" : "Update:Delete",
    "Principal": "*",
    "Resource" : "*"
  }
]
}
```

Consulta anche

Le risorse correlate seguenti possono rivelarsi utili durante l'utilizzo di questi parametri.

- Per ulteriori informazioni sui parametri di CloudFormation azione in CodePipeline, consulta il [riferimento alla configurazione dell'azione di AWS CloudFormation distribuzione nella Guida](#) per l'AWS CodePipeline utente.
- Per i valori del modello di esempio per provider di operazioni, ad esempio per il campo Owner o i campi configuration, consulta il [Riferimento per la struttura delle operazioni](#) nella Guida per l'utente di AWS CodePipeline .
- Per scaricare esempi di modelli di stack di pipeline in formato YAML o JSON, consulta [Tutorial: Create a pipeline with the User Guide](#). AWS CloudFormationAWS CodePipeline

Utilizzo delle funzioni di sovrascrittura dei parametri con le pipeline CodePipeline

In una CodePipeline fase, potete specificare le [sostituzioni dei parametri per le azioni](#). AWS CloudFormation Le sostituzioni dei parametri consentono di specificare valori dei parametri del modello che sostituiscono i valori in un file di configurazione del modello. AWS CloudFormation fornisce funzioni che consentono di specificare valori dinamici (valori sconosciuti fino all'esecuzione della pipeline).

Argomenti

- [Fn::GetArtifactAtt](#)
- [Fn::GetParam](#)
- [Consulta anche](#)

Fn::GetArtifactAtt

La funzione `Fn::GetArtifactAtt` recupera il valore di un attributo da un artefatto di input, come il nome del bucket S3 in cui l'artefatto viene archiviato. Utilizzate questa funzione per specificare gli attributi di un artefatto, come il nome del file o Amazon S3 il nome del bucket.

Quando esegui una pipeline, CodePipeline copia e scrive i file nell'archivio degli artefatti della pipeline (un bucket S3). CodePipeline genera i nomi dei file nell'archivio degli artefatti. Tali nomi file sono sconosciuti prima dell'esecuzione della pipeline.

Ad esempio, nella vostra pipeline, potreste avere una fase di origine in cui CodePipeline copia il codice sorgente AWS Lambda della funzione nell'archivio degli artefatti. Nella fase successiva, si dispone di un AWS CloudFormation modello che crea la funzione Lambda, ma AWS CloudFormation richiede il nome del file per creare la funzione. È necessario utilizzare la funzione `Fn::GetArtifactAtt` per passare il nome esatto del bucket S3 e del file.

Sintassi

Usa la sintassi seguente per recuperare il valore di un attributo di un artefatto.

```
{ "Fn::GetArtifactAtt" : [ "artifactName", "attributeName" ] }
```

`artifactName`

Il nome dell'artefatto di input. È necessario dichiarare questo artefatto come input per l'operazione associata.

`attributeName`

Il nome dell'attributo dell'artefatto di cui vuoi recuperare il valore. Per ulteriori informazioni sull'attributo di ogni artefatto, consulta la sezione [Attributi](#) di seguito.

Esempio

Le seguenti sostituzioni di parametro specificano i parametri `BucketName` e `ObjectKey` recuperando il nome del bucket S3 e il nome file dell'artefatto `LambdaFunctionSource`. Questo esempio presuppone che il codice sorgente della funzione CodePipeline Lambda sia stato copiato e salvato come artefatto, ad esempio come parte di uno stadio sorgente.

```
{
```

```
"BucketName" : { "Fn::GetArtifactAtt" : ["LambdaFunctionSource", "BucketName"] },
"ObjectKey" : { "Fn::GetArtifactAtt" : ["LambdaFunctionSource", "ObjectKey"] }
}
```

Attributes

Puoi recuperare i seguenti attributi per un artefatto.

BucketName

Il nome del bucket S3 in cui l'artefatto viene archiviato.

ObjectKey

Il nome del .zip file che contiene l'elemento generato da, ad esempio. CodePipeline
1ABCyZZ.zip

URL

L'URL Amazon Simple Storage Service (Amazon S3) dell'artefatto, ad esempio `https://s3.us-west-2.amazonaws.com/artifactstorebucket-yivczw8jma0c/test/TemplateSo/1ABCyZZ.zip`.

Fn::GetParam

La funzione `Fn::GetParam` restituisce un valore da una coppia chiave-valore in un file in formato JSON. Il file JSON deve essere incluso in un artefatto.

Utilizzate questa funzione per recuperare i valori di output da uno AWS CloudFormation stack e usarli come input per un'altra azione. Ad esempio, se specificate un nome di file di output per un'AWS CloudFormation azione, CodePipeline salva l'output in un file JSON e quindi lo aggiunge al file dell'elemento di output. .zip Utilizza la funzione `Fn::GetParam` per recuperare il valore di output e utilizzarlo come input per un'altra operazione.

Sintassi

Utilizza la sintassi seguente per recuperare un valore da una coppia chiave-valore.

```
{ "Fn::GetParam" : [ "artifactName", "JSONFileName", "keyName" ] }
```

artifactName

Il nome dell'artefatto che deve essere incluso come artefatto di input per l'azione associata.

JSONFileName

Il nome di un file JSON contenuto nell'artefatto.

keyName

Il nome della chiave di cui vuoi recuperare il valore.

Esempi

Gli esempi seguenti illustrano come utilizzare la funzione `Fn::GetParam` in una sostituzione di parametro.

Sintassi

La seguente sostituzione di parametro specifica il parametro `WebSiteURL` recuperando il valore della chiave `URL` dal file `stack-output.json` che si trova nell'artefatto `WebStackOutput`.

```
{
  "WebSiteURL" : { "Fn::GetParam" : ["WebStackOutput", "stack-output.json", "URL"]}
}
```

AWS CloudFormation frammenti di modello

I seguenti frammenti AWS CloudFormation di modello, tratti da una `CodePipeline` pipeline, mostrano come passare gli output dello stack. Questi frammenti mostrano due fasi di definizione della pipeline. La prima fase crea uno stack e ne salva gli output nel file `TestOutput.json` nell'artefatto `StackAOutput`. Questi valori sono specificate dalle proprietà `OutputFileName` e `OutputArtifacts`.

Il nome dell'artefatto di input di origine per le fasi è `TemplateSource`. Il nome file del modello di stack è `teststackA.yaml` e il nome del file di configurazione è `test-configuration.json`. In entrambe le fasi, questi valori sono specificati per le proprietà `TemplateConfiguration` e `TemplatePath` come mostrato di seguito:

```
TemplateConfiguration: TemplateSource::test-configuration.json
TemplatePath: TemplateSource::teststackA.yaml
```

Example Fase di creazione dello stack A

```
- Name: CreateTestStackA
  Actions:
    - Name: CloudFormationCreate
      ActionTypeId:
        Category: Deploy
        Owner: AWS
        Provider: CloudFormation
        Version: '1'
      Configuration:
        ActionMode: CREATE_UPDATE
        Capabilities: CAPABILITY_IAM
        OutputFileName: TestOutput.json
        RoleArn: !GetAtt [CFNRole, Arn]
        StackName: StackA
        TemplateConfiguration: TemplateSource::test-configuration.json
        TemplatePath: TemplateSource::teststackA.yaml
      InputArtifacts:
        - Name: TemplateSource
      OutputArtifacts:
        - Name: StackAOutput
      RunOrder: '1'
```

In una fase seguente, lo stack B utilizza gli output dello stack A. Nella proprietà `ParameterOverrides`, l'esempio utilizza la funzione `Fn::GetParam` per specificare il parametro `StackBInputParam`. Il valore risultante è il valore associato alla chiave `StackAOutputName`.

Example Fase di creazione dello stack B

```
- Name: CreateTestStackB
  Actions:
    - Name: CloudFormationCreate
      ActionTypeId:
        Category: Deploy
        Owner: AWS
        Provider: CloudFormation
        Version: '1'
      Configuration:
        ActionMode: CREATE_UPDATE
        Capabilities: CAPABILITY_IAM
        RoleArn: !GetAtt [CFNRole, Arn]
        StackName: StackB
```



```
TemplateConfiguration: TemplateSource::test-configuration.json
TemplatePath: TemplateSource::teststackB.yaml
ParameterOverrides: |
  {
    "StackBInputParam" : { "Fn::GetParam" : ["StackA0Output", "TestOutput.json",
"StackA0OutputName"]}
  }
InputArtifacts:
  - Name: TemplateSource
  - Name: StackA0Output
RunOrder: '1'
```

Consulta anche

Le risorse correlate seguenti possono rivelarsi utili durante l'utilizzo di questi parametri.

- Per ulteriori informazioni sui parametri di CloudFormation azione in CodePipeline, consulta il riferimento alla [configurazione dell'azione di AWS CloudFormation distribuzione nella Guida](#) per l'utente.AWS CodePipeline
- Per i valori del modello di esempio per provider di operazioni, ad esempio per il campo Owner o i campi configuration, consulta il [Riferimento per la struttura delle operazioni](#) nella Guida per l'utente di AWS CodePipeline .
- Per scaricare esempi di modelli di stack di pipeline in formato YAML o JSON, consulta [Tutorial: Create a pipeline with the User Guide](#). AWS CloudFormationAWS CodePipeline

La guida AWS CloudFormation di riferimento ai modelli

Informazioni dettagliate sulle risorse e sui componenti disponibili per la creazione AWS CloudFormation di modelli sono ora disponibili nella [AWS CloudFormation Template Reference Guide](#). Questa guida funge da riferimento tecnico per i modelli e integra i contenuti introduttivi della Guida per l' CloudFormation utente.

La guida AWS CloudFormation di riferimento ai modelli fornisce dettagli su:

- Tipi di risorse e relative proprietà
- DeletionPolicy e altri attributi a livello di risorsa
- Funzioni intrinseche, come e Ref Sub
- Trasformazioni (macro) CloudFormation
- Script di supporto, ad esempio configurazione EC2
- Definizioni dei tipi di risorse leggibili dalla macchina

Questa guida viene aggiornata regolarmente per riflettere:

- Nuovi tipi di risorsa
- Modifiche alle proprietà
- Nuovi valori restituiti
- Aggiornamenti della documentazione

Sicurezza in AWS CloudFormation

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS CloudFormation, consulta [AWS Servizi nell'ambito del programma di conformitàAWS](#) .
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS CloudFormation. I seguenti argomenti mostrano come configurare per AWS CloudFormation soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS CloudFormation le tue risorse.

Argomenti

- [Proteggi CloudFormation gli stack dall'eliminazione](#)
- [Impedire gli aggiornamenti delle risorse stack](#)
- [Protezione dei dati in AWS CloudFormation](#)
- [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#)
- [Registrazione delle chiamate AWS CloudFormation API con AWS CloudTrail](#)
- [Sicurezza dell'infrastruttura in AWS CloudFormation](#)
- [Resilienza in AWS CloudFormation](#)
- [Convalida della conformità per AWS CloudFormation](#)
- [Analisi della configurazione e delle vulnerabilità in AWS CloudFormation](#)

- [Best practice di sicurezza per CloudFormation](#)
- [Accesso CloudFormation tramite un endpoint di interfaccia \(AWS PrivateLink\)](#)

Proteggi CloudFormation gli stack dall'eliminazione

Puoi impedire che uno stack venga eliminato accidentalmente abilitando la protezione da cessazione sullo stack. Se un utente tenta di eliminare uno stack con protezione da cessazione abilitata, l'eliminazione ha esito negativo e lo stack, incluso lo stato, rimane invariato. Puoi abilitare la protezione da cessazione sullo stack quando lo crei. Per impostazione di default, la protezione da cessazione è disabilitata. È possibile impostare la protezione dalla terminazione su uno stack con qualsiasi stato tranne o. DELETE_IN_PROGRESS DELETE_COMPLETE

L'attivazione o la disabilitazione della protezione da terminazione su uno stack trasferisce la stessa scelta anche a tutti gli stack annidati appartenenti a quello stack. Non è possibile abilitare o disabilitare la protezione da terminazione direttamente su uno stack nidificato. Se un utente cerca di eliminare direttamente uno stack nidificato appartenente a uno stack con protezione da terminazione abilitata, l'operazione ha esito negativo e lo stack nidificato rimane invariato.

Tuttavia, se un utente esegue un aggiornamento dello stack che comporterebbe l'eliminazione dello stack nidificato, AWS CloudFormation elimina quest'ultimo di conseguenza.

La protezione da cessazione è diversa dalla disabilitazione del rollback. La prima si applica solo ai tentativi di eliminazione degli stack, mentre la seconda si applica al rollback automatico nei casi in cui la creazione dello stack ha esito negativo.

Per abilitare la protezione da cessazione durante la creazione di uno stack

Nella pagina Specify stack options (Specifica opzioni stack) della procedura guidata Create stack (Crea stack), in Advanced options (Opzioni avanzate), espandere la sezione Termination Protection (Protezione da cessazione) e selezionare Enable (Abilita). Per ulteriori informazioni, consulta [Configurare le opzioni dello stack](#).

Per abilitare o disabilitare la protezione da cessazione su uno stack esistente

1. [Accedi e apri la console all'indirizzo AWS Management Console /cloudformazione. AWS CloudFormation https://console.aws.amazon.com](#)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Selezionare lo stack desiderato.

 Note

Se accanto al nome dello stack compare la dicitura NESTED (NIDIFICATO), si tratta di uno stack nidificato. È possibile modificare la protezione da cessazione soltanto sullo stack radice al quale appartiene lo stack nidificato.

4. Nel riquadro dettagli dello stack, selezionare Stack actions (Operazioni stack), quindi Edit termination protection (Modifica protezione da cessazione).

CloudFormation visualizza la finestra di dialogo Modifica protezione dalla terminazione.

5. Scegliere Enable (Abilita) o Disable (Disabilita), quindi selezionare Save (Salva).

Per abilitare o disabilitare la protezione da cessazione su uno stack nidificato

Se accanto al nome dello stack compare la dicitura NESTED (NIDIFICATO), si tratta di uno stack nidificato. È possibile modificare la protezione da cessazione soltanto sullo stack radice al quale appartiene lo stack nidificato. Per modificare la protezione da cessazione sullo stack radice:

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformazione>.
2. Nella barra di navigazione nella parte superiore dello schermo, scegli il tuo. Regione AWS
3. Selezionare lo stack nidificato desiderato.
4. Nel riquadro Stack info (Info stack), nella sezione Overview (Panoramica), selezionare il nome dello stack presente in elenco come Root stack (Stack root).

CloudFormation visualizza i dettagli dello stack per lo stack principale.

5. Scegliere Stack actions (Operazioni stack), quindi scegliere Edit Termination Protection (Modifica protezione da cessazione).

CloudFormation visualizza la finestra di dialogo Modifica protezione dalla terminazione.

6. Scegliere Enable (Abilita) o Disable (Disabilita), quindi selezionare Save (Salva).

Per abilitare o disabilitare la protezione da interruzione utilizzando la riga di comando

Utilizzo dell'[update-termination-protection](#) comando.

Controllare chi può modificare la protezione da cessazione sugli stack

Per abilitare o disabilitare la protezione da cessazione sullo stack, è necessaria l'autorizzazione per l'operazione `cloudformation:UpdateTerminationProtection`. Ad esempio, la policy di seguito consente agli utenti di abilitare o disabilitare la protezione da cessazione sugli stack.

Per ulteriori informazioni sulla specificazione delle autorizzazioni in AWS CloudFormation, vedere. [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#)

Example Un esempio di policy che assegna le autorizzazioni per modificare la protezione da cessazione per lo stack

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "cloudformation:UpdateTerminationProtection"
    ],
    "Resource": "*"
  }]
}
```

Impedire gli aggiornamenti delle risorse stack

Quando si crea uno stack, sono consentite tutte le operazioni di aggiornamento su tutte le risorse. Per impostazione predefinita, chiunque abbia le autorizzazioni per aggiornare lo stack può aggiornare tutte le risorse nello stack. Durante un aggiornamento, alcune risorse potrebbero richiedere un'interruzione o essere completamente sostituite, con conseguente creazione di un nuovo storage fisico o completamente nuovo. IDs È possibile impedire che le risorse stack vengano involontariamente aggiornate o eliminate durante un aggiornamento dello stack utilizzando le policy stack. Una policy stack è un documento JSON che definisce le azioni di aggiornamento che possono essere eseguite su risorse definite.

Dopo aver impostato una policy stack, tutte le risorse nello stack vengono protette per impostazione predefinita. Per permettere gli aggiornamenti di risorse specifiche, è necessario specificare una dichiarazione `Allow` esplicita per tali risorse nella policy stack. È possibile definire una sola policy stack per stack, ma è possibile proteggere più risorse all'interno di una singola policy. Una policy

stack si applica a tutti gli utenti CloudFormation che tentano di aggiornare lo stack. Non è possibile associare policy stack diverse a utenti diversi.

Una policy stack si applica solo durante gli aggiornamenti dello stack. Non fornisce i controlli di accesso, come per esempio una policy AWS Identity and Access Management (IAM). Utilizzare una policy stack solo come meccanismo a prova di errore per evitare gli aggiornamenti accidentali di specifiche risorse stack. Per controllare l'accesso a AWS risorse o azioni, usa IAM.

Argomenti

- [Esempio di policy stack](#)
- [Definizione di una policy stack](#)
- [Impostazione di una policy stack](#)
- [Aggiornamento delle risorse protette](#)
- [Modifica di una policy stack](#)
- [Ulteriori esempi di policy stack](#)

Esempio di policy stack

L'esempio di stack policy seguente impedisce gli aggiornamenti della risorsa ProductionDatabase:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "LogicalResourceId/ProductionDatabase"
    }
  ]
}
```

Quando si imposta una policy stack, tutte le risorse vengono protette per impostazione predefinita. Per permettere gli aggiornamenti di tutte le risorse, aggiungiamo una dichiarazione Allow che permette tutte le azioni su tutte le risorse. Anche se la dichiarazione Allow specifica tutte le risorse, la dichiarazione esplicita Deny la sostituisce per la risorsa con l'ID logico ProductionDatabase. Questa dichiarazione Deny impedisce tutte le azioni di aggiornamento, come per esempio la sostituzione o l'eliminazione, sulla risorsa ProductionDatabase.

L'elemento Principal è necessario, ma supporta solo il carattere jolly (*), il che significa che la dichiarazione si applica a tutti i [principali](#).

Note

Durante un aggiornamento dello stack, aggiorna CloudFormation automaticamente le risorse che dipendono da altre risorse aggiornate. Ad esempio, CloudFormation aggiorna una risorsa che fa riferimento a una risorsa aggiornata. CloudFormation non apporta modifiche fisiche, come l'ID della risorsa, alle risorse aggiornate automaticamente, ma se a tali risorse è associata una policy di stack, è necessario disporre dell'autorizzazione per aggiornarle.

Definizione di una policy stack

Quando si crea uno stack, non è impostata nessuna policy stack, quindi sono consentite tutte le operazioni di aggiornamento su tutte le risorse. Per proteggere le risorse stack dalle operazioni di aggiornamento, definire una policy stack e quindi impostarla sullo stack. Una politica dello stack è un documento JSON che definisce le azioni di aggiornamento dello CloudFormation stack che CloudFormation gli utenti possono eseguire e le risorse a cui tali azioni si applicano. Si imposta la policy stack al momento della creazione di uno stack, specificando un file di testo che contiene la policy stack o digitandola. Quando si imposta una policy stack sullo stack, qualsiasi aggiornamento non esplicitamente consentito viene negato per impostazione predefinita.

Una policy stack si definisce in cinque elementi: Effect, Action, Principal, Resource e Condition. Il seguente pseudo codice mostra la sintassi di policy stack.

```
{
  "Statement" : [
    {
      "Effect" : "Deny_or-Allow",
      "Action" : "update_actions",
      "Principal" : "*",
```



```
"Resource" : "LogicalResourceId/resource_logical_ID",
"Condition" : {
  "StringEquals_or_StringLike" : {
    "ResourceType" : [resource_type, ...]
  }
}
]
```

Effect

Determina se le azioni specificate vengono negate o consentite sulla/e risorsa/e specificata/e. È possibile specificare solo Deny o Allow, come per esempio:

```
"Effect" : "Deny"
```

Important

Se una policy stack include istruzioni sovrapposte (sia consentendo sia negando gli aggiornamenti di una risorsa), una dichiarazione Deny sostituisce sempre una dichiarazione Allow. Per garantire che una risorsa venga protetta, utilizzare una dichiarazione Deny per tale risorsa.

Azione

Specifica le operazioni di aggiornamento che sono negate o consentite:

Update:Modify

Specifica le operazioni di aggiornamento durante le quali le risorse potrebbero non avere interruzioni o avere alcune interruzioni durante l'applicazione delle modifiche. Tutte le risorse mantengono la loro fisicità. IDs

Update:Replace

Specifica le operazioni di aggiornamento durante le quali le risorse vengono ricreate. CloudFormation crea una nuova risorsa con gli aggiornamenti specificati poi elimina la risorsa precedente. Poiché la risorsa viene ricreata, l'ID fisico della nuova risorsa potrebbe essere diverso.

Update:Delete

Specifica le operazioni di aggiornamento durante le quali le risorse vengono rimosse. Gli aggiornamenti che rimuovono completamente le risorse da un modello stack richiedono questa operazione.

Aggiorna:*

Specifica tutte le operazioni di aggiornamento. L'asterisco è una carta jolly che rappresenta tutte le operazioni di aggiornamento.

L'esempio seguente mostra come specificare solo le operazioni di sostituzione ed eliminazione:

```
"Action" : ["Update:Replace", "Update:Delete"]
```

Per permettere tutte le operazioni di aggiornamento tranne una, utilizzare `NotAction`. Per esempio, per permettere tutte le operazioni di aggiornamento tranne `Update:Delete`, utilizzare `NotAction`, come illustrato in questo esempio:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : "Update:Delete",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Principale

L'elemento `Principal` specifica l'entità a cui si applica la policy. Tale elemento è necessario ma supporta solo il carattere jolly (*), il che significa che la policy si applica a tutti i [principali](#).

Risorsa

Specifica la logica IDs delle risorse a cui si applica la politica. Per specificare i tipi di risorse, utilizzare l'elemento `Condition`.

Per specificare una singola risorsa, utilizzare il suo ID logico. Per esempio:

```
"Resource" : ["LogicalResourceId/myEC2instance"]
```

È possibile utilizzare una wild card con logica IDs. Per esempio, se si utilizza un prefisso comune di ID logico per tutte le risorse correlate, è possibile specificarle tutte con un carattere jolly:

```
"Resource" : ["LogicalResourceId/CriticalResource*"]
```

È inoltre possibile utilizzare un elemento Not con le risorse. Per esempio, per permettere gli aggiornamenti di tutte le risorse tranne una, utilizzare un elemento NotResource per proteggere tale risorsa:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "NotResource" : "LogicalResourceId/ProductionDatabase"
    }
  ]
}
```

Quando si imposta una policy stack, qualsiasi aggiornamento non esplicitamente consentito viene negato. Consentendo gli aggiornamenti di tutte le risorse ad eccezione della risorsa ProductionDatabase, si rifiutano gli aggiornamenti alla risorsa ProductionDatabase.

Condizioni

Specifica il tipo di risorsa a cui si applica la policy. Per specificare la logica IDs di risorse specifiche, usa l'Resourceelemento.

È possibile specificare un tipo di risorsa, ad esempio tutte le istanze DB EC2 e RDS, come illustrato nell'esempio seguente:

```
{
  "Statement" : [
    {
      "Effect" : "Deny",
      "Principal" : "*",
      "Action" : "Update:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "ResourceType" : ["AWS::EC2::Instance", "AWS::RDS::DBInstance"]
    }
},
{
    "Effect" : "Allow",
    "Principal" : "*",
    "Action" : "Update:*",
    "Resource" : "*"
}
]
```

L'Allowistruzione concede le autorizzazioni di aggiornamento a tutte le risorse e l'Denyistruzione nega gli aggiornamenti alle EC2 istanze DB RDS. La dichiarazione Deny sostituisce sempre le operazioni di permesso.

È possibile utilizzare un carattere jolly con i tipi di risorse. Ad esempio, puoi negare le autorizzazioni di aggiornamento a tutte le EC2 risorse Amazon, come istanze, gruppi di sicurezza e sottoreti, utilizzando una wild card, come mostrato nell'esempio seguente:

```
"Condition" : {
    "StringLike" : {
        "ResourceType" : ["AWS::EC2:*"]
    }
}
```

Bisogna utilizzare la condizione StringLike quando si utilizzano i caratteri jolly.

Impostazione di una policy stack

Puoi utilizzare la console o applicare una politica di stack quando crei uno AWS CLI stack. È inoltre possibile utilizzare la AWS CLI per applicare una politica di stack a uno stack esistente. Dopo aver applicato una policy di stack, non è possibile rimuoverla dallo stack, ma è possibile utilizzarla per modificarla. AWS CLI

Le policy dello stack si applicano a tutti CloudFormation gli utenti che tentano di aggiornare lo stack. Non è possibile associare policy stack diverse a utenti diversi.

Per informazioni sulla scrittura delle policy stack, consulta [Definizione di una policy stack](#).

Per impostare una policy stack quando si crea uno stack (console)

1. [Apri la AWS CloudFormation console in /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Nella barra di navigazione nella parte superiore dello schermo, scegli in cui Regione AWS creare lo stack.
3. Nella pagina CloudFormation Pile, scegli Crea pila.
4. Nella procedura guidata Create Stack (Crea stack), nella pagina Configure stack options (Configura opzioni stack), espandere la sezione Advanced (Avanzate), quindi scegliere Stack policy (Policy stack).
5. Specificare la policy dello stack:
 - Per scrivere una policy direttamente nella console, scegliere Enter stack policy (Inserisci policy stack) e quindi la policy di stack direttamente nel campo di testo.
 - Per usare una policy definita in un file separato, scegliere Upload a file (Carica un file), quindi Choose file (Scegli file) per selezionare il file contenente la policy di stack.

Per impostare una policy stack quando crei uno stack (AWS CLI)

- Utilizzare il comando [create-stack](#) con l'opzione `--stack-policy-body` per digitare in una policy modificata o l'opzione `--stack-policy-url` per specificare un file contenente la policy.

Per impostare una politica di stack su uno stack esistente (solo)AWS CLI

- Utilizzare il comando [set-stack-policy](#) con l'opzione `--stack-policy-body` per digitare in una policy modificata o l'opzione `--stack-policy-url` per specificare un file contenente la policy.

Note

Per aggiungere una policy a uno stack esistente, è necessario disporre dell'autorizzazione all'azione. CloudFormation [SetStackPolicy](#)

Aggiornamento delle risorse protette

Per aggiornare le risorse protette, creare una policy temporanea che sovrascriva la policy stack e permetta gli aggiornamenti di tali risorse. Specificare la policy di sostituzione quando si aggiorna lo stack. La policy di sostituzione non modifica in modo permanente la policy stack.

Per aggiornare le risorse protette, è necessario disporre dell'autorizzazione per utilizzare l'CloudFormation [SetStackPolicy](#)azione. Per informazioni sull'impostazione delle autorizzazioni CloudFormation, consulta [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#).

Note

Durante un aggiornamento dello stack, aggiorna CloudFormation automaticamente le risorse che dipendono da altre risorse aggiornate. Ad esempio, CloudFormation aggiorna una risorsa che fa riferimento a una risorsa aggiornata. CloudFormation non apporta modifiche fisiche, come l'ID delle risorse, alle risorse aggiornate automaticamente, ma se a tali risorse è associata una policy di stack, è necessario disporre dell'autorizzazione per aggiornarle.

Per aggiornare una risorsa protetta (console)

1. [Apri la console in AWS CloudFormation /cloudformation. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. Selezionare lo stack che si desidera aggiornare, selezionare Stack actions (Operazioni stack), poi Update Stack (Aggiorna stack).
3. Se non è stato modificato il modello di stack, selezionare Use current template (Utilizza modello corrente), quindi fare clic su Next (Avanti). Se è stato modificato il modello, selezionare Replace current template (Sostituisci modello corrente) e specificare la posizione del modello aggiornato nella sezione Specify template (Specificare modello):
 - Per un modello memorizzato localmente nel computer, selezionare Upload a template file (Carica un file modello). Scegliere Choose File (Scegli file) per accedere al file e selezionarlo e fare clic su Next (Avanti).
 - Per un modello archiviato in un bucket Amazon S3, selezionare URL Amazon S3. Inserire o incollare l'URL per il modello e fare clic su Next (Avanti).

Se hai un modello in un bucket abilitato al controllo delle versioni, puoi specificare una versione specifica del modello aggiungendola all'URL. ?versionId=**version-id** Per ulteriori informazioni, consulta [Lavorare con oggetti in un bucket abilitato al rilascio di versioni nella Guida](#) per l'utente di Amazon Simple Storage Service.

4. Se il modello contiene parametri, nella pagina Specify stack details (Specifica dettagli stack) immettere o modificare i valori di parametro, quindi selezionare Next (Avanti).

CloudFormation popola ogni parametro con il valore attualmente impostato nello stack ad eccezione dei parametri dichiarati con l'attributo. `NoEcho` È possibile utilizzare i valori correnti per questi parametri scegliendo `Use existing value` (Utilizza valore esistente).

Per ulteriori informazioni sull'utilizzo per `NoEcho` mascherare informazioni sensibili e sull'utilizzo di parametri dinamici per la gestione dei segreti, consulta la procedura [Non incorporare le credenziali nei modelli](#) consigliata.

5. Specificare una policy di stack di sostituzione.
 - a. Nella pagina `Configure stack options` (Configura opzioni stack), nella sezione `Advanced options` (Opzioni avanzate), selezionare `Stack policy` (Policy stack).
 - b. Selezionare `Upload a file` (Carica un file).
 - c. Fare clic su `Choose file` (Scegli file) e passare al file che contiene le policy di stack di sostituzione o digitare una policy.
 - d. Scegli `Next` (Successivo).

Le policy di sostituzione devono specificare una dichiarazione `Allow` per le risorse protette che si desidera aggiornare. Per esempio, per aggiornare tutte le risorse protette, specificare una policy di sostituzione temporanea che permetta tutti gli aggiornamenti:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Note

CloudFormation applica la politica di esclusione solo durante questo aggiornamento. La policy di sostituzione non modifica in modo permanente la policy stack. Per modificare una policy stack, consulta [Modifica di una policy stack](#).

6. Esaminare le informazioni stack e le modifiche inviate.

Verificare di aver inviato le informazioni corrette, come i valori dei parametri o l'URL del modello corretti. Se il modello contiene risorse IAM, scegliere `I acknowledge that this template may create IAM resources` (Acconsento che questo modello possa creare risorse IAM) per specificare che si desidera utilizzare risorse IAM nel modello. Per ulteriori informazioni, consulta [Accettazione delle risorse IAM nei modelli CloudFormation](#).

Nella sezione Visualizza l'anteprima delle modifiche, verifica che CloudFormation vengano apportate tutte le modifiche che ti aspetti. Ad esempio, verifica che CloudFormation aggiunga, rimuova e modifichi le risorse che intendevi aggiungere, rimuovere o modificare. CloudFormation genera questa anteprima creando un set di modifiche per lo stack. Per ulteriori informazioni, consulta [Aggiorna CloudFormation gli stack utilizzando i set di modifiche](#).

7. Se le modifiche sono quelle desiderate, fare clic su Update (Aggiorna).

Note

A questo punto, è possibile visualizzare il set di modifiche per rivedere gli aggiornamenti proposti più accuratamente. A tale scopo, fate clic su Visualizza set di modifiche anziché su Aggiorna. CloudFormation visualizza il set di modifiche generato in base agli aggiornamenti. Quando si è pronti per eseguire l'aggiornamento dello stack, fare clic su Execute (Esegui).

CloudFormation visualizza la pagina dei dettagli dello stack relativo allo stack. Lo stato del tuo stack è ora pari a `UPDATE_IN_PROGRESS`. Dopo aver CloudFormation completato con successo l'aggiornamento dello stack, imposta lo stato dello stack su `UPDATE_COMPLETE`.

Se l'aggiornamento dello stack fallisce CloudFormation, ripristina automaticamente le modifiche e imposta lo stato dello stack su `UPDATE_ROLLBACK_COMPLETE`.

Per aggiornare una risorsa protetta (AWS CLI)

- Utilizzare il comando [update-stack](#) con l'opzione `--stack-policy-during-update-body` per digitare in una policy modificata o l'opzione `--stack-policy-during-update-url` per specificare un file contenente la policy.

 Note

CloudFormation applica la politica di esclusione solo durante questo aggiornamento. La policy di sostituzione non modifica in modo permanente la policy stack. Per modificare una policy stack, consulta [Modifica di una policy stack](#).

Modifica di una policy stack

Per proteggere le risorse aggiuntive o per rimuovere la protezione dalle risorse, modificare la policy stack. Per esempio, quando si aggiunge un database che si desidera proteggere allo stack, aggiungere una dichiarazione Deny per quel database alla policy stack. Per modificare la policy, bisogna avere l'autorizzazione a utilizzare l'operazione [SetStackPolicy](#).

Utilizzare il AWS CLI per modificare le politiche dello stack.

Per modificare una policy stack (AWS CLI)

- Utilizzare il comando [set-stack-policy](#) con l'opzione `--stack-policy-body` per digitare in una policy modificata o l'opzione `--stack-policy-url` per specificare un file contenente la policy.

Non è possibile eliminare una policy stack. Per rimuovere tutta la protezione da tutte le risorse, si modifica la policy per permettere esplicitamente tutte le operazioni su tutte le risorse. La policy seguente permette tutti gli aggiornamenti su tutte le risorse:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori esempi di policy stack

Le policy di esempio seguenti mostrano come impedire gli aggiornamenti di tutte le risorse stack e di risorse specifiche e come impedire tipologie specifiche di aggiornamenti.

Impedire gli aggiornamenti di tutte le risorse stack

Per impedire gli aggiornamenti di tutte le risorse stack, la policy seguente specifica una dichiarazione Deny per tutte le operazioni di aggiornamento su tutte le risorse.

```
{
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Impedire gli aggiornamenti di una singola risorsa

La policy seguente nega tutte le operazioni di aggiornamento sul database con l'ID logico MyDatabase. Essa consente tutte le operazioni di aggiornamento su tutte le altre risorse stack con una dichiarazione Allow. La dichiarazione Allow non si applica alla risorsa MyDatabase perché la dichiarazione Deny sostituisce sempre le operazioni di permesso.

```
{
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "LogicalResourceId/MyDatabase"
    },
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

È possibile ottenere lo stesso risultato dell'esempio precedente utilizzando un rifiuto per default. Quando impostate una politica di stack, CloudFormation nega qualsiasi aggiornamento che non sia esplicitamente consentito. La policy seguente consente gli aggiornamenti di tutte le risorse ad eccezione della risorsa `ProductionDatabase`, che viene rifiutata per default.

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "NotResource" : "LogicalResourceId/ProductionDatabase"
    }
  ]
}
```

Important

Vi è rischio nell'utilizzo di un rifiuto per default. Se si dispone di una dichiarazione `Allow` altrove nella policy (come per esempio una dichiarazione `Allow` che utilizza un carattere jolly), è possibile concedere inconsapevolmente l'autorizzazione all'aggiornamento di risorse per le quali non lo si voleva. Poiché un rifiuto esplicito sostituisce qualsiasi operazione di permesso, è possibile fare in modo che una risorsa venga protetta utilizzando una dichiarazione `Deny`.

Impedire gli aggiornamenti di tutte le istanze di un tipo di risorsa

La policy seguente rifiuta tutte le operazioni di aggiornamento nel tipo di risorsa RDS dell'istanza database. Essa consente tutte le operazioni di aggiornamento su tutte le altre risorse stack con una dichiarazione `Allow`. La dichiarazione `Allow` non si applica alle risorse RDS dell'istanza database poiché una dichiarazione `Deny` sostituisce sempre le operazioni di permesso.

```
{
  "Statement" : [
    {
```

```
    "Effect" : "Deny",
    "Action" : "Update:*",
    "Principal": "*",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "ResourceType" : ["AWS::RDS::DBInstance"]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "Update:*",
    "Principal": "*",
    "Resource" : "*"
}
]
```

Impedire gli aggiornamenti di sostituzione per un'istanza

La policy seguente rifiuta gli aggiornamenti che causerebbero una sostituzione dell'istanza con l'ID logico `MyInstance`. Essa consente tutte le operazioni di aggiornamento su tutte le altre risorse `stack` con una dichiarazione `Allow`. La dichiarazione `Allow` non si applica alla risorsa `MyInstance` perché la dichiarazione `Deny` sostituisce sempre le operazioni di permesso.

```
{
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : "Update:Replace",
      "Principal": "*",
      "Resource" : "LogicalResourceId/MyInstance"
    },
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Impedire gli aggiornamenti degli stack nidificati

La seguente politica nega tutte le azioni di aggiornamento sul tipo di risorsa CloudFormation dello stack (stack annidati). Essa consente tutte le operazioni di aggiornamento su tutte le altre risorse stack con una dichiarazione Allow. La dichiarazione Allow non si applica alle risorse stack CloudFormation poiché la dichiarazione Deny sostituisce sempre le operazioni di permesso.

```
{
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ResourceType" : ["AWS::CloudFormation::Stack"]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    }
  ]
}
```

Protezione dei dati in AWS CloudFormation

Il [modello di responsabilità AWS condivisa](#) di si applica alla protezione dei dati in AWS CloudFormation. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AWS CloudFormation o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati inattivi

Seguendo il modello di responsabilità AWS condivisa, AWS CloudFormation archivia i dati crittografati quando sono inattivi. I clienti sono responsabili dell'impostazione delle policy di crittografia e di storage dei dati archiviati nei propri account. Ad esempio, si consiglia di abilitare la crittografia dei dati inattivi per i modelli e altri dati archiviati in bucket S3 o in argomenti SNS. I clienti definiscono in modo simile le impostazioni di crittografia per tutti i sistemi di storage dei dati forniti da CloudFormation.

Crittografia in transito

AWS CloudFormation utilizza canali crittografati per le comunicazioni di servizio nell'ambito del modello di responsabilità condivisa.

Riservatezza del traffico Internet

AWS CloudFormation le comunicazioni di servizio sono crittografate in modo sicuro per impostazione predefinita tra regioni o zone di disponibilità.

Controlla CloudFormation l'accesso con AWS Identity and Access Management

Con AWS Identity and Access Management (IAM), puoi creare utenti IAM e controllarne l'accesso a risorse specifiche del tuo Account AWS. Quando usi IAM, puoi controllare cosa possono fare gli utenti CloudFormation, ad esempio se possono visualizzare modelli di stack, creare stack o eliminare stack.

Oltre CloudFormation alle azioni specifiche, puoi gestire i AWS servizi e le risorse disponibili per ogni utente. In questo modo, puoi controllare a quali risorse gli utenti possono accedere quando le utilizzano CloudFormation. Ad esempio, puoi specificare quali utenti possono creare istanze Amazon, terminare EC2 istanze di database o effettuare aggiornamenti. VPCs Le stesse autorizzazioni si applicano ogni volta che vengono utilizzate CloudFormation per eseguire tali azioni.

Utilizza le informazioni contenute nelle sezioni seguenti per controllare chi può accedere.

CloudFormation Esploreremo anche come autorizzare la creazione di risorse IAM in modelli, fornire alle applicazioni in esecuzione su EC2 istanze le autorizzazioni necessarie e utilizzare credenziali di sicurezza temporanee per una maggiore sicurezza nell'ambiente. AWS

Definizione di policy basate sull'identità IAM per CloudFormation

Per consentirne l'accesso CloudFormation, devi creare e assegnare policy IAM che consentano alle tue identità IAM (come utenti o ruoli) di effettuare le azioni API di cui hanno bisogno.

Con le policy basate sull'identità IAM, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. CloudFormationsupporta azioni, risorse e chiavi di condizione specifiche.

Se non conosci IAM, inizia a familiarizzare con gli elementi di una policy IAM JSON. Per ulteriori informazioni, consulta il [riferimento agli elementi della policy IAM JSON](#) nella IAM User Guide. Per

imparare a creare policy IAM, completa il tutorial [Crea e allega la tua prima policy gestita dai clienti](#) nella documentazione IAM.

Argomenti

- [Azioni politiche per CloudFormation](#)
- [Azioni specifiche per console per CloudFormation](#)
- [Risorse politiche per CloudFormation](#)
- [Chiavi relative alle condizioni politiche per CloudFormation](#)

Azioni politiche per CloudFormation

Nell'Actionelemento della dichiarazione sulla politica IAM, puoi specificare qualsiasi azione API che CloudFormation offra. È necessario anteporre al nome dell'azione la stringa minuscola `cloudformation:`. For example: `cloudformation:CreateStack`, `cloudformation:CreateChangeSet` e `cloudformation:UpdateStack`.

Per specificare più azioni in una singola istruzione, separale con virgole, come segue:

```
"Action": [ "cloudformation:action1", "cloudformation:action2" ]
```

Puoi anche specificare più operazioni tramite caratteri jolly. Ad esempio, è possibile specificare tutte le azioni i cui nomi iniziano con la parola `Get`, nel modo seguente:

```
"Action": "cloudformation:Get*"
```

Per visualizzare un elenco completo delle azioni associate al prefisso del `cloudformation` servizio, consulta [Azioni, risorse e chiavi di condizione per AWS CloudFormation](#) e [Azioni, risorse e chiavi di condizione AWS Cloud Control API](#) nel riferimento sull'autorizzazione del servizio.

Esempi

Di seguito viene mostrato un esempio di una politica di autorizzazioni che concede le autorizzazioni per visualizzare gli stack. CloudFormation

Example 1: Un esempio di policy che concede i permessi di visualizzazione dello stack

```
{
  "Version": "2012-10-17",
  "Statement": [{
```



```
    "Effect": "Allow",
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
    ],
    "Resource": "*"
  ]
}
```

Gli utenti che creano o eliminano gli stack necessitano di autorizzazioni aggiuntive in base ai modelli di stack utilizzati. Ad esempio, se il modello descrive una coda Amazon SQS, gli utenti devono disporre delle autorizzazioni sia per le azioni di Amazon SQS che per quelle di Amazon CloudFormation SQS, come illustrato nella seguente policy di esempio.

Example 2: Un esempio di policy che consente di creare e visualizzare le azioni dello stack e tutte le azioni di Amazon SQS

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": [
      "sqs:*",
      "cloudformation:CreateStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResources",
      "cloudformation:GetTemplate",
      "cloudformation:ValidateTemplate"
    ],
    "Resource": "*"
  } ]
}
```

Azioni specifiche per console per CloudFormation

Gli utenti della CloudFormation console richiedono autorizzazioni aggiuntive oltre a quelle necessarie per la sala operatoria. AWS Command Line Interface CloudFormation APIs Queste autorizzazioni aggiuntive supportano funzionalità specifiche della console, come il caricamento di modelli su bucket Amazon S3 e gli elenchi a discesa per tipi di parametri specifici. AWS

Per tutte le azioni elencate di seguito, concedi le autorizzazioni a tutte le risorse; non limitarle a pile o bucket specifici.

L'azione seguente viene utilizzata solo dalla CloudFormation console e non è documentata nel riferimento all'API. L'operazione consente agli utenti di caricare i modelli nei bucket Amazon S3.

- `cloudformation:CreateUploadBucket`

Quando gli utenti caricano modelli, richiedono anche le seguenti autorizzazioni Amazon S3:

- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetObject`
- `s3:CreateBucket`

Per visualizzare i valori negli elenchi a discesa dei parametri per i modelli con tipi di parametri AWS specifici, gli utenti devono disporre delle autorizzazioni per effettuare le chiamate API di descrizione corrispondenti. Ad esempio, le seguenti autorizzazioni sono necessarie quando questi tipi di parametri vengono utilizzati nel modello:

- `ec2:DescribeKeyPairs`— Obbligatorio per il tipo di `AWS::EC2::KeyPair::KeyName` parametro.
- `ec2:DescribeSecurityGroups`— Obbligatorio per il tipo di `AWS::EC2::SecurityGroup::Id` parametro.
- `ec2:DescribeSubnets`— Obbligatorio per il tipo di `AWS::EC2::Subnet::Id` parametro.
- `ec2:DescribeVpcs`— Obbligatorio per il tipo di `AWS::EC2::VPC::Id` parametro.

Per ulteriori informazioni sui tipi AWS di parametri specifici, vedere [Specificare le risorse esistenti in fase di esecuzione con i CloudFormation tipi di parametri forniti](#).

Risorse politiche per CloudFormation

In una dichiarazione di policy IAM, l'elemento `Resource` specifica l'oggetto o gli oggetti coperti dall'istruzione. Infatti CloudFormation, ogni dichiarazione di policy IAM si applica alle risorse specificate utilizzando i rispettivi Amazon Resource Names (ARNs). Il formato ARN specifico dipende dalla risorsa.

Per un elenco completo dei tipi di CloudFormation risorse e relativi ARNs, vedere [Tipi di risorse definiti da AWS CloudFormation](#) nel Service Authorization Reference. Per informazioni sulle azioni che è possibile specificare con l'ARN di ciascuna risorsa, vedere [Azioni definite](#) da AWS CloudFormation.

È possibile specificare azioni per uno stack specifico, come illustrato nel seguente esempio di policy. Quando fornisci un ARN, sostituiscilo *placeholder text* con le informazioni specifiche della tua risorsa.

Example 1: Un esempio di policy che nega le azioni di eliminazione e aggiornamento dello stack per lo stack specificato

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": [
      "cloudformation:DeleteStack",
      "cloudformation:UpdateStack"
    ],
    "Resource": "arn:aws:cloudformation:region:account-id:stack/MyProductionStack/*"
  ]
}
```

La politica sopra riportata utilizza una wild card alla fine del nome dello stack in modo che l'eliminazione dello stack e l'aggiornamento dello stack vengano negati sia sull'ID completo dello stack (ad esempio) che sul nome dello stack (ad esempio `arn:aws:cloudformation:region:account-id:stack/MyProductionStack/abc9dbf0-43c2-11e3-a6e8-50fa526be49c`). *MyProductionStack*

Per consentire alle AWS::Serverless trasformazioni di creare un set di modifiche, includi l'autorizzazione a livello di `arn:aws:cloudformation:region:aws:transform/Serverless-2016-10-31` risorsa, come illustrato nella seguente politica.

Example 2: Una politica di esempio che consente l'azione di creazione del set di modifiche per la trasformazione specificata

```
{
  "Version": "2012-10-17",
  "Statement": [{
```

```
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateChangeSet"
    ],
    "Resource": "arn:aws:cloudformation:region:aws:transform/Serverless-2016-10-31"
  ]
}
```

Chiavi relative alle condizioni politiche per CloudFormation

In una dichiarazione sulla politica IAM, puoi facoltativamente specificare le condizioni che determinano l'entrata in vigore di una policy. Ad esempio, puoi definire una policy che consenta agli utenti di creare uno stack solo quando specificano un determinato URL del modello. Puoi definire condizioni CloudFormation specifiche e AWS condizioni generali, ad esempio `DateLessThan`, che specificano quando una policy smette di avere effetto. Per ulteriori informazioni e un elenco di condizioni AWS-wide, consulta Condition in [IAM Policy Elements di riferimento nella IAM User Guide](#).

Note

Non utilizzare la condizione `aws:SourceIp` AWS-wide. CloudFormation effettua il provisioning delle risorse utilizzando il proprio indirizzo IP, non l'indirizzo IP della richiesta di origine. Ad esempio, quando crei uno stack, CloudFormation effettua richieste dal suo indirizzo IP per avviare un' EC2 istanza Amazon o per creare un bucket Amazon S3, non dall'indirizzo IP della chiamata o `CreateStack` del comando. `create-stack`

L'elenco seguente descrive le condizioni specifiche. CloudFormation Queste condizioni si applicano solo quando gli utenti creano o aggiornano gli stack:

`cloudformation:ChangeSetName`

Un nome di set di CloudFormation modifiche che si desidera associare a una politica. Utilizza questa condizione per controllare quali set di modifiche gli utenti possono eseguire o eliminare.

`cloudformation:ImportResourceTypes`

I tipi di risorse del modello che desideri associare a una policy, ad esempio `AWS::EC2::Instance`. Utilizza questa condizione per controllare i tipi di risorse che gli utenti possono utilizzare quando importano risorse in uno stack. Questa condizione viene verificata rispetto ai tipi di risorse dichiarati dagli utenti nel `ResourcesToImport` parametro, che attualmente è supportato solo per AWS CLI le richieste API. Quando si utilizza questo parametro,

è necessario specificare tutti i tipi di risorse che si desidera far controllare agli utenti durante le operazioni di importazione. Per ulteriori informazioni sul `ResourcesToImport` parametro, consulta l'[CreateChangeSet](#) operazione nell'AWS CloudFormation API Reference.

Per un elenco dei possibili `ResourcesToImport`, consulta [Supporto per tipi di risorse](#).

Utilizza la convenzione di denominazione delle risorse in tre parti per specificare i tipi di risorse con cui gli utenti possono lavorare, da tutte le risorse di un'organizzazione fino a un singolo tipo di risorsa.

`organization::*`

Specifica tutti i tipi di risorse per una determinata organizzazione.

`organization::service_name::*`

Specifica tutti i tipi di risorse per il servizio specificato all'interno di una determinata organizzazione.

`organization::service_name::resource_type`

Specifica un determinato tipo di risorsa.

Per esempio:

`AWS::*`

Specificare tutti i tipi di AWS risorse supportati.

`AWS::service_name::*`

Specifica tutte le risorse per un determinato servizio AWS .

`AWS::service_name::resource_type`

Specificate un tipo di AWS risorsa specifico, ad esempio `AWS::EC2::Instance` (tutte le EC2 istanze).

`cloudformation:ResourceTypes`

I tipi di risorse del modello, ad esempio `AWS::EC2::Instance`, che vuoi associare a una policy. Utilizza questa condizione per controllare i tipi di risorse che gli utenti possono utilizzare quando creano o aggiornano uno stack. La condizione viene verificata in base ai tipi di risorse che gli utenti dichiarano nel parametro `ResourceTypes`, attualmente supportato solo per la AWS CLI e richieste API. Quando si utilizza questo parametro, gli utenti devono specificare tutti i tipi di risorse disponibili nel modello. Per ulteriori informazioni sul `ResourceTypes` parametro, consulta l'[CreateStack](#) operazione nell'AWS CloudFormation API Reference.

Per un elenco dei tipi di risorse, consulta [AWS CloudFormation Template Reference Guide](#).

Utilizza la convenzione di denominazione delle risorse in tre parti per specificare i tipi di risorse con cui gli utenti possono lavorare, da tutte le risorse di un'organizzazione fino a un singolo tipo di risorsa.

*organization::**

Specifica tutti i tipi di risorse per una determinata organizzazione.

*organization::service_name::**

Specifica tutti i tipi di risorse per il servizio specificato all'interno di una determinata organizzazione.

organization::service_name::resource_type

Specifica un determinato tipo di risorsa.

Per esempio:

*AWS::**

Specificate tutti i tipi di AWS risorse supportati.

*AWS::service_name::**

Specifica tutte le risorse per un determinato servizio AWS .

AWS::service_name::resource_type

Specificate un tipo di AWS risorsa specifico, ad esempio *AWS::EC2::Instance* (tutte le EC2 istanze).

*Alexa::ASK::**

Specifica tutti i tipi di risorse in Alexa Skill Kit.

Alexa::ASK::Skill

Specificate il tipo di [risorsa individuale Alexa: :ASK: :Skill](#).

*Custom::**

Specifica tutte le risorse personalizzate.

Per ulteriori informazioni, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

Custom::*resource_type*

Specificare un tipo specifico di risorsa personalizzata.

Per ulteriori informazioni, consulta [Crea una logica di provisioning personalizzata con risorse personalizzate](#).

cloudformation:RoleARN

L'Amazon Resource Name (ARN) di un ruolo del servizio IAM da associare a una policy. Utilizza questa condizione per controllare quale ruolo del può essere usato dagli utenti quando lavorano con gli stack o i set di modifiche.

cloudformation:StackPolicyUrl

L'URL della policy di uno stack Amazon S3 da associare a una policy. Utilizza questa condizione per controllare quali policy di stack gli utenti possono associare a uno stack durante la creazione o l'aggiornamento di un'operazione dello stack. Per ulteriori informazioni sulle policy degli stack, consulta [Impedire gli aggiornamenti delle risorse stack](#).

 Note

Per garantire che gli utenti possano creare o aggiornare gli stack solo con le policy di stack che hai caricato, imposta il bucket S3 in modo che sia di sola lettura per quegli utenti.

cloudformation:TemplateUrl

L'URL del modello Amazon S3 da associare a una policy. Utilizza questa condizione per controllare quali modelli gli utenti possono usare quando creano o aggiornano gli stack.

 Note

Per garantire che gli utenti possano creare o aggiornare gli stack solo con i modelli che hai caricato, imposta il bucket S3 in modo che sia di sola lettura per quegli utenti.

 Note

Le seguenti condizioni CloudFormation specifiche si applicano ai parametri API con lo stesso nome:

- `cloudformation:ChangeSetName`
- `cloudformation:RoleARN`
- `cloudformation:StackPolicyUrl`
- `cloudformation:TemplateUrl`

Ad esempio, si applica `cloudformation:TemplateUrl` solo al `TemplateUrl` parametro for `CreateStackUpdateStack`, e `CreateChangeSet` APIs.

Per esempi di policy IAM che utilizzano chiavi condizionali per controllare l'accesso, consulta [Esempi di policy basate sull'identità IAM per CloudFormation](#).

Accettazione delle risorse IAM nei modelli CloudFormation

Prima di poter creare uno stack, CloudFormation convalida il modello. Durante la convalida, CloudFormation verifica nel modello la presenza di risorse IAM che potrebbe creare. Le risorse IAM, ad esempio un utente con accesso completo, possono accedere e modificare tutte le risorse nell' Account AWS. Pertanto, ti consigliamo di esaminare le autorizzazioni associate a ogni risorsa IAM prima di continuare, in modo da non creare inavvertitamente le risorse con autorizzazioni di escalation. Per assicurarti di averlo fatto, devi riconoscere che il modello contiene tali risorse e fornisce CloudFormation le funzionalità specificate prima di creare lo stack.

Puoi riconoscere le funzionalità dei CloudFormation modelli utilizzando la CloudFormation console, AWS Command Line Interface (AWS CLI) o l'API:

- Nella CloudFormation console, nella pagina Configura le opzioni dello stack delle procedure guidate Create Stack o Update Stack, scegli Riconosco che questo modello può creare risorse IAM.
- In AWS CLI, quando usi [update-stack](#) i comandi [create-stack](#) and, specifica il `CAPABILITY_NAMED_IAM` valore `CAPABILITY_IAM` o per l'opzione. `--capabilities` Se il modello comprende risorse IAM, è possibile specificare qualsiasi funzionalità. Se il modello comprende nomi personalizzati per le risorse IAM, occorre specificare `CAPABILITY_NAMED_IAM`.
- Nell'API, quando utilizzi le [UpdateStack](#) azioni [CreateStack](#) and, specifica `Capabilities.member.1=CAPABILITY_IAM` o `Capabilities.member.1=CAPABILITY_NAMED_IAM`. Se il modello comprende risorse IAM, è possibile specificare qualsiasi funzionalità. Se il modello comprende nomi personalizzati per le risorse IAM, occorre specificare `CAPABILITY_NAMED_IAM`.

 Important

Se il modello contiene risorse IAM con nomi personalizzati, non occorre creare più stack che riutilizzino lo stesso modello. Le risorse IAM devono essere univoche a livello globale nell'account. Se utilizzi lo stesso modello per creare più stack in Regioni diverse, gli stack potrebbero condividere le stesse risorse IAM anziché avere ognuno una risorsa univoca. Le risorse condivise tra stack possono avere conseguenze indesiderate irreversibili. Ad esempio, se si eliminano o si aggiornano risorse IAM condivise all'interno di uno stack, si potrebbero involontariamente modificare le risorse di altri stack.

Gestione delle credenziali per le applicazioni in esecuzione su istanze Amazon EC2

Se hai un'applicazione che viene eseguita su un' EC2 istanza Amazon e devi effettuare richieste a AWS risorse come i bucket Amazon S3 o una tabella DynamoDB, l'applicazione richiede credenziali di sicurezza. AWS Tuttavia, la distribuzione e l'incorporamento delle credenziali di sicurezza a lungo termine in ogni istanza avviata è una sfida nonché un potenziale rischio per la sicurezza. Invece di utilizzare credenziali a lungo termine, come le credenziali utente IAM, ti consigliamo di creare un ruolo IAM associato a un' EC2 istanza Amazon all'avvio dell'istanza. Un'applicazione può quindi ottenere credenziali di sicurezza temporanee dall' EC2 istanza Amazon. Non è necessario incorporare le credenziali a lungo termine nell'istanza. Inoltre, per semplificare la gestione delle credenziali, puoi specificare un solo ruolo per più EC2 istanze Amazon; non devi creare credenziali uniche per ogni istanza.

Per un frammento di modello che mostra come avviare un'istanza con un ruolo, consulta [Esempi di modello per i ruoli IAM](#).

 Note

Le applicazioni che si basano sulle istanze che utilizzano credenziali di sicurezza temporanee possono chiamare qualsiasi azione CloudFormation . Tuttavia, poiché CloudFormation interagisce con molti altri AWS servizi, devi verificare che tutti i servizi che desideri utilizzare supportino credenziali di sicurezza temporanee. Per un elenco dei servizi che accettano credenziali di sicurezza temporanee, consulta la sezione [AWS Servizi che funzionano con IAM](#) nella Guida per l'utente di IAM.

Concessione dell'accesso temporaneo (accesso federato)

In alcuni casi, potresti voler concedere agli utenti senza AWS credenziali l'accesso temporaneo al tuo Account AWS. Invece di creare ed eliminare credenziali a lungo termine ogni volta che desideri concedere un accesso temporaneo, usa AWS Security Token Service (AWS STS). Ad esempio, puoi utilizzare i ruoli IAM. Da un ruolo IAM, è possibile creare e distribuire in modo programmatico molte credenziali di sicurezza temporanee (che includono una chiave di accesso, una chiave di accesso segreta e un token di sicurezza). Queste credenziali hanno una durata limitata, quindi non possono essere utilizzate per accedere alle tue credenziali Account AWS dopo la loro scadenza. Puoi anche creare più ruoli IAM per concedere ai singoli utenti livelli di autorizzazioni diversi. I ruoli IAM sono utili per scenari quali le identità federate e i Single Sign-On (SSO).

Un'identità federata è un'identità distinta che puoi utilizzare in più sistemi. Per gli utenti enterprise con un sistema di identità locale (ad esempio LDAP o Active Directory), è possibile gestire tutte le autenticazioni con il sistema di identità locale. Dopo l'autenticazione dell'utente, è necessario fornire le credenziali di sicurezza temporanee dell'utente o ruolo IAM corrispondente. Ad esempio, puoi creare un ruolo di amministratore e un ruolo di sviluppatore, in cui gli amministratori abbiano pieno accesso all'AWS account e gli sviluppatori abbiano le autorizzazioni per lavorare solo con gli stack CloudFormation. Dopo l'autenticazione, l'amministratore è autorizzato a ottenere credenziali di sicurezza temporanee dal ruolo di amministratore. Tuttavia, gli sviluppatori possono ottenere credenziali di sicurezza temporanee solo dal ruolo di sviluppatore.

È inoltre possibile concedere agli utenti federati l'accesso alla AWS Management Console. Dopo l'autenticazione degli utenti con il sistema di identità locale, è possibile creare un URL temporaneo a livello di codice che offra un accesso diretto alla AWS Management Console. Quando gli utenti utilizzano l'URL temporaneo, non avranno bisogno di accedere ad AWS perché sono già stati autenticati (single sign-on). Inoltre, poiché l'URL viene creato in base alle credenziali di sicurezza temporanee degli utenti, le autorizzazioni disponibili con tali credenziali definiscono le autorizzazioni degli utenti in AWS Management Console.

È possibile utilizzarle diversamente per generare credenziali AWS STS API di sicurezza temporanee. Per ulteriori informazioni sull'API da utilizzare, [consulta *Compare AWS STS credentials*](#) nella IAM User Guide.

 Important

Non è possibile lavorare con IAM quando si utilizzano credenziali di sicurezza temporanee generati dall'API `GetFederationToken`. Al contrario, se è necessario utilizzare IAM, usare le credenziali di sicurezza temporanee di un ruolo.

CloudFormation interagisce con molti altri AWS servizi. Quando utilizzi credenziali di sicurezza temporanee con CloudFormation, verifica che tutti i servizi che desideri utilizzare supportino credenziali di sicurezza temporanee. Per un elenco dei servizi che accettano credenziali di sicurezza temporanee, consulta [AWS i servizi che funzionano con IAM](#) nella Guida per l'utente di IAM.

Per ulteriori informazioni, consulta le seguenti risorse correlate nella Guida per l'utente IAM:

- [Scenari comuni per le credenziali temporanee](#)
- [Abilita l'accesso personalizzato da parte di un broker di identità alla console AWS](#)

Esempi di policy basate sull'identità IAM per CloudFormation

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse CloudFormation. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o API. AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli. Per ulteriori informazioni, consulta [Definizione di policy basate sull'identità IAM per CloudFormation](#).

Gli esempi seguenti mostrano le dichiarazioni politiche che è possibile utilizzare per consentire o negare le autorizzazioni all'uso di una o più CloudFormation azioni.

Argomenti

- [Richiedi un URL specifico per il modello](#)
- [Nega tutte le operazioni di importazione CloudFormation](#)
- [Consenti operazioni di importazione per tipi di risorse specifici](#)
- [Nega le risorse IAM nei modelli di stack](#)
- [Consenti la creazione di stack con tipi di risorse specifici](#)
- [Controlla l'accesso in base alle azioni API che modificano le risorse](#)

- [Limita le operazioni relative ai set di stack in base alla regione e ai tipi di risorse](#)
- [Consenti tutte le operazioni del generatore IAC](#)

Richiedi un URL specifico per il modello

La seguente politica concede le autorizzazioni per utilizzare solo l'URL del *https://s3.amazonaws.com/amzn-s3-demo-bucket/test.template* modello per creare o aggiornare uno stack.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "cloudformation:CreateStack", "cloudformation:UpdateStack" ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudformation:TemplateUrl": [ "https://s3.amazonaws.com/amzn-s3-demo-bucket/test.template" ]
        }
      }
    }
  ]
}
```

Nega tutte le operazioni di importazione CloudFormation

La seguente politica concede le autorizzazioni per completare tutte le CloudFormation operazioni tranne le operazioni di importazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllStackOperations",
      "Effect": "Allow",
      "Action": "cloudformation:*",
      "Resource": "*"
    },
    {
```

```

    "Sid": "DenyImport",
    "Effect": "Deny",
    "Action": "cloudformation:*",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringLike": {
        "cloudformation:ImportResourceTypes": [
          "*"
        ]
      }
    }
  ]
}

```

Consenti operazioni di importazione per tipi di risorse specifici

La seguente politica concede le autorizzazioni a tutte le operazioni di stack, oltre alle operazioni di importazione solo su risorse specifiche (in questo esempio, `AWS::S3::Bucket`)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowImport",
      "Effect": "Allow",
      "Action": "cloudformation:*",
      "Resource": "*"
      "Condition": {
        "ForAllValues:StringEqualsIgnoreCase": {
          "cloudformation:ImportResourceTypes": [
            "AWS::S3::Bucket"
          ]
        }
      }
    }
  ]
}

```

Nega le risorse IAM nei modelli di stack

La seguente policy concede le autorizzazioni per creare stack ma nega le richieste se il modello dello stack include risorse del servizio IAM. Inoltre, in base a questa policy gli utenti devono anche

specificare il parametro `ResourceTypes`, disponibile solo per la AWS CLI e per le richieste API. Questa policy usa istruzioni di rifiuto esplicito, pertanto se altre policy concedono autorizzazioni aggiuntive, questa policy resta sempre valida (un'istruzione di rifiuto esplicito ha sempre la precedenza su un'istruzione di consenso esplicito).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "cloudformation:CreateStack" ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [ "cloudformation:CreateStack" ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLikeIfExists" : {
          "cloudformation:ResourceTypes" : [ "AWS::IAM::*" ]
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": [ "cloudformation:CreateStack" ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:ResourceTypes": "true"
        }
      }
    }
  ]
}
```

Consenti la creazione di stack con tipi di risorse specifici

La seguente politica è simile all'esempio precedente. La policy concede le autorizzazioni per creare uno stack a meno che il modello dello stack non includa risorse del servizio IAM. Richiede inoltre agli utenti di specificare il `ResourceTypes` parametro, che è disponibile solo per AWS CLI le richieste

API. Questa policy è più semplice, ma non utilizza istruzioni di rifiuto esplicito. Altre policy, che concedono autorizzazioni aggiuntive, potrebbe sostituire questa policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "cloudformation:CreateStack" ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLikeIfExists" : {
          "cloudformation:ResourceTypes" : [ "AWS::IAM::*" ]
        },
        "Null": {
          "cloudformation:ResourceTypes": "false"
        }
      }
    }
  ]
}
```

Controlla l'accesso in base alle azioni API che modificano le risorse

La seguente politica concede le autorizzazioni per filtrare l'accesso in base al nome di un'azione API che modifica le risorse. Viene utilizzato per controllare quali utenti API IAM possono utilizzare per aggiungere o rimuovere tag su uno stack o un set di stack. L'operazione utilizzata per aggiungere o rimuovere tag deve essere aggiunta come valore per la chiave di condizione. La seguente politica concede TagResource e UntagResource autorizzazioni all'operazione di modifica. CreateStack

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "CreateActionConditionPolicyForTagUntagResources",
    "Effect": "Allow",
    "Action": [
      "cloudformation:TagResource",
      "cloudformation:UntagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
```

```

        "cloudformation:CreateAction": [
            "CreateStack"
        ]
    }
}
}]
}

```

Limita le operazioni relative ai set di stack in base alla regione e ai tipi di risorse

La seguente politica concede le autorizzazioni per set di stack gestiti dal servizio. Un utente con questa policy può eseguire operazioni solo sui set di stack con modelli contenenti tipi di risorse Amazon S3 (AWS::S3::*) o il tipo di risorsa AWS::SES::ConfigurationSet. Se ha effettuato l'accesso all'account di gestione dell'organizzazione con ID123456789012, l'utente può anche eseguire operazioni solo su set di stack destinati all'unità organizzativa con ID *ou-1fsfsrsdsfrewr* e può eseguire solo operazioni sullo stack impostato con ID che ha come destinazione il with ID. *stack-set-id* Account AWS *987654321012*

Le operazioni di stack set hanno esito negativo se il modello di stack set contiene tipi di risorse diversi da quelli specificati nella policy o se gli obiettivi di distribuzione sono unità organizzative o account IDs diversi da quelli specificati nella politica per gli account di gestione e i set di stack corrispondenti.

Queste restrizioni di policy si applicano solo quando le operazioni sul set di stack sono destinate alle Regioni us-east-1, us-west-2 o eu-west-2 Regioni AWS.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stackset/*",
        "arn:aws:cloudformation:*:*:type/resource/AWS-S3-*",
        "arn:aws:cloudformation:us-west-2:*:type/resource/AWS-SES-ConfigurationSet",
        "arn:aws:cloudformation:*:123456789012:stackset-target/*/ou-1fsfsrsdsfrewr",
        "arn:aws:cloudformation:*:123456789012:stackset-target/stack-set-id/987654321012"
      ]
    }
  ]
}

```



```

    ],
    "Condition": {
      "ForAllValues:StringEqualsIgnoreCase": {
        "cloudformation:TargetRegion": [
          "us-east-1",
          "us-west-2",
          "eu-west-1"
        ]
      }
    }
  }
]
}

```

Consenti tutte le operazioni del generatore IAC

La seguente politica consente l'accesso alle CloudFormation azioni relative alla scansione delle risorse del generatore IAC e alla gestione dei modelli. La prima istruzione concede le autorizzazioni per descrivere, elencare e avviare scansioni delle risorse. Consente inoltre l'accesso a permessi aggiuntivi richiesti (`cloudformation:GetResourcecloudformation:ListResources`, `cloudformation:ListTypes`) che consentono al generatore IAC di recuperare informazioni sulle risorse e sui tipi di risorse disponibili. La seconda istruzione concede le autorizzazioni complete per creare, eliminare, descrivere, elencare e aggiornare i modelli generati.

È inoltre necessario concedere le autorizzazioni di lettura per i AWS servizi di destinazione a chiunque esegua la scansione delle risorse con il generatore IAC. Per ulteriori informazioni, consulta [Autorizzazioni IAM necessarie per la scansione delle risorse](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ResourceScanningOperations",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeResourceScan",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListResourceScanRelatedResources",
        "cloudformation:ListResourceScanResources",
        "cloudformation:ListResourceScans",
        "cloudformation:ListTypes",

```

```
        "cloudformation:StartResourceScan"
    ],
    "Resource": "*"
  },
  {
    "Sid": "TemplateGeneration",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateGeneratedTemplate",
      "cloudformation>DeleteGeneratedTemplate",
      "cloudformation:DescribeGeneratedTemplate",
      "cloudformation:GetResource",
      "cloudformation:GetGeneratedTemplate",
      "cloudformation:ListGeneratedTemplates",
      "cloudformation:UpdateGeneratedTemplate"
    ],
    "Resource": "*"
  }
]
```

AWS CloudFormation ruolo di servizio

Un ruolo di servizio è un ruolo AWS Identity and Access Management (IAM) che consente di CloudFormation effettuare chiamate alle risorse in uno stack per tuo conto. Puoi specificare un ruolo IAM che permette a CloudFormation di creare, aggiornare o eliminare le risorse del tuo stack. Per impostazione predefinita, CloudFormation utilizza una sessione temporanea generata dalle credenziali utente per le operazioni dello stack. Se si specifica un ruolo di servizio, CloudFormation utilizza le credenziali di quel ruolo.

Utilizza un ruolo di servizio per specificare in modo esplicito le azioni che CloudFormation è possibile eseguire, che potrebbero non essere sempre le stesse azioni eseguite da te o da altri utenti. Ad esempio, potresti avere privilegi amministrativi, ma puoi limitare CloudFormation l'accesso solo alle EC2 azioni di Amazon.

Puoi creare il ruolo del servizio e le sue policy di autorizzazione con il servizio IAM. Per ulteriori informazioni sulla creazione di un ruolo di servizio, consulta [Creare un ruolo per delegare le autorizzazioni a un AWS servizio](#) nella Guida per l'utente IAM. Specifica CloudFormation (cloudformation.amazonaws.com) come servizio che può assumere il ruolo.

Per associare un ruolo del servizio con uno stack, specifica il ruolo al momento della creazione dello stack. Per informazioni dettagliate, consultare [Configurare le opzioni dello stack](#). Puoi anche modificare il ruolo del servizio quando aggiorni lo stack nella console, oppure [DeleteStack](#) lo stack tramite l'API. Prima di specificare un ruolo del servizio, assicurarsi di disporre dell'autorizzazione per passarlo (`iam:PassRole`). L'autorizzazione `iam:PassRole` specifica quali ruolo puoi utilizzare. Per ulteriori informazioni, consulta [Concedere a un utente le autorizzazioni per passare un ruolo a un AWS servizio nella Guida](#) per l'utente IAM.

Important

Quando specifichi un ruolo di servizio, utilizza CloudFormation sempre quel ruolo per tutte le operazioni eseguite su quello stack. Non è possibile rimuovere un ruolo di servizio collegato a uno stack dopo la creazione dello stack. Gli altri utenti che dispongono delle autorizzazioni per eseguire operazioni su questo stack possono utilizzare questo ruolo, indipendentemente dal fatto che tali utenti dispongano dell'`iam:PassRole` autorizzazione o meno. Se il ruolo include le autorizzazioni di cui l'utente non dovrebbe disporre, puoi riassegnare involontariamente le autorizzazioni di un utente. Assicurati che il ruolo garantisca i privilegi minimi. Per ulteriori informazioni, consulta [Applicazione delle autorizzazioni del privilegio minimo](#) nella Guida per l'utente di IAM.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra diversi servizi può portare alla confusione del problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi, con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Si consiglia di utilizzare [aws:SourceArn](#) e [aws:SourceAccount](#) chiavi di contesto globali nelle politiche delle risorse per limitare le autorizzazioni che AWS CloudFormation forniscono un altro servizio a una risorsa specifica, ad esempio un' CloudFormation estensione. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Assicurati che il valore di `aws:SourceArn` sia un ARN della risorsa archiviata. CloudFormation

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio `arn:aws:cloudformation:*:123456789012:*`.

Se il `aws:SourceArn` valore non contiene l'ID dell'account, devi utilizzare entrambe le chiavi di contesto della condizione globale per limitare le autorizzazioni.

L'esempio seguente mostra come utilizzare le chiavi di contesto della `aws:SourceArn` condizione `aws:SourceAccount` globale CloudFormation per evitare il confuso problema del vice.

Esempio di politica di fiducia che utilizza **aws:SourceArn** e **aws:SourceAccount** condiziona le chiavi

Per i servizi di registro, CloudFormation effettua chiamate a AWS Security Token Service (AWS STS) per assumere un ruolo di servizio nell'account. Questo ruolo è `ExecutionRoleArn` configurato per [RegisterType](#) funzionamento e `LogRoleArn` impostazione in [LoggingConfig](#) operazione. Per ulteriori informazioni, consulta [Configura un ruolo di esecuzione con autorizzazioni IAM e una policy di fiducia per l'accesso alle estensioni pubbliche](#).

Questo esempio di policy di fiducia per i ruoli utilizza istruzioni condizionali per limitare la `AssumeRole` capacità del ruolo di servizio alle sole azioni sull' CloudFormation estensione specificata nell'account specificato. Le condizioni `aws:SourceArn` e `aws:SourceAccount` sono valutate in modo indipendente. Qualsiasi richiesta di utilizzare il ruolo di servizio deve soddisfare entrambe le condizioni.

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

```
    "StringEquals": {
      "aws:SourceAccount": "123456789012"
    },
    "StringLike": {
      "aws:SourceArn": "arn:aws:cloudformation:us-east-1:123456789012:type/resource/Organization-Service-Resource/*"
    }
  }
}
```

Informazioni aggiuntive

Ad esempio, le politiche che utilizzano `aws:SourceArn` le chiavi di contesto della condizione `aws:SourceAccount` globale per un ruolo di servizio utilizzato da StackSets, vedere [Configurazione di chiavi globali per mitigare i problemi di "confused deputy"](#).

Per ulteriori informazioni, consulta [Aggiornare una policy di trust per i ruoli](#) nella Guida per l'utente IAM.

Richieste di sessioni di accesso inoltrato (FAS) e valutazione delle autorizzazioni

Durante la creazione, l'aggiornamento e l'eliminazione degli CloudFormation stack, gli utenti possono facoltativamente specificare un ARN del ruolo IAM. Se non viene fornito alcun ruolo, CloudFormation utilizza il meccanismo di servizio predefinito per interagire con altri servizi. AWS In questo scenario, il chiamante deve disporre delle autorizzazioni necessarie per le risorse gestite. In alternativa, quando un utente fornisce il proprio ruolo IAM, CloudFormation assumerà tale ruolo per eseguire le interazioni di servizio per suo conto.

Indipendentemente dal fatto che l'utente fornisca o meno un ruolo IAM, CloudFormation genera un nuovo token FAS con estensione limitata per ogni operazione sulle risorse. Di conseguenza, le [chiavi di condizione relative a FAS, incluse `aws:ViaAWSService`, vengono compilate](#) in entrambi gli scenari.

L'uso del FAS influisce sul modo in cui le policy IAM vengono valutate durante le operazioni. CloudFormation Quando si crea uno stack con un modello che include risorse interessate dalle chiavi di condizione relative al FAS, possono verificarsi negazioni delle autorizzazioni.

Policy IAM di esempio

Considerate la seguente politica IAM. Statement2impedirà costantemente la creazione di una `AWS::KMS::Key` risorsa in CloudFormation. La restrizione verrà applicata in modo coerente, indipendentemente dal fatto che venga fornito o meno un ruolo IAM durante l'operazione stack. Questo perché la chiave di `aws:ViaAWSService` condizione è sempre impostata su `true` causa dell'uso di FAS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "Statement2",
      "Effect": "Deny",
      "Action": [
        "kms:CreateKey"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
    }
  ]
}
```

Esempio di modello di pila

Ad esempio, quando un utente crea uno stack con il seguente modello di esempio, `aws:ViaAWSService` viene impostato su `true` e le autorizzazioni di ruolo verranno sostituite dalla

politica FAS. true La creazione dello stack sarà influenzata dalla Statement2 policy IAM, che nega l'azione. CreateKey Ciò si traduce in un errore di autorizzazione negata.

```
Resources:
  myPrimaryKey:
    Type: AWS::KMS::Key
    Properties:
      Description: An example multi-Region primary key
      KeyPolicy:
        Version: '2012-10-17'
        Id: key-default-1
        Statement:
          - Sid: Enable IAM User Permissions
            Effect: Allow
            Principal:
              AWS: !Join
                - ''
                - - 'arn:aws:iam::'
                  - !Ref AWS::AccountId
                  - ':root'
            Action: kms:*
            Resource: '*'
```

Per ulteriori informazioni su FAS, consulta [Forward access sessions](#) nella IAM User Guide.

Note

La maggior parte delle risorse aderisce a questo comportamento. Tuttavia, se riscontri un successo o un fallimento inaspettato durante la creazione, l'aggiornamento o l'eliminazione di una risorsa e la tua policy IAM include chiavi di condizione relative a FAS, è probabile che la risorsa in questione appartenga a un piccolo sottoinsieme di risorse che non seguono questo modello standard.

Registrazione delle chiamate AWS CloudFormation API con AWS CloudTrail

AWS CloudFormation è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in CloudFormation. CloudTrail acquisisce tutte le chiamate API relative CloudFormation agli eventi, incluse le chiamate dalla CloudFormation

console e le chiamate in codice a. CloudFormation APIs Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. CloudFormation Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata CloudFormation, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

Argomenti

- [CloudFormation informazioni in CloudTrail](#)
- [Comprensione delle CloudFormation voci dei file di registro](#)

CloudFormation informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in CloudFormation, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS . Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di CloudFormation, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consultare:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte CloudFormation le azioni vengono registrate CloudTrail e documentate nell'[AWS CloudFormation API Reference](#). Ad esempio, le chiamate alle `ListStacks` sezioni `CreateStackDeleteStack`, e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Comprensione delle CloudFormation voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l>CreateStackoperazione. L'operazione è stata effettuata da un utente IAM di nome Alice.

Note

Solo i nomi delle chiavi dei parametri di input vengono registrati. I valori dei parametri non vengono registrati.

```
{
  "eventVersion": "1.01",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAABCDEFGHijklmOPQ",
    "arn": "arn:aws:iam::012345678910:user/Alice",
    "accountId": "012345678910",
    "accessKeyId": "AKIDEXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2014-03-24T21:02:43Z",
```

```
"eventSource": "cloudformation.amazonaws.com",
"eventName": "CreateStack",
"awsRegion": "us-east-1",
"sourceIPAddress": "127.0.0.1",
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": {
  "templateURL": "templateURL",
  "tags": [
    {
      "key": "test",
      "value": "tag"
    }
  ],
  "stackName": "my-test-stack",
  "disableRollback": true,
  "parameters": [
    {
      "parameterKey": "password"
    },
    {
      "parameterKey": "securitygroup"
    }
  ]
},
"responseElements": {
  "stackId": "arn:aws:cloudformation:us-east-1:012345678910:stack/my-test-stack/a38e6a60-b397-11e3-b0fc-08002755629e"
},
"requestID": "9f960720-b397-11e3-bb75-a5b75389b02d",
"eventID": "9bf6cfb8-83e1-4589-9a70-b971e727099b"
}
```

Il seguente esempio mostra che Alice ha chiamato l'operazione UpdateStack sullo stack my-test-stack:

```
{
  "eventVersion": "1.01",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAABCDEFGHijklmOPQ",
    "arn": "arn:aws:iam::012345678910:user/Alice",
    "accountId": "012345678910",
    "accessKeyId": "AKIDEXAMPLE",
```

```

    "userName": "Alice"
  },
  "eventTime": "2014-03-24T21:04:29Z",
  "eventSource": "cloudformation.amazonaws.com",
  "eventName": "UpdateStack",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "templateURL": "templateURL",
    "parameters": [
      {
        "parameterKey": "password"
      },
      {
        "parameterKey": "securitygroup"
      }
    ],
    "stackName": "my-test-stack"
  },
  "responseElements": {
    "stackId": "arn:aws:cloudformation:us-east-1:012345678910:stack/my-test-stack/a38e6a60-b397-11e3-b0fc-08002755629e"
  },
  "requestID": "def0bf5a-b397-11e3-bb75-a5b75389b02d",
  "eventID": "637707ce-e4a3-4af1-8edc-16e37e851b17"
}

```

Il seguente esempio mostra che Alice ha chiamato l'operazione ListStacks.

```

{
  "eventVersion": "1.01",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAABCDEFGHijklmnopq",
    "arn": "arn:aws:iam::012345678910:user/Alice",
    "accountId": "012345678910",
    "accessKeyId": "AKIDEXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2014-03-24T21:03:16Z",
  "eventSource": "cloudformation.amazonaws.com",
  "eventName": "ListStacks",

```

```
"awsRegion": "us-east-1",
"sourceIPAddress": "127.0.0.1",
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": null,
"responseElements": null,
"requestID": "b7d351d7-b397-11e3-bb75-a5b75389b02d",
"eventID": "918206d0-7281-4629-b778-b91eb0d83ce5"
}
```

Il seguente esempio mostra che Alice ha chiamato l'operazione `DescribeStacks` sullo stack `my-test-stack`.

```
{
  "eventVersion": "1.01",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAABCDEFGHijklmOPQ",
    "arn": "arn:aws:iam::012345678910:user/Alice",
    "accountId": "012345678910",
    "accessKeyId": "AKIDEXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2014-03-24T21:06:15Z",
  "eventSource": "cloudformation.amazonaws.com",
  "eventName": "DescribeStacks",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "stackName": "my-test-stack"
  },
  "responseElements": null,
  "requestID": "224f2586-b398-11e3-bb75-a5b75389b02d",
  "eventID": "9e5b2fc9-1ba8-409b-9c13-587c2ea940e2"
}
```

Il seguente esempio mostra che Alice ha chiamato l'operazione `DeleteStack` sullo stack `my-test-stack`.

```
{
  "eventVersion": "1.01",
  "userIdentity": {
```

```
{
  "type": "IAMUser",
  "principalId": "AIDAABCDEFGHijklMNOPQ",
  "arn": "arn:aws:iam::012345678910:user/Alice",
  "accountId": "012345678910",
  "accessKeyId": "AKIDEXAMPLE",
  "userName": "Alice"
},
{
  "eventTime": "2014-03-24T21:07:15Z",
  "eventSource": "cloudformation.amazonaws.com",
  "eventName": "DeleteStack",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "stackName": "my-test-stack"
  },
  "responseElements": null,
  "requestID": "42dae739-b398-11e3-bb75-a5b75389b02d",
  "eventID": "4965eb38-5705-4942-bb7f-20ebe79aa9aa"
}
```

Sicurezza dell'infrastruttura in AWS CloudFormation

In quanto servizio gestito, AWS CloudFormation è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS CloudFormation attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi richiamare queste operazioni API da qualsiasi posizione di rete, AWS CloudFormation ma supportano politiche di accesso basate sulle risorse, che possono includere restrizioni basate sull'indirizzo IP di origine. Puoi anche utilizzare AWS CloudFormation le policy per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) specifici o specifici. VPCs In effetti, questo isola l'accesso alla rete a una determinata AWS CloudFormation risorsa solo dal VPC specifico all'interno AWS della rete.

Resilienza in AWS CloudFormation

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

Convalida della conformità per AWS CloudFormation

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Governance e conformità per la sicurezza](#): queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- [Riferimenti sui servizi conformi ai requisiti HIPAA](#): elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.

- [AWS Risorse per](#) la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Analisi della configurazione e delle vulnerabilità in AWS CloudFormation

La configurazione e i controlli IT sono una responsabilità condivisa tra voi AWS e voi, nostri clienti. Per ulteriori informazioni, consulta il [modello di responsabilità AWS condivisa](#).

Best practice di sicurezza per CloudFormation

AWS CloudFormation fornisce una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Argomenti

- [Utilizza IAM per controllare gli accessi](#)
- [Non incorporare le credenziali nei modelli](#)
- [Utilizzato AWS CloudTrail per registrare CloudFormation le chiamate](#)

Utilizza IAM per controllare gli accessi

IAM è un AWS servizio che puoi utilizzare per gestire gli utenti e le relative autorizzazioni. AWS Puoi utilizzare IAM con CloudFormation per specificare quali CloudFormation azioni gli utenti possono eseguire, come visualizzare modelli di stack, creare stack o eliminare stack. Inoltre, chiunque gestisca gli CloudFormation stack richiederà le autorizzazioni per le risorse all'interno di tali stack. Ad esempio, se gli utenti desiderano avviare, aggiornare o chiudere EC2 le istanze Amazon, devono avere l'autorizzazione a richiamare le azioni Amazon EC2 pertinenti. CloudFormation

Nella maggior parte dei casi, gli utenti richiedono l'accesso completo per gestire tutte le risorse in un modello. CloudFormation esegue chiamate per creare, modificare ed eliminare tali risorse per conto degli utenti. Per separare le autorizzazioni tra un utente e il CloudFormation servizio, utilizza un ruolo di servizio. CloudFormation utilizza la politica del ruolo di servizio per effettuare chiamate anziché la politica dell'utente. Per ulteriori informazioni, consulta [AWS CloudFormation ruolo di servizio](#).

Non incorporare le credenziali nei modelli

Invece di incorporare informazioni sensibili nei CloudFormation modelli, consigliamo di utilizzare riferimenti dinamici nel modello di stack.

I riferimenti dinamici offrono un modo compatto e potente per fare riferimento a valori esterni archiviati e gestiti in altri servizi, come AWS Systems Manager Parameter Store o AWS Secrets Manager. Quando si utilizza un riferimento dinamico, CloudFormation recupera il valore del riferimento specificato quando necessario durante le operazioni di stack e change set e passa il valore alla risorsa appropriata. Tuttavia, CloudFormation non memorizza mai il valore di riferimento effettivo. Per ulteriori informazioni, consulta [Ottieni valori archiviati in altri servizi utilizzando riferimenti dinamici](#).

[AWS Secrets Manager](#) consente di crittografare, archiviare e utilizzare in modo sicuro le credenziali per database e altri servizi. AWS Archivio parametri di [Systems Manager](#) fornisce uno storage sicuro e gerarchico per la gestione dei dati di configurazione.

Per ulteriori informazioni sulla definizione dei parametri del modello, consulta [CloudFormation Parameters sintassi del modello](#).

Utilizzato AWS CloudTrail per registrare CloudFormation le chiamate

AWS CloudTrail tiene traccia di chiunque effettui chiamate CloudFormation API nel tuo Account AWS. Le chiamate API vengono registrate ogni volta che qualcuno utilizza l' CloudFormation API, la CloudFormation console, una console di back-end o i comandi. CloudFormation AWS CLI Attivare la registrazione e specificare un bucket Amazon S3 in cui archiviare i log. In questo modo, in caso di necessità, puoi controllare chi ha effettuato quale chiamata CloudFormation nel tuo account. Per ulteriori informazioni, consulta [Registrazione delle chiamate AWS CloudFormation API con AWS CloudTrail](#).

Accesso CloudFormation tramite un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. CloudFormation Puoi accedere CloudFormation come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. CloudFormation

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a CloudFormation.

CloudFormation supporta l'effettuazione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Considerazioni sugli endpoint CloudFormation VPC

Prima di configurare un endpoint di interfaccia, assicurati di aver soddisfatto i prerequisiti nell'argomento [Accedere a un AWS servizio utilizzando un endpoint VPC](#) con interfaccia nella Guida.AWS PrivateLink

I seguenti prerequisiti e considerazioni aggiuntivi si applicano alla configurazione di un endpoint di interfaccia per: CloudFormation

- Se hai risorse all'interno del tuo VPC che devono rispondere a una richiesta di risorse personalizzata o a una condizione di attesa, assicurati che abbiano accesso ai bucket Amazon

CloudFormation S3 specifici richiesti. CloudFormation [dispone di bucket S3 in ogni regione per monitorare le risposte a una richiesta di risorse personalizzata o a una condizione di attesa](#). Se un modello include risorse personalizzate o condizioni di attesa in un VPC, la policy di endpoint VPC deve consentire agli utenti di inviare risposte ai seguenti bucket:

- Per le risorse personalizzate, consenti il traffico verso il bucket `cloudformation-custom-resource-response-region`. Quando si utilizzano risorse personalizzate, Regione AWS i nomi non contengono trattini. Ad esempio `uswest2`.
- Per le condizioni di attesa, consenti il traffico verso il bucket `cloudformation-waitcondition-region`. Quando si utilizzano le condizioni di attesa, Regione AWS i nomi contengono trattini. Ad esempio `us-west-2`.

Se la policy dell'endpoint blocca il traffico verso questi bucket, CloudFormation non riceverà risposte e l'operazione stack avrà esito negativo. Ad esempio, se disponi di una risorsa in un VPC nella Regione `us-west-2` che deve rispondere a una condizione di attesa, la risorsa deve essere in grado di inviare una risposta al bucket `cloudformation-waitcondition-us-west-2`.

Per un elenco di Regioni AWS dove CloudFormation è attualmente disponibile, consulta la pagina degli [AWS CloudFormation endpoint e delle quote](#) nel. Riferimenti generali di Amazon Web Services

- Gli endpoint VPC attualmente non supportano le richieste interregionali: assicurati di creare l'endpoint nella stessa regione in cui intendi effettuare le chiamate API. CloudFormation
- Gli endpoint VPC supportano solo il DNS fornito da Amazon tramite Route 53. Se si desidera utilizzare il proprio DNS, è possibile usare l'inoltro condizionale sul DNS. Per ulteriori informazioni, consulta i [set di opzioni DHCP in Amazon VPC](#) nella Amazon VPC User Guide.
- Il gruppo di sicurezza collegato all'endpoint VPC deve consentire le connessioni in entrata sulla porta 443 dalla sottorete privata del VPC.

Creazione di un endpoint VPC interfaccia per l' CloudFormation

Puoi creare un endpoint VPC per CloudFormation utilizzare la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint VPC](#) nella Guida di AWS PrivateLink .

Crea un endpoint di interfaccia per CloudFormation utilizzare il seguente nome di servizio:

- `com.amazonaws. region. formazione di nuvole`

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API CloudFormation utilizzando il nome DNS regionale predefinito. Ad esempio `cloudformation.us-east-1.amazonaws.com`.

Creazione di una policy di endpoint VPC per l' CloudFormation

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo CloudFormation tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito CloudFormation dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta [Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint](#) nella Guida.AWS PrivateLink

Esempio: policy di endpoint VPC per le operazioni dell' CloudFormation

Di seguito è riportato un esempio di policy sugli endpoint per. CloudFormation Se associata a un endpoint, questa politica consente l'accesso alle CloudFormation azioni elencate per tutti i principali su tutte le risorse. L'esempio seguente nega a tutti gli utenti l'autorizzazione a creare stack tramite l'endpoint VPC e consente l'accesso completo a tutte le altre azioni sul servizio. CloudFormation

```
{
  "Statement": [
    {
      "Action": "cloudformation:*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    },
    {
      "Action": "cloudformation:CreateStack",
      "Effect": "Deny",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

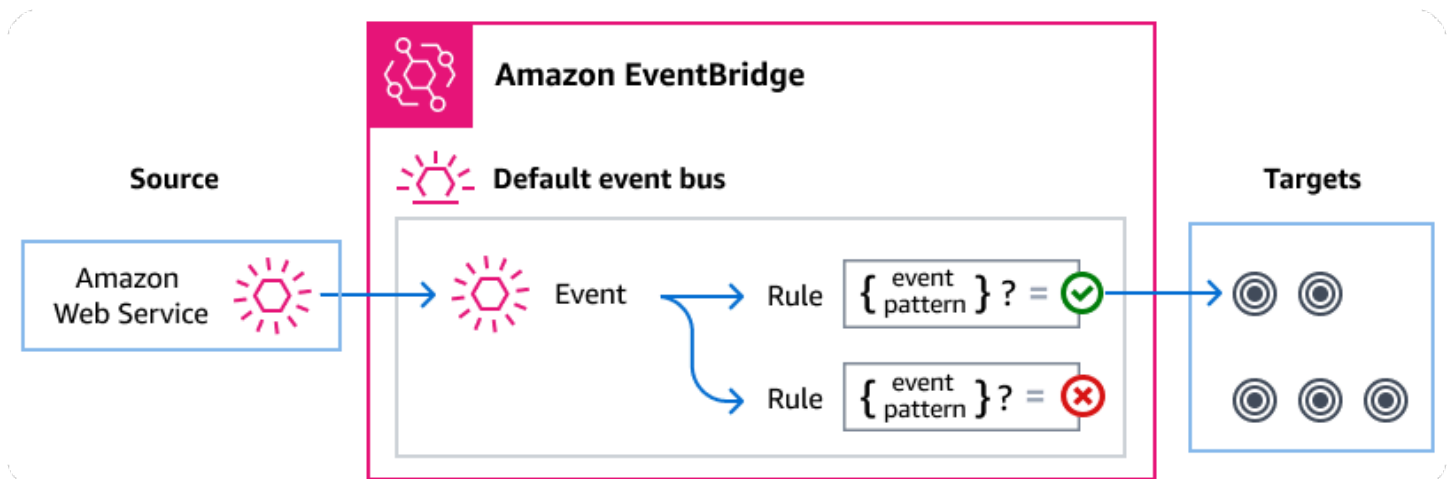
```
}  
]  
}
```

Monitoraggio CloudFormation e sincronizzazione degli eventi Git con EventBridge

Amazon EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, semplificando la creazione di applicazioni scalabili basate sugli eventi. L'architettura basata su eventi è uno stile di creazione di sistemi software ad accoppiamento debole che interagiscono emettendo e rispondendo a eventi. Gli eventi rappresentano un cambiamento in una risorsa o in un ambiente.

Come molti AWS servizi, CloudFormation genera e invia eventi al bus eventi EventBridge predefinito, che viene fornito automaticamente in ogni Account AWS. Un router di eventi è un router che riceve eventi e li invia a nessuna o a più destinazioni o target. Le regole specificate per il bus degli eventi valutano gli eventi non appena arrivano. Ogni regola verifica se un evento corrisponde al modello di evento della regola. Se l'evento corrisponde, il bus degli eventi invia l'evento alle destinazioni specificate.

Per ulteriori informazioni, consulta la sezione Guida [introduttiva ad Amazon EventBridge](#) nella Amazon EventBridge User Guide.



Argomenti

- [CloudFormation e panoramica degli eventi di sincronizzazione Git](#)
- [EventBridge Autorizzazioni Amazon](#)
- [Creazione di un modello di evento personalizzato per una EventBridge regola](#)
- [CloudFormation riferimento ai dettagli degli eventi](#)

CloudFormation e panoramica degli eventi di sincronizzazione Git

CloudFormation invia eventi EventBridge ogni volta che viene eseguita un'operazione di creazione, aggiornamento, eliminazione o rilevamento della deriva su uno stack. CloudFormation invia anche eventi EventBridge per modificare lo stato dei set di stack e delle istanze di stack set. È possibile utilizzare EventBridge le regole per indirizzare gli eventi verso obiettivi definiti. La consegna di questi eventi è garantita e potrebbero non funzionare correttamente.

Poiché CloudFormation gli eventi rappresentano modifiche agli stack o ai set di stack e alle relative risorse, è possibile utilizzarli per avviare flussi di lavoro associati ai rispettivi eventi. Per esempio:

- Crea tag specifici per stack o set di stack su tutte le risorse fornite tramite CloudFormation.
- Stabilisci un'associazione tra uno CloudFormation stack o un set di stack e un Amazon WorkSpaces Application Manager (Amazon WAM).
- Specificate un'associazione con uno AppRegistry per lo stack o il set di stack creato.

I seguenti eventi vengono generati CloudFormation e inviati al bus di eventi predefinito in EventBridge. Per ulteriori informazioni, consulta [???](#).

Tipo di evento	Descrizione	Origine eventi
Modifica dello stato delle risorse	Qualsiasi aggiornamento eseguito su uno stack che modifica le proprietà delle risorse sottostanti. Per un elenco completo dei tipi di AWS risorse supportati, consulta il riferimento ai tipi di AWS risorse e proprietà .	AWS CloudFormation
Modifica dello stato dello stack	Rappresenta una modifica dello stato di un determinato stack. Per i dettagli del codice, consulta Codici di stato dello stack .	AWS CloudFormation
Modifica dello stato di rilevamento della deriva	Rappresenta un aggiornamento del rilevamento delle deviazioni avviato dall'utente su un determinato stack.	AWS CloudFormation

Tipo di evento	Descrizione	Origine eventi
	Per un elenco completo dei tipi completamente mutabili e immutabili che supportano il rilevamento della deriva, vedere Supporto per tipi di risorse	
StackSetModifica dello stato	Rappresenta una modifica dello stato di un determinato set di stack.	AWS CloudFormation
StackSet Modifica dello stato dell'istanza Stack	Rappresenta una modifica dello stato di un'istanza dello StackSet stack specifica. Per i dettagli sul codice, vedere Codici di stato delle istanze di stack .	AWS CloudFormation
StackSet stato dell'operazione	Rappresenta una modifica dello stato di una determinata StackSet operazione. Per i dettagli sul codice, vedere StackSets codici di stato .	AWS CloudFormation

Inoltre, AWS CloudFormation Git sync invia eventi per le modifiche di stato per le sincronizzazioni dei repository e le sincronizzazioni delle risorse con EventBridge.

I seguenti eventi di sincronizzazione Git vengono generati CodeConnections e inviati al bus eventi predefinito in EventBridge. Per ulteriori informazioni, consulta [???](#).

Tipo di evento	Descrizione	Origine eventi
Modifica dello stato di sincronizzazione del repository	Rappresenta una modifica dello stato di una sincronizzazione del repository Git.	AWS CodeConnections
Modifica dello stato di sincronizzazione delle risorse	Rappresenta una modifica dello stato di una sincronizzazione delle risorse Git.	AWS CodeConnections

EventBridge Autorizzazioni Amazon

CloudFormation non richiede autorizzazioni aggiuntive per l'organizzazione di eventi. EventBridge Gli eventi contengono informazioni già disponibili tramite le CloudFormation operazioni API.

Le destinazioni specificate potrebbero richiedere autorizzazioni o configurazioni specifiche. Per maggiori dettagli sull'utilizzo di servizi specifici per gli obiettivi, consulta [Amazon EventBridge targets](#) nella Amazon EventBridge User Guide.

Creazione di un modello di evento personalizzato per una EventBridge regola

Puoi trovare diversi modelli predefiniti negli eventi EventBridge for CloudFormation e Git sync. Ciò semplifica il modo in cui viene creato un modello di eventi. Invece di scrivere modelli di eventi personalizzati, puoi selezionare i valori dei campi su un modulo e EventBridge generare lo schema automaticamente. È possibile creare una nuova regola utilizzando uno di questi modelli di eventi predefiniti o creare un modello di evento personalizzato.

Quando un servizio come CloudFormation invia un evento al bus di eventi predefinito, EventBridge utilizza lo schema di eventi definito nella regola per determinare se l'evento deve essere inviato ai destinatari della regola. Un modello di eventi corrisponde ai dati negli CloudFormation eventi desiderati.

Ogni modello di evento è un oggetto JSON che contiene:

- Un `source` attributo che identifica il servizio da cui proviene l'evento. Ad esempio `aws.cloudformation` o `aws.codeconnections`.
- (Facoltativo): Un attributo `detail-type` che contiene una serie di tipi di eventi da abbinare.
- (Facoltativo): Un attributo `detail` contenente qualsiasi altro dato relativo all'evento da abbinare.

Ad esempio, l'ID dello stack, le risorse coinvolte, lo stato delle varie risorse e altri dati relativi a un particolare tipo di eventi.

Ad esempio, il seguente schema di eventi corrisponde a tutti gli eventi di modifica dello stato delle risorse:

```
{
```



```
"source": ["aws.cloudformation"],
"detail-type": ["CloudFormation Resource Status Change"]
}
```

Mentre il seguente modello di eventi utilizza i dati di dettaglio degli eventi per abbinare solo gli eventi di modifica dello stato delle risorse, in cui CloudFormation crea una nuova `AWS::S3::Bucket` o `AWS::SNS::Topic` risorsa:

```
{
  "source": ["aws.cloudformation"],
  "detail-type": ["CloudFormation Resource Status Change"],
  "detail": {
    "status-details": {
      "status": ["CREATE_COMPLETE"]
    },
    "resource-type": ["AWS::S3::Bucket", "AWS::SNS::Topic"]
  }
}
```

Per ulteriori informazioni sulla scrittura di pattern di eventi, consulta [Event pattern](#) nella Amazon EventBridge User Guide.

CloudFormation riferimento ai dettagli degli eventi

Tutti gli eventi AWS dei servizi dispongono di un set comune di campi contenenti metadati relativi all'evento, ad esempio il AWS servizio da cui è generato l'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è verificato l'evento e altri. Per le definizioni di questi campi generali, consulta i [metadati degli eventi di AWS servizio](#) nella Guida agli AWS eventi.

Inoltre, ogni evento ha un campo `detail` che contiene dati specifici per quel particolare evento. Il riferimento seguente definisce i campi di dettaglio per i vari CloudFormation eventi.

Quando si utilizza EventBridge per selezionare e gestire CloudFormation eventi, è utile tenere presente quanto segue:

- Il `source` campo specifica l'origine dell'evento.

Ad esempio `aws.cloudformation` o `aws.codeconnections`.

- Il campo `detail-type` specifica il tipo di evento.

Ad esempio CloudFormation Resource Status Change o CloudFormation Drift Detection Status Change.

- Il campo `detail` contiene i dati specifici di quel particolare evento.

Ad esempio, l'ID dello stack, le risorse coinvolte, lo stato delle varie risorse e altri dati relativi a un particolare tipo di eventi.

Per informazioni sulla creazione di modelli di eventi che consentono alle regole di abbinare CloudFormation gli eventi, consulta [Event pattern](#) nella Amazon EventBridge User Guide.

Per ulteriori informazioni sugli eventi e su come li EventBridge elabora, consulta [EventBridge gli eventi](#) nella Amazon EventBridge User Guide.

Argomenti

- [Dettagli dell'evento Resource Status Change](#)
- [Dettagli dell'evento Stack Status Change](#)
- [Drift Detection Status Modifica i dettagli dell'evento](#)
- [StackSet Dettagli dell'evento Status Change](#)
- [StackSet Dettagli dell'evento Stack Instance Status Change](#)
- [StackSet Dettagli dell'evento Operation Status Change](#)
- [Repository Sync Status Modifica dettagli dell'evento](#)
- [Resource Sync Status Modifica dettagli dell'evento](#)

Dettagli dell'evento Resource Status Change

Di seguito sono riportati i campi di dettaglio per gli eventi di modifica dello stato delle risorse.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "CloudFormation Resource Status Change",
  "source": "aws.cloudformation",
  . . . ,
}
```

```
"detail": {
  "stack-id" : "string",
  "logical-resource-id" : "string",
  "physical-resource-id": "string",
  "status-details": {
    "status": "string",
    "status-reason": "string"
  },
  "resource-type": "string",
  "client-request-token": "string"
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi sullo stato delle risorse, questo valore è `CloudFormation Resource Status Change`.

source

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è `aws.cloudformation`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi sullo stato delle risorse, questi dati includono:

stack-id

L'ID stack univoco associato allo stack.

logical-resource-id

Il nome logico della risorsa, come specificato nel modello.

physical-resource-id

Il nome o l'identificatore univoco che corrisponde a un ID di istanza fisica di una risorsa supportata da CloudFormation.

status-details

status

Stato della risorsa.

status-reason

Motivo dello stato della risorsa.

resource-type

Tipo di risorsa. Ad esempio `AWS::S3::Bucket`.

client-request-token

Un token di accesso utilizzato per richiamare l'API. A tutti gli eventi che vengono attivati da una determinata operazione dello stack viene assegnato lo stesso token di richiesta client, che puoi utilizzare per monitorare le operazioni. Le operazioni di stack avviate dalla console utilizzano il formato token Console - StackOperation -ID, che consente di identificare facilmente l'operazione dello stack. Ad esempio, se crei uno stack utilizzando la console, a ogni evento stack risultante verrà assegnato lo stesso token nel formato seguente: `Console-CreateStack-7f59c3cf-00d2-40c7-b2ff-e75db0987002`.

Example Esempio: evento Resource Status Change

Di seguito è riportato un esempio per l'evento di stato della risorsa. Questo evento descrive in dettaglio che CloudFormation la risorsa richiesta, un bucket Amazon S3, è stata creata con successo nello stack specificato.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "CloudFormation Resource Status Change",
  "source": "aws.cloudformation",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack"
  ],
  "detail": {
    "stack-id": "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack",
    "logical-resource-id": "my-s3-bucket",
```

```
    "physical-resource-id":"arn:aws:s3::my-s3-bucket-us-east-1",
    "status-details":{
        "status":"CREATE_COMPLETE",
        "status-reason":""
    },
    "resource-type":"AWS::S3::Bucket",
    "client-request-token":""
}
```

Dettagli dell'evento Stack Status Change

Di seguito sono riportati i campi di dettaglio per gli eventi Stack Status Change.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type":"CloudFormation Stack Status Change",
  "source":"aws.cloudformation",
  . . . ,
  "detail":{
    "stack-id":"string",
    "status-details":{
      "status":"string",
      "status-reason":"string"
    },
    "client-request-token":"string"
  }
}
```

`detail-type`

Identifica il tipo di evento.

Per gli eventi sullo stato dello stack, questo valore è `CloudFormation Stack Status Change`.

`source`

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è `aws.cloudformation`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi sullo stato dello stack, questi dati includono:

stack-id

L'ID stack univoco associato allo stack.

status-details

status

Lo stato dello stack.

Per un elenco completo dei codici di stato dello stack, vedere [Codici di stato dello stack](#).

status-reason

Motivo dello stato della risorsa.

client-request-token

Un token di accesso utilizzato per richiamare l'API. A tutti gli eventi che vengono attivati da una determinata operazione dello stack viene assegnato lo stesso token di richiesta client, che puoi utilizzare per monitorare le operazioni. Le operazioni di stack avviate dalla console utilizzano il formato token Console - StackOperation -ID, che consente di identificare facilmente l'operazione dello stack. Ad esempio, se crei uno stack utilizzando la console, a ogni evento stack risultante verrà assegnato lo stesso token nel formato seguente: Console-CreateStack-7f59c3cf-00d2-40c7-b2ff-e75db0987002.

Example Esempio: evento Stack Status

Di seguito è riportato un esempio di evento di stato dello stack, in cui CloudFormation è stato creato con successo lo stack richiesto, `teststack`

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "CloudFormation Stack Status Change",
  "source": "aws.cloudformation",
```

```

    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack"
    ],
    "detail": {
        "stack-id": "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack",
        "status-details": {
            "status": "CREATE_COMPLETE",
            "status-reason": ""
        },
        "client-request-token": ""
    }
}

```

Drift Detection Status Modifica i dettagli dell'evento

Di seguito sono riportati i campi di dettaglio per gli eventi di stato di rilevamento delle deviazioni nello stack.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```

{
    . . . ,
    "detail-type": "CloudFormation Drift Detection Status Change",
    "source": "aws.cloudformation",
    . . . ,
    "detail": {
        "stack-id": "string",
        "stack-drift-detection-id": "string",
        "status-details": {
            "stack-drift-status": "string",
            "detection-status": "string"
        },
        "drift-detection-details": {
            "drifted-stack-resource-count": integer
        },
        "client-request-token": "string"
    }
}

```

detail-type

Identifica il tipo di evento.

Per gli eventi di rilevamento delle deviazioni nello stack, questo valore è `CloudFormation Drift Detection Status Change`.

source

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è `aws.cloudformation`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi di rilevamento delle deviazioni nello stack, questi dati includono:

stack-id

L'ID stack univoco associato allo stack.

stack-drift-detection-id

L'ID del rilevamento delle deviazioni nello stack.

status-details

stack-drift-status

Stato della deviazione dello stack.

detection-status

Stato dell'operazione di rilevamento delle deviazioni.

drift-detection-details

drifted-stack-resource-count

Il numero di risorse in deviazione. Quando il valore è `-1`, il rilevamento delle deviazioni è in corso. Tutti gli altri numeri interi non negativi rappresentano il numero effettivo di risorse in deviazione.

client-request-token

Un token di accesso utilizzato per richiamare l'API. A tutti gli eventi che vengono attivati da una determinata operazione dello stack viene assegnato lo stesso token di richiesta

client, che puoi utilizzare per monitorare le operazioni. Le operazioni di stack avviate dalla console utilizzano il formato token Console- StackOperation -ID, che consente di identificare facilmente l'operazione di stack. Ad esempio, se crei uno stack utilizzando la console, a ogni evento stack risultante verrà assegnato lo stesso token nel formato seguente: Console-CreateStack-7f59c3cf-00d2-40c7-b2ff-e75db0987002.

Example Esempio: evento Stack Drift Detection

Di seguito è riportato un esempio di evento Stack Drift Detection. Questo evento indica se CloudFormation è stato completato il rilevamento della deriva sullo stack specificato e che lo stack ha attualmente uno stato di DRIFTED deriva dovuto a una risorsa alla deriva.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "CloudFormation Drift Detection Status Change",
  "source": "aws.cloudformation",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": ["string"],
  "detail": {
    "stack-id": "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack",
    "stack-drift-detection-id": "624af370-311a-11e8-b6b7-500cexample",
    "status-details": {
      "stack-drift-status": "DRIFTED",
      "detection-status": "DETECTION_COMPLETE"
    },
    "drift-detection-details": {
      "drifted-stack-resource-count": 1
    },
    "client-request-token": ""
  }
}
```

StackSet Dettagli dell'evento Status Change

Di seguito sono riportati i campi di dettaglio per gli eventi di modifica StackSet dello stato.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "CloudFormation StackSet Status Change",
  "source": "aws.cloudformation",
  . . . ,
  "detail": {
    "stack-set-arn" : "string",
    "status-details": {
      "status": "string"
    }
  }
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi relativi StackSet allo stato, questo valore è `CloudFormation StackSet Status Change`.

source

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è `aws.cloudformation`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi relativi agli eventi di StackSet stato, questi dati includono:

stack-set-arn

Il nome della risorsa Amazon (ARN) associato al set di stack.

status-details

status

Lo StackSet stato.

Valori validi: `ACTIVE` | `DELETED`

Example Esempio: evento StackSet Status Change

Di seguito è riportato un esempio di evento StackSet Status Change. Questo evento descrive in dettaglio chi CloudFormation ha eliminato il set di stack specificato.

```
{
  "version": "0",
  "id": "42h6hb90-hg0w-11op-b01v-0xnhh0934z09",
  "detail-type": "CloudFormation StackSet Status Change",
  "source": "aws.cloudformation",
  "account": "111122223333",
  "time": "2021-09-23T17:06:18Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:cloudformation:us-east-1:111122223333:stackset/test12345:3f3a3fbe-c937-4eb3-a87d-e36a0af3f663"
  ],
  "detail": {
    "stack-set-arn" : "arn:aws:cloudformation:us-east-1:111122223333:stackset/test12345:3f3a3fbe-c937-4eb3-a87d-e36a0af3f663",
    "status-details": {
      "status": "DELETED"
    }
  }
}
```

StackSet Dettagli dell'evento Stack Instance Status Change

Di seguito sono riportati i campi di dettaglio per gli eventi relativi allo stato delle istanze dello StackSet stack.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "CloudFormation StackSet StackInstance Status Change",
  "source": "aws.cloudformation",
  . . . ,
  "detail": {
    "stack-set-arn" : "string",
    "stack-id" : "string",
```

```
"action" : "string",
"status-details": {
  "status": "string",
  "status-reason": "string",
  "detailed-status": "string"
}
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi di stato delle istanze dello StackSet stack, questo valore è CloudFormation StackSet StackInstance Status Change.

source

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è aws.cloudformation.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi di stato delle istanze dello StackSet stack, questi dati includono:

stack-set-arn

L'Amazon Resource Name (ARN) associato a. StackSet

stack-id

L'ID stack univoco associato all'istanza di stack.

action

Il tipo di operazione di stack set.

Valori validi: CREATE | UPDATE | DELETE | DETECT_DRIFT

status-details

status

Lo stato dell' StackSet istanza.

Per ulteriori dettagli, consulta [Codici di stato delle istanze di stack](#).

Valori validi: CURRENT | OUTDATED | INOPERABLE

status-reason

Motivo dello stato dell' StackSet istanza.

detailed-status

Lo stato dettagliato dell' StackSet istanza.

Valori validi: CANCELLED FAILED | FAILED_IMPORT | INOPERABLE | PENDING | RUNNING
| SKIPPED_SUSPENDED_ACCOUNT | SUCCEEDED

Example Esempio: evento StackSet Stack Instance Status Change

Di seguito è riportato un esempio di evento StackSet Stack Instance Status Change.

```
{
  "version": "0",
  "id": "42h6hb90-hg0w-11op-b01v-0xnhh0934z09",
  "detail-type": "CloudFormation StackSet StackInstance Status Change",
  "source": "aws.cloudformation",
  "account": "111122223333",
  "time": "2021-09-22T19:19:23Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:cloudformation:us-east-1:111122223333:stackset/test1234:e5f54eea-d041-44ad-94f8-b8268aca1e59"
  ],
  "detail": {
    "stack-set-arn": "arn:aws:cloudformation:us-east-1:111122223333:stackset/test1234:e5f54eea-d041-44ad-94f8-b8268aca1e59",
    "stack-id": "arn:aws:cloudformation:us-west-1:111122223333:stack/teststack",
    "status-details": {
      "status": "OUTDATED",
      "status-reason": "User Initiated",
      "detailed-status": "PENDING"
    }
  }
}
```

StackSet Dettagli dell'evento Operation Status Change

Di seguito sono riportati i campi di dettaglio per gli eventi di modifica dello stato StackSet dell'operazione.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "CloudFormation StackSet Operation Status Change",
  "source": "aws.cloudformation",
  . . . ,
  "detail": {
    "stack-set-arn" : "string",
    "stack-set-operation-id" : "string",
    "status-details": {
      "status": "string"
    }
  }
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi relativi allo stato dell' StackSet operazione, questo valore è `CloudFormation StackSet Operation Status Change`.

source

Identifica il servizio che ha generato l'evento. Per CloudFormation gli eventi, questo valore è `aws.cloudformation`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi relativi allo stato dell' StackSet operazione, questi dati includono:

stack-set-arn

L'Amazon Resource Name (ARN) associato a. StackSet

stack-set-operation-id

L'ID univoco associato all' StackSetoperazione.

status-details

status

Lo stato StackSet dell'operazione.

Per ulteriori dettagli, consulta [StackSets codici di stato](#).

Valori validi: RUNNING | SUCCEEDED | FAILED | STOPPING | STOPPED | QUEUED

Example Esempio: evento StackSet Operation Status Change

Di seguito è riportato un esempio di evento StackSet Operation Status Change. I dettagli dell'evento che CloudFormation ha completato con successo l'operazione richiesta sullo stack set specificato.

```
{
  "version": "0",
  "id": "4de89905-fd92-6a6b-9509-23c04bcb6a21",
  "detail-type": "CloudFormation StackSet Operation Status Change",
  "source": "aws.cloudformation",
  "account": "111122223333",
  "time": "2021-09-22T05:46:24Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:cloudformation:us-east-1:111122223333:stackset/test1234:e5f54eea-d041-44ad-94f8-b8268aca1e59"
  ],
  "detail": {
    "stack-set-arn": "arn:aws:cloudformation:us-east-1:111122223333:stackset/test1234:e5f54eea-d041-44ad-94f8-b8268aca1e59",
    "stack-set-operation-id": "ce69adce-2221-4483-8c4b-c51f284f25e8",
    "status-details": {
      "status": "SUCCEEDED"
    }
  }
}
```

Repository Sync Status Modifica dettagli dell'evento

Di seguito sono riportati i campi di dettaglio per gli eventi di modifica dello stato di Repository Sync.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "Git Sync Repository Sync Status Change",
  "source": "aws.codeconnections",
  . . . ,
  "detail": {
    "connectionArn" : "string",
    "providerType" : "string",
    "repositoryName": "string",
    "providerType": "string",
    "repositoryName": "string",
    "repositoryArn": "string",
    "repositoryLinkId": "string",
    "ownerId": "string",
    "commit": "string",
    "branch": "string",
    "syncType": "string",
    "status": "string",
    "previousSync": "string"
  }
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi di stato di Repository Sync, questo valore è `Git Sync Repository Sync Status Change`.

source

Identifica il servizio che ha generato l'evento. Per gli eventi di sincronizzazione Git, questo valore è `aws.codeconnections`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi sullo stato di sincronizzazione del repository, questi dati includono:

connectionArn

L'Amazon Resource Name (ARN) associato a CodeConnections

providerType

Il provider Git a cui si è connesso CloudFormation.

Valori validi: GitHub | GitHub Enterprise | GitLab | BitBucket

repositoryName

Il nome del repository Git.

repositoryArn

L'ARN associato al repository Git.

repositoryLinkId

L'ID univoco associato al link del repository.

ownerId

L'ID univoco associato al proprietario del repository.

commit

L'ID univoco associato al commit del repository.

branch

L'ID univoco associato al ramo del repository.

syncType

Il tipo di sincronizzazione che viene eseguita.

status

Lo stato attuale di sincronizzazione del repository.

Valori validi: FAILED | INITIATED | IN_PROGRESS | SUCCEEDED

previousSync

Lo stato di sincronizzazione precedente allo stato corrente.

Valori validi: FAILED | INITIATED | IN_PROGRESS | SUCCEEDED

Example Esempio: evento Repository Sync Status Change

Di seguito è riportato un esempio di evento Repository Sync Status Change. I dettagli dell'evento che CodeConnections ha sincronizzato correttamente il repository.

```
{
  "version": "0",
  "id": "1b5d8feb-agbv-4cf7-a9f1-bf3703467718",
  "detail-type": "GitSync Repository Sync Status Change",
  "source": "aws.codeconnections",
  "account": "111122223333",
  "time": "2023-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:aws:codestar-connections:us-east-1:111122223333:repository-link/550e8400-e29b-41d4-a716-446655440000"],
  "detail": {
    "connectionArn": "arn:aws:codestar-connections:us-east-1:111122223333:connection/sample-connection-id",
    "providerType": "GitHub",
    "repositoryName": "sample-repository-name",
    "repositoryArn": "arn:aws:aws:codestar-connections:us-east-1:111122223333:repository-link/550e8400-e29b-41d4-a716-446655440000",
    "repositoryLinkId": "550e8400-e29b-41d4-a716-446655440000",
    "ownerId": "sample-owner-id",
    "commit": "sample-commit-id",
    "branch": "main",
    "syncType": "CFN_STACK_SYNC",
    "status": "SUCCEEDED",
    "previousStatus": "IN_PROGRESS",
  }
}
```

Resource Sync Status Modifica dettagli dell'evento

Di seguito sono riportati i campi di dettaglio per gli eventi di modifica dello stato di Resource Sync.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per AWS CloudFormation gli eventi.

```
{
  . . . ,
  "detail-type": "Git Sync Resource Sync Status Change",
```

```
"source": "aws.codeconnections",  
.  
.  
.  
"detail": {  
  "providerType" : "string",  
  "commit" : "string",  
  "repositoryName": "string",  
  "branch": "string",  
  "syncType": "string",  
  "syncTarget": "string",  
  "status": "string",  
  "previousSync": "string"  
}  
}
```

detail-type

Identifica il tipo di evento.

Per gli eventi di stato di Repository Sync, questo valore è `Git Sync Repository Sync Status Change`.

source

Identifica il servizio che ha generato l'evento. Per gli eventi di sincronizzazione Git, questo valore è `aws.codeconnections`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per gli eventi sullo stato di sincronizzazione delle risorse, questi dati includono:

providerType

Il provider Git a cui si è connesso CloudFormation.

Valori validi: `GitHub` | `GitHub Enterprise` | `GitLab` | `BitBucket`

commit

L'ID univoco associato al commit del repository.

repositoryName

Il nome del repository Git.

branch

L'ID univoco associato al ramo del repository.

syncType

Il tipo di sincronizzazione che viene eseguita.

syncTarget

Lo stack di destinazione per la sincronizzazione delle risorse.

status

Lo stato attuale di sincronizzazione del repository.

Valori validi: FAILED | INITIATED | IN_PROGRESS | SUCCEEDED

previousSync

Lo stato di sincronizzazione precedente allo stato corrente.

Valori validi: FAILED | INITIATED | IN_PROGRESS | SUCCEEDED

Example Esempio: evento Resource Sync Status Change

Di seguito è riportato un esempio di evento di modifica dello stato di sincronizzazione delle risorse. I dettagli dell'evento che CodeConnections ha sincronizzato correttamente la risorsa.

```
{
  "version": "0",
  "id": "1b5d8feb-agbv-4cf7-a9f1-bf3703467718",
  "detail-type": "Git Sync Resource Sync Status Change",
  "source": "aws.codeconnections",
  "account": "111122223333",
  "time": "2023-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:aws:cloudformation:us-east-1:111122223333:stack/targetStack1"],
  "detail": {
    "providerType": "GitHub",
    "commit": "sample-commit-id",
    "repositoryName": "sample-repository-name",
    "branch": "main",
    "syncType": "CFN_STACK_SYNC",
```

```
"syncTarget": "arn:aws:aws:cloudformation:us-east-1:111122223333:stack/  
targetStack1",  
  "status": "SUCCEEDED",  
  "previousStatus": "IN_PROGRESS"  
}  
}
```

Comprendi le CloudFormation quote

Hai delle CloudFormation quote Account AWS che potresti aver bisogno di conoscere quando crei modelli e crei pile. Comprendendo questi limiti, è possibile evitare gli errori di limitazione che potrebbero richiedere di riprogettare i modelli o gli stack.

La tabella seguente mostra le quote. CloudFormation

Quote	Descrizione	Valore	Strategia di ottimizzazione
cfn-signal dati sulle condizioni di attesa	La quantità massima di dati che cfn-signal possono essere trasmessi.	4,096 byte	Per trasferire una quantità maggiore, invia i dati a un bucket Amazon S3, quindi usali cfn-signal per passare l'URL di Amazon S3 a quel bucket.
Risposta di risorsa personalizzata	La quantità massima di dati che un provider di risorse personalizzato può trasmettere.	4,096 byte	
Riferimenti dinamici per modello	Il numero massimo di riferimenti dinamici consentiti in un unico modello di CloudFormation pila.	60 riferimenti dinamici in un modello di pila	
Hooks per account	Il numero massimo di Hooks consentito per account per regione.	100 hook	
Hook per risorsa	Il numero massimo di Hooks che possono	100 hook	

Quote	Descrizione	Valore	Strategia di ottimizzazione
	essere configurati per risorsa.		
Dimensione di configurazione del gancio	La quantità massima di dati di configurazione che un Hook può memorizzare.	204.8 KB	
Mappature	Il numero massimo di mappature che puoi dichiarare nel tuo modello. CloudFormation	200 mappature	Per specificare più mappature, suddividi il modello in più modelli utilizzando, ad esempio, gli stack nidificati .
Attributi di mappatura	Il numero massimo di attributi di mappatura per ogni mappatura che puoi dichiarare e nel tuo modello. CloudFormation	200 attributi	Per specificare altri attributi di mappatura, separa gli attributi in più mappature.
Nome della mappatura e nome dell'attributo della mappatura	La dimensione massima di ogni nome di mappatura.	255 caratteri	
Modules	Il numero massimo di moduli che è possibile registrare nel CloudFormation registro, per account e regione.	100 moduli	

Quote	Descrizione	Valore	Strategia di ottimizzazione
Versioni dei moduli	Il numero massimo di versioni che è possibile registrare nel CloudFormation registro per un determinato modulo.	100 versioni	Per registrare nuove versioni, utilizza innanzitutto DeregisterType per annullare la registrazione delle versioni che non utilizzi più.
Stack nidificati	Il numero massimo di CloudFormation risorse che uno stack annidato può creare, aggiornare o eliminare per operazione. Ad esempio, è possibile disporre di una gerarchia di stack annidati con più di 2500 risorse totali, ma non è possibile creare, aggiornare o eliminare più di 2500 di tali risorse in una singola distribuzione.	2.500 risorse	Dividi la gerarchia dello stack in stack diversi.
Output	Il numero massimo di output che puoi dichiarare nel tuo modello. CloudFormation	200 output	

Quote	Descrizione	Valore	Strategia di ottimizzazione
Nome output	La dimensione massima di un nome di output.	255 caratteri	
Parametri	Il numero massimo di parametri che puoi dichiarare nel tuo CloudFormation modello.	200 parametri	Per specificare più parametri, puoi utilizzare le mappature o gli elenchi per assegnare più valori a un singolo parametro.
Nome del parametro	La dimensione massima del nome di un parametro.	255 caratteri	
Valore del parametro	La dimensione massima del valore di un parametro.	4,096 byte	Per utilizzare un valore parametri zzato più grande, create più parametri e quindi utilizzate la <code>Fn::Join</code> funzione per concatenare più valori in un unico valore.
Risorse private	Il numero massimo di risorse private che è possibile registrare nel registro per account, per CloudFormation regione.	50 risorse private	

Quote	Descrizione	Valore	Strategia di ottimizzazione
Versioni delle risorse private	Il numero massimo di versioni che è possibile registrare nel CloudFormation registro per una determinata risorsa privata.	50 risorse private	Per registrare nuove versioni, utilizza innanzitutto DeregisterType per annullare la registrazione delle versioni che non utilizzi più.
Risorse	Il numero massimo di risorse che puoi dichiarare nel tuo modello. CloudFormation	500 risorse	Per specificare più risorse, suddividi il modello in più modelli utilizzando, ad esempio, gli stack nidificati .
Risorse nelle operazioni di stack simultanee	Il numero massimo di risorse che puoi utilizzare nelle operazioni di stack (operazioni di creazione, aggiornamento o eliminazione) nella tua regione in un determinato momento.	Utilizza l' DescribeAccountLimits API per determinare il limite attuale per un account in una regione specifica.	
Nome risorsa	La dimensione massima del nome di una risorsa.	255 caratteri	

Quote	Descrizione	Valore	Strategia di ottimizzazione
Stack	Il numero massimo di CloudFormation pile che è possibile creare.	2000 stack	Per creare più pile, elimina le pile che non ti servono o richiedi un aumento del numero massimo di pile nel tuo Account AWS. Per ulteriori informazioni, consulta Service Quotas di AWS nella Riferimenti generali di AWS.
Stack name (Nome stack)	La dimensione massima del nome di uno stack.	128 caratteri	
StackSets	Il numero massimo di set di CloudFormation stack che puoi creare nel tuo account amministratore.	1000 set di stack	Per creare altri set di stack, elimina i set di stack che non ti servono o richiedi un aumento del numero massimo di set di stack nel tuo Account AWS. Per ulteriori informazioni, consulta Service Quotas di AWS nella Riferimenti generali di AWS.

Quote	Descrizione	Valore	Strategia di ottimizzazione
Istanze di stack	Il numero massimo di istanze di stack che puoi creare per set di stack.	100.000 istanze di stack per set di stack	Per creare più istanze di stack, elimina le istanze di stack che non ti servono o richiedi un aumento del numero massimo di istanze di stack nel tuo Account AWS. Per ulteriori informazioni, consulta Service Quotas di AWS nella Riferimenti generali di AWS.
StackSets operazioni di istanza	Il numero massimo di istanze dello stack, in tutti i set di stack, su cui è possibile eseguire operazioni contemporaneamente in ciascuna regione, per account amministratore.	10.000 operazioni	Questo limite si applica a tutti i set di stack coinvolti in una Regione. Include le istanze di stack interessate dalle operazioni di creazione e aggiornamento dei set di stack, nonché la creazione, l'aggiornamento e l'eliminazione diretta di istanze di stack.
StackSets operazioni in coda	Il numero massimo di operazioni in coda per uno stack impostato in un dato momento.	10.000 operazioni	

Quote	Descrizione	Valore	Strategia di ottimizzazione
Stack importati utilizzando l'operazione S3 object per stack set	Il numero massimo di stack che è possibile importare utilizzando l'operazione S3 object per stack set.	200 stack	
Stack importati utilizzando stack id in linea per operazione di set di stack	Il numero massimo di stack che è possibile importare utilizzando l'operazione inline stack per stack set. IDs	10 pile	
Dimensioni corpo del modelli in una richiesta	La dimensione massima del corpo del modello che puoi passare in una ValidateTemplate richiesta CreateStack UpdateStack , o.	51,200 byte	Per utilizzare un corpo del modello più grande, suddividi il modello in più modelli utilizzando, ad esempio, gli stack nidificati . In alternativa, puoi caricare il modello su un bucket Amazon S3.

Quote	Descrizione	Valore	Strategia di ottimizzazione
Dimensioni corpo del modello in un oggetto Amazon S3	La dimensione massima del corpo del modello che puoi passare in un oggetto Amazon S3 per una <code>ValidateTemplate</code> richiesta con un <code>CreateStack</code> <code>UpdateStack</code> URL del modello Amazon S3.	1 MB	Per utilizzare un corpo del modello più grande, suddividi il modello in più modelli utilizzando, ad esempio, gli stack nidificati . Oppure usa la minificazione per ridurre le dimensioni del CloudFormation modello.
Descrizione del modello	La dimensione massima della descrizione di un modello.	1.024 byte	
Versioni per gancio	Il numero massimo di versioni che puoi creare per Hook.	100 versioni	

Disponibilità delle funzionalità

Non tutte le funzionalità di CloudFormation potrebbero essere disponibili in tutte le regioni. Per ulteriori informazioni Regioni AWS, consulta la [tabella delle regioni dell'infrastruttura globale](#).

- Le [macros](#) attualmente non sono disponibili nella seguente Regione:
 - Asia Pacifico (Giacarta)
- [L'esecuzione di blue/green distribuzioni ECS tramite CodeDeploy utilizzo](#) non CloudFormation è attualmente disponibile nelle seguenti regioni:
 - Africa (Città del Capo)
 - Asia Pacifico (Osaka-Locale)
 - Europa (Milano)

StackSets e macro

StackSets attualmente non supporta la creazione o l'aggiornamento di set di stack con autorizzazioni gestite dal servizio da modelli che contengono macro. Ciò include le trasformazioni, che sono macro ospitate da CloudFormation. Per ulteriori informazioni sulle macro, consulta [Macro di modello](#).

Risoluzione dei problemi CloudFormation

Quando lo usi CloudFormation, potresti riscontrare problemi durante la creazione, l'aggiornamento o l'eliminazione degli stack. CloudFormation Le sezioni seguenti sono utili per risolvere alcuni dei problemi più comuni che possono verificarsi.

Per domande generali sull'argomento CloudFormation, consulta la [AWS CloudFormation FAQs](#). Puoi anche cercare risposte e pubblicare domande nella [CloudFormation community](#) su AWS re:Post.

Argomenti

- [Guida alla risoluzione dei problemi](#)
- [Risoluzione degli errori](#)
- [Contattare il supporto](#)

Guida alla risoluzione dei problemi

Se CloudFormation non riesci a creare, aggiornare o eliminare lo stack, puoi visualizzare i messaggi di errore o i log per aiutarti a saperne di più sul problema. Le seguenti attività descrivono i metodi generali per la risoluzione di un CloudFormation problema. Per informazioni su errori e soluzioni specifici, consulta la sezione [Risoluzione degli errori](#).

- Utilizza la [console di CloudFormation](#) per visualizzare lo stato dei tuoi stack. Nella console, puoi visualizzare un elenco degli eventi di stack, mentre lo stack viene creato, aggiornato o eliminato. In questo elenco, trova l'evento relativo al problema e quindi visualizzane il motivo dello stato. Il motivo dello stato potrebbe contenere un messaggio di errore da CloudFormation o proveniente da un particolare servizio che può aiutarti a risolvere il problema. Per ulteriori informazioni sulla visualizzazione degli eventi dello stack, consulta [Visualizza gli CloudFormation eventi dello stack](#).
- Per EC2 problemi relativi ad Amazon, visualizza i log `cloud-init` e `cfn`. Questi log vengono pubblicati sull' EC2 istanza Amazon nella `/var/log/` directory. Questi log acquisiscono i processi e gli output dei comandi durante la CloudFormation configurazione dell'istanza. Per Windows, visualizza il servizio EC2 Configure in `%ProgramFiles%\Amazon\EC2ConfigService`, EC2 Launch in `%ProgramData%\Amazon\EC2-Windows\Launch\Logs`, EC2 Launch v2 in `%ProgramData%\Amazon\EC2Launch\log cfn` accedi. `C:\cfn\log`

Puoi anche configurare il CloudFormation modello in modo che i log vengano pubblicati su Amazon CloudWatch, che visualizza i log in AWS Management Console modo da non doverti connettere

alla tua istanza Amazon EC2 . Per ulteriori informazioni, consulta [Visualizza CloudFormation i log nella console nel blog sulla](#) gestione delle applicazioni.

Risoluzione degli errori

Quando riscontri i seguenti errori CloudFormation nello stack, puoi utilizzare le seguenti soluzioni per aiutarti a trovare l'origine dei problemi e risolverli.

Argomenti

- [Impossibile eliminare lo stack](#)
- [Errore di dipendenza](#)
- [AWS Config e conflitti AWS Systems Manager](#)
- [Errore del parametro di analisi durante il passaggio di un elenco](#)
- [Autorizzazioni IAM insufficienti](#)
- [Valore non valido o proprietà della risorsa non supportata](#)
- [Quota superata](#)
- [Stack nidificati bloccati in UPDATE_COMPLETE_CLEANUP_IN_PROGRESS, UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS o UPDATE_ROLLBACK_IN_PROGRESS](#)
- [Nessun aggiornamento da eseguire](#)
- [Impossibile stabilizzare una risorsa durante un'operazione di creazione, aggiornamento o eliminazione dello stack](#)
- [Gruppo di sicurezza non esistente in VPC](#)
- [Impossibile eseguire il rollback dell'aggiornamento](#)
- [La condizione di attesa non ha ricevuto il numero richiesto di segnali da un' EC2istanza Amazon](#)
- [Risorsa rimossa dallo stack ma non eliminata.](#)

Impossibile eliminare lo stack

Per risolvere questa situazione, prova quanto segue:

- Alcune risorse devono essere vuote prima di poter essere eliminate. Ad esempio, devi eliminare tutti gli oggetti in un bucket Amazon S3 o rimuovere tutte le istanze in un gruppo di EC2 sicurezza Amazon prima di poter eliminare il bucket o il gruppo di sicurezza.

- Verifica di disporre delle necessarie autorizzazioni IAM per eliminare le risorse nello stack. Oltre alle CloudFormation autorizzazioni, devi avere il permesso di utilizzare i servizi sottostanti, come Amazon S3 o Amazon EC2.
- Se lo stato degli stack è impostato perché CloudFormation non è DELETE_FAILED stato possibile eliminare una risorsa, esegui nuovamente [l'eliminazione](#) con il `RetainResources` parametro e specifica la risorsa che non può essere eliminata. CloudFormation elimina lo stack senza eliminare la risorsa conservata. La conservazione delle risorse è utile quando non puoi eliminare una risorsa, ad esempio un bucket S3 che contiene oggetti da conservare, ma vuoi comunque eliminare lo stack.

Dopo aver eliminato lo stack, è possibile eliminare manualmente le risorse conservate utilizzando il servizio associato. AWS

In alternativa, puoi prendere in considerazione l'utilizzo dell'`FORCE_DELETE_STACK` opzione con il `DeletionMode` parametro. Per ulteriori informazioni sull'eliminazione forzata di una pila, consulta [Eliminare uno stack dalla console CloudFormation](#).

- Non è possibile eliminare stack per cui è abilitata la protezione da cessazione. Se tenti di eliminare uno stack con protezione da cessazione abilitata, l'eliminazione ha esito negativo e lo stack, incluso lo stato, rimane invariato. Disabilita la protezione da cessazione sullo stack, quindi esegui nuovamente l'operazione di eliminazione.

Questo vale anche per gli [stack nidificati](#) i cui stack radice abbiano abilitata la protezione da cessazione. Disattiva la protezione da cessazione sullo stack radice, quindi esegui nuovamente l'operazione di eliminazione. È consigliabile non eliminare gli stack nidificati direttamente, ma solo nell'ambito dell'eliminazione dello stack radice e di tutte le relative risorse.

Per ulteriori informazioni, consulta [Proteggi CloudFormation gli stack dall'eliminazione](#).

- Per tutti gli altri problemi, se ne hai Supporto AWS, puoi creare un Supporto caso. Consultare [Contattare il supporto](#).

Errore di dipendenza

Per risolvere un errore di dipendenza, aggiungi un attributo `DependsOn` alle risorse che dipendono da altre risorse nel modello. In alcuni casi, è necessario dichiarare esplicitamente le dipendenze in modo da CloudFormation poter creare o eliminare risorse nell'ordine corretto. Ad esempio, se crei un IP elastico e un VPC con un gateway Internet nello stesso stack, l'IP elastico deve dipendere dal collegamento del gateway Internet. Per ulteriori informazioni, consulta [Attributo DependsOn](#).

AWS Config e conflitti AWS Systems Manager

AWS Config e AWS Systems Manager può automatizzare le attività di gestione dell'infrastruttura che possono causare conflitti con l'implementazione di uno CloudFormation stack. Effettuate le seguenti operazioni per evitare potenziali conflitti:

- Esaminare la configurazione di AWS Config e Systems Manager nel file associato Account AWS e Regione AWS.
- Verifica le regole attive o i documenti di automazione che potrebbero essere attivati durante una CloudFormation distribuzione. Questi possono potenzialmente causare conflitti o dipendenze tra le risorse che sono in conflitto con la distribuzione.
- Controlla il tuo CloudFormation modello per eventuali risorse gestite da AWS Config e Systems Manager. Verifica la presenza di potenziali sovrapposizioni o interdipendenze e valuta la possibilità di modificare il modello o la configurazione dell'automazione per evitare conflitti.
- Disattiva o sospendi temporaneamente AWS Config le regole correlate o le automazioni di Systems Manager durante la CloudFormation distribuzione. Ricordati di ripristinare le configurazioni originali dopo la corretta implementazione per mantenere il livello di automazione e conformità desiderato.
- CloudFormation Esamina i log e i messaggi di errore per eventuali riferimenti a AWS Config problemi relativi a Systems Manager per individuare l'origine del conflitto.

[Per ulteriori informazioni sulle AWS Config regole, vedere Evaluating Resources with. Regole di AWS Config](#)

Per ulteriori informazioni sulle automazioni di Systems Manager, vedere [AWS Systems Manager Automazione](#).

Errore del parametro di analisi durante il passaggio di un elenco

Quando usate AWS CLI o CloudFormation per passare in un elenco, aggiungete il carattere escape (\) prima di ogni virgola. L'esempio seguente mostra come specificare un parametro di input nella AWS CLI.

```
ParameterKey=CIDR,ParameterValue='10.10.0.0/16\,10.10.0.0/24\,10.10.1.0/24'
```

Autorizzazioni IAM insufficienti

Quando lavori con uno CloudFormation stack, non solo hai bisogno delle autorizzazioni per utilizzarlo CloudFormation, ma devi anche avere l'autorizzazione per utilizzare i servizi sottostanti descritti nel tuo modello. Ad esempio, se stai creando un bucket Amazon S3 o avviando un' EC2 istanza Amazon, hai bisogno delle autorizzazioni per Amazon S3 o Amazon. EC2 Esamina la policy IAM e verifica di disporre delle autorizzazioni necessarie per utilizzare gli stack CloudFormation . Per ulteriori informazioni, consultare [Controlla CloudFormation l'accesso con AWS Identity and Access Management](#).

Valore non valido o proprietà della risorsa non supportata

Quando crei o aggiorni uno CloudFormation stack, lo stack può fallire a causa di parametri di input non validi, nomi di proprietà delle risorse non supportati o valori di proprietà delle risorse non supportati. Per i parametri di input, verifica che la risorsa esista. Ad esempio, quando specifichi una coppia di EC2 chiavi Amazon o un ID VPC, la risorsa deve esistere nel tuo account e nella regione in cui stai creando o aggiornando lo stack. Puoi utilizzare [tipi di parametri AWS specifici](#) per assicurarti di utilizzare valori validi.

Per i nomi e i valori di proprietà delle risorse, aggiorna il modello per l'utilizzo di nomi e valori validi. Per ulteriori informazioni, consulta il [riferimento ai tipi di AWS risorse e proprietà](#).

Quota superata

Verifica di non aver raggiunto la quota per una risorsa. Ad esempio, il numero massimo predefinito di istanze Amazon EC2 On-Demand che puoi avviare è 5. Se provi a creare più istanze Amazon EC2 On-Demand rispetto alla quota del tuo account, la creazione dell'istanza non riesce e ricevi l'errore. Status=start_failed Per visualizzare le quote AWS predefinite per servizio, consulta [Quote di servizio di AWS](#) in Riferimenti generali di AWS.

Per le CloudFormation quote e le strategie di modifica, consulta. [Comprendi le CloudFormation quote](#)

Inoltre, durante un aggiornamento, se una risorsa viene sostituita, CloudFormation crea una nuova risorsa prima di eliminare quella precedente. Questa sostituzione potrebbe causare lo sconfinamento dell'account rispetto alle quote delle risorse, con conseguente errore nell'aggiornamento. Puoi eliminare le risorse in eccesso o richiedere un [aumento delle quote](#).

Stack nidificati bloccati in **UPDATE_COMPLETE_CLEANUP_IN_PROGRESS**, **UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS** o **UPDATE_ROLLBACK_IN_PROGRESS**

Uno stack nidificato non è stato in grado di eseguire il rollback. A causa delle potenziali dipendenze tra le risorse degli stack nidificati, CloudFormation non inizia a ripulire le risorse degli stack nidificati finché tutti gli stack nidificati non sono stati aggiornati o non sono stati ripristinati. Quando uno stack nidificato non riesce a eseguire il rollback, CloudFormation annulla tutte le operazioni, indipendentemente dallo stato in cui si trovano gli altri stack nidificati. Uno stack nidificato che ha completato l'aggiornamento o il rollback ma non ha ricevuto alcun segnale di avvio della pulizia perché un altro nidificato non è riuscito a ripristinarlo si trova in uno stato or. CloudFormation **UPDATE_COMPLETE_CLEANUP_IN_PROGRESS** **UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS** Uno stack nidificato che non ha potuto completare l'aggiornamento, ma che non ha ricevuto un segnale per avviare il rollback, si trova in uno stato **UPDATE_ROLLBACK_IN_PROGRESS**.

Il rollback di uno stack nidificato potrebbe non riuscire a causa di modifiche apportate all'esterno di CloudFormation, quando il modello dello stack non riflette accuratamente lo stato dello stack. Uno stack nidificato può non riuscire anche se un gruppo con dimensionamento automatico in uno stack nidificato aveva un periodo di timeout del segnale per le risorse insufficiente quando il gruppo è stato creato o aggiornato.

Per risolvere il problema con lo stack, contatta [Supporto AWS](#).

Nessun aggiornamento da eseguire

Per aggiornare uno CloudFormation stack, è necessario inviare le modifiche ai valori del modello o del parametro a. CloudFormation Tuttavia, CloudFormation non riconoscerà alcune modifiche al modello come aggiornamento, ad esempio le modifiche a una politica di eliminazione, una politica di aggiornamento, una dichiarazione di condizione o una dichiarazione di output. Se devi effettuare tali modifiche senza toccare altro, puoi aggiungere o modificare un attributo di metadati per qualsiasi risorsa. L'attributo metadata può essere qualsiasi valore arbitrario, in quanto CloudFormation non ne interpreta il contenuto. Per ulteriori informazioni, consulta [Attributo Metadata](#).

Impossibile stabilizzare una risorsa durante un'operazione di creazione, aggiornamento o eliminazione dello stack

Una risorsa non ha risposto perché l'operazione ha superato il periodo di CloudFormation timeout o un AWS servizio è stato interrotto. In caso di interruzioni del servizio, [verifica](#) che il AWS servizio in questione sia in esecuzione, quindi riprova a eseguire l'operazione stack.

Se i AWS servizi sono stati eseguiti correttamente, controlla se lo stack contiene una delle seguenti risorse:

- `AWS::AutoScaling::AutoScalingGroup` per operazioni di creazione, aggiornamento ed eliminazione
- `AWS::CertificateManager::Certificate` per operazioni di creazione
- `AWS::CloudFormation::Stack` per operazioni di creazione, aggiornamento ed eliminazione
- `AWS::ElasticSearch::Domain` per operazioni di aggiornamento
- `AWS::RDS::DBCluster` per operazioni di creazione e aggiornamento
- `AWS::RDS::DBInstance` per operazioni di creazione, aggiornamento ed eliminazione
- `AWS::Redshift::Cluster` per operazioni di aggiornamento

Le operazioni per queste risorse potrebbero richiedere più tempo del periodo di timeout predefinito. Il periodo di timeout dipende dalla risorsa e dalle credenziali utilizzate. Per estendere il periodo di timeout, specifica un [ruolo di servizio](#) quando esegui l'operazione sullo stack. Se utilizzi già un ruolo di servizio, oppure se il tuo stack contiene una risorsa non in elenco, contatta [Supporto AWS](#).

Se il tuo stack è nello stato `UPDATE_ROLLBACK_FAILED`, consulta [Impossibile eseguire il rollback dell'aggiornamento](#).

Gruppo di sicurezza non esistente in VPC

Verifica che il gruppo di sicurezza esista nel VPC specificato. Se il gruppo di sicurezza esiste, assicurati di specificarne l'ID e non il nome. Ad esempio, la risorsa `AWS::EC2::SecurityGroupIngress` ha le proprietà `SourceSecurityGroupName` e `SourceSecurityGroupId`. Per i gruppi di sicurezza VPC, devi utilizzare la proprietà `SourceSecurityGroupId` e specificare l'ID del gruppo di sicurezza.

Impossibile eseguire il rollback dell'aggiornamento

Una risorsa dipendente non può tornare al suo stato originale, provocando il mancato completamento del rollback (stato `UPDATE_ROLLBACK_FAILED`). Ad esempio, è possibile che uno stack stia eseguendo il rollback a una vecchia istanza database che è stata eliminata al di fuori di CloudFormation. Poiché CloudFormation non sa che il database è stato eliminato, presume che l'istanza del database esista ancora e tenta di ripristinarla, causando il fallimento del rollback dell'aggiornamento.

A seconda del problema, è possibile correggere manualmente gli errori e continuare il rollback. Per continuare il rollback, puoi riportare lo stack allo stato di funzionamento `UPDATE_ROLLBACK_COMPLETE` e quindi provare nuovamente ad aggiornare lo stack. L'elenco seguente descrive le soluzioni a problemi comuni che provocano errori nel rollback dell'aggiornamento:

- Impossibile ricevere il numero richiesto di segnali

Utilizza il comando [signal-resource](#) per inviare manualmente il numero richiesto di segnali di riuscita alla risorsa in attesa, quindi continua con il rollback dell'aggiornamento. Ad esempio, durante il rollback di un aggiornamento, le istanze in un gruppo con dimensionamento automatico potrebbe non riuscire a segnalare la riuscita entro il timeout specificato. Invia manualmente i segnali di successo al gruppo con dimensionamento automatico. Quando continui il rollback dell'aggiornamento, CloudFormation vede i tuoi segnali e procede con il rollback.

- Le modifiche a una risorsa sono state apportate al di fuori di CloudFormation

Sincronizza manualmente le risorse in modo che corrispondano al modello originale dello stack, quindi continua con il rollback dell'aggiornamento. Ad esempio, se hai eliminato manualmente una risorsa a cui CloudFormation stai tentando di eseguire il rollback, devi creare manualmente quella risorsa con lo stesso nome e le stesse proprietà che aveva nello stack originale.

- Autorizzazioni insufficienti

Verifica di disporre delle autorizzazioni IAM sufficienti per modificare le risorse, quindi continua con il rollback dell'aggiornamento. Ad esempio, la tua policy IAM potrebbe consentirti di creare un bucket S3, ma non di modificarlo. Aggiungi le operazioni di modifica alla tua policy.

- Token di sicurezza non valido

CloudFormation richiede un nuovo set di credenziali. Non sono richieste modifiche. Continua con il rollback dell'aggiornamento per aggiornare le credenziali.

- Errore relativo ai limiti

Elimina le risorse che non ti servono o richiedi un [aumento delle quote](#), quindi continua con il rollback dell'aggiornamento. Ad esempio, se la quota del tuo account per il numero di istanze EC2 On-Demand è 5 e il rollback dell'aggiornamento supera tale quota, l'operazione avrà esito negativo.

- La risorsa non si è stabilizzata

Una risorsa non ha risposto perché l'operazione potrebbe aver superato il periodo di CloudFormation timeout o un AWS servizio potrebbe essere stato interrotto. Non sono richieste modifiche. Una volta completato il funzionamento delle risorse o dopo che il AWS servizio è tornato operativo, continua a ripristinare l'aggiornamento.

Per continuare a ripristinare un aggiornamento, puoi utilizzare la CloudFormation console o l'interfaccia a riga di AWS comando (AWS CLI). Per ulteriori informazioni, consulta [Rollback di un aggiornamento](#).

Se nessuna di queste soluzioni funziona, puoi saltare le risorse che non CloudFormation possono essere ripristinate correttamente. Per ulteriori informazioni, consulta il `ResourcesToSkip` parametro per il funzionamento dell'[ContinueUpdateRollbackAPI](#) nell'AWS CloudFormation API Reference. CloudFormation imposta lo stato delle risorse specificate su `UPDATE_COMPLETE` e continua a ripristinare lo stack. Dopo aver completato il rollback, lo stato delle risorse saltate saranno incoerenti con lo stato delle risorse nel modello di stack. Prima di eseguire un altro aggiornamento dello stack, devi modificare le risorse o aggiornare lo stack in modo che siano coerenti. Altrimenti, i successivi aggiornamenti dello stack potrebbero fallire e rendere lo stack irrecuperabile.

La condizione di attesa non ha ricevuto il numero richiesto di segnali da un' EC2istanza Amazon

Per risolvere questa situazione, prova quanto segue:

- Assicurati che l'AMI che stai utilizzando abbia gli script di CloudFormation supporto installati. Se l'AMI non include gli script helper, puoi anche scaricarli sulla tua istanza. Per ulteriori informazioni,

consultate il riferimento agli [script di CloudFormation supporto nella Template Reference](#) Guide.AWS CloudFormation

- Verifica che il comando `cfn-signal` sia stato eseguito sull'istanza. Per aiutarti con il debug dell'avvio dell'istanza, puoi avvalerti dei log, ad esempio `/var/log/cloud-init.log` o `/var/log/cfn-init.log`. Puoi recuperare i log accedendo alla tua istanza, ma devi [disabilitare il rollback in caso di errore](#) oppure CloudFormation elimina l'istanza dopo che lo stack non è riuscito a creare. Puoi anche [pubblicare i log](#) su Amazon CloudWatch. Per Windows, è possibile visualizzare i log in `cfn` e i log in del `C:\cfn\log` servizio EC2 Config. `%ProgramFiles%\Amazon\EC2ConfigService`
- Verifica che l'istanza disponga di una connessione a Internet. Se è in un VPC, l'istanza deve essere in grado di connettersi a Internet attraverso un dispositivo NAT, se si trova in una sottorete privata, o attraverso un gateway Internet, se è in una sottorete pubblica. Per testare la connessione a Internet dell'istanza, cerca di accedere a una pagina Web pubblica, ad esempio `http://aws.amazon.com`. Ad esempio, puoi eseguire il comando seguente sull'istanza. Dovrebbe restituire un codice di stato HTTP 200.

```
curl -I https://aws.amazon.com
```

Per ulteriori informazioni sulla configurazione di un dispositivo NAT, consulta [NAT](#) nella Guida per l'utente di Amazon VPC.

Risorsa rimossa dallo stack ma non eliminata.

Durante un aggiornamento dello stack, CloudFormation ha rimosso una risorsa da uno stack ma non ha eliminato la risorsa. La risorsa esiste ancora, ma non è più accessibile tramite CloudFormation. Ciò può verificarsi durante gli aggiornamenti dello stack in cui:

- CloudFormation deve sostituire una risorsa esistente, quindi crea prima una nuova risorsa, quindi tenta di eliminare la vecchia risorsa.
- La risorsa è stata rimossa dal modello di stack, quindi CloudFormation tenta di eliminarla dallo stack.

Tuttavia, potrebbero esserci casi in cui non è CloudFormation possibile eliminare la risorsa. Ad esempio, se l'utente non dispone delle autorizzazioni per eliminare una risorsa di un determinato tipo.

CloudFormation tenta di eliminare la vecchia risorsa tre volte. Se non CloudFormation riesce a eliminare la vecchia risorsa, rimuove la vecchia risorsa dallo stack e continua ad aggiornare lo stack. Quando l'aggiornamento dello stack è completo, CloudFormation genera un evento `UPDATE_COMPLETE` stack, ma include un evento `StatusReason` che indica che una o più risorse non possono essere eliminate. CloudFormation emette anche un `DELETE_FAILED` evento per la risorsa specifica, con un corrispondente che `StatusReason` fornisce maggiori dettagli sul motivo per cui CloudFormation non è riuscita a eliminare la risorsa.

Per risolvere questo problema, eliminare la risorsa direttamente utilizzando la console o l'API per il servizio sottostante.

Contattare il supporto

In caso Supporto AWS affermativo, è possibile creare una richiesta di supporto tecnico a <https://console.aws.amazon.com/support/casa#/>. Prima di contattare il supporto, raccogli queste informazioni:

- L'ID dello stack. Puoi trovare l'ID dello stack nella scheda Overview (Panoramica) della [console CloudFormation](#). Per ulteriori informazioni, consulta [Visualizza le informazioni sullo stack dalla console CloudFormation](#).

Important

Non apportare modifiche allo stack al di fuori di CloudFormation. Apportare modifiche allo stack all'esterno CloudFormation potrebbe mettere lo stack in uno stato irrecuperabile.

- Eventuali messaggi di errore dello stack. Per informazioni sulla visualizzazione dei messaggi di errore dello stack, consulta la sezione [Guida alla risoluzione dei problemi](#).
- Per EC2 problemi con Amazon, raccogli i log `cloud-init` e `cfn`. Questi log vengono pubblicati sull' EC2 istanza Amazon nella `/var/log/` directory. Questi log acquisiscono gli output di processi e comandi mentre l'istanza viene configurata. Per Windows, raccogli il servizio EC2 Configure e `cfn` accedi e. `%ProgramFiles%\Amazon\EC2ConfigService C:\cfn\log`

Puoi anche cercare risposte e pubblicare domande nella [CloudFormation community](#) su AWS re:Post

Risolvi i problemi di CloudFormation distribuzioni di stack non riuscite con Amazon Q Developer

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale (AI) che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Per informazioni su Amazon Q Developer, consulta la [Amazon Q Developer User Guide](#).

Questo documento descrive come utilizzare Amazon Q Developer per aiutarti a risolvere le distribuzioni non CloudFormation riuscite. Questa funzionalità è progettata per aiutarti a identificare e risolvere rapidamente i problemi riscontrati durante l'implementazione dello stack.

Basato su Amazon Bedrock: Amazon Q è basato su Amazon Bedrock e include il [rilevamento automatico degli abusi](#) implementato in Amazon Bedrock per rafforzare la sicurezza e l'uso responsabile dell'intelligenza artificiale.

Argomenti

- [Funzionalità](#)
- [Come funziona](#)
- [Prezzi](#)
- [Disponibilità regionale](#)
- [Limitazioni](#)

Funzionalità

La risoluzione dei problemi delle distribuzioni dello stack con la soluzione Amazon Q Developer offre le seguenti funzionalità:

- Analisi degli errori: fornisce l'analisi degli errori di easy-to-understand distribuzione degli CloudFormation stack.
- Suggerimenti per la risoluzione: offre step-by-step istruzioni per risolvere i problemi identificati.

Come funziona

Quando la creazione o l'aggiornamento di uno CloudFormation stack non riesce, viene visualizzato un messaggio di errore in AWS Management Console

È possibile scegliere il pulsante Diagnostica con Q accanto al messaggio di errore.

Amazon Q Developer analizza l'errore e fornisce una spiegazione del problema.

Per ulteriore assistenza, scegli Aiutami a risolvere per ricevere i passaggi di risoluzione dettagliati.

Prezzi

Per informazioni sui prezzi, consulta i [prezzi di Amazon Q Developer](#).

Disponibilità regionale

Amazon Q Developer è disponibile nella maggior parte dei casi Regioni AWS. Per un elenco di tutte le regioni in cui Amazon Q Developer è attualmente disponibile, consulta la sezione [Regioni supportate per Amazon Q Developer](#) nella Amazon Q Developer User Guide.

Limitazioni

- Questa funzionalità è accessibile solo tramite AWS Management Console.
- Questa funzionalità copre i 20 errori più comuni. Non copre tutti i possibili errori.
- Casi complessi di risoluzione dei problemi potrebbero comunque richiedere Supporto un intervento.

Cronologia dei documenti per la Guida per AWS CloudFormation l'utente

La tabella seguente descrive le modifiche importanti al contenuto della Guida per l'utente dopo maggio 2018. AWS CloudFormation Per ricevere notifiche sugli aggiornamenti della documentazione, puoi iscriverti a un feed RSS.

Important

Le righe della tabella che descrivono gli aggiornamenti al contenuto di riferimento del modello a partire da maggio 2018 sono state spostate nel nuovo AWS CloudFormation Template Reference. Per questi aggiornamenti e per eventuali modifiche future, consulta la [cronologia del documento per il riferimento al AWS CloudFormation modello](#) nel riferimento al AWS CloudFormation modello.

Modifica	Descrizione	Data
Guida in PDF disponibile	Ora puoi scaricare la Guida AWS CloudFormation per l'utente in formato PDF.	30 maggio 2025
Il contenuto di riferimento del modello è stato spostato in una nuova guida	CloudFormation ha pubblicato la AWS CloudFormation Template Reference Guide. Per i dettagli, consulta The AWS CloudFormation Template Reference Guide .	30 maggio 2025
Il generatore IAc supporta la scansione parziale	È ora possibile scegliere tipi di risorse specifici da ricercare , semplificando la generazione di modelli Infrastructure-as-Code (IaC) a partire dalle risorse esistenti. Per ulteriori informazioni, consulta Avviare	27 marzo 2025

[una scansione delle risorse con il generatore CloudFormation IAc.](#)

[Rifattorizzazione degli stack](#)

Il refactoring dello stack semplifica la riorganizzazione delle risorse negli CloudFormation stack preservando al contempo le proprietà e i dati delle risorse esistenti. [Per ulteriori informazioni, consulta Stack refactoring.](#)

6 febbraio 2025

[Risolvi i problemi di distribuzione degli stack con Amazon Q Developer](#)

Ora puoi usare Amazon Q Developer per risolvere gli errori più comuni durante la distribuzione CloudFormation degli stack. Per ulteriori informazioni, consulta [Risolvere i problemi relativi alle CloudFormation distribuzioni di stack non riuscite con Amazon Q Developer.](#)

22 novembre 2024

[Grafico della cronologia di implementazione dello stack](#)

Ora puoi vedere una rappresentazione visiva della distribuzione dello stack. Il grafico della sequenza temporale di distribuzione dello stack mostra lo stato di distribuzione dello stack, gli stati di distribuzione delle singole risorse e le volte in cui gli stati di distribuzione sono cambiati. Per ulteriori informazioni, consulta [Visualizzare la cronologia di una distribuzione in stack](#). CloudFormation

11 novembre 2024

[Visualizza le risorse scansionate e i modelli generati](#)

Ora puoi semplificare i flussi di lavoro del generatore di Infrastructure as Code (IaC) visualizzando i dettagli di riepilogo delle scansioni e visualizzando in anteprima i modelli generati prima di implementare lo stack di infrastruttura. [Per ulteriori informazioni, consulta Visualizzare il riepilogo della scansione nella CloudFormation console e Creare uno stack dalle risorse scansionate](#). CloudFormation

22 agosto 2024

[EventBridge Integrazione Amazon con AWS CloudFormation Git sync](#)

AWS CloudFormation Git sync ora pubblica le modifiche allo stato di sincronizzazione come eventi su Amazon EventBridge. Per ulteriori informazioni, consulta i dettagli dell'evento [Repository Sync Status Change](#) e i dettagli dell'evento [Resource Sync Status Change](#).

29 luglio 2024

[Eliminazione forzata delle pile bloccate](#)

Sono disponibili due nuove opzioni per forzare l'eliminazione delle pile per le operazioni di eliminazione delle pile bloccate. Ora puoi scegliere di forzare l'eliminazione dello stack ma mantenere la risorsa oppure l'eliminazione forzata dell'intero stack. Per ulteriori informazioni, consulta [Eliminare uno stack dalla console](#).
CloudFormation

22 maggio 2024

[AWS CloudTrail cause principali dell'operazione Event Stack](#)

CloudFormation migliora l'esperienza di risoluzione dei problemi per le operazioni di stack con una nuova integrazione con collegamento diretto AWS CloudTrail. Questa funzionalità collega direttamente gli eventi operativi dello stack nella CloudFormation console agli eventi pertinenti. CloudTrail Per ulteriori informazioni, consulta [Determinare la causa di un errore dello stack](#).

15 maggio 2024

[Set di modifiche a livello di proprietà](#)

I set di modifiche a livello di proprietà consentono di visualizzare in anteprima le modifiche che CloudFormation le distribuzioni apporteranno ai valori delle proprietà delle risorse. Per ulteriori informazioni, consulta [Visualizzare un set di modifiche per uno CloudFormation stack](#).

12 aprile 2024

[CloudFormation introduce l'evento CONFIGURATION_COMPLETE](#)

Ora puoi utilizzare l'CONFIGURATION_COMPLETE evento per abilitare flussi di lavoro più rapidi che prevedono la creazione di risorse. Per ulteriori informazioni, consulta [Comprendere gli eventi di creazione CloudFormation dello stack](#).

11 marzo 2024

[Genera AWS CloudFormation modelli e AWS CDK applicazioni da risorse esistenti AWS](#)

Ora puoi generare un modello utilizzando le risorse fornite nel tuo account che non sono già gestite da CloudFormation. Per ulteriori informazioni, consulta [Generare modelli da risorse esistenti con il generatore IaC](#).

2 febbraio 2024

[StackSets modalità di concorrenza](#)

La modalità di concorrenza è un parametro StackSetOperationPreference che consente di scegliere il comportamento del livello di concorrenza durante le operazioni di stack set. Per ulteriori informazioni, consulta [Scelta della](#) modalità di concorrenza per. CloudFormation StackSets

9 novembre 2023

[Informazioni dettagliate sulla
StackSet deriva](#)

Di seguito è APIs possibile vedere quali istanze dello stack si sono allontanate dal StackSet modello e quali risorse lo sono state.

24 luglio 2023

[ListStackInstanceResourceDrifts](#)

Restituisce informazioni sulla deviazione per le risorse in un'istanza stack.

[StackInstanceResourceDrifts
Summary](#)

La struttura contenente le informazioni di riepilogo sulle deviazioni delle risorse per un'istanza stack.

[CloudFormation StackSets](#)
[APIs AWS Organizations per](#)
[controllare l'accesso affidabile](#)

CloudFormation StackSets
offre ai clienti quanto segue
APIs per la gestione degli
accessi AWS Organizations
fiduciari:

5 giugno 2023

[ActivateOrganizationsAccess](#)

Attiva l'accesso affidabile
con AWS Organizations.
Con l'accesso affidabile
tra StackSets e Organizat
ions attivato, l'account di
gestione dispone delle
autorizzazioni per creare e
gestire StackSets per la tua
organizzazione.

[DeactivateOrganizationsAcce](#)
[ss](#)

Disattiva l'accesso affidabil
e con. AWS Organizations
Se l'accesso affidabile è
disattivato, l'account di
gestione non dispone delle
autorizzazioni per creare
e gestire servizi StackSets
gestiti per l'organizzazione.

[DescribeOrganizationsAccess](#)

Recupera le informazioni
sullo stato dell'account
OrganizationAccess
. Questa API può essere
richiamata dall'account
di gestione o dall'ammi
nistratore delegato utilizzan

do il parametro `CallAs`.
Questa API può essere
chiamata anche senza
il parametro `CallAs`
dall'account di gestione.

[API DescribeStackSet](#)

L'`DescribeStackSet` API
ha un nuovo parametro
nell'elenco delle regioni
in cui viene distribuito un
determinato set di stack. Per
ulteriori informazioni, consulta
[DescribeStackSet](#).

1 febbraio 2023

[Gestione StackSets degli eventi con CloudFormation e Amazon EventBridge](#)

CloudFormation StackSets
notifiche di eventi di lancio
tramite Amazon EventBridge.
Puoi attivare azioni basate
sugli eventi dopo aver creato,
aggiornato o eliminato i
tuoi CloudFormation set di
stack. Per ulteriori informazi
oni, consulta [Monitoraggio
CloudFormation e sincroniz
zazione degli eventi di Git con
EventBridge](#).

16 novembre 2022

[Informazioni migliorate sulle istanze stack per le operazioni relative ai set di stack](#)

CloudFormation StackSets fornisce informazioni più dettagliate sulle istanze dello stack per le operazioni relative ai set di stack:

4 novembre 2022

[DescribeStackSetOperation](#)

È ora possibile utilizzare `DescribeStackSetOperation` per fornire il conteggio delle istanze di stack non riuscite per le operazioni del set di stack durante l'implementazione.

[ListStackInstances](#)

È ora possibile utilizzare e l'opzione di filtro `LastOperationID` per elencare le istanze dello stack per le operazioni del set di stack.

[Gestione degli eventi con CloudFormation e Amazon EventBridge](#)

Ricevi notifiche quando si verificano CloudFormation eventi specifici. Per ulteriori informazioni, consulta [Monitoraggio CloudFormation e sincronizzazione degli eventi di Git con EventBridge](#).

20 luglio 2022

Livello di account

CloudFormation annuncia la disponibilità generale del tipo di filtro dell'account, una funzionalità che consente ai clienti di limitare gli obiettivi di implementazione ai singoli account o di includere account aggiuntivi se fornito OUs. Per ulteriori informazioni, consulta [Obiettivi a livello di account per la gestione dei servizi StackSets](#).

7 luglio 2022

CloudFormation registro

CloudFormation annuncia la disponibilità generale di Hooks, una funzionalità che consente ai clienti di richiamare e una logica personalizzata per automatizzare le azioni o ispezionare le configurazioni delle risorse prima di un'operazione di creazione, aggiornamento o eliminazione dello stack. [Per ulteriori informazioni, consulta la Guida per l'utente di Hooks.AWS CloudFormation](#)

10 febbraio 2022

[Opzioni di errore degli stack](#)

Puoi sviluppare in modo iterativo le applicazioni quando si verificano errori di provisioning iniziando dal punto di errore senza eseguire il rollback delle risorse con provisioning effettuato correttamente. Specificando le opzioni di errore degli stack, puoi risolvere i problemi delle risorse con stato `CREATE_FAILED` o `UPDATE_FAILED`. Puoi effettuare il provisioning di opzioni di errore per tutte le implementazioni di stack e le operazioni di set di modifica. Per ulteriori informazioni, consulta [Scegliere come gestire gli errori durante il provisioning](#) delle risorse.

30 agosto 2021

[Importazione di stack nel set di stack](#)

Ora puoi importare gli stack esistenti in set di stack nuovi o esistenti. Per ulteriori informazioni, consulta [Importazione di pile in CloudFormation StackSets](#)

28 luglio 2021

[Aumento della quota](#)

Ora puoi dichiarare un numero massimo predefinito di pile nel tuo Account AWS. Per ulteriori informazioni, consulta [Comprendere le quote CloudFormation](#)

15 luglio 2021

[Pubblicazione di estensioni
pubbliche di terze parti](#)

Ora puoi utilizzare le estensioni
i pubbliche fornite da editori
di terze parti, proprio come
faresti con le estensioni. AWS
Per ulteriori informazioni,
consulta [Utilizzare estension
i pubbliche di terze parti dal
CloudFormation registro.](#)

21 giugno 2021

[Riferimento alle macro nei
modelli di set di stack](#)

StackSets ora supporta la
creazione o l'aggiornamento di
set di stack con autorizzazioni
autogestite da modelli che
fanno riferimento alle macro.
Per ulteriori informazioni sulle
macro, consulta [Eseguire
l'elaborazione personalizzata
sui CloudFormation](#) modelli
con le macro dei modelli.

14 aprile 2021

[Usa il valore più recente di un
parametro Systems Manager
in un riferimento dinamico](#)

È ora possibile CloudForm
ation utilizzare la versione
più recente di un parametro
Systems Manager ogni volta
che si crea o si aggiorna uno
stack. Non è più necessari
o specificare una versione
specifica. Per ulteriori dettagli,
vedere [Ottenere un valore in
chiaro da Systems Manager
Parameter Store.](#)

13 aprile 2021

[I moduli supportano l'utilizzo di delimitatori di periodo nei nomi delle risorse](#)

È ora possibile utilizzare un punto come delimitatore per specificare il nome logico completo per una risorsa contenuta in un modulo. Per ulteriori informazioni, vedete [Risorse del modulo di riferimento nei CloudFormation modelli](#).

8 aprile 2021

[CloudFormation StackSets ora supporta l'implementazione in regioni parallele](#)

Ora puoi scegliere di eseguire la distribuzione nelle Regioni StackSets in modo sequenziale o in parallelo. Per ulteriori informazioni, vedere [Opzioni per le operazioni dei set di stack](#).

6 aprile 2021

[CloudFormation StackSets ora supporta l'amministratore delegato con AWS Organizations](#)

Oltre al account di gestione dell'organizzazione, gli account amministratore delegati possono creare e gestire set di stack con autorizzazioni gestite dai servizi per la propria organizzazione. Per ulteriori informazioni, consulta [Registrare un account membro amministratore delegato](#) e [Creare CloudFormation StackSets con autorizzazioni gestite dal servizio](#).

18 febbraio 2021

[CloudFormation StackSets](#) [Disponibilità nelle Regioni](#)

CloudFormation StackSets è ora disponibile nella regione Asia Pacifico (Osaka). Per ulteriori informazioni, consulta [Gestire gli stack tra account e regioni](#) con. StackSets

10 febbraio 2021

[Modules](#)

I moduli sono un modo per creare pacchetti di configurazioni delle risorse per l'inclusione su modelli di stack, in modo trasparente, gestibile e ripetibile. I moduli possono incapsulare configurazioni di servizio comuni e best practice come blocchi predefiniti modulari e personalizzabili da includere nei modelli di stack. Per ulteriori informazioni, consulta [Creare configurazioni di risorse riutilizzabili che possono essere incluse nei modelli](#) con moduli. CloudFormation

24 novembre 2020

[Set di modifiche per stack nidificati](#)

18 novembre 2020

Con i set di modifiche per gli stack nidificati è possibile visualizzare in anteprima le modifiche alle risorse dell'applicazione e dell'infrastruttura nell'intera gerarchia dello stack nidificato e procedere con gli aggiornamenti dopo aver confermato che tutte le modifiche sono come previsto. Per ulteriori informazioni, vedere [Set di modifiche per stack nidificati](#).

Aumento delle quote

Le seguenti AWS CloudFormation quote sono state aggiornate.

22 ottobre 2020

- È ora possibile dichiarare un massimo di 200 mapping nel modello AWS CloudFormation .
- Ora puoi dichiarare un massimo di attributi di 200 mappatura per ogni mappatura nel tuo modello. AWS CloudFormation
- Ora puoi dichiarare un massimo di 200 output nel tuo modello AWS CloudFormation .
- È ora possibile dichiarare un massimo di 200 parametri nel modello AWS CloudFormation .
- È ora possibile dichiarare un massimo di 500 risorse nel modello AWS CloudFormation .
- È ora possibile passare un corpo del modello con una dimensione massima di 1 MB in un oggetto Amazon S3.

[Rilevamento della deviazione delle risorse private](#)

CloudFormation ora supporta le operazioni di rilevamento della deriva su un elenco esteso di AWS risorse, nonché su risorse private definite come disponibili nel registro. CloudFormation Per ulteriori informazioni, consulta [Resource](#) type support.

1 ottobre 2020

[Autorizzazioni aggiornate necessarie per la registrazione dei provider di risorse](#)

La registrazione di un provider di risorse nell'account richiede ora di disporre dell'autorizzazione per accedere al pacchetto del gestore dello schema caricato in un bucket S3 per tale provider di risorse. Per ulteriori informazioni, consulta [Autorizzazioni IAM per la registrazione di un'estensione privata di terze parti](#).

7 agosto 2020

[L'importazione di risorse supporta i tipi di risorse private con provisioning](#)

Le operazioni di importazione ora supportano i tipi di risorse private di cui è possibile eseguire il provisioning, ovvero il cui tipo di provisioning è FULLY_MUTABLE o IMMUTABLE . Per ulteriori informazioni, vedere [Risorse che supportano le operazioni di importazione](#).

3 giugno 2020

[Implementazioni ECS tramite blue/green CodeDeploy](#)

Ora puoi utilizzarlo CloudFormation per eseguire distribuzioni ECS blue/green tramite CodeDeploy Blue/green. Le implementazioni sono una strategia di implementazione sicura fornita AWS CodeDeploy per ridurre al minimo le interruzioni causate dalla modifica delle versioni delle applicazioni. Per ulteriori informazioni, vedere [Esecuzione delle distribuzioni ECS tramite utilizzo blue/green](#). CodeDeploy CloudFormation

19 maggio 2020

[CloudFormation StackSets Disponibilità nelle Regioni](#)

CloudFormation StackSets è ora disponibile nella regione AWS GovCloud (Stati Uniti occidentali).

18 maggio 2020

[AWS CloudFormation
StackSets si integra con AWS
Organizations](#)

Ora puoi utilizzarlo StackSets per gestire centralmente le distribuzioni di tutti gli account della tua organizzazione o di unità organizzative specifiche () OUs in. AWS Organizations Puoi abilitare le distribuzioni automatiche a tutti i nuovi account aggiunti alla tua organizzazione o. OUs Le autorizzazioni necessarie per la distribuzione su più account verranno gestite automaticamente da. StackSets Per ulteriori informazioni, consulta [Gestire gli stack tra account e regioni](#) con. StackSets

11 febbraio 2020

[Drift Detection per StackSets](#)

È ora possibile eseguire il rilevamento della deviazione su un set di stack e su tutte le istanze dello stack da esso incluse. Per ulteriori informazioni, vedere [Esecuzione del rilevamento della deriva](#) su. CloudFormation StackSets

19 novembre 2019

[CloudFormation registro ora
disponibile](#)

Ora puoi usare la CloudFormation console per visualizzare le risorse private e pubbliche disponibili per l'uso nel tuo account. Per ulteriori informazioni, consulta [Visualizzare le estensioni disponibili e attivate nel CloudFormation registro.](#)

18 novembre 2019

[CloudFormation azioni dell'API del registro](#)

18 novembre 2019

Le seguenti azioni API per la gestione dei tipi nel CloudFormation registro sono ora disponibili.

[DeregisterType](#)

Rimuove un tipo o una versione del tipo dall'uso attivo nel CloudFormation registro.

[DescribeType](#)

Restituisce informazioni dettagliate su un tipo registrato.

[DescribeTypeRegistration](#)

Restituisce informazioni sulla registrazione di un tipo, inclusi lo stato corrente e gli identificatori di tipo e versione.

[ListTypeRegistrations](#)

Restituisce un elenco di identificatori di richiesta di registrazione per il tipo specificato.

[ListTypes](#)

Restituisce informazioni di riepilogo sui tipi con cui sono stati registrati CloudFormation.

[ListTypeVersions](#)

Restituisce informazioni di riepilogo sulle versioni di un tipo.

[RegisterType](#)

Registra un tipo nel CloudFormation registro. La registrazione di un tipo lo rende disponibile per l'uso nei CloudFormation modelli di Account AWS

[SetTypeDefaultVersion](#)

Specificare la versione predefinita di un tipo. La versione predefinita di un tipo verrà utilizzata nelle CloudFormation operazioni.

Per ulteriori informazioni sul CloudFormation registro, vedere [Gestione delle estensioni con il CloudFormation registro](#)

[Importazione della risorsa aggiunta](#)

Se hai creato una AWS risorsa esterna alla CloudFormation gestione, puoi portare questa risorsa esistente in CloudFormation gestione utilizzando `doresource import`. Per ulteriori informazioni, consulta [Importare AWS risorse in una CloudFormation pila con un'importazione di risorse](#).

11 novembre 2019

[Incrementi del limite del set di stack](#)

Ora puoi creare un massimo di 100 set di stack nell'account amministratore, creare un massimo di 2000 istanze di stack per set di stack ed eseguire un massimo di 3500 operazioni di istanze di stack in ogni Regione contemporaneamente, per account amministratore. Per ulteriori informazioni, consulta [Comprendere le CloudFormation quote](#).

2 agosto 2019

[Limite per risorse in operazioni simultanee di stack](#)

CloudFormation ora impone un limite di account per il numero di risorse nelle operazioni di stack simultanee. Questo limite è determinato dalla Regione. [Per ulteriori informazioni, vedere Understand Quotas. CloudFormation](#)

30 aprile 2019

[Limite delle operazioni di istanze di stack](#)

Infatti StackSets, ora puoi avere un massimo di 1500 operazioni di istanze stack in esecuzione contemporaneamente in una determinata regione, per account amministratore. Per ulteriori informazioni, consulta [CloudFormation Understand Quotas](#).

13 dicembre 2018

[La CAPABILITY_AUTO_EXPAND funzionalità è ora disponibile](#)

È ora possibile utilizzare la CAPABILITY_AUTO_EXPAND funzionalità per creare o aggiornare uno stack direttamente da un modello di stack che contiene macro, senza prima esaminare le modifiche risultanti in un set di modifiche. Per ulteriori informazioni, consulta [CreateStack](#) o [UpdateStack](#) nella Documentazione di riferimento dell'API AWS CloudFormation .

7 dicembre 2018

[Rilevamento delle deviazioni di stack aggiunto](#)

È ora possibile rilevare se la configurazione effettiva di uno stack si è discostata dalla configurazione del modello prevista, come definito all'interno. CloudFormation È possibile rilevare la deriva su un intero stack o su singole risorse dello stack. Per ulteriori informazioni, consulta [Rilevare le modifiche di configurazione non gestite agli stack e alle risorse con il rilevamento delle deviazioni.](#)

13 novembre 2018

[secretsmanager riferimento dinamico ora disponibile](#)

È ora possibile utilizzare il riferimento `secretsmanager` dinamico per recuperare interi segreti o valori segreti archiviati in AWS Secrets Manager. I segreti possono essere le credenziali dei database, le password, le chiavi API di terza parte e anche le parti di testo arbitrario. L'utilizzo del riferimento `secretsmanager` dinamico garantisce che né Secrets Manager né CloudFormation registri o mantenga alcun valore segreto risolto. Per ulteriori informazioni, consulta [Ottenere un valore segreto o segreto da Secrets Manager.](#)

9 novembre 2018

[Macro ora disponibili](#)

Ora puoi utilizzare le macro per eseguire elaborazioni personalizzate sui modelli, da azioni semplici come find-and-replace operazioni a trasformazioni estese di interi modelli. Per ulteriori informazioni, consulta [Eseguire l'elaborazione personalizzata sui CloudFormation modelli con le macro dei modelli.](#)

6 settembre 2018

[CloudFormation ora supporta gli endpoint VPC basati su PrivateLink](#)

Puoi utilizzare un endpoint VPC per creare una connessione privata tra il tuo VPC e CloudFormation senza richiedere l'accesso tramite Internet, mediante un'istanza NAT, una connessione VPN o AWS Direct Connect. Per ulteriori informazioni, consulta [Accesso CloudFormation tramite un'interfaccia endpoint \(\).AWS PrivateLink](#)

22 agosto 2018

[I riferimenti dinamici supportano stringhe sicure](#)

È ora possibile utilizzare nuovi riferimenti dinamici per specificare i valori archiviati e gestiti in altri servizi, inclusi i parametri di SecureString tipo Systems Manager Parameter Store, nei modelli di stack. Per ulteriori informazioni, vedere [Ottenere un valore di stringa sicuro da Systems Manager Parameter Store.](#)

16 agosto 2018

[I set di stack ora supportano ruoli di esecuzione personalizzati](#)

Ora puoi utilizzare ruoli di esecuzione personalizzati negli account di destinazione per controllare le risorse dello stack che utenti o gruppi possono includere nei loro set di stack. Per ulteriori informazioni, consulta [Configurare le opzioni di autorizzazione avanzate per le operazioni di stack](#) set.

30 maggio 2018

[Aggiornamenti selettivi di istanze di stack](#)

Ora puoi utilizzare l'opzione Accounts e Regions i parametri per specificare gli account e le regioni in cui aggiornare le istanze dello stack durante un'operazione di aggiornamento dello stack set. Per ulteriori informazioni, consulta [UpdateStackSet](#) nella documentazione di riferimento dell'API AWS CloudFormation .

30 maggio 2018

[CloudFormation ora crea bucket S3 con crittografia abilitata](#)

Per i bucket Amazon S3 che CloudFormation creano modelli di stack caricati per archiviare, la crittografia lato server è ora abilitata per impostazione predefinita, crittografando così tutti gli oggetti archiviati in quei bucket. [Per ulteriori informazioni, consulta Creare uno stack dalla console. CloudFormation](#)

24 maggio 2018

[Endpoint FIPS aggiunti](#)

17 maggio 2018

CloudFormation ora offre nuovi endpoint che utilizzano moduli crittografici convalidati FIPS 140-2 nelle seguenti regioni pubbliche degli Stati Uniti: US-East-1, US-East-2, US-West-1 e US-West-2. [AWS CloudFormation Consultate gli endpoint e le quote URLs nella sezione dedicata al nuovo endpoint](#) conforme allo standard Riferimenti generali di Amazon Web Services FIPS.

Per gli aggiornamenti alla Guida per l'utente di AWS CloudFormation Hooks, consulta la cronologia dei documenti per la Guida per l'utente [di Hooks nella Guida per l' AWS CloudFormation](#) utente di Hooks.AWS CloudFormation

Aggiornamenti archiviati

La tabella seguente descrive le modifiche importanti apportate in ogni versione della Guida per l' AWS CloudFormation utente prima di maggio 2018.

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	22 luglio 2019	Utilizza la proprietà <code>encryptionOptions</code> per specificare una Chiave di proprietà di AWS o una chiave gestita dal cliente per broker Amazon MQ.	2010-05-15
Convenzione di denominazione dei set di stack	10 aprile 2018	CloudFormation gli stack creati utilizzando i set di stack ora seguono una nuova convenzione di denominazione, in cui il nome dello stack contiene il nome del set di stack.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	10 aprile 2018	AWS::AppSync::ApiKey Utilizzate la <code>AWS::AppSync::ApiKey</code> risorsa per creare una chiave univoca da distribuire ai client che eseguono operazioni GraphQL. AWS AppSync AWS::AppSync::DataSource Usa la <code>AWS::AppSync::DataSource</code> risorsa per creare sorgenti di dati per i resolver in. AWS AppSync AWS::AppSync::GraphQLApi Usa la <code>AWS::AppSync::GraphQLApi</code> risorsa per creare una nuova API AWS AppSync GraphQL. AWS::AppSync::GraphQLSchema Usa la <code>AWS::AppSync::GraphQLSchema</code> risorsa per creare il modello di dati per la tua API AWS AppSync GraphQL. AWS::AppSync::Resolver Utilizza la risorsa <code>AWS::AppSync::Resolver</code> per definire il resolver GraphQL logico che verrà collegato ai campi in uno schema.	2010-05-15
Risorsa aggiornata	10 aprile 2018	AWS::Config::ConfigurationAggregator Utilizza il tipo di <code>OrganizationAggregationSource</code> proprietà per specificare le regioni di AWS Config dati da aggregare in un aggregatore di AWS Config configurazione e il ruolo IAM da utilizzare e per recuperare i dettagli. AWS Organizations	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	4 aprile 2018	AWS::Config::AggregationAuthorization Usa la <code>AWS::Config::AggregationAuthorization</code> risorsa per concedere l'autorizzazione a raccogliere i tuoi dati a un account aggregatore. AWS Config AWS::Config::ConfigurationAggregator Utilizza la risorsa <code>AWS::Config::ConfigurationAggregator</code> per creare un aggregatore di configurazione per AWS Config.	2010-05-15
I set di stack ora supportano ruoli di amministratore personalizzati	29 marzo 2018	Utilizza ruoli di amministratore personalizzati per controllare quali utenti o gruppi possono gestire set di stack specifici all'interno dello stesso account amministratore. Per ulteriori informazioni, consulta Configurare le opzioni di autorizzazione avanzate per le operazioni di stack set.	2010-05-15
Nuova risorsa	29 marzo 2018	AWS::EC2::LaunchTemplate Usa la <code>AWS::EC2::LaunchTemplate</code> risorsa per creare un modello di lancio per un' EC2 istanza Amazon.	2010-05-15
Risorse aggiornate	29 marzo 2018	AWS::AutoScaling::AutoScalingGroup Utilizza la proprietà <code>LaunchTemplate</code> per specificare il modello di avvio da utilizzare per avviare istanze. AWS::EC2::SpotFleet Nel tipo di proprietà SpotFleetRequestConfigData, utilizza la proprietà <code>LaunchTemplateConfigs</code> per descrivere un modello di avvio e le sostituzioni.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova funzione <code>Fn::Cidr</code> intrinseca	6 marzo 2018	Restituisce il blocco dell'indirizzo Cidr specificato. Per ulteriori informazioni, consulta Fn::Cidr .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	6 marzo 2018	AWS::ApiGateway::VpcLink Utilizza la risorsa <code>AWS::ApiGateway::VpcLink</code> per specificare un collegamento a un VPC da API Gateway <code>AWS::ApiGateway::RestApi</code> per accedere alle risorse in un Amazon Virtual Private Cloud (VPC). AWS::GuardDuty::Master Usa la <code>AWS::GuardDuty::Master</code> risorsa per creare un account GuardDuty principale. AWS::GuardDuty::Member Usa la <code>AWS::GuardDuty::Member</code> risorsa per creare un account GuardDuty membro. AWS::SES::ConfigurationSet Utilizza la risorsa <code>AWS::SES::ConfigurationSet</code> per creare gruppi di regole che puoi applicare alle e-mail che invii. AWS::SES::ConfigurationSetEventDestination Utilizza la risorsa <code>AWS::SES::ConfigurationSetEventDestination</code> per specificare una destinazione per il set di configurazione di eventi. AWS::SES::ReceiptFilter Utilizza la risorsa <code>AWS::SES::ReceiptFilter</code> per specificare se accettare o rifiutare le e-mail provenienti da un indirizzo IP o da un intervallo di indirizzi IP.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		<u>AWS::SES::ReceiptRule</u> Utilizza la risorsa <code>AWS::SES::ReceiptRule</code> per specificare le operazioni che Amazon SES deve eseguire quando riceve mail per conto di uno o più indirizzi e-mail o domini di tua proprietà. <u>AWS::SES::ReceiptRuleSet</u> Utilizza la risorsa <code>AWS::SES::ReceiptRuleSet</code> per specificare un set di regole vuoto per Amazon SES. <u>AWS::SES::Template</u> Utilizza la risorsa <code>AWS::SES::Template</code> per specificare i contenuti delle e-mail (costituite da un oggetto, una parte HTML e una parte di solo testo).	

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	6 marzo 2018	AWS::AutoScaling::AutoScalingGroup Utilizza la proprietà <code>AutoScalingGroupName</code> per specificare il nome del gruppo con dimensionamento automatico. AWS::ApiGateway::RestApi Utilizza la proprietà <code>ApiKeySourceType</code> per specificare l'origine della chiave API per le richieste di misurazione in base a un piano di utilizzo. Utilizza la proprietà <code>MinimumCompressionSize</code> per specificare un numero intero che ammette valori Null utilizzato per abilitare o disabilitare la compressione su un'API. AWS::ApplicationAutoScaling::ScalingPolicy Nel tipo di proprietà TargetTrackingScalingPolicyConfiguration, utilizza la proprietà <code>DisableScaleIn</code> per specificare se l'incremento in base alla policy di monitoraggio dei target è disabilitato. AWS::EC2::SpotFleet Nel tipo di LaunchSpecifications proprietà, utilizzate la <code>TagSpecifications</code> proprietà per specificare i tag da applicare durante la <code>SpotFleet</code> creazione. AWS::Elasticsearch::Domain Utilizza l'attributo <code>Arn</code> per fare in modo che <code>Fn::GetAtt</code> restituisca l'Amazon Resource Name (ARN) del dominio. L'attributo <code>DomainArn</code> di <code>Fn::GetAtt</code> è stato reso obsoleto.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::RDS::DBCluster Utilizza la proprietà <code>DBClusterIdentifier</code> per specificare l'identificatore del cluster di database. AWS::RDS::DBCluster Utilizza la proprietà <code>DBClusterIdentifier</code> per specificare l'identificatore del cluster di database. AWS::Redshift::Cluster Utilizza la proprietà <code>ClusterIdentifier</code> per specificare l'identificatore univoco del cluster. AWS::Route53::HealthCheck Nel tipo di HealthCheckConfig proprietà, utilizzate la <code>Regions</code> proprietà per specificare le regioni da cui desiderate che i controllori dello stato di Route 53 controllino l'endpoint specificato. AWS::SSM::Document Utilizza la proprietà <code>Tags</code> per specificare i tag di risorsa CloudFormation da applicare al documento.	
Risorsa aggiornata	19 febbraio 2018	AWS::CodeBuild::Project Utilizza la proprietà <code>Triggers</code> per configurare un webhook per il progetto in modo che inizi a compilare automaticamente il codice sorgente ogni volta che una modifica al codice viene inviata al repository. Questa opzione è disponibile solo per i GitHub progetti in. CloudFormation Non è disponibile per i progetti GitHub Enterprise.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorsa aggiornata	8 febbraio 2018	AWS::DynamoDB::Table Utilizza la proprietà <code>SSESpecification</code> per specificare le impostazioni per abilitare la crittografia lato server.	2010-05-15
Risorsa aggiornata	5 febbraio 2018	AWS::CodeBuild::Project Nel tipo di proprietà Source CodeBuild Project Source: • Utilizza la proprietà <code>GitCloneDepth</code> per specificare il livello della cronologia da scaricare. • Utilizzate la <code>InsecureSsl</code> proprietà per specificare se ignorare gli avvisi SSL durante la connessione all'archivio dei progetti GitHub Enterprise.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	23 gennaio 2018	AWS::AutoScaling::LifecycleHook Utilizza la proprietà <code>LifecycleHookName</code> per specificare il nome dell'hook del ciclo di vita. AWS::DynamoDB::Table La proprietà <code>AttributeDefinitions</code> ora richiede la sostituzione quando viene aggiornata. AWS::EC2::Instance Utilizza la proprietà <code>CreditSpecification</code> per specificare l'opzione di credito per l'utilizzo della CPU di un'istanza T2. Utilizzate la <code>ElasticGpuSpecifications</code> proprietà per specificare le risorse GPU elastiche GPUs che potete collegare all'istanza per accelerare le prestazioni grafiche delle applicazioni. AWS::EC2::VPC La proprietà <code>InstanceTenancy</code> ora non richiede alcuna interruzione quando viene aggiornata da "dedicated" a "default" . AWS::ECS::Service Utilizza la proprietà <code>HealthCheckGracePeriodSeconds</code> per specificare il periodo di tempo, in secondi, durante il quale il pianificatore del servizio Amazon ECS ignora i controlli dello stato del target Elastic Load Balancing dopo l'avvio di un'attività. AWS::IoT::TopicRule Nel tipo di proprietà DynamoDBAction, le proprietà <code>RangeKeyField</code> e <code>RangeKeyValue</code> non sono più necessarie.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::KinesisAnalytics::ApplicationOutput Nel tipo di proprietà ApplicationOutput, utilizza la proprietà <code>LambdaOutput</code> per identificare una funzione Lambda come destinazione durante la configurazione dell'output dell'applicazione. AWS::Kinesis::Stream Utilizzate la <code>StreamEncryption</code> proprietà per abilitare o aggiornare la crittografia lato server utilizzando un AWS KMS key per uno stream specificato. AWS::Lambda::Function Utilizza la proprietà <code>ReservedConcurrentExecutions</code> per specificare il valore massimo di esecuzioni simultanee da riservare per la funzione. AWS::RDS::DBSubnetGroup Utilizza la proprietà <code>DBSubnetGroupName</code> per specificare il nome del gruppo di sottoreti del database. AWS::S3::Bucket Utilizza la <code>BucketEncryption</code> proprietà per specificare la crittografia predefinita per un bucket utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (bucket SSE-S3 o (SSE-KMS). AWS KMS keys Nel tipo di proprietà ReplicationRule, utilizza la proprietà <code>SourceSelectionCriteria</code> per specificare filtri aggiuntivi nell'identificazione degli oggetti di origine che desideri replicare.	

Modifica	Data di rilascio	Descrizione	Versione API
		Nel tipo di proprietà ReplicationDestination: • Usa la <code>AccessControlTranslation</code> proprietà per specificare la proprietà della replica dell'account che possiede il bucket di destinazione. AWS • Utilizza la proprietà <code>Account</code> per specificare l'ID dell'account del proprietario del bucket di destinazione. • Utilizza la proprietà <code>EncryptionConfiguration</code> per specificare informazioni relative alla crittografia per un bucket che è una destinazione per gli oggetti replicati. AWS::SSM::Association Utilizzate la <code>AssociationName</code> proprietà per specificare il nome dell'associazione tra un documento SSM e EC2 le istanze che contengono un agente di configurazione per elaborare il documento.	
Trigger di rollback aggiunti alla console. CloudFormation	15 gennaio 2018	I trigger di rollback consentono di CloudFormation monitorare lo stato dell'applicazione durante la creazione e l'aggiornamento dello stack e di ripristinare tale operazione se l'applicazione supera la soglia di uno degli allarmi specificati. Per ulteriori informazioni, consulta Operazioni di monitoraggio e rollback di stack.	2010-05-15
Risorsa aggiornata	12 gennaio 2018	AWS::SSM::Parameter Utilizza la proprietà <code>AllowedPattern</code> per specificare un'espressione regolare utilizzata per convalidare il valore del parametro.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	5 dicembre 2017	AWS::Inspector::AssessmentTarget Utilizza la risorsa <code>AWS::Inspector::AssessmentTarget</code> per creare un target di valutazione Amazon Inspector. AWS::Inspector::AssessmentTemplate Utilizza la risorsa <code>AWS::Inspector::AssessmentTemplate</code> per creare un modello di valutazione Amazon Inspector. AWS::Inspector::ResourceGroup Utilizza la risorsa <code>AWS::Inspector::ResourceGroup</code> per creare un gruppo di risorse Amazon Inspector che definisce i tag che identificano le risorse AWS che costituiscono un target di valutazione Amazon Inspector. AWS::ServiceDiscovery::Instance Utilizza la risorsa <code>AWS::ServiceDiscovery::Instance</code> per specificare informazioni su un'istanza creata da Amazon Route 53. AWS::ServiceDiscovery::PrivateDnsNamespace Utilizza la risorsa <code>AWS::ServiceDiscovery::PrivateDnsNamespace</code> per specificare informazioni su uno spazio dei nomi privato per Amazon Route 53. AWS::ServiceDiscovery::PublicDnsNamespace Utilizza la risorsa <code>AWS::ServiceDiscovery::PublicDnsNamespace</code> per specificare informazioni su uno spazio dei nomi pubblico per Amazon Route 53.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::ServiceDiscovery::Service Utilizza la risorsa <code>AWS::ServiceDiscovery::Service</code> per definire un modello per un massimo di cinque record e un ulteriore controllo dello stato che Amazon Route 53 deve creare quando registri un'istanza.	
Risorsa aggiornata	5 dicembre 2017	AWS::KinesisAnalytics::Application Nel tipo di proprietà Input , utilizza la proprietà <code>InputProcessingConfiguration</code> per trasformare i record mentre vengono ricevuti dal flusso.	2010-05-15
Risorsa aggiornata	1° dicembre 2017	AWS::CodeBuild::Project Utilizza la proprietà <code>BadgeEnabled</code> per generare un URL accessibile pubblicamente per il badge di compilazione di un progetto. Utilizza la proprietà <code>Cache</code> per configurare le impostazioni della cache per le dipendenze della build. Utilizza la <code>VpcConfig</code> proprietà per abilitare l'accesso CodeBuild alle risorse in un Amazon VPC. Nel tipo di proprietà EnvironmentVariable , utilizza la proprietà <code>Type</code> per specificare il tipo di variabile di ambiente.	2010-05-15
Nuova risorsa	30 novembre 2017	AWS::Cloud9::EnvironmentEC2 Usa la <code>AWS::Cloud9::EnvironmentEC2</code> risorsa per creare un ambiente di EC2 sviluppo Amazon in AWS Cloud9.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	29 novembre 2017	AWS::ECS::TaskDefinition Utilizza la proprietà <code>Cpu</code> per specificare il numero di unità CPU necessarie per l'attività. Utilizza la proprietà <code>ExecutionRoleArn</code> per specificare l'ARN del ruolo per l'esecuzione. Utilizza la proprietà <code>Memory</code> per specificare la quantità (in MiB) di memoria necessaria per l'attività. Utilizza la proprietà <code>RequiresCompatibilities</code> per specificare il tipo di avvio richiesto dall'attività. AWS::ECS::Service Utilizza la proprietà <code>LaunchType</code> per specificare il tipo di avvio su cui eseguire il tuo servizio. Utilizza la proprietà <code>NetworkConfiguration</code> per specificare la configurazione di rete per il servizio. Utilizza la proprietà <code>PlatformVersion</code> per specificare la versione della piattaforma su cui eseguire il tuo servizio.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	28 novembre 2017	AWS::GuardDuty::Detector Usa la <code>AWS::GuardDuty::Detector</code> risorsa per creare un singolo GuardDuty rilevatore Amazon. AWS::GuardDuty::IPSet Usa la <code>AWS::GuardDuty::IPSet</code> risorsa per creare un set di GuardDuty IP Amazon. AWS::GuardDuty::ThreatIntelSet Usa la <code>AWS::GuardDuty::ThreatIntelSet</code> risorsa per creare un ThreatIntelSet.	2010-05-15
Risorse aggiornate	28 novembre 2017	AWS::CodeDeploy::Application Utilizza la <code>ComputePlatform</code> proprietà per specificare una piattaforma di AWS Lambda calcolo su CodeDeploy cui distribuire un'applicazione. AWS::CodeDeploy::DeploymentGroup Nel tipo di proprietà DeploymentStyle, utilizza la proprietà <code>DeploymentType</code> per specificare una distribuzione blu/verde su una piattaforma di calcolo Lambda. AWS::EC2::SpotFleet Nel tipo di proprietà SpotFleetRequestConfigData, la proprietà <code>SpotPrice</code> è ora opzionale. AWS::Lambda::Alias Utilizzate la <code>RoutingConfig</code> proprietà per specificare due diverse versioni di una AWS Lambda funzione, in modo da stabilire quale percentuale di traffico richiamerà ciascuna versione.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova policy di aggiornamento CodeDeployLambdaAliasUpdate	28 novembre 2017	Utilizza la politica di CodeDeployLambdaAliasUpdate per eseguire una CodeDeploy distribuzione quando la versione cambia su una <code>AWS::Lambda::Alias</code> risorsa. Per ulteriori informazioni, consulta UpdatePolicyAttributo .	2010-05-15
Nuovi tipi di parametro SSM	21 Novembre 2017	Seleziona i tipi di parametro SSM per utilizzare i parametri esistenti di Archivio parametri Systems Manager. Nota: attualmente CloudFormation non supporta il tipo <code>SecureString</code> . Per ulteriori informazioni, consulta la sezione sui tipi di parametri di SSM .	2010-05-15
Nuovo campo ResolvedValue per il tipo di dati Parameter	21 Novembre 2017	Il campo <code>ResolvedValue</code> restituisce il valore utilizzato nella definizione dello stack per un parametro SSM. Per ulteriori informazioni, consulta il tipo di dati Parameter nella Documentazione di riferimento delle API AWS CloudFormation.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	20 novembre 2017	AWS::ApiGateway::ApiKey Utilizza la proprietà <code>CustomerId</code> per specificare un identificatore di clienti AWS Marketplace. Utilizza la proprietà <code>GenerateDistinctId</code> per specificare se l'identificatore di chiave è diverso dal valore della chiave API creata. AWS::ApiGateway::Authorizer Utilizza la proprietà <code>AuthType</code> per specificare un campo definito dal cliente utilizzato nelle importazioni/esportazioni Swagger senza impatto funzionale. AWS::ApiGateway::DomainName Utilizza la proprietà <code>EndpointConfiguration</code> per specificare i tipi di endpoint di un nome di dominio di API Gateway. Utilizza la proprietà <code>RegionalCertificateArn</code> come riferimento a un certificato per l'utilizzo da parte dell'endpoint regionale per un nome di dominio. AWS::ApiGateway::Method Nei tipi di proprietà Integration e IntegrationResponse, utilizza la proprietà <code>ContentHandling</code> per specificare il modo in cui gestire le conversioni del tipo di contenuto del payload della richiesta. AWS::ApiGateway::RestApi Utilizza la proprietà <code>EndpointConfiguration</code> per specificare i tipi di endpoint di una REST API di API Gateway.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::ApplicationAutoScaling::ScalableTarget Utilizza la proprietà <code>ScheduledActions</code> per specificare le operazioni pianificate per un target scalabile Application Auto Scaling. AWS::ECR::Repository Utilizza la proprietà <code>LifecyclePolicy</code> per specificare una policy del ciclo di vita per un repository Amazon ECR. AWS::ECS::TaskDefinition Nel tipo di proprietà ContainerDefinition, utilizza la proprietà <code>LinuxParameters</code> per indicare opzioni specifiche di Linux per un container Amazon ECS. AWS::ElastiCache::ReplicationGroup Utilizza la proprietà <code>AtRestEncryptionEnabled</code> per abilitare la crittografia dei dati inattivi. Utilizza la proprietà <code>AuthToken</code> per specificare una password utilizzata per accedere a un server protetto da password. Utilizza la proprietà <code>TransitEncryptionEnabled</code> per abilitare la crittografia dei dati in transito. AWS::ElasticLoadBalancingV2::TargetGroup Utilizza l'attributo <code>TargetGroupName</code> con la funzione <code>Fn::GetAtt</code> per ottenere il nome di un gruppo target Elastic Load Balancing.	

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::Elasticsearch::Domain Utilizzare la <code>VPCOptions</code> proprietà per specificare una configurazione VPC per il dominio OpenSearch Service. AWS::EMR::Cluster Utilizza la proprietà <code>EbsRootVolumeSize</code> per specificare le dimensioni del volume root EBS per un cluster Amazon EMR. AWS::RDS::DBInstance Utilizza le proprietà <code>SourceRegion</code> e <code>KmsKeyId</code> per creare una replica di lettura crittografata da un'istanza database di origine tra Regioni. AWS::Route53::HostedZone Utilizza la proprietà <code>QueryLoggingConfig</code> per specificare una configurazione per la registrazione delle query DNS.	
Nuovo campo <code>NoEcho</code> per gli oggetti <code>Response</code> di risorse personalizzate	20 novembre 2017	Ora puoi utilizzare il campo opzionale <code>NoEcho</code> per mascherare l'output di una risorsa personalizzata. Per ulteriori informazioni, consulta Oggetti di risposta di risorse personalizzate. Il parametro <code>noEcho</code> corrispondente è supportato dal metodo <code>send</code>. Per ulteriori informazioni, consulta cfn-response Module.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Sostituzioni delle istanze di stack aggiunte per i set di stack.	17 Novembre 2017	CloudFormation StackSets consente di sovrascrivere i valori dei parametri nelle istanze dello stack per account e regione. Puoi sostituire i valori dei parametri quando crei istanze di stack o aggiorni istanze di stack esistenti . Per ulteriori informazioni, consulta Sostituzione dei parametri su istanze dello stack .	2010-05-15
Risorsa aggiornata	15 novembre 2017	AWS::StepFunctions::StateMachine Puoi utilizzare <code>AWS::StepFunctions::StateMachine</code> per specificare un <code>StateMachineName</code> durante la creazione di una macchina a stati e puoi aggiornare sia <code>DefinitionString</code> che <code>RoleArn</code> senza sostituire la macchina a stati.	2010-05-15
StackSets ora supporta un massimo di 500 istanze di stack per set di stack.	6 novembre 2017	Ora puoi creare un massimo di 500 istanze di stack per set di stack. Per ulteriori informazioni sui AWS CloudFormation limiti, consulta Understand quote. CloudFormation	2010-05-15
Nuove risorse	2 Novembre 2017	AWS::CloudFront::CloudFrontOriginAccessIdentity Utilizza la <code>AWS::CloudFront::CloudFrontOriginAccessIdentity</code> risorsa per specificare l'identità di accesso all' CloudFront origine di Amazon da associare all'origine di una CloudFront distribuzione. AWS::CloudFront::StreamingDistribution Utilizza la <code>AWS::CloudFront::StreamingDistribution</code> risorsa per specificare una distribuzione di streaming Adobe Real-Time Messaging Protocol (RTMP) per CloudFront.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	2 Novembre 2017	AWS::ApiGateway::Deployment La proprietà <code>StageName</code> è stata resa obsoleta sul tipo di proprietà StageDescription. AWS::ApiGateway::Method Utilizza la proprietà <code>OperationName</code> per assegnare un nome descrittivo a un metodo API Gateway. Utilizza la proprietà <code>RequestValidatorId</code> per associare un validator di richieste a un metodo. AWS::AutoScaling::AutoScalingGroup Utilizza la proprietà <code>LifecycleHookSpecificationList</code> per specificare le operazioni da eseguire quando Auto Scaling avvia o termina istanze. AWS::CloudFront::Distribution Utilizzate la <code>Tags</code> proprietà per specificare un set arbitrario di tag (coppie chiave-valore) da associare a una distribuzione. CloudFront Nei tipi di DefaultCacheBehavior proprietà CacheBehaviorand, utilizzate la <code>LambdaFunctionAssociations</code> proprietà per specificare le associazioni di funzioni Lambda per una CloudFront distribuzione. Nel tipo di proprietà CustomOriginConfig, utilizza la proprietà <code>OriginKeepaliveTimeout</code> per specificare un timeout keep-alive personalizzato e la proprietà <code>OriginReadTimeout</code> per specificare un timeout di lettura origine personalizzato.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		Nel tipo di DistributionConfig proprietà, utilizzate la <code>IPV6Enabled</code> proprietà per specificare se CloudFront risponde alle richieste IPv6 DNS con un IPv6 indirizzo per la distribuzione. AWS::CodeDeploy::DeploymentGroup Nel tipo di proprietà LoadBalancerInfo, utilizza la proprietà <code>TargetGroupInfoList</code> per specificare informazioni su un gruppo target in Elastic Load Balancing da utilizzare in una distribuzione. AWS::EC2::SecurityGroup, AWS::EC2::SecurityGroupEgress e AWS::EC2::SecurityGroupIngress Utilizza la proprietà <code>Description</code> per specificare la descrizione di una regola di un gruppo di sicurezza. AWS::EC2::Subnet La proprietà <code>Ipv6CidrBlock</code> ora supporta gli aggiornamenti <code>No interruption</code>. AWS::EC2::VPNGateway Utilizza la proprietà <code>AmazonSideAsn</code> per specificare un Autonomous System Number (ASN) privato per il lato Amazon di una sessione BGP. AWS::EC2::VPNConnection Utilizza la proprietà <code>VpnTunnelOptionsSpecifications</code> per configurare le opzioni di tunnel per una connessione VPN. AWS::ElasticBeanstalk::ConfigurationTemplate e AWS::ElasticBeanstalk::Environment Nei tipi di proprietà ConfigurationOptionSetting e OptionSetting, utilizza la proprietà <code>ResourceName</code>	

Modifica	Data di rilascio	Descrizione	Versione API
		per specificare un nome di risorsa per un'opzione di configurazione di dimensionamento basata sul tempo. AWS::EMR::Cluster Utilizza la proprietà <code>CustomAmiId</code> personalizzata per specificare un AMI Amazon Linux per un cluster. AWS::KinesisFirehose::DeliveryStream Utilizza l'attributo <code>Arn</code> con la funzione <code>Fn::GetAtt</code> per ottenere l'Amazon Resource Name (ARN) del flusso di distribuzione. AWS::KMS::Key Utilizza la proprietà <code>Tags</code> per specificare un set di tag arbitrario (coppie chiave-valore) da associare a una chiave gestita dal cliente. AWS::OpsWorks::Layer e AWS::OpsWorks::Stack Utilizzate la <code>Tags</code> proprietà per specificare un set arbitrario di tag (coppie chiave-valore) da associare a un livello o a una pila. AWS OpsWorks AWS::RDS::OptionGroup Nel tipo di proprietà OptionConfiguration, utilizza la proprietà <code>OptionVersion</code> per specificare una versione per l'opzione. AWS::S3::Bucket Utilizza la proprietà <code>AnalyticsConfigurations</code> per configurare un filtro di analisi per un bucket Amazon S3.	

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	24 ottobre 2017	AWS::Glue::Classifier Utilizza la risorsa <code>AWS::Glue::Classifier</code> per creare un classificatore AWS Glue . AWS::Glue::Connection Utilizzate la <code>AWS::Glue::Connection</code> risorsa per specificare una AWS Glue connessione a un'origine dati. AWS::Glue::Crawler Utilizza la risorsa <code>AWS::Glue::Crawler</code> per specificare un crawler AWS Glue . AWS::Glue::Database Utilizza la risorsa <code>AWS::Glue::Database</code> per creare un database AWS Glue . AWS::Glue::DevEndpoint Utilizza la risorsa <code>AWS::Glue::DevEndpoint</code> per specificare un endpoint di sviluppo per il debug in remoto di script ETL. AWS::Glue::Job Utilizza la risorsa <code>AWS::Glue::Job</code> per specificare un processo AWS Glue nel catalogo di dati. AWS::Glue::Partition Utilizza la risorsa <code>AWS::Glue::Partition</code> per creare una partizione AWS Glue , che rappresenta una porzione dei dati della tabella. AWS::Glue::Table Utilizza la risorsa <code>AWS::Glue::Table</code> per creare una tabella AWS Glue .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::Glue::Trigger Utilizzate la <code>AWS::Glue::Trigger</code> risorsa per specificare i trigger che eseguono i AWS Glue job.	
Nuove risorse	11 ottobre 2017	AWS::SSM::MaintenanceWindow Utilizzate la <code>AWS::SSM::MaintenanceWindow</code> risorsa per creare una finestra AWS Systems Manager di manutenzione. AWS::SSM::MaintenanceWindowTarget Utilizza la risorsa <code>AWS::SSM::MaintenanceWindowTarget</code> per registrare un target con una finestra di manutenzione. AWS::SSM::MaintenanceWindowTask Utilizza la risorsa <code>AWS::SSM::MaintenanceWindowTask</code> per definire un'attività della finestra di manutenzione. AWS::SSM::PatchBaseline Utilizza la risorsa <code>AWS::SSM::PatchBaseline</code> per definire una base di confronto delle patch per Systems Manager.	2010-05-15
Nuova risorsa	10 Ottobre 2017	AWS::ElasticLoadBalancingV2::ListenerCertificate Utilizza la risorsa <code>AWS::ElasticLoadBalancingV2::ListenerCertificate</code> per specificare certificati per un listener Elastic Load Balancing.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova risorsa	27 settembre 2017	AWS::Athena::NamedQuery Utilizza la risorsa <code>AWS::Athena::NamedQuery</code> per creare una query Amazon Athena.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	27 settembre 2017	AWS::EC2::NatGateway Utilizza la proprietà <code>Tags</code> per specificare i tag delle risorse per un gateway NAT. AWS::ElasticBeanstalk::Application Utilizza la proprietà <code>ResourceLifecycleConfig</code> per definire le impostazioni del ciclo di vita delle risorse che appartengono all'applicazione e il ruolo del servizio assunto da Elastic Beanstalk per applicare impostazioni del ciclo di vita. AWS::ElasticBeanstalk::ConfigurationTemplate e AWS::ElasticBeanstalk::Environment Utilizza la proprietà <code>PlatformArn</code> per specificare una piattaforma personalizzata per Elastic Beanstalk. AWS::ElasticLoadBalancingV2::TargetGroup Nel tipo di proprietà TargetDescription, utilizzare la <code>AvailabilityZone</code> proprietà per specificare la zona di disponibilità in cui registrare l'indirizzo IP. AWS::Events::Rule Nel tipo di proprietà Target, utilizza le seguenti proprietà per la trasformazione in input degli eventi e l'impostazione di target di attività Amazon ECS e di flussi Kinesis. • <code>EcsParameters</code> • <code>InputTransformer</code> • <code>KinesisParameters</code> • <code>RunCommandParameters</code>	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::KinesisFirehose::DeliveryStream Utilizzate la <code>DeliveryStreamType</code> proprietà per specificare il tipo di flusso e la <code>KinesisStreamSourceConfiguration</code> proprietà ARNs per specificare il flusso e il ruolo di un flusso Kinesis utilizzato come origine per un flusso di distribuzione. AWS::RDS::DBInstance Per la proprietà <code>Engine</code>, se hai specificato <code>oracle-se</code> o <code>oracle-se1</code>, puoi effettuare l'aggiornamento a <code>oracle-se2</code> senza sostituire l'istanza database. AWS::S3::Bucket Utilizza la proprietà <code>AccelerateConfiguration</code> per configurare lo stato di Transfer Acceleration per un bucket Amazon S3.	
Protezione da cessazione aggiunta per gli stack.	26 settembre 2017	L'abilitazione della protezione da cessazione su uno stack impedisce che questo venga eliminato accidentalmente. Un utente non può eliminare uno stack con la protezione da cessazione abilitata. Per ulteriori informazioni, consulta Proteggere uno stack dall'eliminazione .	2010-05-15
Valore <code>umask</code> predefinito modificato dalla versione 1.4-22 in poi	14 settembre 2017	Il valore del parametro <code>umask</code> predefinito per il file di configurazione <code>cfh-hup.conf</code> è ora <code>022</code> . Per ulteriori informazioni, consulta cfh-hup .	

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	7 settembre 2017	AWS::ElasticLoadBalancingV2::LoadBalancer Utilizzate la <code>SubnetMappings</code> proprietà per specificare le sottoreti da collegare al sistema IDs di bilanciamento del carico. Utilizza la proprietà <code>Type</code> per specificare il tipo di load balancer da creare. AWS::ElasticLoadBalancingV2::TargetGroup Utilizza la proprietà <code>TargetType</code> per specificare il tipo di registrazione dei target in questo gruppo di target.	2010-05-15
Trigger di rollback aggiunti all'API CloudFormation	31 agosto 2017	I trigger di rollback consentono di CloudFormation monitorare lo stato dell'applicazione durante la creazione e l'aggiornamento dello stack e di ripristinare tale operazione se l'applicazione supera la soglia di uno degli allarmi specificati. Per ulteriori informazioni, consulta RollbackConfiguration nella documentazione di riferimento dell'API AWS CloudFormation .	2010-05-15
Nuovo parametro <code>umask</code> per il file <code>cfn-hup.conf</code>	31 agosto 2017	Utilizza il parametro <code>umask</code> nel file di configurazione <code>cfn-hup.conf</code> per controllare le autorizzazioni dei file utilizzati e dal daemon <code>cfn-hup</code> (versione 1.4-21). Per ulteriori informazioni, consulta cfn-hup.	

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornate risorse per il supporto del dimensionamento del VPC	29 agosto 2017	AWS::EC2::VPCCidrBlock Utilizzare la <code>CidrBlock</code> proprietà per associare un blocco IPv4 CIDR a un VPC. AWS::EC2::VPC Usa l' <code>CidrBlockAssociations</code> attributo con la <code>Fn::GetAtt</code> funzione per ottenere un elenco di associazioni di blocchi IPv4 CIDR IDs associate al VPC.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	23 agosto 2017	AWS::S3::Bucket Nel tipo di proprietà Rule, utilizza la proprietà <code>TagFilters</code> per specificare i tag da utilizzare per identificare un sottoinsieme di oggetti per un bucket Amazon S3. Utilizza la <code>MetricsConfiguration</code> proprietà per specificare una configurazione dei parametri per i parametri di CloudWatch richiesta da un bucket Amazon S3. AWS::IoT::TopicRule Nel tipo di proprietà Action, utilizza la proprietà <code>DynamoDBv2Action</code> per descrivere un'operazione AWS IoT che scrive dati in una tabella DynamoDB. Nel tipo di proprietà Action, la proprietà <code>DynamoDBAction</code> ora supporta le proprietà <code>HashKeyType</code> e <code>RangeKeyType</code>. AWS::Lambda::Permission Utilizza la proprietà <code>EventSourceToken</code> per specificare un token univoco che deve essere fornito dall'entità di sicurezza che invoca la funzione.	2010-05-15
Nuovi pseudoparametri	23 agosto 2017	Utilizza gli pseudoparametri <code>AWS::Partition</code> per ottenere la partizione in cui si trova una risorsa. Utilizza lo pseudoparametro <code>AWS::URLSuffix</code> per ottenere il suffisso per un dominio. Per ulteriori informazioni, consulta Riferimenti agli pseudoparametri.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse per il supporto di DAX	22 agosto 2017	AWS::DAX::Cluster Utilizza la risorsa <code>AWS::DAX::Cluster</code> per creare un cluster DAX da utilizzare con Amazon DynamoDB. AWS::DAX::ParameterGroup Utilizza la risorsa <code>AWS::DAX::ParameterGroup</code> per creare un gruppo di parametri da utilizzare con Amazon DynamoDB. AWS::DAX::SubnetGroup Utilizza la risorsa <code>AWS::DAX::SubnetGroup</code> per creare un gruppo di sottoreti da utilizzare con DAX (accelerator DynamoDB).	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	18 agosto 2017	AWS::ApiGateway::DocumentationPart e AWS::ApiGateway::DocumentationVersion per creare la documentazione per l'API API Gateway. AWS::ApiGateway::GatewayResponse Utilizza la risorsa <code>AWS::ApiGateway::GatewayResponse</code> per creare una risposta personalizzata per l'API API Gateway. AWS::ApiGateway::RequestValidator Utilizza la risorsa <code>AWS::ApiGateway::RequestValidator</code> per configurare regole di convalida per le richieste in entrata all'API API Gateway. AWS::EC2::NetworkInterfacePermission Usa la <code>AWS::EC2::NetworkInterfacePermission</code> risorsa per concedere l'autorizzazione di un AWS account a un'interfaccia di rete.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	18 agosto 2017	AWS::ApiGateway::Stage Utilizza la proprietà <code>DocumentationVersion</code> per specificare uno snapshot con versione delle documentazione dell'API. AWS::AutoScaling::ScalingPolicy Utilizza la proprietà <code>TargetTrackingConfiguration</code> per specificare una configurazione di policy di dimensionamento di monitoraggio dei target Auto Scaling. AWS::CloudTrail::Trail Utilizza la proprietà <code>EventSelectors</code> per il supporto di eventi di dati Amazon S3. AWS::CodeDeploy::DeploymentGroup Utilizza le proprietà <code>LoadBalancerInfo</code> e <code>DeploymentStyle</code> per specificare un load balancer Elastic Load Balancing per una distribuzione in loco. Utilizza la proprietà <code>AutoRollbackConfiguration</code> per configurare il rollback automatico per la distribuzione. AWS::EC2::SpotFleet Nel tipo di proprietà SpotFleetRequestConfigData, utilizza la proprietà <code>ReplaceUnhealthyInstances</code> per indicare se il parco istanze Spot deve sostituire le istanze non integre e la proprietà <code>Type</code> per specificare il tipo di richiesta.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::EC2::Subnet Utilizzate le <code>Ipv6CidrBlock</code> proprietà <code>AssignIpv6AddressOnCreation</code> and per creare una sottorete con un blocco IPv6 CIDR. AWS::KinesisFirehose::DeliveryStream Utilizza la proprietà <code>ExtendedS3DestinationConfiguration</code> per configurare una destinazione in Amazon S3. Utilizza la proprietà secondaria <code>ProcessingConfiguration</code> in ciascuna configurazione di destinazione per invocare funzioni Lambda che trasformano i dati di origine in entrata e distribuiscono i dati trasformati alle destinazioni. AWS::RDS::DBCluster e AWS::RDS::DBInstance L'impostazione predefinita <code>DeletionPolicy</code> è ora <code>Snapshot</code> per <code>AWS::RDS::DBCluster</code> le risorse e per <code>AWS::RDS::DBInstance</code> le risorse che non specificano la <code>DBClusterIdentifier</code> proprietà. Per ulteriori informazioni, consulta DeletionPolicyAttributo. AWS::S3::Bucket Nel tipo di proprietà Rule, utilizza la proprietà <code>AbortIncompleteMultipartUpload</code> per specificare una regola del ciclo di vita che interrompe e caricamenti in più parti incompleti in un bucket Amazon S3. AWS::SQS::Queue Utilizza le proprietà <code>KmsMasterKeyId</code> e <code>KmsDataKeyReusePeriodSeconds</code> per	

Modifica	Data di rilascio	Descrizione	Versione API
		configurare la crittografia lato server per Amazon SQS. Aggiunto l'attributo <code>Arn</code> alla funzione <code>Fn::GetAtt</code> intrinseca per le risorse seguenti: • AWS::CloudTrail::Trail. Aggiunto anche <code>SnsTopicArn</code>. • AWS::CloudWatch::Alarm • AWS::DynamoDB::Table • AWS::ECS::Cluster • AWS::IoT::Policy • AWS::IoT::TopicRule • AWS::Logs::Destination	
Support per gli stack tag negli artefatti CodePipeline	18 agosto 2017	È ora possibile specificare i tag per gli stack nei file di configurazione dei modelli da utilizzare come artefatti per le pipeline. CodePipeline I tag specificati vengono applicati agli stack creati utilizzando il file di configurazione del modello. Per ulteriori informazioni, consulta Artifacts. CloudFormation	2010-05-15
Creazione di file system crittografati	14 agosto 2017	AWS::EFS::FileSystem Utilizza la proprietà <code>Encrypted</code> per eseguire la crittografia di un file system Amazon EFS durante la creazione. Utilizza la proprietà <code>KmsKeyId</code> per specificare in via opzionale una chiave personalizzata gestita dal cliente da utilizzare per proteggere il file system crittografato.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse di supporto AWS Batch	8 agosto 2017	AWS::Batch::ComputeEnvironment Usa la <code>AWS::Batch::ComputeEnvironment</code> risorsa per definire il tuo ambiente di AWS Batch elaborazione. AWS::Batch::JobDefinition Utilizzate la <code>AWS::Batch::JobDefinition</code> risorsa per specificare i parametri per la definizione di un AWS Batch processo. AWS::Batch::JobQueue Utilizzate la <code>AWS::Batch::JobQueue</code> risorsa per definire la vostra coda di AWS Batch lavoro.	2010-05-15
Nuove risorse per il supporto del Servizio gestito da Amazon per Apache Flink	28 luglio 2017	AWS::KinesisAnalytics::Application Utilizza la risorsa <code>AWS::KinesisAnalytics::Application</code> per creare un'applicazione Servizio gestito da Amazon per Apache Flink. AWS::KinesisAnalytics::ApplicationOutput Utilizza la risorsa <code>AWS::KinesisAnalytics::ApplicationOutput</code> per aggiungere una destinazione esterna all'applicazione del servizio gestito da Amazon per Apache Flink. AWS::KinesisAnalytics::ApplicationReferenceDataSource Utilizza la risorsa <code>AWS::KinesisAnalytics::ApplicationReferenceDataSource</code> per aggiungere un'origine dati di riferimento a un'applicazione del Servizio gestito da Amazon per Apache Flink basata su SQL.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Utilizzalo StackSets per gestire centralmente gli stack tra account e regioni	25 luglio 2017	StackSets consente di creare, aggiornare o eliminare gli stack su più account e regioni con un'unica operazione. Utilizzando un account amministratore, è possibile definire e gestire un CloudFormation modello e utilizzarlo come base per il provisioning degli stack in account di destinazione selezionati in aree specifiche. Per ulteriori informazioni, consulta Gestire gli stack tra account e regioni con StackSets	2010-05-15
Visualizzazione di eventi di stack in base al token richiesta client	14 luglio 2017	Nella console, le operazioni di stack mostrano il token di richiesta client nella scheda Events (Eventi). A tutti gli eventi che vengono attivati da una determinata operazione di stack viene assegnato lo stesso token di richiesta client, che puoi utilizzare per monitorare le operazioni. Per ulteriori informazioni, consulta Visualizzazione dei dati e delle risorse CloudFormation dello stack su AWS Management Console e StackEvent nel riferimento AWS CloudFormation API.	2010-05-15
Utilizzo dei collegamenti di creazione rapida degli stack	14 luglio 2017	Utilizza i collegamenti di creazione rapida per rendere operativi gli stack in modo rapido e semplice. Puoi specificare l'URL del modello, il nome dello stack e i parametri del modello per precompilare una singola pagina Create Stack Wizard (Creazione guidata di stack). Per ulteriori informazioni, consulta Creazione di collegamenti di creazione rapida per gli stack .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse per il supporto AWS Database Migration Service	12 luglio 2017	AWS::DMS::Certificate Utilizza la <code>AWS::DMS::Certificate</code> risorsa per creare un certificato SSL che crittografa le connessioni tra gli AWS DMS endpoint e l'istanza di replica. AWS::DMS::Endpoint Utilizza la risorsa <code>AWS::DMS::Endpoint</code> per creare un endpoint AWS DMS . AWS::DMS::EventSubscription Usa la <code>AWS::DMS::EventSubscription</code> risorsa per ricevere notifiche di AWS DMS eventi tramite Amazon Simple Notification Service. AWS::DMS::ReplicationInstance Usa la <code>AWS::DMS::ReplicationInstance</code> risorsa per creare un'istanza di AWS DMS replica. AWS::DMS::ReplicationSubnetGroup Utilizzate la <code>AWS::DMS::ReplicationSubnetGroup</code> risorsa per creare un sottogruppo di AWS DMS replica. AWS::DMS::ReplicationTask Utilizzate la <code>AWS::DMS::ReplicationTask</code> risorsa per creare un'attività di AWS DMS replica.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	5 luglio 2017	AWS::CloudWatch::Dashboard Usa la <code>AWS::CloudWatch::Dashboard</code> risorsa per specificare una CloudWatch dashboard personalizzata per la tua CloudWatch console. AWS::ApiGateway::DomainName Utilizza la risorsa <code>AWS::ApiGateway::DomainName</code> per specificare un URL personalizzato breve per l'API distribuita in Amazon API Gateway. AWS::EC2::EgressOnlyInternetGateway Utilizza la risorsa <code>AWS::EC2::EgressOnlyInternetGateway</code> per creare un gateway Internet di sola uscita per il VPC. InstanceFleetConfig Utilizza la risorsa <code>InstanceFleetConfig</code> per configurare un parco istanze Spot per un cluster Amazon EMR.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	5 luglio 2017	AWS::ApiGateway::RestApi Utilizza la proprietà <code>BinaryMediaTypes</code> per specificare i tipi di file multimediali binari supportati. AWS::ApplicationAutoScaling::ScalingPolicy Utilizza la proprietà <code>TargetTrackingScalingPolicyConfiguration</code> per specificare una configurazione di policy di dimensionamento di monitoraggio dei target. AWS::CloudTrail::Trail Utilizzate la <code>TrailName</code> proprietà per specificare un nome personalizzato per una AWS CloudTrail risorsa. Utilizza la proprietà <code>Tags</code> per specificare i tag delle risorse. AWS::CodeDeploy::DeploymentGroup Utilizza la proprietà <code>AlarmConfiguration</code> per configurare allarmi per il gruppo di distribuzione. Utilizza la proprietà <code>TriggerConfigurations</code> per configurare trigger di notifica per il gruppo di distribuzione. AWS::EMR::Cluster Utilizza la <code>CoreInstanceFleet</code> proprietà e la <code>MasterInstanceFleet</code> proprietà nel tipo di JobFlowInstancesConfig proprietà per configurare la flotta di istanze Spot per un cluster Amazon EMR.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::DynamoDB::Table Utilizza la proprietà <code>TimeToLiveSpecification</code> per specificare le impostazioni Time To Live (TTL) per una tabella Amazon DynamoDB. Utilizza la proprietà <code>Tags</code> per specificare i tag delle risorse per una tabella DynamoDB. AWS::EC2::Instance La proprietà <code>IamInstanceProfile</code> ora supporta gli aggiornamenti <code>No interruption</code> . AWS::EC2::Route Utilizza la proprietà <code>EgressOnlyInternetGatewayId</code> per specificare un gateway Internet di sola uscita per un percorso. EC2 AWS::Kinesis::Stream Utilizza la proprietà <code>RetentionPeriodHours</code> per specificare il numero di ore in cui i record dei dati archiviati negli shard rimangono accessibili. AWS::RDS::DBCluster Utilizza la proprietà <code>ReplicationSourceIdentifier</code> per creare un cluster di database come replica di lettura di un altro cluster di database o di un'istanza database MySQL Amazon RDS. AWS::Redshift::Cluster Utilizza la proprietà <code>LoggingProperties</code> per creare file di log di audit e archivarli in Amazon S3.	

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	6 giugno 2017	AWS::EMR::SecurityConfiguration È possibile utilizzare la risorsa <code>AWS::EMR::SecurityConfiguration</code> per creare una configurazione di sicurezza, che viene archiviata nel servizio e può essere specificata al momento della creazione di un cluster.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	6 giugno 2017	AWS::AutoScaling::LifecycleHook Le proprietà <code>NotificationTargetARN</code> e <code>RoleARN</code> sono ora opzionali. AWS::CloudWatch::Alarm Ora puoi utilizzare le proprietà <code>EvaluateLowSampleCountPercentile</code>, <code>ExtendedStatistic</code> e <code>TreatMissingData</code> durante la creazione di risorse <code>AWS::CloudWatch::Alarm</code>. AWS::EC2::SpotFleet CloudFormation supporta modifiche mutabili alle proprietà del parco veicoli Spot. Le seguenti proprietà della proprietà <code>SpotFleetRequestConfigData</code> supportano gli aggiornamenti <code>Replacement</code>: • <code>AllocationStrategy</code> • <code>IamFleetRole</code> • <code>LaunchSpecifications</code> • <code>SpotPrice</code> • <code>TerminateInstancesWithExpiration</code> • <code>ValidFrom</code> • <code>ValidUntil</code> Le seguenti proprietà della proprietà <code>SpotFleetRequestConfigData</code> supportano gli aggiornamenti <code>No interruption</code>: • <code>ExcessCapacityTerminationPolicy</code> • <code>TargetCapacity</code>	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::EMR::InstanceGroupConfig CloudFormation ora supporta i gruppi di istanze di attività Auto Scaling for Amazon EMR. AWS::Events::Rule La proprietà RoleArn è obsoleta sulla risorsa Rule. Utilizza la proprietà RoleArn sul tipo di proprietà Target per specificare il ruolo IAM da utilizzare per un target. AWS::Kinesis::Stream La proprietà ShardCount ora supporta gli aggiornamenti No interruption . AWS::Lambda::Function Utilizza la proprietà TracingConfig per configurare le impostazioni di tracciamento per le funzioni Lambda. AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, e AWS::Redshift::ClusterSubnetGroup Utilizza la proprietà Tags per specificare i tag delle risorse. AWS::RDS::DBCluster Aggiunto l'attributo ReadEndpoint.Address alla funzione Fn::GetAtt intrinseca. AWS::S3::Bucket Aggiunto l'attributo Arn alla funzione Fn::GetAtt intrinseca.	

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	11 maggio 2017	Le seguenti nuove risorse supportano l'utilizzo AWS WAF con Elastic Load Balancing (ELB) Application Load Balancing (ELB). AWS::WAFRegional::ByteMatchSet Utilizza la risorsa <code>AWS::WAFRegional::ByteMatchSet</code> per identificare una parte di una richiesta Web che desideri esaminare. AWS::WAFRegional::IPSet Utilizza la risorsa <code>AWS::WAFRegional::IPSet</code> per specificare quali richieste Web consentire o bloccare in base agli indirizzi IP da cui le richieste sono originate. AWS::WAFRegional::Rule Utilizza la risorsa <code>AWS::WAFRegional::Rule</code> per specificare una combinazione di oggetti <code>IPSet</code>, <code>ByteMatchSet</code> e <code>SqlInjectionMatchSet</code> che identificano le richieste Web da consentire, bloccare o contare. AWS::WAFRegional::SizeConstraintSet Utilizza la risorsa <code>AWS::WAFRegional::SizeConstraintSet</code> per specificare un vincolo di dimensione utilizzato per verificare le dimensioni di una richiesta Web e quali parti della richiesta controllare. AWS::WAFRegional::SqlInjectionMatchSet Utilizza la risorsa <code>AWS::WAFRegional::SqlInjectionMatchSet</code> per consentire, bloccare o contare le richieste che contengono codice	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		SQL dannoso in una parte specifica delle richieste Web. AWS::WAFRegional::WebACL Utilizza la risorsa <code>AWS::WAFRegional::WebACL</code> per identificare le richieste Web che desideri consentire, bloccare o contare. AWS::WAFRegional::WebACLAssociation Utilizza la risorsa <code>AWS::WAFRegional::WebACLAssociation</code> per associare un gruppo di controllo degli accessi (ACL) Web a una risorsa. AWS::WAFRegional::XssMatchSet Utilizza la risorsa <code>AWS::WAFRegional::XssMatchSet</code> per specificare le parti delle richieste Web che desideri far esaminare da AWS WAF per individuare attacchi di scripting intersito e il nome dell'intestazione da esaminare.	

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	28 aprile 2017	AWS::Cognito::IdentityPool Utilizza la risorsa <code>AWS::Cognito::IdentityPool</code> per creare un pool di identità Amazon Cognito. AWS::Cognito::IdentityPoolRoleAttachment Utilizza la risorsa <code>AWS::Cognito::IdentityPoolRoleAttachment</code> per gestire la configurazione del ruolo per un pool di identità Amazon Cognito. AWS::Cognito::UserPool Utilizza la risorsa <code>AWS::Cognito::UserPool</code> per creare un pool di utenti Amazon Cognito. AWS::Cognito::UserPoolClient Utilizza la risorsa <code>AWS::Cognito::UserPoolClient</code> per creare un client del pool di utenti. AWS::Cognito::UserPoolGroup Utilizza la risorsa <code>AWS::Cognito::UserPoolGroup</code> per creare un gruppo di utenti in un pool di utenti Amazon Cognito. AWS::Cognito::UserPoolUser Utilizza la risorsa <code>AWS::Cognito::UserPoolUser</code> per creare un utente di un pool di utenti Amazon Cognito. AWS::Cognito::UserPoolUserToGroupAttachment Utilizza la risorsa <code>AWS::Cognito::UserPoolUserToGroupAttachment</code> per collegare	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		un utente a un gruppo di pool di utenti Amazon Cognito.	

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	28 aprile 2017	SourceDetails Utilizza la proprietà secondaria <code>MaximumExecutionFrequency</code> della risorsa <code>AWS::Config::ConfigRule</code> per eseguire valutazioni per una regola personalizzata utilizzando un trigger periodico. AWS::EC2::Volume Ora sono supportati i volumi elastici per Amazon Elastic Block Store (Amazon EBS) in CloudFormation CloudFormation. Sono ora supportati gli aggiornamenti <code>No interruption</code> su tre proprietà: <code>VolumeType</code>, <code>Size</code> e <code>Iops</code>. AWS::EC2::SecurityGroup Usa la <code>GroupName</code> proprietà per specificare un nome per il tuo gruppo EC2 di sicurezza Amazon. AWS::ECS::Service Sono state introdotte tre nuove proprietà per <code>AWS::ECS::Service</code>: <code>PlacementConstraints</code>, <code>PlacementStrategies</code> e <code>ServiceName</code>. AWS::ECS::TaskDefinition Utilizza la proprietà <code>PlacementConstraints</code> per definire i vincoli di collocazione per le attività nel servizio. AWS::ElastiCache::ReplicationGroup Aggiunto l'attributo <code>ConfigurationEndpoint.Address</code> e l'attributo <code>ConfigurationEndpoint.Port</code> alla funzione <code>Fn::GetAtt</code> intrinseca.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		<u>AWS::ElasticLoadBalancingV2::LoadBalancer</u> Utilizza la proprietà <code>IpAddressType</code> per specificare il tipo di indirizzi IP utilizzati dalle sottoreti del load balancer. <u>AWS::EMR::Cluster</u> CloudFormation ora supporta Auto Scaling per i cluster Amazon EMR. <u>AWS::IAM::ManagedPolicy</u> Utilizza la proprietà <code>ManagedPolicyName</code> per specificare un nome personalizzato per la policy gestita IAM. <u>AWS::Lambda::Function</u> Utilizza la proprietà <code>Tags</code> per aggiungere tag alla funzione Lambda. <u>AWS::OpsWorks::Instance</u> Aggiunti i seguenti attributi alla funzione <code>Fn::GetAtt</code> intrinseca: <code>AvailabilityZone</code>, <code>PrivateDnsName</code>, <code>PrivateIp</code> e <code>PublicDnsName</code>. <u>AWS::OpsWorks::UserProfile</u> Utilizza la proprietà <code>SshUsername</code> per specificare il nome SSH di un utente. Aggiunto l'attributo <code>SshUsername</code> alla funzione <code>Fn::GetAtt</code> intrinseca. <u>AWS::Redshift::Cluster</u> Utilizza la <code>IamRoles</code> proprietà per fornire un elenco di uno o più AWS Identity and Access Management	

Modifica	Data di rilascio	Descrizione	Versione API
		ruoli che il cluster Amazon Redshift può utilizzare per accedere ad altri AWS servizi.	
Modifica i modelli in YAML e JSON utilizzando Designer AWS CloudFormation	6 Aprile 2017	Quando crei CloudFormation modelli utilizzando Designer, ora puoi modificare il modello sia in YAML che in JSON nell'editor integrato. Puoi anche convertire i modelli JSON in YAML e viceversa, a seconda del linguaggio di creazione di modelli che preferisci. Per ulteriori informazioni, consulta What Is Designer? CloudFormation .	2010-05-15
Nuova risorsa	6 Aprile 2017	AWS::SSM::Parameter Utilizza la risorsa <code>AWS::SSM::Parameter</code> per creare un parametro SSM in Archivio parametri.	2010-05-15
Trasformazione <code>AWS::Include</code>	28 marzo 2017	Utilizza la trasformazione <code>AWS::Include</code> per fare riferimento a frammenti riutilizzabili archiviati in un bucket Amazon S3. Per ulteriori informazioni, consulta Trasformazione AWS::Include .	2010-05-15
Peering del Amazon VPC con un altro account	28 marzo 2017	Ora puoi utilizzarlo CloudFormation per peerizzare il tuo Amazon VPC con un VPC in un altro account. AWS Per ulteriori informazioni, consulta Peer with an Amazon VPC in AWS un altro account.	2010-05-15
Nuova risorsa	28 marzo 2017	AWS::ApiGateway::UsagePlanKey Utilizza la risorsa <code>AWS::ApiGateway::UsagePlanKey</code> per associare una chiave del piano di utilizzo e determinare a quali utenti si applica il piano di utilizzo.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	28 marzo 2017	AWS::EC2::VPCPeeringConnection Utilizza la proprietà <code>PeerOwnerId</code> e la proprietà <code>PeerRoleArn</code> per eseguire il peering con un VPC in un altro account AWS . Per ulteriori informazioni, consulta Peer with an Amazon VPC in AWS un altro account. AWS::IAM::InstanceProfile Utilizza la proprietà <code>InstanceProfileName</code> per configurare un profilo dell'istanza. AWS::Lambda::Function Utilizza la proprietà <code>DeadLetterConfig</code> per configurare il modo in cui AWS Lambda gestisce gli eventi che non è in grado di elaborare. Node.js v0.10 non è più supportato per la proprietà <code>Runtime</code>. AWS::Route53::HealthCheck Sono stati introdotti sette nuovi tipi di proprietà secondarie delle risorse per la proprietà HealthCheckConfig <code>HealthCheckConfig</code> : <code>AlarmIdentifier</code> , <code>ChildHealthChecks</code> , <code>EnableSNI</code> , <code>HealthThreshold</code> , <code>InsufficientDataHealthStatus</code> , <code>Inverted</code> e <code>MeasureLatency</code> . AWS::SQS::Queue Usa le proprietà <code>FifoQueue</code> <code>ContentBasedDeduplication</code> and per creare code First-In-First-Out (FIFO) di Amazon Simple Queue Service.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::S3::Bucket Ora puoi specificare i nomi di IPv6 dominio per i tuoi bucket Amazon S3.	
Nuove risorse	10 febbraio 2017	AWS::StepFunctions::Activity Usa la <code>AWS::StepFunctions::Activity</code> risorsa per creare un' AWS Step Functions attività. AWS::StepFunctions::StateMachine Utilizza la risorsa <code>AWS::StepFunctions::StateMachine</code> per creare una macchina a stati Step Functions.	2010-05-15
Nuova funzione intrinseca	17 gennaio 2017	Utilizza la funzione <code>Fn::Split</code> per dividere una stringa in un elenco di valori di stringa. Per ulteriori informazioni, consulta Fn::Split .	2010-05-15
Supporto della console per la descrizione delle importazioni	17 gennaio 2017	Usa la CloudFormation console per vedere tutti gli stack che importano un valore di output esportato. Per ulteriori informazioni, consulta Creazione di elenchi di stack che importano un valore di output esportato .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	17 gennaio 2017	AWS::AutoScaling::AutoScalingGroup La proprietà <code>LoadBalancerNames</code> può essere aggiornata senza la sostituzione del gruppo con dimensionamento automatico. AWS::ECS::TaskDefinition Aggiunte le proprietà <code>NetworkMode</code> e <code>MemoryReservation</code>. AWS::RDS::DBCluster CloudFormation supporta gli aggiornamenti della proprietà. <code>Tags</code> AWS::RDS::DBInstance Aggiunta la proprietà <code>Timezone</code>. FirehoseAction Aggiunta la proprietà <code>Separator</code>. AWS::OpsWorks::Instance Aggiunto l'attributo <code>PublicIp</code> per la funzione <code>Fn::GetAtt</code> intrinseca.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	01 dicembre 2016	AWS::CodeBuild::Project Usa la <code>AWS::CodeBuild::Project</code> risorsa per creare un AWS CodeBuild progetto che definisca la modalità di CodeBuild compilazione del codice sorgente. AWS::SSM::Association Usa la <code>AWS::SSM::Association</code> risorsa per associare un documento Amazon EC2 Systems Manager alle EC2 istanze. AWS::EC2::SubnetCidrBlock Usa la <code>AWS::EC2::SubnetCidrBlock</code> risorsa per associare un singolo blocco IPv6 CIDR a una sottorete Amazon VPC. AWS::EC2::VPCCidrBlock Usa la <code>AWS::EC2::VPCCidrBlock</code> risorsa per associare un singolo blocco IPv6 CIDR fornito da Amazon a un Amazon VPC.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate per il supporto IPv6	01 dicembre 2016	AWS::EC2::Instance Aggiunte le proprietà <code>Ipv6AddressCount</code> e <code>Ipv6Addresses</code> . AWS::EC2::NetworkAclEntry Aggiunta la proprietà <code>Ipv6CidrBlock</code> . AWS::EC2::NetworkInterface Aggiunte le proprietà <code>Ipv6AddressCount</code> e <code>Ipv6Addresses</code> . AWS::EC2::Route Aggiunta la proprietà <code>DestinationIpv6CidrBlock</code> . AWS::EC2::SecurityGroupEgress Aggiunta la proprietà <code>CidrIpv6</code>. AWS::EC2::SecurityGroupIngress Aggiunta la proprietà <code>CidrIpv6</code>. AWS::EC2::SpotFleet Aggiunte le proprietà <code>Ipv6AddressCount</code> e <code>Ipv6Addresses</code> per le interfacce di rete nelle specifiche di avvio. AWS::EC2::Subnet Aggiunto l'attributo <code>Ipv6CidrBlocks</code> per la funzione <code>Fn::GetAtt</code> . AWS::EC2::VPC Aggiunto l'attributo <code>Ipv6CidrBlocks</code> per la funzione <code>Fn::GetAtt</code> .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::SSM::Document Aggiunta la proprietà DocumentType .	
Specifica delle risorse	22 Novembre 2016	Utilizza le specifiche CloudFormation delle risorse per creare strumenti che ti aiutino a creare CloudFormation modelli. La specifica è un file di testo in formato JSON leggibile dal computer. Per ulteriori informazioni, vedere CloudFormation Resource Specification .	2010-05-15
Nuove risorse	22 Novembre 2016	AWS::OpsWorks::UserProfile Usa la <code>AWS::OpsWorks::UserProfile</code> risorsa per configurare l'accesso SSH per gli utenti che richiedono l'accesso alle istanze in uno AWS OpsWorks stack. AWS::OpsWorks::Volume Usa la <code>AWS::OpsWorks::Volume</code> risorsa per registrare un volume Amazon Elastic Block Store con uno AWS OpsWorks stack.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	22 Novembre 2016	AWS::OpsWorks::App Aggiunta la proprietà <code>DataSources</code> . AWS::OpsWorks::Instance Aggiunte le proprietà <code>BlockDeviceMappings</code> , <code>AgentVersion</code> , <code>ElasticIps</code> , <code>Hostname</code> , <code>Tenancy</code> e <code>Volumes</code>. AWS::OpsWorks::Layer Aggiunte le proprietà <code>CustomJson</code> e <code>VolumeConfigurations</code> . AWS::OpsWorks::Stack Aggiunte le proprietà <code>ElasticIps</code> , <code>EcsClusterArn</code> , <code>RdsDbInstances</code> , <code>CloneAppIds</code> , <code>ClonePermissions</code> e <code>SourceStackId</code> . AWS::RDS::DBInstance Aggiunta la proprietà <code>CopyTagsToSnapshot</code> .	2010-05-15
Elenco importazioni	22 Novembre 2016	Elenca le importazioni di un valore di output esportato per tenere traccia CloudFormation degli stack che lo stanno importando. Per ulteriori informazioni, consulta Creazione di elenchi di stack che importano un valore di output esportato.	2010-05-15
Trasformazioni	17 Novembre 2016	Specificare il AWS Serverless Application Model (AWS SAM) CloudFormation utilizzato per elaborare la sintassi AWS SAM per le applicazioni serverless. Per ulteriori informazioni, consulta Trasformazione .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova risorsa	17 Novembre 2016	AWS::SNS::Subscription Utilizza la risorsa <code>AWS::SNS::Subscription</code> per sottoscrivere un endpoint a un argomento Amazon Simple Notification Service.	2010-05-15
Risorsa aggiornata	17 Novembre 2016	AWS::Lambda::Function Utilizzate la <code>Environment</code> proprietà per specificare coppie chiave-valore (variabili di ambiente) a cui la funzione può accedere. AWS Lambda Utilizzate la <code>KmsKeyArn</code> proprietà per specificare una chiave KMS da utilizzare per crittografare e AWS Lambda decrittografare le variabili di ambiente.	2010-05-15
Nuovi comandi CLI	17 Novembre 2016	Caricamento di artefatti locali in un bucket S3 Usa il package comando per caricare gli artefatti locali a cui si fa riferimento in un modello in un bucket S3. CloudFormation Distribuzione rapida dei modelli con trasformazioni Utilizza il comando <code>deploy</code> per combinare le operazioni di creazione ed esecuzione di gruppi di modifiche in un unico comando. Questo comando è utile per creare o aggiornare in modo rapido stack che contengono trasformazioni.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorsa aggiornata	03 Novembre 2016	AWS::CloudFront::Distribution Per la DistributionConfig proprietà, utilizza la <code>HttpVersion</code> proprietà per specificare la versione HTTP più recente che gli spettatori possono utilizzare per comunicare con Amazon CloudFront. Per la ForwardedValues proprietà, utilizza la <code>QueryStringCacheKeys</code> proprietà per specificare i parametri della stringa di query da utilizzare per determinare il contenuto da memorizzare nella cache. CloudFront	2010-05-15
Elenco esportazioni stack	03 Novembre 2016	Utilizza la CloudFormation console, l'API o AWS CLI per visualizzare un elenco di tutti i valori di output esportati per una regione. Per ulteriori informazioni, consulta Esportazione dei valori di output dello stack .	2010-05-15
Distribuzione continua with stack	03 Novembre 2016	Utilizzalo AWS CodePipeline per creare flussi di lavoro di distribuzione continua con CloudFormation stack. Per ulteriori informazioni, consulta Continuous Delivery with CodePipeline	2010-05-15
Ignorare risorse durante il rollback	03 Novembre 2016	Se disponi di uno stack nello stato <code>UPDATE_ROLLBACK_FAILED</code> , utilizza il parametro <code>ResourcesToSkip</code> per l'operazione <code>ContinueUpdateRollback</code> per ignorare risorse di cui CloudFormation non è in grado di effettuare il rollback. Per ulteriori informazioni, consulta la sezione di risoluzione dei problemi in Impossibile eseguire il rollback dell'aggiornamento .	2010-05-15
Miglioramento dei set di modifiche	03 Novembre 2016	Puoi creare un nuovo stack utilizzando un set di modifiche .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorsa aggiornata	12 Ottobre 2016	AWS::ElastiCache::CacheCluster Aggiorna la proprietà <code>CacheNodeType</code> senza sostituire il cluster. AWS::ElastiCache::ReplicationGroup Puoi creare un gruppo di repliche Redis (modalità cluster abilitata) che può contenere più gruppi di nodi (shard), ognuno con un cluster primario e repliche di lettura. AWS::ElastiCache::SubnetGroup Utilizza la <code>CacheSubnetGroupName</code> proprietà per specificare un nome per un ElastiCache sottogruppo di Amazon.	2010-05-15
Nuove risorse	06 Ottobre 2016	AWS::ApiGateway::UsagePlan Utilizza la <code>AWS::ApiGateway::UsagePlan</code> risorsa per specificare un piano di utilizzo per Amazon API Gateway APIs distribuito. AWS::CodeCommit::Repository Usa la <code>AWS::CodeCommit::Repository</code> risorsa per creare un CodeCommit repository ospitato da Amazon Web Services.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	06 Ottobre 2016	AWS::ApiGateway::Authorizer Utilizza la proprietà <code>ProviderARNs</code> per utilizzare pool di utenti Amazon Cognito come autorizzazioni API Amazon API Gateway. AWS::ApiGateway::Deployment La proprietà <code>StageName</code> non è più richiesta. AWS::ElasticLoadBalancingV2::TargetGroup Per la <code>GetAtt</code> funzione, utilizza l'<code>LoadBalancerArns</code> attributo per recuperare gli Amazon Resource Names (ARNs) dei sistemi di bilanciamento del carico che indirizzano il traffico verso il gruppo di destinazione. AWS::RDS::DBInstance Scegli le proprietà <code>Domain</code> e <code>DomainIAMRoleName</code> per utilizzare l'autenticazione Windows quando gli utenti si connettono all'istanza database RDS. AWS::EC2::SecurityGroupEgress Utilizza la <code>DestinationPrefixListId</code> proprietà per specificare il prefisso del AWS servizio di un endpoint Amazon VPC.	2010-05-15
Miglioramento dei riferimenti tra stack	06 Ottobre 2016	Utilizza le funzioni intrinseche per personalizzare il valore Name di un'esportazione o per fare riferimento a un valore nella funzione ImportValue .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
CloudFormation ruolo di servizio	26 settembre 2016	Utilizza un ruolo di servizio AWS Identity and Access Management (IAM) per le operazioni di CloudFormation stack. CloudFormation utilizza le credenziali del ruolo per effettuare chiamate allo stack delle risorse per tuo conto. Per ulteriori informazioni, consulta AWS CloudFormation service role.	2010-05-15
Nuova caratteristica	19 settembre 2016	Puoi utilizzare il campo di output <code>Export</code> e la funzione <code>Fn::ImportValue</code> intrinseca in modo che uno stack faccia riferimento agli output delle risorse in un altro stack. Per ulteriori informazioni, vedere Output e procedura dettagliata: fare riferimento a Resource Output in Another Stack . <code>Fn::ImportValue</code> CloudFormation	2010-05-15
Supporto per YAML	19 settembre 2016	Puoi usare il formato YAML per creare modelli. CloudFormation YAML consente inoltre di aggiungere, ad esempio, commenti a tuoi modelli o di utilizzare il formato breve per le funzioni intrinseche. Per ulteriori informazioni, consulta il formato CloudFormation del modello .	2010-05-15
Nuova funzione intrinseca	19 settembre 2016	Utilizza la funzione <code>Fn::Sub</code> per sostituire le variabili in una stringa di input con i valori che specifichi. Per ulteriori informazioni, consulta Fn::Sub .	2010-05-15
Nuove risorse	19 settembre 2016	AWS::KMS::Alias Utilizza la risorsa <code>AWS::KMS::Alias</code> per creare un alias per una AWS KMS key.	

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	19 settembre 2016	AWS::EC2::SpotFleet Per la proprietà <code>LaunchSpecifications</code> , utilizza la proprietà <code>SpotPrice</code> per specificare un prezzo di offerta per un determinato tipo di istanza. AWS::ECS::Cluster Utilizza la proprietà <code>ClusterName</code> per specificare un nome per un cluster Amazon Elastic Container Service. AWS::ECS::TaskDefinition Utilizza la proprietà <code>TaskRoleArn</code> proprietà per specificare un AWS Identity and Access Management ruolo utilizzato dai contenitori Amazon Elastic Container Service per effettuare AWS chiamate per tuo conto. Utilizza la proprietà <code>Family</code> per registrare una definizione dell'attività a una famiglia specifica. AWS::Elasticsearch::Domain Utilizza la proprietà <code>ElasticsearchVersion</code> per specificare la versione di Elasticsearch da utilizzare.	2010-05-15
Nuove risorse	11 agosto 2016	Utilizza le seguenti risorse Elastic Load Balancing Application Load Balancer per distribuire il traffico delle applicazioni in entrata su più destinazioni, ad esempio istanze, in più EC2 zone di disponibilità: • AWS::ElasticLoadBalancingV2::Listener • AWS::ElasticLoadBalancingV2::ListenerRule • AWS::ElasticLoadBalancingV2::LoadBalancer • AWS::ElasticLoadBalancingV2::TargetGroup	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorsa aggiornata	11 agosto 2016	AWS::AutoScaling::AutoScalingGroup Utilizza la proprietà <code>TargetGroupARNs</code> per associare il gruppo con dimensionamento automatico a uno o più gruppi di destinazione Application Load Balancer. AWS::ECS::Service Per la proprietà di caricamento <code>LoadBalancers</code>, utilizza la proprietà <code>TargetGroupArn</code> per associare un servizio Amazon Elastic Container Service a un gruppo target Application Load Balancer.	2010-05-15
Nuove risorse	09 agosto 2016	CloudFormation ha aggiunto le seguenti risorse: AWS::ApplicationAutoScaling::ScalableTarget e AWS::ApplicationAutoScaling::ScalingPolicy Utilizza una policy di dimensionamento Application Auto Scaling per definire quando e come una risorsa target esegue il dimensionamento. AWS::CertificateManager::Certificate Fornisci un AWS Certificate Manager certificato che puoi utilizzare con altri AWS servizi per abilitare connessioni sicure.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	09 agosto 2016	CloudFormation ha aggiornato le seguenti risorse: AWS::CloudFront::Distribution Per la proprietà della configurazione di distribuzione <code>ViewerCertificate</code>, puoi specificare un certificato AWS Certificate Manager. Per la proprietà della configurazione di distribuzione <code>Origin</code>, puoi specificare intestazioni personalizzate e protocolli SSL per origini personalizzate. AWS::EFS::FileSystem Puoi specificare la modalità prestazioni per un file system Amazon Elastic File System.	2010-05-15
Nuove risorse	20 luglio 2016	AWS IoT AWS IoT Da utilizzare per dichiarare una AWS IoT politica, un certificato X.509, un'associazione tra una politica e un principale (un certificato X.509 o altra credenziale), un AWS IoT oggetto, un'associazione tra un principale e un oggetto o una regola. AWS IoT • AWS::IoT::Certificate • AWS::IoT::Policy • AWS::IoT::PolicyPrincipalAttachment • AWS::IoT::Thing • AWS::IoT::ThingPrincipalAttachment • AWS::IoT::TopicRule	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	20 luglio 2016	CloudFormation ha aggiornato le seguenti risorse: AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User Utilizza le proprietà del nome per specificare un nome personalizzato per le risorse AWS Identity and Access Management (IAM). AWS::ApiGateway::Method Per la proprietà <code>Integration</code>, puoi utilizzare la proprietà <code>PassthroughBehavior</code> per specificare quando Amazon API Gateway passa le richieste al back-end target. AWS::ApiGateway::Model e AWS::ApiGateway::RestApi Puoi specificare oggetti JSON per le proprietà <code>Schema</code> e <code>Body</code>.	2010-05-15
Gruppo Auto Scaling UpdatePolicy	9 giugno 2016	Per l'attributo <code>UpdatePolicy</code>, utilizza la proprietà <code>AutoScalingReplacingUpdate</code> per specificare se un gruppo con dimensionamento automatico e le istanze in esso contenute vengono sostituiti quando aggiorni il gruppo con dimensionamento automatico. Durante una sostituzione, CloudFormation mantiene il vecchio gruppo Auto Scaling fino a quando non crea correttamente quello nuovo, in modo CloudFormation che possa tornare al vecchio gruppo Auto Scaling se l'aggiornamento fallisce. Per ulteriori informazioni, consulta UpdatePolicy Attribute.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova risorsa	9 giugno 2016	CloudFormation ha aggiunto le seguenti risorse: AWS::EC2::FlowLog Crea un log di flusso Amazon Elastic Compute Cloud che acquisisce il traffico IP per un'interfaccia di rete, una sottorete o un VPC specificati. AWS::KinesisFirehose::DeliveryStream Crea un flusso di distribuzione che fornisce dati di streaming in tempo reale verso una destinazione, come Amazon Simple Storage Service, Amazon Redshift o Amazon OpenSearch Service.	2010-05-15
Risorse aggiornate	9 giugno 2016	CloudFormation ha aggiornato le seguenti risorse: AWS::Kinesis::Stream Utilizza la proprietà Name per specificare un nome per un flusso Amazon Kinesis. AWS::Lambda::Function Per la proprietà Code, puoi utilizzare la proprietà ZipFile e il modulo di risposta cfn per gli ambienti di runtime nodejs4.3 . AWS::SNS::Topic CloudFormation aggiornamenti abilitati per la risorsa tematica Amazon Simple Notification Service.	2010-05-15
Nuova risorsa	25 Aprile 2016	Usa la AWS::EC2::Hostrisorsa per allocare un server fisico completamente dedicato per il lancio EC2 delle istanze.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	25 Aprile 2016	AWS::EC2::Instance Utilizza le proprietà <code>Affinity</code> e <code>HostId</code> per avviare istanze su un host dedicato Amazon Elastic Compute Cloud. AWS::ECS::Service Utilizza la proprietà <code>DeploymentConfiguration</code> per configurare il modo in cui numerose attività possono essere eseguite durante una distribuzione. AWS::ECS::TaskDefinition CloudFormation ha aggiunto il supporto per ulteriori proprietà di definizione dei contenitori Amazon Elastic Container Service. AWS::GameLift::Fleet Utilizza le proprietà <code>MinSize</code> e <code>MaxSize</code> per specificare il numero massimo e minimo di EC2 istanze consentite nella tua flotta di GameLift server Amazon. AWS::Lambda::Function Usa la proprietà <code>FunctionName</code> per specificare un nome per la tua AWS Lambda funzione. Puoi anche utilizzare Python 2.7 per specificare una funzione inline.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	18 Aprile 2016	Amazon API Gateway Usa le risorse di Amazon API Gateway per pubblicare, gestire e monitorare API su qualsiasi scala. Puoi fare in modo API che i clienti possano chiamare per accedere ai tuoi servizi di back-end, come applicazioni che eseguono EC2 istanze o codice in esecuzione su AWS Lambda • AWS::ApiGateway::Account • AWS::ApiGateway::ApiKey • AWS::ApiGateway::Authorizer • AWS::ApiGateway::BasePathMapping • AWS::ApiGateway::ClientCertificate • AWS::ApiGateway::Deployment • AWS::ApiGateway::Method • AWS::ApiGateway::Model • AWS::ApiGateway::Resource • AWS::ApiGateway::RestApi • AWS::ApiGateway::Stage AWS::Events::Rule Crea una regola Amazon CloudWatch Events che monitora le modifiche alle AWS risorse nel tuo account (eventi). Se un evento in arrivo soddisfa le condizioni descritte nella regola, Amazon CloudWatch Events invia messaggi e attiva gli obiettivi specificati, come AWS Lambda funzioni o argomenti di Amazon Simple Notification Service.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::WAF::SizeConstraintSet e AWS::WAF::XssMatchSet Utilizza le due AWS WAF regole per verificare la dimensione di una richiesta web o per prevenire attacchi di cross-site scripting.	
Nuove risorse	31 marzo 2016	Usa la AWS::Lambda::Alias risorsa per creare alias per le tue AWS Lambda funzioni e la AWS::Lambda::Version risorsa per creare versioni delle tue funzioni.	2010-05-15
Risorse aggiornate	31 marzo 2016	CloudFormation ha aggiornato le seguenti risorse: AWS::EMR::Cluster e AWS::EMR::InstanceGroupConfig Utilizza la proprietà <code>EbsConfiguration</code> per configurare volumi di storage Amazon Elastic Block Store per i cluster o i gruppi di istanze Amazon EMR. AWS::Lambda::Function Utilizza la proprietà <code>VpcConfig</code> per abilitare l'accesso da parte delle funzioni AWS Lambda alle risorse in un VPC. AWS::S3::Bucket Per le regole del ciclo di vita Amazon Simple Storage Service, puoi indicare più regole di transizione che specificano quando gli oggetti eseguono la transizione a una classe di storage specificata.	2010-05-15
Set di modifiche	29 marzo 2016	Prima di aggiornare stack, utilizza set di modifiche per visualizzare il modo in cui le modifiche potrebbero influenzare le tue risorse in esecuzione. Per ulteriori informazioni, consulta Aggiornamento degli stack utilizzando il set di modifiche.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	15 marzo 2016	Usa le AWS::GameLift::Fleet risorse AWS::GameLift::Alias AWS::GameLift::Build , e per distribuire server di gioco multiplayer in AWS.	2010-05-15
Nuove risorse	26 febbraio 2016	CloudFormation ha aggiunto le seguenti risorse: AWS::ECR::Repository Crea repository Amazon Elastic Container Registry in cui gli utenti possono inviare ed estrarre le immagini Docker. AWS::EC2::NatGateway Utilizza il gateway NAT (Network Address Translator) per consentire alle EC2 istanze di una sottorete privata di connettersi a Internet. AWS::Elasticsearch::Domain Crea domini Amazon OpenSearch Service che eseguono cluster OSS Elasticsearch legacy. AWS::EMR::Cluster, AWS::EMR::InstanceGroupConfig, AWS::EMR::Step Utilizza le risorse Amazon EMR per aiutarti ad analizzare ed elaborare grandi quantità di dati. Puoi creare cluster su cui eseguire processi.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Risorse aggiornate	26 febbraio 2016	CloudFormation ha aggiornato le seguenti risorse: AWS::CloudTrail::Trail Utilizzate la <code>IsMultiRegionTrail</code> proprietà per specificare se creare un AWS CloudTrail percorso nella regione in cui create una pila o in tutte le regioni. AWS::Config::ConfigurationRecorder Per il gruppo di registrazione, utilizza la proprietà <code>IncludeGlobalResourceTypes</code> per registrare tutti i tipi di risorse globali. AWS::RDS::DBCluster Utilizza le proprietà <code>KmsKeyId</code> e <code>StorageEncrypted</code> per crittografare le istanze database nel cluster.	2010-05-15
Conservazione di risorse	26 febbraio 2016	Per gli stack nello stato <code>DELETE_FAILED</code> , utilizza il parametro <code>RetainResources</code> per conservare risorse che CloudFormation non può eliminare. Per ulteriori informazioni, consulta Eliminare errori degli stack .	2010-05-15
Aggiornamento dei tag degli stack	26 febbraio 2016	Puoi aggiungere, modificare o rimuovere tag di stack quando aggiorni uno stack. Per ulteriori informazioni, consulta CloudFormation Stacks Updates.	2010-05-15
Continuazione del rollback di aggiornamenti non riusciti	25 gennaio 2016	Per uno stack nello stato <code>UPDATE_ROLLBACK_FAILED</code> , puoi continuare il rollback dell'aggiornamento per portare lo stack nello stato attivo. In questo modo, puoi ripristinare le impostazioni originali dello stack e provare nuovamente ad aggiornarlo. Per ulteriori informazioni, consulta Continuare il ripristino di un aggiornamento .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuovi modelli di esempio disponibili per la Regione Asia Pacifico (Seul).	7 gennaio 2016	La seguente raccolta di modelli di CloudFormation esempio si riferisce alla regione ap-northeast-2: • Soluzioni di esempio • Framework di applicazioni • Servizi Per ulteriori informazioni, vedere Lavorare con i modelli. CloudFormation	2010-05-15
Nuove risorse	28 dicembre 2015	CloudFormation ha aggiunto le seguenti risorse: AWS::DirectoryService::MicrosoftAD Usa la risorsa Microsoft Active Directory per creare una directory Microsoft Active Directory in AWS. AWS::Logs::Destination e AWS::Logs::LogStream Utilizza le risorse Amazon CloudWatch Logs per creare una destinazione per l'elaborazione in tempo reale dei dati di log o per creare flussi di log, rispettivamente. AWS::WAF::ByteMatchSet, AWS::WAF::IPSet, AWS::WAF::Rule, AWS::WAF::SqlInjectionMatchSet, e AWS::WAF::WebACL Usa le AWS WAF risorse per controllare e monitorare le richieste web ai tuoi contenuti.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamenti delle risorse	28 dicembre 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::CloudFront::Distribution Per la configurazione della distribuzione, utilizza la WebACLId proprietà per associare una lista di controllo degli accessi AWS WAF Web (ACL) a una CloudFront distribuzione Amazon. Per il comportamento cache e il comportamento cache predefinito, puoi specificare un valore Time To Live (TTL) predefinito e massimo. AWS::DynamoDB::Table Puoi creare, aggiornare o eliminare un indice secondario globale senza sostituire la tabella Amazon DynamoDB. AWS::S3::Bucket Utilizza la proprietà ReplicationConfiguration per specificare quali oggetti replicare e dove vengono archiviati. Utilizza le proprietà nella proprietà NotificationConfiguration per specificare i filtri in modo che Amazon Simple Storage Service invii notifiche per gli oggetti che specifichi.	2010-05-15
Raggruppamento e ordinamento dei parametri	3 dicembre 2015	Usa la chiave AWS::CloudFormation::Interface dei metadati per raggruppare e ordinare i parametri nella CloudFormation console quando gli utenti creano o aggiornano uno stack con il tuo modello.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamento dell'attributo della policy	3 dicembre 2015	Per un attributo di policy di aggiornamento Auto Scaling, utilizza la proprietà <code>MinSuccessfulInstancesPercent</code> per specificare la percentuale di istanze che devono segnalare un esito positivo affinché l'aggiornamento riesca.	2010-05-15
Nuove risorse	3 dicembre 2015	CloudFormation ha aggiunto le seguenti risorse: AWS::CodePipeline::Pipeline e AWS::CodePipeline::CustomActionType Utilizza le CodePipeline risorse per creare una pipeline che descriva come le modifiche al software passano attraverso un processo di rilascio. AWS::Config::ConfigurationRecorder, AWS::Config::DeliveryChannel e AWS::Config::ConfigRule Utilizza le AWS Config risorse per monitorare le modifiche alla configurazione di AWS risorse specifiche. AWS::KMS::Key Utilizzate la risorsa AWS Key Management Service (AWS KMS) per creare chiavi gestite dal cliente AWS KMS che gli utenti possano utilizzare per crittografare piccole quantità di dati. AWS::SSM::Document Usa Amazon EC2 Systems Manager per creare un documento che specifichi le configurazioni sull'istanza.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamento delle risorse	3 dicembre 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::AutoScaling::LaunchConfiguration Specifica se i volumi EBS sono crittografati. AWS::AutoScaling::ScalingPolicy Puoi utilizzare due diversi tipi di policy (scalabilità semplice e graduale) per specificare la scalabilità di un gruppo di Auto Scaling in caso di violazione di un allarme CloudWatch Amazon CloudWatch (). AWS::CloudTrail::Trail Usa le CloudWatch proprietà per inviare i log a un gruppo di log. CloudWatch È possibile aggiungere tag a un percorso e specificare AWS KMS key quello che si desidera utilizzare per crittografare i log. AWS::CodeDeploy::Application, AWS::CodeDeploy::DeploymentConfig e AWS::CodeDeploy::DeploymentGroup Utilizzate le <code>DeploymentGroupName</code> proprietà <code>ApplicationName</code> <code>DeploymentConfigName</code> , e per specificare nomi personalizzati per CodeDeploy le risorse. AWS::DynamoDB::Table Utilizza la proprietà <code>StreamSpecification</code> per specificare impostazioni per l'acquisizione di modifiche agli elementi archiviati in una tabella Amazon DynamoDB (DynamoDB).	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::EC2::Instance Utilizza la <code>SsmAssociations</code> proprietà per associare un documento Amazon EC2 Systems Manager a un'istanza. AWS::EC2::SpotFleet Utilizza la proprietà <code>AllocationStrategy</code> per specificare come allocare la capacità target tra pool Spot. Utilizza la proprietà <code>ExcessCapacityTerminationPolicy</code> per specificare in che modo le istanze vengono terminate se la capacità target è inferiore alle dimensioni del parco istanze Spot. AWS::Redshift::Cluster Utilizza la proprietà <code>KmsKeyId</code> per specificare una AWS KMS key per la crittografia dei dati in un cluster Amazon Redshift. AWS::WorkSpaces::Workspace Utilizza le proprietà di crittografia per crittografare i dati archiviati su volumi.	
Aggiornamento delle risorse	4 novembre 2015	Per quanto riguarda la AWS::EC2::Volume risorsa, utilizza la <code>AutoEnableIO</code> proprietà per riprendere automaticamente I/O le operazioni se i dati di un volume diventano incoerenti.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	1° ottobre 2015	CloudFormation ha aggiunto le seguenti risorse: AWS::CodeDeploy::Application, AWS::CodeDeploy::DeploymentGroup e AWS::CodeDeploy::DeploymentConfig Utilizza le CodeDeploy risorse per creare e applicare distribuzioni a EC2 o istanze locali. AWS::DirectoryService::SimpleAD Utilizza la risorsa Simple Active Directory per creare un Simple AD AWS Directory Service , ovvero una directory compatibile con Microsoft Active Directory. AWS::EC2::PlacementGroup Utilizza un gruppo di posizionamento per creare un cluster di istanze in una rete a bassa latenza. AWS::EC2::SpotFleet Utilizza un parco istanze Spot per avviare una raccolta di istanze Spot che eseguono attività interrompibili. AWS::Lambda::EventSourceMapping Utilizzate la risorsa di mappatura dell'origine degli eventi per specificare un flusso come origine di eventi per una funzione AWS Lambda (Lambda). AWS::Lambda::Permission Utilizza un'autorizzazione Lambda per aggiungere e una dichiarazione a una policy della funzione Lambda.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::Logs::SubscriptionFilter Utilizza il filtro sottoscrizioni per definire quali eventi di log vengono distribuiti al tuo flusso Kinesis. AWS::RDS::DBCluster e AWS::RDS::DBClusterParameterGroup Utilizza le risorse dei cluster e dei gruppi di parametri dei cluster per creare un cluster di database Amazon Aurora. AWS::WorkSpaces::Workspace Utilizzalo WorkSpaces per creare esperienze desktop basate sul cloud.	

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamenti delle risorse	1° ottobre 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::ElastiCache::ReplicationGroup Utilizza la funzione <code>Fn::GetAtt</code> intrinseca per ottenere un elenco di indirizzi e porte per la replica di sola lettura. AWS::OpsWorks::Stack Utilizzate la <code>AgentVersion</code> proprietà per specificare un AWS OpsWorks agente particolare. AWS::OpsWorks::App Utilizzate la <code>Environment</code> proprietà per specificare le variabili di ambiente per un' AWS OpsWorks app. AWS::S3::Bucket Per la NotificationConfiguration proprietà, puoi configurare le impostazioni di notifica per le funzioni Lambda e le code Amazon Simple Queue Service (Amazon SQS).	2010-05-15
Chiavi di condizione IAM	1° ottobre 2015	Per le policy AWS Identity and Access Management (IAM), usa chiavi CloudFormation di condizione specifiche e per specificare quando una policy IAM ha effetto. Per ulteriori informazioni, vedere Controlling Access with AWS Identity and Access Management.	2010-05-15
AWS CloudFormation Designer	1° ottobre 2015	Utilizzate AWS CloudFormation Designer per creare e modificare modelli utilizzando un' drag-and-drop interfaccia.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova risorsa	24 agosto 2015	Usa la AWS::EC2::VPCEndpoint risorsa per stabilire una connessione privata tra il tuo VPC e un altro AWS servizio.	2010-05-15
Aggiornamenti delle risorse	24 agosto 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::ElasticBeanstalk::Environment Utilizzate la Tags proprietà per specificare i tag (coppie chiave-valore) per un ambiente AWS Elastic Beanstalk (Elastic Beanstalk). AWS::Lambda::Function Per la proprietà Code, utilizza la proprietà ZipFile per scrivere il codice sorgente della tua funzione Lambda direttamente in un modello. Al momento, puoi utilizzare la proprietà ZipFile solo per gli ambienti di runtime nodejs. Puoi comunque scegliere di puntare a un file in un bucket S3 per tutti gli ambienti di runtime, ad esempio java8 e nodejs. AWS::OpsWorks::Instance Utilizza la proprietà EbsOptimized per indicare se un'istanza è ottimizzata per le operazioni di I/O di Amazon Elastic Block Store (Amazon EBS). AWS::RDS::DBInstance Per la proprietà SourceDBInstanceIdentifier , puoi specificare un'istanza database in un'altra Regione per creare una replica di lettura in più Regioni.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
URL del modello Amazon S3	24 agosto 2015	Per i bucket abilitati al controllo delle versioni, puoi specificare un ID della versione in un URL del modello Amazon S3 quando crei o aggiorni uno stack, ad esempio <code>https://s3.amazonaws.com/templates/myTemplate.template?versionId=123ab1cdeKd0W5IH4GAcYbEngcpTJTDW</code> .	2010-05-15
Nuova risorsa	3 agosto 2015	Utilizza la risorsa AWS::EFS::FileSystem per creare un file system Amazon Elastic File System (Amazon EFS) e la risorsa AWS::EFS::MountTarget per creare un punto di montaggio per un file system.	2010-05-15
Modifica ai requisiti di autorizzazione	11 giugno 2015	Quando crei o aggiorni una risorsa AWS::RDS::DBInstance , ora devi disporre anche dell'autorizzazione per chiamare l'operazione <code>ec2:DescribeAccountAttributes</code> .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	11 giugno 2015	CloudFormation ha aggiunto le seguenti risorse: AWS::DataPipeline::Pipeline Utilizza le pipeline di dati per automatizzare il trasferimento e la trasformazione dei dati. Risorse di Amazon Elastic Container Service Usa le AWS::ECS::TaskDefinition risorse AWS::ECS::Service AWS::ECS::Cluster, e per creare contenitori Docker su un cluster di EC2 istanze. AWS::ElastiCache::ReplicationGroup Utilizza gruppi di replica per creare una raccolta di nodi con un cluster primario di lettura e scrittura e un massimo di cinque cluster secondari di sola lettura. AWS::IAM::ManagedPolicy Utilizza le policy gestite per creare policy nel tuo AWS account che puoi utilizzare per applicare le autorizzazioni a utenti, gruppi e ruoli IAM. AWS::Lambda::Function Utilizza le funzioni di Lambda per eseguire codice in risposta a eventi. AWS::RDS::OptionGroup Utilizza gruppi di opzioni per semplificare la creazione e la gestione di database Amazon Relational Database Service (Amazon RDS).	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamenti delle risorse	11 giugno 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::EC2::Subnet Utilizza la proprietà <code>MapPublicIpOnLaunch</code> per assegnare automaticamente indirizzi IP pubblici alle istanze in una sottorete. AWS::ElastiCache::CacheCluster Utilizza la proprietà <code>SnapshotName</code> per ripristinare i dati degli snapshot in un nuovo cluster di cache Redis. AWS::IAM::User Per la proprietà <code>LoginProfile</code>, utilizza la proprietà <code>PasswordResetRequired</code> per richiedere agli utenti di impostare una nuova password quando accedono alla AWS Management Console. AWS::OpsWorks::Layer Utilizzate la <code>LifecycleEventConfiguration</code> proprietà per configurare gli eventi del ciclo di vita per un AWS OpsWorks livello. AWS::S3::Bucket Per la proprietà <code>LifecycleConfiguration</code>, utilizza le proprietà <code>NoncurrentVersionExpirationInDays</code> e <code>NoncurrentVersionTransition</code> per specificare le regole del ciclo di vita per le versioni degli oggetti non correnti.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuovi tipi di parametro	19 maggio 2015	Ogni volta che utilizzi la CloudFormation console per creare o aggiornare uno stack, puoi cercare valori di tipo di parametro AWS specifici per ID, nome o valore del tag Name. CloudFormation ha inoltre aggiunto il supporto per i seguenti tipi di AWS parametri specifici. Per ulteriori informazioni, consulta Parametri. • <code>AWS::EC2::AvailabilityZone::Name</code> • <code>List<AWS::EC2::AvailabilityZone ::Name></code> • <code>AWS::EC2::Instance::Id</code> • <code>List<AWS::EC2::Instance ::Id></code> • <code>AWS::EC2::Image::Id</code> • <code>List<AWS::EC2::Image::Id ></code> • <code>AWS::EC2::SecurityGroup::GroupName</code> • <code>List<AWS::EC2::SecurityGroup::Gr oupName ></code> • <code>AWS::EC2::Volume::Id</code> • <code>List<AWS::EC2::Volume::Id ></code> • <code>AWS::Route53::HostedZone::Id</code> • <code>List<AWS::Route53::HostedZone ::Id></code>	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove risorse	16 Aprile 2015	CloudFormation ha aggiunto le seguenti risorse: AWS::AutoScaling::LifecycleHook Puoi utilizzare hook del ciclo di vita Auto Scaling per controllare lo stato di un'istanza dopo che è stata avviata o terminata. AWS::RDS::EventSubscription Utilizza le sottoscrizioni a eventi per ricevere notifiche sugli eventi Amazon RDS.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamenti delle risorse	16 Aprile 2015	CloudFormation ha aggiornato le seguenti risorse: AWS::AutoScaling::AutoScalingGroup Utilizza la proprietà <code>NotificationConfigurations</code> per specificare più notifiche. AWS::AutoScaling::LaunchConfiguration Utilizza la proprietà <code>PlacementTenancy</code> per specificare la tenancy delle istanze. Utilizza le <code>ClassicLinkVPCSecurityGroups</code> proprietà <code>ClassicLinkVPCId</code> and per collegare le istanze EC2 -Classic a un VPC ClassicLink abilitato. AWS::AutoScaling::ScalingPolicy Utilizza la proprietà <code>MinAdjustmentStep</code> per specificare il numero minimo di istanze che vengono aggiunte o rimosse durante un evento di dimensionamento. AWS::CloudFront::Distribution Per i certificati del visualizzatore, utilizza la proprietà <code>MinimumProtocolVersion</code> per specificare una versione minima del protocollo. Per i comportamenti della cache, usa la <code>CachedMethods</code> proprietà per specificare per quali metodi Amazon CloudFront (CloudFront) memorizza nella cache le risposte. Per le origini, usa <code>OriginPath</code> per specificare un percorso da utilizzare per richiedere il contenuto. CloudFront AWS::ElastiCache::CacheCluster Per i cluster di cache Memcached, utilizzate le <code>PreferredAvailabilityZones</code> proprietà	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		AZMode and per specificare i nodi in più zone di disponibilità (). AZs AWS::EC2::Volume Utilizza la proprietà KmsKeyId per specificare una chiave gestita dal cliente per i volumi crittografati. AWS::OpsWorks::Instance Utilizza la proprietà TimeBasedAutoScaling per ridimensionare automaticamente le istanze in base alla pianificazione che specifichi. AWS::OpsWorks::Layer Utilizza la proprietà LoadBasedAutoScaling per specificare policy di dimensionamento basato sul carico. Per le configurazioni dei volumi, utilizzate le Iops proprietà VolumeType and per specificare rispettivamente un tipo di volume e il numero di I/O operazioni al secondo. AWS::RDS::DBInstance Utilizza la proprietà CharacterSetName per specificare un set di caratteri per i motori di database supportati. Utilizza la proprietà StorageEncrypted per indicare se le istanze database verranno crittografate e KmsKeyId per specificare una chiave gestita dal cliente per le istanze database crittografate. AWS::Route53::HealthCheck Utilizza la proprietà HealthCheckTags per associare tag ai controlli dello stato.	

Modifica	Data di rilascio	Descrizione	Versione API
		AWS::Route53::HostedZone Utilizza la proprietà VPCs per creare zone ospitate private. Utilizza la proprietà HostedZoneTags per associare tag alle zone ospitate.	
Nuova sezione dei modelli	16 Aprile 2015	Aggiungi la sezione dei metadati ai tuoi modelli per includere oggetti JSON arbitrari che descrivono i modelli, ad esempio i dettagli della progettazione o dell'implementazione.	2010-05-15
Aggiornamento delle risorse	8 Aprile 2015	Per la AWS::CloudFormation::CustomResource risorsa, puoi specificare la funzione Lambda Amazon Resource Names (ARNs) nella ServiceToken proprietà.	2010-05-15
Amazon RDS update	24 dicembre 2014	CloudFormation ha aggiunto due nuove proprietà per le istanze DB RDS. Puoi associare un gruppo di opzioni a un'istanza database e specificare il tipo di storage dell'istanza database. Per ulteriori informazioni, consulta AWS::RDS::DBInstance .	2010-05-15
Elastic Load Balancing update	24 dicembre 2014	Puoi utilizzare la proprietà ConnectionSettings per specificare il periodo di tempo in cui le connessioni possono rimanere inattive. Per ulteriori informazioni, consulta AWS::ElasticLoadBalancing::LoadBalancer .	2010-05-15
Aggiornamento di Route 53	6 Novembre 2014	Ora puoi eseguire il provisioning e gestire zone ospitate , controlli dell'integrità , set di record di failover e set di record di geolocalizzazione di Route 53.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Miglioramento dell'aggiornamento in sequenza Auto Scaling	6 Novembre 2014	Durante un aggiornamento, puoi utilizzare il <code>WaitOnResourceSignals</code> flag per indicare CloudFormation di attendere che le istanze segnalino l'esito positivo. In questo modo, CloudFormation non aggiornerà il prossimo batch di istanze finché il batch corrente non è pronto. Per ulteriori informazioni, consulta <code>UpdatePolicy</code> Attributo.	2010-05-15
Nuovo VPC Fn: attributi <code>GetAtt</code>	6 Novembre 2014	Utilizzano l'ID di un VPC, puoi recuperare il gruppo di sicurezza predefinito e la lista di controllo degli accessi di rete per quel VPC. Per ulteriori informazioni, consulta Fn::GetAtt .	2010-05-15
Nuovi tipi AWS di parametri specifici	6 Novembre 2014	Puoi specificare tipi AWS di parametri specifici nei tuoi CloudFormation modelli. Nella CloudFormation console, questi tipi di parametri forniscono un elenco a discesa di valori validi. Con l'API or AWS CLI, CloudFormation puoi convalidare rapidamente i valori per questi tipi di parametri prima di creare o aggiornare uno stack. Per ulteriori informazioni, consulta Parametri .	2010-05-15
CreationPolicy attributo	6 Novembre 2014	Con l' <code>CreationPolicy</code> attributo, puoi indicare CloudFormation di attendere che le applicazioni siano pronte sulle EC2 istanze prima di procedere con la creazione dello stack. Puoi utilizzare una policy di creazione invece di una condizione di attesa e di un handle di condizione di attesa. Per ulteriori informazioni, consulta <code>Attributo</code>. <code>CreationPolicy</code>	2010-05-15
Valori CloudFront inoltrati da Amazon	29 settembre 2014	Per i comportamenti cache, puoi inoltrare le intestazioni all'origine. Consultare ForwardedValues .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
AWS OpsWorks update	29 settembre 2014	Per Chef 11.10, puoi utilizzare la proprietà <code>ChefConfiguration</code> per abilitare Berkshelf. Puoi anche utilizzare i gruppi di sicurezza AWS OpsWorks integrati con i tuoi AWS OpsWorks stack. Per ulteriori informazioni, consulta AWS::OpsWorks::Stack .	2010-05-15
Supporto di tagging per Elastic Load Balancing	29 settembre 2014	AWS CloudFormation tag Elastic Load Balancing: sistemi di bilanciamento del carico con tag a livello di stack. Puoi anche aggiungere i tuoi tag a un load balancer. Consultare AWS::ElasticLoadBalancing::LoadBalancer .	2010-05-15
Aggiornamento della policy di argomento Amazon Simple Notification Service	29 settembre 2014	Ora puoi aggiornare policy di argomento Amazon SNS. Per ulteriori informazioni, consulta AWS::SNS::TopicPolicy .	2010-05-15
Aggiornamento di istanze database di RDS	5 settembre 2014	Puoi specificare se un'istanza database è connessa a Internet utilizzando la proprietà <code>PubliclyAccessible</code> nella risorsa AWS::RDS::DBInstance .	2010-05-15
UpdatePolicy aggiornamento degli attributi	05 settembre 2014	Puoi specificare una policy di aggiornamento per un gruppo con dimensionamento automatico al quale è associata un'operazione pianificata. Per ulteriori informazioni, vedete UpdatePolicyAttributo .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
CloudWatch Assistenza Amazon	10 luglio 2014	Puoi utilizzarlo CloudFormation per fornire e gestire gruppi di CloudWatch log e filtri metrici di Amazon CloudWatch Logs (Logs). Per ulteriori informazioni, consulta AWS::Logs::LogGroup o AWS::Logs::MetricFilter .	2010-05-15
Aggiornamento CloudFront della configurazione della distribuzione Amazon	17 giugno 2014	Puoi specificare proprietà di configurazione CloudFront di distribuzione aggiuntive: • Le risposte di errore personalizzate definiscono i messaggi di errore personalizzati per i codici di stato HTTP 4xx e 5xx. • La categoria di prezzo definisce il prezzo massimo che intendi pagare per il servizio CloudFront . • Le limitazioni definiscono chi può visualizzare i tuoi contenuti. • Il certificato visualizzatore specifica il certificato da utilizzare quando i visualizzatori utilizzano HTTPS. • Per comportamenti cache, puoi specificare i metodi HTTP consentiti e indicare se inoltrare i cookie. Per ulteriori informazioni, consulta AWS::CloudFront::Distribution.	2010-05-15
EC2 aggiornamento dell'istanza	17 giugno 2014	Puoi specificare se un'istanza viene arrestata o interrotta quando invochi il comando per l'arresto del sistema operativo dell'istanza. Per ulteriori informazioni, consulta AWS::EC2::Instance .	2010-05-15
Aggiornamento del volume EBS	17 giugno 2014	Puoi utilizzare volumi EBS crittografati con i tipi di istanze supportati. Per ulteriori informazioni, consulta AWS::EC2::Volume .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova connessione di peering Amazon VPC	17 giugno 2014	Puoi utilizzarla CloudFormation per creare una connessione peering Amazon Virtual Private Cloud (Amazon VPC), che stabilisce una connessione di rete tra due VPCs. Per ulteriori informazioni, consulta AWS::EC2::VPCPeeringConnection .	2010-05-15
Aggiornamento del EC2 gruppo Amazon Auto Scaling	17 giugno 2014	Puoi specificare un gruppo di posizionamento del cluster esistente in cui avviare le istanze per un gruppo Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta AWS::AutoScaling::AutoScalingGroup .	2010-05-15
AWS CloudTrail supporto	17 giugno 2014	CloudFormation supporta AWS CloudTrail, che possono acquisire le chiamate API effettuate dal tuo AWS account e pubblicare i log in una posizione designata dall'utente. Per ulteriori informazioni, consulta AWS::CloudTrail::Trail .	2010-05-15
Miglioramenti all'aggiornamento degli stack	12 maggio 2014	CloudFormation supporta funzionalità aggiuntive per l'aggiornamento degli stack: • È possibile aggiornare i parametri CloudFormation dello stack senza inviare nuovamente il modello dello stack. • Puoi aggiungere o rimuovere gli argomenti di notifica Amazon SNS per uno stack CloudFormation. Per ulteriori informazioni, consulta Stacks Updates. CloudFormation	2010-05-15
Supporto di Amazon Kinesis	6 maggio 2014	Puoi utilizzarlo CloudFormation per creare stream Amazon Kinesis che acquisiscono e trasportano record di dati da fonti di dati. Per ulteriori informazioni, consulta AWS::Kinesis::Stream .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuove proprietà dei bucket S3	5 maggio 2014	CloudFormation supporta proprietà aggiuntive del bucket S3: • La funzione Cross-Origin Resource Sharing (CORS) definisce la condivisione multiorigine di oggetti in un bucket. • Il ciclo di vita definisce il modo in cui Amazon S3 gestisce gli oggetti durante il loro ciclo di vita. • La policy di registrazione degli accessi acquisisce informazioni sulle richieste relative al tuo bucket. • Le notifiche definiscono quali eventi segnalare e a quale argomento Amazon SNS inviare messaggi. • La funzione Versioni multiple abilita diverse varianti di tutti gli oggetti in un bucket. • Le regole di reindirizzamento e routing regolamentano il comportamento di reindirizzamento per le richieste effettuate all'endpoint del sito Web di un bucket. Per ulteriori informazioni, consulta AWS::S3::Bucket.	2010-05-15
Supporto per Amazon EC2 Auto Scaling	5 maggio 2014	CloudFormation supporta la raccolta di metriche per un gruppo Auto Scaling. Per ulteriori informazioni, consulta AWS::AutoScaling::AutoScalingGroup.	2010-05-15
Fn::If update	5 maggio 2014	Puoi utilizzare la funzione Fn::If intrinseca nella sezione di output di un modello. Per ulteriori informazioni, consulta la sezione sulle funzioni di condizione.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Registrazione API con AWS CloudTrail	2 aprile 2014	Puoi usare AWS CloudTrail (CloudTrail) per registrar e CloudFormation le richieste. Con CloudTrail puoi ottenere una cronologia delle chiamate CloudFormation API per il tuo account. Per ulteriori informazioni, consulta Registrazione delle chiamate CloudFormation API con AWS CloudTrail .	2010-05-15
Elastic Load Balancing update	20 marzo 2014	Puoi specificare una policy di registrazione degli accessi per acquisire informazioni sulle richieste relative al tuo load balancer. Puoi anche specificare una policy di Connection Draining che descrive come gestire le richieste in transito quando la registrazione delle istanze viene annullata o quando queste diventano non integre. Per ulteriori informazioni, consulta AWS::ElasticLoadBalancing::LoadBalancer .	2010-05-15
AWS OpsWorks supporto	3 marzo 2014	È possibile utilizzarlo CloudFormation per fornire e gestire gli AWS OpsWorks stack. Per ulteriori informazioni, consulta AWS::OpsWorks::Stack i nostri AWS OpsWorks Template Snippets .	2010-05-15
Incremento del limite delle dimensioni del modello Amazon S3	18 febbraio 2014	Puoi specificare dimensioni del modello fino a 460.800 byte in Amazon S3.	2010-05-15
Supporto di Amazon Redshift	10 febbraio 2014	Puoi utilizzarlo CloudFormation per effettuare il provisioning e gestire i cluster Amazon Redshift. Per ulteriori informazioni, consulta Frammenti del modello di Amazon Redshift o AWS::Redshift::Cluster .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Aggiornamento delle policy dei bucket e dei bucket S3	10 febbraio 2014	Puoi aggiornare alcune proprietà delle risorse delle policy relative ai bucket e ai bucket S3. Per ulteriori informazioni, consulta AWS::S3::Bucket o AWS::S3::BucketPolicy .	2010-05-15
Aggiornamento degli ambienti e delle versioni delle applicazioni di Elastic Beanstalk	10 febbraio 2014	Puoi aggiornare le configurazioni e le versioni delle applicazioni dell'ambiente Elastic Beanstalk. Per ulteriori informazioni, consulta AWS::ElasticBeanstalk::Environment , AWS::ElasticBeanstalk::ConfigurationTemplate o AWS::ElasticBeanstalk::ApplicationVersion .	2010-05-15
Amazon SQS update	29 gennaio 2014	Puoi specificare una coda DLQ per una coda Amazon SQS. Per ulteriori informazioni, consulta AWS::SQS::Queue .	2010-05-15
Operazioni Auto Scaling pianificate	27 gennaio 2014	È possibile scalare il numero di EC2 istanze in un gruppo di Auto Scaling in base a una pianificazione. L'utilizzo di una pianificazione ti consente di dimensionare le applicazioni per rispondere alle variazioni di carico prevedibili. Per ulteriori informazioni, consulta AWS::AutoScaling::ScheduledAction .	2010-05-15
Indici secondari DynamoDB	27 gennaio 2014	Puoi creare indici secondari locali e globali per database DynamoDB. L'utilizzo di indici secondari ti consente di accedere in modo efficiente ai dati con attributi diversi dalla chiave primaria. Per ulteriori informazioni, consulta AWS::DynamoDB::Table .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Auto Scaling update	2 gennaio 2014	Puoi specificare un ID istanza per un gruppo o una configurazione di avvio Auto Scaling. Puoi inoltre specificare ulteriori proprietà del dispositivo a blocchi Auto Scaling. Per ulteriori informazioni, consulta AWS::AutoScaling::AutoScalingGroup o AWS::AutoScaling::LaunchConfiguration .	2010-05-15
Amazon SQS update	2 gennaio 2014	Puoi aggiornare le code SQS e specificare proprietà aggiuntive. Per ulteriori informazioni, consulta AWS::SQS::Queue .	2010-05-15
Aumenti dei limiti	2 gennaio 2014	Puoi specificare fino a 60 parametri e fino a 60 output nei tuoi modelli CloudFormation.	2010-05-15
Nuova console	19 dicembre 2013	La nuova CloudFormation console aggiunge funzionalità come l'aggiornamento automatico degli eventi dello stack e l'ordinamento alfabetico dei parametri dello stack.	2010-05-15
load balancer su più zone	19 dicembre 2013	Con il bilanciamento del carico tra zone, puoi indirizzare il traffico verso le istanze di back-end in tutte le zone di disponibilità (). AZs Per ulteriori informazioni, consulta AWS::ElasticLoadBalancing::LoadBalancer .	2010-05-15
AWS Elastic Beanstalk livelli di ambiente	19 dicembre 2013	È possibile specificare se effettuare il provisioning delle risorse per supportare un server Web o per gestire le attività di elaborazione in background. Per ulteriori informazioni, consulta AWS::ElasticBeanstalk::Environment .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nomi delle risorse	19 dicembre 2013	È possibile assegnare nomi (fisici IDs) alle seguenti risorse: - ElastiCache cluster - load balancer Elastic Load Balancing - istanze database RDS Per ulteriori informazioni, consulta Tipo di nome.	2010-05-15
Supporto per VPN	22 Novembre 2013	Puoi abilitare un gateway virtuale privato (VGW) per propagare gli instradamenti alle tabelle di routing di un VPC. Per ulteriori informazioni, consulta AWS::EC2::VPNGatewayRoutePropagation.	2010-05-15
Creazione di risorse e assegnazione di proprietà in modo condizionale	8 Novembre 2013	L'utilizzo di parametri di input ti consente di controllare la creazione e le impostazioni delle risorse di stack designate mediante la definizione di condizioni nei tuoi modelli CloudFormation. Ad esempio, puoi utilizzare condizioni per creare risorse di stack per un ambiente di produzione. Utilizzando lo stesso modello, puoi creare risorse di stack simili con capacità inferiore per un ambiente di test. Per ulteriori informazioni, consulta la sezione sulle funzioni di condizione.	2010-05-15
Prevenzione di aggiornamenti accidentali alle risorse di stack	8 Novembre 2013	Puoi prevenire aggiornamenti dello stack che potrebbero causare modifiche involontarie alle risorse dello stack. Ad esempio, se disponi di uno stack con un livello di database che dovrebbe essere aggiornato raramente, puoi impostare una policy di stack che impedisce alla maggior parte degli utenti di aggiornare il livello di database in questione. Per ulteriori informazioni, consulta Impedire gli aggiornamenti delle risorse stack.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Assegnazione di nomi alle risorse	8 Novembre 2013	Invece di utilizzare CloudFormation -generated physical IDs, puoi assegnare nomi a determinate risorse. Le seguenti CloudFormation risorse supportano la denominazione • CloudWatch Allarmi Amazon • Tabelle DynamoDB • AWS Elastic Beanstalk applicazioni e ambienti • Bucket Amazon S3 • Argomenti di Amazon SNS • Code Amazon SQS Per ulteriori informazioni, consulta Tipo di nome.	2010-05-15
Assegnazione di tipi di risorse personalizzate	8 Novembre 2013	Nei modelli, puoi specificare il tipo di risorsa per le risorse personalizzate CloudFormation (<code>AWS::CloudFormation::CustomResource</code>). Utilizzando il tuo nome del tipo di risorsa personalizzata, puoi individuare rapidamente il tipo di risorse personalizzate presenti nello stack. Ad esempio, puoi specificare "Type": "<code>Custom:: <i>MyCustomResource</i></code>". Per ulteriori informazioni, consulta AWS::CloudFormation::CustomResource.	2010-05-15
Aggiunta di pseudoparametri	8 Novembre 2013	Ora puoi fare riferimento all' AWS AccountID all'interno dei CloudFormation modelli facendo riferimento allo <code>AWS::AccountId</code> pseudo parametro. Per ulteriori informazioni, consulta Riferimenti agli pseudoparametri.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Specifica di stack nelle policy IAM	8 Novembre 2013	Puoi consentire o negare a utenti, gruppi o ruoli IAM di operare su stack specifici. CloudFormation Ad esempio, puoi impedire l'operazione di eliminazione di stack su un determinato ID di stack. Per ulteriori informazioni, vedere Controlling Access with AWS Identity and Access Management .	2010-05-15
Supporto di federazioni	14 ottobre 2013	CloudFormation supporta le credenziali di sicurezza temporanee dei ruoli IAM, che abilitano scenari come la federazione e il single sign-on a. AWS Management Console Puoi anche effettuare chiamate CloudFormation da EC2 istanze senza incorporare credenziali di sicurezza a lungo termine utilizzando i ruoli IAM. Per ulteriori informazioni su CloudFormation e IAM, consulta Controlling Access with AWS Identity and Access Management .	2010-05-15
Supporto delle repliche di lettura Amazon RDS	24 settembre 2013	Ora puoi creare repliche di lettura Amazon RDS da un'istanza database di origine. Per maggiori informazioni, consulta la proprietà SourceDBInstanceId entifier nella risorsa AWS::RDS::DBInstance .	2010-05-15
Associazione di un indirizzo IP pubblico a istanze in un gruppo con dimensionamento automatico	19 settembre 2013	Ora puoi associare indirizzi IP pubblici a istanze in un gruppo con dimensionamento automatico. Per ulteriori informazioni, consulta AWS::AutoScaling::LaunchConfiguration .	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Ulteriore supporto di VPC	17 settembre 2013	CloudFormation aggiunge diversi miglioramenti per supportare le funzionalità VPC e VPN • Puoi associare un indirizzo IP pubblico e più indirizzi IP privati alle interfacce di EC2 rete Amazon. Per ulteriori informazioni, consulta AWS::EC2::NetworkInterface. Puoi inoltre associare un indirizzo IP privato primario a un indirizzo IP elastico (EIP). • Puoi abilitare il supporto DNS e specificare nomi host DNS. Per ulteriori informazioni, consulta AWS::EC2::VPC. • Puoi specificare un instradamento statico tra un gateway virtuale privato e il tuo gateway VPN. Per ulteriori informazioni, consulta AWS::EC2::VPNConnectionRoute.	2010-05-15
Supporto per gruppi di sicurezza Redis e VPC per Amazon ElastiCache	3 settembre 2013	Ora puoi specificare Redis come motore di cache per un cluster Amazon ElastiCache (ElastiCache). Ora puoi anche assegnare gruppi ElastiCache di sicurezza VPC ai cluster. Per ulteriori informazioni, consulta AWS::ElastiCache::CacheCluster.	2010-05-15
Creazione, aggiornamento ed eliminazione di stack in parallelo e aggiornamento degli stack nidificati	12 agosto 2013	AWS CloudFormation ora crea, aggiorna ed elimina risorse in parallelo, migliorando le prestazioni delle operazioni. Se aggiorni un modello di primo livello, AWS CloudFormation aggiorna automaticamente gli stack nidificati interessati dalle modifiche. Per ulteriori informazioni, consulta CloudFormation Stacks Updates.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
I gruppi di sicurezza VPC possono ora essere impostati in istanze database RDS	28 febbraio 2013	Ora puoi assegnare gruppi di sicurezza VPC a un'istanza a database RDS con CloudFormation. Per ulteriori informazioni, vedere la proprietà VPCSecurityGroups in AWS::RDS::DBInstance .	2010-05-15
Implementazioni continue per gruppi Amazon Auto EC2 Scaling	20 febbraio 2013	CloudFormation ora supporta le politiche di aggiornamento sui gruppi Amazon EC2 Auto Scaling, che descrivono come le istanze del gruppo Amazon EC2 Auto Scaling vengono sostituite o modificate quando il gruppo Amazon Auto Scaling EC2 aggiunge o rimuove istanze. Puoi modificare queste impostazioni durante la creazione o l'aggiornamento di uno stack. Per ulteriori informazioni e un esempio, consulta Attribute . UpdatePolicy	2010-05-15
Operazione di annullamento e rollback per gli aggiornamenti degli stack	20 febbraio 2013	CloudFormation supporta la possibilità di annullare un aggiornamento dello stack. Lo stack deve essere nello stato UPDATE_IN_PROGRESS quando viene eseguita la richiesta di aggiornamento. Ulteriori informazioni sono disponibili nei seguenti argomenti: • Annullamento di un aggiornamento dello stack • cancel-update-stack • CancelUpdateStack nel Documentazione di riferimento API di CloudFormation	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Istanze ottimizzate per EBS per gruppi Amazon Auto Scaling EC2	20 febbraio 2013	Ora puoi effettuare il provisioning di istanze ottimizzate per EBS nei gruppi Amazon EC2 Auto Scaling per un throughput dedicato ad Amazon Elastic Block Store (Amazon EBS) in istanze con scalabilità automatica. L'implementazione è simile a quella del supporto rilasciato in precedenza per le EC2 istanze Amazon EBS ottimizzate. Per ulteriori informazioni, consulta la nuova proprietà <code>EbsOptimized</code> in AWS::AutoScaling::LaunchConfiguration.	2010-05-15
Nuova documentazione	21 dicembre 2012	AWS::EC2::Instance ora fornisce una <code>BlockDeviceMappings</code> proprietà che ti consente di impostare mappature dei dispositivi a blocchi per la tua istanza. EC2 Con questa modifica sono stati aggiunti due nuovi tipi: • BlockDeviceMapping • Dispositivo a blocchi	2010-05-15
Nuova documentazione	21 dicembre 2012	Sono state aggiunte nuove sezioni per descrivere le procedure di creazione e visualizzazione di stack utilizzando la nuova AWS Management Console. Sono disponibili qui: • Creare uno stack dalla console CloudFormation • Visualizza le informazioni sullo stack dalla console CloudFormation	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova documentazione	15 Novembre 2012	Informazioni sulle risorse personalizzate sono fornite nei seguenti argomenti: • Risorse personalizzate • AWS::CloudFormation::CustomResource • Riferimento a risorse personalizzate	2010-05-15
Documentazione aggiornata	15 Novembre 2012	CloudFormation ora supporta la specifica I/O delle operazioni di provisioning per secondo (IOPS) per le istanze DB RDS. Questo valore può essere compreso tra 1.000 e 10.000 in incrementi di 1.000 IOPS utilizzando la nuova proprietà IOPS in AWS::RDS::DBInstance. Per ulteriori informazioni sulla definizione di IOPS per le istanze database RDS, consulta Provisioned IOPS nella Guida per l'utente di Amazon Relational Database Service.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Documentazione nuova e aggiornata	27 agosto 2012	Gli argomenti sono stati riorganizzati per fornire più chiaramente informazioni specifiche sull'uso AWS Management Console e sull'utilizzo dell'interfaccia a riga di CloudFormation comando (CLI). Sono state aggiunte informazioni sugli CloudFormation stack di tag, tra cui nuove guide e argomenti di riferimento aggiornati: • Nuovo argomento: Configurare le opzioni dello stack. • Nuove informazioni sui tag nella Documentazione di riferimento delle API CloudFormation : CreateStack, Stack e Tag. Nuove informazioni sull'utilizzo di stack Windows: • Microsoft Windows Amazon Machine Images (AMIs) e AWS CloudFormation modelli • Avvio degli stack di Windows AWS CloudFormation Nuovo argomento: Uso delle espressioni regolari nei modelli. CloudFormation	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova caratteristica	25 Aprile 2012	CloudFormation ora fornisce il supporto completo per la sicurezza del Virtual Private Cloud (VPC) con Amazon. EC2 Ora puoi creare e popolare un intero VPC con ogni tipo di risorsa VPC (sottoreti, gateway, ACLs rete, tabelle di routing e così via) utilizzando un unico modello. CloudFormation La documentazione per i seguenti tipi di risorse è stata aggiornata: • AWS::EC2::SecurityGroup • AWS::EC2::SecurityGroupIngress • AWS::EC2::SecurityGroupEgress • AWS::EC2::Instance • AWS::AutoScaling::AutoScalingGroup • AWS::EC2::EIP • AWS::EC2::EIPAssociation • AWS::ElasticLoadBalancing::LoadBalancer Sono stati aggiunti nuovi tipi di risorse alla documentazione: • AWS::EC2::VPC • AWS::EC2::InternetGateway • AWS::EC2::DHCPOptions • AWS::EC2::DHCPOptions • AWS::EC2::RouteTable • AWS::EC2::NetworkAcl • AWS::EC2::NetworkAclEntry • AWS::EC2::Subnet • AWS::EC2::VPNGateway	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
		• AWS::EC2::CustomerGateway	
Nuova caratteristica	13 Aprile 2012	CloudFormation ora consente di aggiungere o rimuovere elementi da una pila durante l'aggiornamento. CloudFormation Stacks Updates è stato aggiornato ed è stata aggiunta una nuova sezione alla procedura dettagliata: Change the Stack's Resources, che descrive come aggiungere e rimuovere risorse durante l'aggiornamento dello stack.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova caratteristica	2 febbraio 2012	CloudFormation ora fornisce supporto per le risorse in un Amazon Virtual Private Cloud (Amazon VPC) esistente. Questa release ti consente di: • Avvia un'istanza EC2 dedicata in un Amazon VPC esistente. Per ulteriori informazioni, consulta AWS::EC2::Instance. • Imposta l'<code>SourceDestCheck</code> attributo di un' EC2 istanza che risiede in un Amazon VPC esistente. Per ulteriori informazioni, consulta AWS::EC2::Instance. • Creare indirizzi IP elastici in un Amazon VPC esistente . Per ulteriori informazioni, consulta AWS::EC2::EIP. • Utilizzalo CloudFormation per creare gruppi di sicurezza Amazon VPC e regole di ingresso/uscita in un VPC esistente. Per ulteriori informazioni, consulta AWS::EC2::SecurityGroup. • Associare un gruppo con dimensionamento automatico a un Amazon VPC esistente impostando la proprietà <code>VPCZoneIdentifier</code> della tua risorsa <code>AWS::AutoScaling::AutoScalingGroup</code> . Per ulteriori informazioni, consulta AWS::AutoScaling::AutoScalingGroup. • Collegare un load balancer Elastic Load Balancing a una sottorete Amazon VPC e creare gruppi di sicurezza per il load balancer. Per ulteriori informazioni, consulta AWS::ElasticLoadBalancing::LoadBalancer. • Creare un'istanza database RDS in un Amazon VPC esistente. Per ulteriori informazioni, consulta AWS::RDS::DBInstance.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuova caratteristica	2 febbraio 2012	Ora puoi aggiornare le proprietà per le seguenti risorse in uno stack esistente: • AWS::EC2::SecurityGroupIngress • AWS::EC2::SecurityGroupEgress • AWS::EC2::EIPAssociation • AWS::RDS::DBSubnetGroup • AWS::RDS::DBSecurityGroup • AWS::RDS::DBSecurityGroupIngress • AWS::Route53::RecordSetGroup Per un elenco completo di risorse aggiornabili e dettagli su cosa considerare quando si aggiorna uno stack, consulta Stacks Updates. CloudFormation	2010-05-15
Guida ristrutturata	2 febbraio 2012	Sezioni esistenti riorganizzate in nuove sezioni: Utilizzo dei CloudFormation modelli e Gestione degli stack. Spostato l'argomento Riferimenti dei modelli al livello principale del sommario. È stata spostata la stima del costo dello CloudFormation stack nella sezione Guida introduttiva.	2010-05-15

Modifica	Data di rilascio	Descrizione	Versione API
Nuovo contenuto	2 febbraio 2012	Sono state aggiunte nuove sezioni: • Procedura guidata: aggiornamento di uno stack è un tutorial che guida attraverso il processo di aggiornamento di uno stack LAMP. • Deploying Applications on Amazon EC2 AWS CloudFormation descrive come utilizzare gli script di CloudFormation supporto per distribuire applicazioni utilizzando i metadati archiviati nel modello. • CloudFormationHelper Scripts Reference fornisce materiale di riferimento per gli script di CloudFormation supporto (cfn-init, cfn-signal e cfn-hup). cfn-get-metadata	2010-05-15
Nuova caratteristica	26 maggio 2011	CloudFormation ora fornisce il <code>list-stacks</code> comando, che consente di elencare gli stack filtrati in base allo stato dello stack. Gli stack eliminati possono essere elencati per un massimo di 90 giorni dopo l'eliminazione. Per ulteriori informazioni, consulta Descrivere e elencare gli stack.	2010-05-15
Nuove funzionalità	26 maggio 2011	Ora i comandi <code>describe-stack-resources</code> e <code>get-template</code> consentono di ottenere informazioni dagli stack che sono stati eliminati per 90 giorni dopo la loro eliminazione. Per ulteriori informazioni, consulta Elencare le risorse e recuperare un modello.	2010-05-15
Nuovo collegamento	1 marzo 2011	CloudFormation le informazioni sull'endpoint si trovano ora in. Riferimenti generali di AWS Per ulteriori informazioni, consulta la pagina relativa a regioni ed endpoint nelle informazioni di riferimento generali su AWS .	2010-05-15
Rilascio iniziale	25 febbraio 2011	La versione pubblica iniziale di CloudFormation	2010-05-15

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.