



Guida per l'utente

AWS Control Tower



AWS Control Tower: Guida per l'utente

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

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

Table of Contents

Cos'è AWS Control Tower?	1
Funzionalità	1
In che modo AWS Control Tower interagisce con gli altri AWS services	2
Sei un First-Time utente di AWS Control Tower?	3
Come funziona	4
Struttura di una zona di atterraggio AWS Control Tower	4
Cosa succede quando configuri una landing zone	5
Cosa sono gli account condivisi?	6
Come funzionano i controlli	7
Come funziona AWS Control Tower con StackSets	8
Terminologia	9
Prezzi	13
Configurazione	14
Registrati per AWS	14
Iscriviti per un Account AWS	14
Approfondimenti	14
Nozioni di base	15
Guida di avvio rapido	15
Pre-launch controlli	17
Considerazioni per Centro identità AWS IAM clienti (IAM Identity Center)	18
Configura l'ambiente dedicato ai controlli	19
Nozioni di base	20
Considerazioni su AWS Config	20
Processo di implementazione	20
Note importanti	20
Inizia dalla console	21
Aspettative per la configurazione della zona di atterraggio	21
Passaggio 1: crea gli indirizzi email del tuo account condiviso	22
Passaggio 2. Configura e avvia la tua zona di atterraggio	24
Fase 3. Rivedi e configura la zona di atterraggio	33
Inizia a usare le API	34
Aspettative per la configurazione delle landing zone con le API	35
Fase 1: Configura la tua landing zone	36
Fase 2: Avvia la landing zone utilizzando le API AWS Control Tower	39

Identifica la tua landing zone	43
Aggiorna la tua landing zone	43
Reimposta la landing zone per risolvere la deriva	45
Visualizza i dettagli del file manifesto della tua zona di atterraggio	46
Visualizza lo stato delle operazioni della tua zona di atterraggio	51
Esempi: configura una landing zone di AWS Control Tower solo con API	53
Schemi delle zone di atterraggio	61
Avvia una landing zone usando CloudFormation	84
Fasi successive	90
Limitazioni e quote	92
Limitazioni note in AWS Control Tower	92
Richiesta di un aumento della quota	95
Limitazioni di controllo	96
Trova i controlli e le aree disponibili	98
Limitazioni basate sul sottostante AWS services	98
Differenze regionali	100
La guida di riferimento di Controls	102
Le migliori pratiche per gli amministratori	103
Spiegazione dell'accesso agli utenti	103
Spiegazione dell'accesso alle risorse	103
Spiegazione dei controlli preventivi	104
Pianifica la tua landing zone	105
Confronta le funzionalità	106
Avvia AWS Control Tower in un'organizzazione esistente	107
Lancio di AWS Control Tower in una nuova organizzazione	108
Procedure consigliate: configurare una landing AWS zone con più account	109
Allineati alle linee guida relative a più account AWS	109
Linee guida per configurare un ambiente ben progettato	110
Allinea la struttura dell'unità organizzativa con AWS strategia multi-account	113
Informazioni su Root	114
Suggerimenti amministrativi per la configurazione delle landing zone	114
Guida alla migrazione di Landing Zone v4.0	115
Modifiche chiave	116
Aggiornamenti di AWS Config	120
Confronto delle funzionalità con e senza AWS Config integrazione	123
Consigli per la configurazione di gruppi, ruoli e politiche	125

Linee guida sulle risorse AWS Control Tower	126
Quando accedere come utente root	128
AWS Organizations linee guida	129
Linee guida per IAM Identity Center	130
Guida Account Factory	132
Linee guida sulla sottoscrizione a SNS Topics	133
Linee guida per le chiavi KMS	134
Aggiornamenti della zona di atterraggio	135
Politiche per AI-based i servizi	138
Gestione degli aggiornamenti della configurazione	139
Informazioni sugli aggiornamenti	141
Aggiorna la tua landing zone	142
Procedura di aggiornamento standard	143
Seleziona una versione di landing zone	143
Aggiornamenti dell'account, versioni delle landing zone e linee di base	145
Conserva i percorsi degli account	145
Risolvi la deriva con Reset e Re-register	147
Fornisci e aggiorna gli account utilizzando l'automazione	148
Automatizza le attività	150
AWS CloudShell e il AWS CLI	152
Ottieni le autorizzazioni IAM per AWS CloudShell	153
Interagisci con AWS Control Tower attraverso AWS CloudShell	154
AWS CloudFormation risorse	157
AWS Control Tower and CloudFormation modelli	157
Scopri di più su CloudFormation	157
Personalizza la tua zona di atterraggio	159
Personalizza dalla console AWS Control Tower	159
Automatizza le personalizzazioni all'esterno della console AWS Control Tower	161
AWS Control Tower e LZA	161
Vantaggi delle personalizzazioni per AWS Control Tower (cFCT)	162
Esempi cFCT aggiuntivi	163
Panoramica sulle personalizzazioni per AWS Control Tower (cFCT)	164
Architecture	164
Costo	167
Servizi relativi ai componenti	167
AWS CodeCommit	168

AWS CodePipeline	168
AWS Key Management Service	168
AWS Lambda	169
Amazon Simple Notification Service	169
Amazon Simple Storage Service	169
Amazon Simple Queue Service	170
AWS Step Functions	170
AWS Systems Manager Parameter Store	170
Considerazioni sull'implementazione	170
Preparati per la distribuzione	170
Per aggiornare le personalizzazioni per AWS Control Tower	172
Modello e codice sorgente	172
Codice sorgente	173
Implementa cFCT	173
Prerequisiti	173
Fasi della distribuzione	173
Fase 1: Avvio dello stack	174
Fase 2: Crea un pacchetto personalizzato	178
Aggiorna lo stack	178
Eliminazione di un set di stack	179
Configura Amazon S3 come origine di configurazione	180
Imposta GitHub come fonte di configurazione	181
Preparare un repository GitHub	182
Crea la connessione GitHub	182
Distribuisci il CloudFormation stack	182
Parametri operativi	183
Guida alla personalizzazione cFCT	184
Panoramica della pipeline di codice	184
Definire una configurazione personalizzata	187
Unità organizzativa principale	194
Unità organizzativa annidata	195
Crea le tue personalizzazioni	196
Aggiornamenti di versione per il manifesto cFCT	204
Rete	207
VPC e AWS Regioni in AWS Control Tower	207
Panoramica di AWS Control Tower e VPC	208

CIDR e peering per VPC e AWS Control Tower	209
AWS PrivateLink	211
Considerazioni	211
Creazione di un endpoint di interfaccia	212
Creazione di una policy dell'endpoint	212
Ruoli e autorizzazioni	214
Ruoli e account	215
Ruoli e creazione di account	215
AWSControlTowerExecution ruolo	215
Condizioni opzionali per il ruolo, le relazioni di fiducia	217
Come si aggrega AWS Control Tower AWS Config regole nelle unità organizzative e negli account non gestiti	220
Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower	223
Effettuazione del provisioning automatico degli account con ruoli IAM	227
Gestione delle risorse	229
Configura le regioni	230
Configura le tue regioni AWS Control Tower	231
Evita una governance mista durante la configurazione delle regioni	233
Informazioni sulle regioni con opzione opt-in	235
Configurare la regione per negare il controllo	238
Le considerazioni relative alla OU-level regione negano il controllo	239
Informazioni sugli account	240
Cosa succede quando AWS Control Tower crea un account	240
Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti	241
Account di integrazione dei servizi	242
Gestione dell'account	242
CloudTrail account amministratore	243
Account aggregatore Config	244
Risorse degli account di integrazione dei servizi	245
Risorse dell'account di gestione	245
CloudTrail risorse per gli account di amministratore	250
Risorse dell'account Config Aggregator	253
Informazioni sugli account dei membri	256
Interagisci con gli account AWS Control Tower da AWS Service Catalog	257
Crea ed esegui il provisioning di un account	257

Automatizza il provisioning degli account nelle API AWS Control Tower tramite Service Catalog	259
Aggiornare il prodotto fornito in Service Catalog	263
Annullare la registrazione di un account in Service Catalog	265
Eseguire il provisioning e gestire gli account	267
Autorizzazioni richieste	267
Metodi di provisioning	268
Esegui il provisioning degli account nella console	270
Visualizza i tuoi account	271
Informazioni sulla registrazione degli account	272
Cosa succede durante la registrazione dell'account	273
Registra gli account esistenti con i VPC	274
Registra gli account con AWS Config risorse	275
Prerequisiti per l'iscrizione	275
Auto-enrollment opzione	277
Registrati dalla console	279
Se l'account non soddisfa i prerequisiti	283
Aggiungi manualmente il ruolo IAM richiesto a un ruolo IAM esistente Account AWS e iscrivilo	285
Registra account esistenti AWS Config risorse	288
Passaggio 1: contatta l'assistenza per aggiungere account all'elenco degli account consentiti	290
Fase 2: Crea un nuovo ruolo IAM nell'account del membro	290
Passaggio 3: Identifica il AWS Regioni con risorse preesistenti	291
Fase 4: Identifica il AWS Regioni senza AWS Config risorse	292
Passaggio 5: modifica le risorse esistenti in ciascuna AWS Region	292
Fase 5a. AWS Config risorse del registratore	292
Fase 5b. Modify (Modifica) AWS Config risorse del canale di distribuzione	293
Fase 5c. Modify (Modifica) AWS Config risorse di autorizzazione all'aggregazione	294
Fase 6: Creare risorse dove non esistono, nelle regioni governate da AWS Control Tower ..	294
Fase 7: Registrazione dell'unità organizzativa con AWS Control Tower	296
Factory account	296
Permissions	297
Considerazioni relative all'account	297
Aggiorna e sposta gli account	298
Modificare l'indirizzo email di un account registrato	299

Modificare il nome di un account registrato	300
Configura le impostazioni di Amazon VPC	301
Annullare la registrazione di un account	303
Chiudi un account	304
Risorse Account Factory	306
Personalizzazione di Account Factory (AFC)	308
Configura per la personalizzazione	310
Crea un account personalizzato partendo da un blueprint	317
Personalizza gli account con AFC man mano che li registri	318
Aggiungi un blueprint a un account AWS Control Tower	319
Aggiorna un blueprint	319
Rimuovi un blueprint da un account	320
Progetti dei partner	321
Considerazioni sulle personalizzazioni di Account Factory (AFC)	321
In caso di errore del blueprint	322
Personalizzazione del documento programmatico per i progetti AFC in base a CloudFormation	323
Sono necessarie autorizzazioni aggiuntive per creare un Terraform-based prodotto Service Catalog	325
Transizione al tipo di prodotto esterno	326
AWS Control Tower Account Factory per Terraform (AFT)	327
Prerequisiti	328
Panoramica di AFT	329
Implementa AFT	332
Fornisci un nuovo account	341
Richieste multiple relative all'account	343
Aggiorna un account esistente	344
Versioni supportate	346
Abilita le opzioni delle funzionalità	350
Risorse per AFT	354
Ruoli richiesti	359
Servizi relativi ai componenti	363
Pipeline di provisioning degli account AFT	365
Personalizzazioni dell'account	368
Trigger di personalizzazione	376
VCS alternativo	379

Protezione dei dati	383
Rimuovere un account	384
Parametri operativi	386
Guida alla risoluzione dei problemi	387
Deviazione	392
Rilevamento della deriva	392
Visualizzazione della deriva	394
Risolvere la deriva	394
Considerazioni sulla deriva e sulla scansione delle politiche	396
Tipi di deriva da risolvere immediatamente	397
Modifiche riparabili alle risorse	398
Drift e fornitura di nuovi account	398
Tipi di deriva della governance	399
Account membro trasferito	401
Account membro rimosso	403
Aggiornamento non pianificato a SCP gestito	404
SCP scollegato dall'unità organizzativa gestita	405
Foundational OU eliminata	406
Deriva di controllo CSPM del Security Hub	407
Controlla la deriva delle politiche	408
Accesso affidabile disabilitato	409
Deriva dell'ereditarietà sulle linee di base abilitate	410
Modifica dell'ereditarietà sui controlli abilitati	411
EventBridge creazione	413
Se gestisci risorse all'esterno di AWS Control Tower	414
Facendo riferimento a risorse esterne a AWS Control Tower	416
Modifica esterna dei nomi delle risorse di AWS Control Tower	416
Eliminazione dell'unità organizzativa di sicurezza	417
Rimozione di un account dall'unità organizzativa di sicurezza	418
Modifiche esterne che vengono aggiornate automaticamente	420
Organizations	423
Procedura guidata: video	424
Argomenti	424
Estendere la governance a un'organizzazione esistente	424
Video: abilita una zona di atterraggio esistente AWS Organizations	426
Considerazioni per IAM Identity Center e le organizzazioni esistenti	426

Accesso ad altri AWS services	426
Unità organizzative annidate	426
Procedura guidata: video	427
Espandi da una struttura OU piatta a una struttura OU annidata	427
Controlli preliminari della registrazione dell'unità organizzativa Nested	428
Unità organizzative e ruoli annidati	428
Cosa succede durante la registrazione e la nuova registrazione delle unità organizzative e degli account annidati	429
Considerazioni sulla registrazione dell'unità organizzativa annidata	429
Limiti dell'unità organizzativa annidata	430
Unità organizzative annidate e conformità	430
Unità organizzative annidate e deriva	431
Unità operative e controlli annidati	431
Unità organizzative annidate e radice	433
Registra un'unità organizzativa per registrare più account	433
Registrare un'unità organizzativa esistente	435
Crea una nuova unità organizzativa	437
Rimuovere un'unità organizzativa	438
Cause comuni di errore durante la registrazione o la nuova registrazione	439
Aggiorna le organizzazioni	442
Quando aggiornare le unità organizzative e gli account	442
Aggiorna più account in un'unica unità organizzativa	442
Cosa succede durante la nuova registrazione	443
Aggiorna un singolo account	444
Trasferisci un account	445
Prerequisiti	445
Fase 1: Annullare la registrazione dell'account da AWS Control Tower	445
Fase 2: Trasferire l'account all'organizzazione di destinazione	446
Fase 3: Registrare l'account nell'organizzazione di destinazione	446
Ulteriori considerazioni	446
Servizi integrati	448
AWS Backup	448
CloudFormation	449
CloudTrail	449
CloudWatch	449
AWS Config	450

Integrazione di AWS Config nella Control Tower Landing Zone 4.0	450
AWS Identity and Access Management	453
AWS Key Management Service	453
AWS Lambda	454
AWS Organizations	454
Considerazioni	455
Simple Storage Service (Amazon S3)	455
Security Hub CSPM	455
AWS Service Catalog	455
Amazon SNS	456
Funzioni Step	457
Gestione dell'identità e degli accessi	458
Autenticazione	458
Controllo accessi	460
IAM Identity Center e AWS Control Tower	461
Gruppi di utenti, ruoli e set di autorizzazioni	462
Cose da sapere sugli account IAM Identity Center e AWS Control Tower	463
Gruppi IAM Identity Center per AWS Control Tower	463
Panoramica sulla gestione dell'accesso alle risorse con IAM	467
Risorse e operazioni di AWS Control Tower	468
Informazioni sulla proprietà delle risorse	468
Gestisci l'accesso alle risorse	469
Specifica gli elementi delle policy: azioni, effetti e principi	479
Specifica delle condizioni in una policy	480
Previene attacchi confusi tra vice	480
Politiche IAM per AWS Control Tower	481
Autorizzazioni necessarie per utilizzare la console AWS Control Tower	481
AWS ControlTowerAdmin ruolo	483
AWS ControlTowerServiceRolePolicy	484
AWS ControlTowerIdentityCenterManagementPolicy	485
AWS ControlTowerStackSetRole	485
AWS ControlTowerCloudTrailRolePolicy	486
AWS ControlTowerBlueprintAccess requisiti di ruolo	488
AWSServiceRoleForAWSControlTower	489
AWS ControlTowerAccountServiceRolePolicy	490
Policy gestite per AWS Control Tower	490

Sicurezza	502
Protezione dei dati	502
Crittografia dei dati inattivi	504
Crittografia in transito	504
Limitazione dell'accesso ai contenuti	504
Convalida della conformità	504
Resilienza	505
Sicurezza dell'infrastruttura	506
Registrazione di log e monitoraggio	507
Informazioni sulla registrazione in AWS Control Tower	508
Policy del bucket S3	509
Landing zone versione 3.3 e precedenti	509
Landing zone versione 4.0 e successive	511
Panoramica del monitoraggio	514
Registrazione delle azioni di AWS Control Tower con AWS CloudTrail	515
Informazioni su AWS Control Tower in CloudTrail	515
Esempio: voci del file di registro di AWS Control Tower	517
Monitora le modifiche alle risorse con AWS Config	519
Gestisci i costi di Config	520
Visualizza il AWS Config dati del registratore sugli account registrati	521
Risoluzione dei problemi AWS Config in AWS Control Tower	522
Eventi del ciclo di vita	523
CreateManagedAccount	528
UpdateManagedAccount	529
EnableGuardrail	530
DisableGuardrail	532
SetupLandingZone	533
UpdateLandingZone	535
RegisterOrganizationalUnit	537
DeregisterOrganizationalUnit	538
PrecheckOrganizationalUnit	539
EnableBaseline	541
ResetEnabledBaseline	543
UpdateEnabledBaseline	544
DisableBaseline	545
EnableControl	547

ResetEnabledControl	548
UpdateEnabledControl	550
DisableControl	551
Notifiche all'utente	552
Backup	555
Prerequisiti	556
Abilitare i backup	558
Prima parte: configura i backup per la tua landing zone	558
Parte successiva: abilitare i backup sulle unità organizzative	560
Disattiva i backup	562
Primo passaggio: disattivare i backup sulle unità organizzative	562
Passaggio successivo: spegnere AWS Backup per la tua landing zone	563
Account spostati	564
Deriva di Backup	564
Risorse di Backup	565
Controlli per AWS Backup	569
Smantellamento di una landing zone	570
Panoramica del processo di smantellamento	571
Come disattivare una landing zone	572
Disattiva la tua landing zone con le API	573
Attività di pulizia manuale necessarie dopo la disattivazione	574
Risorse non rimosse durante la disattivazione	575
Rimuovi le risorse AWS Control Tower	578
Ho bisogno della disattivazione anziché dell'eliminazione?	579
Informazioni sulla rimozione delle risorse AWS Control Tower	580
Eliminare SCPs	580
Elimina e impila StackSets	581
Eliminare i bucket Amazon S3 nell'account Log Archive	582
Rimuovi un portafoglio e un prodotto Account Factory	583
Rimuovi i ruoli e le policy di AWS Control Tower	584
Guida alle risorse AWS Control Tower	586
Configurazione dopo la disattivazione di una landing zone	586
Procedure guidate	588
Procedura dettagliata: passa da ALZ a AWS Control Tower	588
Procedura dettagliata: configura AWS Control Tower senza un VPC	588
Elimina il VPC di AWS Control Tower	589

Facoltativamente, pulisci la risorsa VPC nell'account	590
Crea un account in AWS Control Tower senza un VPC	590
Procedura dettagliata: configura gruppi di sicurezza in AWS Control Tower con AWS Firewall Manager	591
Configura i gruppi di sicurezza con AWS Firewall Manager	592
Risoluzione dei problemi	593
Avvio della landing zone non riuscito	593
Aggiornamento della zona di atterraggio non riuscito con errore KMS	594
Impossibile aggiornare la zona di atterraggio	595
Errore relativo alla zona di atterraggio non aggiornata	596
Provisioning del nuovo account non riuscito	597
Registrazione di un account esistente non riuscita	598
Impossibile aggiornare un account di Factory Account	598
Errore, errore che menziona AWS Config	600
Errore nel portafoglio AWS Control Tower Account Factory	602
È stato ricevuto un errore di autorizzazioni insufficienti	602
I controlli investigativi non hanno effetto sugli account	603
Frequenza superata (errore restituito dal AWS Organizations "Hello, World!"	603
Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower	604
AWS Supporto	606
Baseline	607
Tipi di base applicabili a livello di unità organizzativa	607
Tipi di base che si applicano agli account di integrazione dei servizi durante la configurazione delle landing zone	609
Iscrizione parziale	611
Confronta console e API	611
Linee di base e account dei membri abilitati	612
Linee di base e impostazioni predefinite per il controllo delle versioni	613
AWSControlTowerBaseline tabella	613
Esempi: registrazione di un'unità organizzativa AWS Control Tower solo con API	618
Esempi di API di base	620
DisableBaseline	620
EnableBaseline	621
GetBaseline	623
GetBaselineOperation	624

GetEnabledBaseline	624
ListBaselines	625
ListEnabledBaselines	627
ResetEnabledBaseline	632
UpdateEnabledBaseline	632
Informazioni aggiuntive	634
Tutorial e laboratori	634
Rete	207
Sicurezza, identità e registrazione	635
Distribuzione delle risorse e gestione dei carichi di lavoro	636
Lavorare con organizzazioni e account esistenti	636
Automazione e integrazione	636
Migrazione dei carichi di lavoro	637
Servizi AWS correlati	637
Marketplace AWS soluzioni	638
Note di rilascio	639
gennaio 2026 - Presente	639
Account Factory for Terraform (AFT) supporta le esecuzioni di personalizzazione solo in base al piano	639
AWS Control Tower disponibile nel cloud sovrano europeo	640
gennaio 2025 - dicembre 2025	640
Zona di destinazione di AWS Control Tower versione 4.0	641
AWS Control Tower ne aggiunge altri 279 AWS Config controlli per Control Catalog	643
AWS Control Tower è disponibile nella regione Asia Pacifico (Nuova Zelanda)	643
AWS Control Tower supporta la registrazione automatica degli account	643
AWS Control Tower aggiorna la versione Python	644
AWS Control Tower riduce la deriva	644
AWS Control Tower supporta gli indirizzi IPv6	645
Disponibile la versione 1.15.0 di Account Factory per Terraform	645
Controlli aggiornati con tipi di istanza Nitro	645
AWS Control Tower è disponibile nella regione Asia Pacifico (Taipei)	647
AWS Control Tower supporta PrivateLink	647
Supporto per framework di settore aggiuntivi, metadati aggiornati	647
Service-linked AWS Config controlli	648
La visualizzazione della console dei controlli abilitati offre una visibilità centralizzata	650

Account Factory for Terraform (AFT) supporta nuove configurazioni in fase di distribuzione	650
AWS Control Tower introduce la reportistica a livello di account per le API di base	651
AWS Control Tower è disponibile in AWS Regioni dell'Asia Pacifico (Thailandia) e del Messico (centrale)	651
Aggiuntivo AWS Config controlli disponibili	652
Annulla la registrazione e l'eliminazione delle azioni per le unità organizzative	652
Control Catalog supporta gli indirizzi IPv6	653
gennaio - dicembre 2024	653
Supporti GitHub AWS Control Tower cFCT e RCP	654
AWS Control Tower aggiunge controlli preventivi con policy dichiarative	654
AWS Control Tower aggiunge opzioni di piano di backup prescrittive	655
AWS Control Tower si integra AWS Config controlli	655
AWS Control Tower migliora la gestione degli hook e aggiunge regioni di controllo proattive	655
AWS Control Tower lancia politiche di controllo delle risorse gestite	656
AWS Control Tower segnala una deriva delle politiche di controllo	657
Nuova API ResetEnabledControl	657
API di controllo degli aggiornamenti del catalogo GetControl	658
AWS Control Tower AFT supporta GitLab	658
AWS Control Tower è disponibile in AWS Regione Asia Pacifico (Malesia)	658
AWS Control Tower supporta fino a 1000 account per unità organizzativa	659
AWS Control Tower aggiunge la selezione della versione della zona di destinazione	659
API di controllo descrittiva disponibile, accesso esteso a regioni e controlli	660
AWS Control Tower supporta AFT e cFCT nelle regioni opt-in	661
AWS Control Tower aggiunge l'API ListLandingZoneOperations	661
AWS Control Tower supporta fino a 100 operazioni di controllo simultanee	661
AWS Control Tower è disponibile in AWS Canada occidentale (Calgary)	662
AWS Control Tower supporta l'adeguamento delle quote in modalità self-service	663
AWS Control Tower rilascia il Guida di riferimento ai controlli	664
AWS Control Tower aggiorna e rinomina due controlli proattivi	664
I controlli obsoleti non sono più disponibili	665
AWS Control Tower supporta l'etichettatura EnabledControl delle risorse in CloudFormation	665
AWS Control Tower supporta le API per la registrazione e la configurazione delle unità organizzative con linee di base	666

gennaio - dicembre 2023	667
Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 3)	668
Zona di destinazione di AWS Control Tower versione 3.3	669
Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 2)	670
AWS Control Tower annuncia i controlli per agevolare la sovranità digitale	670
API per le zone di destinazione di AWS Control Tower	673
API di tagging di controllo di AWS Control Tower	674
AWS Control Tower è disponibile in AWS Asia Pacifico (Melbourne)	674
Transizione verso una nuova AWS Service Catalog Tipo di prodotto esterno (fase 1)	674
AWS Control Tower aggiunge una nuova API di controllo	675
AWS Control Tower aggiunge nuovi controlli	675
AWS Control Tower rileva una deriva attendibile degli accessi	675
AWS Control Tower è disponibile in quattro versioni aggiuntive Regioni AWS	676
AWS Control Tower è disponibile in AWS Israele (Tel Aviv)	676
AWS Control Tower aggiunge 28 nuovi controlli proattivi	676
AWS Control Tower rende obsoleti due controlli	677
Zona di destinazione di AWS Control Tower versione 3.2	677
AWS Control Tower aggiunge la mappatura da email a ID per IAM Identity Center	679
AWS Control Tower ne aggiunge altre AWS Security Hub CSPM controlli	679
AWS Control Tower pubblica metadati per AWS Security Hub CSPM controlli	680
AWS Control Tower aggiunge Account Factory Customization (AFC) per Terraform	680
AWS Control Tower aggiunge un centro di identità IAM autogestito	680
AWS Control Tower aggiunge una nota di governance mista	681
AWS Control Tower aggiunge nuovi controlli proattivi	681
AWS Control Tower aggiorna i controlli Amazon EC2	681
AWS Control Tower è disponibile in sette versioni aggiuntive Regioni AWS	682
AWS Control Tower Account Factory Customization (AFC) e tracciamento delle richieste sono generalmente disponibili	682
Zona di destinazione di AWS Control Tower versione 3.1	682
I controlli proattivi di AWS Control Tower sono generalmente disponibili	684
gennaio - dicembre 2022	684
Operazioni simultanee sugli account	685
Personalizzazione dell'account di fabbrica (AFC)	685
I controlli completi aiutano a AWS approvvigionamento e gestione delle risorse	686
Stato di conformità visualizzabile per tutti AWS Config rules	687
API per i controlli e una nuova CloudFormation risorsa	687

cFCT supporta l'eliminazione di set di stack	688
Conservazione personalizzata dei log	689
È disponibile la riparazione di Role Drift	689
Zona di destinazione AWS Control Tower versione 3.0	689
La pagina Organizzazione combina le visualizzazioni delle unità organizzative e degli account	693
Creazione e registrazione dell'account semplificate	694
AFT supporta la personalizzazione automatica per gli account AWS Control Tower condivisi	694
Operazioni simultanee per tutti i controlli opzionali	695
Account di sicurezza e registrazione esistenti	696
Zona di destinazione di AWS Control Tower versione 2.9	696
Zona di destinazione di AWS Control Tower versione 2.8	697
gennaio - dicembre 2021	698
Funzionalità di negazione delle regioni	698
Funzionalità di residenza dei dati	699
AWS Control Tower introduce il provisioning e la personalizzazione degli account Terraform	699
È disponibile un nuovo evento sul ciclo di vita	700
AWS Control Tower abilita le unità organizzative annidate	700
Concorrenza del controllo investigativo	701
Sono disponibili due nuove regioni	702
Deselezione della regione	702
AWS Control Tower funziona con AWS Sistemi di gestione delle chiavi	703
Controlli rinominati, funzionalità invariata	704
AWS Control Tower esegue quotidianamente la scansione degli SCP per verificare eventuali deviazioni	704
Nomi personalizzati per unità organizzative e account	704
Zona di atterraggio AWS Control Tower versione 2.7	705
Tre nuovi AWS Regioni disponibili	707
Governa solo le regioni selezionate	707
AWS Control Tower ora estende la governance alle unità organizzative esistenti nel tuo AWS organizations	708
AWS Control Tower fornisce aggiornamenti in blocco degli account	708
gennaio - dicembre 2020	709
La console AWS Control Tower ora si collega a siti esterni AWS Regole di configurazione ..	709

AWS Control Tower è ora disponibile in regioni aggiuntive	710
Aggiornamento Guardrail	710
La console AWS Control Tower mostra ulteriori dettagli sulle unità organizzative e sugli account	711
Usa AWS Control Tower per configurare nuovi account multipli AWS ambienti in AWS Organizations	711
Personalizzazioni per la soluzione AWS Control Tower	712
Disponibilità generale della versione 2.3 di AWS Control Tower	713
Single-step provisioning degli account in AWS Control Tower	713
Strumento di smantellamento di AWS Control Tower	714
Notifiche degli eventi del ciclo di vita di AWS Control Tower	714
giugno - dicembre 2019	715
Disponibilità generale della versione 2.2 di AWS Control Tower	715
Nuovi controlli elettivi in AWS Control Tower	716
Nuovi controlli investigativi in AWS Control Tower	716
AWS Control Tower accetta indirizzi e-mail per account condivisi con domini diversi rispetto all'account di gestione	717
Disponibilità generale della versione 2.1 di AWS Control Tower	717
Cronologia dei documenti	719
AWS Glossario	742
.....	dccxlili

Cos'è AWS Control Tower?

AWS Control Tower offre un modo semplice per configurare e governare un ambiente con AWS più account, seguendo le migliori pratiche prescrittive. AWS Control Tower orchestra le funzionalità di diversi altri [AWS servizi](#), tra cui e AWS Organizations AWS Service Catalog Centro identità AWS IAM, per creare una zona di atterraggio in meno di un'ora. Le risorse vengono configurate e gestite per tuo conto.

L'orchestrazione di AWS Control Tower estende le funzionalità di AWS Organizations. Per evitare che le tue organizzazioni e i tuoi account si discostino dalle best practice, AWS Control Tower applica dei controlli (a volte chiamati guardrail). Ad esempio, puoi utilizzare i controlli per garantire che i log di sicurezza e le necessarie autorizzazioni di accesso tra account vengano creati e non modificati.

Se stai ospitando più di una manciata di account, è utile disporre di un livello di orchestrazione che faciliti la distribuzione e la governance degli account. Puoi adottare AWS Control Tower come metodo principale per il provisioning di account e infrastrutture. Con AWS Control Tower, puoi aderire più facilmente agli standard aziendali, soddisfare i requisiti normativi e seguire le migliori pratiche.

AWS Control Tower consente agli utenti finali dei team distribuiti di effettuare rapidamente il provisioning di nuovi AWS account, tramite modelli di account configurabili in Account Factory. Nel frattempo, gli amministratori centrali del cloud possono monitorare che tutti gli account siano allineati alle politiche di conformità stabilite a livello aziendale.

In breve, AWS Control Tower offre il modo più semplice per configurare e gestire un AWS ambiente sicuro, conforme e con più account basato sulle migliori pratiche stabilite collaborando con migliaia di aziende. Per ulteriori informazioni sulla collaborazione con AWS Control Tower e sulle best practice delineate nella strategia multi-account, consulta AWS . [AWS strategia multi-account: linee guida sulle migliori pratiche](#)

Funzionalità

AWS Control Tower ha le seguenti caratteristiche:

- Zona di atterraggio: una zona di atterraggio è un ambiente <https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/appendix-e-establish-multi-account.html#example-workloads-flat-structure> multi-account ben progettato basato sulle migliori

pratiche di sicurezza e conformità. È il contenitore a livello aziendale che contiene tutte le unità organizzative (OU), gli account, gli utenti e le altre risorse che desideri siano soggette alle normative di conformità. Una landing zone può essere ridimensionata per soddisfare le esigenze di un'azienda di qualsiasi dimensione.

- **Controlli:** un controllo (a volte chiamato *guardrail*) è una regola di alto livello che fornisce una governance continua per l'intero ambiente. AWS È espresso in linguaggio normale. Esistono tre tipi di controlli: preventivo, investigativo e proattivo. Ai controlli si applicano tre categorie di linee guida: obbligatori, fortemente consigliati o elettivi. Per ulteriori informazioni sui controlli, vedere [Come funzionano i controlli](#).
- **Account Factory:** un Account Factory è un modello di account configurabile che aiuta a standardizzare il provisioning di nuovi account con configurazioni di account preapprovate. AWS Control Tower offre un Account Factory integrato che aiuta ad automatizzare il flusso di lavoro di provisioning degli account nell'organizzazione. Per ulteriori informazioni, consulta [Fornisci e gestisci gli account con Account Factory](#).
- **Dashboard:** la dashboard offre una supervisione continua della tua zona di destinazione al tuo team di amministratori cloud centrali. Usa la dashboard per visualizzare gli account a cui è stato assegnato il provisioning in tutta l'azienda, i controlli abilitati per l'applicazione delle policy, i controlli abilitati per il rilevamento continuo delle non conformità alle policy e le risorse non conformi organizzate per account e unità organizzative.

In che modo AWS Control Tower interagisce con gli altri AWS services

AWS Control Tower si basa su AWS servizi affidabili e affidabili AWS Service Catalog, tra cui Centro identità AWS IAM, e AWS Organizations. Per ulteriori informazioni, consulta [Servizi integrati](#).

Puoi incorporare AWS Control Tower con altri AWS servizi in una soluzione che ti aiuti a migrare i carichi di lavoro esistenti verso. AWS Per ulteriori informazioni, consulta [Come sfruttare AWS Control Tower e CloudEndure migrare i carichi di lavoro verso. AWS](#)

Configurazione, governance ed estensibilità

- **Configurazione automatica degli account:** AWS Control Tower automatizza la distribuzione e la registrazione degli account tramite un Account Factory (o «distributore automatico»), creato come un'astrazione sulla base dei prodotti forniti in. AWS Service Catalog Account Factory può creare e registrare AWS account e automatizza il processo di applicazione di controlli e policy a tali

account. Per ulteriori informazioni sulla creazione e il provisioning degli account, consulta [Metodi di provisioning](#).

- **Governance centralizzata:** utilizzando le funzionalità di AWS Organizations, AWS Control Tower crea un framework che garantisce conformità e governance coerenti in tutto l'ambiente con più account. Il AWS Organizations servizio fornisce funzionalità essenziali per la gestione di un ambiente con più account, tra cui governance e gestione centralizzate degli account, creazione di account dalle AWS Organizations API, politiche di controllo dei servizi (SCP) e politiche di controllo delle risorse (RCP).
- **Estensibilità:** puoi creare o estendere il tuo ambiente AWS Control Tower lavorando direttamente nella console AWS Control Tower e nella AWS Organizations stessa. Puoi vedere le modifiche riflesse in AWS Control Tower dopo aver registrato le organizzazioni esistenti e aver registrato i tuoi account esistenti in AWS Control Tower. Puoi aggiornare la zona di destinazione di AWS Control Tower per riflettere le modifiche. Se i carichi di lavoro richiedono ulteriori funzionalità avanzate, puoi sfruttare altre soluzioni dei AWS partner insieme ad AWS Control Tower.

Sei un First-Time utente di AWS Control Tower?

Se è la prima volta che utilizzi questo servizio, ti consigliamo di leggere le informazioni seguenti:

1. Se hai bisogno di ulteriori informazioni su come pianificare e organizzare la tua zona di atterraggio, consulta [Pianifica la tua landing zone di AWS Control Tower](#) e [AWS strategia multi-account per la tua landing zone di AWS Control Tower](#).
2. Se sei pronto per creare la tua prima landing zone, consulta [Guida introduttiva a AWS Control Tower](#).
3. Per informazioni sul rilevamento e la prevenzione della deviazione, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).
4. Per informazioni dettagliate sulla sicurezza, consulta [Sicurezza in AWS Control Tower](#).
5. Per informazioni sull'aggiornamento della zona di atterraggio e degli account dei membri, consulta [Gestione degli aggiornamenti di configurazione in AWS Control Tower](#).

Come funziona AWS Control Tower

Questa sezione descrive in modo approfondito come funziona AWS Control Tower. La tua landing zone è un ambiente multi-account ben progettato per tutte le tue risorse. AWS Puoi utilizzare questo ambiente per applicare le normative di conformità su tutti i tuoi account. AWS

Struttura di una zona di atterraggio AWS Control Tower

La struttura di una landing zone in AWS Control Tower è la seguente:

- Root: l'elemento principale che contiene tutte le altre unità organizzative presenti nella landing zone.
- Unità organizzativa di sicurezza: quando avvii la landing zone, puoi scegliere nomi personalizzati per gli account nell'unità organizzativa di sicurezza e puoi portare AWS gli account esistenti in AWS Control Tower per le integrazioni di servizi.

Nella versione 3.3 e precedenti della landing zone di AWS Control Tower, questa unità organizzativa contiene gli account Log Archive e Audit. Questi account sono chiamati account condivisi. Nella versione 3.3 e precedenti di landing zone, non è possibile aggiungere account esistenti per la sicurezza e la registrazione dopo il lancio iniziale.

Nella versione 4.0 della landing zone di AWS Control Tower, AWS Control Tower non richiede più un'unità organizzativa di sicurezza ed è possibile definire la propria struttura organizzativa.

- Sandbox OU: l'OU Sandbox viene creata all'avvio della landing zone, se la abiliti. Questa e altre unità organizzative registrate contengono gli account registrati con cui gli utenti lavorano per eseguire i propri carichi di lavoro. AWS
- Directory IAM Identity Center: per impostazione predefinita, questa directory ospita gli utenti di IAM Identity Center. Definisce l'ambito delle autorizzazioni per ogni utente IAM Identity Center. Facoltativamente, puoi scegliere di gestire automaticamente la tua identità e il controllo degli accessi. Per ulteriori informazioni, consulta [Working with AWS IAM Identity Center e AWS Control Tower](#).
- Utenti IAM Identity Center: queste sono le identità che i tuoi utenti possono assumere per eseguire i loro AWS carichi di lavoro nella tua landing zone.

Cosa succede quando configuri una landing zone

Quando configuri una landing zone, AWS Control Tower esegue le seguenti azioni nel tuo account di gestione per tuo conto:

- Quando crei una landing zone tramite la console, AWS Control Tower crea due unità AWS Organizations organizzative (OU). Si tratta dell'unità organizzativa di sicurezza e dell'unità organizzativa Sandbox opzionale, contenute nella struttura principale dell'organizzazione. Durante la configurazione, AWS Control Tower seleziona automaticamente l'unità organizzativa di sicurezza come unità organizzativa predefinita per le integrazioni di servizi. Questa unità organizzativa è nota come unità organizzativa designata per l'integrazione dei servizi. È possibile selezionare un'unità organizzativa diversa durante la configurazione della landing zone.

AWS Control Tower richiede che tutti gli account configurati per le integrazioni di AWS servizi si trovino nella stessa unità organizzativa, annidati direttamente in root. Questo requisito non si applica all'account di gestione.

Quando crei la landing zone tramite l'API, non selezioni esplicitamente un'unità organizzativa per le integrazioni di servizi. Gli account di integrazione dei servizi devono trovarsi nella stessa unità organizzativa annidata direttamente in root e l'unità organizzativa che contiene gli account di integrazione dei servizi è l'unità organizzativa di integrazione del servizio designata. Per ulteriori informazioni, consulta [Getting started with AWS Control Tower API](#).

- AWS Control Tower crea o registra account per qualsiasi integrazione di servizi abilitata (ad esempio AWS Config AWS CloudTrail, o AWS Backup) nell'unità organizzativa di integrazione del servizio designata.
- Crea una directory nativa per il cloud in IAM Identity Center, con gruppi preconfigurati e accesso Single Sign-On, se scegli la configurazione AWS Control Tower predefinita o ti consente di gestire autonomamente il tuo provider di identità.
- Applica tutti i controlli preventivi obbligatori per far rispettare le politiche.
- Applica tutti i controlli obbligatori e investigativi per rilevare le violazioni della configurazione.
- I controlli preventivi non vengono applicati all'account di gestione.
- Ad eccezione dell'account di gestione, i controlli vengono applicati all'intera organizzazione.

Gestione sicura delle risorse all'interno della zona di destinazione e degli account AWS Control Tower

- Quando crei la landing zone, vengono create diverse AWS risorse. Per utilizzare AWS Control Tower, non devi modificare o eliminare queste risorse gestite da AWS Control Tower al di fuori dei metodi supportati descritti in questa guida. L'eliminazione o la modifica di queste risorse farà sì che la tua landing zone entri in uno stato sconosciuto. Per maggiori dettagli, consultare [Linee guida per la creazione e la modifica delle risorse AWS Control Tower](#).
- Quando abiliti i controlli opzionali (quelli con linee guida fortemente consigliate o facoltative), AWS Control Tower crea AWS risorse che gestisce nei tuoi account. Non modificare o eliminare risorse create da AWS Control Tower. Ciò può far sì che i controlli entrino in uno stato sconosciuto.

Cosa sono gli account condivisi?

In AWS Control Tower, gli account condivisi nella landing zone vengono forniti durante la configurazione: l'account di gestione, l'account di archiviazione dei log e l'account di audit.

Cos'è l'account di gestione?

Questo è l'account che hai creato appositamente per la tua landing zone. Questo account viene utilizzato per la fatturazione di tutto ciò che si trova nella tua landing zone. Viene anche utilizzato per la fornitura di account da parte di Account Factory, nonché per gestire le unità organizzative e i controlli.

Note

Non è consigliabile eseguire alcun tipo di carico di lavoro di produzione da un account di gestione AWS Control Tower. Crea un account AWS Control Tower separato per eseguire i tuoi carichi di lavoro.

Per ulteriori informazioni, consulta [Gestione dell'account](#).

Cos'è l'account di archiviazione dei log?

Questo account funge da archivio per i registri delle attività delle API e delle configurazioni delle risorse di tutti gli account nella landing zone.

Per ulteriori informazioni, consulta [CloudTrail account amministratore](#).

Cos'è l'account di controllo?

L'account di controllo è un account con restrizioni progettato per consentire ai team di sicurezza e conformità l'accesso in lettura e scrittura a tutti gli account nella landing zone. L'account di audit fornisce l'accesso programmatico per la revisione degli account mediante un ruolo concesso solo alle funzioni Lambda. L'account di audit non consente di accedere manualmente ad altri account. Per ulteriori informazioni sulle funzioni e i ruoli Lambda, consulta [Configurare una funzione Lambda per assumere un ruolo da un'altra](#). Account AWS

Per ulteriori informazioni, consulta [Account aggregatore Config](#).

Come funzionano i controlli

Il controllo è una regola di alto livello che fornisce una governance continua per l'intero AWS ambiente. Ogni controllo applica una singola regola ed è espressa in un linguaggio semplice. Puoi modificare i controlli opzionali o fortemente consigliati in vigore, in qualsiasi momento, dalla console AWS Control Tower o dalle API AWS Control Tower. I controlli obbligatori vengono sempre applicati e non possono essere modificati.

I controlli preventivi impediscono il verificarsi di azioni. Ad esempio, il controllo elettivo denominato Disallow Changes to Bucket Policy per Amazon S3 Buckets (precedentemente chiamato Disallow Policy Changes to Log Archive) impedisce qualsiasi modifica alla policy IAM all'interno dell'account condiviso dell'archivio di log. Gli eventuali tentativi di esecuzione di un'operazione non consentita vengono rifiutati e registrati in CloudTrail. Anche la risorsa è connessa. AWS Config

I controlli Detective rilevano eventi specifici quando si verificano e registrano l'azione CloudTrail. Ad esempio, il controllo fortemente consigliato chiamato Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances rileva se un volume Amazon EBS non crittografato è collegato a un'istanza EC2 nella tua landing zone.

I controlli proattivi verificano se le risorse sono conformi alle politiche e agli obiettivi aziendali, prima che le risorse vengano assegnate ai vostri account. Se le risorse non sono conformi, non vengono fornite. I controlli proattivi monitorano le risorse che verrebbero distribuite nei tuoi account tramite modelli. CloudFormation

Per chi conosce AWS: In AWS Control Tower i controlli preventivi sono implementati con policy di controllo dei servizi (SCP) e politiche di controllo delle risorse (RCP). I controlli investigativi sono implementati con AWS Config regole. I controlli proattivi sono implementati con CloudFormation ganci.

Argomenti correlati

- [Rileva e risolvi la deriva in AWS Control Tower](#)

Come funziona AWS Control Tower con StackSets

CloudFormation StackSets Per impostazione predefinita, AWS Control Tower utilizza per configurare le risorse nei tuoi account. Ogni set di stack StackInstances corrisponde agli account e ai singoli Regioni AWS account. AWS Control Tower distribuisce un'istanza di stack set per account e regione.

AWS Control Tower applica gli aggiornamenti a determinati account e Regioni AWS in modo selettivo, in base a CloudFormation parametri. Quando gli aggiornamenti vengono applicati ad alcune istanze dello stack, altre istanze dello stack potrebbero essere lasciate in stato Outdated (Obsoleto). Questo comportamento è previsto e normale.

Quando un'istanza dello stack entra nello stato Outdated (Obsoleto) in genere significa che lo stack corrispondente a quell'istanza non è allineato con il modello più recente nel set di stack. Lo stack rimane nel modello precedente, quindi potrebbe non includere le risorse o i parametri più recenti. Lo stack è comunque completamente utilizzabile.

Ecco un breve riepilogo del comportamento da aspettarsi, in base ai CloudFormation parametri specificati durante un aggiornamento:

Se l'aggiornamento del set di stack include modifiche al modello (ovvero, se sono specificate TemplateURL le proprietà TemplateBody o) o se la Parameters proprietà è specificata, CloudFormation contrassegna tutte le istanze dello stack con lo stato Obsoleto prima di aggiornare le istanze dello stack negli account specificati e. Regioni AWS Se l'aggiornamento del set di stack non include modifiche al modello o ai parametri, CloudFormation aggiorna le istanze dello stack negli account e nelle regioni specificati, lasciando a tutte le altre istanze dello stack lo stato di istanza dello stack esistente. Per aggiornare tutte le istanze dello stack associate a un set di stack, non specificare le proprietà Regions o Accounts.

Per ulteriori informazioni, consulta [Update Your Stack Set nella Guida per l'utente](#). CloudFormation

Terminologia

Ecco una breve panoramica di alcuni termini che troverai nella documentazione di AWS Control Tower.

Innanzitutto, è utile sapere che AWS Control Tower condivide molta terminologia con il AWS Organizations servizio, inclusi i termini *organizzazione* e *unità organizzativa (OU)*, che compaiono in questo documento.

- Per ulteriori informazioni su organizzazioni e unità organizzative, consulta [AWS Organizations terminologia e concetti](#). Se non conosci AWS Control Tower, questa terminologia è un buon punto di partenza.
- [AWS Organizations](#) è un AWS servizio che ti aiuta a governare centralmente il tuo ambiente man mano che cresci e scali i tuoi carichi di lavoro. AWS AWS Control Tower si basa sulla creazione AWS Organizations di account, sull'applicazione dei controlli preventivi a livello di unità organizzativa e per fornire una fatturazione centralizzata.
- Un [AWS account Account Factory](#) è un account fornito tramite AWS Account Factory in AWS Control Tower. A volte, Account Factory viene chiamato informalmente «distributore automatico» per gli account.
- La tua regione [principale di AWS Control Tower](#) è la AWS regione in cui è stata distribuita la tua zona di destinazione di AWS Control Tower. Puoi visualizzare la tua regione di origine nelle impostazioni della tua zona di destinazione.
- [AWS Service Catalog](#) consente di gestire centralmente i servizi IT di uso comune. Nel contesto di questo documento, Account Factory utilizza il provisioning AWS Service Catalog di nuovi AWS account, inclusi gli account basati su modelli personalizzati.
- [AWS CloudFormation StackSets](#) sono un tipo di risorsa che estende la funzionalità degli stack in modo da poter creare, aggiornare o eliminare stack su più account e regioni con un'unica operazione e un unico modello. CloudFormation
- Un [istanza di stack](#) è un riferimento a uno stack in un account target all'interno di una Regione.
- Uno [stack](#) è una raccolta di AWS risorse che puoi gestire come una singola unità.
- Un [aggregatore](#) è un tipo di AWS Config risorsa che raccoglie dati di AWS Config configurazione e conformità da più account e regioni all'interno dell'organizzazione, consentendo di visualizzare e interrogare questi dati di conformità all'interno di un singolo account.
- Un pacchetto di [conformità](#) è una raccolta di AWS Config regole e azioni correttive che possono essere implementate come singola entità in un account e in una regione o in un'organizzazione in.

AWS Organizations Puoi utilizzare un pacchetto di conformità per personalizzare il tuo ambiente AWS Control Tower. Per i blog tecnici che forniscono maggiori dettagli, consulta [Informazioni correlate](#).

- Una linea di [base](#) in AWS Control Tower è costituita da un gruppo di risorse e configurazioni specifiche che è possibile applicare a un obiettivo. L'obiettivo di base più comune può essere un'unità organizzativa (OU). Ad esempio, la linea di base denominata `AWSControlTowerBaseline` è disponibile per aiutarti a registrare le unità organizzative con AWS Control Tower. Durante la configurazione e l'aggiornamento della zona di atterraggio, l'obiettivo di base può essere un account condiviso o un'impostazione specifica per l'intera zona di atterraggio.
- Blueprint: un blueprint è un artefatto che racchiude alcuni metadati, che descrivono i componenti dell'infrastruttura distribuiti all'interno di un account. Ad esempio, un CloudFormation modello può fungere da modello per un account AWS Control Tower.
- Drift: modifica di una risorsa installata e configurata da AWS Control Tower. Le risorse senza deriva consentono ad AWS Control Tower di funzionare correttamente.
- Non-compliant risorsa: una risorsa che viola una AWS Config regola che definisce un particolare controllo investigativo.
- Account condiviso: uno dei tre account che AWS Control Tower crea automaticamente quando si configura la zona di destinazione: l'account di gestione, l'account di archiviazione dei log e l'account di controllo. È possibile scegliere nomi personalizzati per l'account di archiviazione dei log e l'account di controllo durante la configurazione.
- Account membro: un account membro appartiene all'organizzazione AWS Control Tower. L'account membro può essere registrato o annullato in AWS Control Tower. Quando un'unità organizzativa registrata contiene una combinazione di account iscritti e non registrati:
 - I controlli preventivi abilitati (o ereditati da) l'unità organizzativa si applicano a tutti gli account al suo interno, compresi quelli non registrati. Questo è vero perché i controlli preventivi vengono applicati con SCP, RCPS o politiche dichiarative a livello di unità organizzativa, non a livello di account. Per ulteriori informazioni, vedere [Inheritance for service control policy nella documentazione](#). AWS Organizations
 - I controlli investigativi abilitati nell'unità organizzativa non si applicano agli account non registrati.
 - I controlli proattivi sono implementati tramite ganci. AWS CloudFormation Questi controlli non si applicano agli account non registrati in un'unità organizzativa.

Un account può essere membro di una sola organizzazione alla volta e i relativi addebiti vengono fatturati all'account di gestione di tale organizzazione. Un account membro può essere spostato nel contenitore principale di un'organizzazione.

- **AWS account:** un AWS account funge da contenitore di risorse e limite di isolamento delle risorse. Un AWS account può essere associato alla fatturazione e al pagamento. Un AWS account è diverso da un account utente (a volte chiamato account utente [IAM](#)) in AWS Control Tower. Gli account creati tramite il processo di provisioning di Account Factory sono AWS account. AWS gli account possono anche essere aggiunti ad AWS Control Tower tramite un processo di registrazione dell'account o dell'unità organizzativa.
- **Controllo:** un controllo (noto anche come guardrail) è una regola di alto livello che fornisce una governance continua per l'intero ambiente AWS Control Tower. Ogni controllo applica una singola regola. I controlli preventivi sono implementati con politiche di controllo dei servizi (SCP), politiche di controllo delle risorse (RCP) e politiche dichiarative. I controlli investigativi sono implementati con regole. AWS Config I controlli proattivi sono implementati con CloudFormation ganci. Per ulteriori informazioni, consulta [Come funzionano i controlli](#).
- **Control Catalog:** il catalogo di controllo di AWS Control Tower è il compendio di tutti i controlli disponibili tramite AWS Control Tower, nella console e nelle API. In precedenza si chiamava Control Library. Abbiamo allineato la terminologia al nome del namespace, controlcatalog.
- **Zona di destinazione:** una zona di destinazione è un ambiente cloud che offre un punto di partenza consigliato, inclusi account predefiniti, struttura degli account, layout di rete e sicurezza e così via. Da una zona di atterraggio, puoi distribuire carichi di lavoro che utilizzano le tue soluzioni e applicazioni.
- **Framework:** un framework è uno standard normativo specifico o un requisito di settore. Nell'ontologia Control Catalog, un framework è rappresentato da un controllo Standard. Per ulteriori informazioni, vedere la panoramica dell'[ontologia di Control Catalog](#).
- **Unità organizzativa annidata:** un'unità organizzativa annidata in AWS Control Tower è un'unità organizzativa contenuta in un'altra unità organizzativa. Un'unità organizzativa annidata può avere esattamente un'unità organizzativa principale e ogni account può essere membro di esattamente un'unità organizzativa. Le unità organizzative annidate creano una gerarchia. Quando si collega una policy a una delle unità organizzative della gerarchia, questa scorre verso il basso e influisce su tutte le unità organizzative e gli account sottostanti. Una gerarchia di unità organizzative annidate in AWS Control Tower può avere una profondità massima di cinque livelli.

- **Unità organizzativa principale:** l'unità organizzativa immediatamente superiore all'unità organizzativa corrente nella gerarchia. Ogni unità organizzativa può avere esattamente un'unità organizzativa principale.
- **Unità organizzativa secondaria:** qualsiasi unità organizzativa inferiore all'unità organizzativa corrente nella gerarchia. Un'unità organizzativa può avere molte unità organizzative secondarie.
- **Gerarchia delle unità organizzative:** in AWS Control Tower, la gerarchia delle unità organizzative annidate può avere fino a cinque livelli. L'ordine di nidificazione è denominato Livelli. La parte superiore della gerarchia è indicata come Livello 1.
- **Top-level Unità organizzativa** di primo livello è qualsiasi unità organizzativa che si trova direttamente sotto la radice, non la radice stessa. L'unità principale non è considerata un'unità organizzativa.
- **Governata:** una regione governata è gestita e controllata nel tuo ambiente da AWS Control Tower, in base alle politiche di governance stabilite dalla tua organizzazione. Queste Regioni AWS vengono monitorate per aderire alle migliori pratiche e alle politiche organizzative. Le tue risorse in queste regioni sono protette quando abiliti i controlli AWS Control Tower.
- **Non governate:** le regioni che mostrano lo stato Non governato non sono controllate o monitorate da AWS Control Tower. Di Regioni AWS solito non aderiscono alle stesse politiche di governance applicate da AWS Control Tower. È possibile creare risorse in queste regioni, ma tali risorse non sono protette dai controlli AWS Control Tower.
- **Negata:** una regione negata viene bloccata specificamente da AWS Control Tower. All'interno dell'ambiente AWS Control Tower, non è possibile effettuare il provisioning di risorse in questi ambienti Regioni AWS.

Prezzi

Non sono previsti costi aggiuntivi per l'utilizzo di AWS Control Tower. Paghi solo i AWS servizi abilitati da AWS Control Tower e i servizi che utilizzi nella tua zona di destinazione. Ad esempio, paghi Service Catalog per il provisioning degli account con Account Factory e AWS CloudTrail per gli eventi tracciati nella tua zona di atterraggio. Per informazioni sui prezzi e sulle commissioni associati ad AWS Control Tower, consulta i prezzi di [AWS Control Tower](#).

Se esegui carichi di lavoro temporanei da account in AWS Control Tower, potresti riscontrare un aumento dei costi associati a. AWS Config Per informazioni dettagliate, consulta [Prezzi di AWS Config](#). Contatta il rappresentante AWS del tuo account per informazioni più specifiche sulla gestione di questi costi. Per saperne di più su come AWS Config funziona con AWS Control Tower, consulta [Monitora le modifiche alle risorse con AWS Config](#).

Se implementi AWS CloudTrail percorsi al di fuori di AWS Control Tower, puoi utilizzarli con AWS Control Tower. Tuttavia, potresti incorrere in costi duplicati se scegli anche i percorsi gestiti da AWS Control Tower. Non consigliamo di configurare percorsi esterni, a meno che tu non abbia un requisito specifico. Se scegli di attivarlo durante la configurazione o l'aggiornamento della zona di destinazione, AWS Control Tower configura e attiva per te un CloudTrail percorso a livello di organizzazione nell'account di gestione. Per informazioni sulla gestione dei CloudTrail costi, consulta Gestione dei costi. [CloudTrail](#)

Configurazione

Prima di utilizzarlo AWS Control Tower per la prima volta, segui i passaggi in questa sezione per creare un AWS account e proteggere il tuo account di AWS Control Tower gestione. Per informazioni sulle attività di configurazione aggiuntive specifiche per AWS Control Tower, vedere [Guida introduttiva a AWS Control Tower](#).

Registrati per AWS

Iscriviti per un Account AWS

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

Quando ti registri ad Amazon Web Services (AWS), il tuo AWS account viene automaticamente registrato per tutti i servizi in AWS, inclusi AWS Control Tower. Se hai già un AWS account, passa all'attività successiva. Se non disponi di un AWS account, utilizza la procedura seguente per crearne uno.

Annota il numero del tuo AWS account, perché ti serve per altre attività.

Sicurezza per i tuoi account

Puoi trovare ulteriori indicazioni su come impostare le migliori pratiche per proteggere la sicurezza dei tuoi AWS Control Tower account, nella AWS Organizations documentazione.

- [Le migliori pratiche per l'account di gestione](#)
- [Le migliori pratiche per gli account dei membri](#)

Approfondimenti

[Guida introduttiva a AWS Control Tower](#)

Guida introduttiva a AWS Control Tower

Questa procedura introduttiva è destinata agli amministratori di AWS Control Tower. Segui questa procedura quando sei pronto a configurare la tua zona di destinazione utilizzando la console o le API di AWS Control Tower.

Se AWS al momento sei un cliente, ma sei un nuovo utente di AWS Control Tower, potresti voler consultare la sezione chiamata [Pianifica la tua landing zone di AWS Control Tower](#), prima di procedere.

Argomenti

- [Guida introduttiva rapida di AWS Control Tower](#)
- [Prerequisito: controlli automatici prima del lancio per il tuo account di gestione](#)
- [Configurazione dell'ambiente dedicato ai controlli](#)
- [Inizia a usare AWS Control Tower dalla console](#)
- [Inizia a usare AWS Control Tower utilizzando le API](#)
- [Fasi successive](#)

Guida introduttiva rapida di AWS Control Tower

Se sei un principiante AWS, puoi seguire i passaggi in questa sezione per iniziare rapidamente a usare AWS Control Tower. Se preferisci personalizzare subito il tuo ambiente AWS Control Tower, consulta [Passaggio 2. Configura e avvia la tua zona di atterraggio](#).

Note

AWS Control Tower configura servizi a pagamento AWS CloudTrail AWS Config, come Amazon CloudWatch, Amazon S3 e Amazon VPC. [Se utilizzati, questi servizi possono comportare dei costi, come indicato nella pagina dei prezzi](#). La console AWS di gestione mostra l'utilizzo di tutti i servizi a pagamento e i costi sostenuti. AWS Control Tower non crea costi aggiuntivi.

Prima di iniziare

La decisione più importante da prendere prima di iniziare il processo di configurazione è scegliere la regione di residenza. La tua regione di origine è la AWS regione in cui eseguirai la maggior parte dei tuoi carichi di lavoro o archiverai la maggior parte dei tuoi dati. Non può essere modificato dopo aver configurato la landing zone di AWS Control Tower. Per ulteriori informazioni su come scegliere una regione d'origine, consulta [Suggerimenti amministrativi per la configurazione delle landing zone](#).

Note

Per impostazione predefinita, AWS Control Tower sceglie la regione in cui opera attualmente l'account come regione di residenza. Puoi visualizzare la tua regione attuale nella parte superiore destra della schermata della console di AWS gestione.

La procedura di avvio rapido presuppone che accetterai i valori predefiniti per le risorse nel tuo ambiente AWS Control Tower. Molte di queste scelte possono essere modificate in seguito. Alcune scelte da effettuare una sola volta sono elencate nella sezione [Aspettative per la configurazione della zona di atterraggio](#) denominata.

Se hai creato un nuovo AWS account, questo soddisfa automaticamente i prerequisiti richiesti per la configurazione di AWS Control Tower. Puoi procedere con i passaggi che seguono.

Passaggi di avvio rapido

1. Accedi alla console di AWS gestione con le tue credenziali utente di amministratore.
2. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.
3. Verifica di lavorare nella regione di residenza desiderata.
4. Scegli Enable AWS Control Tower.
5. Segui le istruzioni nella console, accettando tutti i valori predefiniti. Seleziona account esistenti o crea nuovi account per il tuo account Aggregator e CloudTrail l'account amministratore.
6. Rivedi le scelte effettuate. Scegli Enable AWS Control Tower.
7. AWS Control Tower impiega circa 30 minuti per configurare tutte le risorse nella tua landing zone.

Per una versione più dettagliata di come configurare AWS Control Tower, compresi i modi per personalizzare l'ambiente, leggi e segui le procedure nei prossimi argomenti.

 Note

Se sei un cliente alle prime armi e riscontri un problema di configurazione, contatta il [AWS Supporto](#) per ricevere assistenza diagnostica.

Prerequisito: controlli automatici prima del lancio per il tuo account di gestione

Prima che AWS Control Tower configuri la zona di atterraggio, esegue automaticamente una serie di controlli pre-avvio nel tuo account. Non è richiesta alcuna azione da parte tua per questi controlli, che assicurano che il tuo account di gestione sia pronto per le modifiche che stabiliscono la zona di atterraggio. Ecco i controlli eseguiti da AWS Control Tower prima di configurare una zona di atterraggio:

- I limiti di servizio esistenti Account AWS devono essere sufficienti per l'avvio di AWS Control Tower. Per ulteriori informazioni, consulta [Limitazioni e quote in AWS Control Tower](#).
- Account AWS Deve essere abbonato ai seguenti AWS servizi:
 - Amazon Simple Storage Service (Amazon S3)
 - Amazon Elastic Compute Cloud (Amazon EC2)
 - Amazon SNS
 - Amazon Virtual Private Cloud (Amazon VPC) (Amazon VPC)
 - AWS CloudFormation
 - AWS CloudTrail
 - Amazon CloudWatch
 - AWS Config
 - AWS Identity and Access Management (IAM)
 - AWS Lambda

 Note

Per impostazione predefinita, tutti gli account sono abbonati a questi servizi.

Considerazioni per Centro identità AWS IAM clienti (IAM Identity Center)

- Se Centro identità AWS IAM (IAM Identity Center) è già configurato, la regione principale di AWS Control Tower deve essere la stessa della regione IAM Identity Center. Tuttavia, se IAM Identity Center è configurato nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1), AWS Control Tower utilizza tale istanza indipendentemente dalla regione di origine selezionata.
- IAM Identity Center può essere installato solo nell'account di gestione di un'organizzazione.
- Tre opzioni si applicano alla tua directory IAM Identity Center, in base alla fonte di identità scelta:
 - IAM Identity Center User Store: se AWS Control Tower è configurato con IAM Identity Center, AWS Control Tower crea gruppi nella directory IAM Identity Center e fornisce l'accesso a questi gruppi, per l'utente selezionato, per gli account dei membri.
 - Active Directory: se IAM Identity Center for AWS Control Tower è configurato con Active Directory, AWS Control Tower non gestisce la directory IAM Identity Center. Non assegna utenti o gruppi a nuovi AWS account.
 - Provider di identità esterno: se IAM Identity Center for AWS Control Tower è configurato con un provider di identità esterno (IdP), AWS Control Tower crea gruppi nella directory IAM Identity Center e fornisce l'accesso a questi gruppi per l'utente selezionato per gli account dei membri. Puoi specificare un utente esistente del tuo IdP esterno in Account Factory durante la creazione dell'account e AWS Control Tower consente a questo utente di accedere al nuovo account venduto quando sincronizza gli utenti con lo stesso nome tra IAM Identity Center e l'IdP esterno. Puoi anche creare gruppi nel tuo IdP esterno in modo che corrispondano ai nomi dei gruppi predefiniti in AWS Control Tower. Quando assigni utenti a questi gruppi, questi utenti avranno accesso ai tuoi account registrati.

Per ulteriori informazioni su come lavorare con IAM Identity Center e AWS Control Tower, consulta [Cose da sapere sugli account IAM Identity Center e AWS Control Tower](#)

Considerazioni per AWS Config and AWS CloudTrail clienti

- L'accesso affidabile Account AWS non può essere abilitato nell'account di gestione dell'organizzazione per AWS Config. Per informazioni su come disattivare l'accesso affidabile, consulta [la AWS Organizations documentazione su come abilitare o disabilitare l'accesso affidabile](#).
- Se disponi di un AWS Config registratore, di un canale di distribuzione o di aggregazione esistente in qualsiasi account esistente che intendi registrare in AWS Control Tower, devi modificare o

rimuovere queste configurazioni prima di iniziare a registrare gli account, dopo aver impostato la zona di destinazione. Questo controllo preliminare non si applica all'account di gestione di AWS Control Tower durante il lancio della zona di atterraggio. Per ulteriori informazioni, consulta [Registra account esistenti AWS Config risorse](#).

- Se esegui carichi di lavoro temporanei da account in AWS Control Tower, potresti riscontrare un aumento dei costi associati a Config. AWS Contatta il rappresentante AWS del tuo account per informazioni più specifiche sulla gestione di questi costi.
- Quando registri un account in AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso dell'organizzazione AWS Control Tower. Se nell'account è già presente una distribuzione di un CloudTrail percorso, potrebbero verificarsi addebiti duplicati a meno che non elimini il percorso esistente per l'account prima di registrarlo in AWS Control Tower. Per informazioni sui percorsi a livello di organizzazione e su AWS Control Tower, consulta. [Prezzi](#)

Note

Al momento del lancio, gli endpoint AWS Security Token Service (STS) devono essere attivati nell'account di gestione, per tutte le regioni governate da AWS Control Tower. In caso contrario, l'avvio potrebbe non riuscire a metà del processo di configurazione.

Configurazione dell'ambiente dedicato ai controlli

Con AWS Control Tower landing zone 4.0, ora puoi creare un ambiente basato solo sui controlli senza implementare una zona di atterraggio completa. Questa opzione di distribuzione è progettata per i clienti che dispongono di una configurazione AWS Organizations consolidata e desiderano concentrarsi sull'adozione di controlli gestiti tramite [The AWS Control Tower Control Catalog](#).

Argomenti

- [Nozioni di base](#)
- [Considerazioni su AWS Config](#)
- [Processo di implementazione](#)
- [Note importanti](#)

Nozioni di base

Inizia esaminando l'AWS Control Tower Control Catalog dalla home page per comprendere i controlli gestiti disponibili, i relativi framework di conformità e i metadati di controllo. Per abilitare questa esperienza su AWS Control Tower, seleziona **Ho un ambiente esistente e voglio abilitare AWS-managed i controlli** sulla console. Dovrai quindi confermare la tua regione di residenza e, facoltativamente, selezionare altre regioni governate. Durante la configurazione, puoi abilitare la registrazione automatica degli account, che garantisce che gli account ereditino automaticamente i controlli e le configurazioni dall'unità organizzativa (OU) principale quando vengono spostati da un'unità organizzativa all'altra.

Considerazioni su AWS Config

È possibile attivare l'opzione AWS Config durante la configurazione iniziale o successivamente, se necessario. AWS Config è necessario se si prevede di utilizzare i controlli investigativi nel proprio ambiente. Se scegli di abilitare AWS Config, dovrai designare un account aggregatore per raccogliere i dati di configurazione e conformità. Puoi selezionare un account esistente o crearne uno nuovo durante la configurazione. Le opzioni aggiuntive includono la configurazione della crittografia delle AWS KMS chiavi e la specifica dei periodi di conservazione dei log di Amazon S3 per la registrazione.

Processo di implementazione

Se si procede senza AWS Config, l'ambiente sarà immediatamente pronto per i controlli preventivi e proattivi all'interno del Control Catalog.

Tuttavia, quando sarete pronti per attivare il primo controllo investigativo, dovrete abilitare AWS Config la registrazione tramite la nuova funzione `ConfigBaseline` abilitata sulle unità organizzative di destinazione. Si tratta di un processo di configurazione una tantum per unità organizzativa e prevede AWS Config prezzi basati sul numero di account per unità organizzativa e risorse per account, per regione AWS.

Note importanti

La creazione di un ambiente AWS Control Tower stabilisce una relazione di fiducia con AWS Organizations, abilitando il rilevamento delle deviazioni per i controlli preventivi e il monitoraggio delle modifiche agli account e all'unità organizzativa. Durante la configurazione, AWS Control Tower crea una configurazione della zona di destinazione che funge da base per l'ambiente di controlli gestiti.

Per creare il tuo ambiente dedicato ai controlli tramite API, consulta: [Inizia a usare AWS Control Tower utilizzando le API](#) Nota che il campo manifest è ora opzionale con la zona di atterraggio 4.0.

Inizia a usare AWS Control Tower dalla console

Questa procedura introduttiva è destinata agli amministratori di AWS Control Tower. Segui questa procedura quando sei pronto a configurare la tua zona di destinazione utilizzando la console AWS Control Tower. Dall'inizio alla fine, dovrebbe volerci circa mezz'ora. Questa procedura richiede alcuni prerequisiti e tre passaggi principali.

Se AWS al momento sei un cliente, ma sei un nuovo utente di AWS Control Tower, potresti voler consultare la sezione chiamata [Pianifica la tua landing zone di AWS Control Tower](#), prima di procedere.

Argomenti

- [Aspettative per la configurazione della zona di atterraggio](#)
- [Passaggio 1: crea gli indirizzi email del tuo account condiviso](#)
- [Passaggio 2. Configura e avvia la tua zona di atterraggio](#)
- [Fase 3. Rivedi e configura la zona di atterraggio](#)

Aspettative per la configurazione della zona di atterraggio

Il processo di configurazione della zona di destinazione di AWS Control Tower prevede diversi passaggi. Alcuni aspetti della zona di destinazione di AWS Control Tower sono configurabili. Le altre scelte non possono essere modificate dopo la configurazione.

Elementi chiave da configurare durante l'installazione

- È possibile selezionare i nomi delle unità organizzative di primo livello durante la configurazione e modificare i nomi delle unità organizzative dopo aver impostato la zona di atterraggio. Per impostazione predefinita, le unità organizzative di primo livello sono denominate Security e Sandbox. Per ulteriori informazioni, consulta [Linee guida per configurare un ambiente ben progettato](#).
- Durante la configurazione, puoi selezionare nomi personalizzati per gli account condivisi creati da AWS Control Tower, denominati account CloudTrail Administrator e Aggregator per impostazione predefinita.

 Note

Nelle versioni di Landing Zone precedenti alla 4.0, questi account sono denominati «Log Archive» e «Audit» per impostazione predefinita. I clienti che utilizzano versioni precedenti possono ancora vedere i nomi originali.

- Durante la configurazione, è possibile specificare AWS gli account esistenti per AWS Control Tower da utilizzare come account di audit e di archiviazione dei log. Se prevedi di specificare AWS account esistenti e se tali account dispongono di AWS Config risorse esistenti, devi eliminare le AWS Config risorse esistenti prima di poter registrare gli account in AWS Control Tower. (Si tratta di una selezione una tantum).
- Se lo stai configurando per la prima volta o se stai effettuando l'aggiornamento alla versione 3.0 della zona di destinazione, puoi scegliere se consentire ad AWS Control Tower di configurare un AWS CloudTrail percorso a livello di organizzazione per la tua organizzazione oppure puoi scegliere di non accettare i percorsi gestiti da AWS Control Tower e gestire i tuoi percorsi. CloudTrail Puoi attivare o disattivare i percorsi a livello di organizzazione gestiti da AWS Control Tower ogni volta che aggiorni la tua zona di destinazione.
- Facoltativamente, puoi impostare una politica di conservazione personalizzata per il tuo bucket di log e il bucket di accesso ai log di Amazon S3, quando configuri o aggiorni la tua zona di destinazione.
- Facoltativamente, puoi specificare un modello definito in precedenza da utilizzare per il provisioning di account membri personalizzati dalla console AWS Control Tower. Puoi personalizzare gli account in un secondo momento se non hai un blueprint disponibile. Consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

Scelte di configurazione che non possono essere annullate

- Non puoi cambiare la tua regione di residenza dopo aver impostato la zona di atterraggio.
- Se stai effettuando il provisioning degli account Account Factory con VPC, i CIDR VPC non possono essere modificati dopo la loro creazione.

Passaggio 1: crea gli indirizzi email del tuo account condiviso

Se stai configurando la tua zona di atterraggio in una nuova Account AWS, consulta [Configurazione](#).

- Per configurare la tua zona di destinazione con nuovi account condivisi, AWS Control Tower richiede due indirizzi email univoci che non siano già associati a un Account AWS. Ciascuno di questi indirizzi e-mail fungerà da casella di posta collaborativa, un account e-mail condiviso, destinato ai vari utenti dell'azienda che svolgeranno attività specifiche relative ad AWS Control Tower.
- Se stai configurando AWS Control Tower per la prima volta e stai trasferendo gli account di sicurezza e di archiviazione dei log esistenti in AWS Control Tower, puoi inserire gli indirizzi email correnti degli account esistenti AWS .

Gli indirizzi email sono necessari per:

- Account di controllo: questo account è destinato al tuo team di utenti che devono accedere alle informazioni di audit rese disponibili da AWS Control Tower. Puoi anche usare questo account come il punto di accesso per strumenti di terze parti che eseguiranno il controllo a livello di programma dell'ambiente per semplificare la verifica ai fini della conformità.
- Account di archiviazione dei log: questo account è destinato al tuo team di utenti che ha bisogno di accedere a tutte le informazioni di registrazione per tutti gli account registrati all'interno delle unità organizzative registrate nella tua zona di destinazione.

Questi account vengono configurati nell'unità organizzativa di sicurezza al momento della creazione della zona di atterraggio. Come best practice, quando esegui azioni su questi account, ti consigliamo di utilizzare un utente IAM Identity Center con le autorizzazioni appropriate.

Note

Se si specificano AWS account esistenti come account di audit e di archiviazione dei log, gli account esistenti devono superare alcuni controlli prima del lancio per garantire che nessuna risorsa sia in conflitto con i requisiti di AWS Control Tower. Se questi controlli non hanno esito positivo, la configurazione della zona di atterraggio potrebbe non riuscire. In particolare, gli account non devono disporre di AWS Config risorse esistenti. Per ulteriori informazioni, consulta [Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti](#).

Per motivi di chiarezza, questa Guida per l'utente fa sempre riferimento agli account condivisi con i loro nomi predefiniti: archivio di log e controllo. Mentre leggi questo documento, ricordati di

sostituire i nomi personalizzati che hai dato inizialmente a questi account, se scegli di personalizzarli. Puoi visualizzare i tuoi account con i relativi nomi personalizzati nella [pagina dei dettagli dell'account](#).

Note

Stiamo modificando la terminologia relativa ai nomi predefiniti di alcune unità organizzative (OU) di AWS Control Tower per allinearla alla strategia AWS multi-account. Potresti notare alcune incongruenze mentre stiamo effettuando una transizione per migliorare la chiarezza di questi nomi. L'unità organizzativa di sicurezza era precedentemente denominata Core OU. L'unità organizzativa Sandbox era precedentemente chiamata unità organizzativa personalizzata.

Passaggio 2. Configura e avvia la tua zona di atterraggio

Prima di lanciare la tua landing zone di AWS Control Tower, determina la regione principale più appropriata. Per ulteriori informazioni, consulta [Suggerimenti amministrativi per la configurazione delle landing zone](#).

Important

La modifica della regione di origine dopo aver distribuito la zona di atterraggio di AWS Control Tower richiede la disattivazione e l'assistenza del supporto. AWS Questa pratica non è consigliata.

Scopri come configurare e lanciare la tua zona di atterraggio utilizzando AWS CLI in [Inizia a usare AWS Control Tower utilizzando le API](#).

Per configurare e avviare la zona di atterraggio nella console, esegui la seguente serie di passaggi.

Preparazione: accedi alla console AWS Control Tower

1. Apri un browser web e accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.
2. Nella console, verifica di lavorare nella regione principale desiderata per AWS Control Tower. Quindi scegli **Configura la tua zona di atterraggio**.

Fase 2a. Rivedi e seleziona la tua AWS Regioni

Assicurati di aver designato correttamente la AWS regione selezionata per la tua regione di origine. Dopo aver distribuito AWS Control Tower, non puoi cambiare la regione principale.

In questa sezione del processo di configurazione, puoi aggiungere tutte AWS le regioni aggiuntive di cui hai bisogno. Puoi aggiungere altre regioni in un secondo momento, se necessario, e rimuovere le regioni dalla governance.

Per selezionare ulteriori AWS Regioni da governare

1. Il pannello mostra le selezioni attuali delle regioni. Apri il menu a discesa per visualizzare un elenco di regioni aggiuntive disponibili per la governance.
2. Seleziona la casella accanto a ciascuna regione per inserirla nella governance di AWS Control Tower. La selezione della regione d'origine non è modificabile.

Per negare l'accesso a determinate regioni

Per negare l'accesso alle AWS risorse e ai carichi di lavoro in determinate AWS regioni, seleziona **Abilitato** nella sezione relativa alla regione per negare il controllo. Per impostazione predefinita, l'impostazione di questo controllo è **Non abilitata**.

Fase 2b. Configura le tue unità organizzative (OU)

Se accetti i nomi predefiniti di queste unità organizzative, non è necessario intraprendere alcuna azione per continuare la configurazione. Per modificare i nomi delle unità organizzative, inserisci i nuovi nomi direttamente nel campo del modulo.

- **Unità organizzativa fondamentale:** AWS Control Tower si basa su un'unità organizzativa fondamentale inizialmente denominata Security OU. È possibile modificare il nome di questa unità organizzativa durante la configurazione iniziale e successivamente, dalla pagina dei dettagli dell'unità organizzativa. Questa unità organizzativa di sicurezza contiene i due account condivisi, che per impostazione predefinita sono denominati account di archiviazione dei log e account di controllo.
- **Unità organizzative aggiuntive:** AWS Control Tower può configurare una o più unità organizzative aggiuntive per te. Ti consigliamo di effettuare il provisioning di almeno un'unità organizzativa aggiuntiva nella tua zona di atterraggio, oltre all'unità di sicurezza. Se questa unità organizzativa aggiuntiva è destinata a progetti di sviluppo, ti consigliamo di denominarla Sandbox OU, come indicato nel [Linee guida per configurare un ambiente ben progettato](#). Se disponi già di

un'unità organizzativa esistente AWS Organizations, potresti visualizzare l'opzione per saltare la configurazione di un'unità organizzativa aggiuntiva in AWS Control Tower.

Fase 2c. Configura gli account condivisi, la registrazione e la crittografia

In questa sezione del processo di configurazione, il pannello mostra le selezioni predefinite per i nomi degli account AWS Control Tower condivisi. Questi account sono una parte essenziale della tua zona di atterraggio. Non spostare o eliminare questi account condivisi. È possibile scegliere nomi personalizzati per gli account di controllo e di archiviazione dei log durante la configurazione. In alternativa, è possibile specificare, una sola volta, AWS gli account esistenti come account condivisi.

È necessario fornire indirizzi e-mail univoci per l'archivio di log e gli account di controllo e verificare l'indirizzo e-mail fornito in precedenza per l'account di gestione. Scegli il pulsante **Modifica** per modificare i valori predefiniti modificabili.

Informazioni sugli account condivisi

- L'account di gestione: l'account di gestione di AWS Control Tower fa parte del livello Root. L'account di gestione consente la fatturazione di AWS Control Tower. L'account dispone anche delle autorizzazioni di amministratore per la tua zona di atterraggio. Non è possibile creare account separati per la fatturazione e per le autorizzazioni di amministratore in AWS Control Tower.

L'indirizzo email mostrato per l'account di gestione non è modificabile durante questa fase di configurazione. Viene visualizzato come conferma, quindi puoi verificare che stai modificando l'account di gestione corretto, nel caso in cui tu abbia più account.

- I due account condivisi: puoi scegliere nomi personalizzati per questi due account o creare i tuoi account e devi fornire un indirizzo email univoco per ogni account, nuovo o esistente. Se scegli che AWS Control Tower crei nuovi account condivisi per te, gli indirizzi email non devono già avere AWS account associati.

Per configurare gli account condivisi, inserisci le informazioni richieste.

1. Nella console, inserisci un nome per l'account inizialmente chiamato `account di archiviazione dei log`. Molti clienti decidono di mantenere il nome predefinito per questo account.
2. Fornisci un indirizzo email univoco per questo account.
3. Inserisci un nome per l'account inizialmente chiamato `account di controllo`. Molti clienti scelgono di chiamarlo `account di sicurezza`.

4. Fornisci un indirizzo email univoco per questo account.

Facoltativamente, configura la conservazione dei log

Durante questa fase di configurazione, puoi personalizzare la politica di conservazione dei log per i bucket Amazon S3 che archiviano i AWS CloudTrail log in AWS Control Tower, in incrementi di giorni o anni, fino a un massimo di 15 anni. Se scegli di non personalizzare la conservazione dei log, le impostazioni predefinite sono un anno per la registrazione standard dell'account e 10 anni per la registrazione degli accessi. Questa funzionalità è disponibile anche quando si aggiorna o si ripristina la zona di atterraggio.

Facoltativamente, puoi gestirlo autonomamente Account AWS accedi

Puoi scegliere se AWS Control Tower configura Account AWS l'accesso con AWS Identity and Access Management (IAM) o se gestirlo automaticamente Account AWS , con gli utenti, i ruoli e le autorizzazioni di AWS IAM Identity Center che puoi configurare e personalizzare autonomamente o con un altro metodo, ad esempio un IdP esterno, per la federazione diretta degli account o la federazione di più account tramite IAM Identity Center. Puoi modificare questa selezione in un secondo momento.

Per impostazione predefinita, AWS Control Tower configura AWS IAM Identity Center per la tua zona di destinazione, in linea con le linee guida sulle migliori pratiche definite in [Organizzazione AWS dell'ambiente utilizzando più account](#). La maggior parte dei clienti sceglie l'impostazione predefinita. A volte sono necessari metodi di accesso alternativi, per la conformità normativa in settori o paesi specifici o in Regioni AWS cui AWS IAM Identity Center non è disponibile.

La selezione dei provider di identità a livello di account non è supportata. Questa opzione si applica solo all'intera zona di atterraggio.

Per ulteriori informazioni, consulta [Linee guida per IAM Identity Center](#).

Configurare facoltativamente AWS CloudTrail trail

Come procedura consigliata, ti consigliamo di configurare la registrazione. Se desideri consentire ad AWS Control Tower di configurare un CloudTrail percorso a livello di organizzazione e gestirlo per te, scegli Attiva. Se desideri gestire la registrazione con i tuoi CloudTrail percorsi o con uno strumento di registrazione di terze parti, scegli Opt out. Conferma la selezione quando richiesto nella console. Puoi modificare la selezione e attivare o disattivare i percorsi a livello di organizzazione quando aggiorni la zona di atterraggio.

Puoi configurare e gestire i tuoi CloudTrail percorsi in qualsiasi momento, compresi i percorsi a livello di organizzazione e a livello di account. Se imposti CloudTrail percorsi duplicati, potresti incorrere in costi duplicati quando gli eventi vengono registrati. CloudTrail

Facoltativamente, configura AWS KMS keys

Se desideri crittografare e decrittografare le tue risorse con una chiave di AWS KMS crittografia, seleziona la casella di controllo. Se disponi di chiavi esistenti, potrai selezionarle dagli identificatori visualizzati in un menu a discesa. Puoi generare una nuova chiave scegliendo **Crea una chiave**. Puoi aggiungere o modificare una chiave KMS ogni volta che aggiorni la tua zona di atterraggio.

Quando selezioni **Configura zona di destinazione**, AWS Control Tower esegue un controllo preliminare per convalidare la chiave KMS. La chiave deve soddisfare questi requisiti:

- Abilitato
- Simmetria
- Non è una chiave multiregionale
- Sono state aggiunte le autorizzazioni corrette alla policy
- La chiave è nell'account di gestione

È possibile che venga visualizzato un banner di errore se la chiave non soddisfa questi requisiti. In tal caso, scegli un'altra chiave o genera una chiave. Assicurati di modificare la politica delle autorizzazioni della chiave, come descritto nella sezione successiva.

Aggiorna la politica chiave del KMS

Prima di poter aggiornare una politica chiave KMS, devi creare una chiave KMS. Per ulteriori informazioni, consulta [Creazione di una policy delle chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per utilizzare una chiave KMS con AWS Control Tower, devi aggiornare la policy delle chiavi KMS predefinita aggiungendo le autorizzazioni minime richieste per e. AWS Config AWS CloudTrail Come best practice, ti consigliamo di includere le autorizzazioni minime richieste in qualsiasi policy. Quando si aggiorna una policy chiave KMS, è possibile aggiungere le autorizzazioni come gruppo in una singola istruzione JSON o riga per riga.

La procedura descrive come aggiornare la politica delle chiavi KMS predefinita nella AWS KMS console aggiungendo dichiarazioni di politica che consentono AWS Config e da utilizzare CloudTrail

per la crittografia. AWS KMS Le dichiarazioni politiche richiedono l'inclusione delle seguenti informazioni:

- **YOUR-MANAGEMENT-ACCOUNT-ID**— l'ID dell'account di gestione in cui verrà configurata AWS Control Tower.
- **YOUR-HOME-REGION**— la regione principale che selezionerai durante la configurazione di AWS Control Tower.
- **YOUR-KMS-KEY-ID**— l'ID della chiave KMS che verrà utilizzato con la policy.
- **PARTITION**— la partizione della AWS regione in cui hai configurato AWS Control Tower, ad esempio `aws`, `aws-us-gov`, `aws-cn`, o `aws-eu-c`

Per aggiornare la politica chiave del KMS

1. Apri la AWS KMS console all'indirizzo <https://console.aws.amazon.com/kms>
2. Dal pannello di navigazione, scegli Chiavi gestite dal cliente.
3. Nella tabella, seleziona la chiave che desideri modificare.
4. Nella scheda Politica chiave, assicurati di poter visualizzare la politica chiave. Se non riesci a visualizzare la politica principale, scegli Passa alla visualizzazione della politica.
5. Scegli Modifica e aggiorna la politica chiave KMS predefinita aggiungendo le seguenti dichiarazioni politiche per AWS Config e CloudTrail.

AWS Config dichiarazione politica

```
{
  "Sid": "Allow Config to use KMS for encryption",
  "Effect": "Allow",
  "Principal": {
    "Service": "config.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail dichiarazione politica

```
{
  "Sid": "Allow CloudTrail to use KMS for encryption",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Decrypt"
  ],
  "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
    }
  }
}
```

6. Scegli Save changes (Salva modifiche).

Esempio di politica chiave KMS

Il seguente esempio di politica mostra come potrebbe apparire la tua politica chiave KMS dopo aver aggiunto le dichiarazioni politiche che la concedono AWS Config e CloudTrail le autorizzazioni minime richieste. La politica di esempio non include la politica chiave KMS predefinita.

```
{
  "Version": "2012-10-17",
  "Id": "CustomKMSPolicy",
  "Statement": [
    {
      ... YOUR-EXISTING-POLICIES ...
    },
    {
      "Sid": "Allow Config to use KMS for encryption",
      "Effect": "Allow",
```

```

    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
  },
  {
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey*",
      "kms:Decrypt"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
      "StringEquals": {
        "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
      }
    }
  }
]
}

```

Per visualizzare altri esempi di policy, consulta le seguenti pagine:

- [Concessione delle autorizzazioni di crittografia](#) nella Guida per l'AWS CloudTrail utente.
- [Autorizzazioni richieste per la chiave KMS \(quando si utilizza Service-Linked Roleless3 Bucket Delivery\)](#) nella Guida per gli sviluppatori. AWS Config

Proteggiti dagli aggressori

Aggiungendo determinate condizioni alle tue politiche, puoi contribuire a prevenire un tipo specifico di attacco, noto come attacco sostitutivo confuso, che si verifica se un'entità costringe un'entità con più privilegi a compiere un'azione, ad esempio con l'impersonificazione tra servizi. Per informazioni generali sulle condizioni delle polizze, consulta anche. [Specifica delle condizioni in una policy](#)

La AWS Key Management Service (AWS KMS) consente di creare chiavi KMS multiregionali e chiavi asimmetriche; tuttavia, AWS Control Tower non supporta chiavi multiregionali o chiavi asimmetriche. AWS Control Tower esegue un controllo preliminare delle chiavi esistenti. È possibile che venga visualizzato un messaggio di errore se si seleziona una chiave multiregionale o asimmetrica. In tal caso, genera un'altra chiave da utilizzare con le risorse AWS Control Tower.

Per ulteriori informazioni AWS KMS, consulta [la AWS KMS Developer Guide](#).

Tieni presente che i dati dei clienti in AWS Control Tower sono crittografati a riposo, per impostazione predefinita, utilizzando SSE-S3.

Facoltativamente, configura la registrazione automatica per gli account

Quando abiliti questa funzionalità durante la configurazione o in un secondo momento, gli account che vengono spostati tra due unità organizzative registrate o trasferiti nell'ambiente AWS Control Tower per la prima volta, non mostrano più una deriva ereditaria. Gli account ereditano automaticamente le linee di base e i controlli abilitati nella nuova unità organizzativa. I controlli e le baseline della precedente unità organizzativa vengono rimossi.

Per attivare la registrazione automatica in qualsiasi momento dopo la configurazione, vai alla pagina delle impostazioni della zona di destinazione e scegli **Aggiorna zona di destinazione** o chiama l'API `AWS Control Tower.UpdateLandingZone`

Puoi spostare un account tra le unità organizzative tramite l' `AWS Organizations` API o tramite la console AWS Control Tower. Se sposti un account all'esterno di un'unità organizzativa registrata, AWS Control Tower rimuove automaticamente tutte le linee di base e i controlli distribuiti. Sostanzialmente annulla la registrazione dell'account da AWS Control Tower.

 Note

Se scegli di abilitare la funzionalità di registrazione automatica dopo la configurazione iniziale della zona di destinazione, AWS Control Tower non risolve retroattivamente la deriva ereditaria causata dallo spostamento degli account tra le unità organizzative prima che la funzionalità di registrazione automatica fosse abilitata. La risoluzione automatica del drift entra in vigore per gli account che vengono spostati dopo aver abilitato questa impostazione.

Facoltativamente, configura e crea account membri personalizzati

Quando segui il flusso di lavoro di creazione di un account per aggiungere gli account dei membri, puoi facoltativamente specificare un modello definito in precedenza da utilizzare per il provisioning di account membri personalizzati dalla console AWS Control Tower. Puoi personalizzare gli account in un secondo momento se non hai un blueprint disponibile. Consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

Fase 3. Rivedi e configura la zona di atterraggio

La sezione successiva della configurazione mostra le autorizzazioni richieste da AWS Control Tower per la tua zona di destinazione. Scegli una casella di controllo per espandere ogni argomento. Ti verrà chiesto di accettare queste autorizzazioni, che possono interessare più account, e di accettare i Termini di servizio generali.

Per finalizzare

1. Dalla console, rivedi le autorizzazioni del servizio e, quando sei pronto, scegli **Comprendo le autorizzazioni** che AWS Control Tower utilizzerà per amministrare AWS le risorse e far rispettare le regole per mio conto.
2. Per finalizzare le selezioni e inizializzare il lancio, scegli **Configura zona di atterraggio**.

Questa serie di passaggi avvia il processo di configurazione della zona di atterraggio, che può richiedere circa trenta minuti. Durante la configurazione, AWS Control Tower crea il livello root, l'unità organizzativa di sicurezza e gli account condivisi. Altre AWS risorse vengono create, modificate o eliminate.

Conferma gli abbonamenti SNS

L'indirizzo e-mail fornito per l'account di audit riceverà le e-mail di AWS notifica: conferma dell'abbonamento da tutte le AWS regioni supportate da AWS Control Tower. Per ricevere e-mail di conformità nel tuo account di audit, devi scegliere il link [Conferma iscrizione](#) all'interno di ogni e-mail di ciascuna AWS regione supportata da AWS Control Tower.

Inizia a usare AWS Control Tower utilizzando le API

Questa procedura introduttiva è destinata agli amministratori di AWS Control Tower. Questa procedura richiede alcuni prerequisiti e include due passaggi principali.

In questa procedura, utilizzerai le API di AWS Control Tower e altri AWS servizi per configurare e avviare una landing zone. Queste API consentono di creare un ambiente AWS Control Tower in modo programmatico, [tramite la CloudFormation console](#) o tramite AWS CLI.

Prima di lanciare la landing zone di AWS Control Tower, esegui queste attività preliminari:

- Determina la regione d'origine più appropriata. Per ulteriori informazioni, consulta [Suggerimenti amministrativi per la configurazione delle landing zone](#).
- Consulta questa pagina [Prerequisito: controlli automatici prima del lancio per il tuo account di gestione](#) per scoprire i controlli automatici prima del lancio che assicurano che il tuo account di gestione sia pronto per le modifiche che stabiliscono la tua landing zone.

Argomenti

- [Aspettative per la configurazione delle landing zone con le API](#)
- [Fase 1: Configura la tua landing zone](#)
- [Fase 2: Avvia la landing zone utilizzando le API AWS Control Tower](#)
- [Identifica la tua landing zone](#)
- [Aggiorna la tua landing zone](#)
- [Reimposta la landing zone per risolvere la deriva](#)
- [Visualizza i dettagli del file manifesto della tua zona di atterraggio](#)
- [Visualizza lo stato delle operazioni della tua zona di atterraggio](#)

- [Esempi: configura una landing zone di AWS Control Tower solo con API](#)
- [Schemi delle zone di atterraggio](#)
- [Avvia una landing zone usando CloudFormation](#)

Aspettative per la configurazione delle landing zone con le API

Il processo di configurazione della landing zone di AWS Control Tower prevede diversi passaggi. Alcuni aspetti della landing zone di AWS Control Tower sono configurabili. Le altre scelte non possono essere modificate dopo la configurazione.

Elementi chiave da configurare durante l'installazione

- È possibile selezionare i nomi delle unità organizzative fondamentali durante la configurazione e modificare i nomi delle unità organizzative dopo aver configurato la landing zone. Per impostazione predefinita, le OU Foundational sono denominate Security e Sandbox. Per ulteriori informazioni, consulta [Linee guida per configurare un ambiente ben progettato](#).
- Durante la configurazione, puoi selezionare nomi personalizzati per gli account condivisi creati da AWS Control Tower, denominati log archive and audit per impostazione predefinita, ma non puoi modificare questi nomi dopo la configurazione. (Questa è una selezione una tantum).
- Durante la configurazione con le API, è necessario specificare AWS gli account esistenti per AWS Control Tower da utilizzare come account di controllo e archiviazione dei log. Per specificare AWS gli account esistenti, se tali account dispongono di AWS Config risorse esistenti, è necessario eliminare o modificare le AWS Config risorse esistenti prima di poter registrare gli account in AWS Control Tower. (Questa è una selezione una tantum).
- Se stai effettuando la configurazione per la prima volta o se stai effettuando l'aggiornamento alla versione 3.0 di landing zone, puoi scegliere se consentire ad AWS Control Tower di configurare un AWS CloudTrail percorso a livello di organizzazione per la tua organizzazione oppure puoi disattivare i percorsi gestiti da AWS Control Tower e gestire i tuoi percorsi. CloudTrail Puoi attivare o disattivare i percorsi a livello di organizzazione gestiti da AWS Control Tower ogni volta che aggiorni la tua landing zone.
- Facoltativamente, puoi impostare una politica di conservazione personalizzata per il tuo bucket di log Amazon S3 e il tuo bucket di accesso ai log, quando configuri o aggiorni la landing zone.

Scelte di configurazione che non possono essere annullate

- Non puoi cambiare la tua regione d'origine dopo aver configurato la landing zone.

- Se esegui il provisioning degli account con VPC, i CIDR VPC non possono essere modificati dopo la loro creazione.

Le sezioni successive illustrano in dettaglio i prerequisiti e i passaggi di configurazione, con spiegazioni e avvertenze. Per ulteriori esempi di codice, vedere. [Esempi: configura una landing zone di AWS Control Tower solo con API](#)

Fase 1: Configura la tua landing zone

Il processo di configurazione della landing zone di AWS Control Tower prevede diversi passaggi. Alcuni aspetti della landing zone di AWS Control Tower sono configurabili, ma altre scelte non possono essere modificate dopo la configurazione. Per ulteriori informazioni su queste importanti considerazioni prima di lanciare la landing zone, consulta [Expectations for landing zone configuration](#).

Prima di utilizzare le API della landing zone di AWS Control Tower, devi prima chiamare le API di altri AWS servizi per configurare la tua landing zone prima del lancio. Il processo include tre fasi principali:

1. creazione di una nuova organizzazione AWS Organizations,
2. configurazione degli account di integrazione dei servizi,
3. e creando un ruolo IAM o un utente IAM Identity Center con le autorizzazioni necessarie per chiamare le API delle landing zone.

Passaggio 1. Crea l'organizzazione che conterrà la tua landing zone:

Chiama l'CreateOrganizationAPI AWS Organizations e abilita tutte le funzionalità per creare l'unità organizzativa Foundational. AWS Control Tower consiglia inoltre di creare un'unità organizzativa di sicurezza designata. Questa unità organizzativa di sicurezza deve contenere tutti gli account di integrazione del servizio. Questi sarebbero l'account di archiviazione dei log e l'account di controllo per le versioni precedenti di Landing Zone.

```
aws organizations create-organization --feature-set ALL
```

AWS Control Tower può configurare una o più unità organizzative aggiuntive. Ti consigliamo di fornire almeno un'unità organizzativa aggiuntiva nella tua landing zone, oltre all'unità organizzativa di sicurezza. Se questa unità organizzativa aggiuntiva è destinata a progetti di sviluppo, ti consigliamo di denominarla Sandbox OU, come indicato nella [strategia multi-account AWS per la tua landing zone di AWS Control Tower](#).

Passaggio 2. Fornisci account di integrazione dei servizi, se necessario:

Per configurare la landing zone, AWS Control Tower consente ai clienti di configurare le integrazioni dei servizi AWS. Ciascuna di queste integrazioni di servizi può richiedere uno o più account centrali di integrazione dei servizi. Se utilizzi le API di landing zone per configurare AWS Control Tower per la prima volta, devi fornire l'account di integrazione centrale per ogni integrazione di servizi AWS abilitata. Puoi utilizzare account AWS esistenti o effettuare il provisioning di tali account tramite la console AWS Control Tower o AWS le API Organizations. Assicurati che questi account di integrazione dei servizi si trovino nell'unità organizzativa di sicurezza designata, che si trova al livello principale della tua organizzazione.

1. Chiama l'CreateAccountAPI AWS Organizations per creare l'account di archiviazione dei log e l'account di audit nell'unità organizzativa di sicurezza.

```
aws organizations create-account --email mylog@example.com --account-name "Logging Account"
aws organizations create-account --email mysecurity@example.com --account-name "Security Account"
```

(Facoltativo) Controlla lo stato dell'CreateAccountoperazione utilizzando l'DescribeAccountAPI AWS Organizations.

2. Sposta gli account di integrazione del servizio forniti nell'unità organizzativa di sicurezza designata

```
aws organizations move-account \
  --account-id 0123456789012 \
  --source-parent-id r-examplerootid111 \
  --destination-parent-id ou-examplerootid111-security
```

Fase 3. Creare i ruoli di servizio richiesti

Crea i seguenti ruoli di servizio IAM nel percorso `/service-role/` IAM che consentono ad AWS Control Tower di eseguire le chiamate API necessarie per configurare la tua landing zone:

- [AWSControlTowerAdmin](#)
- [AWSControlTowerCloudTrailRole](#)
- [AWSControlTowerStackSetRole](#)

- [AWSControlTowerConfigAggregatorRoleForOrganizations](#) (non richiesto per la versione 4.0 e successive della landing zone)

Per ulteriori informazioni su questi ruoli e le relative politiche, consulta [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#).

Per creare un ruolo IAM:

Crea un ruolo IAM con le autorizzazioni necessarie per chiamare tutte le API delle landing zone. In alternativa, puoi creare un utente IAM Identity Center e assegnare le autorizzazioni necessarie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "backup:UpdateGlobalSettings",
        "controltower:CreateLandingZone",
        "controltower:UpdateLandingZone",
        "controltower:ResetLandingZone",
        "controltower>DeleteLandingZone",
        "controltower:GetLandingZoneOperation",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "controltower:ListLandingZoneOperations",
        "controltower:ListTagsForResource",
        "controltower:TagResource",
        "controltower:UntagResource",
        "servicecatalog:*",
        "organizations:*",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "logs:*",
        "cloudformation:*",
        "kms:*",
        "iam:GetRole",

```

```

        "iam:CreateRole",
        "iam:GetSAMLProvider",
        "iam:CreateSAMLProvider",
        "iam:CreateServiceLinkedRole",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": "*"
}
]
}

```

Note

Quando si esegue l'aggiornamento alla versione 4.0 della landing zone con l'integrazione di AWS Config abilitata, i clienti devono disporre delle autorizzazioni `organizations:ListDelegatedAdministrators`.

Fase 2: Avvia la landing zone utilizzando le API AWS Control Tower

Puoi utilizzare le API AWS Control Tower per avviare la tua landing zone. Questa sezione descrive come creare il file manifest della landing zone richiesto e utilizzarlo con l'operazione `CreateLandingZone` API.

Creazione del file manifest

Il file manifest è un documento JSON che specifica la configurazione della landing zone. Con la versione 4.0 della landing zone, molti componenti sono ora opzionali, il che consente un'implementazione più flessibile.

Struttura del manifesto

Di seguito è riportata la struttura completa del file manifest con tutte le configurazioni disponibili:

```

{
  "accessManagement": {
    "enabled": true    // Required - Controls IAM Identity Center integration
  },
  "backup": {
    "enabled": true,    // Required - Controls AWS Backup integration
    "configurations": {
      "backupAdmin": {
        "accountId": "111122223333"    // Backup administrator account
      },
      "centralBackup": {
        "accountId": "111122224444"    // Central backup account
      },
      "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
    }
  },
  "centralizedLogging": {
    "accountId": "111122225555",    // Log archive account
    "enabled": true,                // Required - Controls centralized logging
    "configurations": {
      "accessLoggingBucket": {
        "retentionDays": 365    // Minimum value: 1
      },
      "loggingBucket": {
        "retentionDays": 365    // Minimum value: 1
      },
      "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
    }
  },
  "config": {
    "accountId": "111122226666",    // Config aggregator account
    "enabled": true,                // Required - Controls AWS Config integration
    "configurations": {
      "accessLoggingBucket": {
        "retentionDays": 365    // Minimum value: 1
      },
      "loggingBucket": {
        "retentionDays": 365    // Minimum value: 1
      },
      "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
    }
  },
  "governedRegions": [              // Optional - List of regions to govern
    "us-east-1",
  ]
}

```

```
    "us-west-2"
  ],
  "securityRoles": {
    "enabled": true,           // Required - Controls security roles creation
    "accountId": "'111122226666'" // Security/Audit account
  }
}
```

Note importanti

- Tutti i `enabled` flag sono obbligatori nel manifesto.
- Se disabiliti AWS Config integration (`"config.enabled": false`), devi disabilitare anche le seguenti integrazioni:
 - Ruoli di sicurezza (`"securityRoles.enabled": false`)
 - Gestione degli accessi (`"accessManagement.enabled": false`)
 - Backup (`"backup.enabled": false`)
- Gli ID account devono essere ID AWS account validi a 12 cifre.
- Gli ARN delle chiavi KMS devono essere ARN chiave validi. AWS KMS
- I giorni di conservazione devono essere almeno 1.

Utilizzo dell' CreateLandingZone API

Per creare la tua landing zone utilizzando l'API:

```
aws controltower create-landing-zone --landing-zone-version 4.0 --manifest file://manifest.json
```

L'API restituirà un Landing Zone Operation ID che potrai utilizzare per monitorare lo stato di avanzamento della creazione della landing zone. Risposta di esempio:

```
{
  "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
  "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXXX"
}
```

Puoi monitorare lo stato dell'operazione utilizzando l'`GetLandingZoneOperationAPI` che restituisce uno stato di `SUCCEEDED`, `FAILED`, oppure `IN_PROGRESS`:

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-eXXX-4XXX-aXXX-44XXXXXXXXXXXX"
```

Cosa è cambiato nella versione 4.0 della landing zone

Modifiche importanti alla struttura e ai requisiti del manifesto:

- **Struttura organizzativa**
 - `organizationStructure` la definizione è stata rimossa dal manifesto
 - I clienti possono ora definire la propria struttura organizzativa
 - Unico requisito: gli account di integrazione dei servizi devono trovarsi nella stessa unità organizzativa direttamente sotto root
- **Bandiere abilitate**
 - Tutte le configurazioni di integrazione dei servizi hanno un `enabled` flag che ora è un campo obbligatorio.
 - I clienti devono sempre fornire un valore booleano. Non vengono forniti valori predefiniti.
 - I clienti devono specificare esplicitamente `enable/disable` ogni configurazione di integrazione del servizio nel manifesto:
 - `accessManagement`
 - `backup`
 - `centralizedLogging`
 - `config`
 - `securityRoles`
- **Ruoli di sicurezza**
 - L'integrazione dei ruoli di sicurezza è ora facoltativa
 - È stato introdotto un nuovo `enabled` flag per gestire la `securityRoles` distribuzione
 - Se disabilitate, le relative funzionalità di sicurezza non verranno implementate
- **AWS Integrazione Config**
 - Nuova sezione di integrazione del servizio AWS Config aggiunta al manifesto `config` con i seguenti campi:
 - `enabled`: flag booleano richiesto per gestire la distribuzione dell'integrazione con AWS Config

- `accountId`: ID account AWS per AWS Config aggregator
- configurazioni:
 - `accessLoggingBucket.retentionDays`: Periodo di conservazione dei log di accesso
 - `loggingBucket.retentionDays`: Periodo di conservazione per i log di AWS Config
 - `kmsKeyArn`: chiave KMS per la crittografia

Identifica la tua landing zone

`ListLandingZones` Le chiamate possono aiutarti a determinare se il tuo account è già configurato con AWS Control Tower. Questa API restituisce un identificatore di zona di atterraggio (ARN) in qualsiasi regione commerciale, indipendentemente dalla regione di origine della landing zone. Gli ARN delle zone di atterraggio sono unici a livello regionale.

```
aws controltower list-landing-zones --region us-east-1
```

Per [le regioni opt-in](#), l'`ListLandingZones` API restituisce l'identificatore della landing zone solo se si chiama l'API nella stessa regione della regione principale dell'API. Ad esempio, se la tua landing zone è configurata in `af-south-1` e chiami `af-south-1`, l'API restituisce l'identificatore della zona di atterraggio. Se la tua landing zone è configurata in `af-south-1` e chiami `ap-east-1`, l'API non **`ListLandingZones`** restituisce l'identificatore della zona di atterraggio.

Output:

```
{
  "landingZones" [
    "arn": "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
  ]
}
```

Aggiorna la tua landing zone

Quando è disponibile una nuova versione della landing zone o per apportare altri aggiornamenti alla configurazione della landing zone, puoi chiamare l'`UpdateLandingZone` API e fare riferimento a un file manifest della zona di atterraggio aggiornato. Questa API restituisce un `OperationIdentifier` file, che puoi quindi utilizzare quando chiami l'`GetLandingZoneOperation` API per verificare lo stato dell'operazione di aggiornamento.

Per aggiornare la landing zone

1. Chiama l'UpdateLandingZoneAPI AWS Control Tower e fai riferimento alla versione aggiornata della landing zone o al file manifest della zona di atterraggio aggiornato.

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H" --manifest file:///LandingZoneManifest.json
```

LandingZoneManifest.jsonFile di esempio, con regioni e registrazione centralizzata:

```
{
  "governedRegions": ["us-west-2", "us-west-1"],
  "organizationStructure": {
    "security": {
      "name": "Security"
    },
    "sandbox": {
      "name": "Sandbox"
    }
  },
  "centralizedLogging": {
    "accountId": "LOG ARCHIVE ACCOUNT ID",
    "configurations": {
      "loggingBucket": {
        "retentionDays": 2555
      },
      "accessLoggingBucket": {
        "retentionDays": 2555
      },
      "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
    },
    "enabled": true
  },
  "securityRoles": {
    "accountId": "SECURITY ACCOUNT ID"
  },
  "accessManagement": {
    "enabled": true
  }
}
```



```
}
```

Output:

```
{  
  "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXXX"  
}
```

 Opzionalmente, Re-register OU per aggiornare gli account

Per le unità organizzative AWS Control Tower registrate con meno di 1000 account, puoi utilizzare la console AWS Control Tower, accedere alla pagina OU nella dashboard e selezionare Re-registerOU per aggiornare gli account in quell'unità organizzativa.

Reimposta la landing zone per risolvere la deriva

Quando crei la landing zone, la landing zone e tutte le unità organizzative (OU), gli account e le risorse sono conformi alle regole di governance applicate dai controlli scelti. Man mano che tu e i membri della tua organizzazione utilizzate la landing zone, potrebbero verificarsi cambiamenti in questo stato di conformità. Queste modifiche sono chiamate deriva.

Per sapere se la tua landing zone è alla deriva, puoi chiamare l'GetLandingZoneAPI. Questa API restituisce lo stato di deriva della zona di atterraggio pari a o. DRIFTED IN_SYNC

Per risolvere la deriva all'interno della tua landing zone, puoi utilizzare l'ResetLandingZoneAPI per ripristinare la configurazione originale della landing zone. Ad esempio, AWS Control Tower abilita IAM Identity Center per impostazione predefinita per aiutarti a gestire i tuoi Account AWS, ma se configuri i parametri originali della landing zone con IAM Identity Center disabilitato, Calling ResetLandingZone mantiene la configurazione IAM Identity Center disabilitata.

Puoi utilizzare l'ResetLandingZoneAPI solo se la tua landing zone è nella versione 3.1 o successiva. Puoi chiamare l'GetLandingZoneAPI per verificare la versione attuale della landing zone. Se la tua landing zone utilizza una versione precedente alla 3.1, l'ResetLandingZoneAPI non è disponibile. In tal caso, almeno [Aggiorna la tua landing zone](#) alla versione 3.1. Il processo di aggiornamento risolve la deriva da solo, quindi non è necessario reimpostarlo separatamente. La reimpostazione della landing zone non comporta l'aggiornamento alla versione più recente disponibile.

1. Chiamata dell'API `GetLandingZone`. Se l'API restituisce uno stato di deriva di `DRIFTED`, la tua landing zone è in deriva.
2. Chiama l'`ResetLandingZoneAPI` per ripristinare la configurazione originale della landing zone.

```
aws controltower reset-landing-zone --landing-zone-identifier  
"arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Output:

```
{  
  "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXXX"  
}
```

 Note

La reimpostazione della landing zone non aggiorna la versione della landing zone. Leggi [Aggiorna la tua landing zone](#) i dettagli sull'aggiornamento della versione landing zone.

Visualizza i dettagli del file manifesto della tua zona di atterraggio

Il file manifest della zona di destinazione di AWS Control Tower è un file di testo che descrive le tue risorse AWS Control Tower. Le sezioni seguenti mostrano definizioni dettagliate delle voci nel file manifesto della zona di destinazione.

Per vedere un esempio completo dello schema della zona di atterraggio, consulta Schemi [delle zone di atterraggio](#).

GovernedRegions: regioni da sottoporre a governance

- Tipo: List of Strings
- Obbligatorio: no
- Esempio:

```
"governedRegions": ["us-west-2", "us-west-1"]
```

OrganizationStructure: seleziona i nomi delle unità organizzative di sicurezza e sandbox da creare nella tua organizzazione

- Tipo: oggetto
- Obbligatorio: sì
- Proprietà:
- Esempio:
 - `security`- un oggetto con una proprietà obbligatoria `name`, che accetta un `String`
 - `sandbox`- un oggetto con una proprietà obbligatoria `name`, che accetta un `String`

```
"organizationStructure": {  
  "security": {  
    "name": "CORE"  
  },  
  "sandbox": {  
    "name": "Sandbox"  
  }  
}
```

 Note

Il `organizationStructure` campo non è presente nella versione 4.0 e successive della zona di atterraggio.

CentralizedLogging: configurazione per AWS CloudTrail

- Tipo: oggetto
- Richiesto: No (versione 4.0 e successive). Sì (versione 3.3 e precedenti).
- Proprietà:
 - `accountID`: a rappresenta `String` l' AWS account in cui deve essere distribuita la risorsa di registrazione
 - `configurazioni` - e con tre proprietà `Object`
 - `loggingBucket`- un oggetto con una proprietà `retentionDays`, che accetta un `Number`
 - `accessLoggingBucket`- un oggetto con una proprietà `retentionDays`, che accetta un `Number`

- kmsKeyArn- un opzionale String
- abilitato - a Boolean (richiesto nella versione 4.0 e successive, opzionale nella versione 3.3 e precedenti)
- Esempio:

```
"centralizedLogging": {
  "accountId": "222222222222",
  "configurations": {
    "loggingBucket": {
      "retentionDays": 60
    },
    "accessLoggingBucket": {
      "retentionDays": 60
    },
    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
  },
  "enabled": true
}
```

Note

Nella versione 4.0 e successive della zona di atterraggio, accountId è richiesto solo se enabled è impostato su true. Il campo enabled è obbligatorio.

SecurityRoles: scegli dove distribuire le risorse centrali per il monitoraggio della sicurezza all'interno della tua organizzazione

- Tipo: oggetto
- Obbligatorio: No (versione 4.0 e successive). Sì (versione 3.3 e precedenti).
- Proprietà:
 - AccountID: un String che rappresenta l' AWS account in cui devono essere distribuite le risorse centrali di monitoraggio della sicurezza. Obbligatorio quando è enabled. true
 - abilitato - a Boolean (richiesto nella versione 4.0 e successive)
- Esempio:

```
"securityRoles": {  
    "accountId": "333333333333",  
    "enabled": true  
}
```

Note

Nella versione 4.0 e successive della zona di atterraggio, `securityRoles` include una proprietà `enabled` booleana obbligatoria. `accountId` è obbligatorio solo se `enabled` è impostato su `true`

Gestione degli accessi: scegli se abilitare la gestione degli accessi

- Tipo: oggetto
- Obbligatorio: no
- Proprietà: `abilitato`: un valore booleano
- Esempio:

```
"accessManagement": {  
    "enabled": true  
}
```

backup — Configurazione per il AWS backup con AWS Control Tower

- Tipo: oggetto
- Obbligatorio: no
- Proprietà:
 - configurazioni - è un `Object` con tre proprietà
 - `centralBackup`- un oggetto con una proprietà `accountId`, che accetta un `String`
 - `backupAdmin`- un oggetto con una proprietà `accountId`, che accetta un `String`
 - `kmsKeyArn`- un opzionale `String`
 - `abilitato` - a `Boolean`
- Esempio:

```
"backup": {
  "configurations": {
    "centralBackup": {
      "accountId": "CENTRAL BACKUP ACCOUNT ID"
    },
    "backupAdmin": {
      "accountId": "BACKUP MANAGER ACCOUNT ID"
    },
    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
  },
  "enabled": true
}
```

config — Configurazione per AWS Config AWS Control Tower

- Tipo: oggetto
- Obbligatorio: no
- Proprietà:
 - AccountID: un String che rappresenta l' AWS account in cui devono essere distribuite le AWS Config risorse. Obbligatorio quando è enabled. true
 - configurazioni: un opzionale Object con tre proprietà
 - loggingBucket- un oggetto con una proprietà retentionDays, che accetta un Number
 - accessLoggingBucket- un oggetto con una proprietà retentionDays, che accetta un Number
 - kmsKeyArn- un opzionale String
 - abilitato - obbligatorio Boolean
- Esempio:

```
"config": {
  "accountId": "444444444444",
  "configurations": {
    "loggingBucket": {
      "retentionDays": 60
    },
    "accessLoggingBucket": {
      "retentionDays": 60
    }
  }
}
```

```
    },
    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
  },
  "enabled": true
}
```

Note

Il config campo è disponibile solo nella versione 4.0 e successive della zona di atterraggio.

Visualizza lo stato delle operazioni della tua zona di atterraggio

L'`ListLandingZoneOperationsAPI` ti consente di visualizzare lo stato delle operazioni di AWS Control Tower che eseguono azioni sulla tua zona di atterraggio.

Per ulteriori informazioni su questa operazione API, consulta [ListLandingZoneOperations](#).

ListLandingZoneOperations

Esempio di input e output per **ListLandingZoneOperations**.

Questo esempio mostra come chiamare l'API senza parametri.

```
aws controltower --region us-east-1 list-landing-zone-operations

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    },
    {
      "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
      "operationType": "DELETE",
      "status": "SUCCEEDED"
    },
    {
      "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
```

```

        "operationType": "CREATE",
        "status": "SUCCEEDED"
    },
    {
        "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
        "operationType": "CREATE",
        "status": "FAILED"
    }
]
}

```

Questo esempio mostra come chiamare l'API e specificare il numero massimo di risultati.

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1
```

```

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    }
  ],
  "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0R1hceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}

```

Questo esempio mostra come chiamare l'API e ottenere un risultato impaginato con nextToken.

```

aws controltower --region us-east-1 list-landing-zone-operations --next-token
AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0R1hceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
  "landingZoneOperations": [
    {

```



```

        "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
        "operationType": "DELETE",
        "status": "SUCCEEDED"
    },
    {
        "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
        "operationType": "CREATE",
        "status": "SUCCEEDED"
    },
    {
        "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
        "operationType": "CREATE",
        "status": "FAILED"
    }
]
}

```

Questo esempio mostra come chiamare l'API con un filtro.

```

aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    },
    {
      "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
      "operationType": "CREATE",
      "status": "FAILED"
    }
  ]
}

```

Esempi: configura una landing zone di AWS Control Tower solo con API

Questa panoramica di esempi è un documento complementare. Per spiegazioni, avvertenze e ulteriori informazioni, consulta [Getting started with AWS Control Tower using APIs.](#)

Prerequisiti

Prima di creare una landing zone di AWS Control Tower, devi creare un'organizzazione, due account condivisi e alcuni ruoli IAM. Questo tutorial dettagliato include questi passaggi, con esempi di comandi e output CLI.

Fase 1: Crea l'organizzazione e i due account richiesti.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
account"
```

Fase 2. Crea i ruoli IAM richiesti.

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file:///controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeAvailabilityZones",
      "Resource": "*"
    }
  ]
}
```

```

    ]
  }
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

```

AWSControlTowerCloudTrailRole

```

cat <<EOF >cloudtrail_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "logs:CreateLogStream",
      "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
      "Effect": "Allow"
    },
    {
      "Action": "logs:PutLogEvents",
      "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
      "Effect": "Allow"
    }
  ]
}
EOF

```

```
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --  
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://  
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "cloudformation.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}  
EOF  
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --  
assume-role-policy-document file://cloudformation_trust.json  
cat <<EOF >stackset_role_policy.json  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": [  
        "sts:AssumeRole"  
      ],  
      "Resource": [  
        "arn:aws:iam::*:role/AWSControlTowerExecution"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}  
EOF  
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name  
AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Fase 3. Ottieni gli ID degli account e genera il file manifesto della zona di atterraggio.

I primi due comandi dell'esempio seguente memorizzano gli ID account per gli account creati nel passaggio 1 in variabili. Queste variabili aiutano quindi a generare il file manifesto della zona di atterraggio.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
"Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
"Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
  "governedRegions": ["us-west-1", "us-west-2"],
  "organizationStructure": {
    "security": {
      "name": "Security"
    },
    "sandbox": {
      "name": "Sandbox"
    }
  },
  "centralizedLogging": {
```

```
    "accountId": "$log_account_id",
    "configurations": {
      "loggingBucket": {
        "retentionDays": 60
      },
      "accessLoggingBucket": {
        "retentionDays": 60
      }
    },
    "enabled": true
  },
  "securityRoles": {
    "accountId": "$sec_account_id"
  },
  "accessManagement": {
    "enabled": true
  }
}
EOF
```

Fase 4. Crea la zona di atterraggio con la versione più recente.

È necessario configurare la zona di atterraggio con il file manifest e la versione più recente. Questo esempio mostra la versione 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

L'output conterrà un `arn` e un `OperationIdentifier`, come mostrato nell'esempio che segue.

```
{
  "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNU0L2AXXX",
  "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

Fase 5: (Facoltativo) Tieni traccia dello stato dell'operazione di creazione della zona di atterraggio, impostando un loop.

Per tenere traccia dello stato, utilizzate l'`OperationIdentifier` dall'output del `create-landing-zone` comando precedente.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Esempio di output sullo stato:

```
{
  "operationDetails": {
    "operationType": "CREATE",
    "startTime": "2024-02-28T21:49:31Z",
    "status": "IN_PROGRESS"
  }
}
```

Puoi usare il seguente script di esempio per aiutarti a configurare un loop, che riporta lo stato dell'operazione più e più volte, come un file di registro. Quindi non è necessario continuare a immettere il comando.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Per mostrare informazioni dettagliate sulla tua zona di atterraggio

Fase 1: Trova l'ARN della zona di atterraggio

```
aws --region us-west-1 controltower list-landing-zones
```

L'output includerà l'identificatore della zona di atterraggio, come mostrato nel seguente esempio di output.

```
{
  "landingZones": [
    {
      "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX"
    }
  ]
}
```

Fase 2. Ottieni le informazioni

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX
```

Ecco un esempio del tipo di output che potresti vedere:

```
{
  "landingZone": {
    "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX",
    "driftStatus": {
      "status": "IN_SYNC"
    },
    "latestAvailableVersion": "3.3",
    "manifest": {
      "accessManagement": {
        "enabled": true
      },
      "securityRoles": {
        "accountId": "9750XXXX4444"
      },
      "governedRegions": [
        "us-west-1",
        "us-west-2"
      ],
      "organizationStructure": {
        "sandbox": {
          "name": "Sandbox"
        },
        "security": {
          "name": "Security"
        }
      },
      "centralizedLogging": {
        "accountId": "012345678901",
        "configurations": {
          "loggingBucket": {
            "retentionDays": 60
          },
          "accessLoggingBucket": {
            "retentionDays": 60
          }
        },
        "enabled": true
      }
    }
  }
}
```



```
    }  
  },  
  "status": "ACTIVE",  
  "version": "3.3"  
}  
}
```

Fase 6: (Facoltativo) Chiama l'**ListLandingZoneOperationsAPI** per visualizzare lo stato di tutte le operazioni che modificano la tua zona di atterraggio.

Per monitorare lo stato di qualsiasi operazione sulla zona di atterraggio, puoi chiamare l'[ListLandingZoneOperationsAPI](#).

Schemi delle zone di atterraggio

Una landing zone è una AWS risorsa creata mediante schemi. Ogni versione della landing zone di AWS Control Tower ha uno schema unico.

Gli schemi per le zone di atterraggio di AWS Control Tower, versione 3.1 e successive, sono pubblicati in questa sezione di riferimento per aiutarti a scegliere una versione compatibile.

Note

Un problema noto relativo alla registrazione degli accessi non necessari è presente nella versione 3.0 della landing zone. Il problema è stato risolto nella versione 3.1 della landing zone. Per ulteriori informazioni sulle modifiche, vedere [Zona di destinazione di AWS Control Tower versione 3.1](#).

Schema della zona di atterraggio 4.0

```
{  
  "type": "object",  
  "required": [],  
  "properties": {  
    "accessManagement": {  
      "$ref": "#/definitions/AccessManagement"  
    },  
    "backup": {  
      "$ref": "#/definitions/Backup"  
    },  
  },  
}
```

```

    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
        "additionalProperties": false
      },
      "additionalProperties": false
    },
    "securityRoles": {
      "$ref": "#/definitions/SecurityRoles"
    },
    "config": {
      "$ref": "#/definitions/Config"
    }
  },
  "additionalProperties": false,
  "definitions": {
    "AccessManagement": {
      "type": "object",
      "required": [
        "enabled"
      ],
      "properties": {
        "enabled": {
          "type": "boolean",
          "additionalProperties": false
        }
      }
    },
    "additionalProperties": false
  },
  "Backup": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "configurations": {
        "$ref": "#/definitions/BackupConfigurations"
      }
    }
  }
}

```

```

    },
    "enabled": {
      "type": "boolean",
      "additionalProperties": false
    }
  },
  "additionalProperties": false,
  "if": {
    "properties": {
      "enabled": {
        "const": true
      }
    }
  },
  "then": {
    "required": [
      "configurations"
    ]
  }
},
"BackupAdminConfigurations": {
  "type": "object",
  "required": [
    "accountId"
  ],
  "properties": {
    "accountId": {
      "type": "string",
      "maxLength": 12,
      "minLength": 12,
      "pattern": "^\\d{12}$",
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"BackupConfigurations": {
  "type": "object",
  "required": [
    "backupAdmin",
    "centralBackup",
    "kmsKeyArn"
  ],
  "properties": {

```

```

    "backupAdmin": {
      "$ref": "#/definitions/BackupAdminConfigurations"
    },
    "centralBackup": {
      "$ref": "#/definitions/CentralBackupConfigurations"
    },
    "kmsKeyArn": {
      "type": "string",
      "maxLength": 2048,
      "minLength": 1,
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"CentralBackupConfigurations": {
  "type": "object",
  "required": [
    "accountId"
  ],
  "properties": {
    "accountId": {
      "type": "string",
      "maxLength": 12,
      "minLength": 12,
      "pattern": "^\\d{12}$",
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"CentralizedLogging": {
  "type": "object",
  "required": [
    "enabled"
  ],
  "properties": {
    "accountId": {
      "type": "string",
      "maxLength": 12,
      "minLength": 12,
      "pattern": "^\\d{12}$",
      "additionalProperties": false
    }
  },

```

```

        "configurations": {
            "$ref": "#/definitions/LoggingConfigurations"
        },
        "enabled": {
            "type": "boolean",
            "additionalProperties": false
        }
    },
    "additionalProperties": false,
    "if": {
        "properties": {
            "enabled": {
                "const": true
            }
        }
    },
    "then": {
        "required": [
            "accountId"
        ]
    }
},
"LoggingConfigurations": {
    "type": "object",
    "properties": {
        "accessLoggingBucket": {
            "$ref": "#/definitions/S3BucketConfiguration"
        },
        "kmsKeyArn": {
            "type": "string",
            "maxLength": 2048,
            "minLength": 1,
            "additionalProperties": false
        },
        "loggingBucket": {
            "$ref": "#/definitions/S3BucketConfiguration"
        }
    },
    "additionalProperties": false
},
"S3BucketConfiguration": {
    "type": "object",
    "properties": {
        "retentionDays": {

```

```

        "type": "number",
        "minimum": 1,
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "SecurityRoles": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "accountId"
      ]
    }
  },
  "Config": {
    "type": "object",
    "required": [
      "enabled"
    ],

```

```

    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      },
      "configurations": {
        "$ref": "#/definitions/ConfigConfiguration"
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "accountId"
      ]
    }
  },
  "ConfigConfiguration": {
    "type": "object",
    "required": [],
    "properties": {
      "loggingBucket": {
        "$ref": "#/definitions/S3BucketConfiguration"
      },
      "accessLoggingBucket": {
        "$ref": "#/definitions/S3BucketConfiguration"
      },
      "kmsKeyArn": {
        "type": "string",
        "maxLength": 2048,
        "minLength": 1,

```

```

        "additionalProperties": false
      }
    }
  }
}

```

Schema della zona di atterraggio 3.3

```

{
  "type": "object",
  "required": [
    "centralizedLogging",
    "organizationStructure",
    "securityRoles"
  ],
  "properties": {
    "accessManagement": {
      "$ref": "#/definitions/AccessManagement"
    },
    "backup": {
      "$ref": "#/definitions/Backup"
    },
    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
        "additionalProperties": false
      },
      "additionalProperties": false
    },
    "organizationStructure": {
      "$ref": "#/definitions/OrganizationStructure"
    },
    "securityRoles": {
      "$ref": "#/definitions/SecurityRoles"
    }
  }
}

```



```
},
"additionalProperties": false,
"definitions": {
  "AccessManagement": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    },
    "additionalProperties": false
  },
  "Backup": {
    "type": "object",
    "properties": {
      "configurations": {
        "$ref": "#/definitions/BackupConfigurations"
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "configurations"
      ]
    }
  },
  "BackupAdminConfigurations": {
```

```
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "BackupConfigurations": {
    "type": "object",
    "required": [
      "backupAdmin",
      "centralBackup",
      "kmsKeyArn"
    ],
    "properties": {
      "backupAdmin": {
        "$ref": "#/definitions/BackupAdminConfigurations"
      },
      "centralBackup": {
        "$ref": "#/definitions/CentralBackupConfigurations"
      },
      "kmsKeyArn": {
        "type": "string",
        "maxLength": 2048,
        "minLength": 1,
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "CentralBackupConfigurations": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
```

```

        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"CentralizedLogging": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        },
        "configurations": {
            "$ref": "#/definitions/LoggingConfigurations"
        },
        "enabled": {
            "type": "boolean",
            "additionalProperties": false,
            "default": true
        }
    },
    "additionalProperties": false
},
"LoggingConfigurations": {
    "type": "object",
    "properties": {
        "accessLoggingBucket": {
            "$ref": "#/definitions/S3BucketConfiguration"
        },
        "kmsKeyArn": {
            "type": "string",
            "maxLength": 2048,
            "minLength": 1,

```

```

        "additionalProperties": false
      },
      "loggingBucket": {
        "$ref": "#/definitions/S3BucketConfiguration"
      }
    },
    "additionalProperties": false
  },
  "OrganizationalUnit": {
    "type": "object",
    "required": [
      "name"
    ],
    "properties": {
      "name": {
        "type": "string",
        "maxLength": 120,
        "minLength": 1,
        "pattern": "^[\\s\\S]*$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "OrganizationStructure": {
    "type": "object",
    "required": [
      "security"
    ],
    "properties": {
      "sandbox": {
        "$ref": "#/definitions/OrganizationalUnit"
      },
      "security": {
        "$ref": "#/definitions/OrganizationalUnit"
      }
    },
    "additionalProperties": false
  },
  "S3BucketConfiguration": {
    "type": "object",
    "properties": {
      "retentionDays": {
        "type": "number",

```

```

        "minimum": 1,
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "SecurityRoles": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  }
}

```

Schema della zona di atterraggio 3.2

```

{
  "type": "object",
  "required": [
    "centralizedLogging",
    "organizationStructure",
    "securityRoles"
  ],
  "properties": {
    "accessManagement": {
      "$ref": "#/definitions/AccessManagement"
    },
    "backup": {
      "$ref": "#/definitions/Backup"
    },
    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    }
  }
}

```

```

    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
        "additionalProperties": false
      },
      "additionalProperties": false
    },
    "organizationStructure": {
      "$ref": "#/definitions/OrganizationStructure"
    },
    "securityRoles": {
      "$ref": "#/definitions/SecurityRoles"
    }
  },
  "additionalProperties": false,
  "definitions": {
    "AccessManagement": {
      "type": "object",
      "required": [
        "enabled"
      ],
      "properties": {
        "enabled": {
          "type": "boolean",
          "additionalProperties": false,
          "default": true
        }
      },
      "additionalProperties": false
    },
    "Backup": {
      "type": "object",
      "properties": {
        "configurations": {
          "$ref": "#/definitions/BackupConfigurations"
        },
        "enabled": {
          "type": "boolean",
          "additionalProperties": false,

```

```

        "default": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "configurations"
      ]
    }
  },
  "BackupAdminConfigurations": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "BackupConfigurations": {
    "type": "object",
    "required": [
      "backupAdmin",
      "centralBackup",
      "kmsKeyArn"
    ],
    "properties": {
      "backupAdmin": {
        "$ref": "#/definitions/BackupAdminConfigurations"
      }
    },

```

```

        "centralBackup": {
            "$ref": "#/definitions/CentralBackupConfigurations"
        },
        "kmsKeyArn": {
            "type": "string",
            "maxLength": 2048,
            "minLength": 1,
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"CentralBackupConfigurations": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"CentralizedLogging": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        },
        "configurations": {
            "$ref": "#/definitions/LoggingConfigurations"
        }
    },

```



```

        "enabled": {
            "type": "boolean",
            "additionalProperties": false,
            "default": true
        }
    },
    "additionalProperties": false
},
"LoggingConfigurations": {
    "type": "object",
    "properties": {
        "accessLoggingBucket": {
            "$ref": "#/definitions/S3BucketConfiguration"
        },
        "kmsKeyArn": {
            "type": "string",
            "maxLength": 2048,
            "minLength": 1,
            "additionalProperties": false
        },
        "loggingBucket": {
            "$ref": "#/definitions/S3BucketConfiguration"
        }
    },
    "additionalProperties": false
},
"OrganizationalUnit": {
    "type": "object",
    "required": [
        "name"
    ],
    "properties": {
        "name": {
            "type": "string",
            "maxLength": 120,
            "minLength": 1,
            "pattern": "^[\\s\\S]*$",
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"OrganizationStructure": {
    "type": "object",

```

```

        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizationalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizationalUnit"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
                "pattern": "^\\d{12}$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    }
}

```

Schema della zona di atterraggio 3.1

```
{
  "type": "object",
  "required": [
    "centralizedLogging",
    "organizationStructure",
    "securityRoles"
  ],
  "properties": {
    "accessManagement": {
      "$ref": "#/definitions/AccessManagement"
    },
    "backup": {
      "$ref": "#/definitions/Backup"
    },
    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
        "additionalProperties": false
      },
      "additionalProperties": false
    },
    "organizationStructure": {
      "$ref": "#/definitions/OrganizationStructure"
    },
    "securityRoles": {
      "$ref": "#/definitions/SecurityRoles"
    }
  },
  "additionalProperties": false,
  "definitions": {
    "AccessManagement": {
      "type": "object",
      "required": [
        "enabled"
      ]
    }
  }
}
```

```

    ],
    "properties": {
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    },
    "additionalProperties": false
  },
  "Backup": {
    "type": "object",
    "properties": {
      "configurations": {
        "$ref": "#/definitions/BackupConfigurations"
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "configurations"
      ]
    }
  },
  "BackupAdminConfigurations": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",

```

```

        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
    }
},
    "additionalProperties": false
},
"BackupConfigurations": {
    "type": "object",
    "required": [
        "backupAdmin",
        "centralBackup",
        "kmsKeyArn"
    ],
    "properties": {
        "backupAdmin": {
            "$ref": "#/definitions/BackupAdminConfigurations"
        },
        "centralBackup": {
            "$ref": "#/definitions/CentralBackupConfigurations"
        },
        "kmsKeyArn": {
            "type": "string",
            "maxLength": 2048,
            "minLength": 1,
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"CentralBackupConfigurations": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        }
    }
}

```

```

    },
    "additionalProperties": false
  },
  "CentralizedLogging": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      },
      "configurations": {
        "$ref": "#/definitions/LoggingConfigurations"
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    }
  },
  "additionalProperties": false
},
"LoggingConfigurations": {
  "type": "object",
  "properties": {
    "accessLoggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    },
    "kmsKeyArn": {
      "type": "string",
      "maxLength": 2048,
      "minLength": 1,
      "additionalProperties": false
    },
    "loggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    }
  }
},
"additionalProperties": false

```

```
    },
    "OrganizationalUnit": {
      "type": "object",
      "required": [
        "name"
      ],
      "properties": {
        "name": {
          "type": "string",
          "maxLength": 120,
          "minLength": 1,
          "pattern": "^[\\s\\S]*$",
          "additionalProperties": false
        }
      },
      "additionalProperties": false
    },
    "OrganizationStructure": {
      "type": "object",
      "required": [
        "security"
      ],
      "properties": {
        "sandbox": {
          "$ref": "#/definitions/OrganizationalUnit"
        },
        "security": {
          "$ref": "#/definitions/OrganizationalUnit"
        }
      },
      "additionalProperties": false
    },
    "S3BucketConfiguration": {
      "type": "object",
      "properties": {
        "retentionDays": {
          "type": "number",
          "minimum": 1,
          "additionalProperties": false
        }
      },
      "additionalProperties": false
    },
    "SecurityRoles": {
```

```
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  }
}
```

Avvia una landing zone usando CloudFormation

Puoi configurare e avviare una landing zone CloudFormation tramite la CloudFormation console, o tramite AWS CLI. Questa sezione fornisce istruzioni ed esempi per avviare una landing zone utilizzando le API tramite CloudFormation.

Argomenti

- [Prerequisiti per il lancio di una landing zone utilizzando CloudFormation](#)
- [Crea una nuova landing zone usando CloudFormation](#)
- [Gestisci una landing zone esistente usando CloudFormation](#)

Prerequisiti per il lancio di una landing zone utilizzando CloudFormation

1. Da AWS CLI, utilizza l' AWS Organizations `CreateOrganizationAPI` per creare un'organizzazione e abilitare tutte le funzionalità.

Per istruzioni più dettagliate, consulta [Fase 1: Configura la tua landing zone](#).

2. Dalla CloudFormation console o utilizzando il AWS CLI, distribuisce un CloudFormation modello che crei le seguenti risorse nell'account di gestione:
 - Account Log Archive (a volte chiamato account «Logging»)
 - Account di controllo (a volte chiamato account «Security»)

- I ruoli `AWSControlTowerAdmin`, `AWSControlTowerCloudTrailRole`, `AWSControlTowerConfigAggregatorRoleForOrganizations`, e `AWSControlTowerStackSetRole` di servizio.

Per informazioni su come AWS Control Tower utilizza questi ruoli per eseguire chiamate API di landing zone, consulta [Fase 1: Configurazione della landing zone](#).

Parameters:

```
LoggingAccountEmail:
  Type: String
  Description: The email Id for centralized logging account
LoggingAccountName:
  Type: String
  Description: Name for centralized logging account
SecurityAccountEmail:
  Type: String
  Description: The email Id for security roles account
SecurityAccountName:
  Type: String
  Description: Name for security roles account
```

Resources:

```
MyOrganization:
  Type: 'AWS::Organizations::Organization'
  Properties:
    FeatureSet: ALL
LoggingAccount:
  Type: 'AWS::Organizations::Account'
  Properties:
    AccountName: !Ref LoggingAccountName
    Email: !Ref LoggingAccountEmail
SecurityAccount:
  Type: 'AWS::Organizations::Account'
  Properties:
    AccountName: !Ref SecurityAccountName
    Email: !Ref SecurityAccountEmail
AWSControlTowerAdmin:
  Type: 'AWS::IAM::Role'
  Properties:
    RoleName: AWSControlTowerAdmin
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
```

```

    Principal:
      Service: controltower.amazonaws.com
      Action: 'sts:AssumeRole'
    Path: '/service-role/'
    ManagedPolicyArns:
      - !Sub >-
        arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
AWSControlTowerAdminPolicy:
  Type: 'AWS::IAM::Policy'
  Properties:
    PolicyName: AWSControlTowerAdminPolicy
    PolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Action: 'ec2:DescribeAvailabilityZones'
          Resource: '*'
    Roles:
      - !Ref AWSControlTowerAdmin
AWSControlTowerCloudTrailRole:
  Type: 'AWS::IAM::Role'
  Properties:
    RoleName: AWSControlTowerCloudTrailRole
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
            Service: cloudtrail.amazonaws.com
          Action: 'sts:AssumeRole'
    Path: '/service-role/'
AWSControlTowerCloudTrailRolePolicy:
  Type: 'AWS::IAM::Policy'
  Properties:
    PolicyName: AWSControlTowerCloudTrailRolePolicy
    PolicyDocument:
      Version: 2012-10-17
      Statement:
        - Action:
            - 'logs:CreateLogStream'
            - 'logs:PutLogEvents'
          Resource: !Sub >-

```

```

        arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
    Effect: Allow
    Roles:
        - !Ref AWSControlTowerCloudTrailRole
AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
        RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
        AssumeRolePolicyDocument:
            Version: 2012-10-17
            Statement:
                - Effect: Allow
                  Principal:
                      Service: config.amazonaws.com
                  Action: 'sts:AssumeRole'
        Path: '/service-role/'
        ManagedPolicyArns:
            - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
        RoleName: AWSControlTowerStackSetRole
        AssumeRolePolicyDocument:
            Version: 2012-10-17
            Statement:
                - Effect: Allow
                  Principal:
                      Service: cloudformation.amazonaws.com
                  Action: 'sts:AssumeRole'
        Path: '/service-role/'
AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
        PolicyName: AWSControlTowerStackSetRolePolicy
        PolicyDocument:
            Version: 2012-10-17
            Statement:
                - Action: 'sts:AssumeRole'
                  Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
    Effect: Allow
    Roles:

```

```
- !Ref AWSControlTowerStackSetRole
```

Outputs:**LogAccountId:****Value:****Fn::GetAtt:** LoggingAccount.AccountId**Export:****Name:** LogAccountId**SecurityAccountId:****Value:****Fn::GetAtt:** SecurityAccount.AccountId**Export:****Name:** SecurityAccountId

Crea una nuova landing zone usando CloudFormation

Dalla CloudFormation console o utilizzando il AWS CLI, implementa il seguente CloudFormation modello per creare una landing zone.

Parameters:**Version:****Type:** String**Description:** The version number of Landing Zone**GovernedRegions:****Type:** CommaDelimitedList**Description:** List of governed regions**SecurityOuName:****Type:** String**Description:** The security Organizational Unit name**SandboxOuName:****Type:** String**Description:** The sandbox Organizational Unit name**CentralizedLoggingAccountId:****Type:** String**Description:** The AWS account ID for centralized logging**SecurityAccountId:****Type:** String**Description:** The AWS account ID for security roles**LoggingBucketRetentionPeriod:****Type:** Number**Description:** Retention period for centralized logging bucket**AccessLoggingBucketRetentionPeriod:**

```
Type: Number
Description: Retention period for access logging bucket
KMSKey:
  Type: String
  Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
  logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
```

```
enabled: true
```

Gestisci una landing zone esistente usando CloudFormation

Puoi utilizzarla CloudFormation per gestire una landing zone che hai già lanciato importando la landing zone in uno CloudFormation stack nuovo o esistente. Per dettagli [e istruzioni, consulta CloudFormation la sezione Gestione delle risorse esistenti](#).

Per [rilevare e risolvere la deriva all'interno di una landing zone](#), puoi utilizzare la console AWS Control Tower AWS CLI, o l'[ResetLandingZoneAPI](#).

Fasi successive

Ora che la tua zona di atterraggio è impostata, è pronta per l'uso.

Per ulteriori informazioni su come utilizzare AWS Control Tower, consulta i seguenti argomenti:

- Per le procedure amministrative consigliate, consultare [Best Practice](#).
- Puoi configurare utenti e gruppi IAM Identity Center con ruoli e autorizzazioni specifici. Per le raccomandazioni, vedere [Consigli per la configurazione di gruppi, ruoli e politiche](#).
- Per iniziare a registrare organizzazioni e account dalle tue AWS Organizations implementazioni, consulta [Gestire le organizzazioni e gli account esistenti](#).
- I tuoi utenti finali possono effettuare il provisioning dei propri AWS account nella tua zona di destinazione utilizzando Account Factory. Per ulteriori informazioni, consulta [Autorizzazioni per la configurazione e il provisioning degli account](#).
- A tal fine [Convalida della conformità per AWS Control Tower](#), gli amministratori del cloud centrale possono esaminare gli archivi di log nell'account Log Archive, mentre i revisori di terze parti designati possono esaminare le informazioni di audit nell'account Audit (condiviso), che è membro dell'unità organizzativa di sicurezza.
- Per saperne di più sulle funzionalità di AWS Control Tower, consulta le informazioni [correlate](#).
- Di tanto in tanto, potrebbe essere necessario aggiornare la zona di destinazione per ottenere gli ultimi aggiornamenti di backend, i controlli più recenti e per mantenerla aggiornata. Per ulteriori informazioni, consulta [Gestione degli aggiornamenti di configurazione in AWS Control Tower](#).
- Se riscontri problemi durante l'utilizzo di AWS Control Tower, consulta [Risoluzione dei problemi](#)

 Important

Se non hai ancora abilitato l'autenticazione a più fattori per l'utente root del tuo account, fallo ora. Per ulteriori informazioni sulle best practice per l'utente root, consulta [Best practice per proteggere l'utente](#) root dell'account.

Limitazioni e quote in AWS Control Tower

Questo capitolo illustra le limitazioni e le quote dei AWS servizi da tenere a mente quando si utilizza AWS Control Tower. Se non riesci a configurare la tua zona di atterraggio a causa di un problema relativo alla quota di servizio, contatta [Supporto AWS](#).

Per ulteriori informazioni sulle limitazioni specifiche dei controlli, consulta [Limitazioni di controllo](#).

La guida di riferimento sui controlli

Le informazioni dettagliate sui controlli AWS Control Tower sono state spostate [nella AWS Control Tower Controls Reference Guide](#).

Limitazioni note in AWS Control Tower

Questa sezione descrive le limitazioni note e i casi d'uso non supportati in AWS Control Tower.

- AWS Control Tower presenta limitazioni generali sulla concorrenza. In generale, è consentita un'operazione alla volta. Sono ammesse due eccezioni a questa limitazione:
 - I controlli opzionali possono essere attivati e disattivati contemporaneamente, tramite un processo asincrono. In totale possono essere eseguite fino a cento (100) operazioni relative al controllo alla volta, indipendentemente dal fatto che vengano richiamate dalla console o da un'API.
 - È possibile effettuare il provisioning, l'aggiornamento e la registrazione degli account contemporaneamente in Account Factory, tramite un processo asincrono, con un massimo di cinque (5) operazioni relative all'account in corso contemporaneamente. L'annullamento della gestione degli account deve essere eseguito un account alla volta.
 - Con la registrazione automatica abilitata, è possibile eseguire una sola operazione sull'account di trasferimento sull'unità organizzativa di destinazione e qualsiasi altra operazione relativa all'account sulla stessa unità organizzativa verrà considerata in conflitto fino al termine dell'operazione di trasferimento dell'account.
- Account Factory for Terraform (AFT) ha parametri di concorrenza aggiuntivi configurati durante l'implementazione. AWS ha testato AFT con questi valori predefiniti:
 - `concurrent_account_factory_actions`: 5 (provisioning dell'account)
 - `maximum_concurrent_customizations`: 5 (pipeline di personalizzazione)

L'aumento di questi limiti oltre i valori predefiniti testati può ridurre la stabilità.

- Gli indirizzi e-mail degli account condivisi nell'unità organizzativa di sicurezza possono essere modificati, ma è necessario aggiornare la zona di destinazione per vedere queste modifiche nella console AWS Control Tower.
- Un limite di dieci (10) SCP per unità organizzativa si applica alle unità organizzative nella zona di atterraggio di AWS Control Tower.
- AWS Control Tower supporta fino a 10.000 account nell'organizzazione della zona di destinazione, suddivisi tra tutte le unità organizzative.
- Le unità organizzative esistenti con oltre 1000 account annidati direttamente non possono essere registrate o registrate nuovamente in AWS Control Tower. Per ulteriori informazioni sulle limitazioni relative alla registrazione delle unità organizzative, consulta [Limitazioni basate sul sottostante AWS services](#)
- Le personalizzazioni per AWS Control Tower (cFCT) non sono disponibili in questi casi Regioni AWS, perché alcune dipendenze non sono disponibili:
 - Europa (Zurigo), eu-central-2
 - Europa (Spagna), eu-south-2
 - Canada occidentale (Calgary) ca-west-1
 - Asia Pacifico (Melbourne), ap-southeast-4
 - Asia Pacifico (Malesia), ap-southeast-5
 - Asia Pacifico (Tailandia), ap-southeast-7
 - Messico (centrale), mx-central-1
 - Asia Pacifico (Nuova Zelanda), ap-southeast-6
 - Asia Pacifico (Taipei), ap-east-2
 - AWS European Sovereign Cloud (Germania), eusc-de-east-1

Puoi distribuire e gestire risorse in queste regioni con cFCT, se distribuisce cFCT nella tua regione principale di AWS Control Tower, ma non puoi creare cFCT in queste regioni.

- AWS Control Tower Account Factory for Terraform (AFT) non è disponibile nelle seguenti aree Regioni AWS, perché alcune dipendenze non sono disponibili:
 - Europa (Zurigo), eu-central-2
 - Europa (Spagna), eu-south-2
 - Canada occidentale (Calgary), ca-west-1

- Asia Pacifico (Melbourne), ap-southeast-4
- Asia Pacifico (Malesia), ap-southeast-5
- Asia Pacifico (Tailandia), ap-southeast-7
- Messico (centrale), mx-central-1
- Asia Pacifico (Nuova Zelanda), ap-southeast-6
- Asia Pacifico (Taipei), ap-east-2
- AWS European Sovereign Cloud (Germania), eusc-de-east-1
- AWS Control Tower Account Factory for Terraform (AFT) non può essere distribuito da nuovi clienti AFT nelle seguenti regioni, perché non AWS CodeConnections è possibile connettersi a un sistema di controllo della versione (VCS) di terze parti:
 - Asia Pacifico (Hong Kong), Africa (Città del Capo), Medio Oriente (Bahrain), Europa (Zurigo), Asia Pacifico (Jakarta), Asia Pacifico (Hyderabad), Asia Pacifico (Osaka), Asia Pacifico (Melbourne), Israele (Tel Aviv), Europa (Spagna), Medio Oriente (Emirati Arabi Uniti), Asia Pacifico (Tailandia), Messico (Centrale)
- Le seguenti regioni non supportano. AWS Service Catalog
 - Canada occidentale (Calgary), ca-west-1
 - Asia Pacifico (Malesia), ap-southeast-5
 - Asia Pacifico (Tailandia), ap-southeast-7
 - Messico (centrale), mx-central-1
 - Asia Pacifico (Nuova Zelanda), ap-southeast-6
 - Asia Pacifico (Taipei), ap-east-2
 - AWS European Sovereign Cloud (Germania), eusc-de-east-1

 Note

Le regioni che non supportano Service Catalog non supportano le personalizzazioni di Account Factory per AWS Control Tower (AFC).

Per ulteriori informazioni sulla funzionalità di AWS Control Tower nelle regioni che non supportano AWS Service Catalog, consulta [AWS Control Tower è disponibile in AWS Canada occidentale \(Calgary\)](#)

- Quando si chiama un'API di controllo per attivare o disattivare un controllo, il limite per `EnableControl` gli `DisableControl` aggiornamenti in AWS Control Tower è di cento (100) operazioni simultanee. Dieci operazioni (10) possono essere eseguite contemporaneamente, con le restanti operazioni in coda. Potrebbe essere necessario modificare il codice per attendere il completamento.
- Quando esegui il provisioning degli account tramite Account Factory Customizations (AFC), con blueprint basati su Terraform, puoi distribuire tali blueprint su uno solo. Regione AWS Per impostazione predefinita, AWS Control Tower viene distribuito nella regione di origine.

Richiesta di un aumento della quota

La console Service Quotas fornisce informazioni sulle quote di AWS Control Tower. Puoi utilizzare la console Service Quotas per visualizzare le quote di servizio predefinite o per [richiedere](#) aumenti delle quote per le quote regolabili.

Note

Gli account e le organizzazioni appena creati potrebbero avere una quota inferiore a quella predefinita di 10 account.

Le seguenti quote possono essere visualizzate tramite la console Service Quotas

- Quota per le operazioni simultanee sull'account: il numero massimo di operazioni simultanee sull'account che possono essere eseguite contemporaneamente. Predefinito: 5, massimo: 10, regolabile
- Numero di account in una singola unità organizzativa: il numero massimo di account gestiti da AWS Control Tower che possono essere presenti in un'unità organizzativa. Se aggiungi account oltre questo limite, il processo di registrazione dell'unità organizzativa in AWS Control Tower non può essere eseguito. Per ulteriori informazioni sul numero di account per unità organizzativa, consulta la documentazione [Limitazioni basate sul sottostante AWS services](#) di AWS Control Tower. Predefinito: 1000, non regolabile.
- Operazioni simultanee per unità organizzative (OU): il numero massimo di OU-related operazioni simultanee che possono essere eseguite contemporaneamente. Predefinito: 1, non regolabile.

Ad esempio, puoi richiedere un aumento della quota da cinque a dieci operazioni simultanee relative all'account. Alcune caratteristiche prestazionali di AWS Control Tower possono cambiare dopo un aumento della quota. Ad esempio, l'aggiornamento di un'unità organizzativa potrebbe richiedere più tempo quando sono presenti più account. Oppure, potrebbe essere necessario più tempo per completare un'azione su un'unità organizzativa con cinque SCP rispetto a tre SCP.

Note

Una richiesta di aumento della quota di servizio può richiedere fino a due giorni prima che diventi effettiva. Assicurati di richiedere l'aumento della quota dalla tua regione principale di AWS Control Tower.

In alternativa, puoi contattare l'[AWS assistenza](#) per richiedere un aumento della quota per alcune risorse in AWS Control Tower. Oppure puoi guardare il video che segue e scoprire come automatizzare determinati aumenti delle quote di servizio.

Video: Automatizza le richieste di aumento delle quote di servizio nei servizi relativi ad AWS Control Tower

Questo video (7:24) descrive come automatizzare gli aumenti delle quote di servizio per i AWS servizi correlati e integrati, in base alle distribuzioni in AWS Control Tower. Mostra anche come automatizzare la registrazione di nuovi account nel supporto Enterprise per l'organizzazione. AWS Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Panoramica video degli aumenti delle quote in AWS Control Tower.](#)

Quando si effettua il provisioning di nuovi account in questo ambiente, è possibile utilizzare gli eventi del ciclo di vita per attivare richieste automatiche di aumenti delle quote di servizio in determinati casi. Regioni AWS

Ulteriori informazioni sulle AWS quote sono disponibili nel Riferimento [AWS](#) generale.

Limitazioni di controllo

AWS Control Tower ti aiuta a mantenere un ambiente sicuro con più account AWS tramite controlli implementati in varie forme, come policy di controllo dei servizi (SCP), AWS Config regole e hook. CloudFormation

La guida di riferimento sui controlli

Le informazioni dettagliate sui controlli AWS Control Tower sono state spostate [nella AWS Control Tower Controls Reference Guide](#).

Se si modificano le risorse di AWS Control Tower, ad esempio un SCP, o si rimuove una AWS Config risorsa, ad esempio un registratore o un aggregatore di configurazione, AWS Control Tower non può più garantire che i controlli funzionino come previsto. Pertanto, la sicurezza dell'ambiente con più account potrebbe essere compromessa. Il modello [di sicurezza a responsabilità AWS](#) condivisa è applicabile a qualsiasi modifica apportata dall'utente.

Note

AWS Control Tower aiuta a mantenere l'integrità dell'ambiente ripristinando gli SCP dei controlli preventivi alla loro configurazione standard quando si aggiorna la zona di atterraggio. Le modifiche che potresti aver apportato agli SCP vengono sostituite dalla versione standard del controllo, in base alla progettazione.

Limitazioni per regione

Alcuni controlli in AWS Control Tower non funzionano in determinati Regioni AWS luoghi in cui AWS Control Tower è disponibile, poiché tali regioni non supportano le funzionalità di base richieste. Di conseguenza, quando si implementa tale controllo, potrebbe non essere operativo in tutte le regioni gestite da AWS Control Tower. Questa limitazione riguarda alcuni controlli investigativi, alcuni controlli proattivi e alcuni controlli nello standard CSPM Service-managed di Security Hub: AWS Control Tower. Per ulteriori informazioni sulla disponibilità regionale, consulta i controlli di Security Hub. <https://docs.aws.amazon.com/controltower/latest/controlreference/security-hub-controls.html> Consulta anche la documentazione dell'elenco dei servizi [regionali](#) e la documentazione di riferimento dei controlli CSPM di [Security Hub](#).

Il comportamento di controllo è limitato anche in caso di governance mista. Per ulteriori informazioni, consulta [Evita una governance mista durante la configurazione delle regioni](#).

Per ulteriori informazioni su come AWS Control Tower gestisce le limitazioni di regioni e controlli, consulta [Considerazioni per l'attivazione AWS Regioni con attivazione](#).

 Note

Per le informazioni più aggiornate sui controlli e sul supporto delle regioni, ti consigliamo di chiamare [GetControl](#) and [ListControls](#) API operations.

Trova i controlli e le aree disponibili

Puoi visualizzare le regioni disponibili per ciascun controllo nella console AWS Control Tower. Puoi visualizzare le regioni disponibili a livello di codice con le [ListControls](#) API [GetControl](#) e di Control Catalog. AWS

Per informazioni sui AWS Security Hub CSPM controlli di Service-Managed Standard: AWS Control Tower che non sono supportati in alcune regioni Regioni AWS, consulta «Regioni non supportate» nello standard [Security Hub CSPM](#).

Limitazioni basate sul sottostante AWS services

Questa pagina descrive le limitazioni che potresti incontrare a causa delle limitazioni di altri AWS servizi e il modo in cui AWS Control Tower funziona con tali servizi.

Linee guida generali

Come regola generale, prevediamo che il numero di account supportati durante la registrazione di un'unità organizzativa diminuisca all'aumentare del numero di regioni governate e del numero di controlli abilitati per tale unità organizzativa. Queste linee guida generali presuppongono che siano abilitati 15 controlli opzionali. Se hai più o meno controlli abilitati sulla tua unità organizzativa, i limiti degli account per unità organizzativa saranno diversi al momento della registrazione.

- Con 15 regioni governate, sono supportate OU con un massimo di 1000 account.
- Con 16-21 regioni governate, la dimensione massima delle unità organizzative supportate è compresa tra 600 e 1000 account.
- Con 22 regioni governate, sono supportate unità organizzative con un massimo di 680 account.
- Con 23 o più regioni governate, la dimensione massima delle unità organizzative supportate è inferiore a 680 account.

In caso di errore

Se la registrazione fallisce, puoi provare Re-register l'unità organizzativa. Inoltre, puoi ridurre le dimensioni dell'unità organizzativa utilizzando un'unità organizzativa annidata o spostando gli account in un'altra unità organizzativa.

Note

I controlli obbligatori che AWS Control Tower applica sempre non vengono conteggiati nel numero di controlli abilitati su un'unità organizzativa, ai fini della registrazione.

CloudFormation limitazioni degli stack set

Se prevedi di registrare un numero elevato di account su più account Regioni AWS, potresti riscontrare dei limiti creati dagli CloudFormation stack set sulle dimensioni complessive di un'organizzazione. Puoi stimare la limitazione con questa formula:

Numero di account gestiti nell'organizzazione x Numero di regioni governate $\leq$ 150.000

Questa limitazione diventa evidente durante il processo di registrazione dell'unità organizzativa. Ad esempio, se sono governate 15 regioni e sono abilitati 15 controlli opzionali, il limite per la registrazione dell'unità organizzativa è di 1000 account. Tuttavia, se devi registrare un'unità organizzativa con più di 1000 account o se hai un numero elevato di controlli opzionali abilitati, devi ridurre il numero di regioni governate al di sotto di 15. Questa riduzione è dovuta alle limitazioni dello stack set.

AWS Config limitazioni

Se prevedi di registrare unità organizzative con un numero elevato di account, potresti riscontrare dei limiti relativi [al numero massimo di account che AWS Config è possibile creare o eliminare ogni settimana](#), in tutti gli aggregatori. Gli account registrati non vengono conteggiati ai fini di questo limite: puoi registrare fino a 1000 nuovi account in AWS Control Tower ogni settimana.

First-time limitazioni per gli account e le regioni opt-in

Se prevedi di registrare OU con un numero elevato di account in più regioni opt-in per la prima volta, potresti riscontrare delle limitazioni dovute alle quote di gestione degli [account](#), che possono portare a una latenza prolungata. Possono verificarsi errori durante la registrazione dell'unità organizzativa a causa della latenza.

Differenze regionali per le funzionalità di AWS Control Tower

Esistono alcune differenze nel comportamento di AWS Control Tower Regioni AWS, poiché AWS Control Tower orchestra il comportamento di altri AWS servizi. Ad esempio:

- AWS Service Catalog non è disponibile in tutti i paesi in Regioni AWS cui è disponibile AWS Control Tower, il che modifica il comportamento di Account Factory in quelle regioni.
- In alcune regioni, Account Factory Customizations (AFC) non è disponibile perché Service Catalog non è disponibile per supportare le funzionalità di base per i blueprint.
- Alcuni controlli non sono disponibili in tutti i casi a Regioni AWS causa della mancanza di funzionalità di base.
- AFT e cFCT non sono completamente disponibili a Regioni AWS causa della mancanza di funzionalità di base.

Per determinare al meglio il comportamento del tuo ambiente AWS Control Tower, verifica la tua regione di residenza. Quindi, valuta i seguenti elementi. Per maggiori dettagli, consulta [Limitazioni e quote in AWS Control Tower](#).

- È AWS Service Catalog disponibile nella regione di origine desiderata?
- Sono disponibili i controlli di cui hai bisogno? Vedi Limitazioni di [controllo](#).
- IAM Identity Center è disponibile nella regione di residenza desiderata?

Regioni implementabili per i controlli

AWS Control Tower non può attivare determinati controlli quando li distribuisce in determinate regioni, a causa della mancanza di dipendenze sottostanti. Puoi trovare le informazioni più aggiornate sulle regioni distribuibili per qualsiasi controllo richiamando le `ListControls` API and. `GetControl` Puoi anche visualizzare le regioni distribuibili nella console AWS Control Tower.

Quando attivi un controllo su un'unità organizzativa governata da AWS Control Tower, l'area effettiva del controllo è l'intersezione delle regioni gestite da AWS Control Tower con le regioni distribuibili del controllo.

Ad esempio, un controllo può essere abilitato su un'unità organizzativa che opera nelle regioni X, Y e Z governate. Ma dopo averlo abilitato, lo stesso controllo viene distribuito solo nelle regioni X e Z, poiché il controllo stesso non supporta la regione Y.

È importante monitorare le relazioni tra i controlli distribuiti e le regioni in cui gestisci i carichi di lavoro in AWS Control Tower, in modo da non riscontrare lacune nella protezione delle risorse. AWS

Come controllare le tue regioni protette

- Nella console AWS Control Tower, puoi visualizzare i controlli e le regioni abilitati nella sezione Controlli abilitati.
- Se chiami l'GetEnabledControlAPI, il parametro targetRegions mostrerà solo le regioni in cui è possibile distribuire il controllo in modo efficace, non le regioni non distribuibili.

La guida di riferimento di AWS Control Tower Controls

Le informazioni dettagliate sui controlli in AWS Control Tower sono state trasferite nella [AWS Control Tower Controls Reference Guide](#) .

Le migliori pratiche per gli amministratori di AWS Control Tower

Questo argomento è destinato principalmente agli amministratori degli account di gestione.

Gli amministratori degli account di gestione hanno la responsabilità di spiegare alcune attività che i controlli di AWS Control Tower impediscono agli amministratori degli account membri di svolgere. Questo argomento descrive alcune best practice e procedure per trasferire queste conoscenze e fornisce altri suggerimenti per configurare e mantenere l'ambiente AWS Control Tower in modo efficiente.

Spiegazione dell'accesso agli utenti

La console AWS Control Tower è disponibile solo per gli utenti con le autorizzazioni di amministratore dell'account di gestione. Solo questi utenti possono svolgere attività amministrative all'interno della tua landing zone. In base alle best practice, ciò significa che la maggior parte degli utenti e degli amministratori degli account membri non vedrà mai la console AWS Control Tower. In qualità di membro del gruppo di amministratori degli account di gestione, è tua responsabilità spiegare le seguenti informazioni agli utenti e agli amministratori dei tuoi account membri, a seconda dei casi.

- Spiega a quali AWS risorse hanno accesso utenti e amministratori all'interno della landing zone.
- Elenca i controlli preventivi che si applicano a ciascuna unità organizzativa (OU) in modo che gli altri amministratori possano pianificare ed eseguire i propri AWS carichi di lavoro di conseguenza.

Spiegazione dell'accesso alle risorse

Alcuni amministratori e altri utenti potrebbero aver bisogno di una spiegazione delle AWS risorse a cui hanno accesso all'interno della tua landing zone. Questo accesso può includere l'accesso programmatico e l'accesso basato sulla console. In generale, è consentito l'accesso in lettura e scrittura alle AWS risorse. Per eseguire Work Within AWS, gli utenti necessitano di un certo livello di accesso ai servizi specifici di cui hanno bisogno per svolgere il proprio lavoro.

Alcuni utenti, ad esempio gli AWS sviluppatori, potrebbero aver bisogno di conoscere le risorse a cui hanno accesso, in modo da poter creare soluzioni ingegneristiche. Gli altri utenti, come gli utenti finali delle applicazioni che eseguono sui AWS servizi, non hanno bisogno di conoscere AWS le risorse all'interno della landing zone.

AWS offre strumenti per identificare l'ambito di accesso alle AWS risorse di un utente. Dopo aver identificato l'ambito dell'accesso di un utente, è possibile condividere tali informazioni con l'utente, in conformità con i criteri di gestione delle informazioni dell'organizzazione. Per ulteriori informazioni su questi strumenti, vedere i collegamenti che seguono.

- **AWS access advisor:** lo strumento Access Advisor AWS Identity and Access Management (IAM) consente di determinare le autorizzazioni di cui dispongono gli sviluppatori analizzando l'ultimo timestamp in cui un'entità IAM, ad esempio un utente, un ruolo o un gruppo, ha chiamato un servizio. AWS È possibile controllare l'accesso al servizio e rimuovere le autorizzazioni non necessarie e automatizzare il processo, se necessario. Per ulteriori informazioni, consulta il [nostro AWS](#) post sul blog sulla sicurezza.
- **Simulatore di policy IAM:** con il simulatore di policy IAM, puoi testare e risolvere i problemi IAM-based delle policy basate sulle risorse. Per ulteriori informazioni, consulta [Testare le politiche IAM con IAM](#) Policy Simulator.
- **AWS CloudTrail log:** puoi esaminare i AWS CloudTrail log per vedere le azioni intraprese da un utente, ruolo o. Servizio AWS Per ulteriori informazioni in merito CloudTrail, consulta la Guida per [l'AWS CloudTrail utente](#).

Le azioni intraprese dagli amministratori delle landing zone di AWS Control Tower sono visualizzabili nell'account di gestione delle landing zone. Le azioni intraprese dagli amministratori e dagli utenti degli account membri sono visualizzabili nell'account di archiviazione dei log condiviso.

Puoi visualizzare una tabella riassuntiva degli eventi di AWS Control Tower nella [pagina Attività](#).

Spiegazione dei controlli preventivi

Un controllo preventivo garantisce che gli account dell'organizzazione mantengano la conformità con le politiche aziendali. Lo stato del controllo preventivo è imposto o non abilitato. Un controllo preventivo previene le violazioni delle politiche utilizzando politiche di controllo dei servizi (SCP), politiche di controllo delle risorse (RCP) o politiche dichiarative. In confronto, un controllo investigativo ti informa di vari eventi o stati esistenti, mediante regole definite. AWS Config

Alcuni utenti, come gli AWS sviluppatori, potrebbero aver bisogno di conoscere i controlli preventivi che si applicano a tutti gli account e le unità organizzative che utilizzano, in modo da poter creare soluzioni ingegneristiche. La procedura seguente offre alcune indicazioni su come fornire queste informazioni agli utenti giusti, in base ai criteri di gestione delle informazioni dell'organizzazione.

 Note

Questa procedura presuppone che tu abbia già creato almeno un'unità organizzativa secondaria all'interno della tua landing zone, oltre ad almeno un Centro identità AWS IAM utente.

Esempio: mostrare i controlli preventivi agli utenti che hanno bisogno di sapere

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower/>.
2. Dalla barra di navigazione a sinistra, scegli Organizzazione.
3. Nella tabella, scegli il nome di una delle unità organizzative per cui l'utente necessita di informazioni sui controlli applicabili.
4. Annota il nome dell'unità organizzativa e i controlli che si applicano a questa unità organizzativa.
5. Ripetere i due passaggi precedenti per ogni unità organizzativa su cui l'utente ha bisogno di informazioni.

Per informazioni dettagliate sui controlli e le relative funzioni, consulta [Informazioni sui controlli in AWS Control Tower](#).

Pianifica la tua landing zone di AWS Control Tower

Durante il processo di configurazione, AWS Control Tower lancia una risorsa chiave associata al tuo account, chiamata landing zone, che funge da home per le tue organizzazioni e i loro account.

 Note

Puoi avere una landing zone per organizzazione.

Per informazioni su alcune best practice da seguire quando pianifichi e configuri la landing zone, consulta [AWS strategia multi-account per la tua landing zone di AWS Control Tower](#).

Modi per configurare AWS Control Tower

Puoi configurare una landing zone di AWS Control Tower in un'organizzazione esistente oppure puoi iniziare creando una nuova organizzazione che contenga la tua landing zone di AWS Control Tower.

- [Avvia AWS Control Tower in un'organizzazione esistente](#): Questa sezione è dedicata ai clienti già AWS Organizations pronti per l'adozione della governance da parte di AWS Control Tower.
- [Lancio di AWS Control Tower in una nuova organizzazione](#): Questa sezione è dedicata ai clienti senza unità AWS Organizations organizzative e account esistenti.

Note

Se disponi già di una AWS Organizations landing zone, puoi estendere la governance di AWS Control Tower dalla landing zone esistente ad alcune o tutte le unità organizzative e gli account esistenti all'interno di un'organizzazione. Vedi [Governare le organizzazioni e gli account esistenti](#).

Confronta le funzionalità

Ecco un breve confronto delle differenze tra l'aggiunta di AWS Control Tower a un'organizzazione esistente o l'estensione della governance di AWS Control Tower alle unità organizzative e agli account. Inoltre, si applicano alcune considerazioni speciali se si passa ad AWS Control Tower dalla soluzione AWS Landing Zone.

Informazioni sull'aggiunta a un'organizzazione esistente: aggiungere AWS Control Tower a un'organizzazione esistente è qualcosa che puoi realizzare all'interno della AWS console. In questo caso, hai già creato un'organizzazione nel AWS Organizations servizio, che non è attualmente registrata presso AWS Control Tower e desideri aggiungere una landing zone in seguito.

Quando aggiungi una landing zone a un'organizzazione esistente, AWS Control Tower imposta una struttura parallela, a AWS Organizations livello. Non modifica le unità organizzative e gli account all'interno dell'organizzazione esistente.

Informazioni sull'estensione della governance: l'estensione della governance si applica a unità organizzative e account specifici all'interno di una singola organizzazione già registrata presso AWS Control Tower, il che significa che esiste già una landing zone per quell'organizzazione. Estendere la governance significa che i controlli di AWS Control Tower vengono estesi in modo che i relativi vincoli si applichino alle unità organizzative e agli account specifici all'interno dell'organizzazione registrata. In questo caso, non stai lanciando una nuova landing zone, stai solo espandendo la landing zone attuale per la tua organizzazione.

 Important

Considerazione speciale: se attualmente utilizzi la [soluzione AWS Landing Zone \(ALZ\)](#) per AWS Organizations, contatta il tuo architetto di AWS soluzioni prima di provare ad abilitare AWS Control Tower nella tua organizzazione. AWS Control Tower non può eseguire controlli preliminari per determinare se AWS Control Tower possa interferire con l'attuale implementazione della landing zone. Per ulteriori informazioni, consulta [Procedura dettagliata: passaggio da ALZ a AWS Control Tower](#). Inoltre, per informazioni sullo spostamento degli account da una landing zone all'altra, vedi [Se l'account non soddisfa i prerequisiti](#)

Avvia AWS Control Tower in un'organizzazione esistente

Configurando una landing zone di AWS Control Tower in un'organizzazione esistente, puoi iniziare a lavorare immediatamente, in parallelo AWS Organizations all'ambiente esistente. Le altre unità organizzative create all'interno AWS Organizations sono invariate, in quanto non sono registrate con AWS Control Tower. Puoi continuare a utilizzare le unità organizzative e gli account esattamente come sono.

AWS Control Tower si consolida utilizzando l'account di gestione dell'organizzazione esistente come account di gestione. Non è necessario un nuovo account di gestione. Puoi avviare la landing zone di AWS Control Tower dal tuo account di gestione esistente.

 Note

Per configurare AWS Control Tower su un'organizzazione esistente, i limiti del servizio devono consentire la creazione di almeno due account aggiuntivi.

Effetti dell'aggiunta di AWS Control Tower all'organizzazione esistente

AWS Control Tower crea due account nell'organizzazione: un account di audit e un account di registrazione. Questi account registrano le azioni intraprese dal team, nei rispettivi account individuali degli utenti finali. Gli account di archiviazione Audit e Log vengono visualizzati nell'unità organizzativa di sicurezza all'interno della landing zone di AWS Control Tower.

Quando configuri la landing zone, gli account aggiunti da AWS Control Tower diventano parte di quelli esistenti AWS Organizations e come tali entrano a far parte della fatturazione dell'organizzazione esistente.

Riepilogo delle funzionalità

L'abilitazione di AWS Control Tower su un' AWS Organizations organizzazione esistente offre diversi importanti miglioramenti all'organizzazione.

- Consente una fatturazione unificata tra i gruppi dell'organizzazione, poiché gli account aggiunti da AWS Control Tower entreranno a far parte dell'organizzazione esistente.
- Ti dà la possibilità di amministrare tutti gli account da un unico account di gestione nell'unità organizzativa.
- Semplifica il modo in cui applichi e applichi i controlli che coprono la sicurezza e la conformità per gli account esistenti e nuovi.

Important

Il lancio della landing zone di AWS Control Tower in un' AWS Organizations organizzazione esistente non consente di estendere la governance di AWS Control Tower da tale organizzazione ad altre unità organizzative o account non registrati presso AWS Control Tower.

Per avviare AWS Control Tower nella tua organizzazione esistente, segui la procedura descritta in [Guida introduttiva a AWS Control Tower](#).

Per ulteriori informazioni su come AWS Control Tower interagisce con AWS Organizations le organizzazioni esistenti, consulta [Gestisci organizzazioni e account con AWS Control Tower](#).

Lancio di AWS Control Tower in una nuova organizzazione

Se non conosci AWS Control Tower e non hai mai lavorato con AWS Organizations, il miglior punto di partenza è leggere il nostro [Configurazione](#) documento.

AWS Control Tower configura automaticamente un'organizzazione per te quando non ne hai una configurata.

AWS strategia multi-account per la tua landing zone di AWS Control Tower

I clienti di AWS Control Tower spesso richiedono indicazioni su come configurare il proprio AWS ambiente e i propri account per ottenere i migliori risultati. AWS ha creato una serie unificata di raccomandazioni, denominata strategia multi-account, per aiutarti a utilizzare al meglio le tue AWS risorse, inclusa la landing zone di AWS Control Tower.

In sostanza, AWS Control Tower funge da livello di orchestrazione che funziona con altri AWS servizi, che ti aiutano a implementare i consigli su AWS più account per AWS account e. AWS Organizations. Dopo aver configurato la landing zone, AWS Control Tower continua ad assisterti nel mantenimento delle policy aziendali e delle pratiche di sicurezza su più account e carichi di lavoro.

La maggior parte delle zone di atterraggio si sviluppa nel tempo. Con l'aumentare del numero di unità organizzative (OU) e account nella landing zone di AWS Control Tower, puoi estendere la distribuzione di AWS Control Tower in modo da organizzare i carichi di lavoro in modo efficace. Questo capitolo fornisce linee guida prescrittive su come pianificare e configurare la landing zone di AWS Control Tower, in linea con la strategia AWS multi-account, ed estenderla nel tempo.

Per una discussione generale sulle migliori pratiche per le unità organizzative, consulta [Best Practices for Organizational Units with AWS Organizations](#).

AWS strategia multi-account: linee guida sulle migliori pratiche

AWS le migliori pratiche per un ambiente ben progettato consigliano di separare le risorse e i carichi di lavoro in più account. AWS Puoi pensare AWS agli account come a contenitori di risorse isolati: offrono la categorizzazione dei carichi di lavoro, oltre a una riduzione del raggio d'azione quando le cose vanno male.

Definizione di account AWS

Un AWS account funge da contenitore di risorse e limite di isolamento delle risorse.

Note

Un AWS account non è uguale a un account utente, che viene configurato tramite Federation o AWS Identity and Access Management (IAM).

Ulteriori informazioni sugli AWS account

Un AWS account offre la possibilità di isolare le risorse e contenere le minacce alla sicurezza per i AWS carichi di lavoro. Un account fornisce anche un meccanismo per la fatturazione e la governance di un ambiente di carico di lavoro.

L' AWS account è il meccanismo di implementazione principale per fornire un contenitore di risorse per i carichi di lavoro. Se l'ambiente è ben progettato, è possibile gestire più AWS account in modo efficace e, quindi, gestire più carichi di lavoro e ambienti.

AWS Control Tower configura un ambiente ben progettato. Si basa anche sugli AWS account che aiutano a gestire le AWS Organizations modifiche all'ambiente che possono estendersi su più account.

Definizione di un ambiente ben progettato

AWS definisce un ambiente ben architettato come un ambiente che inizia con una landing zone.

AWS Control Tower offre una landing zone configurata automaticamente. Applica i controlli per garantire la conformità alle linee guida aziendali, su più account del tuo ambiente.

Definizione di landing zone

La landing zone è un ambiente cloud che offre un punto di partenza consigliato, inclusi account predefiniti, struttura degli account, layout di rete e sicurezza e così via. Da una landing zone, puoi distribuire carichi di lavoro che utilizzano le tue soluzioni e applicazioni.

Linee guida per configurare un ambiente ben progettato

I tre componenti chiave di un ambiente ben progettato, spiegati nelle seguenti sezioni, sono:

- Account multipli AWS
- Unità organizzative multiple (OU)
- Una struttura ben pianificata

Usa più account AWS

Un account non è sufficiente per configurare un ambiente ben progettato. Utilizzando più account, puoi supportare al meglio i tuoi obiettivi di sicurezza e i tuoi processi aziendali. Ecco alcuni vantaggi dell'utilizzo di un approccio multi-account:

- **Controlli di sicurezza:** le applicazioni hanno profili di sicurezza diversi, quindi richiedono politiche e meccanismi di controllo diversi. Ad esempio, è molto più semplice parlare con un revisore e indicare un unico account che ospita il carico di lavoro PCI (Payment Card Industry).
- **Isolamento:** un account è un'unità di protezione della sicurezza. I potenziali rischi e le minacce alla sicurezza possono essere contenuti all'interno di un account senza influire sugli altri. Pertanto, per esigenze di sicurezza potrebbe essere necessario isolare gli account l'uno dall'altro. Ad esempio, potresti avere team con profili di sicurezza diversi.
- **Molti team:** i team hanno responsabilità e esigenze di risorse diverse. Configurando più account, i team non possono interferire l'uno con l'altro, come potrebbero fare quando utilizzano lo stesso account.
- **Isolamento dei dati:** l'isolamento degli archivi dati in un account consente di limitare il numero di persone che hanno accesso ai dati e possono gestire l'archivio dati. Questo isolamento aiuta a prevenire l'esposizione non autorizzata di dati altamente privati. Ad esempio, l'isolamento dei dati aiuta a supportare la conformità al Regolamento generale sulla protezione dei dati (GDPR).
- **Processo aziendale:** le unità aziendali o i prodotti hanno spesso scopi e processi completamente diversi. È possibile creare account individuali per soddisfare esigenze specifiche dell'azienda.
- **Fatturazione:** un account è l'unico modo per separare gli elementi a livello di fatturazione, ad esempio le spese di trasferimento e così via. La strategia multi-account consente di creare elementi fatturabili separati tra unità aziendali, team funzionali o singoli utenti.
- **Allocazione delle AWS quote:** le quote vengono impostate per account. La separazione dei carichi di lavoro in diversi account conferisce a ciascun account (ad esempio un progetto) una quota individuale ben definita.

Utilizza più unità organizzative

AWS Control Tower e altri framework di orchestrazione degli account possono apportare modifiche che superano i confini degli account. Pertanto, le AWS migliori pratiche riguardano le modifiche tra account, che potenzialmente possono danneggiare un ambiente o comprometterne la sicurezza. In alcuni casi, le modifiche possono influire sull'ambiente generale, al di là delle politiche. Di conseguenza, ti consigliamo di configurare almeno due account obbligatori, Production e Staging.

Inoltre, AWS gli account sono spesso raggruppati in unità organizzative (OU), a fini di governance e controllo. Le unità organizzative sono progettate per gestire l'applicazione delle politiche su più account.

La nostra raccomandazione è di creare almeno un ambiente di preproduzione (o staging) distinto dall'ambiente di produzione, con controlli e politiche distinti. Gli ambienti di produzione e messa in scena possono essere creati e gestiti come unità organizzative separate e fatturati come account separati. Inoltre, potresti voler configurare un'unità organizzativa Sandbox per il test del codice.

Usa una struttura ben pianificata per le unità organizzative nella tua landing zone

AWS Control Tower configura automaticamente alcune unità organizzative. Man mano che i carichi di lavoro e i requisiti aumentano nel tempo, puoi estendere la configurazione originale della landing zone in base alle tue esigenze.

Note

I nomi forniti negli esempi seguono le convenzioni di AWS denominazione suggerite per la configurazione di un ambiente con più account. AWS Puoi rinominare le unità organizzative dopo aver configurato la landing zone, selezionando Modifica nella pagina dei dettagli dell'unità organizzativa.

Raccomandazioni

Dopo che AWS Control Tower ha configurato la prima unità organizzativa necessaria per te, l'unità organizzativa di sicurezza, ti consigliamo di creare alcune unità organizzative aggiuntive nella tua landing zone.

Ti consigliamo di consentire ad AWS Control Tower di creare almeno un'unità organizzativa aggiuntiva, chiamata Sandbox OU. Questa unità organizzativa è per i tuoi ambienti di sviluppo software. AWS Control Tower può configurare l'unità organizzativa Sandbox per te durante la creazione di landing zone, se la selezioni.

Altre due unità organizzative consigliate che puoi configurare autonomamente: l'unità organizzativa dell'infrastruttura, per contenere i servizi condivisi e gli account di rete, e un'unità organizzativa per contenere i carichi di lavoro di produzione, chiamata Workloads OU. Puoi aggiungere unità organizzative aggiuntive nella tua landing zone tramite la console AWS Control Tower nella pagina Unità organizzative.

Unità organizzative consigliate oltre a quelle configurate automaticamente

- Infrastructure OU: contiene i servizi condivisi e gli account di rete.

Note

AWS Control Tower non configura l'unità organizzativa dell'infrastruttura per te.

- Sandbox OU: un'unità organizzativa per lo sviluppo di software. Ad esempio, potrebbe avere un limite di spesa fisso o potrebbe non essere connessa alla rete di produzione.

Note

AWS Control Tower consiglia di configurare l'unità organizzativa Sandbox, ma è facoltativa. Può essere configurato automaticamente come parte della configurazione della landing zone.

- Workloads OU: contiene account che eseguono i tuoi carichi di lavoro.

Note

AWS Control Tower non configura l'unità organizzativa Workloads per te.

Per ulteriori informazioni, consulta [Come AWS Control Tower stabilisce il tuo ambiente multi-account](#).

Allinea la struttura dell'unità organizzativa con AWS strategia multi-account

AWS Control Tower supporta una gerarchia di unità organizzative annidate, il che significa che puoi creare una struttura di unità organizzative gerarchica che soddisfi i requisiti della tua organizzazione. Puoi creare un ambiente AWS Control Tower che soddisfi le linee guida sulla strategia AWS multi-account.

Per ulteriori informazioni su come AWS Control Tower funziona con strutture di unità organizzative annidate, consulta [Unità organizzative annidate in AWS Control Tower](#).

Per le unità organizzative e gli account consigliati oltre a quelli configurati di default da AWS Control Tower, consulta le [unità organizzative e gli account consigliati](#) nel AWS white paper.

Informazioni su Root

The Root non è un'unità organizzativa. È un contenitore per l'account di gestione e per tutte le unità organizzative e gli account dell'organizzazione. Concettualmente, il Root contiene tutte le unità organizzative. Non può essere eliminato. Non è possibile gestire gli account registrati a livello di root all'interno di AWS Control Tower. Gestisci invece gli account registrati all'interno delle tue unità organizzative. [Per un diagramma utile, consulta la documentazione. AWS Organizations](#)

Suggerimenti amministrativi per la configurazione delle landing zone

Ecco alcuni suggerimenti per impostare e configurare la landing zone.

- La AWS regione in cui svolgi la maggior parte del lavoro dovrebbe essere la tua regione di origine.
- Configura la tua landing zone e utilizza i tuoi account Account Factory dalla tua regione d'origine.
- Se stai investendo in diverse AWS regioni, assicurati che le tue risorse cloud si trovino nella regione in cui svolgerai la maggior parte del lavoro amministrativo del cloud e gestirai i tuoi carichi di lavoro.
- Mantenendo i carichi di lavoro e i log nella stessa AWS regione, riduci i costi associati allo spostamento e al recupero delle informazioni dei log tra le regioni.
- L'audit e gli altri bucket Amazon S3 vengono creati nella stessa AWS regione da cui si avvia AWS Control Tower. Si consiglia di non spostare questi bucket.
- Puoi creare i tuoi bucket di log nell'account Log Archive, ma non è consigliato. Assicurati di lasciare i bucket creati da AWS Control Tower.
- I log di accesso di Amazon S3 devono trovarsi nella stessa AWS regione dei bucket di origine.
- Al momento del lancio, gli endpoint AWS Security Token Service (STS) devono essere attivati nell'account di gestione, per tutte le regioni supportate da AWS Control Tower. In caso contrario, l'avvio potrebbe non riuscire a metà del processo di configurazione.
- AWS Control Tower supporta l'etichettatura solo per i controlli abilitati. Per ulteriori informazioni, consulta [API di tagging di controllo di AWS Control Tower](#).
- Consigliamo di abilitare l'autenticazione a più fattori (MFA) per ogni account gestito da AWS Control Tower.
- In alternativa, è possibile utilizzare la funzionalità AWS Root Access Management, che consente di eseguire azioni root sugli account dei membri ed elimina la necessità di abilitare l'MFA per ogni

account. Per ulteriori informazioni, vedere [Gestione centralizzata dell'accesso root per i clienti che utilizzano AWS Organizations](#).

Considerazioni sui VPC

- Il VPC creato da AWS Control Tower è limitato a quello Regioni AWS in cui è disponibile AWS Control Tower. Alcuni clienti i cui carichi di lavoro vengono eseguiti in regioni non supportate potrebbero voler disabilitare il VPC creato con il tuo account Account Factory. Potrebbero preferire creare un nuovo VPC utilizzando il portafoglio Service Catalog o creare un VPC personalizzato che funzioni solo nelle regioni richieste.
- Il VPC creato da AWS Control Tower non è lo stesso del VPC predefinito creato per tutti. Account AWS Nelle regioni in cui è supportato AWS Control Tower, AWS Control Tower elimina il VPC predefinito quando crea il VPC AWS Control Tower.
- Se elimini il tuo VPC predefinito nella tua AWS regione d'origine, è meglio eliminarlo in tutte le altre AWS regioni.

Guida alla migrazione di Landing Zone v4.0

AWS Control Tower Landing Zone 4.0 introduce un'importante revisione dell'architettura delle landing zone, offrendo un'esperienza di controllo flessibile dedicata e integrazioni di servizi completamente opzionali. I miglioramenti principali includono la possibilità di abilitare selettivamente AWS Config AWS e AWS Backup le integrazioni CloudTrail SecurityRoles, con risorse dedicate per e AWS Config CloudTrail AWS per un migliore isolamento.

La versione elimina i requisiti obbligatori della struttura organizzativa, permettendo ai clienti di definirne di propri, e introduce al contempo un nuovo supporto ConfigBaseline per i controlli investigativi senza la necessità di una soluzione completa. `AWSControlTowerBaseline` Un Config Aggregator collegato ai servizi sostituisce i metodi di aggregazione precedenti, semplificando la raccolta dei dati di conformità.

Inoltre, il campo manifest diventa opzionale e consente implementazioni minimaliste di landing zone incentrate esclusivamente sull' AWS Organizations integrazione e l'abilitazione del controllo. Queste modifiche offrono maggiori opzioni di personalizzazione pur mantenendo solide capacità di governance, consentendo ai clienti di adattare AWS Control Tower alle loro esigenze specifiche in modo più efficace.

Argomenti

- [Modifiche chiave](#)
- [Aggiornamenti di AWS Config](#)
- [Confronto delle funzionalità con e senza AWS Config integrazione](#)

Modifiche chiave

Note

- La definizione di «registrato» e «registrato» è cambiata con questa nuova versione di AWS Control Tower. Quando su di essa account/OU è abilitata una risorsa AWS Control Tower (ad esempio control o baseline), verrà considerata una risorsa gestita. La definizione non sarà più determinata dalla presenza della linea di `AWSControlTowerBaseline` base.
- Service-Linked I ruoli vengono mantenuti in tutte le versioni delle landing zone e non vengono più eliminati quando le OU diventano «non registrate»
- Service-Linked I ruoli possono essere eliminati manualmente dai clienti solo dopo la disattivazione della landing zone

Aggiornamento dalla versione 3.3 o precedente alla versione 4.0

Non disattivate le integrazioni dei servizi (AWS Config, SecurityRoles) come parte dell'aggiornamento della versione. Nelle versioni 3.3 e precedenti delle landing zone, AWS Config SecurityRoles erano sempre abilitate implicitamente. La versione 4.0 presenta queste integrazioni come opzioni configurabili per la prima volta. Dopo aver eseguito correttamente l'aggiornamento alla versione 4.0, puoi disabilitare le integrazioni dei servizi come desideri.

- Pre-requisite per Landing Zone 4.0: quando esegui l'aggiornamento alla versione 4.0 tramite API, assicurati che il ruolo del `AWSControlTowerCloudTrailRole` servizio utilizzi la nuova politica gestita `AWSControlTowerCloudTrailRolePolicy` anziché la politica in linea esistente. [Scollega la politica in linea corrente e allega la nuova politica gestita come descritto nella documentazione.](#)
- Manifesto opzionale: il campo Manifest nell'API landing zone è ora facoltativo. I clienti possono creare zone di atterraggio senza alcuna integrazione di servizi. Non vi è alcun impatto per i clienti esistenti che utilizzano già il campo manifest.

- **Struttura organizzativa opzionale:** AWS Control Tower non applica o gestisce più la creazione di unità organizzative di sicurezza in modo che i clienti possano definire e gestire la propria struttura organizzativa. Tuttavia, AWS Control Tower richiederà che tutti gli account configurati per ogni integrazione di servizi AWS si trovino nella stessa unità organizzativa principale. Non vi è alcun impatto per i clienti che hanno già configurato AWS Control Tower e dispongono dell'unità organizzativa di sicurezza. AWS Control Tower distribuisce automaticamente le risorse e i controlli necessari per gestire gli account di integrazione dei servizi nell'unità organizzativa di sicurezza. Ad esempio, quando l'integrazione con AWS Config è abilitata, la registrazione con AWS Config è abilitata in [tutti gli](#) account di integrazione dei servizi. La AWS Control Tower Baseline e la AWS Config Baseline non sono applicabili all'unità organizzativa di sicurezza e agli account di integrazione dei servizi. Per modificare le integrazioni dei servizi, aggiorna le impostazioni della landing zone.

Note

- La configurazione della struttura organizzativa per AWS Control Tower landing zone 4.0 è cambiata rispetto alle versioni precedenti. AWS Control Tower non creerà più l'unità organizzativa di sicurezza designata. L'unità organizzativa con gli account di integrazione del servizio sarà l'unità organizzativa di sicurezza designata.
- Se gli account dei membri vengono trasferiti nell'unità organizzativa in cui risiedono gli account per ogni integrazione, i controlli abilitati su quell'unità organizzativa vengono spostati indipendentemente dal fatto che la registrazione automatica sia attivata o disattivata.

Stato di base per l'unità organizzativa di sicurezza: la linea di base e la linea di base di AWS Control Tower non possono essere applicate all'unità organizzativa di sicurezza. AWS Config L'unità organizzativa di sicurezza mostra lo stato di base «Non applicabile» per queste linee di base. Questo stato è previsto. BackupBaseline Può essere applicato all'unità organizzativa di sicurezza.

AWS Control Tower gestisce gli account di integrazione dei servizi tramite la landing zone, non tramite linee di OU-level base. Se un account di integrazione del servizio mostra lo stato di base di «Non abilitato» e l'integrazione del servizio associata è disabilitata, AWS Control Tower non gestisce più quell'account.

Gli account nell'unità organizzativa di sicurezza che non sono designati come account di integrazione del servizio non ricevono risorse di base. Per gestire questi account, spostali in un'unità organizzativa gestita ed estendi la governance.

Set di autorizzazioni IAM Identity Center per gli account di integrazione dei servizi: AWS Control Tower fornisce i set di autorizzazioni IAM Identity Center per l'account di registrazione e l' SecurityRoles account. AWS Control Tower non fornisce set di autorizzazioni per l'account Config o l'account Backup. Per accedere all'account Config o Backup tramite IAM Identity Center, crea manualmente set di autorizzazioni utilizzando le risorse IAM Identity Center distribuite da AWS Control Tower.

- **Notifiche di drift:** AWS Control Tower smetterà di inviare notifiche di drift all'argomento SNS per tutti i clienti sulla landing zone 4.0 e versioni successive e inizierà invece a inviare notifiche di drift all'account EventBridge di gestione. Per ricevere queste notifiche, crea una EventBridge regola nell'account di gestione. Quindi configura una destinazione, ad esempio un argomento SNS o una funzione Lambda. Per ulteriori informazioni sulle notifiche di drift e sugli EventBridge eventi di esempio, consulta [Types of governance drift](#).
- **Integrazioni di servizi opzionali:** ora hai la possibilità di utilizzare enable/disable tutte le integrazioni di AWS Control Tower CloudTrail SecurityRoles, tra cui AWS Config AWS e AWS Backup. Queste integrazioni ora hanno anche dei enabled flag obbligatori nell'API. Le linee di base che possono essere applicate alla tua landing zone o agli account condivisi ora dipendono l'una dall'altra. Le dipendenze specifiche delle integrazioni sono:
 - **Abilitazione:**
 - `CentralSecurityRolesBaseline` → richiede di essere `CentralConfigBaseline` abilitato
 - `IdentityCenterBaseline` → richiede `CentralSecurityRolesBaseline` di essere abilitato
 - `BackupCentralVaultBaseline` → richiede `CentralSecurityRolesBaseline` di essere abilitato
 - `BackupAdminBaseline` → richiede `CentralSecurityRolesBaseline` di essere abilitato
 - `LogArchiveBaseline` → indipendente (nessuna dipendenza)
 - `CentralConfigBaseline` → indipendente (nessuna dipendenza)
 - **Disabilitazione:**

- CentralConfigBaseline può essere disabilitato solo se CentralSecurityRolesBaseline IdentityCenterBaseline, BackupAdminBaseline e le BackupCentralVaultBaseline linee di base vengono disabilitate per prime.
- CentralSecurityRolesBaseline può essere disabilitato solo se IdentityCenterBaseline BackupAdminBaseline e le BackupCentralVaultBaseline linee di base vengono disabilitate per prime.
- IdentityCenterBaseline può essere disabilitato indipendentemente.
- BackupAdminBaseline e le BackupCentralVaultBaseline linee di base possono essere disabilitate indipendentemente
- LogArchiveBaseline può essere disabilitato indipendentemente

⚠ Ambito di AWS Config abilitazione dell'integrazione dei servizi

L'abilitazione dell'integrazione del AWS Config servizio a livello di landing zone distribuisce le risorse di registrazione di Config solo agli account di integrazione del servizio. Per distribuire AWS Config risorse (Config Recorder, Delivery Channel) negli account dei membri, abilita la linea di base su ciascuna unità organizzativa AWS Config gestita singolarmente.

L'abilitazione dell'integrazione Config a livello di landing zone è un prerequisito per abilitare la linea di base Config sulle unità organizzative. L'impostazione a livello di zona di destinazione da sola non distribuisce le risorse Config agli account dei membri.

Per ulteriori informazioni, consulta [Aggiornamenti di AWS Config](#).

⚠ CentralizedLogging modifica del comportamento nella versione 4.0

Nelle versioni 3.3 e precedenti delle landing zone, la disattivazione CentralizedLogging disattivava l'Organizzazione e conservava tutte CloudTrail le risorse dispiegate. Nella versione 4.0, la disabilitazione CentralizedLogging elimina tutte le risorse associate dall'account di registrazione. Queste risorse includono le istanze Config Recorder, Delivery Channel e CloudTrail-related stack. Dopo la disabilitazione, AWS Control Tower non gestisce più l'account di registrazione.

Per ripristinare la gestione dell'account di registrazione, riattiva CentralizedLogging o sposta l'account in un'unità organizzativa gestita ed estendi la governance.

Aggiornamenti di AWS Config

- Risorse dedicate per AWS Config e AWS CloudTrail: AWS Config e AWS CloudTrail ora utilizza bucket S3 dedicati e argomenti SNS separati anziché risorse condivise. I clienti hanno una flessibilità limitata nell'utilizzare un account singolo o separato per più integrazioni.
- Durante l'aggiornamento alla versione 4.0 della landing zone di AWS Control Tower, i dati esistenti e i bucket S3 non vengono spostati. CloudTrail L'integrazione con AWS continua a utilizzare il bucket S3 esistente con prefisso `aws-controltower-logs` I nuovi dati di AWS Config dopo l'operazione di aggiornamento verranno archiviati in un nuovo bucket S3 con prefisso che AWS Control `aws-controltower-config` Tower crea nell'account designato per `CentralConfigBaseline`

Note

Abilitando CloudTrail l'integrazione con AWS sulla landing zone 4.0 per la prima volta verranno creati nuovi bucket S3 ogni volta con prefisso `aws-controltower-cloudtrail`

- Modifiche alla posizione dei dati: i clienti esistenti che effettuano l'aggiornamento da risorse precedentemente condivise a risorse dedicate avranno CloudTrail i dati AWS Config AWS in diversi bucket S3. I flussi di lavoro e gli strumenti consolidati dei clienti potrebbero richiedere aggiornamenti per accedere ai dati da nuove ubicazioni di bucket.
- AWS CloudTrail continuerà a rimanere nello stesso bucket esistente, ma AWS Config i dati si troveranno in un nuovo bucket S3 creato da AWS Control Tower.
- I clienti possono configurare la replica tra bucket se desiderano centralizzare diversi log in un unico bucket. [Per ulteriori informazioni, consulta la documentazione di S3.](#)
- Se hai account registrati con canali di distribuzione AWS Config preesistenti non creati da AWS Control Tower in regioni governate da AWS Control Tower, aggiorna il nome del bucket S3 di Delivery Channels nel nuovo bucket S3 con prefisso `aws-controltower-config-logs` nell'account di integrazione AWS Config per essere coerente con le configurazioni AWS Control Tower sulla landing zone 4.0. Maggiori dettagli sono disponibili in [Registra account esistenti AWS Config risorse](#).
- AWS Config integrazione nella versione 4.0 della landing zone: durante la migrazione alla landing zone 4.0 con AWS Config l'integrazione abilitata, i clienti vedrebbero le seguenti modifiche -
 1. L'account Audit esistente è registrato come amministratore delegato per. AWS Config

2. Service-Linked Config Aggregator viene distribuito nell'account Audit (account aggregatore AWS Config centrale per i nuovi clienti e account Audit per i clienti esistenti). Il nuovo aggregatore può aggregare i dati da qualsiasi AWS Config registratore dell'organizzazione, inclusi gli account gestiti non Control Tower.
 3. Gli aggregatori esistenti verranno eliminati: l'aggregatore di organizzazioni nell'account di gestione (`aws-controltower-ConfigAggregatorForOrganizations`) e l'aggregatore di account nell'account Audit (`aws-controltower-GuardRailsComplianceAggregator`) verranno eliminati.
 4. Poiché Configuration Aggregator è collegato al servizio, i controlli associati agli aggregatori eliminati verranno rimossi automaticamente.
 - a. [Impedisci modifiche ai tag creati da AWS Control Tower per le risorse AWS Config](#)
 - b. [Impedire l'eliminazione delle autorizzazioni di AWS Config Aggregation create da AWS Control Tower](#)
- Nuova **ConfigBaseline** linea di base: ora esiste una soluzione distinta ConfigBaseline a livello di unità organizzativa per il supporto dei controlli investigativi, senza richiedere una soluzione completa. `AWSControlTowerBaseline` Per ulteriori informazioni, consulta [l'elenco dei tipi di base a livello di unità organizzativa](#). Per i clienti esistenti che utilizzano la landing zone predefinita, tutte le integrazioni dei servizi sono ora opzionali, con l'avvertenza dei requisiti di dipendenza descritta in [Modifiche chiave](#)
 - Service-Linked Config Aggregator: sostituisce gli aggregatori di organizzazioni e account nell'account aggregatore centrale. AWS Config
 - Quando si esegue l'aggiornamento alla landing zone 4.0 con AWS Config l'integrazione abilitata, i clienti devono disporre delle autorizzazioni `organizations:ListDelegatedAdministrators`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "backup:UpdateGlobalSettings",
        "controltower:CreateLandingZone",
        "controltower:UpdateLandingZone",
        "controltower:ResetLandingZone",
        "controltower>DeleteLandingZone",
```

```

    "controltower:GetLandingZoneOperation",
    "controltower:GetLandingZone",
    "controltower:ListLandingZones",
    "controltower:ListLandingZoneOperations",
    "controltower:ListTagsForResource",
    "controltower:TagResource",
    "controltower:UntagResource",
    "servicecatalog:*",
    "organizations:*",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:EnableAWSServiceAccess",
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "sso:*",
    "sso-directory:*",
    "logs:*",
    "cloudformation:*",
    "kms:*",
    "iam:GetRole",
    "iam:CreateRole",
    "iam:GetSAMLProvider",
    "iam:CreateSAMLProvider",
    "iam:CreateServiceLinkedRole",
    "iam:ListRolePolicies",
    "iam:PutRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy"
  ],
  "Resource": "*"
}
]
}

```

Important

Dopo aver effettuato l'aggiornamento alla versione 4.0 della landing zone e aver abilitato l' AWS Config integrazione, è necessario completare il processo di abilitazione. Aggiorna o abilita ConfigBaseline su tutte le unità organizzative in cui desideri distribuire AWS

Config le risorse. Finché non completerai questo processo, l' AWS Config Aggregator non riceverà dati dai registratori. Ogni account continua a registrare e archiviare dati. Al termine dell'aggiornamentoConfigBaseline, i dati registrati vengono automaticamente reinseriti nell'aggregatore.

Ti consigliamo di registrare nuovamente le unità organizzative o di abilitarle il prima ConfigBaseline possibile dopo aver abilitato l'integrazione. AWS Config L'aggiornamento della landing zone rimuove le autorizzazioni di AWS Config consegna dalla precedente policy sui bucket S3, ma i canali di consegna vengono reindirizzati al nuovo bucket solo dopo aver completato la nuova registrazione. Fino ad allora, le istantanee di configurazione e la cronologia delle configurazioni non vengono consegnate a S3.

Se la nuova registrazione viene ritardata, alcuni di questi dati potrebbero non essere consegnati a S3 una volta completata la nuova registrazione. Puoi recuperare tutti i dati registrati entro il periodo di conservazione configurato utilizzando l'API.

`config:GetResourceConfigHistory`

Confronto delle funzionalità con e senza AWS Config integrazione

Con Landing Zone 4.0, puoi disabilitare l' AWS Config integrazione. La tabella seguente riassume le funzionalità di AWS Control Tower disponibili con e senza l' AWS Config integrazione abilitata nella landing zone.

Funzionalità	AWS Config Integrazioni abilitata	AWS Config Integrazioni disattivata
Controlli preventivi	✓	✓
Controlli proattivi	✓	✓
Il controllo Region Deny applicato alle unità organizzative	✓	✓
Region Deny control applicato alla landing zone	✓	
Controlli di rilevamento	✓	
Account Factory	✓	Vedi alternativa

Funzionalità	AWS Config Integrazioni abilitata	AWS Config Integrazioni disattivata
Account Factory per Terraform (AFT)	✓	
Personalizzazioni di Account Factory (AFC)	✓	
Integrazione di AWS Service Catalog con Account Factory	✓	
Personalizzazioni per AWS Control Tower (cFCT)	✓	
Linee di base applicate alle unità organizzative	✓	
CloudTrail Integrazione e linee di base con AWS	✓	✓
Integrazione e linee di base con AWS Backup	✓	
Integrazione e linee di base di AWS IAM Identity Center	✓	
Integrazione con AWS SNS per le notifiche di deviazione	✓	
EventBridge Integrazione Amazon per le notifiche di deriva	✓	✓
Registrati OU	✓	Vedi alternativa

Alternative

Account Factory

Se hai disabilitato l' AWS Config integrazione, puoi abilitare la [registrazione automatica](#) e utilizzarla AWS Organizations per creare e spostare account. Gli account ereditano i controlli applicati all'unità organizzativa principale.

Registra OU

Se l'AWS Config integrazione è disattivata, è possibile utilizzarla AWS Organizations per creare unità organizzative. Quindi, abilita i controlli tramite la pagina Control Catalog nella console AWS Control Tower, ripristina i controlli nella pagina Organizzazione o utilizza le API di AWS Control Tower.

Consigli per la configurazione di gruppi, ruoli e politiche

Quando configuri la tua landing zone, è consigliabile decidere in anticipo quali utenti dovranno accedere a determinati account e perché. Ad esempio, un account di sicurezza dovrebbe essere accessibile solo al team di sicurezza, l'account di gestione dovrebbe essere accessibile solo al team degli amministratori del cloud e così via.

Per ulteriori informazioni su questo argomento, vedere. [Gestione delle identità e degli accessi in AWS Control Tower](#)

Restrizioni consigliate

Puoi limitare l'ambito dell'accesso amministrativo alle tue organizzazioni impostando un ruolo o una policy IAM che consenta agli amministratori di gestire solo le azioni di AWS Control Tower. L'approccio consigliato consiste nell'utilizzare la policy `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` IAM. Con il `AWSControlTowerServiceRolePolicy` ruolo abilitato, un amministratore può gestire solo AWS Control Tower. Assicurati di includere in ogni account l'accesso appropriato AWS Organizations per la gestione dei controlli preventivi e degli SCP e l'accesso a AWS Config, per la gestione dei controlli investigativi.

Quando imposti l'account di controllo condiviso nella tua landing zone, ti consigliamo di assegnare il gruppo `AWSSecurityAuditors` a tutti i revisori di terze parti dei tuoi account. Questo gruppo dà ai suoi membri l'autorizzazione di sola lettura. Un account non deve disporre delle autorizzazioni di scrittura per l'ambiente che sta controllando perché può violare la conformità ai requisiti della "separazione dei compiti" per i revisori.

Puoi imporre condizioni nelle policy di fiducia dei ruoli, per limitare gli account e le risorse che interagiscono con determinati ruoli in AWS Control Tower. Ti consigliamo vivamente di limitare l'accesso al `AWSControlTowerAdmin` ruolo, perché consente ampie autorizzazioni di accesso. Per ulteriori informazioni, consulta [Condizioni opzionali per le relazioni di fiducia tra i ruoli](#).

Linee guida per la creazione e la modifica delle risorse AWS Control Tower

Consigliamo le seguenti best practice per creare e modificare risorse in AWS Control Tower. Queste linee guida potrebbero cambiare quando il servizio viene aggiornato. Ricorda che il [modello di responsabilità condivisa](#) si applica al tuo ambiente AWS Control Tower.

Informazioni generali

- Non modificare o eliminare alcuna risorsa creata da AWS Control Tower, incluse le risorse nell'account di gestione, negli account condivisi e negli account dei membri. Se modifichi queste risorse, ti potrebbe essere richiesto di aggiornare la landing zone o registrare nuovamente un'unità organizzativa e la modifica può comportare rapporti di conformità imprecisi.

In particolare:

- Mantieni un AWS Config registratore attivo. Se elimini il tuo registratore Config, i controlli investigativi non possono rilevare e segnalare la deriva. Non-compliant le risorse potrebbero essere segnalate come conformi a causa di informazioni insufficienti.
- Non modificare o eliminare i ruoli AWS Identity and Access Management (IAM) creati all'interno degli account condivisi nell'unità organizzativa (OU) di sicurezza. La modifica di questi ruoli può richiedere l'aggiornamento della landing zone.
- Non eliminare il `AWSControlTowerExecution` ruolo dai tuoi account membro, nemmeno negli account non registrati. In caso affermativo, non sarà possibile registrare questi account con AWS Control Tower o registrare le relative unità organizzative principali.
- Non impedirne l'utilizzo Regioni AWS tramite SCP o Servizio di token di sicurezza AWS ().AWS STS In questo modo, AWS Control Tower entrerà in uno stato non definito. Se non autorizzi le Regioni con AWS STS, la funzionalità fallirà in quelle regioni, poiché l'autenticazione non sarebbe disponibile in quelle regioni. Affidati invece alla funzionalità di negazione della regione AWS Control Tower, come illustrato nel controllo, [Deny access to in AWS base alla richiesta Regione AWS](#), che funziona a livello di landing zone, o alla [regione di controllo Deny control applicata all'unità organizzativa, che funziona a](#) livello di unità organizzativa per limitare l'accesso alle regioni.
- L' `AWS Organizations FullAWSAccessSCP` deve essere applicato e non deve essere unito ad altri SCP. Le modifiche a questo SCP non vengono segnalate come deviazioni; tuttavia, alcune modifiche possono influire sulla funzionalità di AWS Control Tower in modi imprevedibili, se l'accesso a determinate risorse viene negato. Ad esempio, se l'SCP viene scollegato o modificato,

un account potrebbe perdere l'accesso a un AWS Config registratore o creare una lacuna nella registrazione. CloudTrail

- Non utilizzare l' `AWS Organizations DisableAWSServiceAccessAPI` per disattivare l'accesso del servizio AWS Control Tower all'organizzazione in cui hai configurato la landing zone. In tal caso, alcune funzionalità di rilevamento della deriva di AWS Control Tower potrebbero non funzionare correttamente senza il supporto di messaggistica di AWS Organizations. Queste funzionalità di rilevamento delle deviazioni aiutano a garantire che AWS Control Tower sia in grado di riportare in modo accurato lo stato di conformità delle unità organizzative, degli account e dei controlli dell'organizzazione. Per ulteriori informazioni, consulta [API_DisableAWSServiceAccess' AWS Organizations API Reference](#).
- In generale, AWS Control Tower esegue una singola azione alla volta, che deve essere completata prima che possa iniziare un'altra azione. Ad esempio, se si tenta di effettuare il provisioning di un account mentre il processo di attivazione di un controllo è già in corso, il provisioning dell'account avrà esito negativo.

Eccezione:

- AWS Control Tower consente azioni simultanee per distribuire controlli opzionali. Per ulteriori informazioni, consulta [Distribuzione simultanea per](#) i controlli opzionali.
- AWS Control Tower consente fino a dieci azioni simultanee di creazione, aggiornamento o registrazione sugli account, con Account Factory.

Note

Per ulteriori informazioni sulle risorse create da AWS Control Tower, consulta [Cosa sono gli account condivisi?](#).

Suggerimenti su account e unità organizzative

- Si consiglia di mantenere ogni unità organizzativa registrata fino a un massimo di 1000 account, in modo da poter aggiornare tali account con la funzionalità Re-register OU ogni volta che sono necessari aggiornamenti degli account, ad esempio quando si configurano nuove regioni per la governance.
- Per ridurre il tempo necessario per la registrazione di un'unità organizzativa, si consiglia di mantenere il numero di account per unità organizzativa a circa 680, anche se il limite è di 1000 account per unità organizzativa. Come regola generale, il tempo necessario per registrare un'unità

organizzativa aumenta in base al numero di regioni in cui opera l'unità organizzativa, moltiplicato per il numero di account nell'unità organizzativa.

- Secondo le stime, un'unità organizzativa con 680 account può richiedere fino a 2 ore per la registrazione e l'attivazione dei controlli e fino a 1 ora per la nuova registrazione. Inoltre, un'unità organizzativa con molti controlli richiede più tempo per la registrazione rispetto a un'unità organizzativa con pochi controlli.
- Una delle preoccupazioni legate alla concessione di un periodo di tempo più lungo per la registrazione di un'unità organizzativa è che questo processo blocca altre azioni. Alcuni clienti sono disposti a concedere tempi più lunghi per registrare o registrare nuovamente un'unità organizzativa, perché preferiscono consentire più account in ciascuna unità organizzativa.

Quando accedere come utente root

Alcune attività amministrative richiedono l'accesso come utente root. Puoi accedere come utente root a un Account AWS creato da account factory in AWS Control Tower.

È necessario accedere come utente root per eseguire le seguenti operazioni:

- Modificare alcune impostazioni dell'account, tra cui il nome dell'account, la password dell'utente root o l'indirizzo e-mail. Per ulteriori informazioni, consulta [Aggiorna e sposta gli account con AWS Control Tower](#).
- Per [chiudere un Account AWS](#).
- Per ulteriori informazioni sulle azioni che richiedono le credenziali di accesso dell'utente root, vedere [Attività che richiedono le credenziali dell'utente root](#) nella Guida Gestione dell'account AWS di riferimento.

Note

Per modificare o abilitare il tuo [piano AWS Support, devi accedere come utente root o essere un utente con le autorizzazioni IAM appropriate](#).

Per accedere come utente root

1. Apri la pagina di AWS accesso.

Se non disponi dell'indirizzo e-mail Account AWS a cui desideri accedere, puoi ottenerlo da AWS Control Tower. Apri la console per l'account di gestione, scegli Account e cerca l'indirizzo e-mail.

2. Inserisci l'indirizzo e-mail Account AWS a cui desideri accedere, quindi scegli Avanti.
3. Scegliere Forgot password? (Password dimenticata?) per ricevere le istruzioni di reimpostazione della password all'indirizzo e-mail dell'utente root.
4. Aprire il messaggio e-mail di reimpostazione della password dalla casella di posta dell'utente root, quindi seguire le istruzioni per reimpostare la password.
5. Apri la pagina di AWS accesso, quindi accedi con la password di reimpostazione.

In alternativa, puoi utilizzare la funzionalità AWS Root Access Management, che consente di eseguire azioni root sugli account dei membri, senza dover accedere come root. Per ulteriori informazioni, consulta [Gestione centralizzata dell'accesso root per i clienti che utilizzano AWS Organizations](#).

AWS Organizations linee guida

AWS Control Tower è strettamente associata a AWS Organizations. Ecco alcune linee guida specifiche su come collaborano al meglio per proteggere il tuo AWS ambiente.

- Puoi trovare indicazioni sulle migliori pratiche per proteggere la sicurezza del tuo account di gestione AWS Control Tower e degli account dei membri nella AWS Organizations documentazione.
 - [Le migliori pratiche per l'account di gestione](#)
 - [Le migliori pratiche per gli account dei membri](#)
- Non modificare o scollegare le policy di controllo dei servizi (SCP) che AWS Control Tower crea per un'unità organizzativa registrata. La modifica o lo scollegamento di questi SCP può far sì che i controlli entrino in uno stato sconosciuto. In tal caso, devi reimpostare la landing zone o registrare nuovamente l'unità organizzativa in AWS Control Tower. Utilizzali invece AWS Organizations per creare nuovi SCP e collegarli all'unità organizzativa.
- Lo spostamento di singoli account già registrati in AWS Control Tower, dall'esterno di un'unità organizzativa registrata, causa deviazioni che devono essere risolte. Consulta [Tipi di deriva della governance](#).
- Se lo utilizzi AWS Organizations per creare, invitare o spostare account all'interno di un'organizzazione registrata con AWS Control Tower, tali account non vengono registrati da AWS

Control Tower e le modifiche non vengono registrate. Se devi accedere a questi account tramite SSO, consulta [Accesso account membro](#).

- Se si utilizza AWS Organizations per spostare un'unità organizzativa in un'organizzazione creata da AWS Control Tower, l'unità organizzativa esterna non viene registrata da AWS Control Tower.
- AWS Control Tower gestisce il filtraggio delle autorizzazioni in modo diverso da come AWS Organizations lo fa. Se i tuoi account sono forniti con AWS Control Tower account factory, gli utenti finali possono vedere i nomi e i genitori di tutte le unità organizzative nella console AWS Control Tower, anche se non sono autorizzati a recuperare direttamente tali nomi e genitori. AWS Organizations
- AWS Control Tower non supporta autorizzazioni miste sulle organizzazioni, ad esempio l'autorizzazione a visualizzare l'unità principale di un'unità organizzativa ma non a visualizzare i nomi delle unità organizzative. Per questo motivo, gli amministratori di AWS Control Tower devono disporre delle autorizzazioni complete.
- L' AWS Organizations FullAWSAccessSCP deve essere applicato e non deve essere unito ad altri SCP. Le modifiche a questo SCP non vengono segnalate come deviazioni; tuttavia, alcune modifiche possono influire sulla funzionalità di AWS Control Tower in modi imprevedibili, se l'accesso a determinate risorse viene negato. Ad esempio, se l'SCP viene scollegato o modificato, un account potrebbe perdere l'accesso a un AWS Config registratore o creare una lacuna nella registrazione. CloudTrail
- Non utilizzare l' AWS Organizations DisableAWSServiceAccessAPI per disattivare l'accesso del servizio AWS Control Tower all'organizzazione in cui hai configurato la landing zone. In tal caso, alcune funzionalità di rilevamento della deriva di AWS Control Tower potrebbero non funzionare correttamente senza il supporto di messaggistica di. AWS Organizations Queste funzionalità di rilevamento delle deviazioni aiutano a garantire che AWS Control Tower sia in grado di riportare in modo accurato lo stato di conformità delle unità organizzative, degli account e dei controlli dell'organizzazione. Per ulteriori informazioni, consulta [API_DisableAWSServiceAccess' AWS Organizations API Reference](#).

Linee guida per IAM Identity Center

AWS Control Tower consiglia di utilizzare AWS Identity and Access Management (IAM) per regolare l'accesso al tuo Account AWS. Tuttavia, hai la possibilità di scegliere se AWS Control Tower configuri IAM Identity Center per te, se configurare IAM Identity Center per te stesso, in un modo che soddisfi i tuoi requisiti aziendali nel modo più efficace, o se selezionare un altro metodo per l'accesso all'account.

 Note

SSO è un'abbreviazione utilizzata nel settore tecnologico per indicare il single sign-on. In termini generali, SSO è un servizio di autenticazione di sessione e utente. Consente a qualcuno di utilizzare un set di credenziali di accesso per accedere a molte applicazioni. Quando ci riferiamo alla funzionalità Single Sign-On in AWS, ci riferiamo al AWS servizio chiamato AWS Identity and Access Management abbreviato in IAM o IAM Identity Center.

Per impostazione predefinita, AWS Control Tower configura AWS IAM Identity Center per la tua landing zone, in linea con le linee guida sulle best practice definite in [Organizzazione AWS dell'ambiente utilizzando più account](#). La maggior parte dei clienti sceglie l'impostazione predefinita. Talvolta sono necessari metodi di accesso alternativi, per la conformità normativa in settori o paesi specifici o Regioni AWS laddove AWS IAM Identity Center non è disponibile.

Scelta di un'opzione

Dalla console, puoi scegliere di gestire autonomamente IAM Identity Center durante il processo di configurazione della landing zone, anziché consentire ad AWS Control Tower di configurarlo per te. In qualsiasi momento successivo, puoi scegliere di modificare questa selezione, modificando le impostazioni della landing zone e aggiornando la tua landing zone nella pagina Impostazioni della landing zone.

Interrompere AWS IAM Identity Center in AWS Control Tower o per iniziare a usarlo AWS Centro identità IAM

1. Vai alla pagina delle impostazioni della landing zone
2. Seleziona la scheda Configurazioni
3. Quindi scegli il pulsante di opzione appropriato per modificare la selezione per AWS IAM Identity Center.

Dopo aver scelto di gestire autonomamente AWS IAM Identity Center come IdP, AWS Control Tower crea solo i ruoli e le policy necessari per gestire AWS Control Tower, come `AWSControlTowerAdmin` e `AWSControlTowerAdminPolicy`. Per le landing zone autogestite, AWS Control Tower non crea più ruoli e raggruppamenti IAM per uso specifico del cliente, né durante il processo di configurazione della landing zone né durante il provisioning dell'account con Account Factory.

 Note

Se rimuovi AWS IAM Identity Center dalla landing zone di AWS Control Tower, gli utenti, i gruppi e i set di autorizzazioni creati da AWS Control Tower non vengono rimossi. Ti consigliamo di rimuovere queste risorse.

I clienti Account Factory con provider di identità alternativi (IdPs) come Azure AD, Ping o Okta, possono seguire la [procedura](#) di AWS IAM Identity Center per connettersi a un provider di identità esterno e inserire il proprio IdP. Puoi tornare a far sì che AWS Control Tower generi i tuoi raggruppamenti e ruoli in qualsiasi momento, modificando le impostazioni della landing zone.

- Per informazioni specifiche su come AWS Control Tower funziona con IAM Identity Center in base alla tua origine di identità, consulta Considerazioni per Centro identità AWS IAM i clienti nella sezione [Pre-launch controlli](#) della pagina Getting Started di questa Guida per l'utente.
- Per ulteriori informazioni su come il comportamento di AWS Control Tower interagisce con IAM Identity Center e diverse fonti di identità, consulta [Considerations for Changing Your Identity Source nella IAM Identity Center User Guide](#).
- [Lavorare con AWS IAM Identity Center e AWS Control Tower](#) Per ulteriori informazioni sull'utilizzo di AWS Control Tower e IAM Identity Center, consulta la pagina.

Guida Account Factory

 Note

La fornitura, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) abilitata. AWSControlTowerBaseline Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare le ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su quell'unità organizzativa per registrare gli account. Per i dettagli di, vedere:.. AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

È possibile riscontrare problemi quando si utilizza Account Factory per effettuare il provisioning di un nuovo account in AWS Control Tower. Per informazioni su come risolvere questi problemi, consulta

la sezione [Provisioning del nuovo account non riuscito](#) in [Troubleshooting](#) of the AWS Control Tower User Guide.

Ti consigliamo di creare utenti federati o ruoli IAM anziché utenti IAM. Gli utenti federati e i ruoli IAM forniscono credenziali temporanee. Gli utenti IAM dispongono di credenziali a lungo termine che possono essere difficili da gestire. Per ulteriori informazioni, consulta [le identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nella Guida per l'utente IAM.

Se ti sei autenticato come utente IAM o utente IAM Identity Center durante il provisioning di un nuovo account in Account Factory o quando utilizzi la funzionalità dell'account Enroll AWS Control Tower, verifica che il tuo utente abbia accesso al tuo portafoglio. AWS Service Catalog In caso contrario, è possibile che venga visualizzato un messaggio di errore da Service Catalog. Per ulteriori informazioni, consulta [Errore nel portafoglio AWS Control Tower Account Factory](#) la [sezione Risoluzione dei problemi](#) della AWS Control Tower User Guide.

Note

Con la registrazione automatica disattivata: è possibile fornire fino a cinque account contemporaneamente.

Con la registrazione automatica abilitata: è possibile fornire fino a 5 account contemporaneamente, ma qualsiasi operazione di spostamento dell'account attiva per l'unità organizzativa di destinazione blocca tutte le operazioni di provisioning sulla stessa unità organizzativa fino al completamento.

Linee guida sulla sottoscrizione a SNS Topics

Iscriviti agli argomenti SNS per ottenere informazioni sul tuo ambiente AWS Control Tower.

Note

AWS Control Tower interromperà l'invio di notifiche di deviazione all'argomento SNS per tutti i clienti su LZ4.0 +.

- L'argomento `aws-controltower-AllConfigNotifications` SNS riceve tutti gli eventi pubblicati da AWS Config, incluse le notifiche di conformità e le notifiche CloudWatch degli eventi di Amazon. Ad esempio, questo argomento ti informa se si è verificata una violazione del controllo.

Fornisce inoltre informazioni su altri tipi di eventi. (Scopri di più [AWS Config](#) su ciò che pubblicano quando questo argomento è configurato.)

- [I dati degli eventi](#) del `aws-controltower-BaselineCloudTrail` percorso sono impostati per essere pubblicati anche sull'argomento `aws-controltower-AllConfigNotifications` SNS.
- Per ricevere notifiche dettagliate sulla conformità, ti consigliamo di iscriverti all'argomento `aws-controltower-AllConfigNotifications` SNS. Questo argomento aggrega le notifiche di conformità provenienti da tutti gli account per bambini.
- Per ricevere notifiche di deviazione e altre notifiche oltre alle notifiche di conformità, ma in generale un numero inferiore di notifiche, ti consigliamo di iscriverti all'argomento `aws-controltower-AggregateSecurityNotifications` SNS.
- Per ricevere notifiche sugli errori di AWS Control Tower Account Factory for Terraform (AFT), puoi iscriverti a un argomento SNS chiamato [aft_failure_notifications](#), mostrato nel repository AFT. Ad esempio:

```
resource "aws_sns_topic" "aft_failure_notifications" {  
    name = "aft-failure-notifications"  
    kms_master_key_id = "alias/aws/sns"  
}
```

- [Tutti gli argomenti SNS sono crittografati quando sono inattivi con la crittografia del disco. Per ulteriori informazioni, consulta Crittografia dei dati.](#)

[Per ulteriori informazioni sugli argomenti SNS e sulla conformità, consulta Prevenzione e notifica.](#)

Linee guida per le chiavi KMS

AWS Control Tower funziona con AWS Key Management Service (AWS KMS). Facoltativamente, se desideri crittografare e decrittografare le risorse AWS Control Tower con una chiave di crittografia gestita da te, puoi generare e configurare. AWS KMS keys Puoi aggiungere o modificare una chiave KMS ogni volta che aggiorni la tua landing zone. Come best practice, ti consigliamo di utilizzare le tue chiavi KMS e di cambiarle di tanto in tanto.

AWS KMS consente di creare chiavi KMS multiregionali e chiavi asimmetriche. Tuttavia, AWS Control Tower non supporta chiavi multiregionali o chiavi asimmetriche. AWS Control Tower esegue un controllo preliminare delle chiavi esistenti. Potresti visualizzare un messaggio di errore se selezioni una chiave multiregionale o una chiave asimmetrica. In tal caso, genera un'altra chiave da utilizzare con le risorse AWS Control Tower.

Per i clienti che gestiscono un cluster AWS CloudHSM: crea un archivio di chiavi personalizzato associato al tuo cluster CloudHSM. Quindi puoi creare una chiave KMS, che risiede nell'archivio di chiavi personalizzato di CloudHSM che hai creato. Puoi aggiungere questa chiave KMS a AWS Control Tower.

È necessario effettuare un aggiornamento specifico alla policy di autorizzazione di una chiave KMS per farla funzionare con AWS Control Tower. Per i dettagli, consulta la sezione chiamata. [Aggiorna la politica chiave del KMS](#)

Procedure consigliate per gli aggiornamenti delle landing zone

Questa sezione fornisce alcune considerazioni e best practice da tenere a mente quando prendi in considerazione l'aggiornamento della versione della tua landing zone in AWS Control Tower. Il passaggio dalla serie di versioni 2.0 landing zone alla serie di versioni 3.0 landing zone è particolarmente importante. Quando aggiorni la tua landing zone, AWS Control Tower ti sposta automaticamente all'ultima versione disponibile.

Note

È consigliabile eseguire l'aggiornamento alla versione più recente della landing zone.

Riepilogo delle migliori pratiche illustrate in questa sezione

- Procedura consigliata: per motivi di sicurezza e controllo, consigliamo vivamente di abilitare la registrazione su tutti gli account e di inviare le informazioni di registrazione a una posizione centralizzata. In AWS Control Tower, questa posizione centralizzata è l'account di archiviazione dei log, che fornisce un bucket di registrazione Amazon S3.
- Best practice: se disattivi il CloudTrail percorso a livello di organizzazione in AWS Control Tower, configura e gestisci i tuoi percorsi.
- Best practice: quando utilizzi il tuo ambiente AWS Control Tower, configura un ambiente di test.

Vantaggi del passaggio dalla versione 2.x landing zone alla versione 3.x landing zone

- Registra AWS Config le risorse solo nella regione d'origine, il che consente di risparmiare sui costi quando gestisci le risorse globali
- Crittografa il tuo AWS CloudTrail percorso con la tua chiave KMS

- Personalizza il periodo di conservazione dei log
- Controlli obbligatori migliorati
- Maggiore numero di controlli disponibili
- Integrato con AWS Security Hub CSPM
- Aggiornamenti del runtime di Python

Avvertenze per il passaggio dalla versione 2.x landing zone alla versione 3.x landing zone

- Con la landing zone 3.0 e versioni successive, AWS Control Tower non supporta più AWS CloudTrail percorsi a livello di account che AWS gestiscono.
- Hai la possibilità di scegliere un percorso a livello di organizzazione gestito da AWS Control Tower o di disattivarlo e gestire i tuoi percorsi. CloudTrail
- Esiste la possibilità di raddoppiare i costi, soprattutto se alcuni account all'interno di un'unità organizzativa non sono registrati in AWS Control Tower e dispongono di percorsi a livello di account propri che si desidera conservare.

Considerazioni sulla scelta dei percorsi a livello di organizzazione CloudTrail

- Quando esegui l'aggiornamento alla versione 3.0 o successiva, AWS Control Tower elimina i percorsi a livello di account originariamente creati dopo 24 ore. [\[Eccezione\]](#)
- Nessun dato proveniente da questi percorsi viene perso. I registri esistenti vengono conservati anche quando i sentieri vengono rimossi.
- AWS Control Tower crea un nuovo percorso nello stesso bucket Amazon S3 per i trail, per differenziare i percorsi a livello di account da quelli a livello di organizzazione.
 - Il percorso del log di trail dell'account ha la seguente forma: `/orgId/AWSLogs/...`
 - Un percorso di log del trail organizzativo ha la seguente forma: `/orgId/AWSLogs/orgId/...`
- CloudTrail I percorsi aggiuntivi che hai distribuito, percorsi non distribuiti da AWS Control Tower, non vengono toccati.
- Tutti gli account sono inclusi nel percorso a livello di organizzazione, inclusi gli account non registrati in AWS Control Tower, se gli account non registrati fanno parte di un'unità organizzativa registrata.
- Gli CloudWatch allarmi Amazon negli account collegati non vengono attivati.
- Se disattivi un percorso a livello di organizzazione, AWS Control Tower continua a creare il percorso, ma ne imposta lo stato su Disattivato.

- Come best practice, se disattivi il percorso a livello di organizzazione in AWS Control Tower, dovresti configurare e gestire i tuoi percorsi, CloudTrail

Vantaggi dei percorsi a livello di organizzazione

- Il percorso organizzativo funziona su tutti gli account dell'unità organizzativa.
- Gli elementi registrati sono standardizzati e non possono essere modificati dagli utenti dell'account.

Prendi in considerazione un ambiente di test

Quando aggiorni la tua landing zone, AWS Control Tower apporta modifiche solo agli account condivisi e all'unità organizzativa Foundational. Non apporta modifiche agli account dei carichi di lavoro o alle unità organizzative. Tuttavia, come best practice, quando gestisci il tuo ambiente AWS Control Tower, ti consigliamo di configurare un ambiente di test. All'interno dell'ambiente di test isolato, puoi testare gli upgrade delle landing zone di AWS Control Tower, nonché eventuali modifiche apportate alle policy di controllo dei servizi (SCP) e puoi testare i controlli che desideri applicare all'ambiente. Questa raccomandazione è particolarmente utile se operi in un settore regolamentato.

Elenco di controllo per gli errori più comuni durante l'aggiornamento

Ecco un breve elenco di attività che puoi eseguire per evitare errori comuni durante l'aggiornamento della landing zone di AWS Control Tower dalla versione 2.x alla versione 3.x.

Lista di controllo di base per l'aggiornamento

- Controlla la tua landing zone:
 - Accedi al servizio AWS Control Tower, consulta le pagine Unità organizzative e Account, quindi conferma che lo stato dell'account sia impostato su Registrato e registrato.
 - Se applicabile, verifica e conferma che l'ultima esecuzione della pipeline di personalizzazioni sia avvenuta correttamente.
 - Controlla il bucket di registrazione centralizzato di Amazon S3 nell'account Audit, poiché eventuali modifiche precedentemente apportate alla policy del bucket verranno sovrascritte.
- Verifica che eventuali SCP non di proprietà di AWS Control Tower non impediscano al `AWSControlTowerExecution` ruolo di eseguire azioni negli account dei membri o azioni nell'account di gestione per il ruolo amministrativo che esegue l'aggiornamento.

AI-based servizi e AWS Control Tower

È possibile creare policy di controllo dei servizi (SCP) che consentono di disattivare l'archiviazione dei dati da parte dei AI-based servizi. AWS Queste politiche SCP specificano che AI-based i servizi, come Amazon Rekognition o CodeWhisperer Amazon, non possono archiviare e utilizzare i tuoi dati per migliorare altri servizi. AI-based AWS

Queste politiche SCP di opt-out basate sull'IA possono essere applicate all'intera organizzazione, a un'unità organizzativa o a un account specifico. Le politiche sono in vigore a livello globale. Puoi trovare ulteriori informazioni su queste politiche nelle politiche di [opt-out dei servizi AI](#), nella AWS Organizations documentazione.

Per un elenco dei AWS servizi che utilizzano l'intelligenza artificiale, insieme a esempi di politiche, consulta la [sintassi e gli esempi delle politiche di disattivazione dei servizi di intelligenza artificiale nella Guida](#) per l'AWS Organizations utente.

Gestione degli aggiornamenti di configurazione in AWS Control Tower

È responsabilità dei membri del team centrale degli amministratori cloud mantenere aggiornata la landing zone. L'aggiornamento della landing zone garantisce che AWS Control Tower sia patchato e aggiornato. Inoltre, per proteggere la landing zone da potenziali problemi di conformità, i membri del team di amministrazione centrale del cloud dovrebbero risolvere i problemi di deriva non appena vengono rilevati e segnalati.

Note

La console AWS Control Tower indica quando è necessario aggiornare la landing zone. Se non vedi l'opzione di aggiornamento, significa che la tua landing zone è già aggiornata.

La tabella seguente contiene un elenco delle versioni di aggiornamento delle landing zone di AWS Control Tower, con collegamenti alle descrizioni di ciascuna versione.

Versione	Data di rilascio	Description
4.0	17-11-2025	Zona di atterraggio versione 4.0
3.3	12-12-2023	Zona di atterraggio versione 3.3
3.2	6-09-2023	Zona di atterraggio versione 3.2
3.1	2-09-2023	Zona di atterraggio versione 3.1
3.0	26-7-2022	Zona di atterraggio versione 3.0
2.9	22-4-2022	Zona di atterraggio versione 2.9

Versione	Data di rilascio	Description
2.8	2-10-2022	Zona di atterraggio versione 2.8
2.7	4-8-2021	Zona di atterraggio versione 2.7
2.6	29/12/2020	Zona di atterraggio versione 2.6
2.5	18-11-2020	Zona di atterraggio versione 2.5
2.4	Nessuno	Nessuno
2.3	3-5-2020	Zona di atterraggio versione 2.3
2.2	11-13-19	Zona di atterraggio versione 2.2
2.1	6-24-19	Zona di atterraggio versione 2.1

Ogni volta che aggiorni la tua landing zone, hai la possibilità di modificare le impostazioni della landing zone.

Vantaggi dell'aggiornamento

- Puoi modificare le regioni governate
- Puoi modificare la tua politica di conservazione dei log
- Puoi aggiungere o rimuovere il Region Deny Control
- È possibile applicare le chiavi di AWS crittografia KMS
- Puoi attivare o disattivare il percorso a livello di organizzazione CloudTrail .
- Puoi risolvere il [drift delle landing zone](#)

Quando aggiorni la tua landing zone, ricevi automaticamente le funzionalità più recenti per AWS Control Tower. Visualizza la versione attuale della landing zone nella pagina delle impostazioni della zona di atterraggio.

Se un aggiornamento fallisce, AWS Control Tower non torna a una versione precedente di landing zone. Potresti trovare la tua landing zone in uno stato indeterminato. In tal caso, contatta l'AWS assistenza. Per ulteriori informazioni sulla risoluzione di un errore di aggiornamento, consulta [Impossibile aggiornare la zona di atterraggio](#).

Hai la possibilità di cancellare le mappature AWS dell'Identity Center (precedentemente chiamate AWS SSO) non utilizzate quando aggiorni la landing zone. Per ulteriori informazioni, consulta [Field Notes: Cancella automaticamente le mappature di IAM Identity Center non utilizzate durante gli upgrade di AWS Control Tower](#).

 Prerequisito per l'aggiornamento e il ripristino: disattiva Requester Pays

Prima di aggiornare o reimpostare la landing zone, assicurati che nel bucket di registrazione Amazon S3 per l'account Log Archive non sia abilitata la funzione Requester Pays. È necessario disattivare tale funzionalità prima di iniziare il processo di aggiornamento o ripristino. Quando AWS Control Tower configura il tuo bucket di registrazione, questa funzionalità non è abilitata. Pertanto, solo i clienti che hanno successivamente attivato la funzionalità Requester Pays devono disattivarla. Per ulteriori informazioni, consulta la [policy sui bucket di Amazon S3 CloudTrail](#) e [Using Requester Pays](#).

Informazioni sugli aggiornamenti delle landing zone

Gli aggiornamenti sono necessari per correggere la deriva della governance o per passare a una nuova versione di AWS Control Tower. Per eseguire un aggiornamento completo di AWS Control Tower, devi prima aggiornare la landing zone e poi aggiornare gli account registrati singolarmente. Potrebbe essere necessario eseguire tre tipi di aggiornamenti in momenti diversi.

- Un aggiornamento della landing zone: molto spesso questo tipo di aggiornamento viene eseguito selezionando **Aggiorna** nella pagina delle impostazioni della zona di atterraggio. Potrebbe essere necessario eseguire un aggiornamento della landing zone per risolvere determinati tipi di deriva e, se necessario, puoi scegliere **Reset**.

- **Aggiornamento di uno o più account:** è necessario aggiornare gli account se le informazioni associate cambiano o se si sono verificati determinati tipi di difformità. Se un account richiede un aggiornamento, lo stato dell'account mostrerà **Aggiornamento disponibile** nella pagina **Account**.

Per aggiornare un singolo account, vai alla pagina dei dettagli dell'account e seleziona **Aggiorna account**. Gli account possono anche essere aggiornati mediante un processo manuale, scegliendo **Re-register OU**, o con un approccio di scripting automatico, descritto in una sezione successiva di questa pagina.

- **Un aggiornamento completo:** un aggiornamento completo include un aggiornamento della landing zone, seguito da un aggiornamento di tutti gli account registrati nelle unità organizzative registrate. Sono necessari aggiornamenti completi con una nuova versione di AWS Control Tower come 3.0, 3.2 e così via. Per semplificare l'intero processo di aggiornamento, per le unità organizzative con 1000 o meno account, è possibile scegliere **Re-register unità organizzativa** per aggiornare tutti gli account all'interno di tale unità organizzativa e ripetere il comando **Re-registerOU** per ciascuna unità organizzativa.

Per ulteriori informazioni sugli aggiornamenti delle landing zone, consulta [Best practice for landing zone updates](#).

Note

Dopo aver completato un aggiornamento della landing zone, non puoi annullare l'aggiornamento o effettuare il downgrade a una versione precedente.

Aggiorna la tua landing zone

Il modo più semplice per aggiornare la landing zone di AWS Control Tower è tramite la pagina delle impostazioni della zona di atterraggio, raggiungibile selezionando le impostazioni della zona di atterraggio nella barra di navigazione a sinistra della dashboard di AWS Control Tower.

La pagina delle impostazioni della landing zone mostra la versione corrente della tua landing zone ed elenca tutte le versioni aggiornate che potrebbero essere disponibili. È possibile scegliere il pulsante **Update (Aggiorna)** se è necessario aggiornare la versione.

Note

In alternativa, è possibile aggiornare manualmente la zona di destinazione. L'aggiornamento richiede circa lo stesso tempo, sia che si utilizzi il pulsante Update (Aggiorna) sia il processo manuale. Per eseguire un aggiornamento manuale della sola landing zone, vedere le fasi 1 e 2 riportate di seguito.

Procedura di aggiornamento standard

La procedura seguente illustra i passaggi di un aggiornamento completo per AWS Control Tower dalla console. Per aggiornare un singolo account, consulta [Aggiorna l'account nella console](#).

Per aggiornare la landing zone, con un numero qualsiasi di account per unità organizzativa

1. Apri un browser Web e accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower/home/update>.
2. Esaminare le informazioni nella procedura guidata e scegliere Update (Aggiorna). Questo aggiorna il backend della landing zone e i tuoi account condivisi. Questo processo può richiedere poco più di mezz'ora.
3. Aggiorna gli account dei membri (questa procedura deve essere seguita per un'unità organizzativa che contiene più di 1000 account).
4. Dal riquadro di navigazione a sinistra, scegli Organizzazione.
5. Per aggiornare ogni account, segui i passaggi indicati in [Aggiorna l'account nella console](#).

Facoltativamente, Re-register OU per aggiornare gli account

Per le unità organizzative AWS Control Tower registrate con meno di 1000 account, puoi andare alla pagina OU nella dashboard e selezionare Re-register OU per aggiornare gli account in quell'unità organizzativa.

Seleziona una versione di landing zone

Se utilizzi AWS Control Tower landing zone versione 3.1 e successive, puoi scegliere di mantenere la versione corrente oppure effettuare l'aggiornamento a una versione più recente quando esegui

un'operazione di aggiornamento o ripristino delle configurazioni della tua landing zone. L'operazione Reset è il modo migliore per riparare la deriva, nella maggior parte delle situazioni.

Puoi scegliere una versione di landing zone nella console AWS Control Tower o tramite le API AWS Control Tower.

Note

Se scegli di implementare una versione di landing zone che salta una versione intermedia, ad esempio se passi dalla 3.1 alla 3.3, AWS Control Tower distribuisce automaticamente la versione intermedia come parte dell'operazione di aggiornamento.

Nella conversazione, il passaggio a una versione più recente viene spesso definito un aggiornamento, non solo un aggiornamento. Questi due concetti sono distinti, perché puoi aggiornare le impostazioni della landing zone senza passare a una nuova versione, ad esempio cambiando le regioni che gestisci. Nella console, il pulsante Aggiorna esegue un aggiornamento sul posto o un'operazione di upgrade, in base alla versione corrente della landing zone e a quella che scegli di implementare.

Scegli la versione della tua landing zone — procedura da console

1. Dalla console AWS Control Tower, accedi alla pagina delle impostazioni della zona di atterraggio. Nella tabella delle zone di atterraggio disponibili, seleziona la nuova versione. Ricorda che puoi selezionare le versioni 3.1 o successive. Le versioni precedenti alla 3.1 non sono compatibili con questa funzionalità.
2. Quando si seleziona una versione dalla tabella, è possibile visualizzare le azioni disponibili. L'aggiornamento è disponibile se la versione corrente è precedente alla versione selezionata. Il ripristino è disponibile se la versione corrente è 3.1 o successiva.
3. Dopo aver scelto la versione, seleziona il pulsante Aggiorna o il pulsante Ripristina, nell'area in alto a destra dello schermo.
4. Verrà visualizzata una schermata di conferma che mostra la versione della landing zone selezionata per il dispiegamento. Per continuare, scegli Avanti in basso a destra. L'operazione di aggiornamento potrebbe richiedere alcuni minuti o più.
5. Dopo l'aggiornamento della landing zone, potrebbe essere necessario aggiornare le unità organizzative registrate. Per aggiornare un'unità organizzativa, è necessario registrarla nuovamente utilizzando la procedura Re-register OU. Re-registering un'unità organizzativa applica la linea di base aggiornata a tutti gli account di quell'unità organizzativa.

Aggiornamenti dell'account, versioni delle landing zone e linee di base

Le landing zone di AWS Control Tower sono AWS risorse che corrispondono a una serie di configurazioni di base. Non esiste una mappatura individuale delle versioni delle linee di base e delle landing zone. È possibile visualizzare una tabella che mostra. [Compatibilità delle versioni di base delle unità organizzative e delle landing zone](#)

Quando passi a una versione base, devi aggiornare gli account dopo l'aggiornamento della landing zone. Ad esempio, quando effettui l'aggiornamento dalla 3.1 alla 3.2, non è necessario aggiornare i tuoi account, poiché queste versioni di landing zone condividono la stessa linea di base.

Al contrario, se esegui l'aggiornamento dalla 3.1 alla 3.3, dovrai aggiornare gli account, poiché la versione di base è la 4.0, che comprende la 3.2 e la 3.3.

Per ulteriori informazioni sulla relazione tra le versioni delle landing zone e le linee di base, vedere. [Compatibilità delle versioni di base delle unità organizzative e delle landing zone](#)

Conserva i AWS CloudTrail trail durante l'aggiornamento delle landing zone

Puoi scegliere di conservare i AWS CloudTrail percorsi a livello di account quando esegui l'upgrade della versione della landing zone di AWS Control Tower.

Prerequisiti

- La versione della tua landing zone è inferiore alla 3.0.
- L'operazione di creazione o aggiornamento più recente è riuscita.

Per mantenere il percorso a livello di account e optare per i percorsi a livello di organizzazione CloudTrail

1. Contatta l' AWS assistenza con una richiesta per inserire il tuo account nella lista consentita.
2. Il team di supporto conferma quando l'account di destinazione è nella lista consentita.
3. Dopo la conferma, aggiorna la landing zone alla versione 3.1 o successiva e scegli AWS CloudTrail Configurazione - Abilitata.

Per conservare il percorso a livello di account e disattivare i CloudTrail percorsi gestiti da AWS Control Tower

1. Contatta l' AWS assistenza con una richiesta per inserire il tuo account nella lista consentita.
2. Il team di supporto conferma quando l'account di destinazione è nella lista consentita.
3. Dopo la conferma, aggiorna la landing zone alla versione 3.1 o successiva e scegli AWS CloudTrail configurazione - Non abilitato.

 Important

Dopo aver mantenuto i CloudTrail percorsi a livello di account, non possiamo rimuovere i percorsi o rimuovere i tuoi account dall'elenco consentito.

Come effettuare una richiesta di assistenza per conservare gli itinerari a livello di account

Se hai bisogno di conservare i percorsi a livello di account durante un aggiornamento di Landing Zone, devi contattare AWS Support per aggiungere il tuo account all'elenco degli account consentiti di AWS Control Tower. Segui questi passaggi per inviare un ticket di supporto:

1. Accedi alla console AWS di gestione.
2. Vai al AWS Support Center.
3. Scegli Crea caso.
4. Per Tipo di custodia, seleziona Supporto tecnico.
5. Per Service, scegli AWS Control Tower.
6. Per Categoria, seleziona Guida generale.
7. Nella riga Oggetto, includi la seguente frase:

`Allow retention of account-level trails during Landing Zone update`

8. Nel campo Descrizione, fornisci i seguenti dettagli:

- Il numero AWS del tuo account di gestione
- La regione d'origine selezionata per il tuo ambiente AWS Control Tower

9. Completa tutti gli altri campi obbligatori nel modulo di richiesta di supporto.

10. Scegli Invia per creare la richiesta di supporto.

Dopo aver inviato il ticket, AWS Support esamina la tua richiesta e aggiunge il tuo account all'elenco degli account consentiti, se appropriato. Riceverai ulteriori istruzioni e conferme tramite il canale di comunicazione dei casi di assistenza.

Note

Per eliminare l'itinerario a livello di account dopo che è stato inserito nell'elenco consentito, utilizza l'account di gestione per eliminare il set di stack o un'istanza di CloudFormation stack specifica. Tutte le risorse dello stack vengono eliminate.

Risolvi la deriva con Reset e Re-register

La deriva si verifica spesso quando tu e i membri della tua organizzazione utilizzate la landing zone.

Il rilevamento della deriva è automatico in AWS Control Tower. Le scansioni automatiche degli SCP ti aiutano a identificare le risorse che necessitano di modifiche o aggiornamenti di configurazione da apportare per risolvere il problema.

Per riparare molti tipi di deriva, scegli Ripristina nella pagina delle impostazioni della zona di atterraggio della console. Inoltre, puoi risolvere alcuni tipi di deriva scegliendo Re-register un'unità organizzativa nella console. Per quanto riguarda i controlli, è possibile risolvere la deriva a livello di codice chiamando l'API. `ResetEnabledControl` Per ulteriori informazioni sui tipi di deriva e su come risolverli, consulta e. [Tipi di deriva della governance](#) [Rileva e risolvi la deriva in AWS Control Tower](#)

Un caso speciale di risoluzione della deriva si verifica per la deriva dei ruoli. Se un ruolo richiesto non è disponibile, la console mostra una pagina di avviso e alcune istruzioni su come ripristinare il ruolo. La landing zone non è disponibile finché non viene risolto il problema del ruolo. Questo drift reset non è lo stesso di un reset completo della landing zone. Per ulteriori informazioni, consulta [Non eliminare i ruoli richiesti nella sezione chiamata Tipi di deriva da risolvere immediatamente](#).

 Quando si interviene per risolvere il problema della deriva in una versione con landing zone, il comportamento dipende dalla versione corrente.

- Se utilizzi la versione 3.1 o successiva della landing zone, puoi scegliere **Aggiorna** per modificare la configurazione della landing zone senza aggiornare le versioni, oppure scegliere **Ripristina** per riapplicare le configurazioni salvate alle risorse della tua drifted landing zone. La deriva viene risolta come parte del processo di aggiornamento.

- Se utilizzi una versione di landing zone precedente alla 3.1, non puoi scegliere Reset. Devi scegliere Aggiorna e aggiornare la tua landing zone almeno alla versione 3.1.

Fornisci e aggiorna gli account utilizzando l'automazione

Note

La fornitura, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) con AWSControlTowerBaseline abilitato. Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare le ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su quell'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

Puoi effettuare il provisioning o aggiornare singoli account in AWS Control Tower con diversi metodi:

- Puoi effettuare il provisioning e personalizzare gli account con AWS Control Tower Account Factory for Terraform (AFT). Per ulteriori informazioni, consulta [Panoramica di AWS Control Tower Account Factory for Terraform \(AFT\)](#).
- Puoi aggiornare gli account con Customizations for AWS Control Tower (cFCT). Per ulteriori informazioni, consulta [Panoramica sulle personalizzazioni per AWS Control Tower \(cFCT\)](#).
- Automazione degli script: se preferisci utilizzare un approccio API, puoi aggiornare gli account utilizzando il [framework API](#) di Service Catalog e AWS CLI aggiornare gli account in un processo in batch. Dovresti chiamare l'[UpdateProvisionedProduct](#) API di Service Catalog per ogni account. È possibile scrivere uno script per aggiornare gli account, uno per uno, con questa API. Ulteriori informazioni su questo approccio, quando si aggiungono le regioni per la governance, sono disponibili in un post sul blog, [Enabling guardrails in new AWS Regions](#).

Puoi aggiornare fino a cinque (5) account alla volta. È necessario attendere che almeno un aggiornamento dell'account abbia esito positivo prima di iniziare il successivo aggiornamento dell'account. Pertanto, il processo potrebbe richiedere molto tempo se si dispone di molti account, ma non è complicato. Per ulteriori informazioni su questo approccio, vedere il [Automatizza il provisioning degli account nelle API AWS Control Tower tramite Service Catalog](#).

 Procedura guidata: video

[Procedura guidata: video](#) È progettato per il provisioning automatico degli account con uno script, ma i passaggi si applicano anche all'aggiornamento dell'account. Utilizza l'UpdateProvisionedProductAPI anziché l'ProvisionProductAPI.

Un ulteriore passaggio dell'automazione tramite script consiste nel verificare lo stato di Succeed dell'evento del UpdateLandingZone ciclo di vita di AWS Control Tower. Usalo come trigger per iniziare ad aggiornare i singoli account come descritto nel video. Un evento del ciclo di vita segna il completamento di una sequenza di attività, quindi il verificarsi di questo evento indica che l'aggiornamento della landing zone è completo. L'aggiornamento della landing zone deve essere completato prima dell'inizio degli aggiornamenti dell'account. Per ulteriori informazioni sull'utilizzo degli eventi del ciclo di vita, vedere [Eventi del ciclo di vita](#).

Consulta anche:

- [Utilizzo AWS CloudShell con cui lavorare AWS Control Tower](#).
- [Automatizza le attività in AWS Control Tower](#).

Automatizza le attività in AWS Control Tower

Molti clienti preferiscono automatizzare le attività in AWS Control Tower, come il provisioning degli account, l'assegnazione dei controlli e l'audit. Puoi configurare queste azioni automatiche con chiamate a:

- [AWS Service Catalog API](#)
- [AWS Organizations API](#)
- [API AWS Control Tower](#)
- [l'interfaccia a riga di comando AWS](#)
- [Eventi del ciclo di vita](#)

La [Informazioni e link aggiuntivi](#) pagina contiene collegamenti a molti eccellenti post di blog tecnici che possono aiutarti ad automatizzare le attività in AWS Control Tower. Le sezioni che seguono forniscono collegamenti ad aree di questa Guida per l'utente di AWS Control Tower che possono aiutarti ad automatizzare le attività.

Automazione delle attività di controllo

È possibile automatizzare le attività relative all'applicazione e alla rimozione dei controlli (noti anche come guardrail) tramite l'API AWS Control Tower. Per i dettagli, consulta l'[AWS Control Tower API Reference](#).

Per ulteriori informazioni su come eseguire operazioni di controllo con le API di AWS Control Tower, consulta il post sul blog [AWS Control Tower rilascia API, controlli predefiniti per le tue unità organizzative](#).

Automatizzazione delle attività nelle zone di atterraggio

Le API delle zone di atterraggio di AWS Control Tower ti aiutano ad automatizzare determinate attività relative alla tua zona di atterraggio. Per informazioni dettagliate, consulta l'[AWS Control Tower API Reference](#).

Automatizzazione della registrazione dell'unità organizzativa

Le API di base di AWS Control Tower ti aiutano ad automatizzare determinate attività, come la registrazione di un'unità organizzativa. Per informazioni dettagliate, consulta l'[AWS Control Tower API Reference](#).

Chiusura automatica dell'account

Puoi automatizzare la chiusura degli account dei membri di AWS Control Tower con un' AWS Organizations API. Per ulteriori informazioni, consulta [Chiudi un account membro di AWS Control Tower tramite AWS Organizations](#).

Provisioning e aggiornamento automatici degli account

AWS Control Tower Account Factory Customization (AFC) ti aiuta a creare account dalla console AWS Control Tower, con CloudFormation modelli personalizzati che chiamiamo blueprint. Questo processo è automatizzato, nel senso che è possibile creare nuovi account e aggiornare gli account ripetutamente, dopo aver impostato un singolo progetto, senza mantenere le pipeline.

AWS Control Tower Account Factory for Terraform (AFT) segue un GitOps modello per automatizzare i processi di provisioning e aggiornamento degli account in AWS Control Tower. Per ulteriori informazioni, consulta [Effettua il provisioning degli account con AWS Control Tower Account Factory for Terraform \(AFT\)](#).

Customizations for AWS Control Tower (cFCT) ti aiuta a personalizzare la zona di destinazione di AWS Control Tower e a rimanere in linea con le best practice. AWS Le personalizzazioni sono implementate con AWS CloudFormation modelli, politiche di controllo dei servizi (SCP) e politiche di controllo delle risorse (RCP). Per ulteriori informazioni, consulta [Panoramica sulle personalizzazioni per AWS Control Tower \(cFCT\)](#).

Per ulteriori informazioni e un video sul provisioning automatico degli account, vedi [Walkthrough: Automated account provisioning in AWS Control Tower](#) e Automated provisioning with IAM roles. <https://docs.aws.amazon.com/controltower/latest/userguide/roles-how.html#automated-provisioning>

Vedi anche [Aggiornare gli account tramite script](#).

Revisione programmatica dei conti

Per ulteriori informazioni sul controllo [programmatico degli account](#), consulta [Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower](#).

Automazione di altre attività

Per informazioni su come aumentare determinate quote di servizio AWS Control Tower con un metodo di richiesta automatizzato, guarda questo video: [Automatizzare gli aumenti dei limiti di servizio](#).

Per i blog tecnici che trattano i casi d'uso dell'automazione e dell'integrazione, consulta [Automazione e integrazione](#).

Sono disponibili due esempi open source GitHub per aiutarti con determinate attività di automazione legate alla sicurezza.

- L'esempio chiamato [aws-control-tower-org-setup-sample](#) mostra come automatizzare la configurazione dell'account Audit come amministratore delegato per i servizi relativi alla sicurezza.
- L'esempio chiamato [aws-control-tower-account-setup-using-step-functions](#) mostra come [automatizzare le migliori pratiche](#) di sicurezza utilizzando Step Functions, durante il provisioning e la configurazione di nuovi account. Questo esempio include l'aggiunta di titolari a portafogli condivisi a livello organizzativo e l'associazione automatica di gruppi IAM Identity Center a livello di organizzazione a nuovi account. AWS Service Catalog AWS Illustra inoltre come eliminare il VPC predefinito in ogni regione.

La AWS Security Reference Architecture include esempi di codice per automatizzare le attività relative ad AWS Control Tower. Per ulteriori informazioni, consulta le pagine [AWS Prescriptive Guidance](#) e il [repository associato. GitHub](#)

Per informazioni sull'utilizzo di AWS Control Tower con AWS CloudShell, un AWS servizio che facilita il lavoro nella CLI, consulta e la AWS CLI. [AWS CloudShell AWS](#)

Poiché AWS Control Tower è un livello di orchestrazione per AWS Organizations, molti altri AWS servizi sono disponibili tramite API e CLI. AWS Per ulteriori informazioni, consulta Servizi correlati. [AWS](#)

Puoi estendere l'automazione utilizzando gli eventi del ciclo di vita emessi da AWS Control Tower. Questi eventi possono essere monitorati tramite una EventBridge regola Amazon, che può quindi attivare un'automazione personalizzata, ad esempio richiamando una AWS Lambda funzione per applicare tag, configurare risorse o notificare ai team quando si verificano eventi specifici relativi all'account o al controllo nella tua zona di destinazione.

Per ulteriori informazioni sugli eventi del ciclo di vita, consulta Eventi del ciclo di vita in [AWS Control Tower](#).

Utilizzo AWS CloudShell con cui lavorare AWS Control Tower

AWS CloudShell è un AWS servizio che facilita il lavoro nella AWS CLI: è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Non è necessario

scaricare o installare strumenti da riga di comando. Puoi eseguire AWS CLI comandi AWS Control Tower e altri AWS servizi dalla tua shell preferita (Bash PowerShell o Z shell).

All'[avvio AWS CloudShell da Console di gestione AWS](#), le AWS credenziali utilizzate per accedere alla console sono disponibili in una nuova sessione di shell. Puoi saltare l'immissione delle credenziali di configurazione quando interagisci con altri AWS servizi AWS Control Tower e utilizzerai la AWS CLI versione 2, che è preinstallata nell'ambiente di elaborazione della shell. Sei preautenticato con AWS CloudShell

Ottieni le autorizzazioni IAM per AWS CloudShell

AWS Identity and Access Management fornisce risorse di gestione degli accessi che consentono agli amministratori di concedere le autorizzazioni agli utenti IAM e agli utenti dell'IAM Identity Center per l'accesso a AWS CloudShell

Il modo più rapido per un amministratore di concedere l'accesso agli utenti è tramite una AWS policy gestita. Una [policy gestita da AWS](#) è una policy autonoma che viene creata e amministrata da AWS. La seguente policy AWS gestita per CloudShell può essere associata alle identità IAM:

- **AWSCloudShellFullAccess**: concede il permesso di utilizzo AWS CloudShell con accesso completo a tutte le funzionalità.

Se desideri limitare l'ambito delle azioni con cui un utente IAM o un utente IAM Identity Center può eseguire AWS CloudShell, puoi creare una policy personalizzata che utilizzi la policy **AWSCloudShellFullAccess** gestita come modello. Per ulteriori informazioni sulla limitazione delle azioni disponibili per gli utenti in CloudShell, consulta [Gestire AWS CloudShell l'accesso e l'utilizzo con le politiche IAM](#) nella Guida per l'AWS CloudShell utente.

Note

La tua identità IAM richiede anche una policy che conceda il permesso di effettuare chiamate a AWS Control Tower. Per ulteriori informazioni, consulta [Autorizzazioni necessarie per utilizzare la AWS Control Tower console](#).

Avvia AWS CloudShell

Da Console di gestione AWS, puoi avviare CloudShell scegliendo le seguenti opzioni disponibili nella barra di navigazione:

- Scegli l' CloudShell icona.
- Inizia a digitare «cloudshell» nella casella di ricerca, quindi scegli l'opzione. CloudShell

Ora che hai iniziato CloudShell, puoi inserire tutti AWS CLI i comandi con cui hai bisogno di lavorare. AWS Control Tower Ad esempio, puoi controllare il tuo AWS Config stato.

Interagisci con AWS Control Tower attraverso AWS CloudShell

Dopo l'avvio AWS CloudShell da Console di gestione AWS, puoi iniziare immediatamente a interagire con AWS Control Tower dall'interfaccia a riga di comando. AWS CLI i comandi funzionano nel modo standard in CloudShell.

Note

Quando si utilizza AWS CLI in AWS CloudShell, non è necessario scaricare o installare risorse aggiuntive. Sei già autenticato all'interno della shell, quindi non devi configurare le credenziali prima di effettuare chiamate.

Utilizzo AWS CloudShell per facilitare la configurazione AWS Control Tower

Prima di eseguire queste procedure, se non diversamente indicato, è necessario accedere alla regione di origine della propria zona di atterraggio e come utente IAM Identity Center o utente IAM con autorizzazioni amministrative per l'account di gestione che contiene la zona di atterraggio.

Console di gestione AWS

1. Ecco come utilizzare i comandi AWS Config CLI AWS CloudShell per determinare lo stato del registratore di configurazione e del canale di consegna prima di iniziare a configurare la AWS Control Tower zona di atterraggio.

Esempio: controlla il tuo stato AWS Config

Comandi di visualizzazione:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- La risposta normale è qualcosa del genere "name": "default"

2. Se hai un AWS Config registratore o un canale di consegna esistente che devi eliminare prima di configurare la tua zona di AWS Control Tower atterraggio, ecco alcuni comandi che puoi inserire:

Esempio: gestisci le tue risorse preesistenti AWS Config

Elimina comandi:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

 Important

Non eliminare le AWS Control Tower risorse per AWS Config. La perdita di queste risorse può causare AWS Control Tower il passaggio a uno stato incoerente.

Per ulteriori informazioni, consulta la AWS Config documentazione

- [Gestione del Configuration Recorder \(AWS CLI\)](#)

-

[Gestione del Canale di Distribuzione](#)

3. Questo esempio mostra i comandi AWS CLI da immettere AWS CloudShell per abilitare o disabilitare l'accesso affidabile. AWS Organizations Poiché AWS Control Tower non è necessario abilitare o disabilitare l'accesso affidabile per AWS Organizations, è solo un esempio. Tuttavia, potrebbe essere necessario abilitare o disabilitare l'accesso affidabile per altri AWS servizi se stai automatizzando o personalizzando le azioni in. AWS Control Tower

Esempio: abilitare o disabilitare l'accesso ai servizi attendibili

- `aws organizations enable-aws-service-access`
- `aws organizations disable-aws-service-access`

Esempio: crea un bucket Amazon S3 con AWS CloudShell

Nel seguente esempio, puoi utilizzarlo AWS CloudShell per creare un bucket Amazon S3 e quindi utilizzare il `PutObject` metodo per aggiungere un file di codice come oggetto in quel bucket.

1. Per creare un bucket in una AWS regione specificata, inserisci il seguente comando nella riga di comando: CloudShell

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

Se la chiamata ha esito positivo, la riga di comando visualizza una risposta del servizio simile al seguente output:

```
{
  "Location": "/insert-unique-bucket-name-here"
}
```

Note

Se non rispetti [le regole per la denominazione dei bucket](#) (utilizzando solo lettere minuscole, ad esempio), viene visualizzato il seguente errore: Si è verificato un errore (InvalidBucketName) durante la chiamata all' `CreateBucket` operazione: Il bucket specificato non è valido.

2. Per caricare un file e aggiungerlo come oggetto al bucket appena creato, chiama il `PutObject` metodo:

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body add_prog.py
```

Se l'oggetto viene caricato correttamente nel bucket Amazon S3, la riga di comando mostra una risposta dal servizio simile al seguente output:

```
{
  "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebcea56\""
}
```

ETagÈ l'hash dell'oggetto che è stato archiviato. Può essere utilizzato per [verificare l'integrità dell'oggetto caricato su Amazon S3](#).

Crea AWS Control Tower risorse con AWS CloudFormation

AWS Control Tower è integrato con AWS CloudFormation, un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri, ad esempio `AWS::ControlTower::EnabledControl` per i controlli. CloudFormation effettua il provisioning e configura tali risorse per te.

Quando lo utilizzi CloudFormation, puoi riutilizzare il modello per impostare le AWS Control Tower risorse in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi esegui il provisioning delle stesse risorse più e più volte in più Account AWS regioni.

AWS Control Tower and CloudFormation modelli

Per effettuare il provisioning e configurare le risorse AWS Control Tower e i servizi correlati, è necessario conoscere [CloudFormation i modelli](#). I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui desideri effettuare il provisioning nei tuoi CloudFormation stack. Se non hai familiarità con JSON o YAML, puoi utilizzare AWS Infrastructure Composer per iniziare a usare i modelli. CloudFormation Per ulteriori informazioni, consulta [Cos'è AWS Infrastructure Composer?](#) nella Guida per l'utente di AWS Infrastructure Composer.

AWS Control Tower supporta la creazione `AWS::ControlTower::EnabledControl` (risorse di controllo), `AWS::ControlTower::LandingZone` (zone di atterraggio) e `AWS::ControlTower::EnabledBaseline` (linee di base) in. CloudFormation Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per questi tipi di risorse, consulta [AWS Control Tower](#) la Guida per l'utente. AWS CloudFormation

Note

Il limite per `EnableControl` `DisableControl` gli aggiornamenti AWS Control Tower è di 100 operazioni simultanee.

Per visualizzare alcuni AWS Control Tower esempi per la CLI e la console, vedi [Abilitare i controlli con. CloudFormation](#)

Scopri di più su CloudFormation

Per saperne di più CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guida per l'utente](#)
- [Documentazione di riferimento dell'API CloudFormation](#)
- [AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando](#)

Personalizza la tua landing zone di AWS Control Tower

Alcuni aspetti della zona di destinazione di AWS Control Tower sono configurabili nella console, come la selezione delle regioni e i controlli opzionali. Altre modifiche possono essere apportate all'esterno della console, con automazione.

Ad esempio, puoi creare personalizzazioni più estese della tua zona di destinazione con la funzionalità Customizations for AWS Control Tower, un framework di GitOps-style personalizzazione che funziona con AWS CloudFormation modelli ed eventi del ciclo di vita di AWS Control Tower.

Personalizza dalla console AWS Control Tower

Per apportare queste personalizzazioni alla tua zona di destinazione, segui i passaggi indicati dalla console AWS Control Tower.

Seleziona nomi personalizzati durante la configurazione

- È possibile selezionare i nomi delle unità organizzative di primo livello durante la configurazione. Puoi rinominare le unità organizzative in qualsiasi momento utilizzando la AWS Organizations console, ma apportare modifiche alle unità organizzative AWS Organizations potrebbe causare problemi [riparabili](#).
- È possibile selezionare i nomi degli account Audit e Log Archive condivisi, ma non è possibile modificarli dopo la configurazione. (Si tratta di una selezione una tantum).

Suggerimento

Ricorda che la ridenominazione di un'unità organizzativa AWS Organizations non comporta l'aggiornamento del corrispondente prodotto fornito in Account Factory. Per aggiornare automaticamente il prodotto a cui è stato assegnato il provisioning (ed evitare la deriva), è necessario eseguire l'operazione dell'unità organizzativa tramite AWS Control Tower, inclusa la creazione, l'eliminazione o la nuova registrazione di un'unità organizzativa.

Select AWS Regioni

- Puoi personalizzare la tua zona di destinazione selezionando regioni specifiche per la governance. AWS Segui i passaggi nella console AWS Control Tower.

- Puoi selezionare e deselezionare AWS le regioni per la governance quando aggiorni la tua zona di atterraggio.
- Puoi impostare il controllo Region Deny su Abilitato o Non abilitato e controllare l'accesso degli utenti alla maggior parte dei AWS servizi nelle regioni non AWS governate.

Per informazioni sui limiti di implementazione Regioni AWS di cFCT, consulta. [Limitazioni di controllo](#)

Personalizza aggiungendo controlli opzionali

- I controlli facoltativi e fortemente consigliati sono opzionali, il che significa che puoi personalizzare il livello di applicazione per la tua zona di atterraggio scegliendo quali attivare. [I controlli opzionali non](#) sono abilitati per impostazione predefinita.
- I controlli opzionali [sulla residenza dei dati](#) consentono di personalizzare le regioni in cui archiviare e consentire l'accesso ai dati.
- I controlli opzionali che fanno parte dello standard integrato Security Hub CSPM consentono di scansionare l'ambiente AWS Control Tower per verificare la presenza di rischi per la sicurezza.
- I controlli proattivi opzionali consentono di controllare le CloudFormation risorse prima del provisioning, per assicurarsi che le nuove risorse siano conformi agli obiettivi di controllo dell'ambiente.

Personalizza le tue AWS CloudTrail trail

- Quando aggiorni la tua zona di destinazione alla versione 3.0 o successiva, puoi scegliere di attivare o disattivare i CloudTrail percorsi a livello di organizzazione gestiti da AWS Control Tower. Puoi modificare questa selezione ogni volta che aggiorni la zona di atterraggio. AWS Control Tower crea un percorso a livello di organizzazione nel tuo account di gestione e tale percorso diventa attivo o inattivo, in base alla tua scelta. La Landing zone 3.0 non supporta i CloudTrail percorsi a livello di account; tuttavia, se ne hai bisogno, puoi configurare e gestire i tuoi percorsi. Potresti incorrere in costi aggiuntivi per percorsi duplicati.

Crea account utente personalizzati nella console

- Puoi creare account membro di AWS Control Tower personalizzati e aggiornare gli account membri esistenti per aggiungere personalizzazioni, dalla console AWS Control Tower. Per ulteriori informazioni, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

Automatizza le personalizzazioni all'esterno della console AWS Control Tower

Alcune personalizzazioni non sono disponibili tramite la console AWS Control Tower, ma possono essere implementate in altri modi. Ad esempio:

- Puoi personalizzare gli account durante il provisioning, in un GitOps-style flusso di lavoro, con [Account Factory for Terraform \(AFT\)](#).

AFT è distribuito con un modulo Terraform, disponibile nel repository AFT. https://github.com/aws-ia/terraform-aws-control_tower_account_factory/tree/main

- Puoi personalizzare la tua landing zone di AWS Control Tower con [Customizations for AWS Control Tower](#) (cFCT), un pacchetto di funzionalità basato su AWS CloudFormation modelli e politiche di controllo dei servizi (SCP). Puoi distribuire modelli e policy personalizzati su singoli account e unità organizzative (OU) all'interno della tua organizzazione.

Il codice sorgente per cFCT è disponibile in un [GitHub repository](#).

- Puoi personalizzare la tua landing zone di AWS Control Tower attivando Landing Zone Accelerator (LZA). AWS La soluzione LZA è progettata per allinearsi alle AWS migliori pratiche e conformarsi a diversi framework di conformità globali. Ti consigliamo di implementare AWS Control Tower come zona di atterraggio fondamentale e quindi di potenziare le funzionalità della zona di destinazione con LZA, se necessario. Per ulteriori informazioni, consulta [AWS Control Tower e Landing zone Accelerator](#).

Torre di controllo AWS e acceleratore di zona di atterraggio

Questa sezione descrive i vantaggi della collaborazione con AWS Control Tower e la soluzione Landing Zone Accelerator (LZA) insieme.

Puoi personalizzare la tua landing zone di AWS Control Tower attivando Landing Zone Accelerator (LZA). AWS

LZA è una soluzione che implementa un set fondamentale di funzionalità progettate per allinearsi alle AWS best practice e a molteplici framework di conformità globali, per aiutarti a gestire e governare un ambiente con più account. LZA è costruito utilizzando il Cloud Development Kit (CDK). AWS

LZA configura automaticamente un ambiente cloud adatto per ospitare carichi di lavoro sicuri. Questa soluzione può essere implementata ovunque Regioni AWS, per aiutarti a mantenere la coerenza

delle operazioni e della governance. La soluzione LZA è progettata per allinearsi alle AWS migliori pratiche e per essere conforme a diversi framework di conformità globali.

Ti consigliamo di implementare AWS Control Tower come zona di destinazione di base e quindi di potenziare le funzionalità della zona di destinazione con LZA, se necessario. La combinazione di LZA e AWS Control Tower fornisce una soluzione completa e senza codice che aiuta a gestire e governare un ambiente con più account: è progettata per supportare carichi di lavoro altamente regolamentati e requisiti di conformità complessi. Insieme, AWS Control Tower e Landing Zone Accelerator ti aiutano a stabilire la preparazione della piattaforma, comprese le funzionalità di sicurezza, conformità e operative.

Il codice sorgente per LZA è disponibile in un repository. [GitHub](#)

Per ulteriori informazioni su come combinare LZA e AWS Control Tower, consulta [la guida all'implementazione di LZA](#).

Vantaggi delle personalizzazioni per AWS Control Tower (cFCT)

Il pacchetto di funzionalità a cui ci riferiamo come Customizations for AWS Control Tower (cFCT) ti aiuta a creare personalizzazioni più estese per la tua zona di destinazione rispetto a quelle che puoi creare nella console AWS Control Tower. Offre un processo automatizzato GitOps-style. Puoi rimodellare la tua zona di atterraggio per soddisfare le tue esigenze aziendali.

Questo processo di personalizzazione dell'infrastruttura come codice integra i AWS CloudFormation modelli con le politiche di controllo dei AWS servizi (SCP), le politiche di controllo delle risorse (RCP) e gli eventi del [ciclo di vita di AWS Control Tower, in modo che le distribuzioni delle risorse rimangano sincronizzate con la tua zona di destinazione](#). Ad esempio, quando crei un nuovo account con Account Factory, le risorse collegate all'account e all'unità organizzativa possono essere distribuite automaticamente.

Note

A differenza di Account Factory e AFT, cFCT non ha lo scopo specifico di creare nuovi account, ma di personalizzare gli account e le unità organizzative nella tua zona di destinazione implementando le risorse specificate.

 Note

L'unità organizzativa (OU) di destinazione configurata in cFCT deve essere AWSControlTowerBaseline abilitata in AWS Control Tower. Per i dettagli AWSControlTowerBaseline, consulta: [Tipi di base applicabili a livello di unità organizzativa](#).

Vantaggi

- Espandi un AWS ambiente personalizzato e sicuro: puoi espandere più rapidamente il tuo ambiente AWS Control Tower con più account e incorporare le AWS migliori pratiche in un flusso di lavoro di personalizzazione ripetibile.
- Crea un'istanza dei tuoi requisiti: puoi personalizzare la tua landing zone di AWS Control Tower in base alle tue esigenze aziendali, con i AWS CloudFormation modelli e le politiche di controllo dei servizi che esprimono le tue intenzioni politiche.
- Automatizza ulteriormente con gli eventi del ciclo di vita di AWS Control Tower: gli eventi del ciclo di vita consentono di distribuire le risorse in base al completamento di una serie precedente di eventi. Puoi fare affidamento su un evento del ciclo di vita per aiutarti a distribuire le risorse su account e unità organizzative in modo automatico.
- Estendi l'architettura di rete: puoi implementare architetture di rete personalizzate che migliorano e proteggono la tua connettività, come un gateway di transito.

Esempi cFCT aggiuntivi

- Un esempio di caso d'uso di rete con Customizations for AWS Control Tower (cFCT) è riportato nel post del blog AWS Architecture, [Deploy consistent DNS with Service Catalog e AWS Control Tower customizations](#).
- Un esempio specifico [relativo a cFCT e Amazon GuardDuty](#) è disponibile nel repository. GitHub [aws-samples](#)
- Ulteriori esempi di codice relativi a cFCT sono disponibili come parte della AWS Security Reference Architecture, nel repository. [aws-samples](#) Molti di questi esempi contengono manifest.yaml file di esempio in una directory denominata. customizations_for_aws_control_tower

Per ulteriori informazioni sulla AWS Security Reference Architecture, consulta le pagine [AWS Prescriptive Guidance](#).

Panoramica sulle personalizzazioni per AWS Control Tower (cFCT)

Le personalizzazioni per AWS Control Tower (cFCT) ti aiutano a personalizzare la tua landing zone di AWS Control Tower e a rimanere in linea con AWS le best practice. Le personalizzazioni sono implementate con AWS CloudFormation modelli, policy di controllo dei servizi (SCP) e politiche di controllo delle risorse (RCP).

Questa funzionalità cFCT è integrata con gli eventi del ciclo di vita di AWS Control Tower, in modo che le distribuzioni delle risorse rimangano sincronizzate con la landing zone. Ad esempio, quando viene creato un nuovo account tramite account factory, tutte le risorse collegate all'account vengono distribuite automaticamente. È possibile distribuire i modelli e le politiche personalizzati su singoli account e unità organizzative (OU) all'interno dell'organizzazione.

Note

L'unità organizzativa (OU) di destinazione configurata in cFCT deve essere AWSControlTowerBaseline abilitata in AWS Control Tower. Per i dettagli di AWSControlTowerBaseline, consulta: [Tipi di base applicabili a livello di unità organizzativa](#).

Il video seguente descrive le migliori pratiche per l'implementazione di una pipeline cFCT scalabile e le personalizzazioni cFCT comuni.

La sezione seguente fornisce considerazioni sull'architettura e i passaggi di configurazione per la distribuzione di personalizzazioni per AWS Control Tower (cFCT). Include un collegamento al [AWS CloudFormation](#) modello che avvia, configura ed esegue i AWS servizi richiesti, in linea con le migliori pratiche di sicurezza e disponibilità. AWS

Questo argomento è destinato agli architetti e agli sviluppatori di infrastrutture IT che hanno esperienza pratica nell'architettura nel cloud. AWS

Per informazioni sugli aggiornamenti e le modifiche più recenti a Customizations for AWS Control Tower (cFCT), consulta il [CHANGELOG.md file nel repository](#). GitHub

Panoramica dell'architettura

L'implementazione di cFCT crea il seguente ambiente nel AWS cloud, con un bucket Amazon S3 come origine di configurazione.

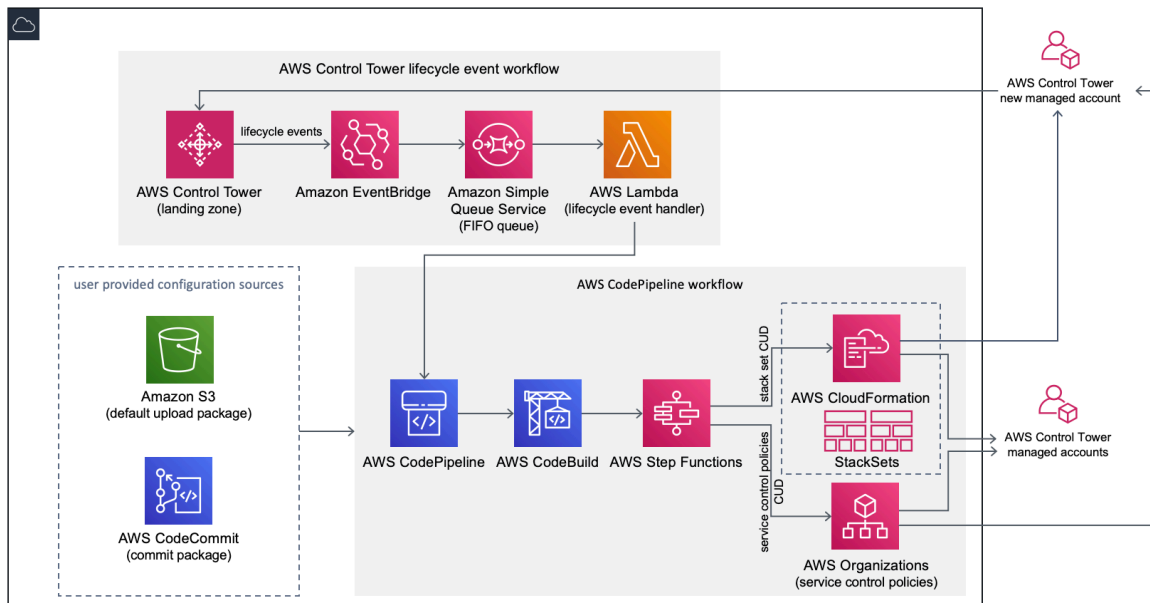


Figura 1: Personalizzazioni per l'architettura AWS Control Tower

cFct include un AWS CloudFormation modello da distribuire nel tuo account di gestione AWS Control Tower. Il modello avvia tutti i componenti necessari per creare i flussi di lavoro, in modo da poter personalizzare la landing zone di AWS Control Tower.

Nota

cFct deve essere distribuito nella regione principale di AWS Control Tower e nell'account di gestione AWS Control Tower, perché è lì che viene distribuita la landing zone di AWS Control Tower. Per informazioni sulla configurazione di una landing zone di AWS Control Tower, consulta [Nozioni di base](#).

Durante la distribuzione, cFct impacchetta e carica le risorse personalizzate nel codice sorgente della pipeline, tramite Amazon [Simple Storage Service \(Amazon S3\)](#). Il processo di caricamento richiama automaticamente la macchina a stati delle politiche di controllo dei servizi (SCP), la macchina a stati delle politiche di controllo delle risorse (RCP) e la macchina a [AWS CloudFormation StackSets](#) stati per distribuire SCP e RCP a livello di unità organizzativa o per distribuire istanze stack a livello di unità organizzativa o di account.

 Nota

Per impostazione predefinita, cFct crea un bucket Amazon S3 per archiviare l'origine della pipeline. Se disponi di un AWS CodeCommit repository esistente, puoi modificare la posizione in un repository. [CodeCommit](#) Per ulteriori informazioni, consulta [Configurare Amazon S3 come origine di configurazione](#).

cFCT implementa due flussi di lavoro:

- [AWS CodePipeline](#) un flusso di lavoro
- e un flusso di lavoro relativo agli eventi del ciclo di vita di AWS Control Tower.

Il flusso di lavoro AWS CodePipeline

Il AWS CodePipeline flusso di lavoro configura AWS CodePipeline, [AWS CodeBuild](#) progetta e [AWS Step Functions](#) coordina la gestione di AWS CloudFormation StackSets SCP e RCP all'interno dell'organizzazione.

Quando caricate il pacchetto di configurazione, cFct richiama la pipeline di codice per eseguire quattro fasi.

- Build Stage: convalida il contenuto del pacchetto di configurazione utilizzando AWS CodeBuild.
- SCP Stage: richiama la macchina a stati della policy di controllo del servizio, che chiama l' AWS Organizations API per creare SCP.
- RCP Stage: richiama la macchina a stati della politica di controllo delle risorse, che chiama l'API per creare RCP. AWS Organizations
- CloudFormation Stage: [richiama lo stack set state machine per distribuire le risorse specificate nell'elenco di account o unità organizzative, che hai fornito nel file manifest.](#)

In ogni fase, la pipeline del codice richiama le funzioni stack set, SCP e RCP step, che distribuiscono set di stack, SCP e RCP personalizzati ai singoli account di destinazione o a un'intera unità organizzativa.

 Nota

Per informazioni dettagliate sulla personalizzazione del pacchetto di configurazione, fare riferimento a. [Guida alla personalizzazione cFCT](#)

Il flusso di lavoro degli eventi del ciclo di vita di AWS Control Tower

Quando viene creato un nuovo account in AWS Control Tower, un [evento del ciclo](#) di vita può richiamare il flusso di lavoro. AWS CodePipeline Puoi personalizzare il pacchetto di configurazione tramite questo flusso di lavoro, che consiste in una regola di EventBridge eventi [Amazon](#), una coda FIFO (First-in First-Out) di Amazon [Simple Queue Service](#) (Amazon SQS) e una funzione. [AWS Lambda](#)

Quando la regola EventBridge degli eventi di Amazon rileva un evento del ciclo di vita corrispondente, passa l'evento alla coda FIFO di Amazon SQS, richiama la AWS Lambda funzione e richiama la pipeline di codice per eseguire la distribuzione a valle di stack set, SCP e RCP.

Costo

Il costo di esecuzione di cFCT dipende dal numero di AWS CodePipeline esecuzioni, dalla durata delle AWS CodeBuild esecuzioni, dal numero e dalla durata delle AWS Lambda funzioni e dal numero di EventBridge eventi Amazon pubblicati. Ad esempio, se esegui 100 build in un mese utilizzando build.general1.small, in cui ogni build viene eseguita per cinque minuti, il costo approssimativo per l'esecuzione di cFCT è di 3,00 USD al mese. Per tutti i dettagli, puoi consultare la pagina web dei prezzi per ogni servizio che utilizzi. AWS

Le risorse del bucket AWS CodeCommit Git-based e del repository Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) vengono conservate dopo l'eliminazione del modello, per proteggere le informazioni di configurazione. A seconda dell'opzione selezionata, i costi vengono addebitati in base alla quantità di dati archiviati nel bucket Amazon S3 e al numero di richieste Git (non applicabile alla risorsa Amazon S3). Per ulteriori informazioni, consulta [Amazon S3](#) e [AWS CodeCommit](#) prezzi.

Servizi relativi ai componenti

I seguenti AWS servizi sono componenti di Customizations for AWS Control Tower (cFCT).

AWS CodeCommit

Se disponi di un AWS CodeCommit repository esistente, puoi configurarlo come fonte per la tua pipeline, in alternativa ad Amazon S3.

In base ai dati inseriti nel CloudFormation modello, cFCT può creare un [AWS CodeCommit](#) repository con la stessa configurazione di esempio spiegata nella sezione Amazon Simple Storage Service.

Per clonare il AWS CodeCommit repository cFCT sul tuo computer locale, devi creare credenziali che ti consentano di accedere temporaneamente al repository, come spiegato nella Guida per l'utente.

[AWS CodeCommit](#) Per informazioni sulla compatibilità delle versioni, consulta Configurazione per.

[AWS CodeCommit](#)

Note

Se non lo usi già CodeCommit, l'unica opzione è configurare il bucket Amazon S3 come posizione di archiviazione per il pacchetto di configurazione. CodeCommit non è disponibile se stai implementando cFCT per la prima volta.

AWS CodePipeline

AWS CodePipeline convalida, testa e implementa le modifiche in base agli aggiornamenti del pacchetto di configurazione, che effettuerai nel bucket Amazon S3 predefinito o nel repository. AWS CodeCommit Per ulteriori informazioni sul controllo del codice sorgente di configurazione, consulta [Using Amazon S3 as the Configuration Source](#). La pipeline include fasi per convalidare e gestire i file e i modelli di configurazione, gli account principali, le politiche di controllo dei AWS Organizations servizi e. AWS CloudFormation StackSets Per ulteriori informazioni sulle fasi della pipeline, consulta [Guida alla personalizzazione cFCT](#)

AWS Key Management Service

CFct crea una chiave di CustomControlTowerKMSKey crittografia [AWS Key Management Service](#) (AWS KMS). Questa chiave viene utilizzata per crittografare gli oggetti nel bucket di configurazione Amazon S3, nella coda Amazon SQS e nei parametri sensibili nel Systems Manager Parameter Store. AWS Per impostazione predefinita, solo i ruoli assegnati da cFCT sono autorizzati a eseguire operazioni di crittografia o decrittografia con questa chiave. Per accedere al file di configurazione, alla coda FIFO o ai SecureString valori del Parameter Store, è necessario aggiungere amministratori

alla policy. CustomControlTowerKMSKey La rotazione automatica dei tasti è abilitata per impostazione predefinita.

AWS Lambda

cFCT utilizza AWS Lambda funzioni per richiamare i componenti di installazione durante l'installazione iniziale e la distribuzione di AWS CloudFormation StackSets o AWS Organizations SCP durante un evento del ciclo di vita di AWS Control Tower.

Amazon Simple Notification Service

cFCT può pubblicare notifiche, ad esempio l'approvazione della pipeline per gli argomenti di Amazon Simple Notification Service ([Amazon SNS](#)) durante il flusso di lavoro. Amazon SNS viene avviato solo quando scegli di ricevere notifiche di approvazione della pipeline.

Amazon Simple Storage Service

Quando distribuisce cFCT, cFCT crea un bucket Amazon Simple Storage Service (Amazon S3) con un nome univoco:

Esempio: nome del bucket Amazon S3

`custom-control-tower-configuration-accountID-region`

Il bucket contiene un file di configurazione di esempio chiamato `_custom-control-tower-configuration.zip`

Notate il carattere di sottolineatura iniziale nel nome del file.

Questo file zip fornisce un manifesto di esempio e i relativi modelli di esempio che descrivono la struttura delle cartelle necessaria. Questi esempi ti aiutano a sviluppare un pacchetto di configurazione per personalizzare la tua zona di destinazione di AWS Control Tower. Il manifesto di esempio identifica le configurazioni richieste per gli stack set e le policy di controllo dei servizi (SCP) di cui avrai bisogno quando implementi le personalizzazioni.

Puoi utilizzare questo pacchetto di configurazione di esempio come modello per sviluppare e caricare il tuo pacchetto personalizzato, che attiva automaticamente la pipeline di configurazione cFCT.

Per informazioni sulla personalizzazione del file di configurazione, vedere. [Guida alla personalizzazione cFCT](#)

Amazon Simple Queue Service

cFCT utilizza una coda FIFO di Amazon Simple Queue Service (Amazon SQS) per acquisire gli eventi del ciclo di vita da Amazon. EventBridge Attiva una funzione che richiama i nostri SCP per la distribuzione. AWS Lambda AWS CodePipeline AWS CloudFormation StackSets Per ulteriori informazioni sugli SCP, vedere. [AWS Organizations](#)

AWS Step Functions

CfCT crea Step Functions per orchestrare le implementazioni di personalizzazione. Queste Step Functions traducono i file di configurazione per distribuire le personalizzazioni necessarie in tutti gli ambienti.

AWS Systems Manager Parameter Store

[AWS Systems Manager Parameter Store](#) memorizza i parametri di configurazione cFCT. Questi parametri consentono di integrare i modelli di configurazione correlati. Ad esempio, puoi configurare ciascun account per registrare AWS CloudTrail i dati in un bucket Amazon S3 centralizzato. Inoltre, il Systems Manager Parameter Store fornisce una posizione centralizzata in cui gli amministratori possono visualizzare gli input e i parametri CFCT.

Considerazioni sull'implementazione

Assicurati di avviare Customizations for AWS Control Tower (cFCT) nello stesso account e nella stessa regione in cui è distribuita la landing zone di AWS Control Tower; ovvero, devi distribuirla nell'account di gestione AWS Control Tower nella tua regione di origine di AWS Control Tower. Per impostazione predefinita, cFct crea ed esegue il pacchetto di configurazione delle landing zone impostando una pipeline di configurazione in quell'account e nella regione.

Preparati per la distribuzione

Hai a disposizione alcune opzioni quando prepari il CloudFormation modello per la distribuzione iniziale. È possibile scegliere l'origine della configurazione e consentire l'approvazione manuale delle distribuzioni della pipeline. Le due sezioni successive spiegano di più su queste opzioni.

Scegliete la fonte di configurazione

Per impostazione predefinita, il modello crea un bucket Amazon Simple Storage Service (Amazon S3) per archiviare il pacchetto di configurazione di esempio come file chiamato. `.zip_custom-`

`control-tower-configuration.zip` Il bucket Amazon S3 è controllato dalla versione ed è possibile aggiornare il pacchetto di configurazione in base alle esigenze. Per informazioni sull'aggiornamento del pacchetto di configurazione, consulta [Utilizzo di Amazon S3 come origine di configurazione](#).

 Ricordati di rimuovere il carattere di sottolineatura

Il nome del file del pacchetto di configurazione di esempio inizia con un carattere di sottolineatura (`_`) in modo che AWS CodePipeline non venga avviato automaticamente. Quando hai finito di personalizzare il pacchetto di configurazione, assicurati di caricare il file `custom-control-tower-configuration.zip` senza il carattere di sottolineatura (`_`) per iniziare la distribuzione in AWS CodePipeline

Se disponi di un AWS CodeCommit repository Git esistente, puoi modificare la posizione di archiviazione del pacchetto di configurazione dal bucket Amazon S3 a un AWS CodeCommit repository Git. Per farlo, seleziona l'opzione `CodeCommit` nel parametro `CloudFormation`

 Comprimere o non comprimere?

Quando utilizzi il bucket S3 predefinito, assicurati che il pacchetto di configurazione sia disponibile come `.zip` file. Se utilizzi il AWS CodeCommit repository, assicurati di inserire il pacchetto di configurazione nel repository senza comprimere i file. Per informazioni sulla creazione e l'archiviazione del pacchetto di configurazione in AWS CodeCommit, consulta [Guida alla personalizzazione cFCT](#)

È possibile utilizzare il pacchetto di configurazione di esempio per creare una fonte di configurazione personalizzata. Quando sei pronto per distribuire le configurazioni personalizzate, carica manualmente il pacchetto di configurazione, nel bucket Amazon S3 o nel repository AWS CodeCommit. La pipeline inizia automaticamente quando carichi il file di configurazione.

Scegliete i parametri di approvazione della configurazione della pipeline

Il AWS CloudFormation modello offre la possibilità di approvare manualmente l'implementazione delle modifiche alla configurazione. Per impostazione predefinita, l'approvazione manuale non è abilitata. Per ulteriori informazioni, fare riferimento alla [Fase 1. Avvia lo stack](#).

Quando l'approvazione manuale è abilitata, la pipeline di configurazione convalida le personalizzazioni apportate al file manifest e ai modelli di AWS Control Tower, quindi sospende il processo fino a quando non viene concessa l'approvazione manuale. Dopo l'approvazione, la distribuzione procede all'esecuzione delle fasi rimanenti della pipeline, in base alle necessità, per implementare la funzionalità Customizations for AWS Control Tower (cFCT).

Puoi utilizzare il parametro di approvazione manuale per impedire l'esecuzione delle personalizzazioni per la configurazione di AWS Control Tower, rifiutando il primo tentativo di esecuzione attraverso la pipeline. Questo parametro consente inoltre di convalidare manualmente le personalizzazioni per le modifiche alla configurazione di AWS Control Tower, come controllo finale prima dell'implementazione.

Per aggiornare le personalizzazioni per AWS Control Tower

Se hai già distribuito cFCT, devi aggiornare lo CloudFormation stack per ottenere la versione più recente del framework cFCT. [Per i dettagli, consulta Update the Stack.](#)

Modello e codice sorgente

Le personalizzazioni per AWS Control Tower (cFCT) vengono distribuite nel tuo account di gestione dopo il lancio del modello. AWS CloudFormation Puoi scaricare [il modello](#) da GitHub e poi avviarlo da. [AWS CloudFormation](#)

Il customizations-for-aws-control-tower.template implementa quanto segue:

- AWS CodeBuild Un progetto
- Un AWS CodePipeline progetto
- Una EventBridge regola Amazon
- AWS Lambda funzioni
- Una coda Amazon Simple Queue Service
- Un bucket Amazon Simple Storage Service con un pacchetto di configurazione di esempio
- AWS Step Functions

Note

Puoi personalizzare il modello in base alle tue esigenze specifiche.

Archivio del codice sorgente

Puoi visitare il nostro [GitHub repository](#) per scaricare i modelli e gli script per cFCT e condividere le personalizzazioni delle tue landing zone con altri.

Implementazione automatica

Prima di avviare la distribuzione automatizzata, esamina le [considerazioni](#). Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nel tuo account di gestione AWS Control Tower.

Tempo di implementazione: circa 15 minuti

Prerequisiti

cFct deve essere distribuito nel tuo account di gestione AWS Control Tower e nella tua regione di origine AWS Control Tower. Se non hai configurato una landing zone, vedi [Nozioni di base](#).

Fasi della distribuzione

La procedura per l'implementazione del cFCT consiste in due fasi principali. Per istruzioni dettagliate, segui i collegamenti per ciascuna fase.

[Fase 1: Avvio dello stack](#)

- Avvia il CloudFormation modello nel tuo account di gestione.
- Rivedi i parametri del modello e modificali se necessario.

[Fase 2: Crea un pacchetto personalizzato](#)

- Crea un pacchetto di configurazione personalizzato.

Important

Per scaricare il AWS CloudFormation modello corretto e avviare cFCT, segui il GitHub link fornito in questa sezione. Non seguite i link più vecchi verso i bucket S3 precedentemente specificati.

Fase 1: Avvio dello stack

Il CloudFormation modello in questa sezione distribuisce personalizzazioni per AWS Control Tower (cFCT) nel tuo account.

Nota

Sei responsabile del costo dei AWS servizi utilizzati durante l'esecuzione di cFCT. Per ulteriori dettagli, consulta [Costo](#).

1. Per avviare Customizations for AWS Control Tower, [scarica il modello da GitHub](#) e avvialo da [AWS CloudFormation](#).
2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare cFCT in un'altra AWS regione, utilizza il selettore della regione nella barra di navigazione della console.

Note

cFct deve essere lanciato nella stessa regione e nello stesso account in cui hai distribuito la landing zone di AWS Control Tower, che è la tua regione di origine.

3. Nella pagina Create stack, verifica che l'URL del modello corretto sia visualizzato nella casella di testo dell'URL e scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack cFCT.
5. In Parametri, esaminate i seguenti parametri e modificali nel modello, se necessario.

Configurazione della pipeline

Parametro	Predefinito	Descrizione
Fase di approvazione della pipeline	No	Scegliete se modificare la configurazione della pipeline dalla fase di approvazione automatica predefinita a una fase di approvazione manuale. Per ulteriori

Configurazione della pipeline		
Parametro	Predefinito	Descrizione
		informazioni, consulta the section called “Guida alla personalizzazione cFCT” .
Indirizzo e-mail di approvazione della pipeline	<Optional Input>	L'indirizzo e-mail per le notifiche di approvazione. Per utilizzare questo parametro, è necessario impostare il parametro Pipeline Approval Yes Stage su.
CodePipelineFonte AWS	Amazon S3	La fonte per AWS CodePipeline per aiutarti a scegliere dove archiviare e configurare le personalizzazioni cFCT.
CodeCommit Configurazione AWS		
Parametro	Predefinito	Descrizione
CodeCommitRepository esistente?	No	Scegli se usare un repository CodeCommit Git esistente. Se si sceglie Yes , è necessario impostare il parametro CodePipeline Source su AWS CodeCommit .

CodeCommit Configurazione AWS

Parametro	Predefinito	Descrizione
CodeCommit Nome del repository	<code>custom-control-tower-configuration</code>	Se fornisci il nome di un repository Git esistente , devi impostare l'Existing CodeCommitRepository? parametrizza Yes e inserisci il nome esatto di quel repository.
CodeCommit Nome del ramo	<code>main</code>	Il ramo Git in cui è archiviato il pacchetto di personalizzazione. Per utilizzare questo parametro, è necessario impostare il parametro CodePipeline Source suAWS CodeCommit .

CloudFormation StackSets Configurazione

Parametro	Predefinito	Descrizione
Tipo di concorrenza regionale	<code>PARALLEL</code>	Seleziona il tipo di concorrenza delle StackSets operazioni di distribuzione nelle regioni. Questa impostazione è applicabile per la creazione , l'aggiornamento e l'eliminazione dei flussi di lavoro. L'altro valore consentito è <code>SEQUENTIAL</code> .

CloudFormation StackSets Configurazione		
Parametro	Predefinito	Descrizione
Percentuale simultanea massima	100	La percentuale massima di account in cui eseguire questa operazione simultaneamente. Il valore massimo consentito è 100. Per ulteriori informazioni, consulta le opzioni operative di Stack Set .
Percentuale di tolleranza agli errori	10	La percentuale di account, per regione, per i quali questa operazione di stack può fallire prima che AWS CloudFormation interrompa l'operazione in quella regione. Il valore minimo consentito è 0 e il valore massimo consentito è 100. Per ulteriori informazioni, consulta le opzioni operative di Stack Set .

6. Scegli Next (Successivo).
7. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
8. Nella pagina Rivedi, verifica e conferma le impostazioni. Assicurati di selezionare la casella di controllo di conferma per la creazione delle risorse (IAM) AWS Identity and Access Management da parte del modello.
9. Seleziona Create (Crea) per implementare lo stack.

È possibile visualizzare lo stato dello stack nella CloudFormation console nella colonna Status. Dovresti vedere lo stato di CREATE_COMPLETE tra circa 15 minuti.

Fase 2: Crea un pacchetto personalizzato

Con lo stack lanciato, puoi aggiungere personalizzazioni alla landing zone di AWS Control Tower e alle policy di controllo dei servizi (SCPs) personalizzando il pacchetto di configurazione incluso. Per istruzioni dettagliate sulla creazione di un pacchetto personalizzato, consulta. [Guida alla personalizzazione cFCT](#)

Nota

La pipeline non viene eseguita senza caricare il pacchetto di configurazione personalizzato.

Aggiorna lo stack

Se in precedenza hai distribuito Customizations for AWS Control Tower (cFCT), segui la procedura per aggiornare lo AWS CloudFormation stack per l'ultima versione del framework cFCT.

Important

Prima di completare la seguente procedura, devi caricare il [modello più recente da](#) in un GitHub bucket Amazon Simple Storage Service (Amazon S3). Per istruzioni su come iniziare a usare Amazon S3, consulta la sezione [Guida introduttiva ad Amazon S3 nella Guida per l'utente di Amazon](#) Simple Storage Service.

1. Accedi alla [AWS CloudFormation console](#).
2. Seleziona lo CloudFormation stack Customizations for AWS Control Tower (cFCT) esistente, quindi seleziona Update.
3. In Prerequisito: prepara il modello, seleziona Sostituisci il modello corrente.
4. In Specificare il modello, procedi come segue:
 - a. Per Origine del modello, selezionate Sostituisci il modello corrente.
 - b. Per l'URL di Amazon S3, inserisci l'URL del modello da GitHub cui hai precedentemente caricato su Amazon S3, quindi scegli Avanti.
 - c. Verifica che l'URL del modello sia corretto. Quindi scegli nuovamente Avanti e Avanti.
5. In Parametri, rivedi i parametri del modello e modificali se necessario. Fate riferimento alla [Fase 1. Avvia lo stack](#) per i dettagli sui parametri.

6. Scegli Next (Successivo).
7. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
8. Nella pagina Rivedi, verifica e conferma le impostazioni. Assicurati di selezionare la casella che conferma che il modello potrebbe creare risorse AWS Identity and Access Management (IAM).
9. Scegli Visualizza set di modifiche e verifica le modifiche.
10. Scegli Aggiorna stack per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti vedere lo stato di UPDATE_COMPLETE tra circa 15 minuti.

Eliminazione di un set di stack

Puoi eliminare un set di stack se hai abilitato l'eliminazione dello stack set nel file manifest. Per impostazione predefinita, il parametro `enable_stack_set_deletion` è impostato su `false`. In questa configurazione, non viene intrapresa alcuna azione per eliminare il set di stack associato quando una risorsa viene rimossa dal file manifest cFct.

Se modificate il valore di `enable_stack_set_deletion` to `true` nel file manifest, cFct elimina lo stack set e tutte le relative risorse quando rimuovete una risorsa associata dal file manifest.

Questa funzionalità è supportata nella versione 2 del file manifest.

Important

Quando impostate inizialmente il valore di `enable_stack_set_deletion` to `true`, la volta successiva che richiamate cfCT, TUTTE le risorse che iniziano con il prefisso `CustomControlTower-`, a cui è associato il tag chiave e che non sono dichiarate nel file manifesto `Key: AWS_Solutions, Value: CustomControlTowerStackSet`, vengono predisposte per l'eliminazione.

Ecco un esempio di come impostare questo parametro in un file: `manifest.yaml`

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true    #New opt-in functionality
```

```
resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
  regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
  regions:
    - us-east-1
    - eu-north-1
```

Configura Amazon S3 come origine di configurazione

Quando configuri Personalizzazioni per AWS Control Tower, memorizza un file di configurazione iniziale, chiamato `_custom-control-tower-configuration.zip` file, in un bucket Amazon Simple Storage Service (Amazon S3) denominato `custom-control-tower-configuration-account-ID-region`

Nota

Se scegli di scaricare e modificare questo file, ricordati di comprimere le modifiche, salvarlo come nuovo file denominato `custom-control-tower-configuration.zip` e quindi caricarlo nuovamente nello stesso bucket Amazon S3.

Il bucket Amazon S3 è l'origine predefinita della pipeline. Una volta impostate le impostazioni predefinite, il caricamento di un file zip di configurazione senza il prefisso di sottolineatura nel nome del file nel bucket S3 avvierà automaticamente la pipeline.

Il file zip è protetto da Server-Side Encryption (SSE) con AWS Key Management Service (AWS KMS) e negazione dell'uso della chiave KMS. Per accedere al file zip, è necessario aggiornare la politica delle chiavi KMS per specificare i ruoli a cui deve essere concesso l'accesso. Il ruolo può essere un ruolo di amministratore, un utente o entrambi. Segui questa procedura:

1. Passare alla [console AWS Key Management Service](#).
2. In Customer Managed Keys, seleziona CustomControlTowerKMSKey.
3. Seleziona la scheda Politica chiave. Quindi, seleziona Modifica.
4. Nella pagina Modifica politica chiave, trova la sezione Consenti l'uso della chiave nel codice e aggiungi una delle seguenti autorizzazioni:
 - Per aggiungere un ruolo amministrativo:

```
arn:aws:iam::<account-ID>:role/<administrator-role>
```
 - Per aggiungere un utente:

```
arn:aws:iam::<account-ID>:user/<username>
```
5. Seleziona Save changes (Salva modifiche).
6. Accedi alla [console Amazon S3](#), trova il bucket S3 contenente il file zip di configurazione e seleziona download.
7. Apporta le modifiche di configurazione necessarie al file manifest e ai file modello. Per informazioni sulla personalizzazione dei file di manifesto e modello, vedere [the section called “Guida alla personalizzazione cFCT”](#).
8. Carica le tue modifiche:
 - a. Comprimi i file di configurazione modificati e assegna un nome al file: custom-control-tower-configuration.zip.
 - b. Carica il file su Amazon S3 utilizzando SSE con la AWS KMS chiave master:
CustomControlTowerKMSKey

Imposta GitHub come fonte di configurazione

Questa sezione spiega come distribuire Customizations for AWS Control Tower (cFCT) con GitHub come sorgente. Il processo prevede tre fasi principali:

- Preparare un GitHub repository
- Crea la connessione tramite GitHub codice

- Distribuisci lo stack CloudFormation

Preparare un repository GitHub

Crea un repository all'interno del tuo GitHub account, il nome predefinito utilizzato nel modello è `custom-control-tower-configuration`. Valuta la possibilità di rendere privato il repository di destinazione. Definirai le tue personalizzazioni in un `yaml` file chiamato `manifest.yaml` nella cartella di [distribuzione del repository](#) cFCT.

La guida alla personalizzazione di [cFCT](#) fornisce una guida dettagliata sulla creazione di una configurazione delle personalizzazioni. `manifest.yaml`

Crea la connessione GitHub

Dalla tua istanza Developer Tools --Connections per Github, procedi nel seguente modo:

1. Seleziona Crea connessione e scegli GitHub come provider
2. Scegli Crea una connessione all' GitHub app e, nel campo Nome connessione, inserisci GitHub cFCT o qualsiasi nome tu scelga
3. Seleziona Connetti a, GitHub quindi scegli Installa una nuova app
4. Seleziona l' GitHub utente o l'organizzazione per il tuo repository
5. In Accesso al repository, scegli Seleziona solo i repository, quindi seleziona il repository che hai creato in precedenza e Salva il tuo lavoro.
6. Annota l'ARN di Code Connections: ti servirà per distribuire lo stack. CloudFormation

Distribuisci il CloudFormation stack

- Scarica il `custom-control-tower-initiation.template` file dal repository.
- Crea un nuovo CloudFormation stack utilizzando il `custom-control-tower-initiation.template` file.
- In AWS CodePipeline Source, scegli GitHub (tramite Code Connection).
- In GitHub Configurazione, specifica questi campi:
 - Per l'ARN di Code Connection, fornisci l'ARN di Code Connection
 - per GitHub Utente o Organizzazione, fornisci il nome dell' GitHub utente o dell'organizzazione con cui hai creato il repository

- Per Nome del GitHub repository, inserisci il nome del repository (il valore predefinito è) `custom-control-tower-configuration`
- Per Nome GitHub filiale, inserisci il nome della filiale (il valore predefinito è) `main`

Raccolta di metriche operative

Le personalizzazioni per AWS Control Tower (cFCT) includono un'opzione per inviare metriche operative anonime a AWS. AWS utilizza questi dati per capire in che modo i clienti utilizzano cFCT e altri servizi e prodotti correlati. Quando la raccolta dei dati è abilitata, le seguenti informazioni vengono inviate a AWS:

- ID soluzione: l'identificatore della AWS soluzione
- ID univoco (UUID): identificatore univoco generato casualmente per ogni implementazione
- Timestamp: marcatura temporale di raccolta dati
- Numero di esecuzioni della macchina a stati: conta in modo incrementale il numero di volte in cui questa macchina a stati viene eseguita
- Versione manifesto: la versione manifest utilizzata nella configurazione

Note

AWS possiede i dati che raccoglie. La raccolta dei dati è soggetta all'[AWS Informativa sulla privacy](#).

Per disattivare l'invio di metriche operative anonime a AWS, completa una delle seguenti attività:

- Aggiorna la sezione AWS CloudFormation di mappatura dei modelli come segue:

da

```
AnonymousData:  
  SendAnonymousData:  
    Data: Yes
```

Da a

```
AnonymousData:
  SendAnonymousData:
    Data: No
```

- Dopo aver distribuito cFct, trova la chiave del parametro **/org/primary/metrics_flag** SSM nella console Parameter Store e aggiorna il valore su **No**

Guida alla personalizzazione cFCT

La guida Customizations for AWS Control Tower (cFCT) è destinata ad amministratori, DevOps professionisti, fornitori di software indipendenti, architetti di infrastrutture IT e integratori di sistemi che desiderano personalizzare ed estendere i propri ambienti AWS Control Tower per la propria azienda e i propri clienti. Fornisce informazioni sulla personalizzazione e l'estensione dell'ambiente AWS Control Tower con il pacchetto di personalizzazione cFCT.

Note

Per distribuire e configurare (cFCT), è necessario distribuire ed elaborare un pacchetto di configurazione tramite AWS CodePipeline. Le sezioni seguenti descrivono il processo in dettaglio.

Panoramica della pipeline di codice

Il pacchetto di configurazione richiede Amazon Simple Storage Service (Amazon S3) e AWS CodePipeline. Il pacchetto di configurazione contiene i seguenti elementi:

- Un file manifesto
- Un set di modelli di accompagnamento
- Altri file JSON per descrivere e implementare le personalizzazioni dell'ambiente AWS Control Tower

Per impostazione predefinita, il pacchetto di `_custom-control-tower-configuration.zip` configurazione viene caricato in un bucket Amazon S3 con la seguente convenzione di denominazione:

`custom-control-tower-configuration-accountID-region`.

Note

Per impostazione predefinita, cFCT crea un bucket Amazon S3 per archiviare l'origine della pipeline. La maggior parte dei clienti mantiene questa impostazione predefinita. Se disponi di un AWS CodeCommit repository esistente, puoi modificare la posizione di origine nel tuo AWS CodeCommit repository. Per ulteriori informazioni, consulta [Modificare una pipeline CodePipeline](#) nella Guida per l'AWS CodePipeline utente.

Il file `manifest` è un file di testo che descrive le AWS risorse che puoi implementare per personalizzare la tua zona di atterraggio. CodePipeline svolge le seguenti attività:

- estrae il file manifest, il set di modelli che lo accompagna e altri file JSON
- esegue le convalide dei manifest e dei template
- richiama le sezioni del file manifesto cFCT per eseguire fasi specifiche [della pipeline](#).

Quando si aggiorna il pacchetto di configurazione personalizzando il file manifest e rimuovendo il carattere di sottolineatura (`_`) dal nome del file del pacchetto di configurazione, viene avviato automaticamente. AWS CodePipeline

Ricorda il carattere di sottolineatura

Il nome del file del pacchetto di configurazione di esempio inizia con un carattere di sottolineatura (`_`) in modo che non AWS CodePipeline venga attivato automaticamente. Una volta completata la personalizzazione del pacchetto di configurazione, carica il file `custom-control-tower-configuration.zip` senza il carattere di sottolineatura (`_`) per attivare la distribuzione in. AWS CodePipeline

AWS CodePipeline fasi

La pipeline cFCT richiede diverse AWS CodePipeline fasi per implementare e aggiornare l'ambiente AWS Control Tower.

1. Fase di origine

La fase sorgente è la fase iniziale. Il pacchetto di configurazione personalizzato avvia questa fase della pipeline. L'origine AWS CodePipeline può essere un bucket Amazon S3 o un AWS CodeCommit repository, in cui può essere ospitato il pacchetto di configurazione.

2. Fase di costruzione

La fase di compilazione richiede AWS CodeBuild la convalida del contenuto del pacchetto di configurazione. Questi controlli includono il test della sintassi e dello schema del `manifest.yaml` file, insieme a tutti i CloudFormation modelli inclusi nel pacchetto o ospitati in remoto, utilizzando `CloudFormation validate-template cfn_nag`. Se il file manifest e CloudFormation i modelli superano i test, la pipeline passa alla fase successiva. Se i test falliscono, puoi esaminare i CodeBuild log per identificare il problema e modificare il file sorgente di configurazione secondo necessità.

3. Fase di approvazione manuale (opzionale)

La fase di approvazione manuale è facoltativa. Se abiliti questa fase, fornisce un controllo aggiuntivo sulla pipeline di configurazione. Mette in pausa la pipeline durante la distribuzione, fino a quando non viene data l'approvazione. Puoi attivare l'approvazione manuale modificando il parametro `Pipeline Approval Stage` su `Sì` all'avvio dello stack.

4. Fase della politica di controllo del servizio

La fase Service Control Policy richiama la macchina a stati della Service Control Policy (SCP) per chiamare le AWS Organizations API che creano SCP.

5. Fase della politica di controllo delle risorse

La fase Resource Control Policy richiama la macchina a stati RCP (Resource Control Policy) per chiamare le AWS Organizations API che creano RCP.

6. CloudFormation fase delle risorse

La fase CloudFormation delle risorse richiama lo stack set state machine per distribuire le risorse specificate nell'elenco di account o unità organizzative (OU), fornito nel file manifest. La macchina a stati crea le CloudFormation risorse nell'ordine in cui sono specificate nel file manifesto. Per specificare una dipendenza tra le risorse, disponi l'ordine in cui le risorse sono specificate nel file manifesto. L'ordine delle risorse all'interno del file manifesto è l'unico modo per specificare una dipendenza.

Definire una configurazione personalizzata

Definirai la tua configurazione AWS Control Tower personalizzata con il file manifest cFCT, il set di modelli allegato e altri file JSON. Comprimerai questi file in una struttura di cartelle e li inserirai nel bucket Amazon S3 come .zip file, come mostrato nel seguente esempio di codice.

Struttura delle cartelle di configurazione personalizzata

```
- manifest.yaml
- policies/                                [optional]
  - service control policies files (*.json)
- templates/                              [optional]
  - template files for AWS CloudFormation Resources (*.template)
```

L'esempio precedente illustra la struttura di una cartella di configurazione personalizzata. La struttura delle cartelle rimane invariata indipendentemente dal fatto che tu scelga Amazon S3 o un AWS CodeCommit repository come posizione di archiviazione di origine. Se scegli Amazon S3 come storage di origine, comprimi tutte le cartelle e i file in un file e carica solo `custom-control-tower-configuration.zip` il .zip file nel bucket Amazon S3 designato.

Note

Se lo stai utilizzando AWS CodeCommit, inserisci i file nel repository senza comprimerli.

Il file manifesto cFCT

Il file cFCT è un `manifest.yaml` file di testo che descrive le tue AWS risorse. L'esempio seguente mostra la struttura del file manifesto cFct.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources, SCP policies, or RCP policies
...
```

Come mostrato nell'esempio di codice precedente, le prime due righe del file manifesto specificano i valori della regione e le parole chiave della versione. Ecco le definizioni di tali parole chiave.

regione: una stringa di testo per la regione predefinita di AWS Control Tower. Questo valore deve essere un nome di AWS regione valido (ad esempio `us-east-1`, `eu-west-1`, `ap-southeast-1`). La regione principale di AWS Control Tower è l'impostazione predefinita quando si creano risorse AWS Control Tower personalizzate (ad esempio CloudFormation StackSets), a meno che non venga specificata una regione più specifica per le risorse.

```
region: your-home-region
```

version: il numero di versione dello schema manifesto. L'ultima versione supportata è il 15/03/2021.

```
version: 2021-03-15
```

Note

Ti consigliamo vivamente di utilizzare la versione più recente. Per aggiornare le proprietà del manifesto nella versione più recente, fare riferimento a [Aggiornamenti di versione per il manifesto cFCT](#).

La parola chiave successiva mostrata nell'esempio precedente è la parola chiave `resources`. La sezione delle risorse del file manifesto è altamente strutturata. Contiene un elenco dettagliato delle AWS risorse, che verranno distribuite automaticamente dalla pipeline cFCT. Queste descrizioni delle risorse e dei relativi parametri disponibili sono riportate nella sezione successiva.

La sezione delle risorse del file manifesto cFCT

Questo argomento descrive la sezione delle risorse del file manifesto cFct, in cui definirai le risorse necessarie per le tue personalizzazioni. Questa sezione del file manifesto cFCT inizia dalla parola chiave `resources` e continua fino alla fine del file.

La sezione delle risorse del file manifesto specifica gli CloudFormation StackSets, o AWS Organizations SCP e RCP, che cFCT distribuisce automaticamente attraverso la pipeline di codice. Puoi elencare OU, account e regioni per distribuire istanze di stack.

Le istanze Stack vengono distribuite a livello di account anziché a livello di unità organizzativa. Gli SCP e gli RCP vengono implementati a livello di unità organizzativa. Per ulteriori informazioni, consulta [Crea le tue personalizzazioni](#).

Il seguente modello di esempio descrive le possibili voci disponibili per la sezione delle risorse del file manifesto.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set | rcp
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: ${output_ApplicationId}
    regions: #list of strings
      - [String]
```

Il resto di questo argomento fornisce definizioni dettagliate per le parole chiave mostrate nell'esempio di codice precedente.

nome: il nome associato a CloudFormation StackSets.

La stringa fornita assegna un nome più intuitivo per uno stack set.

- Tipo: stringa
- Obbligatorio: sì
- Valori validi: a-z A-Z, 0-9 e un trattino (-). Il nome deve iniziare con un carattere alfabetico.

descrizione: la descrizione della risorsa.

- Tipo: stringa
- Obbligatorio: no

`resource_file`: questo file può essere specificato come posizione relativa al file manifesto, un URI o un URL di Amazon S3 che rimanda a un CloudFormation modello o a una politica di controllo del AWS Organizations servizio in JSON per la creazione di CloudFormation risorse, SCP o RCP.

- Tipo: stringa
- Obbligatorio: sì

1. L'esempio seguente mostra il `resource_file`, fornito come posizione relativa al file di risorse all'interno del pacchetto di configurazione.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. L'esempio seguente mostra il file di risorse fornito come URI Amazon S3

```
resources:
  - name: SecurityRoles
    resource_file: s3://amzn-s3-demo-bucket/[key-name]
```

3. L'esempio seguente mostra il file di risorse fornito come URL HTTPS di Amazon S3

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

Note

Se fornisci un URL Amazon S3, verifica che la policy del bucket consenta l'accesso in lettura per l'account di gestione di AWS Control Tower da cui stai distribuendo cFCT. Se fornisci un URL HTTPS di Amazon S3, verifica che il percorso utilizzi la notazione a punti. Ad esempio, `S3.us-west-1`. cFCT non supporta gli endpoint che contengono un trattino tra S3 e la regione, ad esempio. `S3-us-west-2`

4. L'esempio seguente mostra una policy sui bucket Amazon S3 e un ARN in cui vengono archiviate le risorse.

```
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": {"AWS": "arn:aws:iam::AccountId:root"},  
    "Action": "s3:GetObject",  
    "Resource": "arn:aws:s3:::my-bucket/*"  
  }  
]  
}
```

Sostituirai la *AccountId* variabile mostrata nell'esempio con l'ID dell' AWS account di gestione che sta implementando cFCT. Per altri esempi, consulta gli esempi di policy [Bucket](#) nella Amazon Simple Storage Service User Guide.

parametri: specifica il nome e il valore dei parametri. CloudFormation

- Type MapList:
- Obbligatorio: no

La sezione dei parametri contiene coppie di key/value parametri. Il seguente pseudo modello delinea la sezione dei parametri.

```
parameters:  
  - parameter_key: [String]  
    parameter_value: [String]
```

- parameter_key — La chiave associata al parametro.
 - Tipo: stringa
 - Obbligatorio: Sì (nella proprietà dei parametri)
 - Valori validi: a-z e A-Z 0-9
- parameter_value — Il valore di input associato al parametro.
 - Tipo: stringa
 - Obbligatorio: Sì (nella proprietà dei parametri)

`deploy_method`: il metodo di distribuzione per la distribuzione delle risorse nell'account. Attualmente, `deploy_method` supporta la distribuzione delle risorse utilizzando l'`stack_set` opzione per la distribuzione delle risorse tramite CloudFormation StackSets, l'opzione `scp` se si stanno distribuendo SCP o l'`rcp` opzione se si stanno distribuendo RCP. `rcp`

- Tipo: stringa
- Valori validi: `stack_set` | `scp` | `rcp`
- Obbligatorio: sì

`deployment_targets` — Elenco di account o unità organizzative (OU), in cui cFCT distribuirà le risorse, specificate come `account` o `organizational_units`. CloudFormation

 Note

Se desideri distribuire un SCP o un RCP, l'obiettivo deve essere un'unità organizzativa, non un account.

- Digitare: Elenco di stringhe `account_name` o `account_number` per indicare che questa risorsa verrà distribuita nell'elenco di account specificato o `OU_names` per indicare che questa risorsa verrà distribuita nell'elenco OU specificato.
- Obbligatorio: almeno uno degli `account` o `organizational_units`

- conti:

Digitare: elenco di stringhe `account_name` o `account_number` per indicare che questa risorsa verrà distribuita nell'elenco di account specificato.

- `unità_organizzative`:

Tipo: Elenco di stringhe `OU_names` per indicare che questa risorsa verrà distribuita in un determinato elenco di unità organizzative. Se fornisci un'unità organizzativa che non contiene account e la proprietà degli account non viene aggiunta, cFct crea solo lo stack set.

 Note

L'ID dell'account di gestione dell'organizzazione non è un valore consentito. Per impostazione predefinita, cFCT non supporta la distribuzione di istanze di stack

nell'account di gestione dell'organizzazione. Se hai un caso d'uso speciale, consulta [Root OU](#).

`export_outputs` — Elenco di name/value coppie che indicano le chiavi dei parametri SSM. Queste chiavi dei parametri SSM consentono di memorizzare gli output del modello nell'archivio dei parametri SSM. L'output è destinato alla consultazione da parte di altre risorse, definite in precedenza nel file manifesto.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- Tipo: Elenco di coppie di chiavi con nome e valore. Il nome contiene la name stringa di una chiave di archiviazione dei parametri SSM e il valore contiene la value stringa del parametro.
- Valori validi: qualsiasi stringa o `[$[output_CfnOutput-Logical-ID]]` variabile in cui *CfnOutput-Logical-ID* corrisponde alla variabile di output del modello. Per ulteriori informazioni sulla sezione Output di un CloudFormation modello, vedere [Output](#) nella Guida per l'CloudFormation utente.
- Obbligatorio: no

Ad esempio, il seguente frammento di codice memorizza la variabile di VPCID output del modello nella chiave del parametro SSM denominata. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

Note

Il nome della chiave `export_outputs` può contenere un valore diverso da. output Ad esempio, se il nome è `/org/environment-name`, il valore può essere. `production`

`regioni`: elenco delle regioni in cui cFCT distribuirà le istanze dello CloudFormation stack.

- **Digita:** qualsiasi elenco di nomi di regioni AWS commerciali, per indicare che questa risorsa verrà distribuita nell'elenco delle regioni specificato. Se questa parola chiave non esiste nel file manifesto, le risorse vengono distribuite solo nella regione di origine.
- **Obbligatorio:** no

Unità organizzativa principale

cFCT supporta `Root` come valore per un'unità organizzativa (OU) `organizational_units` nella versione `manifest V2 (15/03/2021)`.

- Se scegli il metodo di distribuzione di `scp orcp`, quando aggiungi `Root` in `inorganizational_units`, AWS Control Tower applica le policy a tutte le unità organizzative incluse nella colonna `Root`. Se scegli il metodo di distribuzione `distack_set`, quando aggiungi `Root` in `inorganizational_units`, cFCT distribuisce gli stack set in tutti gli account sotto `Root` che sono registrati in AWS Control Tower, ad eccezione dell'account di gestione.
- Secondo le best practice di AWS Control Tower, l'account di gestione è destinato esclusivamente alla gestione degli account dei membri e ai fini della fatturazione. Non eseguire carichi di lavoro di produzione nell'account di gestione di AWS Control Tower.

In conformità con le linee guida sulle migliori pratiche, l'implementazione di AWS Control Tower colloca l'account di gestione nell'unità organizzativa principale, in modo che abbia pieno accesso e non esegua risorse aggiuntive. Per questo motivo, il `AWSControlTowerExecution` ruolo non viene distribuito all'account di gestione.

- Ti consigliamo di seguire queste best practice per l'account di gestione. Se hai un caso d'uso specifico che richiede la distribuzione di stackset nell'account di gestione, includi gli account come destinazione di distribuzione e specifica l'account di gestione. Altrimenti, non includere gli account come destinazione di distribuzione. È necessario creare le risorse mancanti, inclusi i ruoli IAM richiesti, nell'account di gestione.

Per distribuire gli stackset nell'account di gestione, includeteli `accounts` come target di distribuzione e specificate l'account di gestione. Altrimenti, non includere gli account come destinazione di distribuzione.

```
---  
region: your-home-region  
version: 2021-03-15
```

```
resources:

  ...truncated...

  deployment_targets:
    organizational_units:
      - Root
```

Note

La funzionalità Root OU è supportata solo nella versione V2 del file manifest (15/03/2021). Se aggiungi Root come unità organizzativa in `organizational_units`, non aggiungere altre unità organizzative.

Unità organizzativa annidata

cFCT supporta l'elenco di una o più unità organizzative annidate sotto la `organizational_units` parola chiave nella versione manifest V2 (2021-03-15).

È necessario un percorso completo (escluso Root) per l'unità organizzativa annidata, utilizzando i due punti come separatore tra le unità organizzative. Per il metodo di distribuzione `scp` o `orcp`, AWS Control Tower distribuisce gli SCP o gli RCP nell'ultima unità organizzativa nel percorso dell'unità organizzativa annidata. Per quanto riguarda il metodo di distribuzione `stack_set`, AWS Control Tower distribuisce gli stack set su tutti gli account dell'ultima unità organizzativa nel percorso dell'unità organizzativa annidata.

Ad esempio, considera il percorso. `OUName1:OUName2:OUName3` L'ultima unità organizzativa del percorso è `OUName3`. cFCT distribuisce gli SCP o gli RCP `OUName3` e impila i set solo su tutti gli account direttamente sotto. `OUName3`

```
---
region: your-home-region
version: 2021-03-15

resources:

  ...truncated...

  deployment_targets:
```

```
organizational_units:
  - OuName1:OuName2:OuName3
```

Note

La funzionalità di unità organizzativa annidata è supportata solo nella versione V2 del file manifest (15/03/2021).

Crea le tue personalizzazioni

Per creare le tue personalizzazioni, puoi modificare il `manifest.yaml` file cFCT aggiungendo o aggiornando le politiche di controllo dei servizi (SCP), le politiche di controllo delle risorse (RCP) e le risorse. CloudFormation Per le risorse che devono essere distribuite, puoi aggiungere o rimuovere account e unità organizzative. È possibile aggiungere o modificare i modelli nelle cartelle dei pacchetti, creare cartelle personalizzate e fare riferimento ai modelli o alle cartelle nel `manifest.yaml` file.

Questa sezione spiega le due parti principali della creazione di personalizzazioni personalizzate:

- come impostare il proprio pacchetto di configurazione per le politiche di controllo del servizio
- come impostare il proprio pacchetto di configurazione per gli AWS CloudFormation stack set

Configura un pacchetto di configurazione per SCP o RCP

Questa sezione spiega come creare un pacchetto di configurazione per le politiche di controllo dei servizi (SCP) o le politiche di controllo delle risorse (RCP). Le due parti principali di questo processo sono (1) preparare il file manifesto cFCT e (2) preparare la struttura delle cartelle.

Passo 1: Modificare il file `manifest.yaml`

Usa il `manifest.yaml` file di esempio come punto di partenza. Inserisci tutte le configurazioni necessarie. Aggiungi i `deployment_targets` dettagli `resource_file` e.

Lo snippet seguente mostra il file manifest predefinito.

```
---
region: us-east-1
```



```
version: 2021-03-15

resources: []
```

Il valore per `region` viene aggiunto automaticamente durante la distribuzione. Deve corrispondere alla regione in cui è stato implementato cFCT. Questa regione deve essere la stessa della regione AWS Control Tower.

Per aggiungere un SCP o RCP personalizzato nella `example-configuration` cartella del pacchetto zip archiviato nel bucket Amazon S3, apri il `example-manifest.yaml` file e inizia a modificarlo.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

...truncated...
```

Lo snippet seguente mostra un esempio di file manifest personalizzato. È possibile aggiungere più di una policy in una singola modifica.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
```

```
deployment_targets:
  organizational_units: #array of strings
    - OUName1
    - OUName2
```

Passaggio 2: creare una struttura di cartelle

Puoi saltare questo passaggio se utilizzi un URL Amazon S3 per il file di risorse e utilizzi parametri con key/value coppie.

È necessario includere una policy SCP o una policy RCP in formato JSON per supportare il manifest, poiché il file manifesto fa riferimento al file JSON. Assicuratevi che i percorsi dei file corrispondano alle informazioni sul percorso fornite nel file manifesto.

- Un file JSON di policy contiene gli SCP o gli RCP da distribuire nelle unità organizzative.

Lo snippet seguente mostra la struttura delle cartelle per il file manifest di esempio.

```
- manifest.yaml
- policies/
  - block-s3-public.json
```

Il frammento seguente è un esempio di file di policy. `block-s3-public.json`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GuardPutAccountPublicAccessBlock",
      "Effect": "Deny",
      "Action": "s3:PutAccountPublicAccessBlock",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Configura un pacchetto di configurazione per CloudFormation StackSets

Questa sezione spiega come impostare un pacchetto di configurazione per CloudFormation StackSets. Le due parti principali di questo processo sono: (1) preparare il file manifest e (2) aggiornare la struttura delle cartelle.

Fase 1: Modificare il file manifest esistente

Aggiungi le nuove CloudFormation StackSets informazioni al file manifesto che hai modificato in precedenza.

Solo per una revisione, il seguente frammento contiene lo stesso file manifest personalizzato mostrato in precedenza per impostare un pacchetto di configurazione per SCP o RCP. Ora puoi modificare ulteriormente questo file, per includere i dettagli sulle tue risorse.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp / rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
      - OUName1
      - OUName2
```

Lo snippet seguente mostra un file manifesto di esempio modificato che contiene i dettagli. `resources` L'ordine di `resources` determina l'ordine di esecuzione per la creazione delle dipendenze. `resources` È possibile modificare il seguente file manifesto di esempio in base ai requisiti aziendali.

```
---
region: your-home-region
version: 2021-03-15

...truncated...
```

```

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: ${output_ApplicationId}
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
    regions:
      - region-name

```

L'esempio seguente mostra che è possibile aggiungere più di una CloudFormation risorsa nel file manifesto.

```

---
region: us-east-1
version: 2021-03-15

```

```
resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp / rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: ${output_TransitGatewayID}
    regions:
      - us-east-1
```

Passaggio 2: aggiornamento della struttura delle cartelle

Quando si aggiorna la struttura delle cartelle, è possibile includere tutti i file CloudFormation modello di supporto e i file di policy SCP o RCP presenti nel file manifest. Verificate che i percorsi dei file corrispondano a quelli forniti nel file manifesto.

- Un file modello contiene le AWS risorse da distribuire nelle unità organizzative e negli account.
- Un file di policy contiene i parametri di input utilizzati nel file modello.

L'esempio seguente mostra la struttura delle cartelle per il file manifesto di esempio creato nel [passaggio 1](#).

```
- manifest.yaml
- policies/
```

```
- block-s3-public.json
- templates/
- transit-gateway.template
```

L'aiutante 'alfred' e il CloudFormation file di parametri

cFct fornisce un meccanismo noto come `alfred` helper per ottenere il valore di una [chiave](#) SSM Parameter Store definita nel modello. CloudFormation Usando l'helper `alfred`, puoi usare i valori memorizzati nell'SSM Parameter Store e senza aggiornare il modello. CloudFormation Per ulteriori informazioni, consulta [Cos'è un modello? CloudFormation](#) nella Guida CloudFormation per l'utente.

Important

L'`alfred` helper ha due limitazioni. I parametri sono disponibili solo nella regione principale dell'account di gestione AWS Control Tower. Come best practice, valuta la possibilità di lavorare con valori che non cambiano da istanza di stack a istanza di stack. Quando l'helper '`alfred`' recupera i parametri, sceglie un'istanza di stack casuale dallo stack set che esporta la variabile.

Esempio

Supponiamo di avere due set di stack. CloudFormation Lo stack set 1 ha un'istanza di stack e viene distribuito su un account in una regione. Crea un Amazon VPC e delle sottoreti in una zona di disponibilità e il valore VPC ID and subnet ID deve essere passato allo stack set 2 come valori dei parametri. Prima che l'VPC ID and subnet ID possa essere passato allo stack set 2, l'VPC ID and subnet ID deve essere archiviato nello stack set 1 utilizzando.

`AWS::SSM::Parameter` Per ulteriori informazioni, consulta [AWS::SSM::Parameter](#) nella Guida per l'utente di CloudFormation .

CloudFormation stack set 1:

Nel frammento seguente, l'helper `alfred` può ottenere il valore per VPC ID and subnet ID dall'archivio dei parametri e passarlo come input alla macchina a stati. StackSet

```
VpcIdParameter:
  Type: AWS::SSM::Parameter
  Properties:
    Name: '/stack_1/vpc/id'
    Description: Contains the VPC id
```

```
Type: String
Value: !Ref MyVpc
```

```
SubnetIdParameter:
  Type: AWS::SSM::Parameter
  Properties:
    Name: '/stack_1/subnet/id'
    Description: Contains the subnet id
    Type: String
    Value: !Ref MySubnet
```

CloudFormation stack set 2:

Lo snippet mostra i parametri specificati nel file CloudFormation stack 2manifest.yaml.

```
parameters:
  - parameter_key: VpcId
    parameter_value: ${alfred_ssm_/stack_1/vpc/id}
  - parameter_key: SubnetId
    parameter_value: ${alfred_ssm_/stack_1/subnet/id}
```

CloudFormation stack set 2.1:

Lo snippet mostra che è possibile elencare alfred_ssm le proprietà per supportare i parametri di tipo. CommaDelimitedList Per ulteriori informazioni, consulta [Parameters](#) nella Guida per l'utente di CloudFormation .

```
parameters:
  - parameter_key: VpcId # Type: String
    parameter_value: ${alfred_ssm_/stack_1/vpc/id'}
  - parameter_key: SubnetId # Type: String
    parameter_value: ${alfred_ssm_/stack_1/subnet/id'}
  - parameter_key: AvailabilityZones # Type: CommaDelimitedList
    parameter_value:
  - "${alfred_ssm_/availability_zone_1}"
  - "${alfred_ssm_/availability_zone_2}"
```

Schema JSON per il pacchetto di personalizzazione

Lo schema JSON per il pacchetto di personalizzazione per cFCT si trova nel repository del [codice sorgente su. GitHub](#) Puoi utilizzare lo schema con molti dei tuoi strumenti di

sviluppo preferiti e potresti trovarlo utile per ridurre gli errori quando crei il tuo file `cFCT.manifest.yaml`.

Aggiornamenti di versione per il manifesto cFCT

Per informazioni sull'ultima versione di Customizations for AWS Control Tower (cFCT), consulta il [CHANGELOG.md file](#) nel repository. GitHub

Warning

La versione 2.2.0 di Customizations for AWS Control Tower (cFCT) ha introdotto uno schema manifesto cFCT (versione 2021-03-15) per l'allineamento con le relative API di servizio. AWS Lo schema manifest consente a un singolo file `manifest.yaml` di gestire le risorse supportate (modelli, SCP e RCP) tramite flussi di lavoro disaccoppiati. CloudFormation DevOps

Consigliamo vivamente di aggiornare lo schema manifesto cFCT dalla versione 2020-01-01 alla versione 2021-03-15 o successiva.

CfCT continua a supportare le versioni 2021-03-15 e 2020-01-01 del file. `manifest.yaml` Non sono necessarie modifiche alla configurazione esistente. Tuttavia, la versione 2020-01-01 è al termine del supporto. Non forniamo più aggiornamenti o aggiungiamo miglioramenti alla versione 2020-01-01. Le funzionalità Root OU e nested OU non sono supportate nella versione 2020-01-01.

Proprietà obsolete nella versione manifest di cFCT 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```


Fasi obbligatorie di aggiornamento di CfCT

Quando si esegue l'aggiornamento alla versione dello schema manifesto CfCT, versione 2021-03-15, ecco le modifiche da apportare per aggiornare i file. Le sezioni successive descrivono le modifiche obbligatorie e consigliate per la transizione.

Politiche delle organizzazioni

1. Sposta gli SCP o gli RCP in `organization_policies` in nuove risorse di proprietà.
2. Cambia la proprietà `policy_file` nella nuova proprietà `resource_file`.
3. Cambia `apply_to_accounts_in_ou` con una nuova proprietà `deployment_targets`. L'elenco delle unità organizzative deve essere definito nella sottoproprietà `organizational_units`. La sottoproprietà `accounts` non è supportata per le politiche delle organizzazioni.
4. Aggiungi una nuova proprietà `deploy_method` con il valore `scp` o `rcp`.

CloudFormation risorse

1. Sposta le CloudFormation risorse in `cloudformation_resources` in nuove risorse di proprietà.
2. Cambia la proprietà `template_file` nella nuova proprietà `resource_file`.
3. Cambia `deploy_to_ou` nella nuova proprietà `deployment_targets`. L'elenco delle unità organizzative deve essere definito nella sottoproprietà `organizational_units`.
4. Modificare `deploy_to_accounts` nella nuova proprietà `deployment_targets`. L'elenco degli account deve essere definito in conti di sottoproprietà.
5. Modificare la proprietà `ssm_parameters` nella nuova proprietà `export_outputs`.

Fasi di aggiornamento CfCT altamente consigliate

CloudFormation parametri

1. Modificare la proprietà `parameter_file` con nuovi parametri di proprietà.
2. Rimuovete il percorso del file nel valore della proprietà `parameter_file`.
3. Copia la chiave e il valore del parametro dal file JSON dei parametri esistente nel nuovo formato per la proprietà `parameters`. Questo ti aiuterà a gestirli nel file manifest.

 Note

La proprietà `parameter_file` è supportata nella versione manifest di cFCT 2021-03-15.

Rete in AWS Control Tower

AWS Control Tower fornisce supporto di base per il networking tramite VPC.

Se la configurazione o le funzionalità predefinite di AWS Control Tower VPC non soddisfano le tue esigenze, puoi utilizzare altri AWS servizi per configurare il tuo VPC. Per ulteriori informazioni su come lavorare con VPC e AWS Control Tower, consulta [Creazione di un'infrastruttura di rete scalabile e sicura. Multi-VPC AWS](#)

AWS Control Tower supporta i protocolli IPv4 e IPv6, tramite indirizzi IP dual-stack. Per ulteriori informazioni, consulta Endpoint e quote di [AWS Control Catalog e endpoint e quote di AWS Control Tower](#). <https://docs.aws.amazon.com/general/latest/gr/controltower.html>

Argomenti correlati

- Per informazioni su come funziona AWS Control Tower quando registri account con VPC esistenti, consulta. [Registra gli account esistenti con i VPC](#)
- Con Account Factory, puoi effettuare il provisioning di account che includono un AWS Control Tower VPC oppure puoi effettuare il provisioning di account senza un VPC. Per informazioni su come eliminare AWS Control Tower VPC o configurare gli account AWS Control Tower senza un VPC, consulta. [Procedura dettagliata: configura AWS Control Tower senza un VPC](#)
- Per informazioni su come modificare le impostazioni degli account per i VPC, consulta la documentazione di [Account Factory](#) sull'aggiornamento di un account.
- Per ulteriori informazioni su come lavorare con reti e VPC in AWS Control Tower, consulta la sezione [sulla](#) rete nella pagina delle informazioni correlate di questa Guida per l'utente.

VPC e AWS Regioni in AWS Control Tower

Come parte standard della creazione dell'account, AWS crea un VPC AWS predefinito in ogni regione, anche nelle regioni che non governi con AWS Control Tower. Questo VPC predefinito non è lo stesso di un VPC creato da AWS Control Tower per un account con provisioning, ma il VPC AWS predefinito in una regione non governata può essere accessibile agli utenti IAM.

Gli amministratori possono abilitare la Region Deny Control, in modo che gli utenti finali non abbiano il permesso di connettersi a un VPC in una regione supportata da AWS Control Tower ma al di fuori delle regioni governate. Per configurare il controllo negato della regione, vai alla pagina delle impostazioni della zona di destinazione e seleziona Modifica impostazioni.

La modalità Region Deny Control blocca le chiamate API alla maggior parte dei servizi non gestiti. Regioni AWS Per ulteriori informazioni, consulta [Negare l'accesso a in AWS base alla richiesta. Regione AWS](#).

Note

Il Region Deny Control potrebbe non impedire agli utenti IAM di connettersi a un VPC AWS predefinito in una regione in cui AWS Control Tower non è supportato.

Facoltativamente, puoi rimuovere i VPC AWS predefiniti nelle regioni non governate. Per elencare i VPC predefiniti in una regione puoi utilizzare un comando CLI simile a questo esempio:

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

Panoramica di AWS Control Tower e VPC

Ecco alcuni dati essenziali sui VPC AWS Control Tower:

- Il VPC creato da AWS Control Tower quando si effettua il provisioning di un account in Account Factory non è lo stesso del AWS VPC predefinito.
- AWS Control Tower elimina automaticamente il VPC predefinito nelle regioni governate selezionate (AWS le regioni che AWS Control Tower governa nella tua landing zone) per gli account che crei dalla console AWS Control Tower. AWS Control Tower non elimina il VPC predefinito negli account esistenti, inclusi gli account forniti nel file `CreateLandingZone` manifest o selezionati dall'AWS organizzazione durante la configurazione della Control Tower.
- A ogni account AWS Control Tower è consentito un VPC creato da AWS Control Tower. Un account può avere AWS VPC aggiuntivi entro il limite dell'account.
- Ogni VPC AWS Control Tower ha tre zone di disponibilità in tutte le regioni ad eccezione della regione Stati Uniti occidentali (California settentrionale) e due zone di disponibilità all'interno. `us-west-1 us-west-1` Per impostazione predefinita, a ogni zona di disponibilità è assegnata una sottorete pubblica e due sottoreti private. Pertanto, nelle regioni ad eccezione degli Stati Uniti occidentali (California settentrionale), ogni VPC AWS Control Tower contiene nove sottoreti per impostazione predefinita, suddivise in tre zone di disponibilità. Negli Stati Uniti occidentali (California settentrionale), sei sottoreti sono suddivise in due zone di disponibilità.
- A ciascuna delle sottoreti del tuo VPC AWS Control Tower viene assegnato un intervallo univoco, di uguali dimensioni.

- Il numero di sottoreti in un VPC è configurabile. Per ulteriori informazioni su come modificare la configurazione delle sottoreti del VPC, consulta [l'argomento Account Factory](#).
- Poiché gli indirizzi IP non si sovrappongono, le sei o nove sottoreti all'interno del tuo VPC AWS Control Tower possono comunicare tra loro senza restrizioni.

Quando si lavora con VPC, AWS Control Tower non fa distinzioni a livello di regione. Ogni sottorete viene allocata secondo l'esatto intervallo CIDR specificato. Le sottoreti VPC possono esistere in qualsiasi regione.

Note

Gestisci i costi del VPC

Se imposti la configurazione VPC di Account Factory in modo che le sottoreti pubbliche siano abilitate durante il provisioning di un nuovo account, Account Factory configura VPC per creare un gateway NAT. Ti verrà addebitato l'utilizzo da parte di Amazon VPC.

VPC e impostazioni di controllo

Se esegui il provisioning di account Account Factory con le impostazioni di accesso a Internet VPC abilitate, tale impostazione Account Factory ha la precedenza sul controllo Impedisci l'[accesso a Internet per un'istanza Amazon VPC gestita](#) da un cliente. Per evitare di abilitare l'accesso a Internet per gli account appena assegnati, è necessario modificare l'impostazione in Account Factory. Per ulteriori informazioni, consulta [Procedura dettagliata: Configurazione di AWS Control Tower senza un VPC](#).

CIDR e peering per VPC e AWS Control Tower

Questa sezione è destinata principalmente agli amministratori di rete. L'amministratore di rete della tua azienda di solito è la persona che seleziona l'intervallo CIDR complessivo per la tua organizzazione AWS Control Tower. L'amministratore di rete alloca quindi le sottoreti a partire da tale intervallo per scopi specifici.

Quando scegli un intervallo CIDR per il tuo VPC, AWS Control Tower convalida gli intervalli di indirizzi IP in base alla specifica RFC 1918. Account Factory consente un blocco CIDR fino /16 a intervalli di:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10(solo se il tuo provider Internet consente l'utilizzo di questo intervallo)

Il delimitatore /16 consente fino a 65.536 indirizzi IP distinti.

È possibile assegnare qualsiasi indirizzo IP valido dai seguenti intervalli:

- 10.0.x.x to 10.255.x.x
- 172.16.x.x – 172.31.x.x
- 192.168.0.0 – 192.168.255.255 (nessun IP al di fuori dell'intervallo 192.168)

Se l'intervallo specificato non rientra in questi valori, AWS Control Tower fornisce un messaggio di errore.

L'intervallo CIDR predefinito è 172.31.0.0/16.

Quando AWS Control Tower crea un VPC utilizzando l'intervallo CIDR selezionato, assegna lo stesso intervallo CIDR a ogni VPC per ogni account creato all'interno dell'unità organizzativa (OU). A causa della sovrapposizione predefinita degli indirizzi IP, questa implementazione inizialmente non consente il peering tra nessuno dei tuoi VPC AWS Control Tower nell'unità organizzativa.

Sottoreti

All'interno di ogni VPC, AWS Control Tower divide l'intervallo CIDR specificato in modo uniforme in nove sottoreti (tranne negli Stati Uniti occidentali (California settentrionale), dove è composto da sei sottoreti). Nessuna delle sottoreti all'interno di un VPC si sovrappone. Pertanto, tutti possono comunicare tra loro, all'interno del VPC.

In sintesi, per impostazione predefinita, la comunicazione tra sottoreti all'interno del VPC è illimitata. La best practice per controllare la comunicazione tra le sottoreti VPC, se necessario, è quella di configurare liste di controllo degli accessi con regole che definiscono il flusso di traffico consentito. Per il controllo del traffico tra istanze specifiche, utilizza i gruppi di sicurezza. Per ulteriori informazioni sulla configurazione di gruppi di sicurezza e firewall in AWS Control Tower, consulta [Walkthrough: Configurare i gruppi di sicurezza in AWS Control Tower With Firewall Manager AWS](#).

Peering

AWS Control Tower non limita il VPC-to-VPC peering per la comunicazione tra più VPC. Tuttavia, per impostazione predefinita, tutti i VPC AWS Control Tower hanno lo stesso intervallo CIDR predefinito. Per supportare il peering, è possibile modificare l'intervallo CIDR nelle impostazioni di Account Factory in modo che gli indirizzi IP non si sovrappongano.

Se modifichi l'intervallo CIDR nelle impostazioni di Account Factory, a tutti i nuovi account che vengono successivamente creati da AWS Control Tower (utilizzando Account Factory) viene assegnato il nuovo intervallo CIDR. I vecchi account non vengono aggiornati. Ad esempio, è possibile creare un account, quindi modificare l'intervallo CIDR e creare un nuovo account e i VPC allocati a questi due account possono essere collegati in peering. Il peering è possibile perché i relativi intervalli di indirizzi IP non sono identici.

Accedi ad AWS Control Tower utilizzando un endpoint di interfaccia (AWS PrivateLink)

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e AWS Control Tower. Puoi accedere ad AWS Control Tower come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere ad AWS Control Tower.

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. Si tratta di interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato ad AWS Control Tower.

Per ulteriori informazioni, consulta [Access Servizi AWS through AWS PrivateLink](#) nella Guida. AWS PrivateLink

Considerazioni per AWS Control Tower

Prima di configurare un endpoint di interfaccia per AWS Control Tower, consulta [le considerazioni contenute](#) nella Guida. AWS PrivateLink

AWS Control Tower supporta l'esecuzione di chiamate a tutte le azioni API tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per AWS Control Tower

Puoi creare un endpoint di interfaccia per AWS Control Tower utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per AWS Control Tower utilizzando i seguenti nomi di servizio:

```
com.amazonaws.region.controltower
com.amazonaws.region.controltower-fips
```

Se abiliti il DNS privato per l'endpoint di interfaccia, puoi effettuare richieste API ad AWS Control Tower utilizzando il nome DNS regionale predefinito. Ad esempio, `controltower.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita sugli endpoint consente l'accesso completo ad AWS Control Tower tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito ad AWS Control Tower dal tuo VPC, allega una policy personalizzata sugli endpoint all'endpoint dell'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 la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Esempio: policy sugli endpoint VPC per le azioni di AWS Control Tower

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando colleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni AWS Control Tower elencate per tutti i principali su tutte le risorse.

```
{
  "Statement": [
```



```
{
  "Principal": "*",
  "Effect": "Allow",
  "Action": [
    "controltower:ListEnabledControls",
    "controltower:ListLandingZones"
  ],
  "Resource": "*"
}
```

 Note

Per un elenco completo delle operazioni API di AWS Control Tower, consulta l'[AWS Control Tower API Reference](#).

Ruoli e autorizzazioni correlati

AWS Control Tower utilizza i ruoli IAM per aiutare a gestire l'accesso alle risorse.

Per informazioni generali sui ruoli, consulta [Gruppi di utenti, ruoli e set di autorizzazioni](#).

Informazioni sulle autorizzazioni

- Per informazioni sui gruppi IAM e le relative autorizzazioni in AWS Control Tower, consulta [IAM Identity Center groups for AWS Control Tower](#).
- Per informazioni sulle autorizzazioni necessarie per effettuare il provisioning degli account, consulta [Autorizzazioni richieste per](#) gli account.
- Per informazioni sulle autorizzazioni della console richieste per AWS Control Tower, consulta [Autorizzazioni richieste per utilizzare la console AWS Control Tower](#).

Informazioni sui ruoli

- Per informazioni su come creare un ruolo, incluse le autorizzazioni progettate per l'accesso programmatico, consulta [Creare ruoli e assegnare autorizzazioni e Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower](#).
- Per informazioni sugli altri ruoli utilizzati da AWS Control Tower per gestire gli account, consulta [Using identity based policy \(IAM policies\) per AWS Control Tower](#) e [Managed policies for AWS Control Tower](#).
- Per informazioni su AWS Control Tower e sui AWS Config ruoli, consulta [AWS Control Tower ConfigRecorderRole](#).
- Per informazioni sui ruoli utilizzati da AWS Control Tower per aggregare AWS Config le informazioni per i tuoi account, consulta [Come AWS Control Tower aggrega AWS Config le regole nelle unità organizzative e negli account non gestiti](#).
- [Per informazioni su come proteggere le risorse durante l'assegnazione di ruoli e autorizzazioni, consulta Condizioni opzionali per le relazioni di fiducia tra ruoli, Configurazione facoltativa delle AWS KMSchiavi e Prevenzione dell'impersonificazione tra servizi](#).
- Per informazioni specifiche sul provisioning automatico degli account in AWS Control Tower con ruoli IAM, consulta [Automated Account Provisioning with IAM](#) Roles.
- Per visualizzare la politica che protegge l'argomento AWS Config SNS, consulta l'argomento [La politica sull'argomento AWS Config SNS](#).

In che modo AWS Control Tower funziona con i ruoli per creare e gestire account

In generale, i ruoli fanno parte della gestione delle identità e degli accessi (IAM) in AWS. Per informazioni generali su IAM e i ruoli in AWS, consulta [l'argomento sui ruoli IAM nella Guida per l'utente AWS IAM](#).

Ruoli e creazione di account

AWS Control Tower crea l'account di un cliente chiamando l'CreateAccountAPI di AWS Organizations. Quando AWS Organizations crea questo account, crea un ruolo all'interno di quell'account, che AWS Control Tower nomina passando un parametro all'API. Il nome del ruolo è `AWSControlTowerExecution`.

AWS Control Tower assume il `AWSControlTowerExecution` ruolo di tutti gli account creati da Account Factory. Utilizzando questo ruolo, AWS Control Tower definisce le linee di base dell'account e applica i controlli obbligatori (e tutti gli altri abilitati), il che comporta la creazione di altri ruoli. Questi ruoli a loro volta vengono utilizzati da altri servizi, come AWS Config

Note

Per basare un account è necessario impostare le sue risorse, che includono i [modelli di Account Factory](#), a volte denominati blueprint, e i controlli. Il processo di baselining imposta anche i ruoli centralizzati di registrazione e controllo di sicurezza sull'account, come parte della distribuzione dei modelli. Le linee di base di AWS Control Tower sono contenute nei ruoli che applichi a ogni account registrato.

Per ulteriori informazioni su account e risorse, consulta. [Informazioni Account AWS in AWS Control Tower](#)

Il `AWSControlTowerExecution` ruolo, spiegato

Il ruolo `AWSControlTowerExecution` deve essere presente in tutti gli account registrati. Consente ad AWS Control Tower di gestire i tuoi account individuali e di riportare informazioni su di essi agli account Audit e Log Archive.

Il `AWSControlTowerExecution` ruolo può essere aggiunto a un account in diversi modi, come segue:

- Per gli account nell'unità organizzativa di sicurezza (a volte chiamati account core), AWS Control Tower crea il ruolo al momento della configurazione iniziale di AWS Control Tower.
- Per un account Account Factory creato tramite la console AWS Control Tower, AWS Control Tower crea questo ruolo al momento della creazione dell'account.
- Per la registrazione di un singolo account, chiediamo ai clienti di creare manualmente il ruolo e quindi registrare l'account in AWS Control Tower.
- Quando si estende la governance a un'unità organizzativa, AWS Control Tower utilizza la `StackSet-AWSCoontrolTowerExecutionRole` per creare il ruolo in tutti gli account di quell'unità organizzativa.

Note

Quando annulli la registrazione di un account, AWS Control Tower rimuove il `AWSCoontrolTowerExecution` ruolo, indipendentemente dal fatto che sia stato creato manualmente o dalla stessa AWS Control Tower.

Scopo del ruolo: `AWSCoontrolTowerExecution`

- `AWSCoontrolTowerExecution` consente di creare e registrare account, automaticamente, con script e funzioni Lambda.
- `AWSCoontrolTowerExecution` consente di configurare la registrazione delle organizzazioni, in modo che tutti i registri di ogni account vengano inviati all'account di registrazione.
- `AWSCoontrolTowerExecution` consente di registrare un account individuale in AWS Control Tower. Innanzitutto, devi aggiungere il `AWSCoontrolTowerExecution` ruolo a quell'account. Per istruzioni su come aggiungere il ruolo, consulta [Aggiungi manualmente il ruolo IAM richiesto a un ruolo IAM esistente Account AWS e iscrivilo](#).

Come funziona il `AWSCoontrolTowerExecution` ruolo con le unità organizzative:

Il `AWSCoontrolTowerExecution` ruolo garantisce che i controlli AWS Control Tower selezionati si applichino automaticamente a ogni singolo account, in ogni unità organizzativa, nell'organizzazione e a ogni nuovo account creato in AWS Control Tower. Di conseguenza:

- [Puoi fornire report di conformità e sicurezza più facilmente, in base alle funzionalità di audit e registrazione incorporate nei controlli di AWS Control Tower.](#)

- I team di sicurezza e conformità possono verificare che tutti i requisiti siano soddisfatti e che non si sia verificata alcuna deriva organizzativa.

Per ulteriori informazioni sulla deriva, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

In sintesi, il ruolo `AWSControlTowerExecution` e i relativi criteri associati consentono un controllo flessibile della sicurezza e della conformità nell'intera organizzazione. Pertanto, è meno probabile che si verifichino violazioni della sicurezza o del protocollo.

Condizioni opzionali per il ruolo, le relazioni di fiducia

Per aggiungere ulteriori livelli di sicurezza al tuo ambiente AWS Control Tower, puoi imporre condizioni nelle policy di fiducia dei ruoli, per limitare gli account e le risorse che interagiscono con determinati ruoli in AWS Control Tower. Ad esempio, puoi limitare ulteriormente l'accesso al `AWSControlTowerAdmin` ruolo, perché consente ampie autorizzazioni di accesso.

Per impedire a un autore di minacce di accedere alle tue risorse, modifica manualmente la policy di fiducia di AWS Control Tower aggiungendone almeno una `aws:SourceArn` o in base a `aws:SourceAccount` determinate condizioni all'informativa sulla policy. Come ulteriore best practice di sicurezza, puoi aggiungere la `aws:SourceArn` condizione, perché è più `aws:SourceAccount` specifica della limitazione dell'accesso a un account specifico e a una risorsa specifica.

Se non conosci l'ARN completo della risorsa o se stai specificando più risorse, puoi utilizzare la `aws:SourceArn` condizione con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:controltower:*:123456789012:*` funziona se non desideri specificare una regione.

L'esempio seguente dimostra l'uso della condizione `aws:SourceArn` IAM con le policy di fiducia dei ruoli IAM. Aggiungi la condizione nella tua relazione di fiducia per il `AWSControlTowerAdmin` ruolo, perché il responsabile del servizio AWS Control Tower interagisce con esso.

Come mostrato nell'esempio, l'ARN di origine ha il formato:

```
arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:
```

Sostituisci le stringhe `${HOME_REGION}` `${CUSTOMER_AWSACCOUNT_id}` con la tua regione di residenza e l'ID dell'account chiamante.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

Nell'esempio, l'ARN di origine designato come `arn:aws:controltower:us-west-2:012345678901:*` è l'unico ARN autorizzato a eseguire l'azione `sts:AssumeRole`. In altre parole, solo gli utenti che possono accedere all'ID dell'account `012345678901`, nella `us-west-2` regione, possono eseguire azioni che richiedono questo ruolo specifico e una relazione di fiducia per il servizio AWS Control Tower, designato come `controltower.amazonaws.com`.

Il prossimo esempio mostra le `aws:SourceArn` condizioni `aws:SourceAccount` e applicate alla policy di fiducia dei ruoli.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
```

```
        "controltower.amazonaws.com"
    ],
    },
    "Action": "sts:AssumeRole",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "012345678901"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
    }
}
]
```

L'esempio illustra l'istruzione `aws:SourceArn` condizionale, con un'istruzione di `aws:SourceAccount` condizione aggiunta. Per ulteriori informazioni, consulta [Impedisci l'impersonificazione tra servizi](#).

Per informazioni generali sulle politiche di autorizzazione in AWS Control Tower, consulta [Gestisci l'accesso alle risorse](#).

Raccomandazioni:

Ti consigliamo di aggiungere condizioni ai ruoli creati da AWS Control Tower, poiché tali ruoli vengono assunti direttamente da altri servizi AWS. Per ulteriori informazioni, consulta l'esempio di `AWSControlTowerAdmin`, mostrato in precedenza in questa sezione. Per il ruolo di AWS Config registratore, consigliamo di aggiungere la `aws:SourceArn` condizione, specificando l'ARN del registratore Config come ARN di origine consentito.

Per ruoli simili `AWSControlTowerExecution` [altri ruoli programmatici che possono essere assunti](#) dall'account AWS Control Tower Audit in tutti gli account gestiti, ti consigliamo di aggiungere la `aws:PrincipalOrgID` condizione alla policy di fiducia per questi ruoli, che verifica che il principale che accede alla risorsa appartenga a un account dell'organizzazione corretta AWS. Non aggiungere l'istruzione `aws:SourceArn` condizionale, perché non funzionerà come previsto.

 Note

In caso di deriva, è possibile che un ruolo di AWS Control Tower venga ripristinato in determinate circostanze. Si consiglia di ricontrollare periodicamente i ruoli, se li hai personalizzati.

Come si aggrega AWS Control Tower AWS Config regole nelle unità organizzative e negli account non gestiti

- L'account di gestione AWS Control Tower crea un aggregatore a livello di organizzazione, che aiuta a rilevare AWS Config le regole esterne, in modo che AWS Control Tower non debba accedere agli account non gestiti. La console AWS Control Tower mostra quante AWS Config regole create esternamente hai per un determinato account. È possibile visualizzare i dettagli su tali regole esterne nella scheda External Config Rule Compliance della pagina dei dettagli dell'account.
- Per creare l'aggregatore, AWS Control Tower aggiunge un ruolo con le autorizzazioni necessarie per descrivere un'organizzazione ed elencare gli account al suo interno. Il `AWSControlTowerConfigAggregatorRoleForOrganizations` ruolo richiede la policy `AWSConfigRoleForOrganizations` gestita e una relazione di fiducia con `config.amazonaws.com`

 Note

I clienti che utilizzano la versione 4.0 della landing zone non avranno bisogno di questo ruolo perché AWS Control Tower è migrata dall'aggregatore di configurazione esistente a livello di organizzazione all'aggregatore di configurazione collegato al servizio

 Note

Quando abiliti l'accesso affidabile all'organizzazione che contiene la tua landing zone, AWS Control Tower può creare ruoli, gestire risorse e leggere dati per tutti gli account dell'organizzazione. Tramite un accesso affidabile, qualsiasi account o unità organizzativa

dell'organizzazione è disponibile per AWS Control Tower, indipendentemente dal fatto che sia registrato e registrato, sia che non sia registrato e non registrato.

Ecco la policy IAM (artifact JSON) allegata al ruolo:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Ecco la relazione di fiducia `AWSCloudControlTowerConfigAggregatorRoleForOrganizations`:

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

Per distribuire questa funzionalità nell'account di gestione, vengono aggiunte le seguenti autorizzazioni nella politica gestita `AWSControlTowerServiceRolePolicy`, utilizzata dal `AWSControlTowerAdmin` ruolo al momento della creazione dell'AWS Config aggregatore:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:PutConfigurationAggregator",
        "config>DeleteConfigurationAggregator",
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:role/service-role/AWSControlTowerConfigAggregatorRoleForOrganizations",
        "arn:aws:config:us-east-1:123456789012:config-aggregator/"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*"
    }
  ]
}
```

Nuove risorse create: `AWSCONFIG:PutConfigurationAggregatorRoleForOrganizations` `aws-controltower-ConfigAggregatorForOrganizations`

Quando sei pronto, puoi registrare gli account singolarmente o registrarli come gruppo registrando un'unità organizzativa. Quando registri un account, se crei una regola in AWS Config, AWS Control Tower rileva la nuova regola. L'aggregatore mostra il numero di regole esterne e fornisce un collegamento alla AWS Config console in cui puoi visualizzare i dettagli di ciascuna regola esterna per il tuo account. Utilizza le informazioni nella AWS Config console e nella console AWS Control Tower per determinare se hai abilitato i controlli appropriati per l'account.

Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower

Puoi accedere all'account di audit e assumere il ruolo di esaminare altri account in modo programmatico. L'account di audit non consente di accedere manualmente ad altri account.

L'account di controllo consente l'accesso programmatico ad altri account, tramite alcuni ruoli concessi solo alle funzioni AWS Lambda. Per motivi di sicurezza, questi ruoli intrattengono rapporti di fiducia con altri ruoli, il che significa che le condizioni in base alle quali i ruoli possono essere utilizzati sono rigorosamente definite.

Lo stack AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` crea questi ruoli IAM esclusivamente programmatici e multiaccount in ogni account gestito, incluso l'account Config aggregator (precedentemente l'account di audit). L'account di aggregazione Config assume i seguenti ruoli di esecuzione per accedere ad altri account a livello di codice:

- `aws-controltower- AdministratorExecutionRole`
- `aws-controltower- ReadOnlyExecutionRole`

Lo stack AWS Control Tower `StackSet-AWSControlTowerSecurityResources` crea questi ruoli IAM solo programmatici e multiaccount nell'account di audit:

- `aws-controltower- AuditAdministratorRole`
- `aws-controltower- AuditReadOnlyRole`

`ReadOnlyExecutionRole`: Tieni presente che questo ruolo consente all'account di controllo di leggere gli oggetti nei bucket Amazon S3 in tutta l'organizzazione (a differenza della `SecurityAudit` policy, che consente solo l'accesso ai metadati).

`aws-controltower- AdministratorExecutionRole`

- Dispone delle autorizzazioni di amministratore
- Non può essere assunto dalla console
- Può essere assunto solo da un ruolo nell'account di controllo: il `aws-controltower- AuditAdministratorRole`

Il seguente artefatto mostra la relazione di fiducia per `aws-controltower-AdministratorExecutionRole`. Il numero segnaposto `012345678901` verrà sostituito dal `Audit_acct_ID` numero del tuo account di verifica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

`aws-controltower-: AuditAdministratorRole`

- Può essere assunto solo dal servizio AWS Lambda
- È autorizzato a eseguire operazioni di lettura (Get) e scrittura (Put) su oggetti Amazon S3 con nomi che iniziano con la stringa `log`

Politiche allegate:

1. `AWSLambdaExecute`— politica AWS gestita
2. `AssumeRole-aws-controltower-AuditAdministratorRole`— policy in linea: creata da AWS Control Tower, segue l'artefatto.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
```

```

    "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
  ],
  "Effect": "Allow"
}
]
}

```

Il seguente artefatto mostra la relazione di fiducia per: `aws-controltower-AuditAdministratorRole`

```

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

```

`aws-controltower-: ReadOnlyExecutionRole`

- Non può essere assunto dalla console
- Può essere assunto solo da un altro ruolo nell'account di controllo: il `AuditReadOnlyRole`

Il seguente artefatto mostra la relazione di fiducia per: `aws-controltower-ReadOnlyExecutionRole` Il numero segnaposto `012345678901` verrà sostituito dal `Audit_acct_ID` numero del tuo account di verifica.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },

```

```
    "Action": "sts:AssumeRole"
  }
]
}
```

aws-controltower-: AuditReadOnlyRole

- Può essere assunto solo dal servizio AWS Lambda
- È autorizzato a eseguire operazioni di lettura (Get) e scrittura (Put) su oggetti Amazon S3 con nomi che iniziano con la stringa log

Politiche allegate:

1. AWSLambdaExecute— politica AWS gestita
2. AssumeRole-aws-controltower-AuditReadOnlyRole— policy in linea: creata da AWS Control Tower, segue l'artefatto.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Il seguente artefatto mostra la relazione di fiducia per: aws-controltower-AuditReadOnlyRole

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "lambda.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
]
```

Effettuazione del provisioning automatico degli account con ruoli IAM

Per configurare gli account Account Factory in modo più automatizzato, puoi creare funzioni Lambda nell'account di gestione AWS Control Tower, che [assume il `AWSControlTowerExecution` ruolo](#) nell'account membro. Quindi, utilizzando il ruolo, l'account di gestione esegue i passaggi di configurazione desiderati in ciascun account membro.

Se esegui il provisioning degli account utilizzando le funzioni Lambda, l'identità che eseguirà questo lavoro deve avere la seguente politica di autorizzazioni IAM, oltre a `AWSServiceCatalogEndUserFullAccess`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSControlTowerAccountFactoryAccess",
      "Effect": "Allow",
      "Action": [
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:AssociateProfile",
        "sso:CreateApplicationInstance",
        "sso:GetSSOStatus",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:GetApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:ListPermissionSets",
        "sso:GetPermissionSet",
        "sso:ListProfileAssociations",

```

```
        "sso-directory:ListMembersInGroup",
        "sso-directory:AddMemberToGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeGroups",
        "sso-directory:DescribeDirectory",
        "sso-directory:GetUserPoolInfo",
        "controltower:CreateManagedAccount",
        "controltower:DescribeManagedAccount",
        "controltower:DeregisterManagedAccount",
        "s3:GetObject",
        "organizations:describeOrganization",
        "sso:DescribeRegisteredRegions"
    ],
    "Resource": "*"
}
]
```


Risorse in AWS Control Tower

- Per informazioni generali sulla proprietà delle risorse in AWS Control Tower, consulta [Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#).
- Per informazioni sulle risorse che AWS Control Tower crea negli account condivisi, consulta [Account di integrazione dei servizi](#).
- Per informazioni sulle risorse che AWS Control Tower crea quando effettua il provisioning di un account tramite Account Factory, consulta [Considerazioni sulle risorse per Account Factory](#).
- Per visualizzare i dettagli sui tipi di AWS risorse definiti da AWS Control Tower, da utilizzare con [le API AWS Control Tower](#), consulta il [riferimento al tipo di risorsa AWS Control Tower](#) nella Guida per l'AWS CloudFormation utente.

In che modo AWS Le regioni funzionano con AWS Control Tower

AWS Control Tower è supportato nelle seguenti AWS regioni:

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (Oregon)
- Canada (Centrale)
- Asia Pacifico (Sydney)
- Asia Pacifico (Singapore)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (London)
- Europa (Stoccolma)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seul)
- Asia Pacifico (Tokyo)
- Europa (Parigi)
- Sud America (San Paolo)
- Stati Uniti occidentali (California settentrionale)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Osaka)
- Europa (Milano)
- Africa (Città del Capo)
- Medio Oriente (Bahrein)
- Israele (Tel Aviv)
- Medio Oriente (Emirati Arabi Uniti)
- Europa (Spagna)

- Asia Pacifico (Hyderabad)
- Europa (Zurigo)
- Asia Pacifico (Melbourne)
- Canada occidentale (Calgary)
- Malesia (Kuala Lumpur)
- Asia Pacifico (Thailandia)
- Messico (centrale)
- Asia Pacifico (Taipei)

Informazioni sulla tua regione

Quando crei una zona di atterraggio, la regione utilizzata per accedere alla console di AWS gestione diventa la tua AWS regione di residenza per AWS Control Tower. Durante il processo di creazione, alcune risorse vengono fornite nella regione di origine. Le altre risorse, come le unità organizzative e AWS gli account, sono globali.

Dopo aver selezionato una regione di origine, non puoi modificarla.

Controlli e regioni

Attualmente, tutti i controlli preventivi funzionano a livello globale. I controlli investigativi e proattivi, tuttavia, funzionano solo nelle regioni in cui è supportato AWS Control Tower. Per ulteriori informazioni sul comportamento dei controlli quando si attiva AWS Control Tower in una nuova regione, consulta. [Configura le tue regioni AWS Control Tower](#)

Configura le tue regioni AWS Control Tower

Questa sezione descrive il comportamento che puoi aspettarti quando estendi la zona di destinazione di AWS Control Tower in una nuova AWS regione o rimuovi una regione dalla configurazione della zona di destinazione. In genere, questa azione viene eseguita tramite la funzione Update della console AWS Control Tower.

Note

Ti consigliamo di evitare di espandere la zona di destinazione di AWS Control Tower in AWS regioni in cui non è necessario l'esecuzione dei carichi di lavoro. La disattivazione di una

regione non impedisce di distribuire risorse in quella regione, ma tali risorse rimarranno al di fuori della governance di AWS Control Tower.

Durante la configurazione di una nuova regione, AWS Control Tower aggiorna la zona di atterraggio, vale a dire che è la base della zona di atterraggio:

- operare attivamente in tutte le regioni appena selezionate e
- cessare di governare le risorse nelle Regioni deselezionate.

I singoli account all'interno delle unità organizzative (OU) gestiti da AWS Control Tower non vengono aggiornati nell'ambito di questo processo di aggiornamento della zona di destinazione. Pertanto, è necessario aggiornare gli account registrando nuovamente le unità organizzative.

Quando configuri le tue regioni AWS Control Tower, tieni presente i seguenti consigli e limitazioni:

- Seleziona le regioni in cui intendi ospitare AWS risorse o carichi di lavoro.
- La disattivazione di una regione non impedisce di distribuire risorse in quella regione, ma tali risorse rimarranno al di fuori della governance di AWS Control Tower.

Quando configuri la tua zona di destinazione per nuove regioni, i controlli investigativi di AWS Control Tower rispettano le seguenti regole:

- Ciò che esiste rimane uguale. Il comportamento di controllo, investigativo e preventivo, è invariato per gli account esistenti, nelle unità organizzative esistenti, nelle regioni esistenti.
- Non puoi applicare nuovi controlli investigativi alle unità organizzative esistenti contenenti account non aggiornati. Dopo aver configurato la zona di atterraggio di AWS Control Tower in una nuova regione (aggiornando la zona di atterraggio), devi aggiornare gli account esistenti nelle unità organizzative esistenti prima di poter abilitare nuovi controlli investigativi su tali unità organizzative e account.
- I controlli investigativi esistenti iniziano a funzionare nelle regioni appena configurate non appena aggiorni gli account. Quando aggiorni la zona di destinazione di AWS Control Tower per configurare nuove regioni e quindi aggiorni un account, i controlli detective già abilitati nell'unità organizzativa inizieranno a funzionare su quell'account nelle regioni appena configurate.

Configura le regioni AWS Control Tower

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>
2. Nel menu di navigazione nel riquadro sinistro, seleziona Impostazioni della zona di destinazione.
3. Nella pagina delle impostazioni della zona di destinazione, nella sezione Dettagli, scegli il pulsante Modifica impostazioni in alto a destra. Verrai indirizzato al flusso di lavoro per l'aggiornamento della zona di atterraggio.
4. In Regioni governate aggiuntive, cerca le regioni che vuoi governare (o smettere di governare).
5. Seleziona la casella di controllo per ogni regione aggiuntiva da governare. Deseleziona la casella di controllo per ogni regione da cui stai rimuovendo la governance.

Note

Se scegli di non governare una regione, puoi comunque distribuire risorse in quella regione, ma tali risorse rimarranno al di fuori della governance di AWS Control Tower.

6. Completa il resto del flusso di lavoro, quindi scegli Update landing zone.
7. Una volta completata la configurazione della zona di atterraggio, Re-register le unità organizzative per aggiornare gli account nelle nuove regioni. Per ulteriori informazioni, consulta [Quando aggiornare le unità organizzative e gli account AWS Control Tower](#).

Un metodo alternativo per il provisioning o l'aggiornamento dei singoli account dopo la configurazione di nuove regioni consiste nell'utilizzare [il framework API di Service Catalog](#) e AWS CLI [aggiornare](#) gli account in un processo batch. Per ulteriori informazioni, consulta [Fornisci e aggiorna gli account utilizzando l'automazione](#).

Evita una governance mista durante la configurazione delle regioni

È importante aggiornare tutti gli account in un'unità organizzativa dopo aver esteso la governance di AWS Control Tower a una nuova Regione AWS unità organizzativa e dopo aver rimosso la governance di AWS Control Tower da una regione.

La governance mista è una situazione indesiderabile che può verificarsi se i controlli che governano un'unità organizzativa non corrispondono completamente ai controlli che governano ciascun account all'interno di un'unità organizzativa. La governance mista si verifica in un'unità organizzativa se gli

account non vengono aggiornati dopo che AWS Control Tower ha esteso la governance a una nuova Regione AWS o la rimuove.

In questa situazione, ad alcuni account all'interno di un'unità organizzativa possono essere applicati controlli diversi in diverse regioni, rispetto ad altri account dell'unità organizzativa o rispetto alla posizione generale di governance della zona di atterraggio.

In un'unità organizzativa con governance mista, se si effettua il provisioning di un nuovo account, tale nuovo account riceve la stessa posizione di governance per regione e unità organizzativa (aggiornata) della zona di atterraggio. Tuttavia, gli account esistenti non ancora aggiornati non ricevono la posizione di governance della regione aggiornata.

In generale, una governance mista può creare indicatori di stato contraddittori o imprecisi nella console AWS Control Tower. Ad esempio, durante la governance mista, le regioni opt-in vengono visualizzate con lo stato Non governato, nelle unità organizzative registrate, per gli account che non sono ancora stati aggiornati.

Note

AWS Control Tower non consente l'abilitazione dei controlli durante uno stato di governance mista.

Comportamento dei controlli durante la governance mista

- Durante la governance mista, AWS Control Tower non può distribuire in modo coerente controlli basati su AWS Config regole (ovvero controlli investigativi) in regioni che l'unità organizzativa già indica come governate, perché alcuni account dell'unità organizzativa non sono stati aggiornati. Potresti ricevere un `FAILED_TO_ENABLE` messaggio di errore.
- Durante la governance mista, se estendi la governance della zona di atterraggio a una regione con accesso facoltativo mentre un account dell'unità organizzativa non è ancora stato aggiornato, l'operazione `EnableControl` API sull'unità organizzativa fallisce per i controlli investigativi e proattivi. Riceverai un messaggio `FAILED_TO_ENABLE` di errore, poiché gli account membri non aggiornati all'interno dell'OU non sono ancora stati attivati in quelle regioni.
- Durante la governance mista, i controlli che fanno parte dello Service-managed standard Security Hub CSPM: AWS Control Tower non possono segnalare la conformità in modo accurato nelle regioni in cui c'è una discrepanza tra la configurazione della zona di destinazione e gli account che non sono aggiornati.

- La governance mista non modifica il comportamento dei SCP-based controlli (controlli preventivi), che si applicano in modo uniforme a tutti gli account di un'unità organizzativa, in ogni regione governata.

Note

La governance mista non equivale alla deriva e non viene segnalata come deriva.

Riparare una governance mista

- I clienti sono ora in grado di ripristinare la governance mista ripristinando i controlli regionali. Tutti i controlli non globali sono regionali (controlli investigativi e proattivi). Verrai avvisato che la tua unità organizzativa è in una governance mista tramite un banner di avviso.

Considerazioni per l'attivazione AWS Regioni con attivazione

Sebbene la maggior parte Regioni AWS sia attiva per impostazione predefinita Account AWS, alcune regioni vengono attivate solo quando le selezioni manualmente. Questo documento fa riferimento a tali regioni come regioni `opt-in`. Al contrario, le regioni attive per impostazione predefinita, non appena Account AWS vengono create, vengono denominate regioni `commerciali`, regioni predefinite o semplicemente regioni.

Il termine `opt-in` ha una base storica. Quelle Regioni AWS introdotte dopo il 20 marzo 2019 vengono utilizzate come regioni `opt-in`. In una regione con attivazione obbligatoria, il tuo account non è abilitato all'interno di tale regione e la tua identità non viene replicata nella regione, a meno che tu non scelga di accettare l'uso di tale regione. Tutti i dati gestiti tramite il servizio IAM sono considerati dati di identità, inclusi utenti, gruppi, ruoli, policy, provider di identità, i dati associati (ad esempio, certificati di X.509 firma o credenziali specifiche del contesto) e altre impostazioni a livello di account, come la politica delle password e l'alias dell'account.

È possibile attivare automaticamente le regioni `opt-in` durante la configurazione della zona di atterraggio, selezionandole. La tua zona di atterraggio diventa attiva in tutte le regioni selezionate.

Se scegli di selezionare una regione `opt-in` come regione principale di AWS Control Tower, attivala prima seguendo i passaggi in [Abilitazione di una regione](#), dopo aver effettuato l'accesso alla Console di AWS gestione. Per importare i tuoi account Log Archive e Audit esistenti da una regione con `opt-in`, attiva prima manualmente tale regione.

Le regioni AWS opt-in includono diverse regioni in cui è disponibile AWS Control Tower:

- Regione Asia Pacifico (Hong Kong), ap-east-1
- Regione Asia Pacifico (Jakarta), ap-southeast-3
- Regione Europa (Milano), eu-south-1
- Regione Africa (Città del Capo), af-south-1
- Regione del Medio Oriente (Bahrain), me-south-1
- Israele (Tel Aviv), il-central-1
- Regione del Medio Oriente (Emirati Arabi Uniti), me-central-1
- Regione Europa (Spagna), eu-south-2
- Regione Asia Pacifico (Hyderabad), ap-south-2
- Regione Europa (Zurigo), eu-central-2
- Regione Asia Pacifico (Melbourne), ap-southeast-4
- Regione Canada occidentale (Calgary), ca-west-1
- Asia Pacifico (Tailandia), ap-southeast-7
- Messico (centrale), mx-central-1
- Asia Pacifico (Taipei), ap-east-2
- Asia Pacifico (Nuova Zelanda), ap-southeast-6

AWS Control Tower dispone di alcuni controlli che funzionano in modo diverso nelle regioni opt-in rispetto alle regioni predefinite (altre regioni commerciali). Per ulteriori informazioni, consulta [Limitazioni di controllo](#). Ecco alcune considerazioni da tenere a mente quando si distribuiscono carichi di lavoro in regioni con opt-in.

Governare o attivare?

Ricorda che la gestione di una regione è un'azione che puoi selezionare dalla console AWS Control Tower, in modo che i controlli possano essere applicati nella regione. L'attivazione o la disattivazione di una regione opt-in è un'azione diversa che puoi scegliere nella AWS console, che apre la regione al tuo account, in modo da poter distribuire risorse e carichi di lavoro nella regione.

Considerazioni comportamentali

- Se scegli di gestire le regioni con opt-in, ti consigliamo di non disattivare (rinunciare) a nessuna delle regioni soggette all'opt-in, perché ciò può portare al fallimento dei carichi di lavoro. AWS Control Tower non consente la disattivazione di una regione governata dall'interno della console AWS Control Tower, ma assicurati di non disattivare le regioni governate da una fonte esterna ad AWS Control Tower, come la console di AWS fatturazione o l' AWS SDK.
- Quando AWS Control Tower estende la governance a una regione opt-in, si attiva (opts-in) alla regione in tutti gli account dei membri. Quando rimuovi una regione dalla governance, AWS Control Tower non la disattiva (disattiva) la regione negli account dei membri.
- Durante la deselezionazione di una regione, AWS Control Tower salta la rimozione delle risorse da una regione opt-in se tale regione è stata disattivata manualmente per un account da una fonte esterna ad AWS Control Tower, come la console di fatturazione o l'SDK. AWS AWS Ti consigliamo di rimuovere le risorse dalle regioni che hai disattivato, altrimenti potresti ricevere addebiti di fatturazione imprevisti per tali risorse.
- Se la tua zona di atterraggio viene disattivata, AWS Control Tower ripulisce le risorse in tutte le regioni governate, comprese le regioni con opt-in. Tuttavia, AWS Control Tower non disattiva le regioni opt-in. È possibile disattivare le regioni opt-in come passaggio aggiuntivo dopo la disattivazione.
- Se la tua regione di residenza è una regione opt-in e intendi registrare account esistenti come account Log Archive e Audit, devi attivare manualmente la regione opt-in prima di poterla selezionare come regione di residenza per la tua zona di atterraggio. Vedi [Abilitazione di una regione](#).
- Se AWS Control Tower è configurato con una regione opt-in come regione principale e se visiti il servizio AWS Control Tower dalla AWS console in qualsiasi altra regione, la console non ti reindirizza automaticamente alla regione principale.
- L'API sottostante ha dei limiti di capacità, che possono aumentare la latenza da pochi minuti a molte ore, a seconda del numero di regioni, account e carico del servizio. Come best practice, attiva solo quelle su Regioni AWS cui eseguirai i carichi di lavoro e attiva una regione alla volta.

Limitazioni importanti per la governance e gli account

- Se sono regolamentate 16 o più regioni commerciali in cui è disponibile AWS Control Tower, incluse le regioni opt-in, il limite massimo del numero di account per unità organizzativa (OU) viene ridotto al momento della registrazione di un'unità organizzativa. Per ulteriori informazioni, consulta [Limitazioni basate sui servizi sottostanti. AWS](#)

Configurare la regione per negare il controllo

AWS Control Tower offre due controlli di negazione delle restrizioni regionali. Un controllo, se attivato `AWS-GR_REGION_DENY`, si applica all'intera zona di atterraggio. Un altro controllo `CT.MULTISERVICE.PV.1`, se attivato, può essere applicato a unità organizzative specifiche specificate dall'utente. Per ulteriori informazioni, vedi [Negare l'accesso a AWS in base alla richiesta Regione AWS](#) e [Region Deny control applicato all'unità organizzativa](#).

Le considerazioni sulla regione negano il controllo della zona di atterraggio

La Regione nega il controllo, [AWS-GR_REGION_DENY](#) è un caso unico, in quanto si applica alla zona di atterraggio nel suo insieme, piuttosto che a una specifica unità organizzativa. Per configurare il controllo del rifiuto da parte della regione, vai alla pagina delle impostazioni della zona di destinazione e seleziona `Modifica impostazioni`.

- Questa impostazione può essere modificata in un secondo momento.
- Se abilitato, questo controllo si applica a tutte le unità organizzative con l'AWSControlTowerBaseline opzione abilitata.
- Questo controllo non può essere configurato per singole unità organizzative.

Note

Prima di abilitare il controllo Region Deny, assicurati di non disporre di risorse esistenti in queste aree, poiché non potrai accedere alle tue risorse dopo aver applicato il controllo. Mentre il controllo è abilitato, non sarai in grado di distribuire risorse nelle regioni negate.

Quando abiliti il controllo, si applica a tutte le unità organizzative di primo livello con le unità organizzative AWSControlTowerBaseline abilitate e viene ereditato dalle unità organizzative inferiori nella gerarchia organizzativa. Quando rimuovi il controllo, questo viene rimosso su tutte le unità organizzative applicate in precedenza, tutte le regioni non governate in AWS Control Tower rimangono in uno stato Non governato ed è possibile distribuire risorse in regioni al di fuori della disponibilità di AWS Control Tower.

Eccezioni

Non puoi negare l'accesso alla tua regione di origine. Alcuni AWS servizi globali, come IAM e AWS Organizations, sono esenti dalla Region Negano il controllo. Per saperne di più, consulta [Negare l'accesso a in AWS base a quanto richiesto. Regione AWS](#)

- Nome completo del controllo: nega l'accesso a in AWS base alla AWS regione richiesta per la zona di atterraggio
- Descrizione del controllo: impedisce l'accesso a operazioni non elencate nei servizi globali e regionali al di fuori delle regioni specificate per la zona di atterraggio.
- Si tratta di un controllo elettivo con guida preventiva.

Per visualizzare il modello per la Region Deny Control SCP, consulta [Deny access to AWS based on the richiesto Regione AWS](#) nel riferimento di AWS Control Tower Control. L'SCP di AWS Control Tower è simile a SCP for [AWS Organizations](#), ma non identico.

Puoi determinare gli endpoint dei servizi regionali nella pagina dei servizi [regionali](#).

Le considerazioni relative alla OU-level regione negano il controllo

La considerazione principale sul controllo negato dalla OU-level regione è determinare in che modo interagirà con la zona di atterraggio, se entrambi sono attivati. Per ulteriori informazioni, consulta la sezione [Region deny control applicato all'unità organizzativa](#).

Potresti anche consultare la sezione [Configura il controllo di negazione della regione](#).

Informazioni Account AWS in AWS Control Tower

An Account AWS è il contenitore per tutte le risorse di tua proprietà. Queste risorse includono le identità AWS Identity and Access Management (IAM) accettate dall'account, che determinano chi ha accesso a tale account. Le identità IAM possono includere utenti, gruppi, ruoli e altro ancora. Per ulteriori informazioni su come lavorare con IAM, utenti, ruoli e policy in AWS Control Tower, consulta [Gestione delle identità e degli accessi in AWS Control Tower](#).

Risorse e ora di creazione dell'account

Quando AWS Control Tower crea o registra un account, implementa la configurazione minima delle risorse necessaria per l'account. Ad esempio, può includere risorse sotto forma di [modelli Account Factory](#) e altre risorse nella landing zone, come ruoli IAM, AWS CloudTrail percorsi, [prodotti forniti di Service Catalog](#) e utenti di IAM Identity Center. AWS Control Tower distribuisce anche risorse, come richiesto dalla configurazione di controllo, per l'unità organizzativa (OU) in cui il nuovo account è destinato a diventare un account membro.

AWS Control Tower orchestra la distribuzione di queste risorse per tuo conto. Potrebbero essere necessari diversi minuti per risorsa per completare la distribuzione, quindi considera il tempo totale prima di creare o registrare un account. Per ulteriori informazioni sulla gestione delle risorse nei tuoi account, consulta [Linee guida per la creazione e la modifica delle risorse AWS Control Tower](#).

Cosa succede quando AWS Control Tower crea un account

I nuovi account in AWS Control Tower vengono creati e quindi forniti da un'interazione tra AWS Control Tower e AWS Service Catalog. AWS Organizations Puoi creare account e registrare account esistenti dalla console AWS Control Tower. Per i passaggi dettagliati per registrare un dispositivo esistente Account AWS utilizzando la console AWS Control Tower, consulta [Registra un account esistente dalla console AWS Control Tower](#).

Dietro le quinte della creazione dell'account

1. Puoi avviare la richiesta, ad esempio, dalla pagina AWS Control Tower Account Factory, direttamente dalla AWS Service Catalog console o chiamando l'ProvisionProductAPI Service Catalog.
2. AWS Service Catalog chiama AWS Control Tower.
3. AWS Control Tower avvia un flusso di lavoro che, come primo passo, richiama l' AWS Organizations CreateAccountAPI.

4. Dopo aver AWS Organizations creato l'account, AWS Control Tower completa il processo di provisioning applicando blueprint e controlli.
5. Service Catalog continua a sondare AWS Control Tower per verificare il completamento del processo di provisioning.
6. Quando il flusso di lavoro in AWS Control Tower è completo, Service Catalog finalizza lo stato dell'account e informa l'utente (il richiedente) del risultato.

Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti

Prima di accettare un Account AWS account di sicurezza (nome predefinito: Config aggregator) o di registrazione (nome predefinito: CloudTrail amministratore), AWS Control Tower verifica l'eventuale presenza di risorse in conflitto con i requisiti di AWS Control Tower. Ad esempio, potresti avere un bucket di registrazione con lo stesso nome richiesto da AWS Control Tower. Inoltre, AWS Control Tower verifica che l'account sia in grado di effettuare il provisioning delle risorse, ad esempio assicurando che Servizio di token di sicurezza AWS (AWS STS) sia abilitato, che l'account non sia sospeso e che AWS Control Tower sia autorizzata a fornire risorse all'interno dell'account.

AWS Control Tower non rimuove alcuna risorsa esistente negli account di registrazione e sicurezza forniti. Tuttavia, se scegli di abilitarlo, la regione di negazione del controllo di accesso di AWS Control Tower impedisce l'accesso alle risorse nelle regioni negate.

Sicurezza per i tuoi account

Puoi trovare indicazioni sulle migliori pratiche per proteggere la sicurezza del tuo account di gestione AWS Control Tower e degli account dei membri nella AWS Organizations documentazione.

- [Le migliori pratiche per l'account di gestione](#)
- [Le migliori pratiche per gli account dei membri](#)

Account di integrazione dei servizi

AWS Control Tower utilizza tre account speciali Account AWS: l'account di gestione, l'account di aggregazione Config e l'account CloudTrail amministratore. AWS Control Tower si riferisce all'account aggregatore Config e all'account CloudTrail amministratore come account di integrazione del servizio.

Nomi di account precedenti

Nelle versioni delle landing zone precedenti alla 4.0, questi account venivano chiamati account condivisi (o talvolta account core).

- Puoi selezionare nomi personalizzati per gli account di integrazione del servizio durante la configurazione della landing zone. Per informazioni sulla modifica del nome di un account, consulta [Modificare esternamente i nomi delle risorse AWS Control Tower](#).
- Puoi anche specificare un account di integrazione del servizio AWS Control Tower esistente Account AWS durante il processo di configurazione iniziale della landing zone. Questa opzione elimina la necessità per AWS Control Tower di creare nuovi account. (Questa è una selezione una tantum).

Per ulteriori informazioni sugli account di integrazione dei servizi e sulle risorse associate, vedere [Risorse create negli account di integrazione dei servizi](#).

Gestione dell'account

Questo Account AWS lancia AWS Control Tower. Per impostazione predefinita, l'utente root di questo account e l'utente IAM o l'utente amministratore IAM per questo account hanno accesso completo a tutte le risorse all'interno della landing zone.

Note

Come best practice, consigliamo di accedere come utente IAM Identity Center con privilegi di amministratore quando esegue funzioni amministrative all'interno della console AWS Control Tower, anziché accedere come utente root o utente amministratore IAM per questo account.

Per ulteriori informazioni sui ruoli e le risorse disponibili nell'account di gestione, consulta [Risorse create negli account di integrazione dei servizi](#).

CloudTrail account amministratore

AWS Control Tower configura l'account CloudTrail amministratore quando abiliti l'integrazione AWS CloudTrail centralizzata della registrazione. In alternativa, puoi utilizzare un AWS account esistente come account CloudTrail amministratore. Potresti conoscere questo account con il suo nome precedente: l'account di archiviazione dei registri.

Questo account contiene un bucket Amazon S3 centrale che archivia i file di registro per tutti gli altri account nella tua landing zone. Nelle versioni delle landing zone precedenti alla 4.0, questo bucket memorizza sia AWS CloudTrail i file di registro che i file di AWS Config registro. Nella versione 4.0 e successive della landing zone, questo bucket memorizza solo i file di AWS CloudTrail registro. AWS Config archivia i file di registro in un bucket dedicato nell'account dell'aggregatore Config.

Come best practice, limita l'accesso a questo account ai team responsabili della conformità e delle indagini e ai relativi strumenti di sicurezza o controllo. Puoi utilizzare questo account per controlli di sicurezza automatici. Puoi anche ospitare funzioni personalizzate Regole di AWS Config, come le funzioni Lambda, per eseguire azioni di riparazione.

Politica sui bucket Amazon S3

Per la landing zone di AWS Control Tower versione 3.3 e successive, gli account devono soddisfare una `aws:SourceOrgID` condizione per qualsiasi autorizzazione di scrittura nel bucket Audit. Questa condizione garantisce che CloudTrail solo i log possano scrivere log per conto degli account all'interno dell'organizzazione nel bucket S3; impedisce ai CloudTrail log esterni all'organizzazione di scrivere nel bucket AWS Control Tower S3. Per ulteriori informazioni, consulta [Zona di destinazione di AWS Control Tower versione 3.3](#).

Per ulteriori informazioni sui ruoli e le risorse disponibili nell'account di archiviazione dei log, consulta [CloudTrail risorse per gli account di amministratore](#)

Note

Questi registri non possono essere modificati. Tutti i registri vengono archiviati ai fini delle indagini di controllo e conformità relative all'attività dell'account.

Account aggregatore Config

AWS Control Tower configura l'account Config aggregator quando abiliti l'integrazione del AWS Config servizio. In alternativa, puoi utilizzare un AWS account esistente come account di aggregazione Config. Potresti conoscere questo account con il suo nome precedente: account di controllo.

L'account Config aggregator dovrebbe essere riservato ai team di sicurezza e conformità con ruoli di auditor (sola lettura) e amministratore (accesso completo) su più account per tutti gli account nella landing zone. Questi ruoli sono destinati a essere utilizzati dai team di sicurezza e conformità per:

- Esegui controlli tramite AWS meccanismi, come l'hosting di funzioni Lambda con AWS Config regole personalizzate.
- Esegui operazioni di sicurezza automatizzate, come azioni di riparazione.

L'account Config aggregator riceve notifiche anche tramite il servizio Amazon Simple Notification Service (Amazon SNS). Puoi ricevere tre categorie di notifiche:

- Tutti gli eventi di configurazione: questo argomento aggrega tutte CloudTrail le AWS Config notifiche provenienti da tutti gli account nella tua landing zone.
- Notifiche di sicurezza aggregate: questo argomento aggrega tutte le notifiche di sicurezza relative a CloudWatch eventi specifici, eventi di modifica dello stato di Regole di AWS Config conformità e risultati. GuardDuty
- Notifiche di deriva: questo argomento aggrega tutti gli avvisi di deriva rilevati in tutti gli account, gli utenti, le unità organizzative e gli SCP nella tua landing zone. Per ulteriori informazioni sulla deriva, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Le notifiche di controllo attivate all'interno di un account membro possono anche inviare avvisi su un argomento locale di Amazon SNS. Questa funzionalità consente agli amministratori degli account di iscriversi alle notifiche di controllo specifiche per un singolo account membro. Di conseguenza, gli amministratori possono risolvere i problemi che riguardano un singolo account, aggregando comunque tutte le notifiche dell'account nell'account aggregatore Config centralizzato. Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di Amazon Simple Notification Service](#).

Per ulteriori informazioni sui ruoli e le risorse disponibili nell'account Config aggregator, vedere.

[Risorse dell'account Config Aggregator](#)

Per ulteriori informazioni sul controllo programmatico, consulta [Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower](#).

Important

L'indirizzo e-mail fornito per l'account Config aggregator riceve e-mail di AWS notifica - conferma della sottoscrizione da tutte le piattaforme Regione AWS supportate da AWS Control Tower. Per ricevere e-mail di conformità nel tuo account Config Aggregator, devi scegliere il link Conferma iscrizione all'interno di ogni e-mail Regione AWS supportata da AWS Control Tower.

Risorse create negli account di integrazione dei servizi

Questa sezione mostra le risorse che AWS Control Tower crea negli account di integrazione dei servizi, quando configuri la landing zone.

Per informazioni sulle risorse degli account dei membri, consulta [Considerazioni sulle risorse per Account Factory](#).

Risorse dell'account di gestione

Quando configuri la landing zone, all'interno del tuo account di gestione vengono create le seguenti AWS risorse.

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS Organizations	Account	Config aggregator (audit)
		CloudTrail administrator (log archive)
AWS Organizations	Unità organizzative	Security Sandbox
AWS Organizations	Policy di controllo dei servizi	aws-guardrails-*

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(nella versione 2.6 e successive della landing zone; non implementato nella versione di landing zone 4.0 e successive)

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Non utilizzato nella versione 3.0 e successive della landing zone)
		AWSControlTowerBP-BASELINE-CLOUDWATCH
		AWSControlTowerBP-BASELINE-CONFIG
		AWSControlTowerBP-BASELINE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE(Implementato nella versione 3.2 e successive della landing zone)
		AWSControlTowerBP-SECURITY-TOPICS
		AWSControlTowerLoggingResources
		AWSControlTowerSecurityResources
		AWSControlTowerExecutionRole
		AWSControlTowerBP-CONFIG-CENTRAL-S3-

Servizio AWS	Tipo di risorsa	Nome risorsa
		BUCKET(Implementato nella versione 4.0 e successive della landing zone)
AWS Service Catalog	Prodotto	Account Factory DI AWS Control Tower
AWS Config	Aggregatore	aws-controltower-ConfigAggregatorForOrganizations(Non utilizzato nella versione 4.0 e successive della landing zone)
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Registri	aws-controltower/CloudTrail Logs
AWS Identity and Access Management	Roles	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

Servizio AWS	Tipo di risorsa	Nome risorsa
Centro identità AWS IAM	Gruppi di directory	AWSAccountFactory
		AWSAuditAccountAdmins
		AWSControlTowerAdmins
		AWSLogArchiveAdmins
		AWSLogArchiveViewers
		AWSSecurityAuditors
		AWSSecurityAuditPowerUsers
		AWSServiceCatalogAdmins
Centro identità AWS IAM	Set di autorizzazioni	AWSAdministratorAccess
		AWSPowerUserAccess
		AWSServiceCatalogAdminFullAccess
		AWSServiceCatalogEndUserAccess
		AWSReadOnlyAccess
		AWSOrganizationsFullAccess

Note

Non CloudFormation StackSet BP_BASELINE_CLOUDTRAIL è utilizzato nelle versioni 3.0 o successive delle landing zone. Tuttavia, continua a esistere nelle versioni precedenti della landing zone, fino a quando non aggiorni la landing zone.

A partire da giugno 2025, AWS Control Tower implementa i controlli investigativi come AWS Config regole collegate ai servizi direttamente negli account registrati, anziché tramite CloudFormation StackSets. Le istanze StackSets AWSControlTowerGuardrailAWS-GR-

AUDIT-BUCKET-PUBLIC-READ-PROHIBITED and AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED e lo stack ad esse associate non vengono più distribuite. Per ulteriori informazioni, consulta [Support for detective controls implementato come regole AWS Config collegate ai servizi](#).

CloudTrail risorse per gli account di amministratore

Quando configuri la landing zone, le seguenti AWS risorse vengono create all'interno del tuo account CloudTrail amministratore.

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-
		StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later)
		StackSet-AWSControlTowerBP-BASELINE-ROLES-

Servizio AWS	Tipo di risorsa	Nome risorsa
		StackSet-AWSControlTowerLoggingResources-
AWS Config	Regole di AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Regole dell'evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registri	/aws/lambda/aws-controltower-NotificationForwarder

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole
		aws-controltower-CloudWatchLogsRole
		aws-controltower-ConfigRecorderRole
		aws-controltower-ForwardSnsNotificationRole
		aws-controltower-ReadOnlyExecutionRole
		AWSControlTowerExecution
		AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Argomenti	aws-controltower-SecurityNotifications
AWS Lambda	Applicazioni	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funzioni	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Bucket	aws-controltower-logs-*
		aws-controltower-s3-access-logs-*

Risorse dell'account Config Aggregator

Quando configuri la landing zone, le seguenti AWS risorse vengono create all'interno del tuo account Config aggregator.

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-
		StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later)
		StackSet-AWSControlTowerBP-SECURITY-TOPICS-
		StackSet-AWSControlTowerBP-BASELINE-ROLES-
		StackSet-AWSControlTowerSecurityResources-*

Servizio AWS	Tipo di risorsa	Nome risorsa
		StackSet-AWSControlTowerBP-CONFIG-CENTRAL-S3-BUCKET-(Implementato nella versione 4.0 e successive della landing zone)
AWS Config	Aggregatore	aws-controltower-GuardrailsComplianceAggregator(Non utilizzato nella versione 4.0 e successive della landing zone)
AWS Config	Aggregatore	aws-controltower-ConfigAggregatorForOrganizations(Implementato nella versione 4.0 e successive della landing zone)
AWS Config	Regole di AWS Config	<p>AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED</p> <p>AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED</p>
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Regole dell'evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registri	/aws/lambda/aws-controltower-NotificationForwarder

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole
		aws-controltower-CloudWatchLogsRole
		aws-controltower-ConfigRecorderRole
		aws-controltower-ForwardSnsNotificationRole
		aws-controltower-ReadOnlyExecutionRole
		aws-controltower-AuditAdministratorRole
		aws-controltower-AuditReadOnlyRole
		AWSControlTowerExecution
		AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Argomenti	aws-controltower-AggregateSecurityNotifications
		aws-controltower-AllConfigNotifications
		aws-controltower-SecurityNotifications

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS Lambda	Funzioni	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Bucket	aws-controltower-config-logs-*(Implementato nella versione 4.0 e successive della landing zone) aws-controltower-config-access-logs-*(Implementato nella versione 4.0 e successive della landing zone)

Informazioni sugli account dei membri

Gli account membro sono gli account tramite i quali gli utenti eseguono i propri AWS carichi di lavoro. Gli account dei membri di AWS Control Tower possono essere creati e personalizzati con vari metodi, inclusi metodi automatizzati. In alcuni casi, puoi importare sistemi esistenti Account AWS in AWS Control Tower. Quando gli account dei membri vengono creati o registrati, devono esistere all'interno di un'unità organizzativa (OU) creata nella console AWS Control Tower o registrata presso AWS Control Tower. Per ulteriori informazioni, consulta questi argomenti correlati:

- [Metodi di approvvigionamento](#)
- [Fornisci e gestisci gli account con Account Factory](#)
- [Automatizza le attività in AWS Control Tower](#)
- [Sposta e registra gli account con la registrazione automatica](#)
- [Effettua il provisioning degli account con AWS Control Tower Account Factory for Terraform \(AFT\)](#)
- [AWS Terminologia e concetti relativi alle organizzazioni](#) nella Guida per l'AWS Organizations utente.

Account e controlli

Gli account dei membri possono essere registrati in AWS Control Tower o annullati. I controlli si applicano in modo diverso agli account registrati e non registrati e i controlli possono applicarsi agli account nelle unità organizzative annidate in base all'ereditarietà.

Per informazioni sulle risorse degli account dei membri che AWS Control Tower alloca, consulta [Considerazioni sulle risorse per Account Factory](#).

Interagisci con gli account AWS Control Tower da AWS Service Catalog

Questa sezione spiega come gestire i tuoi account AWS Control Tower con le funzionalità di AWS Service Catalog.

Argomenti

- [Esegui il provisioning degli account nella console Service Catalog, con Account Factory](#)
- [Automatizza il provisioning degli account nelle API AWS Control Tower tramite Service Catalog](#)
- [Aggiornare il prodotto fornito in Service Catalog](#)
- [Annullare la registrazione di un account in Service Catalog](#)

Esegui il provisioning degli account nella console Service Catalog, con Account Factory

La procedura seguente descrive come creare e fornire account come utente in IAM Identity Center tramite AWS Service Catalog. Questa procedura viene anche definita fornitura avanzata degli account o fornitura manuale degli account. Facoltativamente, potresti essere in grado di effettuare il provisioning degli account AWS Control Tower a livello di codice, con la AWS CLI, con le API Service Catalog o con AWS Control Tower Account Factory for Terraform (AFT). Potresti essere in grado di fornire account personalizzati nella console se in precedenza hai configurato blueprint personalizzati. Per ulteriori informazioni sulla personalizzazione, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#)

 Note

Se hai disabilitato IAM Identity Center nelle impostazioni della landing zone, i parametri utente SSO (SSOUserEmailSSOUserFirstName, eSSOUserLastName) non vengono utilizzati durante il provisioning dell'account. Se lo desideri, puoi fornire valori segnaposto per questi parametri obbligatori e modificarli in un secondo momento seguendo le istruzioni riportate in [Aggiornare il prodotto fornito in Service Catalog](#)

Per effettuare il provisioning degli account individualmente in Account Factory, come utente

1. Accedi dall'URL del portale utente.
2. Da Le tue applicazioni, scegli AWS Account.
3. Dall'elenco degli account, scegli l'ID dell'account per il tuo account di gestione. Questo ID può anche avere un'etichetta, ad esempio (Gestione).
4. Da AWSServiceCatalogEndUserAccess, scegli Console di gestione. Verrà aperta la finestra Console di gestione AWS per questo utente in questo account.
5. Assicurati di aver selezionato l'account corretto Regione AWS per il provisioning, che dovrebbe essere la tua regione AWS Control Tower.
6. Cerca e scegli Service Catalog per aprire la console Service Catalog.
7. Nel riquadro di navigazione, scegli Prodotti.
8. Seleziona AWS Control Tower Account Factory, quindi scegli il pulsante Launch product. Questa selezione avvia la procedura guidata per effettuare il provisioning di un nuovo account.
9. Compilare le informazioni e tenere presente quanto segue:
 - SSOUserEmailPuò essere un nuovo indirizzo e-mail o l'indirizzo e-mail associato a un utente IAM Identity Center esistente. A prescindere dalla scelta, questo utente dispone dell'accesso a livello amministrativo all'account di cui si sta effettuando il provisioning.
 - AccountEmailDeve essere un indirizzo e-mail che non sia già associato a un Account AWS. Se hai usato un nuovo indirizzo email in SSOUserEmail, puoi usare quell'indirizzo email qui.
10. Non definire TagOptionse non abilitare le notifiche, altrimenti il provisioning dell'account potrebbe non essere eseguito. Quando hai finito, scegli Launch product.
11. Esaminare le impostazioni dell'account, quindi scegliere Launch (Avvia). Non creare un piano di risorse, altrimenti il provisioning dell'account non verrà eseguito.

12. L'account è ora in fase di provisioning. Il completamento può richiedere alcuni minuti. Puoi ricaricare la pagina per aggiornare le informazioni sullo stato visualizzate.

Note

È possibile effettuare il provisioning di fino a cinque account alla volta.

Automatizza il provisioning degli account nelle API AWS Control Tower tramite Service Catalog

AWS Control Tower è integrato con diversi altri AWS servizi, ad esempio AWS Service Catalog. Puoi utilizzare le API per creare e fornire i tuoi account membro in AWS Control Tower o per registrare account membro esistenti.

Note

Se hai disabilitato IAM Identity Center nelle impostazioni della landing zone, i parametri utente SSO (`SSOUserEmail`, `SSOUserFirstName`, `eSSOUserLastName`) non vengono utilizzati durante il provisioning dell'account. Se lo desideri, puoi fornire valori segnaposto per questi parametri obbligatori e modificarli in un secondo momento seguendo le istruzioni riportate in [Aggiornare il prodotto fornito in Service Catalog](#)

Il video mostra come effettuare il provisioning degli account in modo automatico e in batch, richiamando le AWS Service Catalog API. Per il provisioning, chiamerai l'[ProvisionProduct](#) API dall'interfaccia a riga di AWS comando (CLI) e specificherai un file JSON che contiene i parametri per ogni account che desideri configurare. Il video illustra l'installazione e l'utilizzo dell'ambiente di sviluppo [AWS Cloud9](#) per eseguire questo lavoro. I comandi CLI sarebbero gli stessi se si utilizza AWS Cloudshell anziché Cloud9. AWS

Note

Puoi anche adattare questo approccio per automatizzare gli aggiornamenti degli account, chiamando l'[UpdateProvisionedProduct](#) API di per ogni account. AWS Service Catalog È possibile scrivere uno script per aggiornare gli account, uno per uno.

Trattandosi di un metodo di automazione completamente diverso, se conosci Terraform, puoi effettuare il [provisioning degli account con AWS Control Tower Account Factory for Terraform \(AFT\)](#).

Esempio di ruolo di amministrazione dell'automazione

Ecco un modello di esempio che puoi utilizzare per configurare il tuo ruolo di amministrazione dell'automazione nell'account di gestione. È necessario configurare questo ruolo nel proprio account di gestione in modo che possa eseguire l'automazione con l'accesso di amministratore negli account di destinazione.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
    Policies:
      - PolicyName: AssumeSampleAutoAdminRole
        PolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Action:
                - sts:AssumeRole
              Resource:
                - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Esempio di ruolo di esecuzione dell'automazione

Di seguito è riportato un modello di esempio che è possibile utilizzare per configurare il ruolo di esecuzione dell'automazione. Dovresti configurare questo ruolo negli account di destinazione.


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

```
Description: "Create automation execution role for creating Sample Additional Role."
```

Parameters:

```
AdminAccountId:
```

```
  Type: "String"
```

```
  Description: "Account ID for the administrator account (typically management, security or shared services)."
```

```
AdminRoleName:
```

```
  Type: "String"
```

```
  Description: "Role name for automation administrator access."
```

```
  Default: "SampleAutomationAdministrationRole"
```

```
ExecutionRoleName:
```

```
  Type: "String"
```

```
  Description: "Role name for automation execution."
```

```
  Default: "SampleAutomationExecutionRole"
```

```
SessionDurationInSecs:
```

```
  Type: "Number"
```

```
  Description: "Maximum session duration in seconds."
```

```
  Default: 14400
```

Resources:

```
# This needs to run after AdminRoleName exists.
```

```
ExecutionRole:
```

```
  Type: "AWS::IAM::Role"
```

```
  Properties:
```

```
    RoleName: !Ref ExecutionRoleName
```

```
    MaxSessionDuration: !Ref SessionDurationInSecs
```

```
    AssumeRolePolicyDocument:
```

```
      Version: "2012-10-17"
```

```
      Statement:
```

```
        - Effect: "Allow"
```

```
          Principal:
```

```
            AWS:
```

```
              - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
```

```
          Action:
```

```
            - "sts:AssumeRole"
```

```
  Path: "/"
```

```
  ManagedPolicyArns:
```

```
    - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Dopo aver configurato questi ruoli, chiami le AWS Service Catalog API per eseguire le attività automatiche. I comandi CLI sono riportati nel video.

Esempio di input di provisioning per l'API Service Catalog

Ecco un esempio dell'input che puoi fornire all'API Service Catalog se utilizzi l'ProvisionProductAPI per fornire nuovi account AWS Control Tower o per registrare account membri esistenti:

Note

Per registrare un account membro esistente utilizzando l'ProvisionProductAPI, il ruolo `AWSControlTowerExecution` IAM deve esistere sull'account di destinazione prima di chiamare l'API. Puoi utilizzare gli stessi parametri di input mostrati nell'esempio seguente sia per il provisioning di nuovi account che per la registrazione di account esistenti.

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
```

```
    value: "Smith"
  }
],
provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Per ulteriori informazioni, consulta il [riferimento all'API per Service Catalog](#).

Note

Si noti che il formato della stringa di input per il valore di `ManagedOrganizationalUnit` è cambiato da `OU_NAME` a `OU_NAME (OU_ID)`. Il video che segue non menziona questa modifica.

Procedura guidata: video

Questo video (6:58) descrive come automatizzare le distribuzioni degli account in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sul provisioning automatizzato degli account in AWS Control Tower.](#)

Aggiornare il prodotto fornito in Service Catalog

La procedura seguente illustra come aggiornare l'account in Account Factory o spostarlo in una nuova unità organizzativa, aggiornando il prodotto fornito dall'account in Service Catalog.

Note

Se hai disabilitato IAM Identity Center nelle impostazioni della landing zone, i parametri utente SSO (`SSOUserEmail`, `SSOUserFirstName`, e `SSOUserLastName`) non vengono utilizzati durante il provisioning dell'account. Se lo desideri, puoi fornire valori segnaposto per questi parametri obbligatori e modificarli in un secondo momento seguendo le istruzioni in questa sezione.

Per aggiornare un account Account Factory o modificarne l'unità organizzativa tramite Service Catalog

1. Accedi alla console di AWS gestione e apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.

Note

È necessario accedere come utente con le autorizzazioni per fornire nuovi prodotti in Service Catalog (ad esempio, un utente IAM Identity Center in uno AWSAccountFactory o più AWSServiceCatalogAdmins gruppi).

2. Nel riquadro di navigazione, scegli Provisioning, quindi scegli Provisioned products.
3. Per ciascuno degli account membro elencati, esegui le seguenti operazioni per aggiornare tutti gli account membro:
 - a. Seleziona un account membro. Verrai indirizzato alla pagina dei dettagli del prodotto Provisioned relativa a quell'account.
 - b. Nella pagina dei dettagli del prodotto Provisioned, scegli la scheda Eventi.
 - c. Prendere nota dei seguenti parametri:
 - SSOUserEmail(Disponibile nei dettagli del prodotto fornito)
 - AccountEmail(Disponibile nei dettagli del prodotto fornito)
 - SSOUserFirstName(Disponibile in IAM Identity Center)
 - SSOUserLastName(Disponibile in IAM Identity Center)
 - AccountName(Disponibile in IAM Identity Center)
 - d. Da Actions (Operazioni), scegliere Update (Aggiorna).
 - e. Scegliere il pulsante accanto alla casella Version (Versione) del prodotto da aggiornare e selezionare Next (Avanti).
 - f. Fornire i valori dei parametri citati in precedenza.
 - Se desideri mantenere l'unità organizzativa esistente ManagedOrganizationalUnit, scegli l'unità organizzativa in cui si trovava già l'account.
 - Se desideri migrare l'account verso una nuova unità organizzativa ManagedOrganizationalUnit, scegli la nuova unità organizzativa per l'account.

Un amministratore cloud centrale può trovare queste informazioni nella console AWS Control Tower, nella pagina Organizzazione.

- g. Scegli Avanti.
- h. Rivedere le modifiche, quindi scegliere Update (Aggiorna). Questo processo può richiedere alcuni minuti per account.

Annullare la registrazione di un account in Service Catalog

L'annullamento della registrazione di un account può essere effettuato nella console Service Catalog da un utente IAM Identity Center del AWSAccountFactory gruppo, interrompendo il Provisioned Product. Per ulteriori informazioni sugli utenti o i gruppi di IAM Identity Center, consulta [Gestione degli utenti](#) e accesso tramite. Centro identità AWS IAM La procedura seguente descrive come annullare la registrazione di un account membro in Service Catalog.

Per annullare la registrazione di un account registrato tramite Service Catalog

1. Apri la console Service Catalog nel tuo browser web all'indirizzo <https://console.aws.amazon.com/servicecatalog>.
2. Nel riquadro di navigazione a sinistra, scegli Elenco dei prodotti Provisioned.
3. Dall'elenco degli account assegnati, scegli il nome dell'account che desideri che AWS Control Tower non gestisca più.
4. Nella pagina Provisioned product details (Dettagli del prodotto per cui è stato effettuato il provisioning), dal menu Actions (Operazioni), scegliere Terminate (Termina).
5. Dalla finestra di dialogo che viene visualizzata, scegliere Terminate (Termina).

Important

La parola terminare è specifica di Service Catalog. Quando si chiude un account in Service Catalog Account Factory, l'account non viene chiuso. Questa azione rimuove l'account dalla relativa unità organizzativa e dalla landing zone.

6. Quando l'account è stato annullato, il suo stato diventa Non abilitato.
7. Se non ti serve più l'account, chiudilo. Per ulteriori informazioni sulla chiusura AWS degli account, consulta [Chiusura di un account](#) nella Guida AWS Billing per l'utente

 Note

Attendi che lo stato dell'account venga visualizzato come Non abilitato.

Esegui il provisioning e gestisci gli account in AWS Control Tower

Questo capitolo include:

- una panoramica e le procedure per il provisioning e la gestione di nuovi account membri in AWS Control Tower.
- una panoramica e le procedure per la registrazione di un AWS account esistente in AWS Control Tower.

Per informazioni generali sugli account in AWS Control Tower, consulta [Informazioni Account AWS in AWS Control Tower](#). Per informazioni sulla registrazione di più account in AWS Control Tower, consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#)

Note

La fornitura, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) abilitata. AWSControlTowerBaseline Se un'unità organizzativa non è AWSControlTowerBaseline abilitata, puoi attivare la registrazione automatica dell'account o utilizzare delle ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su tale unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

Note

È possibile eseguire fino a cinque (5) operazioni relative all'account contemporaneamente, tra cui provisioning, aggiornamento e registrazione.

Autorizzazioni richieste per il provisioning degli account

Con le autorizzazioni appropriate per i gruppi di utenti, i provider possono specificare linee di base e configurazioni di rete standardizzate per qualsiasi account della propria organizzazione.

Quando crei account dalla console AWS Control Tower con Account Factory, devi accedere a un account con un utente IAM con la `AWSServiceCatalogEndUserFullAccess` policy abilitata, insieme alle autorizzazioni per utilizzare la console AWS Control Tower, e non puoi accedere come utente root.

Note

Quando si effettua il provisioning di un account, il richiedente deve sempre disporre delle autorizzazioni `CreateAccount` e delle relative autorizzazioni. `DescribeCreateAccountStatus` Questo set di autorizzazioni fa parte del ruolo di amministratore e viene assegnato automaticamente quando un richiedente assume il ruolo di amministratore. Se deleghi l'autorizzazione al provisioning degli account, potrebbe essere necessario aggiungere queste autorizzazioni direttamente per i richiedenti dell'account.

Per informazioni generali sulle autorizzazioni richieste in AWS Control Tower, consulta [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#). Per informazioni su ruoli e account in AWS Control Tower, consulta [Ruoli e account](#).

Fornisci account all'interno di AWS Control Tower

AWS Control Tower offre diversi metodi per creare e aggiornare gli account dei membri. Alcuni metodi sono principalmente basati su console e altri metodi sono principalmente automatizzati.

Panoramica

Un modo standard per creare account membri in AWS Control Tower è tramite Account Factory, un prodotto basato su console che fa parte del Service Catalog. Inoltre, dalla console AWS Control Tower, puoi utilizzare `Create account` come metodo per effettuare il provisioning di nuovi account, nonché `Enroll account` per registrare AWS account esistenti in AWS Control Tower, se la tua zona di destinazione non è in uno stato di deriva.

Con Account Factory, puoi effettuare il provisioning di account di base, basandoti sulle impostazioni predefinite di AWS Control Tower. È inoltre possibile effettuare il provisioning di account personalizzati che soddisfano i requisiti per casi d'uso specializzati.

[Account Factory Customization \(AFC\)](#) è un modo per effettuare il provisioning di account personalizzati dalla console AWS Control Tower e automatizza la personalizzazione e la distribuzione

degli account. Consente il provisioning automatico basato su console, dopo alcuni passaggi di configurazione una tantum, eliminando la necessità di scrivere script o configurare pipeline. Per ulteriori informazioni, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

Iscrizione automatica

Puoi anche creare unità organizzative Account AWS esterne ad AWS Control Tower e spostarle in un'unità organizzativa registrata con AWS Control Tower, senza creare una deriva ereditaria, se attivi la funzionalità di registrazione automatica degli account nelle impostazioni della tua zona di destinazione. Per ulteriori informazioni, consulta [Sposta e registra gli account con la registrazione automatica](#).

Console-based metodi:

- Tramite la console Account Factory di cui fa parte AWS Service Catalog, per account di base o personalizzati. Consulta [Fornisci e gestisci gli account con Account Factory](#) la pagina per dettagli e istruzioni.
- Tramite la registrazione automatica, spostando un account in un'unità organizzativa dalla console. Per informazioni, consultare [Sposta e registra gli account con la registrazione automatica](#)
- Tramite la funzione Enroll account all'interno di AWS Control Tower, se la tua zona di atterraggio non è in uno stato di deriva. Consulta [Registra un account esistente dalla console AWS Control Tower](#).
- Nella console AWS Control Tower, puoi utilizzare Account Factory per creare, aggiornare o registrare fino a cinque account contemporaneamente.

Metodi automatici:

- Codice Lambda: dall'account di gestione della zona di destinazione di AWS Control Tower, utilizzando il codice Lambda e i ruoli IAM appropriati. Vedi Provisioning [automatico degli account con ruoli IAM](#).
- Terraform: da AWS Control Tower Account Factory for Terraform (AFT), che si basa su Account Factory e su un GitOps modello per consentire l'automazione del provisioning e dell'aggiornamento degli account. Consulta [Effettua il provisioning degli account con AWS Control Tower Account Factory for Terraform \(AFT\)](#).

- Tramite la registrazione automatica, spostando un account esistente in un'unità organizzativa utilizzando le API. Per informazioni, consultare [Sposta e registra gli account con la registrazione automatica](#)
- Personalizzazione di Account Factory nella console AWS Control Tower: dopo le fasi di configurazione, il provisioning futuro di account personalizzati non richiede alcuna configurazione aggiuntiva o manutenzione della pipeline. Il provisioning degli account viene effettuato tramite un AWS Service Catalog prodotto chiamato blueprint. Un progetto può utilizzare CloudFormation modelli o modelli Terraform.

Note

CloudFormation i blueprint possono distribuire risorse in più regioni. I blueprint Terraform possono distribuire risorse solo in una singola regione. Per impostazione predefinita, questa è la regione di origine.

Effettua il provisioning degli account nella console AWS Control Tower

La procedura seguente descrive come creare e fornire account come utente in IAM Identity Center tramite la console AWS Control Tower. Questa procedura viene anche chiamata provisioning manuale degli account. Facoltativamente, puoi effettuare il provisioning degli account AWS Control Tower a livello di codice, con la AWS CLI APIs, con Service Catalog o con AWS Control Tower Account Factory for Terraform (AFT), oppure registrare automaticamente un account esistente in un'unità organizzativa registrata. Potresti essere in grado di fornire account personalizzati nella console se in precedenza hai configurato blueprint personalizzati. Per ulteriori informazioni sulla personalizzazione, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#)

Per effettuare il provisioning degli account individualmente nella console AWS Control Tower, come utente

1. Accedi AWS e accedi alla console AWS Control Tower.
2. Dalla barra di navigazione a sinistra, scegli Organizations per visualizzare la pagina Organizzazione.
3. In alto a destra, scegli Crea risorse.
4. Nel menu a discesa, scegli Crea account.

5. Inserisci le informazioni sulla pagina e tieni presente quanto segue:
 - L'e-mail dell'account deve essere un indirizzo e-mail che non sia già associato a un Account AWS.
 - Il nome visualizzato è il nome che desideri visualizzare per questo account.
6. Compila i campi per definire la configurazione di Access, con un indirizzo email e un nome utente IAM Identity Center.
7. Seleziona un'unità organizzativa registrata dall'elenco a discesa per indicare l'unità organizzativa in cui desideri effettuare il provisioning dell'account.
8. Facoltativamente, utilizza un blueprint predefinito per fornire al tuo account risorse personalizzate. È possibile eseguire questa operazione in un secondo momento.
9. Controlla le selezioni dell'account, quindi scegli Crea account in basso a destra.
10. L'account è ora in fase di provisioning. Il completamento può richiedere alcuni minuti. Puoi ricaricare la pagina per aggiornare le informazioni sullo stato visualizzate.

Note

È possibile effettuare il provisioning di fino a cinque account alla volta.

Visualizza i tuoi account

La pagina **Organizzazione** elenca tutte le unità organizzative e gli account dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di iscrizione in AWS Control Tower. Puoi visualizzare e registrare gli account dei membri in AWS Control Tower, individualmente o per gruppi di unità organizzative, se ciascun account soddisfa i prerequisiti per l'iscrizione.

Per visualizzare un account specifico

- Vai alla pagina **Organizzazione**.
- Puoi scegliere **Account solo** dal menu a discesa in alto a destra.
- Quindi, seleziona il nome del tuo account dalla tabella.
- In alternativa, puoi selezionare il nome dell'unità organizzativa principale dalla tabella e visualizzare un elenco di tutti gli account all'interno di tale unità organizzativa nella pagina **Dettagli** relativa a tale unità organizzativa.

Nella pagina **Organizzazione** e nella pagina dei dettagli dell'account, puoi vedere lo stato dell'account, che è uno dei seguenti:

- **Non registrato:** l'account è membro dell'unità organizzativa principale, ma non è completamente gestito da AWS Control Tower. Se l'unità organizzativa principale è registrata, l'account è regolato dai controlli preventivi configurati per l'unità organizzativa principale registrata, ma i controlli investigativi dell'unità organizzativa principale non si applicano a questo account. Se l'unità organizzativa principale non è registrata, a questo account non si applica alcun controllo.
- **Iscrizione:** l'account viene inserito nella governance da AWS Control Tower. Stiamo allineando l'account alla configurazione di controllo per l'unità organizzativa principale. Questo processo può richiedere diversi minuti per risorsa dell'account.
- **Iscritto:** l'account è regolato dai controlli configurati per l'unità organizzativa principale. È completamente gestito da AWS Control Tower.
- **Iscrizione non riuscita:** non è stato possibile registrare l'account in AWS Control Tower. Per ulteriori informazioni, consulta [Cause comuni di mancata registrazione](#).
- **Aggiornamento disponibile:** l'account ha un aggiornamento disponibile. Gli account in questo stato sono ancora registrati, ma l'account deve essere aggiornato per riflettere le recenti modifiche apportate all'ambiente. Per aggiornare un singolo account, vai alla pagina dei dettagli dell'account e seleziona **Aggiorna account**.

Se disponi di più account con questo stato in un'unica unità organizzativa, puoi scegliere **Re-register l'unità organizzativa** e aggiornare gli account insieme.

Informazioni sulla registrazione degli account esistenti

È possibile estendere la governance di AWS Control Tower a un individuo esistente Account AWS registrandolo in un'unità organizzativa (OU) già governata da AWS Control Tower. Gli account idonei esistono in unità organizzative non registrate che fanno parte della stessa AWS Organizations organizzazione dell'unità organizzativa di AWS Control Tower.

Esistono diversi metodi per registrare gli account in AWS Control Tower. Le informazioni in questa pagina si applicano a tutti i metodi di registrazione.

 Note

Non è possibile registrare un AWS account esistente per fungere da account di controllo o di archiviazione dei log se non durante la configurazione iniziale della zona di atterraggio.

Cosa succede durante la registrazione dell'account

Durante il processo di registrazione, AWS Control Tower esegue queste azioni:

- Baseline dell'account, che include la distribuzione di questi set di stack:
 - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
 - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
 - `AWSControlTowerBP-BASELINE-CONFIG`
 - `AWSControlTowerBP-BASELINE-ROLES`
 - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
 - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
 - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

Ti consigliamo di rivedere i modelli di questi set di stack e assicurarti che non siano in conflitto con le policy esistenti.

- Identifica l'account tramite o. Centro identità AWS IAM AWS Organizations
- Inserisce l'account nell'unità organizzativa specificata. Assicurati di applicare tutte le SCP applicate nell'unità organizzativa corrente, in modo che la posizione di sicurezza rimanga coerente.
- Applica i controlli obbligatori all'account tramite gli SCP che si applicano all'unità organizzativa selezionata nel suo insieme.
- Lo abilita AWS Config e lo configura per registrare tutte le risorse dell'account.
- Aggiunge le AWS Config regole che applicano i controlli investigativi di AWS Control Tower all'account.

 Account e percorsi a livello di organizzazione CloudTrail

Per le versioni 3.1 e successive della zona di atterraggio, se hai selezionato l' AWS CloudTrail integrazione opzionale nelle impostazioni della zona di atterraggio:

- Tutti gli account dei membri di un'unità organizzativa sono regolati dal AWS CloudTrail percorso dell'unità organizzativa, iscritti o meno.
- Quando registri un account in AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso della nuova organizzazione. Se disponi di una distribuzione esistente di un CloudTrail percorso, potresti ricevere addebiti duplicati a meno che non elimini il percorso esistente per l'account prima di registrarlo in AWS Control Tower.
- Se sposti un account in un'unità organizzativa registrata, ad esempio tramite la AWS Organizations console o le API, potresti voler rimuovere eventuali percorsi rimanenti a livello di account per l'account. Se disponi già di una distribuzione di un percorso, ti verranno addebitati doppi costi CloudTrail . CloudTrail

Se aggiorni la tua zona di atterraggio e scegli di disattivare i percorsi a livello di organizzazione o se la tua zona di atterraggio è precedente alla versione 3.0, i percorsi a livello di organizzazione CloudTrail non si applicano ai tuoi account.

Registra gli account esistenti con i VPC

AWS Control Tower gestisce i VPC in modo diverso quando si effettua il provisioning di un nuovo account in Account Factory rispetto a quando si registra un account esistente.

- Quando si crea un nuovo account, AWS Control Tower rimuove automaticamente il VPC AWS predefinito e crea un nuovo VPC per quell'account.
- Quando registri un account esistente, AWS Control Tower non crea un nuovo VPC per quell'account.
- Quando registri un account esistente, AWS Control Tower non rimuove alcun VPC esistente o VPC AWS predefinito associato all'account.

Tip

Puoi modificare il comportamento predefinito per i nuovi account configurando Account Factory, in modo che non configuri un VPC di default per gli account della tua organizzazione in AWS Control Tower. Per ulteriori informazioni, consulta [Crea un account in AWS Control Tower senza un VPC](#).

Registra gli account con AWS Config risorse

L'account da registrare non deve disporre di risorse esistenti AWS Config . Vedi [Registrare gli account che dispongono di risorse esistenti AWS Config](#) .

Ecco alcuni esempi di comandi AWS Config CLI che puoi utilizzare per determinare lo stato delle AWS Config risorse del tuo account esistente, come il registratore di configurazione e il canale di consegna.

Comandi di visualizzazione:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

La risposta normale è qualcosa del tipo "name": "default"

Elimina comandi:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Prerequisiti per l'iscrizione

Questa sezione descrive come registrare un AWS account esistente in AWS Control Tower se non è stata selezionata la funzione opzionale di registrazione automatica nella pagina delle impostazioni della zona di destinazione o se si opera con una versione della zona di destinazione precedente alla 3.1.

Questi prerequisiti sono necessari prima di poter registrare un prodotto esistente Account AWS in AWS Control Tower:

 Note

Il prerequisito per aggiungere il `AWSControlTowerExecution` ruolo non è richiesto se hai attivato la funzionalità di registrazione automatica di AWS Control Tower nella pagina delle impostazioni della zona di destinazione o se stai registrando l'account come parte di un processo di registrazione OU. Tuttavia, in tutti i casi, l'account da registrare potrebbe non disporre di risorse esistenti. AWS Config Vedi [Registrazione degli account che dispongono di risorse esistenti AWS Config](#)

1. Per registrarne uno esistente Account AWS, il `AWSControlTowerExecution` ruolo deve essere presente nell'account che stai registrando. Puoi consultare [Registrazione un account](#) per dettagli e istruzioni.
2. Oltre al `AWSControlTowerExecution` ruolo, l'esistente Account AWS che desideri iscrivere deve disporre delle seguenti autorizzazioni e relazioni di fiducia. In caso contrario, la registrazione avrà esito negativo.

Autorizzazione al ruolo: `AdministratorAccess` (politica AWS gestita)

Ruolo, rapporto di fiducia:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Consigliamo che l'account non disponga di un registratore di AWS Config configurazione o di un canale di distribuzione. Questi possono essere eliminati o modificati AWS CLI prima di poter registrare un account. Altrimenti, consulta [Enroll account che dispongono di AWS Config risorse esistenti](#) per istruzioni su come modificare le risorse esistenti.

4. L'account che desideri registrare deve esistere nella stessa AWS Organizations organizzazione dell'account di gestione di AWS Control Tower. L'account esistente può essere registrato solo nella stessa organizzazione dell'account di gestione AWS Control Tower, in un'unità organizzativa già registrata con AWS Control Tower.

Per verificare altri prerequisiti per l'iscrizione, consulta [Getting Started with AWS Control Tower](#).

Note

Quando registri un account in AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso dell'organizzazione AWS Control Tower. Se disponi già di una distribuzione di un CloudTrail percorso, potresti ricevere addebiti duplicati a meno che non elimini il percorso esistente per l'account prima di registrarlo in AWS Control Tower.

Informazioni sull'accesso affidabile con il ruolo **AWSControlTowerExecution**

Prima di poter registrare un account esistente Account AWS in AWS Control Tower, devi autorizzare AWS Control Tower a gestire o governare l'account. In particolare, AWS Control Tower richiede l'autorizzazione per stabilire un accesso affidabile tra AWS CloudFormation e AWS Organizations per conto dell'utente, in modo da CloudFormation poter distribuire automaticamente lo stack negli account dell'organizzazione selezionata. Con questo accesso affidabile, il **AWSControlTowerExecution** ruolo svolge le attività necessarie per gestire ciascun account. Ecco perché è necessario aggiungere questo ruolo a ciascun account prima di registrarlo.

Quando l'accesso affidabile è abilitato, CloudFormation puoi creare, aggiornare o eliminare stack su più account e Regioni AWS con un'unica operazione. AWS Control Tower si affida a questa capacità di fiducia in modo da poter applicare ruoli e autorizzazioni agli account esistenti prima di trasferirli in un'unità organizzativa registrata e quindi di assoggettarli alla governance.

Per saperne di più sull'accesso affidabile e AWS CloudFormation StackSets, consulta [AWS CloudFormation StackSets e. AWS Organizations](#)

Sposta e registra gli account con la registrazione automatica

La funzione di registrazione automatica dell'account è disponibile per le zone di atterraggio della versione 3.1 e successive.

Se opzionalmente abiliti questa funzionalità, puoi utilizzare le AWS Organizations API e la console per spostare gli account in AWS Control Tower, senza creare una deriva ereditaria. L'account riceve automaticamente le risorse di base e le configurazioni di controllo dall'unità organizzativa (OU) di destinazione in AWS Control Tower. Questa funzionalità opzionale consente inoltre di spostare gli account tra le unità organizzative all'interno di AWS Control Tower, senza creare una deriva ereditaria, se le due unità organizzative hanno la stessa configurazione di base e gli stessi controlli abilitati.

Per attivare la registrazione automatica: puoi selezionare la registrazione automatica degli account nella pagina delle impostazioni della zona di destinazione nella console AWS Control Tower o richiamando AWS Control Tower o le UpdateLandingZone API, con il valore del parametro impostato su CreateLandingZone Inheritance Drift. RemediationType

Per registrare gli account: dopo aver attivato la registrazione automatica, sposta un account in un'unità organizzativa registrata utilizzando la console, l'API o la console AWS Control Tower. AWS Organizations MoveAccount L'account riceve automaticamente risorse e controlli di base da tale unità organizzativa. Ciò vale sia per gli account esistenti che per gli account appena creati (che vengono creati nella radice dell'organizzazione per impostazione predefinita).

Per annullare la registrazione di un account: sposta l'account in un'unità organizzativa non registrata presso AWS Control Tower o nella directory principale dell'organizzazione. AWS Control Tower rimuove automaticamente tutte le risorse e i controlli di base distribuiti.

Note

Se le unità organizzative di origine e di destinazione in AWS Control Tower hanno configurazioni diverse, è possibile che l'account mostri una deriva. [Account membro trasferito](#)

Prerequisiti: configurazione per la registrazione automatica

- È necessario eseguire la landing zone di AWS Control Tower versione 3.1 o successiva.
- Attiva la funzionalità di registrazione automatica di AWS Control Tower tramite la pagina delle impostazioni della zona di destinazione nella console o tramite le API della zona di destinazione di AWS Control Tower, impostando il valore del parametro su RemediationTypes Inheritance Drift Una volta effettuata l'attivazione, AWS Control Tower reagisce agli move account eventi e corregge immediatamente la deriva ereditaria degli account trasferiti AWS Organizations, per tuo conto.

Autorizzazioni richieste

Per utilizzare l'API e l'API sono necessari ruoli e autorizzazioni specifici. AWS Organizations CreateAccount MoveAccount Per ulteriori informazioni sull'utilizzo AWS Organizations con AWS Control Tower, consulta [AWS Control Tower e AWS Organizations](#).

Esempi di utilizzo delle API

Per ulteriori informazioni ed esempi su queste API, consulta [CreateAccount](#) e [MoveAccount](#) nella sezione AWS Organizations API Reference.

Considerazioni

- Cronologia delle iscrizioni: un account spostato in un'unità organizzativa registrata con AWS Control Tower viene registrato con un eventuale modello di coerenza. Questo processo richiede in genere alcuni minuti, fino a diverse ore, a seconda del numero di account da spostare.
- AWS Prodotti forniti da Service Catalog: Auto-enrollment non crea, modifica o termina i prodotti forniti da AWS Service Catalog. Se un account è stato precedentemente registrato tramite Account Factory e a cui è associato un prodotto con provisioning, tale prodotto rimane nell'account di gestione dopo la cancellazione dell'account. Per ripulire i prodotti con provisioning orfani, vedere [Eliminazione dei prodotti sottoposti a provisioning nella Service Catalog User Guide](#). AWS

Registra un account esistente dalla console AWS Control Tower

Esistono due modi comuni per iscrivere una persona Account AWS in AWS Control Tower.

1. Dopo aver selezionato la funzionalità di registrazione automatica nella pagina Impostazioni, puoi creare un'unità organizzativa Account AWS esterna ad AWS Control Tower e spostarla direttamente in un'unità organizzativa registrata. Per ulteriori informazioni, consulta [Spostare e registrare gli account automaticamente](#). Questa opzione è disponibile per le versioni 3.1 e successive della zona di atterraggio.
2. Puoi registrare manualmente un account esistente dalla console AWS Control Tower.

Le sezioni seguenti descrivono la seconda opzione, che non richiede alcuna configurazione precedente dell'ambiente AWS Control Tower. Account AWS Devono soddisfare i [prerequisiti](#) richiesti.

Visualizza i tuoi account idonei nella console:

1. Accedi alla pagina dell'organizzazione in AWS Control Tower.
2. Trova il nome dell'account che desideri registrare. Per trovarlo, scegli Solo account dal menu a discesa in alto a destra, quindi individua il nome dell'account nella tabella filtrata.

Successivamente, segui i passaggi per la registrazione di un singolo account, come mostrato nella sezione. [Procedura per registrare un account manualmente](#)

Considerazioni per la registrazione dalla console

- La funzionalità Enroll account disponibile nella console AWS Control Tower è destinata alla registrazione degli account esistenti in Account AWS modo che siano governati da AWS Control Tower. Per ulteriori informazioni, consulta [Registrare un esistente. Account AWS](#)
- La funzionalità dell'account Enroll basata su console è disponibile quando la zona di atterraggio non è in uno stato di deriva. <https://docs.aws.amazon.com/controltower/latest/userguide/drift.html> Se la landing zone si trova in uno stato di deviazione, potresti non essere in grado di utilizzare correttamente la funzionalità Enroll account (Registra account) . Dovrai effettuare il provisioning di nuovi account tramite Account Factory o un altro metodo, fino a quando la deviazione dalla zona di atterraggio non sarà risolta.
- Quando registri account dalla console AWS Control Tower, devi accedere a un account con un utente con la `AWSServiceCatalogEndUserFullAccess` policy abilitata, insieme alle autorizzazioni di accesso dell'amministratore per utilizzare la console AWS Control Tower, e non puoi accedere come utente root.
- Gli account registrati possono essere aggiornati tramite AWS Control Tower Account Factory, così come si aggiorna qualsiasi altro account. Le procedure di aggiornamento sono fornite nella sezione chiamata [Aggiorna e sposta gli account con AWS Control Tower](#).

Note

Quando registri un indirizzo email esistente Account AWS, assicurati di verificare l'indirizzo email esistente. Altrimenti, potrebbe essere creato un nuovo account.

Procedura per registrare un account manualmente

Dopo aver ottenuto `AdministratorAccess` l'autorizzazione di accesso (politica) nel tuo Account AWS account esistente, segui questi passaggi per registrare l'account:

Per registrare un account individuale in AWS Control Tower dalla console

- Vai alla pagina AWS Control Tower Organization.
- Nella pagina Organizzazione, gli account idonei alla registrazione consentono di selezionare Enroll dal menu a discesa Azioni nella parte superiore della sezione. Questi account mostrano anche un pulsante Registra account quando li visualizzi nella pagina dei dettagli dell'account.
- Quando scegli Registra account, viene visualizzata una pagina Registra account, in cui ti viene richiesto di aggiungere il `AWSControlTowerExecution` ruolo all'account. Per alcune istruzioni, consulta [Aggiungi manualmente il ruolo IAM richiesto a un ruolo IAM esistente Account AWS e iscrivilo](#)
- Quindi, seleziona un'unità organizzativa registrata dall'elenco a discesa. Se l'account è già in un'unità organizzativa registrata, questo elenco mostrerà l'unità organizzativa.
- Scegli Enroll account (Registra account).
- Vedrai un promemoria modale per aggiungere il `AWSControlTowerExecution` ruolo e confermare l'azione.
- Scegli Iscriviti.
- AWS Control Tower avvia il processo di registrazione e verrai reindirizzato alla pagina dei dettagli dell'account.

Cause comuni di mancata registrazione

- Per registrare un account esistente, il `AWSControlTowerExecution` ruolo deve essere presente nell'account che stai registrando.
- L'entità IAM potrebbe non disporre delle autorizzazioni necessarie per effettuare il provisioning di un account.
- Servizio di token di sicurezza AWS (AWS STS) è disabilitato Account AWS nella tua regione di origine o in qualsiasi regione supportata da AWS Control Tower.
- Potresti aver effettuato l'accesso come utente o ruolo IAM che deve essere aggiunto all'Account Factory Portfolio in AWS Service Catalog. L'utente o il ruolo deve essere aggiunto prima di poter accedere ad Account Factory in modo da poter creare o registrare un account in AWS Control Tower. Se l'utente o il ruolo appropriato non viene aggiunto al portafoglio Account Factory, riceverai un errore quando tenti di aggiungere un account. Per istruzioni su come concedere l'accesso ai AWS Service Catalog portafogli, consulta [Concessione dell'accesso agli utenti](#).
- È possibile che sia stato eseguito l'accesso come root.

- L'account che stai tentando di registrare potrebbe avere AWS Config impostazioni residue. In particolare, l'account potrebbe avere un registratore di configurazione o un canale di distribuzione. Questi devono essere eliminati o modificati AWS CLI prima di poter registrare un account. Per ulteriori informazioni, consulta [Registra account esistenti AWS Config risorse](#) e [Interagisci con AWS Control Tower attraverso AWS CloudShell](#).
- Se l'account appartiene a un'altra unità organizzativa con un account di gestione, inclusa un'altra unità organizzativa di AWS Control Tower, devi chiudere l'account nell'unità organizzativa corrente prima che possa entrare a far parte di un'altra unità organizzativa. Le risorse esistenti devono essere rimosse nell'unità organizzativa originale. In caso contrario, la registrazione avrà esito negativo.
- Il provisioning e la registrazione dell'account non riescono se gli SCP dell'unità organizzativa di destinazione non consentono di creare tutte le risorse necessarie per quell'account. Ad esempio, un SCP nell'unità organizzativa di destinazione potrebbe bloccare la creazione di risorse senza determinati tag. In questo caso, il provisioning o la registrazione dell'account non riescono perché AWS Control Tower non supporta l'etichettatura delle risorse. Per assistenza, contatta il rappresentante del tuo account, o. Supporto

Per ulteriori informazioni su come AWS Control Tower funziona con i ruoli durante la creazione di nuovi account o la registrazione di account esistenti, consulta [Ruoli e account](#).

Tip

Se non riesci a confermare che un'unità organizzativa esistente Account AWS soddisfi i prerequisiti di iscrizione, puoi configurare un'unità organizzativa di iscrizione e registrare l'account in tale unità organizzativa. Una volta completata la registrazione, è possibile spostare l'account nell'unità organizzativa desiderata. Se la registrazione non va a buon fine, nessun altro account o unità organizzativa è interessato dall'errore.

Se hai dubbi sulla compatibilità degli account esistenti e delle relative configurazioni con AWS Control Tower, puoi seguire le best practice consigliate nella sezione seguente.

Consigliato: puoi impostare un approccio in due passaggi per la registrazione dell'account

- Innanzitutto, utilizza un pacchetto di AWS Config conformità per valutare in che modo i tuoi account potrebbero essere influenzati da alcuni controlli AWS Control Tower. Per determinare in

che modo l'iscrizione ad AWS Control Tower può influire sui tuoi account, consulta [Estendere la governance di AWS Control Tower utilizzando i pacchetti di conformità. AWS Config](#)

- Successivamente, potresti voler registrare l'account. Se i risultati di conformità sono soddisfacenti, il percorso di migrazione è più semplice perché puoi registrare l'account senza conseguenze impreviste.
- Dopo aver completato la valutazione, se decidi di configurare una landing zone di AWS Control Tower, potresti dover rimuovere il canale di AWS Config distribuzione e il registratore di configurazione creati per la valutazione. Quindi sarai in grado di configurare correttamente AWS Control Tower.

Note

Il pacchetto di conformità funziona anche in situazioni in cui gli account si trovano in unità organizzative registrate da AWS Control Tower, ma i carichi di lavoro vengono eseguiti in AWS regioni che non dispongono del supporto di AWS Control Tower. Puoi utilizzare il pacchetto di conformità per gestire le risorse negli account esistenti nelle regioni in cui AWS Control Tower non è distribuito.

Se l'account non soddisfa i prerequisiti

Ricorda che, come prerequisito, gli account idonei a essere iscritti alla governance di AWS Control Tower devono far parte della stessa organizzazione generale. Per soddisfare questo prerequisito per la registrazione dell'account, puoi seguire questi passaggi preparatori per trasferire un account nella stessa organizzazione di AWS Control Tower.

Fasi preparatorie per inserire un account nella stessa organizzazione di AWS Control Tower

1. Elimina l'account dall'organizzazione esistente. Se utilizzi questo metodo di pagamento, devi fornire un metodo di pagamento separato.
2. Invita l'account a entrare a far parte dell'organizzazione AWS Control Tower. Per ulteriori informazioni, consulta [Invitare un AWS account a entrare nella tua organizzazione](#) nella Guida per l'AWS Organizations utente.
3. Accetta l'invito. L'account viene visualizzato nella directory principale dell'organizzazione. Questo passaggio sposta l'account nella stessa organizzazione di AWS Control Tower e stabilisce gli SCP e la fatturazione consolidata.

 Tip

Puoi inviare l'invito per la nuova organizzazione prima che l'account esca dalla vecchia organizzazione. L'invito sarà in attesa quando l'account uscirà ufficialmente dalla sua organizzazione esistente.

Passaggi per soddisfare i restanti prerequisiti:

1. Crea il `AWSControlTowerExecution` ruolo necessario.
2. Cancella il VPC predefinito. (Questa parte è opzionale. AWS Control Tower non modifica il tuo VPC predefinito esistente.)
3. Elimina o modifica qualsiasi registratore AWS Config di configurazione o canale di distribuzione esistente tramite o. AWS CLI AWS CloudShell Per ulteriori informazioni, consulta [Registra gli account con AWS Config risorse](#) e [Registra account esistenti AWS Config risorse](#).

Dopo aver completato questi passaggi preparatori, puoi registrare l'account in AWS Control Tower. Per ulteriori informazioni, consulta [Procedura per registrare un account manualmente](#). Questo passaggio introduce l'account nella governance completa di AWS Control Tower.

Passaggi opzionali per annullare il provisioning di un account, in modo che possa essere registrato e mantenerne lo stack

1. Per mantenere lo CloudFormation stack applicato, elimina l'istanza dello stack dai set di stack e scegli `Retain stacks` per l'istanza.
2. Chiudi il prodotto fornito dall'account in AWS Service Catalog Account Factory. (Questo passaggio rimuove solo il prodotto fornito da AWS Control Tower. Non elimina l'account.)
3. Configura l'account con i dati di fatturazione necessari, come richiesto per qualsiasi account che non appartiene a un'organizzazione. Quindi rimuovi l'account dall'organizzazione. (Lo fai, in modo che l'account non venga conteggiato nel totale della tua AWS Organizations quota.)
4. Pulisci l'account se rimangono risorse, quindi chiudilo seguendo la procedura di chiusura dell'account [Annulla la registrazione di un account](#).
5. Se disponi di un'unità organizzativa sospesa con controlli definiti, puoi spostarvi l'account anziché eseguire il passaggio 1.

Aggiungi manualmente il ruolo IAM richiesto a un ruolo IAM esistente Account AWS e iscrivilo

Se hai già configurato la tua landing zone di AWS Control Tower, puoi iniziare a registrare gli account della tua organizzazione in un'unità organizzativa registrata presso AWS Control Tower. Se non hai configurato la tua zona di destinazione, segui i passaggi descritti nella Guida per l'utente di AWS Control Tower in [Getting Started, Step 2](#). Una volta che la zona di destinazione è pronta, completa i seguenti passaggi per portare gli account esistenti alla governance di AWS Control Tower, manualmente.

Assicurati di leggere quanto [Prerequisiti per l'iscrizione](#) indicato in precedenza in questo capitolo.

Prima di registrare un account con AWS Control Tower, devi autorizzare AWS Control Tower a gestire tale account. A tale scopo, aggiungerai un ruolo con accesso completo all'account, come mostrato nei passaggi seguenti. Questi passaggi devono essere eseguiti per ogni account registrato.

Per ogni account:

Passaggio 1: accedi con accesso amministratore all'account di gestione dell'organizzazione che attualmente contiene l'account che desideri registrare.

Ad esempio, se hai creato questo account da AWS Organizations e utilizzi un ruolo IAM con più account per accedere, puoi seguire questi passaggi:

1. Accedi all'account di gestione della tua organizzazione.
2. Passa a AWS Organizations.
3. In Account, seleziona l'account che desideri registrare e copia il relativo ID account.
4. Apri il menu a discesa dell'account nella barra di navigazione in alto e scegli **Cambia ruolo**.
5. Nel modulo **Cambia ruolo**, compila i seguenti campi:
 - In Account, inserisci l'ID dell'account che hai copiato.
 - In Ruolo, inserisci il nome del ruolo IAM che consente l'accesso tra più account a questo account. Il nome di questo ruolo è stato definito al momento della creazione dell'account. Se non hai specificato un nome di ruolo durante la creazione dell'account, inserisci il nome del ruolo predefinito, `OrganizationAccountAccessRole`.
6. Seleziona **Switch Role (Cambia ruolo)**.
7. Ora dovresti aver effettuato l'accesso Console di gestione AWS come account figlio.
8. Quando hai finito, resta nell'account figlio per la parte successiva della procedura.

9. Prendi nota dell'ID dell'account di gestione, perché dovrai inserirlo nel passaggio successivo.

Passaggio 2: autorizza AWS Control Tower a gestire l'account.

1. Vai a IAM.
2. Vai a Ruoli.
3. Scegliere Crea ruolo.
4. Quando ti viene chiesto di selezionare il servizio a cui è destinato il ruolo, scegli Politica di fiducia personalizzata.
5. Copia l'esempio di codice mostrato qui e incollalo nel Documento Policy. Sostituisci la stringa *Management Account ID* con l'ID effettivo dell'account di gestione del tuo account di gestione. Ecco la politica da incollare:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

6. Quando ti viene chiesto di allegare le politiche, scegli AdministratorAccess.
7. Scegli Next:Tags.
8. Potresti visualizzare una schermata opzionale intitolata Aggiungi tag. Salta questa schermata per ora scegliendo Next:Review
9. Nella schermata Revisione, nel campo Nome ruolo, inserisci AWSControlTowerExecution.
10. Inserisci una breve descrizione nella casella Descrizione, ad esempio Consente l'accesso completo all'account per la registrazione.
11. Scegliere Crea ruolo.

Passaggio 3: registra l'account spostandolo in un'unità organizzativa registrata e verifica l'iscrizione.

Dopo aver impostato le autorizzazioni necessarie creando il ruolo, segui questi passaggi per registrare l'account e verificare l'iscrizione.

1. Accedi nuovamente come amministratore e vai a AWS Control Tower.
2. Registra l'account.
 - Dalla pagina Organizzazione in AWS Control Tower, seleziona il tuo account, quindi scegli Enroll dal menu a discesa Azioni in alto a destra.
 - Segui i passaggi per registrare un account individuale, come mostrato nella pagina. [Procedura per registrare un account manualmente](#)
3. Verifica l'iscrizione.
 - Da AWS Control Tower, scegli Organizzazione nella barra di navigazione a sinistra.
 - Cerca l'account che hai registrato di recente. Lo stato iniziale mostrerà lo stato di Iscrizione.
 - Quando lo stato cambia in Abilitato, lo spostamento è andato a buon fine.

Per continuare questo processo, accedi a ogni account della tua organizzazione che desideri registrare in AWS Control Tower. Ripeti i passaggi dei prerequisiti e i passaggi di registrazione per ogni account.

Esempio di aggiunta del ruolo **AWSControlTowerExecution**

Il seguente modello YAML può aiutarti a creare il ruolo richiesto in un account, in modo che possa essere registrato a livello di codice.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
```

```
Type: AWS::IAM::Role
Properties:
  RoleName: AWSControlTowerExecution
  AssumeRolePolicyDocument:
    Version: 2012-10-17
    Statement:
      - Effect: Allow
        Principal:
          AWS:
            - !Ref AdministratorAccountId
        Action:
          - sts:AssumeRole
  Path: /
  ManagedPolicyArns:
    - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

Registra account esistenti AWS Config risorse

Questo argomento fornisce un approccio dettagliato su come registrare account che dispongono di risorse esistenti. AWS Config Per esempi su come controllare le risorse esistenti, consulta. [Registra gli account con AWS Config risorse](#)

Esempi di AWS Config risorse

Ecco alcuni tipi di AWS Config risorse che il tuo account potrebbe già avere. Potrebbe essere necessario modificare queste risorse in modo da poter registrare il proprio account in AWS Control Tower.

- AWS Config registratore
- AWS Config canale di consegna
- AWS Config autorizzazione all'aggregazione

Limitazioni

- L'account Enroll con la risorsa AWS Config esistente non è supportato per gli account di gestione o gli account di integrazione dei servizi configurati nella landing zone.
- L'account può essere registrato solo utilizzando il flusso di lavoro di registrazione o ri-registrazione dell'unità organizzativa che abilita il. `AWSControlTowerBaseline` L'account non può essere registrato abilitando o reimpostando il. `ConfigBaseline`

- L'account con una risorsa AWS Config esistente non è supportato da. [Sposta e registra gli account con la registrazione automatica](#)
- Se le risorse vengono modificate e creano una deriva sull'account, AWS Control Tower non aggiorna le risorse.
- AWS Config le risorse nelle regioni che non sono governate da AWS Control Tower non vengono modificate.

Presupposti

- Hai implementato una landing zone di AWS Control Tower.
- Il tuo account non è ancora registrato presso AWS Control Tower.
- Il tuo account ha almeno una AWS Config risorsa preesistente in almeno una delle regioni governate da AWS Control Tower.
- Il tuo account non è soggetto a cambiamenti di governance.

Note

Se tenti di registrare un account che dispone di risorse Config esistenti, senza che l'account venga aggiunto all'elenco consentito, la registrazione avrà esito negativo. Successivamente, se successivamente si tenta di aggiungere lo stesso account all'elenco degli account consentiti, AWS Control Tower non può verificare che l'account sia stato fornito correttamente. È necessario rimuovere l'account da AWS Control Tower prima di poter richiedere l'elenco degli account consentiti e quindi registrarlo. Se si sposta l'account solo in un'altra unità organizzativa AWS Control Tower, si verifica un cambiamento di governance, che impedisce anche l'aggiunta dell'account all'elenco degli account consentiti.

Per un blog che descrive un approccio automatizzato alla registrazione di account con AWS Config risorse esistenti, consulta [Automate enrollment of account con AWS Config risorse esistenti in AWS Control Tower](#).

Questo processo prevede 5 fasi principali.

1. Aggiungi gli account all'elenco degli account consentiti di AWS Control Tower.
2. Crea un nuovo ruolo IAM nell'account.
3. Modifica le AWS Config risorse preesistenti.

4. Crea AWS Config risorse nelle AWS regioni in cui non esistono.
5. Registra l'account con AWS Control Tower.

Prima di procedere, considera le seguenti aspettative relative a questo processo.

- AWS Control Tower non crea alcuna AWS Config risorsa in questo account.
- Dopo la registrazione, i controlli AWS Control Tower proteggono automaticamente le AWS Config risorse create, incluso il nuovo ruolo IAM.
- Se vengono apportate modifiche alle AWS Config risorse dopo la registrazione, tali risorse devono essere aggiornate per allinearle alle impostazioni di AWS Control Tower prima di poter registrare nuovamente l'account.

Passaggio 1: contatta l'assistenza per aggiungere account all'elenco degli account consentiti

Includi questa frase nell'oggetto del ticket:

Registra account che dispongono di AWS Config risorse esistenti in AWS Control Tower

Includi i seguenti dettagli nel corpo del ticket:

- Numero dell'account di gestione
- Numeri di account degli account dei membri che dispongono di AWS Config risorse esistenti. Potrai creare una richiesta di supporto per tutti gli account che desideri registrare.
- La regione d'origine selezionata per la configurazione di AWS Control Tower

Note

Il tempo necessario per aggiungere il tuo account all'elenco degli account consentiti è di 2 giorni lavorativi.

Fase 2: Crea un nuovo ruolo IAM nell'account del membro

1. Apri la CloudFormation console per l'account membro.
2. Crea un nuovo stack utilizzando il seguente modello

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Fornisci il nome dello stack come `CustomerCreatedConfigRecorderRoleForControlTower`
4. Creare lo stack.

Note

Qualsiasi SCP che crei dovrebbe escludere un `aws-controltower-ConfigRecorderRole*` ruolo. Non modificate le autorizzazioni che limitano la capacità AWS Config delle regole di eseguire valutazioni. Segui queste linee guida in modo da non ricevere un messaggio `AccessDeniedException` quando hai SCP che `aws-controltower-ConfigRecorderRole*` impediscono di chiamare Config.

Passaggio 3: Identifica il AWS Regioni con risorse preesistenti

Per ogni regione governata (gestita da AWS Control Tower) nell'account, identifica e annota le regioni che hanno almeno uno degli esempi di AWS Config risorse esistenti mostrati in precedenza.

Fase 4: Identifica il AWS Regioni senza AWS Config risorse

Per ogni regione governata (gestita da AWS Control Tower) nell'account, identifica e annota le regioni in cui non sono presenti AWS Config risorse dei tipi di esempio mostrati in precedenza.

Passaggio 5: modifica le risorse esistenti in ciascuna AWS Region

Per questa fase, sono necessarie le seguenti informazioni sulla configurazione di AWS Control Tower.

- **AUDIT_ACCOUNT**- l'ID dell'account di integrazione del servizio AWS Config (precedentemente noto come account Audit)
- **CONFIG_BUCKET**- il bucket AWS S3 a cui AWS Config fornisce snapshot di configurazione e file di cronologia della configurazione. Individua e conferma l'esistenza del bucket AWS S3 prima di procedere con i passaggi successivi.
 - Per la versione 3.3 o precedente della landing zone, viene denominato il bucket AWS S3 `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`, che si trova nell'account Logging.
 - Per la versione 4.0 o successiva della landing zone, viene denominato il bucket AWS S3 `aws-controltower-config-logs-AUDIT_ACCOUNT-<SUFFIX_STRING>`, che si trova nell'account di integrazione del servizio AWS Config (precedentemente noto come account Audit).
- **IAM_ROLE_ARN**- il ruolo IAM ARN creato nella Fase 2
- **ORGANIZATION_ID**- l'ID dell'organizzazione per l'account di gestione
- **MEMBER_ACCOUNT_NUMBER**- l'account del membro che viene modificato
- **HOME_REGION**- la regione di origine per la configurazione di AWS Control Tower.

Modifica ogni risorsa esistente seguendo le istruzioni fornite nelle sezioni da 5a a 5c, che seguono.

Fase 5a. AWS Config risorse del registratore

Può esistere un solo AWS Config registratore per regione. AWS Se ne esiste uno, modificate le impostazioni come mostrato. Sostituisci l'articolo `GLOBAL_RESOURCE_RECORDING` con `true` nella tua regione d'origine. Sostituisci l'elemento con `false` per le altre regioni in cui esiste un AWS Config registratore.

- Nome: **DON'T CHANGE**

- ROLearn: IAM_ROLE_ARN
 - RecordingGroup:
 - AllSupported: vero
 - IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
 - ResourceTypes: Vuoto

Questa modifica può essere effettuata tramite la AWS CLI utilizzando il seguente comando. Sostituite la stringa RECORDER_NAME con il nome del AWS Config registratore esistente.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
  allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

Fase 5b. Modify (Modifica) AWS Config risorse del canale di distribuzione

Può esistere un solo canale di AWS Config distribuzione per regione. Se ne esiste un altro, modifica le impostazioni come mostrato.

- Nome: DON'T CHANGE
- ConfigSnapshotDeliveryProperties: TwentyFour _Ore
- S3BucketName: CONFIG_BUCKET
- S3KeyPrefix: ORGANIZATION_ID
- SnsTopicARN: l'ARN dell'argomento SNS dell'account di controllo, con il seguente formato:

```
arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
```

Questa modifica può essere effettuata tramite la AWS CLI utilizzando il seguente comando. Sostituite la stringa DELIVERY_CHANNEL_NAME con il nome del AWS Config registratore esistente.

```
aws configservice put-delivery-channel --delivery-channel
name=DELIVERY_CHANNEL_NAME,s3BucketName=CONFIG_BUCKET,s3KeyPrefix="ORGANIZATION_ID",configSnap
controltower-AllConfigNotifications --region CURRENT_REGION
```

Fase 5c. Modify (Modifica) AWS Config risorse di autorizzazione all'aggregazione

Note

Questo passaggio non è necessario per la versione 4.0 o successiva della landing zone.

Possono esistere più autorizzazioni di aggregazione per regione. AWS Control Tower richiede un'autorizzazione di aggregazione che specifichi l'account di audit come account autorizzato e abbia la regione di origine per AWS Control Tower come regione autorizzata. Se non esiste, creane uno nuovo con le seguenti impostazioni:

- `AuthorizedAccountId`: L'ID dell'account Audit
- `AuthorizedAwsRegion`: La regione principale per la configurazione di AWS Control Tower

Questa modifica può essere effettuata tramite la AWS CLI utilizzando il seguente comando:

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

Fase 6: Creare risorse dove non esistono, nelle regioni governate da AWS Control Tower

Modifica il CloudFormation modello, in modo che nella tua regione d'origine il `IncludeGlobalResourcesTypes` parametro abbia il valore `GLOBAL_RESOURCE_RECORDING`, come mostrato nell'esempio che segue. Aggiorna anche i campi obbligatori nel modello, come specificato in questa sezione.

Sostituisci l'articolo `GLOBAL_RESOURCE_RECORDING` con `true` nella tua regione d'origine. Sostituisci l'elemento con `false` per le altre regioni in cui non esiste un AWS Config registratore.

1. Accedi alla CloudFormation console dell'account di gestione.
2. Creane uno nuovo StackSet con il nome CustomerCreatedConfigResourcesForControlTower.
3. Copia e aggiorna il seguente modello:

Note

La CustomerCreatedAggregationAuthorization risorsa nel modello non è richiesta per la versione 4.0 o successiva della landing zone.

```

AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: CONFIG_BUCKET
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION

```

Aggiorna il modello con i campi obbligatori:

- a. Nel S3BucketNamecampo, sostituisci il *CONFIG_BUCKET*
 - b. Sul S3KeyPrefixcampo, sostituire il *ORGANIZATION_ID*
 - c. Nel campo SnsTopicARN, sostituire *AUDIT_ACCOUNT*
 - d. Nel AuthorizedAccountIdcampo, sostituire il *AUDIT_ACCOUNT*
 - e. Sul AuthorizedAwsRegioncampo, sostituire il *HOME_REGION*
4. Durante la distribuzione sulla CloudFormation console, aggiungi il numero di account del membro.
 5. Aggiungi le AWS regioni identificate nel passaggio 4.
 6. Distribuisci lo stack set.

Fase 7: Registrazione dell'unità organizzativa con AWS Control Tower

Nella dashboard di AWS Control Tower, registra l'unità organizzativa.

Note

Il flusso di lavoro dell'account Enroll non avrà successo per questa operazione. È necessario scegliere Register OU o Re-registerOU.

Fornisci e gestisci gli account con Account Factory

Note

Il provisioning, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) AWSControlTowerBaseline abilitata. Se un'unità organizzativa non è AWSControlTowerBaseline abilitata, puoi attivare la registrazione automatica dell'account o utilizzare delle ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su tale unità organizzativa per registrare gli account. Per i dettagli di, vedere:.. AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

Questo capitolo include una panoramica e le procedure per il provisioning di nuovi account membri in una landing zone di AWS Control Tower con Account Factory.

Autorizzazioni per la configurazione e il provisioning degli account

AWS Control Tower Account Factory consente agli amministratori e agli utenti del cloud di Centro identità AWS IAM effettuare il provisioning degli account nella tua zona di destinazione. Per impostazione predefinita, gli utenti di IAM Identity Center che effettuano il provisioning degli account devono appartenere al AWSAccountFactory gruppo o al gruppo di gestione.

Note

Fai attenzione quando lavori dall'account di gestione, come faresti quando utilizzi qualsiasi account con autorizzazioni in tutta l'organizzazione.

L'account di gestione di AWS Control Tower ha un rapporto di fiducia con il `AWSControlTowerExecution` ruolo, che consente la configurazione dell'account dall'account di gestione, inclusa la configurazione automatica dell'account. Per ulteriori informazioni sul `AWSControlTowerExecution` ruolo, consulta [Ruoli e account](#).

Note

Per iscrivere un utente esistente Account AWS in AWS Control Tower, tale account deve avere il `AWSControlTowerExecution` ruolo abilitato. Per ulteriori informazioni su come registrare un account esistente, consulta [Informazioni sulla registrazione degli account esistenti](#).

Per ulteriori informazioni sulle autorizzazioni, consultare [Autorizzazioni richieste per il provisioning degli account](#).

Considerazioni sulla gestione degli account in Account Factory

Puoi aggiornare, annullare la registrazione e chiudere gli account creati e gestiti tramite Account Factory. Puoi riciclare gli account aggiornando i parametri utente negli account che desideri riutilizzare. Puoi anche modificare l'unità organizzativa (OU) di un account.

 Note

Quando si aggiorna un prodotto sottoposto a provisioning associato a un account fornito da Account Factory, se si specifica un nuovo indirizzo email utente Centro identità AWS IAM, AWS Control Tower crea un nuovo utente in IAM Identity Center. L'account creato in precedenza non viene rimosso. Per informazioni sulla rimozione del precedente indirizzo email dell'utente IAM Identity Center da IAM Identity Center, consulta [Disabilitazione di un utente](#).

Aggiorna e sposta gli account con AWS Control Tower

Il modo più semplice per aggiornare un account registrato è tramite la console AWS Control Tower. Gli aggiornamenti dei singoli account sono utili per risolvere problemi di errore, ad esempio. [Account membro trasferito](#) Gli aggiornamenti dell'account sono necessari anche come parte di un aggiornamento completo della zona di atterraggio.

Aggiorna l'account nella console

Per aggiornare un account nella console AWS Control Tower

1. Una volta effettuato l'accesso ad AWS Control Tower, vai alla pagina **Organizzazione**.
2. Nell'elenco delle unità organizzative e degli account, seleziona il nome dell'account che desideri aggiornare. Gli account disponibili per l'aggiornamento mostrano lo stato **Aggiornamento disponibile**.
3. Successivamente vedrai la pagina dei dettagli dell'account per l'account selezionato.
4. In alto a destra, scegli **Aggiorna account**.

Se sposti un account da un'unità organizzativa (OU) a un'altra, ricorda che i controlli applicati dalla nuova unità organizzativa potrebbero essere diversi dai controlli della precedente unità organizzativa. Assicurati che i controlli nella nuova unità organizzativa soddisfino i requisiti delle politiche per l'account.

Gli account AWS Control Tower vengono modificati in modo diverso, a seconda che tu abbia optato per la registrazione automatica degli account o meno. Per ulteriori informazioni sulla registrazione automatica, consulta. [Facoltativamente, configura la registrazione automatica per gli account](#)

Controlla il comportamento quando gli account vengono spostati tra

unità organizzative, con registrazione automatica abilitata

Quando sposti un account in una nuova unità organizzativa, AWS Control Tower applica all'account le linee di base e i controlli abilitati dell'unità organizzativa. I controlli e le linee di base della precedente unità organizzativa vengono rimossi. Se sposti un account all'esterno di un'unità organizzativa registrata, AWS Control Tower rimuove tutte le linee di base e i controlli distribuiti.

Controlla il comportamento quando gli account vengono spostati tra unità organizzative, senza registrazione automatica

Quando si sposta un account tra le unità organizzative, i controlli per l'unità organizzativa di destinazione vengono applicati a account. Tuttavia, i controlli applicati all'account dalla precedente unità organizzativa non lo sono rimosso. L'esatto comportamento dei controlli è specifico per l'implementazione di controlli attivi sulla precedente unità organizzativa e sull'unità organizzativa di destinazione.

- Per i controlli implementati con AWS Config regole: i controlli dell'unità organizzativa precedente non vengono rimossi. Questi controlli devono essere rimossi manualmente.
- Per i controlli implementati con SCP: i SCP-based controlli dell'unità organizzativa precedente sono rimosso. I SCP-based controlli per l'unità organizzativa di destinazione entrano in vigore su questo account.
- Per i controlli implementati con CloudFormation hook: questo comportamento dipende dallo stato dei controlli nella nuova unità organizzativa.
 - Se l'unità organizzativa di destinazione non ha controlli basati su hook attivi: la vecchia i controlli rimangono attivi per l'account spostato, a meno che non vengano rimossi manualmente.
 - Se l'unità organizzativa di destinazione ha i controlli hook attivi: i vecchi controlli sono vengono rimossi e i controlli nell'unità organizzativa di destinazione vengono applicati a account.

Modificare l'indirizzo email di un account registrato

Per modificare l'indirizzo email di un account AWS Control Tower registrato, segui la procedura descritta in questa sezione.

Modifica degli indirizzi email degli account di gestione

Per modificare l'indirizzo email di un account di AWS gestione, accedi come utente root con autorizzazioni di amministratore.

Cambia l'indirizzo email utilizzando AWS Organizations

1. Per istruzioni sull'aggiornamento dell'indirizzo e-mail dell'utente root, consulta [Aggiornare l'indirizzo e-mail dell'utente root per un account membro](#) nella Guida di riferimento per la gestione degli AWS account.
2. Dopo aver aggiornato l'indirizzo email, aggiorna l'account in AWS Control Tower. Questo aggiornamento associa il nuovo indirizzo e-mail all'account in AWS Control Tower. Se si aggiorna l'account tramite il prodotto fornito da Service Catalog, specifica il vecchio indirizzo email come valore per il `AccountEmail` parametro.

Modificare l'indirizzo e-mail utilizzando le credenziali dell'utente root

1. Recupera la password dell'utente root per l'account. Per istruzioni sul recupero di una password persa, vedi [Come posso recuperare una AWS password persa o dimenticata?](#)
2. Accedi all'account con la password dell'utente root.
3. Cambia l'indirizzo email come faresti per qualsiasi altro Account AWS indirizzo e attendi che la modifica abbia effetto AWS Organizations. Potresti riscontrare un ritardo durante il completamento dell'aggiornamento della modifica dell'indirizzo email.
4. Dopo aver aggiornato l'indirizzo email, aggiorna l'account in AWS Control Tower. Questo aggiornamento associa il nuovo indirizzo e-mail all'account in AWS Control Tower. Se si aggiorna l'account tramite il prodotto fornito da Service Catalog, specifica il vecchio indirizzo email come valore per il `AccountEmail` parametro.

Modificare il nome di un account registrato

Segui la procedura descritta in questa sezione per modificare il nome di un account AWS Control Tower registrato.

 Note

Per modificare il nome di un account AWS amministratore, devi disporre delle autorizzazioni di amministratore ed essere loggato come utente root dell'account.

Per modificare il nome di un account creato da AWS Control Tower, utilizzando AWS Organizations console o API

- Segui le [istruzioni disponibili](#) nella Guida di riferimento per la gestione degli AWS account.

Metodo alternativo per modificare il nome di un account creato da AWS Control Tower

1. Recupera la password principale dell'account. Puoi seguire i passaggi descritti in questo articolo, [Come posso recuperare una AWS password persa o dimenticata?](#)
2. Accedi all'account con la password di root.
3. Nella AWS Billing console, vai alla pagina delle impostazioni dell'account.
4. Cambia il nome nelle impostazioni dell'account, come faresti per qualsiasi altro Account AWS.
5. AWS Control Tower si aggiorna automaticamente per riflettere la modifica del nome. Questo aggiornamento non si rifletterà nel prodotto fornito in AWS Service Catalog.

Configura Account Factory con le impostazioni di Amazon Virtual Private Cloud

Account Factory ti consente di creare linee di base e opzioni di configurazione preapprovate per gli account della tua organizzazione. Puoi configurare ed effettuare il provisioning di nuovi account tramite AWS Service Catalog.

Nella pagina Account Factory, puoi visualizzare un elenco delle unità organizzative (OU) e il relativo stato nell'elenco delle autorizzazioni. Per impostazione predefinita, tutte le OU sono incluse nell'elenco dei valori ammessi, il che significa che è possibile assegnarle agli account. È possibile disattivare determinate unità organizzative per il provisioning degli account tramite AWS Service Catalog.

Puoi visualizzare le opzioni di configurazione di Amazon VPC disponibili per i tuoi utenti finali quando effettuano il provisioning di nuovi account.

Per configurare le impostazioni di Amazon VPC in Account Factory

1. In qualità di amministratore del cloud centrale, accedi alla console AWS Control Tower con le autorizzazioni di amministratore nell'account di gestione.
 2. Dal lato sinistro della dashboard, seleziona **Account Factory** per accedere alla pagina di configurazione della rete di Account Factory. Qui è possibile accedere alle impostazioni di rete predefinite visualizzate. Per modificare, seleziona **Modifica** e visualizza la versione modificabile delle impostazioni di configurazione di rete di Account Factory.
 3. È possibile modificare ogni campo delle impostazioni predefinite in base alle esigenze. Scegli le opzioni di configurazione VPC che desideri impostare per tutti i nuovi account Account Factory che gli utenti finali potrebbero creare e inserisci le tue impostazioni nei campi.
- Scegli **disabilitato** o **abilitato** per creare una sottorete pubblica in Amazon VPC. Per impostazione predefinita, la sottorete accessibile da Internet non è consentita.

Note

Se si imposta la configurazione VPC di Account Factory in modo che le sottoreti pubbliche siano abilitate durante il provisioning di un nuovo account, Account Factory configura Amazon VPC per creare un [gateway NAT](#). Ti verrà addebitato l'utilizzo da parte di Amazon VPC. Per ulteriori informazioni, consulta [Prezzi di VPC](#).

- Scegli il numero massimo di sottoreti private in Amazon VPC dall'elenco. Per impostazione predefinita, è selezionato 1. Il numero massimo di sottoreti private consentite è 2 per zona di disponibilità.
- Inserire l'intervallo di indirizzi per creare i VPC dell'account. Il valore deve essere sotto forma di blocco Classless Inter-Domain Routing (CIDR) (ad esempio 172.31.0.0/16). Questo blocco CIDR fornisce l'intervallo complessivo di indirizzi IP di sottorete per il VPC che Account Factory crea per il tuo account. All'interno del VPC, le sottoreti vengono assegnate automaticamente dall'intervallo specificato e hanno dimensioni uguali. Per impostazione predefinita, le sottoreti all'interno del VPC non si sovrappongono. Tuttavia, gli intervalli di indirizzi IP delle sottoreti nei VPC di tutti gli account assegnati potrebbero sovrapporsi.
- Quando si effettua il provisioning di un account, scegliere una regione o tutte le regioni per creare un VPC. Per impostazione predefinita, sono selezionate tutte le regioni disponibili.
- Dall'elenco, scegliere il numero di zone di disponibilità per configurare le sottoreti in ciascun VPC. Il numero predefinito e consigliato è 3.

- Selezionare Salva.

Puoi impostare queste opzioni di configurazione per creare nuovi account che non includono un VPC. Consulta la [procedura dettagliata](#).

Annulla la registrazione di un account

Se hai creato un account in Account Factory o ne hai registrato uno Account AWS e non desideri più che sia gestito da AWS Control Tower in una zona di destinazione, puoi annullare la registrazione dell'account dalla console AWS Control Tower.

Quando annulli la registrazione di un account AWS Control Tower, tutte le risorse fornite da AWS Control Tower vengono rimosse, inclusi i controlli e i progetti. L'account viene spostato da qualsiasi unità organizzativa di AWS Control Tower e nell'area principale. L'account non fa più parte di un'unità organizzativa registrata e non è più soggetto agli SCP di AWS Control Tower. Puoi chiudere l'account tramite AWS Organizations.

Per annullare la registrazione di un account registrato dalla console AWS Control Tower

1. Apri la console AWS Control Tower nel tuo browser web all'indirizzo <https://console.aws.amazon.com/controltower>
2. Nel riquadro di navigazione a sinistra, scegli Organizzazione.
3. Nella pagina Organizzazione, espandi l'unità organizzativa che contiene l'account selezionando il pulsante + vicino all'unità organizzativa.
4. Seleziona l'account e quindi scegli Annulla gestione.

Note

Attendi che lo stato dell'account venga visualizzato Non registrato.

Se l'account non ti serve più, chiudilo. Per ulteriori informazioni sulla chiusura AWS degli account, vedere [Chiusura di un account](#) nella Guida AWS Billing per l'utente

Annulla la registrazione di un account quando la registrazione automatica è attiva

Se la funzionalità di registrazione automatica è attiva nella pagina Impostazioni, puoi anche annullare la registrazione di un account spostandolo in un'unità organizzativa non

registrata in AWS Control Tower. Tutte le risorse AWS Control Tower vengono rimosse. Tieni presente che non annulli accidentalmente l'account in questo modo. Tuttavia, puoi registrare nuovamente l'account restituendolo all'unità organizzativa.

Quando si annulla la registrazione di un account personalizzato, AWS Control Tower rimuove le risorse distribuite nella zona di destinazione e tutte le altre risorse create da AWS Control Tower all'interno dell'account. AWS Control Tower rimuove anche il `AWSControlTowerExecution` ruolo, anche se è stato aggiunto manualmente. La rimozione di questo ruolo è in linea con il principio del privilegio minimo, poiché un ruolo di esecuzione del servizio non deve rimanere in un account non gestito.

Dopo aver annullato la registrazione dell'account, puoi chiuderlo tramite [AWS Organizations](#)

Note

Un account non registrato non viene chiuso o eliminato. Quando l'account è stato annullato, l'utente IAM Identity Center selezionato al momento della creazione dell'account in Account Factory dispone ancora dell'accesso amministrativo all'account. Se non desideri che questo utente abbia accesso amministrativo, devi modificare questa impostazione in IAM Identity Center aggiornando l'account in Account Factory e cambiando l'indirizzo email dell'utente di IAM Identity Center per l'account. Per ulteriori informazioni, consulta [Aggiorna e sposta gli account con AWS Control Tower](#).

Procedura guidata: video

Questo video (3:25) descrive come rimuovere un account da AWS Control Tower, ottenere l'accesso root all'account e infine chiudere il Account AWS. Puoi anche chiudere un account con [un' AWS Organizations API](#). Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sulla chiusura di un account in AWS Control Tower.](#)

Chiudi un account creato in Account Factory

Gli account creati in Account Factory sono Account AWS. Per informazioni sulla chiusura Account AWS, consulta [Chiusura di un account](#) nella Guida di riferimento per la gestione degli [AWS account](#)

 Note

Chiudere un account non Account AWS equivale ad annullare la registrazione di un account da AWS Control Tower: si tratta di azioni separate. È necessario annullare la registrazione dell'account prima di chiuderlo.

Chiudi un account membro di AWS Control Tower tramite AWS Organizations

Puoi chiudere gli account dei membri di AWS Control Tower dall'account di gestione della tua organizzazione senza dover accedere a ciascun account membro individualmente con le credenziali di AWS Organizations root, tramite. Tuttavia, non puoi chiudere il tuo account di gestione in questo modo.

Quando chiami l' AWS Organizations [CloseAccountAPI](#) o chiudi un account nella AWS Organizations console, l'account membro rimane isolato per 90 giorni, come qualsiasi altro Account AWS. L'account mostra lo stato Sospeso in AWS Control Tower e AWS Organizations. Se si tenta di utilizzare l'account durante i 90 giorni, AWS Control Tower restituisce un messaggio di errore.

 Note

Se un'unità organizzativa ha sospeso gli account, EnabledControl le operazioni relative ai controlli regionali sulla destinazione falliranno.

Prima della scadenza dei 90 giorni, puoi ripristinare l'account membro, come puoi fare con qualsiasi altro Account AWS. Trascorsi i 90 giorni, i record dell'account vengono rimossi.

Ti consigliamo, come best practice, di annullare la registrazione di un account membro prima di chiuderlo. Se chiudi un account membro senza prima annullarne la gestione, AWS Control Tower mostra lo stato dell'account come Sospeso, ma anche come Iscritto. Di conseguenza, se tenti di accedere all'unità organizzativa Re-register dell'account durante quel periodo di 90 giorni, AWS Control Tower genera un messaggio di errore. L'account sospeso blocca essenzialmente le azioni di nuova registrazione con un errore di verifica preliminare. Se rimuovi l'account dall'unità organizzativa, puoi farlo Re-register dall'unità organizzativa, ma AWS potresti generare un errore relativo a un metodo di pagamento mancante per l'account. Per ovviare a questo vincolo, crea un'altra unità organizzativa e sposta l'account in tale unità organizzativa prima di provare a registrarti nuovamente. Ti consigliamo di denominare questa unità organizzativa sospesa.

Note

Se non annulli la registrazione dell'account prima di chiuderlo, devi eliminare il prodotto fornito dall'account al AWS Service Catalog termine di questi 90 giorni.

Per ulteriori informazioni, consulta la AWS Organizations documentazione sull'API. [CloseAccount](#)

Considerazioni sulle risorse per Account Factory

Quando viene effettuato il provisioning di un account con Account Factory, all'interno dell'account vengono create AWS le seguenti risorse.

AWS servizio	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-*(Non implementato nella versione 3.0 e successive della zona di atterraggio)
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-*
		StackSet-AWSControlTowerBP-BASELINE-ROLES-*
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*

AWS servizio	Tipo di risorsa	Nome risorsa
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
AWS Config	Canale di consegna	aws-controltower-BaselineConfigDeliveryChannel
AWS Config	Registratore	aws-controltower-BaselineConfigRecorder
Amazon CloudWatch	CloudWatch Registri	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole(Non implementato nella versione 3.0 e successive della zona di atterraggio) aws-controltower-ConfigRecorderRole(Non implementato nella versione 2.8 e successive della zona di atterraggio) aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Argomenti	aws-controltower-SecurityNotifications

AWS servizio	Tipo di risorsa	Nome risorsa
AWS Lambda	Applicazioni	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funzioni	aws-controltower-NotificationForwarder
Amazon EventBridge	Regola	AWSControlTowerManagedRule
Amazon EventBridge	Regola	aws-controltower-ConfigComplianceChangeEventRule

Personalizza gli account con Account Factory Customization (AFC)

Note

La fornitura, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) AWSControlTowerBaseline abilitata. Se un'unità organizzativa non è AWSControlTowerBaseline abilitata, puoi attivare la registrazione automatica dell'account o utilizzare delle ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su tale unità organizzativa per registrare gli account. Per i dettagli di, vedere:.. AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

AWS Control Tower ti consente di personalizzare nuove ed esistenti Account AWS quando esegui il provisioning delle loro risorse dalla console AWS Control Tower. Dopo aver impostato la personalizzazione di Account Factory, AWS Control Tower automatizza questo processo per il provisioning futuro, in modo da non dover mantenere alcuna pipeline. Gli account personalizzati sono disponibili per l'uso subito dopo il provisioning delle risorse.

Effettua il provisioning di nuovi account con blueprint

Il provisioning degli account personalizzati viene eseguito in AWS Control Tower Account Factory, tramite CloudFormation modelli o con Terraform. Definirai un modello che funge da modello di

account personalizzato. Il tuo blueprint descrive le risorse e le configurazioni specifiche necessarie per il provisioning di un account. Pre-defined Sono disponibili anche i blueprint, creati e gestiti dai AWS partner. Per ulteriori informazioni sui blueprint gestiti dai partner, consulta la Getting Started Library. [AWS Service Catalog](#)

Applica i blueprint agli account esistenti

Puoi applicare blueprint personalizzati agli account esistenti, inoltre, seguendo la procedura di aggiornamento dell'account nella console AWS Control Tower. Per informazioni dettagliate, vedi [Aggiorna l'account nella console](#).

Definizione: il tuo account hub

I blueprint del tuo account sono archiviati in un Account AWS, che per i nostri scopi viene definito account hub. I blueprint vengono archiviati sotto forma di un prodotto del Service Catalog. Chiamiamo questo prodotto un progetto, per distinguerlo da qualsiasi altro prodotto del Service Catalog. Per saperne di più su come creare prodotti Service Catalog, vedi [Creazione di prodotti](#) nella Guida per l'AWS Service Catalog amministratore.

Note

AWS Control Tower contiene controlli proattivi che monitorano CloudFormation le risorse in AWS Control Tower. Facoltativamente, puoi attivare questi controlli nella tua zona di atterraggio. Quando applichi i controlli proattivi, questi controllano che le risorse che stai per distribuire sui tuoi account siano conformi alle politiche e alle procedure dell'organizzazione. Per ulteriori informazioni sui controlli proattivi, consulta Controlli proattivi. <https://docs.aws.amazon.com/controltower/latest/userguide/proactive-controls.html>

Per ulteriori informazioni sull'utilizzo di AFC, consulta [Automatizzare la personalizzazione degli account utilizzando Account Factory Customization in AWS Control Tower](#).

Prerequisiti

Prima di iniziare a creare account personalizzati con AWS Control Tower Account Factory, devi disporre di un ambiente di destinazione AWS Control Tower distribuito e di un'unità organizzativa (OU) registrata presso AWS Control Tower, dove verranno collocati gli account appena creati.

Preparazione per la personalizzazione

- Designare un account hub: puoi creare un nuovo account che funga da account hub oppure puoi utilizzarne uno esistente. Account AWS Ti consigliamo vivamente di non utilizzare l'account di gestione di AWS Control Tower come account hub blueprint.
- Aggiungi il ruolo necessario: se intendi iscriverti Account AWS ad AWS Control Tower e personalizzarli, devi prima aggiungere il `AWSControlTowerExecution` ruolo a tali account, come faresti per qualsiasi altro account che stai registrando in AWS Control Tower.
- Configurazione dei blueprint dei partner (opzionale): se prevedi di utilizzare blueprint dei partner con requisiti di abbonamento al marketplace, devi configurarli dal tuo account di gestione di AWS Control Tower prima di distribuire i blueprint dei partner come blueprint di personalizzazione dell'account factory.

Argomenti

- [Configura per la personalizzazione](#)
- [Crea un account personalizzato partendo da un blueprint](#)
- [Personalizza gli account con AFC man mano che li registri](#)
- [Aggiungi un blueprint a un account AWS Control Tower](#)
- [Aggiorna un blueprint](#)
- [Rimuovi un blueprint da un account](#)
- [Progetti dei partner](#)
- [Considerazioni sulle personalizzazioni di Account Factory \(AFC\)](#)
- [In caso di errore del blueprint](#)
- [Personalizzazione del documento programmatico per i progetti AFC in base a CloudFormation](#)
- [Sono necessarie autorizzazioni aggiuntive per creare un Terraform-based prodotto Service Catalog](#)
- [Transizione al AWS Service Catalog Tipo di prodotto esterno](#)

Configura per la personalizzazione

Le sezioni successive descrivono i passaggi per configurare Account Factory per il processo di personalizzazione. Ti consigliamo di configurare l'amministratore [delegato](#) per l'account hub prima di iniziare questi passaggi.

Riepilogo

- Fase 1: Crea il ruolo richiesto. Crea un ruolo IAM che conceda l'autorizzazione ad AWS Control Tower di accedere all'account (hub), in cui sono archiviati i prodotti del Service Catalog, chiamati anche blueprint.
- Fase 2. Crea il prodotto. AWS Service Catalog Crea il AWS Service Catalog prodotto (chiamato anche «prodotto modello») di cui avrai bisogno per creare le basi dell'account personalizzato.
- Fase 3. Rivedi il tuo progetto personalizzato. Ispeziona il AWS Service Catalog prodotto (progetto) che hai creato.
- Fase 4. Richiama il tuo progetto per creare un account personalizzato. Inserisci le informazioni sul modello di prodotto e le informazioni sul ruolo nei campi appropriati in Account Factory, nella console AWS Control Tower, durante la creazione dell'account.

Passaggio 1. Crea il ruolo richiesto

Prima di iniziare a personalizzare gli account, devi configurare un ruolo che contenga una relazione di fiducia tra AWS Control Tower e il tuo account hub. Se assunto, il ruolo concede ad AWS Control Tower l'accesso per amministrare le risorse nell'account hub. Il ruolo deve essere denominato. `AWSControlTowerBlueprintAccess`

AWS Control Tower assume questo ruolo per creare una risorsa di portafoglio per tuo conto AWS Service Catalog, quindi aggiungere il tuo progetto come prodotto Service Catalog a questo portafoglio e quindi condividere questo portafoglio e il tuo progetto con il tuo account membro durante il provisioning dell'account.

Creerai il `AWSControlTowerBlueprintAccess` ruolo, come spiegato nelle sezioni seguenti. Puoi configurare il ruolo in un account registrato o non registrato.

 Accedi alla console IAM per configurare il ruolo richiesto.

Per configurare il `AWSControlTowerBlueprintAccess` ruolo in un account AWS Control Tower registrato

1. Effettua la federazione o accedi come principale nell'account di gestione di AWS Control Tower.

2. Dal responsabile federato nell'account di gestione, assumi o cambia ruolo al `AWSControlTowerExecution` ruolo nell'account AWS Control Tower registrato che scegli come account hub blueprint.
3. Dal `AWSControlTowerExecution` ruolo nell'account AWS Control Tower registrato, crea il `AWSControlTowerBlueprintAccess` ruolo con le autorizzazioni appropriate e le relazioni di fiducia.

 Important

Per rispettare le linee guida sulle AWS best practice, è importante uscire dal `AWSControlTowerExecution` ruolo subito dopo averlo creato.

`AWSControlTowerBlueprintAccess`

Per evitare modifiche involontarie alle risorse, il `AWSControlTowerExecution` ruolo è destinato esclusivamente a AWS Control Tower.

Se il tuo account Blueprint Hub non è registrato in AWS Control Tower, il `AWSControlTowerExecution` ruolo non esisterà nell'account e non è necessario assumerlo prima di continuare con la configurazione del ruolo. `AWSControlTowerBlueprintAccess`

Per configurare il `AWSControlTowerBlueprintAccess` ruolo in un account membro non registrato

1. Effettua la federazione o accedi come principale nell'account che desideri designare come account hub, utilizzando il metodo che preferisci.
2. Una volta effettuato l'accesso come principale nell'account, crea il `AWSControlTowerBlueprintAccess` ruolo con le autorizzazioni appropriate e le relazioni di fiducia.

Il `AWSControlTowerBlueprintAccess` ruolo deve essere impostato per concedere la fiducia a due titolari:

- Il principale (utente) che esegue AWS Control Tower nell'account di gestione di AWS Control Tower.
- Il ruolo indicato `AWSControlTowerAdmin` nell'account di gestione di AWS Control Tower.

Ecco un esempio di politica di fiducia, simile a quella che dovrai includere per il tuo ruolo. Questa politica dimostra la migliore pratica di concessione dell'accesso con privilegi minimi. Quando crei la tua policy, sostituisci il termine *YourManagementAccountId* con l'ID account effettivo del tuo account di gestione AWS Control Tower e sostituisci il termine *YourControlTowerUserRole* con l'identificatore del ruolo IAM per il tuo account di gestione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/service-role/AWSControlTowerAdmin",
          "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Politica delle autorizzazioni richieste

AWS Control Tower richiede che la policy gestita `AWSServiceCatalogAdminFullAccess` denominata sia associata al `AWSControlTowerBlueprintAccess` ruolo. Questa policy fornisce le autorizzazioni necessarie quando consente ad AWS Control Tower di amministrare il portafoglio e le risorse dei AWS Service Catalog prodotti. AWS Service Catalog Puoi allegare questa policy quando crei il ruolo nella console IAM.

Potrebbero essere necessarie autorizzazioni aggiuntive

- Se archivi i tuoi blueprint in Amazon S3, AWS Control Tower richiede anche la politica di `AmazonS3ReadOnlyAccess` autorizzazione per il ruolo. `AWSControlTowerBlueprintAccess`

- Il tipo di prodotto AWS Service Catalog Terraform richiede l'aggiunta di alcune autorizzazioni aggiuntive alla politica IAM personalizzata di AFC, se non si utilizza la politica di amministrazione predefinita. Queste sono necessarie in aggiunta alle autorizzazioni necessarie per creare le risorse definite nel modello terraform.

Passaggio 2. Crea il AWS Service Catalog product

Per creare un AWS Service Catalog prodotto, segui i passaggi indicati in [Creazione di prodotti](#) nella Guida per l'AWS Service Catalog amministratore. Aggiungerai il blueprint del tuo account come modello quando crei il AWS Service Catalog prodotto.

Important

A seguito HashiCorp dell'aggiornamento delle licenze Terraform, è stato AWS Service Catalog modificato il supporto per i prodotti Terraform Open Source e fornito i prodotti a un nuovo tipo di prodotto, chiamato External. Per saperne di più sugli effetti di questa modifica su AFC, incluso come aggiornare i blueprint degli account esistenti con il tipo di prodotto esterno, [consulta la sezione Transizione al tipo di prodotto esterno](#).

Riepilogo dei passaggi per creare un progetto

- Crea o scarica un CloudFormation modello o un file di configurazione Terraform tar.gz che diventerà il modello del tuo account. Alcuni esempi di template sono riportati più avanti in questa sezione.
- Accedi al sito in Account AWS cui archivi i tuoi blueprint di Account Factory (a volte chiamato account hub).
- Accedi alla AWS Service Catalog console. Scegli Elenco prodotti, quindi scegli Carica nuovo prodotto.
- Nel riquadro Dettagli del prodotto, inserisci i dettagli del prodotto modello, ad esempio nome e descrizione.
- Seleziona Usa un file modello, quindi seleziona Scegli file. Seleziona o incolla il modello o il file di configurazione che hai sviluppato o scaricato per utilizzarlo come progetto.
- Scegli Crea prodotto nella parte inferiore della pagina della console.

Puoi scaricare un CloudFormation modello dal repository dell'architettura AWS Service Catalog di riferimento. [Un esempio tratto da quel repository aiuta a configurare un piano di backup per le risorse.](#)

Ecco un modello di esempio, per un'azienda fittizia chiamata Best Pets. Aiuta a stabilire una connessione al database degli animali domestici.

Resources:

ConnectionStringGeneratorLambdaRole:

Type: AWS::IAM::Role

Properties:

AssumeRolePolicyDocument:

Version: "2012-10-17"

Statement:

- Effect: Allow

Principal:

Service:

- lambda.amazonaws.com

Action:

- "sts:AssumeRole"

ConnectionStringGeneratorLambda:

Type: AWS::Lambda::Function

Properties:

FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]

Description: Retrieves the connection string for this account to access the Pet
Database

Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn

Runtime: nodejs22.x

Handler: index.handler

Timeout: 5

Code:

ZipFile: >

```
export const handler = async (event, context) => {
  const awsAccountId = context.invokedFunctionArn.split(":")[4]
  const connectionString= "fake connection for account " + awsAccountId;
  const response = {
    statusCode: 200,
    body: connectionString
  };
  return response;
};
```

ConnectionString:

```
Type: Custom::ConnectionStringGenerator
Properties:
  ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

PetDatabaseConnectionString:
  DependsOn: ConnectionString
  # For example purposes we're using SSM parameter store.
  # In your template, use secure alternatives to store
  # sensitive values such as connection strings.
  Type: AWS::SSM::Parameter
  Properties:
    Name: pet-database-connection-string
    Description: Connection information for the BestPets pet database
    Type: String
    Value: !GetAtt ConnectionString.Value
```

Fase 3. Rivedi il tuo progetto personalizzato

Puoi visualizzare il tuo blueprint nella AWS Service Catalog console. Per ulteriori informazioni, vedere [Managing products](#) nella Service Catalog Administrator Guide.

Passaggio 4. Richiama il tuo progetto per creare un account personalizzato

Quando segui il flusso di lavoro per la creazione di un account nella console AWS Control Tower, vedrai una sezione opzionale in cui puoi inserire informazioni sul blueprint da utilizzare per personalizzare gli account.

Prerequisiti

È necessario configurare l'account dell'hub di personalizzazione e aggiungere almeno un blueprint (prodotto Service Catalog) prima di poter inserire tali informazioni nella console AWS Control Tower e iniziare a fornire account personalizzati.

Crea o aggiorna un account personalizzato nella console AWS Control Tower.

1. Inserisci l'ID dell'account che contiene i tuoi blueprint.
2. Da quell'account, seleziona un prodotto Service Catalog esistente (blueprint esistente).
3. Seleziona la versione corretta del blueprint (prodotto Service Catalog), se hai più di una versione.

4. (Facoltativo) È possibile aggiungere o modificare una politica di fornitura del blueprint a questo punto del processo. La policy di provisioning del blueprint è scritta in JSON e associata a un ruolo IAM, quindi può fornire le risorse specificate nel modello del blueprint. AWS Control Tower crea questo ruolo nell'account membro in modo che Service Catalog possa distribuire risorse utilizzando stack set. CloudFormation Il ruolo è denominato `AWSControlTower-BlueprintExecution-bp-xxxx`. La `AdministratorAccess` policy viene applicata qui per impostazione predefinita.
5. Scegli la Regione AWS o le regioni in cui desideri distribuire gli account in base a questo blueprint.
6. Se il blueprint contiene parametri, puoi inserire i valori dei parametri in campi aggiuntivi nel flusso di lavoro di AWS Control Tower. I valori aggiuntivi possono includere: un nome di GitHub repository, un GitHub ramo, un nome di cluster Amazon ECS e un' GitHub identità per il proprietario del repository.
7. Puoi personalizzare gli account in un secondo momento seguendo la procedura di aggiornamento dell'account, se l'account hub o i blueprint non sono ancora pronti.

Per ulteriori dettagli, consultare [Crea un account personalizzato partendo da un blueprint](#).

Crea un account personalizzato partendo da un blueprint

Dopo aver creato progetti personalizzati, puoi iniziare a creare account personalizzati in AWS Control Tower account factory.

Segui questi passaggi per distribuire un blueprint personalizzato quando ne crei uno nuovo AWS account:

1. Vai a AWS Control Tower nel Console di gestione AWS.
2. Seleziona **Account factory** e **Crea account**.
3. Inserisci i dettagli dell'account come il nome dell'account e l'indirizzo email.
4. Configura i dettagli di IAM Identity Center con indirizzo email e nome utente.
5. Seleziona un'unità organizzativa registrata a cui verrà aggiunto il tuo account.
6. Espandi la sezione di personalizzazione dell'account di fabbrica.
7. Inserisci l'ID dell'account Blueprint Hub che contiene i prodotti del Service Catalog e scegli **Convalida**. Per ulteriori informazioni su un account Blueprint Hub, consulta. [Personalizza gli account con Account Factory Customization \(AFC\)](#)

8. Seleziona il menu a discesa che contiene tutti i blueprint dall'elenco di prodotti del Service Catalog (tutti i blueprint personalizzati e dei partner). Scegli un blueprint e la versione corrispondente da distribuire.
9. Se il blueprint contiene parametri, questi campi vengono visualizzati per essere compilati. I valori predefiniti sono precompilati.
10. Infine, seleziona dove distribuire il tuo blueprint: `Home Region` o `Tutte le regioni governate`. Le risorse globali, come `Route 53` o `IAM`, potrebbero dover essere distribuite solo in una singola regione. Le risorse regionali, come le istanze Amazon EC2 o i bucket Amazon S3, potrebbero essere distribuite in tutte le regioni governate.
11. Dopo aver completato tutti i campi, seleziona `Crea account`.

Note

I blueprint creati con Terraform possono essere distribuiti in una sola regione, non in più regioni.

Puoi visualizzare lo stato di avanzamento della fornitura del tuo account nella pagina `Organizzazione`. Una volta completato il provisioning dell'account, le risorse specificate dal blueprint sono già distribuite al suo interno. Per visualizzare i dettagli dell'account e del blueprint, vai alla pagina `Dettagli dell'account`.

Personalizza gli account con AFC man mano che li registri

Per registrare e personalizzare gli account nella console AWS Control Tower.

1. Accedi alla console AWS Control Tower e seleziona `Organization` dalla barra di navigazione a sinistra.
2. Vedrai un elenco dei tuoi account disponibili. Identifica l'account che desideri registrare con un blueprint personalizzato. La colonna `Stato dell'account` deve indicare lo stato dell'account `non registrato`.
3. Seleziona il pulsante di opzione a sinistra dell'account e scegli il menu a discesa `Azioni`, in alto a destra dello schermo. Qui selezionerai l'opzione `Iscriviti`.
4. Completa la sezione di configurazione degli accessi con le informazioni sull'IAM Identity Center dell'account.
5. Seleziona l'unità organizzativa registrata di cui il tuo account diventerà membro.

6. Completa la sezione di personalizzazione dell'account di fabbrica seguendo gli stessi passaggi descritti nella procedura 7-12 della procedura di creazione dell'account. Per ulteriori informazioni, consulta [Provision Account Factory accounts with. AWS Service Catalog](#)

Puoi visualizzare lo stato dei progressi del tuo account nella pagina **Organizzazione**. Una volta completata la registrazione dell'account, le risorse specificate dal blueprint sono già distribuite al suo interno.

Aggiungi un blueprint a un account AWS Control Tower

Per aggiungere un blueprint a un account membro di AWS Control Tower esistente, segui il flusso di lavoro di aggiornamento dell'account nella console AWS Control Tower e scegli un nuovo blueprint da aggiungere all'account. Per ulteriori informazioni, consulta [Aggiornare e spostare gli account Account Factory con AWS Control Tower o con. AWS Service Catalog](#)

Note

Se aggiungi un nuovo blueprint a un account, il blueprint esistente viene sovrascritto.

Note

È possibile distribuire un blueprint per account AWS Control Tower.

Aggiorna un blueprint

Le seguenti procedure descrivono come aggiornare i blueprint personalizzati e come distribuirli.

Per aggiornare i tuoi blueprint personalizzati

1. Aggiorna il CloudFormation modello o il file Terraform tar.gz (blueprint) con le nuove configurazioni.
2. Salva il blueprint aggiornato come nuova versione in. AWS Service Catalog

Per distribuire il blueprint aggiornato

1. Accedi alla pagina **Organizzazione** nella console AWS Control Tower.

2. Filtra la pagina dell'organizzazione per nome e versione del blueprint.
3. Segui la procedura di aggiornamento dell'account e implementa la versione più recente del blueprint nel tuo account.

Se l'aggiornamento di un blueprint non ha esito positivo

AWS Control Tower consente l'aggiornamento dei blueprint quando il prodotto fornito è nello stato in cui è stato effettuato il provisioning. AVAILABLE Se il prodotto sottoposto a provisioning è in uno TAINTED stato, l'aggiornamento avrà esito negativo. Consigliamo la seguente soluzione alternativa:

1. Nella AWS Service Catalog console, aggiorna manualmente il prodotto TAINTED fornito per modificarne lo stato. AVAILABLE Per ulteriori informazioni, vedere [Aggiornamento dei prodotti forniti](#).
2. Quindi, segui la procedura di aggiornamento dell'account da AWS Control Tower per correggere l'errore di distribuzione del blueprint.

Consigliamo questo passaggio manuale perché: quando rimuovi un blueprint, può causare la rimozione delle risorse nell'account membro. La rimozione delle risorse può influire sui carichi di lavoro esistenti. Per questo motivo, consigliamo questo metodo anziché il metodo alternativo di aggiornamento di un blueprint, ossia rimuovendo e sostituendo il blueprint originale, soprattutto se si eseguono carichi di lavoro di produzione.

Rimuovi un blueprint da un account

Per rimuovere un blueprint da un account, segui il workflow di aggiornamento dell'account per rimuovere il blueprint e riportare l'account alle configurazioni predefinite di AWS Control Tower.

Quando entri nel flusso di lavoro di aggiornamento dell'account nella console, vedrai che tutti i dettagli dell'account sono compilati e i dettagli di personalizzazione non sono compilati. Se lasci vuoti questi dettagli AFC, AWS Control Tower rimuove il blueprint dall'account. Verrà visualizzato un messaggio di avviso prima dell'inizio dell'azione.

Note

AWS Control Tower aggiunge un blueprint a un account solo se lo selezioni durante il processo di creazione dell'account o di aggiornamento dell'account.

Progetti dei partner

AWS Control Tower Account Factory Customization (AFC) fornisce l'accesso a modelli di personalizzazione predefiniti creati e gestiti dai partner. AWS Questi modelli per i partner ti aiutano a personalizzare i tuoi account per casi d'uso specifici. I blueprint di ciascun partner ti aiutano a creare account personalizzati, preconfigurati per funzionare con le offerte di prodotti di quel particolare partner.

Per visualizzare un elenco completo dei blueprint dei partner di AWS Control Tower, accedi alla [Service Catalog Getting Started Library](#) nella tua console. Cerca il tipo di sorgente `AWS Control Tower Blueprints`.

Considerazioni sulle personalizzazioni di Account Factory (AFC)

- AFC supporta la personalizzazione utilizzando un solo prodotto blueprint. AWS Service Catalog
- I prodotti AWS Service Catalog blueprint devono essere creati nell'account hub e nella stessa regione della regione di origine della zona di destinazione di AWS Control Tower.
- Il ruolo `AWSControlTowerBlueprintAccess` IAM deve essere creato con il nome, le autorizzazioni e la policy di fiducia corretti.
- AWS Control Tower supporta due opzioni di distribuzione per i blueprint: distribuzione solo nella regione di origine o distribuzione in tutte le regioni governate da AWS Control Tower. La selezione delle regioni non è disponibile.
- Quando si aggiorna un blueprint in un account membro, l'ID dell'account blueprint hub e il prodotto AWS Service Catalog blueprint non possono essere modificati.
- AWS Control Tower non supporta la rimozione di un blueprint esistente e l'aggiunta di un nuovo blueprint in un'unica operazione di aggiornamento del blueprint. È possibile rimuovere un blueprint e quindi aggiungerne uno nuovo in operazioni separate.
- AWS Control Tower modifica il comportamento, a seconda che tu stia creando o registrando account personalizzati o account non personalizzati. Se non stai creando o registrando account personalizzati con blueprint, AWS Control Tower crea un prodotto fornito da Account Factory (tramite Service Catalog) nell'account di gestione di AWS Control Tower. Se si specifica la personalizzazione durante la creazione o la registrazione di account con blueprint, AWS Control Tower non crea un prodotto con provisioning Account Factory nell'account di gestione di AWS Control Tower.

In caso di errore del blueprint

Errore durante l'applicazione di un blueprint

Se si verifica un errore durante il processo di applicazione di un blueprint a un account, un nuovo account o un account esistente che stai registrando in AWS Control Tower, la procedura di ripristino è la stessa. L'account esisterà, ma non è personalizzato e non è registrato in AWS Control Tower. Per continuare, segui i passaggi per registrare l'account in AWS Control Tower e aggiungere il blueprint al momento della registrazione.

Errore durante la creazione del ruolo e soluzioni **AWSControlTowerBlueprintAccess** alternative

Quando si crea il **AWSControlTowerBlueprintAccess** ruolo da un account AWS Control Tower, è necessario accedere come principale utilizzando il ruolo. **AWSControlTowerExecution** Se hai effettuato l'accesso come qualsiasi altro utente, l'**CreateRole** operazione viene impedita da un SCP, come mostrato nell'artefatto che segue:

```
{
  "Condition": {
    "ArnNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    }
  },
  "Action": [
    "iam:AttachRolePolicy",
    "iam:CreateRole",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::*:role/aws-controltower-*",
    "arn:aws:iam::*:role/*AWSControlTower*",
  ]
}
```

```
        "arn:aws:iam::*:role/stacksets-exec-*"  
    ],  
    "Effect": "Deny",  
    "Sid": "GRIAMROLEPOLICY"  
}
```

Sono disponibili le seguenti soluzioni alternative:

- (Scelta consigliata) Assumi il `AWSControlTowerExecution` ruolo e crealo.
`AWSControlTowerBlueprintAccess` Se scegli questa soluzione alternativa, assicurati di disconnetterti dal `AWSControlTowerExecution` ruolo subito dopo, per evitare modifiche involontarie alle risorse.
- Accedi a un account non registrato in AWS Control Tower e quindi non soggetto a questo SCP.
- Modifica temporaneamente questo SCP per consentire l'operazione.
- (Fortemente sconsigliato) Usa il tuo account di gestione AWS Control Tower come account hub, in modo che non sia soggetto all'SCP.

Personalizzazione del documento programmatico per i progetti AFC in base a CloudFormation

Quando abiliti un blueprint tramite account factory, AWS Control Tower ordina di crearne uno CloudFormation per tuo conto. StackSet CloudFormation richiede l'accesso al tuo account gestito per creare CloudFormation stack in. StackSet Sebbene disponga CloudFormation già dei privilegi di amministratore nell'account gestito tramite il `AWSControlTowerExecution` ruolo, questo ruolo non è assumibile da. CloudFormation

Come parte dell'abilitazione di un progetto, AWS Control Tower crea un ruolo nell'account membro, che CloudFormation può assumere il completamento delle StackSet attività di gestione. Il modo più semplice per abilitare il tuo blueprint personalizzato tramite account factory è utilizzare una policy all-allow, perché tali policy sono compatibili con qualsiasi modello di blueprint.

Tuttavia, le best practice suggeriscono di limitare le autorizzazioni per CloudFormation l'account di destinazione. Puoi fornire una policy personalizzata, che AWS Control Tower applica al ruolo creato CloudFormation per essere utilizzato. Ad esempio, se il tuo progetto crea un parametro SSM chiamato `something-important`, potresti fornire la seguente policy:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFormationActionsOnStacks",
      "Effect": "Allow",
      "Action": "cloudformation:*",
      "Resource": "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid": "AllowSsmParameterActions",
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParameter",
        "ssm:GetParameters"
      ],
      "Resource": "arn:*:ssm:*:*:parameter/something-important"
    }
  ]
}
```

La `AllowCloudFormationActionsOnStacks` dichiarazione è obbligatoria per tutte le politiche personalizzate AFC; CloudFormation utilizza questo ruolo per creare istanze di stack, pertanto richiede l'autorizzazione per eseguire azioni sugli stack. CloudFormation La `AllowSsmParameterActions` sezione è specifica per il modello da abilitare.

Risolvi i problemi di autorizzazione

Quando abiliti un blueprint con una policy limitata, potresti scoprire che non ci sono autorizzazioni sufficienti per abilitare il blueprint. Per risolvere questi problemi, rivedi il documento della politica e aggiorna le preferenze del blueprint dell'account membro per utilizzare la politica corretta. Per verificare che la policy sia sufficiente per abilitare il blueprint, assicurati che le CloudFormation autorizzazioni siano concesse e che tu possa creare uno stack utilizzando direttamente quel ruolo.

Sono necessarie autorizzazioni aggiuntive per creare un Terraform-based prodotto Service Catalog

Quando si crea un prodotto AWS Service Catalog esterno con un file di configurazione Terraform per AFC, è AWS Service Catalog necessario aggiungere determinate autorizzazioni alla politica IAM personalizzata di AFC, oltre alle autorizzazioni necessarie per creare le risorse definite nel modello. Se scegli la politica di amministrazione completa predefinita, non è necessario aggiungere queste autorizzazioni aggiuntive.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "resource-groups:CreateGroup",
        "resource-groups:ListGroupResources",
        "resource-groups>DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
"s3:ExistingObjectTag/servicecatalog:provisioning": "true"  
  }  
}   
  }  
}   
  ]  
}
```

Per ulteriori informazioni sulla creazione di prodotti Terraform utilizzando il tipo di prodotto esterno in AWS Service Catalog, consulta la [Fase 5: Create launch roles](#) nella Service Catalog Administrator Guide.

Transizione al AWS Service Catalog Tipo di prodotto esterno

AWS Service Catalog ha modificato il supporto per i prodotti Terraform Open Source e i prodotti predisposti con un nuovo tipo di prodotto, chiamato External. Per saperne di più su questa transizione, consulta [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti predisposti al tipo di prodotto esterno](#) nella guida per l'amministratore. AWS Service Catalog

Questa modifica ha effetto sugli account esistenti che hai creato o registrato con la personalizzazione di fabbrica degli account AWS Control Tower. Per passare da questi account al tipo di prodotto esterno, è necessario apportare modifiche sia in AWS Control Tower che AWS Service Catalog in AWS Control Tower.

Per passare al tipo di prodotto esterno

1. Aggiorna il tuo motore di riferimento Terraform esistente per includere AWS Service Catalog il supporto per i tipi di prodotto External e Terraform Open Source. Per istruzioni sull'aggiornamento del tuo Terraform Reference Engine, consulta il Repository. [AWS Service Catalog GitHub](#)
2. In AWS Service Catalog, duplica tutti i prodotti Terraform Open Source (progetti) esistenti, con i duplicati utilizzando il nuovo tipo di prodotto esterno. Non terminare i progetti Terraform Open Source esistenti.
3. In AWS Control Tower, aggiorna ogni account utilizzando un blueprint open source Terraform per utilizzare il nuovo blueprint esterno.
 - a. Per aggiornare un blueprint, devi prima rimuovere completamente il blueprint Terraform Open Source. Per maggiori dettagli, consulta [Rimuovere un progetto da un account](#).

- b. Aggiungi il nuovo blueprint esterno allo stesso account. Per maggiori dettagli, consulta [Aggiungere un blueprint a un account AWS Control Tower](#).
4. Dopo che tutti gli account che utilizzano i blueprint open source Terraform sono stati aggiornati in blueprint esterni, ripristina AWS Service Catalog e chiudi tutti i prodotti che utilizzano Terraform Open Source come tipo di prodotto.
5. In futuro, tutti gli account creati o registrati utilizzando l'account factory customization di AWS Control Tower dovranno fare riferimento ai blueprint utilizzando il tipo di prodotto o External. CloudFormation

Per i blueprint creati utilizzando il tipo di prodotto esterno, AWS Control Tower supporta solo le personalizzazioni degli account che utilizzano modelli Terraform e il motore di riferimento Terraform. Per saperne di più, consulta [Set up for customization](#).

Note

AWS Control Tower non supporta Terraform Open Source come tipo di prodotto per la creazione di nuovi account. Per ulteriori informazioni su queste modifiche, consulta la sezione [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti con provisioning al tipo di prodotto esterno](#) nella guida per l'AWS Service Catalog amministratore. AWS Service Catalog supporterà i clienti durante questa transizione del tipo di prodotto, se necessario. Contatta il rappresentante del tuo account per richiedere assistenza.

Effettua il provisioning degli account con AWS Control Tower Account Factory for Terraform (AFT)

AWS Control Tower Account Factory for Terraform (AFT) adotta un GitOps modello che automatizza il processo di provisioning e aggiornamento degli account in AWS Control Tower.

Con AFT, crei un file Terraform per la richiesta di account, che contiene l'input che richiama il flusso di lavoro AFT. Al termine del provisioning e dell'aggiornamento dell'account, il flusso di lavoro AFT continua eseguendo il framework di provisioning degli account AFT e le fasi di personalizzazione dell'account.

AFT non influisce sulle prestazioni del flusso di lavoro in AWS Control Tower. Se esegui il provisioning di un account tramite AFT o Account Factory, si verifica lo stesso flusso di lavoro di backend.

Prerequisiti

Note

Il provisioning di un account AFT deve essere indirizzato a un'unità organizzativa (OU) `AWSControlTowerBaseline` abilitata in AWS Control Tower. Per i dettagli `AWSControlTowerBaseline`, consulta: [Tipi di base applicabili a livello di unità organizzativa](#).

Quando inizi con AFT, creerai quanto segue:

- In AWS Control Tower, crea l'unità organizzativa e quindi l'account di gestione AFT per il tuo ambiente AFT. Prendi nota dell'ID dell'account, in modo da poterlo inserire nel `main.tf` file in un secondo momento, quando distribuisce AFT con il modulo Terraform. Puoi visualizzare questo ID account nella pagina dei dettagli di AWS Control Tower Control. Per ulteriori informazioni, consulta la documentazione <https://developer.hashicorp.com/terraform/tutorials/aws/aws-control-tower-aft> Terraform.
- Uno o più git repository per il tuo ambiente AFT completamente implementato. Per ulteriori informazioni, consulta [Post-deployment i passaggi per AFT](#).
- Un ambiente AFT completamente implementato. Per ulteriori informazioni, consulta [Panoramica di AWS Control Tower Account Factory for Terraform \(AFT\)](#) e [Deploy AWS Control Tower Account Factory for Terraform \(AFT\)](#). Vedi anche la documentazione [di](#) Terraform.

Tip

Puoi creare l'account di gestione AFT dalla console AWS Control Tower con `Create account`. Per ulteriori informazioni, consulta [Metodi di provisioning](#). Inoltre, facoltativamente, puoi creare una cartella di modelli di account per aiutarti a definire i tuoi account aggiuntivi, nel repository `aft-account-customizations`.

Per gli account registrati tramite Auto Enroll:

- La creazione di nuovi account tramite AFT continua a funzionare normalmente.
- L'importazione di account esistenti richiede passaggi aggiuntivi:
 - Registra l'unità organizzativa per creare i prodotti predisposti necessari prima dell'importazione.
 - Register OU emetterà UpdateManagedAccount eventi CreateManagedAccount e abiliterà le personalizzazioni AFT.

Per informazioni sulle limitazioni Regioni AWS di distribuzione di AFT, vedere e. [Limitazioni e quote in AWS Control Tower](#) [Limitazioni di controllo](#)

La documentazione [Terraform](#) contiene una buona panoramica su come configurare AWS Control Tower Account Factory for Terraform (AFT).

Panoramica di AWS Control Tower Account Factory for Terraform (AFT)

Account Factory for Terraform (AFT) configura una pipeline Terraform per aiutarti a fornire e personalizzare gli account in AWS Control Tower. AFT ti offre il vantaggio del provisioning degli Terraform-based account, consentendoti al contempo di gestire i tuoi account con AWS Control Tower.

Con AFT crei un file Terraform di richiesta di account per ottenere l'input che attiva il flusso di lavoro AFT per il provisioning degli account. Una volta completata la fase di provisioning dell'account, AFT esegue automaticamente una serie di passaggi prima che inizi la fase di personalizzazione dell'account. Per ulteriori informazioni, consulta la pipeline di provisioning degli account [AFT](#).

AFT supporta HCP Terraform, Terraform Enterprise e Terraform Community Edition. Con AFT puoi avviare la creazione dell'account utilizzando un file di input e un semplice `git push` comando e personalizzare account nuovi o esistenti. La creazione dell'account include tutti i vantaggi della governance di AWS Control Tower e le personalizzazioni degli account che ti aiutano a soddisfare le procedure di sicurezza standard e le linee guida di conformità della tua organizzazione.

AFT supporta il tracciamento delle richieste di personalizzazione degli account. Ogni volta che invii una richiesta di personalizzazione dell'account, AFT genera un token di tracciamento univoco che passa attraverso una macchina a AWS Step Functions stati delle personalizzazioni AFT, che registra il token come parte della sua esecuzione. Puoi quindi utilizzare le query di Amazon CloudWatch Logs Insights per cercare intervalli di timestamp e recuperare il token di richiesta. Di conseguenza, puoi visualizzare i payload che accompagnano il token, in modo da poter tracciare la richiesta di personalizzazione dell'account durante l'intero flusso di lavoro AFT. Per informazioni su CloudWatch Logs e Step Functions, consulta quanto segue:

- [Che cos'è Amazon CloudWatch Logs?](#) nella Guida per l'utente di Amazon CloudWatch Logs
- [Che cos'è AWS Step Functions?](#) nella Guida per gli sviluppatori di AWS Step Functions

AFT combina le funzionalità di altri AWS servizi come [Servizi relativi ai componenti](#), per creare un framework, con pipeline che implementano Terraform Infrastructure as Code (IaC). AFT ti consente di:

- Inviare richieste di provisioning e aggiornamento dell'account in un modello GitOps
- Archivia i metadati dell'account e la cronologia degli audit
- Applica tag a livello di account
- Aggiungi personalizzazioni a tutti gli account, a un set di account o a singoli account
- Abilita le opzioni delle funzionalità

AFT crea un account separato, chiamato account di gestione AFT, per implementare le funzionalità AFT. Prima di poter configurare AFT, devi disporre di una zona di atterraggio AWS Control Tower esistente. L'account di gestione AFT non è lo stesso dell'account di gestione AWS Control Tower.

AFT offre flessibilità

- Flessibilità per la tua piattaforma: AFT supporta qualsiasi distribuzione Terraform per l'implementazione iniziale e il funzionamento continuo: Community Edition, Cloud ed Enterprise.
- Flessibilità per il tuo sistema di controllo della versione: supporti AWS CodeCommit AFT e fonti di controllo della versione alternative tramite AWS CodeConnections

AFT offre opzioni di funzionalità

È possibile abilitare diverse opzioni di funzionalità, in base alle migliori pratiche:

- Creazione di un livello di organizzazione per la registrazione degli eventi relativi CloudTrail ai dati
- Eliminazione del VPC predefinito per gli account AWS
- Registrazione degli account con provisioning nel piano Enterprise Support AWS

Note

La pipeline AFT non è destinata all'uso nella distribuzione di risorse, come le istanze Amazon EC2, necessarie agli account per eseguire le applicazioni. È destinato esclusivamente al provisioning e alla personalizzazione automatici degli account AWS Control Tower.

Procedura guidata: video

Questo video (7:33) descrive come distribuire account con AWS Control Tower Account Factory for Terraform. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato del provisioning automatizzato degli account in AWS Control Tower.](#)

Architettura AFT

Ordine delle operazioni

Le operazioni AFT vengono eseguite nell'account di gestione AFT. Per un flusso di lavoro completo per il provisioning dell'account, l'ordine delle fasi da sinistra a destra nel diagramma è il seguente:

1. Le richieste di account vengono create e inviate alla pipeline. Puoi creare e inviare più di una richiesta di account alla volta. Account Factory elabora le richieste in base all'ordine «first in first-out». Per ulteriori informazioni, consulta [Inviare più richieste di account](#).
2. A ogni account viene assegnato un provisioning. Questa fase viene eseguita nell'account di gestione di AWS Control Tower.
3. Le personalizzazioni globali vengono eseguite nelle pipeline create per ogni account venduto.
4. Se le personalizzazioni sono specificate nelle richieste iniziali di provisioning degli account, le personalizzazioni vengono eseguite solo sugli account mirati. Se hai già effettuato il provisioning di un account, devi avviare ulteriori personalizzazioni manualmente nella pipeline dell'account.

AWS Control Tower Account Factory per Terraform: flusso di lavoro per il provisioning degli account

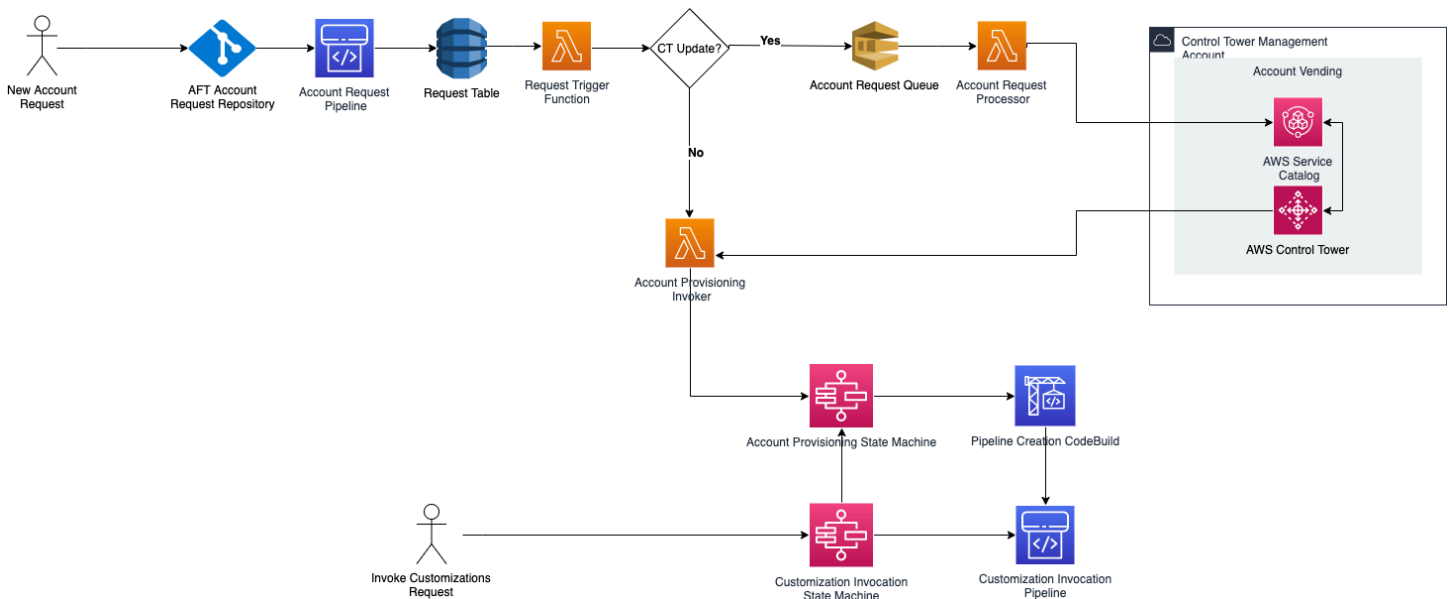


Figura 1: AWS Control Tower Account Factory per Terraform

Costo

Non esistono costi aggiuntivi per AFT. Paghi solo per le risorse distribuite da AFT, i AWS servizi abilitati da AFT e le risorse che distribuisce nel tuo ambiente AFT.

La configurazione AFT predefinita include l'allocazione degli AWS PrivateLink endpoint, per una maggiore protezione e sicurezza dei dati, e un gateway NAT necessario per il supporto. AWS CodeBuild Per informazioni dettagliate sui prezzi di questa infrastruttura, consulta i [AWS PrivateLink prezzi](#) e i prezzi di [Amazon VPC per NAT Gateway](#). Contatta il rappresentante AWS del tuo account per informazioni più specifiche sulla gestione di questi costi. È possibile modificare queste impostazioni predefinite per AFT.

Implementa AWS Control Tower Account Factory per Terraform (AFT)

Questa sezione è dedicata agli amministratori di ambienti AWS Control Tower che desiderano configurare Account Factory for Terraform (AFT) nel loro ambiente esistente. Descrive come configurare un ambiente Account Factory for Terraform (AFT) con un nuovo account di gestione AFT dedicato.

Note

Un modulo Terraform implementa AFT. Questo modulo è disponibile nel [repository AFT](#) su GitHub e l'intero repository AFT è considerato il modulo.

Si consiglia di fare riferimento ai moduli AFT su GitHub invece di clonare il repository AFT. In questo modo è possibile controllare e utilizzare gli aggiornamenti dei moduli non appena sono disponibili.

Per informazioni dettagliate sulle versioni più recenti della funzionalità AWS Control Tower Account Factory for Terraform (AFT), consulta [il file Releases](#) per questo GitHub repository.

Prerequisiti di distribuzione

Prima di configurare e avviare l'ambiente AFT, è necessario disporre delle seguenti risorse:

- Una regione d'origine per la tua landing zone di AWS Control Tower. Per ulteriori informazioni, consulta [How Regioni AWS work with AWS Control Tower](#).
- Una landing zone di AWS Control Tower. Per ulteriori informazioni, consulta [Pianifica la tua landing zone di AWS Control Tower](#).
- Un account di gestione AFT, che puoi fornire in AWS Control Tower o fornire con altri mezzi e registrarlo in AWS Control Tower.
- Una versione e una distribuzione di Terraform. Per ulteriori informazioni, consulta le versioni [Terraform e AFT](#).
- Un provider VCS per il monitoraggio e la gestione delle modifiche al codice e ad altri file. Per impostazione predefinita, AFT utilizza AWS CodeCommit. Per ulteriori informazioni, vedete [Cos'è AWS CodeCommit?](#) nella Guida AWS CodeCommit per l'utente.

Se state distribuendo AFT per la prima volta e non disponete di un CodeCommit repository esistente, dovete scegliere un provider VCS esterno, ad esempio o. GitHub BitBucket Per ulteriori informazioni, consulta [Alternative per il controllo della versione del codice sorgente](#) in AFT.

- Un ambiente di runtime in cui è possibile eseguire il modulo Terraform che installa AFT.
- Opzioni delle funzionalità AFT. Per ulteriori informazioni, vedete [Abilitare le opzioni delle funzionalità](#).

Configura e avvia il tuo AWS Control Tower Account Factory per Terraform

I passaggi seguenti presuppongono che tu abbia familiarità con il flusso di lavoro Terraform. Puoi anche saperne di più sulla distribuzione di AFT seguendo il laboratorio [Introduzione a AFT](#) sul sito Web di AWS Workshop Studio.

Fase 1: Avvia la landing zone di AWS Control Tower

Per istruzioni su come iniziare a usare AWS Control Tower, consulta [Getting started with AWS Control Tower](#). Qui puoi creare l'account di gestione AWS Control Tower e configurare la tua landing zone AWS Control Tower.

Note

Assicurati di creare un ruolo per l'account di gestione AWS Control Tower con AdministratorAccesscredenziali. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Identità IAM \(utenti, gruppi di utenti e ruoli\) nella Guida per l'AWS Identity and Access Management utente](#)
- [AdministratorAccess](#) nella AWS Managed Policy Reference Guide

Fase 2: Creare una nuova unità organizzativa per AFT (fortemente consigliata)

Ti consigliamo di creare un'unità organizzativa separata nella landing zone di AWS Control Tower. Questa unità organizzativa è il luogo in cui si effettua il provisioning dell'account di gestione AFT. Crea la nuova unità organizzativa e l'account di gestione AFT dal tuo account di gestione AWS Control Tower. Per ulteriori informazioni, consulta [Creare una nuova unità organizzativa](#).

Fase 3: Eseguire il provisioning dell'account di gestione AFT

AFT richiede il provisioning di un AWS account dedicato alle operazioni di gestione AFT. Crea l'account di gestione AFT dopo aver effettuato l'accesso all'account di gestione AWS Control Tower associato alla tua landing zone AWS Control Tower. Puoi effettuare il provisioning dell'account di gestione AFT dalla console AWS Control Tower selezionando Crea account nella pagina Organizzazione o con altri mezzi. Per ulteriori informazioni, consulta [Fornire account con AWS Service Catalog Account Factory](#).

Note

Se hai creato un'unità organizzativa separata per AFT, assicurati di selezionarla quando crei l'account di gestione AFT.

Il provisioning completo dell'account di gestione AFT può richiedere fino a 30 minuti.

Fase 4: Verificare che l'ambiente Terraform sia disponibile per l'implementazione

Questo passaggio presuppone che tu abbia esperienza con Terraform e disponga di procedure per l'esecuzione di Terraform. Per ulteriori informazioni, consulta [Command: init](#) sul sito Web per sviluppatori. HashiCorp

Note

AFT supporta la versione Terraform 1.6.1 o successiva.

Fase 5: configurazioni opzionali

- Impostare facoltativamente la configurazione del cloud privato virtuale (VPC)

Il modulo AFT include un `aft_enable_vpc` parametro che specifica se AWS Control Tower effettua il provisioning delle risorse dell'account all'interno di un VPC nell'account di gestione AFT centrale. Per impostazione predefinita, il parametro è impostato su `true`. Se imposti questo parametro su `false`, AWS Control Tower distribuisce AFT senza l'uso di un VPC e di risorse di rete private, come gateway NAT o endpoint VPC. La disabilitazione `aft_enable_vpc` può aiutare a ridurre i costi operativi di AFT per alcuni modelli di utilizzo. L'aggiunta di qualsiasi configurazione VPC ha la precedenza sul parametro impostato su `aft_enable_vpc false`.

Note

Re-enabling il `aft_enable_vpc` parametro (che cambia il valore da `false` a `true`) potrebbe richiedere l'esecuzione del `terraform apply` comando due volte di seguito.

Invece di effettuare il provisioning di un nuovo VPC, puoi configurare AFT per utilizzare un VPC esistente nel tuo account. Per utilizzare il tuo VPC, fornisci i seguenti parametri di configurazione VPC:

- `aft_customer_vpc_id`- L'ID del tuo VPC esistente
- `aft_customer_private_subnets`- Un elenco di ID di sottorete privati nel tuo VPC

Configurazione di esempio:

```
module "aft" {
```

```
source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

# VPC configuration
aft_customer_vpc_id = "vpc-0123456789abcdef0"
aft_customer_private_subnets = ["subnet-0123456789abcdef0",
"subnet-0123456789abcdef1"]

# Other AFT parameters...
}
```

Important

Non è consigliabile utilizzare l'opzione VPC personalizzata se si dispone di una distribuzione AFT esistente. Potresti avere dipendenze dalle funzioni Lambda CodePipeline o dipendere dalle risorse all'interno del VPC esistente sottostante.

- Facoltativamente, configura il nome del progetto Terraform

È possibile personalizzare il nome del progetto Terraform utilizzato da AFT impostando il parametro. `terraform_project_name` Per impostazione predefinita, AFT inserisce l'implementazione nel progetto «predefinito» in HCP Terraform o Terraform Enterprise.

Configurazione di esempio:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Project name configuration
  terraform_project_name = "my-organization-aft"

  # Other AFT parameters...
}
```

Note

Questo parametro è applicabile solo alle implementazioni Terraform Enterprise o Terraform Cloud.

- Facoltativamente, applica tag personalizzati alle risorse AFT

È possibile applicare tag personalizzati a tutte le risorse AFT utilizzando il `tags` parametro. Questi tag aiutano nell'organizzazione delle risorse, nell'allocazione dei costi e nel controllo degli accessi.

Configurazione di esempio:

```
module "aft" {  
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"  
  
  # Custom tags configuration  
  tags = {  
    Environment = "Production"  
    CostCenter  = "IT-12345"  
    Project     = "AFT-Deployment"  
    Owner       = "platform-team@example.com"  
  }  
  
  # Other AFT parameters...  
}
```

Questi tag vengono applicati a tutte le risorse create dal modulo AFT. AFT aggiunge automaticamente un `managed_by = "AFT"` tag a tutte le risorse, che non può essere sovrascritto dai tag personalizzati.

Note

I tag personalizzati possono essere aggiunti in qualsiasi momento, non solo durante la distribuzione iniziale.

- Facoltativamente, applica una chiave di crittografia AWS KMS gestita dal cliente (CMK) ai gruppi di CloudWatch log e agli argomenti SNS

Per abilitare la crittografia KMS CMK per i gruppi di log e gli argomenti SNS, imposta le variabili `and.cloudwatch_log_group_enable_cmk_encryption` e `sns_topic_enable_cmk_encryption`

Se attivi queste impostazioni, AFT utilizza la CMK esistente per CloudWatch crittografare i log e gli alias/argumenti SNS. Questo CMK viene creato quando AFT viene distribuito nell'account di gestione AFT e può essere applicato a gruppi di log e argomenti SNS.

- Se la variabile `cloudwatch_log_group_enable_cmk_encryption` è impostata su `true`, i gruppi di CloudWatch log per AFT vengono crittografati utilizzando CMK. Se la variabile è impostata su `false`, che è il valore predefinito, i registri vengono crittografati utilizzando la [crittografia lato server con l'impostazione predefinita dei CloudWatch log](#).
- Se la variabile `sns_topic_enable_cmk_encryption` è impostata su `true`, le notifiche inviate agli argomenti AFT SNS (`aft-notifications` e `aft-failure-notification`) vengono crittografate utilizzando il CMK. Se la variabile è impostata su `false`, che è il valore predefinito, i messaggi SNS vengono crittografati con la chiave: `/sns. AWS-managed alias/aws` Per ulteriori informazioni, consulta i termini chiave [SSE](#).
- Facoltativamente, modifica il tipo di elaborazione CodeBuild

Durante la distribuzione, per modificare il tipo di calcolo utilizzato da AFT CodeBuild, imposta la variabile `aft_codebuild_compute_type`

Per informazioni sui tipi di calcolo accettati, consulta [Informazioni sui tipi di ambiente on-demand](#). Il tipo di calcolo predefinito è `BUILD_GENERAL1_MEDIUM`

- Configura opzionalmente OpenID Connect (OIDC) per Terraform

I clienti che utilizzano Terraform Enterprise o HCP Terraform (precedentemente Terraform Cloud) possono utilizzare i token di identità Workload di Terraform (o credenziali dinamiche del provider), basati sul protocollo OIDC, per connettere e autenticare in modo sicuro gli spazi di lavoro con AFT.

È possibile `true` abilitare l'integrazione OIDC per gli spazi di lavoro AFT impostando il parametro su `terraform_oidc_integration` Il valore del parametro è `false` per impostazione predefinita. Quando si abilita questo parametro, i `terraform_oidc_hostname` parametri `terraform_oidc_aws_audience` and devono essere esaminati e configurati se i valori predefiniti (`aws.workload.identityapp.terraform.io`, rispettivamente) non corrispondono all'ambiente in uso.

Configurazione di esempio:

```
module "aft" {  
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"
```

```
# Terraform distribution must be "tfc" or "tfe" for OIDC
terraform_distribution = "tfc"

# Terraform OIDC Configuration
terraform_oidc_integration = true
terraform_oidc_aws_audience = "aws.workload.identity" # default
terraform_oidc_hostname     = "app.terraform.io"       # default; set to your TFE
hostname if applicable

# Other AFT parameters...
}
```

Note

Questo parametro è applicabile solo alle implementazioni Terraform Enterprise o HCP Terraform.

Note

Se attualmente stai utilizzando un provider OIDC per Terraform nell'account di gestione AFT, devi eliminare quel provider prima di aderire a questa integrazione. AFT ricreerà quel provider per te al momento della distribuzione.

Passaggio 6: chiama il modulo Account Factory for Terraform per implementare AFT

Chiama il modulo AFT con il ruolo che hai creato per l'account di gestione AWS Control Tower con AdministratorAccesscredenziali. AWS Control Tower fornisce un modulo Terraform tramite l'account di gestione AWS Control Tower, che stabilisce tutta l'infrastruttura necessaria per orchestrare le richieste di AWS Control Tower Account Factory.

[È possibile visualizzare il modulo AFT nel repository AFT su GitHub](#). L'intero GitHub repository è considerato il modulo AFT. Fate riferimento al [file README](#) per informazioni sugli input necessari per eseguire il modulo AFT e distribuire AFT. [In alternativa, puoi visualizzare il modulo AFT nel registro Terraform.](#)

Se nel tuo ambiente disponi di pipeline stabilite per la gestione di Terraform, puoi integrare il modulo AFT nel tuo flusso di lavoro esistente. Altrimenti, esegui il modulo AFT da qualsiasi ambiente autenticato con le credenziali richieste.

Il timeout causa il fallimento della distribuzione. Ti consigliamo di utilizzare le credenziali Servizio di token di sicurezza AWS (STS) per assicurarti di avere un timeout sufficiente per una distribuzione completa. Il timeout minimo per le AWS STS credenziali è di 60 minuti. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM nella Guida](#) per l'AWS Identity and Access Management utente.

Note

Potresti attendere fino a 30 minuti prima che AFT completi la distribuzione tramite il modulo Terraform.

Passaggio 7: gestire il file di stato Terraform

Un file di stato Terraform viene generato quando si distribuisce AFT. Questo artefatto descrive lo stato delle risorse create da Terraform. Se prevedi di aggiornare la versione AFT, assicurati di conservare il file di stato Terraform o di configurare un backend Terraform utilizzando Amazon S3 e DynamoDB. Il modulo AFT non gestisce uno stato Terraform di backend.

Note

Sei responsabile della protezione del file di stato di Terraform. Alcune variabili di input potrebbero contenere valori sensibili, come una ssh chiave privata o un token Terraform. A seconda del metodo di distribuzione, questi valori possono essere visualizzati come testo semplice nel file di stato Terraform. Per ulteriori informazioni, consulta [Dati sensibili nello stato sul HashiCorp sito Web](#).

Post-deployment passaggi

Una volta completata l'implementazione dell'infrastruttura AFT, segui questi passaggi aggiuntivi per completare il processo di configurazione e prepararti al provisioning degli account.

Fase 1: Completare AWS CodeConnections con il provider VCS desiderato

Se scegliete un provider VCS di terze parti, AFT lo stabilisce e voi AWS CodeConnections lo confermate. Fate riferimento [Alternative per il controllo della versione del codice sorgente in AFT](#) a come configurare AFT con il vostro VCS preferito.

La fase iniziale per stabilire la AWS CodeStar connessione viene eseguita da AFT. È necessario confermare la connessione.

Fase 2: Compila ogni repository

AFT richiede la gestione di [quattro repository](#):

1. Richieste di account: questo repository gestisce l'inserimento o l'aggiornamento delle richieste di account. [Esempi disponibili](#). Per ulteriori informazioni sulle richieste di account AFT, vedere [Effettua il provisioning di un nuovo account con AFT](#).
2. Personalizzazioni del provisioning degli account AFT: questo repository gestisce le personalizzazioni che vengono applicate a tutti gli account creati e gestiti con AFT, prima di iniziare la fase di personalizzazione globale. [Esempi disponibili](#). Per creare personalizzazioni per il provisioning degli account AFT, vedere [Crea la tua macchina a stati per il provisioning delle personalizzazioni dell'account AFT](#).
3. Personalizzazioni globali: questo repository gestisce le personalizzazioni applicate a tutti gli account creati e gestiti con AFT. [Esempi disponibili](#). Per creare personalizzazioni globali AFT, vedere [Applica personalizzazioni globali](#).
4. Personalizzazioni degli account: questo repository gestisce le personalizzazioni applicate solo a account specifici creati e gestiti con AFT. [Esempi disponibili](#). Per creare personalizzazioni dell'account AFT, vedere [Applica le personalizzazioni dell'account](#).

AFT prevede che ciascuno di questi repository segua una struttura di directory specifica. [I modelli utilizzati per popolare i repository e le istruzioni che descrivono come compilare i modelli sono disponibili nel modulo Account Factory for Terraform nel repository github AFT](#).

Effettua il provisioning di un nuovo account con AFT

Questa sezione presuppone che tu abbia già impostato AFT e il tuo account di gestione AFT e che tu stia effettuando il provisioning di account aggiuntivi.

Per effettuare il provisioning di un nuovo account con AFT, crea un file Terraform di richiesta di account. Questo file contiene l'input per i parametri nel repository `aft-account-request`. Dopo aver creato un file Terraform per la richiesta di account, inizia a elaborare la richiesta di account

eseguendo `git push` Questo comando richiama l'`ct-aft-account-request` operazione in AWS CodePipeline, che viene creata nell'account di gestione AFT al termine del provisioning dell'account. Per ulteriori informazioni, vedere [AFT account provisioning pipeline](#).

Parametri del file Terraform per la richiesta dell'account

È necessario includere i seguenti parametri nel file Terraform di richiesta dell'account. Puoi visualizzare [un esempio di file](#) Terraform per la richiesta di account su GitHub

- Il valore di `module name` deve essere univoco per la Account AWS richiesta.
- Il valore di `module source` è il percorso del modulo Terraform di richiesta dell'account fornito da AFT.
- Il valore di `control_tower_parameters` acquisisce l'input richiesto per creare un account AWS Control Tower. Il valore include i seguenti campi di input:
 - `AccountEmail`
 - `AccountName`
 - `ManagedOrganizationalUnit`
 - `SSOUserEmail`
 - `SSOUserFirstName`
 - `SSOUserLastName`

Note

L'input fornito non `control_tower_parameters` può essere modificato durante il provisioning dell'account.

I formati supportati per la specificazione `ManagedOrganizationalUnit` nel repository `aft-account-request` includono `e. OUName OUName (OU-ID)` Per le unità organizzative annidate (un'unità organizzativa all'interno di un'unità organizzativa), è necessario utilizzare il formato `OUName (OU-ID)` Per un esempio, vedi https://github.com/aws-ia/terraform-aws-control_tower_account_factory/blob/main/sources/aft-customizations-repos/aft-account-request/examples/account-request.tf#L12-L13 `account-request.tf` in GitHub

- `account_tags` acquisisce chiavi e valori definiti dall'utente, che possono essere etichettati in base a criteri aziendali. Account AWS Per ulteriori informazioni, vedere AWS Organizations Risorse relative ai [tag](#) nella Guida per l'AWS Organizations utente.

- Il valore di `change_management_parameters` acquisisce informazioni aggiuntive, ad esempio il motivo per cui è stata creata una richiesta di account e chi ha avviato la richiesta di account. Il valore include i seguenti campi di input:
 - `change_reason`
 - `change_requested_by`
- `custom_fields` acquisisce metadati aggiuntivi con chiavi e valori che vengono distribuiti come parametri SSM nell'account venduto in `/-fields/.aft/account request/custom`. Puoi fare riferimento a questi metadati durante la personalizzazione dell'account per implementare i controlli appropriati. Ad esempio, un account soggetto alla conformità normativa potrebbe implementarne altri. Regole di AWS Config I metadati raccolti `custom_fields` possono richiedere un'elaborazione aggiuntiva durante il provisioning e l'aggiornamento dell'account. Se un campo personalizzato viene rimosso dalla richiesta dell'account, il campo personalizzato viene rimosso dall'SSM Parameter Store per l'account venduto.
- (Facoltativo) `account_customizations_name` acquisisce la cartella del modello di account nel repository `aft-account-customizations`. Per ulteriori informazioni, consulta Personalizzazioni dell'account. <https://docs.aws.amazon.com/controltower/latest/userguide/aft-account-customization-options.html>

Invia più richieste di account

AFT elabora le richieste di account una alla volta, ma è possibile inviare più richieste di account alla pipeline AFT. Quando invii più richieste di account alla pipeline AFT, AFT mette in coda ed elabora le richieste di account in base all'ordine «first in», «first-out».

Note

Puoi creare un file Terraform di richiesta di account per ogni account di cui desideri che AFT esegua il provisioning o raggruppare più richieste di account in un unico file Terraform di richiesta di account.

Aggiorna un account esistente

Compatibilità con la registrazione automatica

Se la tua organizzazione utilizza Auto Enroll per la registrazione automatica degli account, tieni presente che AFT ha delle limitazioni nell'importazione di questi account. Gli account registrati tramite Auto Enroll non dispongono dei prodotti forniti dal Service Catalog richiesti dal flusso di importazione di AFT.

Soluzione alternativa: utilizza la funzione Register OU per creare prodotti con provisioning per gli account registrati automaticamente. Ciò abilita gli eventi del ciclo di vita necessari per le personalizzazioni AFT.

È possibile aggiornare gli account forniti da AFT modificando le richieste di account inviate in precedenza ed eseguendole. `git push` Questo comando richiama il flusso di lavoro di provisioning degli account e può elaborare le richieste di aggiornamento degli account. È possibile aggiornare l'input `perManagedOrganizationalUnit`, che fa parte del valore richiesto per `control_tower_parameters`

`ManagedOrganizationalUnit` è l'unico parametro che può essere aggiornato, tra tutti `control_tower_parameters`. Tuttavia, è possibile aggiornare altri parametri che fanno parte del file Terraform di richiesta dell'account, ad esempio `custom_fields`. Per ulteriori informazioni, vedi [Fornire un nuovo account con AFT](#).

Ad esempio, per aggiornare il nome o l'indirizzo email di un account AFT, puoi definire le specifiche come `custom_fields` nel file di richiesta dell'account. In questo modo, crei parametri SSM, che puoi passare alla `aws_account_alternate_contact` risorsa durante le personalizzazioni globali.

```
resource "aws_account_alternate_contact" "operations" {  
  
    alternate_contact_type = "OPERATIONS"  
  
    name           = "Example"  
    title          = "Example"  
    email_address  = "someone@example.com"  
    phone_number   = "+1234567890"  
}
```

Puoi aggiungere campi simili per altri tipi di contatto, ad esempio operazioni e sicurezza. In Personalizzazioni globali, aggiungi ricerche di dati per ogni campo personalizzato, per assicurarti di cercare tutti i campi che hai creato in Richiesta di account:

```
data "aws_ssm_parameter" "billing_name" {
  name = "/aft/account-request/custom-fields/billing_name"
}

data "aws_ssm_parameter" "billing_title" {
  name = "/aft/account-request/custom-fields/billing_title"
}

data "aws_ssm_parameter" "billing_email_address" {
  name = "/aft/account-request/custom-fields/billing_email_address"
}

data "aws_ssm_parameter" "billing_phone_number" {
  name = "/aft/account-request/custom-fields/billing_phone_number"
}
```

Infine, sempre nel file Global Customizations, crea le risorse di contatto alternative. Dovrai definire uno di questi blocchi per ogni tipo di contatto creato in Richiesta di account:

```
resource "aws_account_alternate_contact" "billing" {

  alternate_contact_type = "BILLING"

  name          = data.aws_ssm_parameter.billing_name.value
  title         = data.aws_ssm_parameter.billing_title.value
  email_address = data.aws_ssm_parameter.billing_email_address.value
  phone_number  = data.aws_ssm_parameter.billing_phone_number.value
}
```

Note

L'input fornito non `control_tower_parameters` può essere modificato durante il provisioning dell'account.

I formati supportati per la specificazione `ManagedOrganizationalUnit` nel repository `aft-account-request` includono `e. OUName OUName (OU-ID)` Per le unità organizzative annidate (un'unità organizzativa all'interno di un'unità organizzativa), è necessario utilizzare il formato. `OUName (OU-ID)` Per un esempio, vedi <https://github.com/aws-ia/terraform->

aws-control_tower_account_factory/blob/main/sources/aft-customizations-repos/aft-account-request/examples/account-request.tf#L12-L13 account-request.tf in. GitHub

Aggiorna un account non fornito da AFT

Puoi aggiornare gli account AWS Control Tower creati al di fuori di AFT specificando l'account nel repository `aft-account-request`.

Note

Assicurati che tutti i dettagli dell'account siano corretti e coerenti con l'organizzazione AWS Control Tower e il rispettivo prodotto fornito. AWS Service Catalog

Prerequisiti per l'aggiornamento di un esistente Account AWS con AFT

- Account AWS Devono essere registrati in AWS Control Tower.
- Account AWS Deve far parte dell'organizzazione AWS Control Tower.

Versioni Terraform e AFT

Account Factory for Terraform (AFT) supporta la versione Terraform 1.6.1 o successiva. È necessario fornire una versione Terraform come parametro di input per il processo di distribuzione AFT, come mostrato nell'esempio che segue.

```
terraform_version = "1.6.1"
```

Distribuzioni Terraform

AFT supporta tre distribuzioni Terraform:

- Terraform Community Edition
- HCP Terraform
- Terraform Enterprise

Queste distribuzioni sono spiegate nelle sezioni che seguono. Fornisci la distribuzione Terraform di tua scelta come parametro di input durante il processo di bootstrap AFT. Per ulteriori informazioni

sulla distribuzione di AFT e sui parametri di input, vedere. [Implementa AWS Control Tower Account Factory per Terraform \(AFT\)](#)

Se scegli le distribuzioni HCP Terraform o Terraform Enterprise, il [token API](#) specificato `terraform_token` deve essere un token API User o Team. Un token Organization non è supportato per tutte le API richieste. Per motivi di sicurezza, è necessario evitare di registrare il valore di questo token nel sistema di controllo della versione (VCS) assegnando una [variabile terraform](#), come mostrato nell'esempio che segue.

```
# Sensitive variable managed in HCP Terraform:
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

Quando selezioni Terraform Community Edition come distribuzione, AFT gestisce il backend Terraform per te nell'account di gestione AFT. AFT scarica la versione `terraform-cli` di Terraform specificata per eseguirla durante le fasi di implementazione di AFT e la pipeline AFT. La configurazione dello stato Terraform risultante viene archiviata in un bucket Amazon S3, denominato con il seguente modulo:

```
aft-backend-[account_id]-primary-region
```

AFT crea anche un bucket Amazon S3 che replica la configurazione dello stato di Terraform in un altro Regione AWS, per scopi di disaster recovery, denominato con il seguente modulo:

```
aft-backend-[account_id]-secondary-region
```

Ti consigliamo di abilitare l'autenticazione a più fattori (MFA) per le funzioni di eliminazione su questi bucket Amazon S3 dello stato Terraform. [Per saperne di più su Terraform Community Edition, consulta la documentazione di Terraform.](#)

Per selezionare Terraform OSS come distribuzione, fornisci il seguente parametro di input:

```
terraform_distribution = "oss"
```

HCP Terraform

Quando selezionate HCP Terraform come distribuzione, AFT crea spazi di lavoro per i seguenti componenti nell'organizzazione HCP Terraform, che avvia un flusso di lavoro. API-driven

- Richiesta di account
- Personalizzazioni AFT per gli account forniti da AFT
- Personalizzazioni degli account per gli account che prevedono AFT
- Personalizzazioni globali per gli account forniti da AFT

HCP Terraform gestisce la configurazione dello stato Terraform risultante.

Quando selezioni HCP Terraform come distribuzione, fornisci i seguenti parametri di input:

- `terraform_distribution = "tfc"`
- `terraform_token`— Questo parametro contiene il valore del token HCP Terraform. AFT lo contrassegna come sensibile e memorizza il valore come stringa sicura nell'archivio dei parametri SSM nell'account di gestione AFT. Ti consigliamo di ruotare periodicamente il valore del token Terraform in base alle politiche di sicurezza e alle linee guida di conformità della tua azienda. Il token Terraform deve essere un token API a livello di utente o team. I token organizzativi non sono supportati.
- `terraform_org_name`— Questo parametro contiene il nome della tua organizzazione HCP Terraform.

Note

Non sono supportate più implementazioni AFT in una singola organizzazione HCP Terraform.

[Per informazioni su come configurare HCP Terraform, consulta la documentazione Terraform.](#)

Terraform Enterprise

Quando selezioni Terraform Enterprise come distribuzione, AFT crea spazi di lavoro per i seguenti componenti nella tua organizzazione Terraform Enterprise e attiva il API-driven flusso di lavoro per le esecuzioni Terraform risultanti.

- Richiesta di account
- Personalizzazioni del provisioning degli account AFT per gli account forniti da AFT
- Personalizzazioni degli account per gli account forniti da AFT
- Personalizzazioni globali per gli account forniti da AFT

La configurazione dello stato Terraform risultante è gestita dalla configurazione di Terraform Enterprise.

Per selezionare Terraform Enterprise come distribuzione, fornisci i seguenti parametri di input:

- `terraform_distribution = "tfe"`
- `terraform_token`— Questo parametro contiene il valore del token Terraform Enterprise. AFT contrassegna il suo valore come sensibile e lo memorizza come stringa sicura nell'archivio dei parametri SSM, nell'account di gestione AFT. Ti consigliamo di ruotare periodicamente il valore del token Terraform, in base alle politiche di sicurezza e alle linee guida di conformità della tua azienda.
- `terraform_org_name`— Questo parametro contiene il nome della tua organizzazione Terraform Enterprise.
- `terraform_api_endpoint`— Questo parametro contiene l'URL del tuo ambiente Terraform Enterprise. Il valore di questo parametro deve essere nel formato:

```
https://{fqdn}/api/v2/
```

Consulta [la documentazione di Terraform](#) per saperne di più su come configurare Terraform Enterprise.

Controlla la versione AFT

Puoi controllare la versione AFT distribuita interrogando la chiave AWS SSM Parameter Store:

```
/aft/config/aft/version
```

Se si utilizza il metodo del registro, è possibile aggiungere la versione.

```
module "control_tower_account_factory" {  
  source = "aws-ia/control_tower_account_factory/aws"  
  version = "1.3.2"  
  # insert the 6 required variables here  
}
```

È possibile visualizzare ulteriori informazioni sulle versioni AFT nel [repository AFT](#).

Aggiornate la versione AFT

Accedi all'account di gestione AWS Control Tower per avviare questo aggiornamento AFT.

Puoi aggiornare la versione AFT distribuita estraendola dal ramo del main repository:

```
terraform get -update
```

Una volta completato il pull, puoi eseguire nuovamente il piano Terraform o eseguire apply per aggiornare l'infrastruttura AFT con le ultime modifiche.

Abilita le opzioni delle funzionalità

AFT offre opzioni di funzionalità basate sulle migliori pratiche. È possibile attivare queste funzionalità, tramite i flag di funzionalità, durante l'implementazione di AFT. [Effettua il provisioning di un nuovo account con AFT](#) Per ulteriori informazioni sui parametri di configurazione di input AFT, fare riferimento a.

Queste funzionalità non sono abilitate per impostazione predefinita. È necessario abilitarle in modo esplicito nel proprio ambiente.

Argomenti

- [AWS CloudTrail eventi di dati](#)
- [AWS Piano Enterprise Support](#)
- [Elimina le foto o i video AWS VPC predefinito](#)
- [Esporta l'output del piano Terraform su Amazon S3](#)

AWS CloudTrail eventi di dati

Se abilitata, l'opzione AWS CloudTrail data events configura queste funzionalità.

- Crea un Organization Trail nell'account di gestione AWS Control Tower, per CloudTrail
- Attiva la registrazione per gli eventi relativi ai dati di Amazon S3 e Lambda
- Crittografa ed esporta tutti gli eventi CloudTrail relativi ai dati in un bucket `aws-aft-logs-*` S3 nell'account AWS Control Tower Log Archive, con crittografia AWS KMS
- Attiva l'impostazione di convalida del file di registro

Per abilitare questa opzione, imposta il seguente flag di funzionalità su True nella configurazione di input della distribuzione AFT.

```
aft_feature_cloudtrail_data_events
```

Prerequisito

Prima di abilitare questa opzione di funzionalità, assicuratevi che l'accesso affidabile per AWS CloudTrail sia abilitato nella vostra organizzazione.

Per verificare lo stato dell'accesso affidabile per CloudTrail :

1. Vai alla AWS Organizations console.
2. Scegli Servizi > CloudTrail.
3. Quindi seleziona Abilita accesso affidabile in alto a destra, se necessario.

Potresti ricevere un messaggio di avviso che ti consiglia di utilizzare la AWS CloudTrail console, ma in questo caso ignora l'avviso. AFT crea il percorso come parte dell'attivazione di questa opzione di funzionalità, dopo aver consentito l'accesso attendibile. Se l'accesso affidabile non è abilitato, riceverai un messaggio di errore quando AFT tenta di creare il percorso per gli eventi relativi ai dati.

Note

Questa impostazione funziona a livello di organizzazione. L'attivazione di questa impostazione ha effetto su tutti gli account AWS Organizations, indipendentemente dal fatto che siano gestiti da AFT o meno. Tutti i bucket presenti nell'account AWS Control Tower Log Archive al momento dell'attivazione sono esclusi dagli eventi relativi ai dati di Amazon S3. Per ulteriori informazioni, consulta [la Guida per l' AWS CloudTrail utente](#). CloudTrail

AWS Piano Enterprise Support

Quando questa opzione è abilitata, la pipeline AFT attiva il piano AWS Enterprise Support per gli account forniti da AFT.

AWS per impostazione predefinita, gli account hanno il piano AWS Basic Support abilitato. AFT fornisce l'iscrizione automatica al livello di supporto aziendale, per gli account forniti da AFT. Il

processo di provisioning apre un ticket di supporto per l'account, richiedendo che venga aggiunto al piano Enterprise AWS Support.

Per abilitare l'opzione Enterprise Support, imposta il seguente flag di funzionalità su True nella configurazione di input della distribuzione AFT.

```
aft_feature_enterprise_support=false
```

[Consulta Compare AWS Support Plans](#) per saperne di più sui piani di AWS supporto.

Note

Per consentire il funzionamento di questa funzionalità, è necessario registrare l'account del pagatore nel piano Enterprise Support.

Elimina le foto o i video AWS VPC predefinito

Quando abiliti questa opzione, AFT elimina tutti i VPC AWS predefiniti nell'account di gestione AFT e in tutto Regioni AWS, anche se non sono state distribuite risorse AWS Control Tower in tali account.

Regioni AWS

AFT non elimina automaticamente i VPC AWS predefiniti per nessun account AWS Control Tower di cui AFT fornisce o per AWS gli account esistenti registrati in AWS Control Tower tramite AFT.

Per impostazione predefinita, i nuovi AWS account vengono creati con un VPC configurato in ciascuno Regione AWS di essi. La tua azienda potrebbe avere procedure standard per la creazione di VPC, che richiedono di eliminare il VPC AWS predefinito ed evitare di abilitarlo, in particolare per l'account di gestione AFT.

Per abilitare questa opzione, imposta il seguente flag di funzionalità su True nella configurazione di input della distribuzione AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Di seguito è riportato un esempio di configurazione di input di distribuzione AFT.

```
module "aft" {  
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"  
  ct_management_account_id = var.ct_management_account_id
```

```

log_archive_account_id      = var.log_archive_account_id
audit_account_id            = var.audit_account_id
aft_management_account_id   = var.aft_management_account_id
ct_home_region              = var.ct_home_region
tf_backend_secondary_region = var.tf_backend_secondary_region

vcs_provider                 = "github"
account_request_repo_name    = "${var.github_username}/learn-
terraform-aft-account-request"
account_provisioning_customizations_repo_name = "${var.github_username}/learn-
terraform-aft-account-provisioning-customizations"
global_customizations_repo_name    = "${var.github_username}/learn-
terraform-aft-global-customizations"
account_customizations_repo_name    = "${var.github_username}/learn-
terraform-aft-account-customizations"

# Optional Feature Flags
aft_feature_delete_default_vpcs_enabled = true
aft_feature_cloudtrail_data_events      = false
aft_feature_enterprise_support          = false
}

```

Per ulteriori informazioni sui [VPC predefiniti](#), consulta [VPC predefiniti e sottoreti](#) predefinite.

Note

L'eliminazione predefinita di un VPC è la procedura migliore per. Regione AWS Se l'endpoint di una regione è temporaneamente irraggiungibile, AFT ignora quella regione e continua a eliminare i VPC predefiniti nelle restanti regioni. Le regioni ignorate vengono riprovate alla successiva esecuzione della pipeline di personalizzazione. Per verificare se alcune regioni sono state ignorate, cerca il messaggio nei log delle funzioni `aft-delete-default-vpc` Lambda. `Skipping default VPC deletion in region`

Esporta l'output del piano Terraform su Amazon S3

Quando distribuisce AFT, AFT crea un bucket Amazon S3 dedicato e crittografato con output del piano nell'account di gestione AFT. AFT crea questo bucket su ogni implementazione AFT, indipendentemente dalla distribuzione Terraform. Il bucket memorizza l'output JSON delle esecuzioni di personalizzazione solo del piano. Per ulteriori informazioni sulle esecuzioni basate solo sul piano, consulta [Re-invoke personalizzazioni](#)

Il bucket plan-output ha le seguenti proprietà:

- Crittografato con la chiave AFT AWS KMS
- Controllo delle versioni abilitato
- Accesso pubblico bloccato
- Accesso in scrittura limitato al ruolo di creazione delle personalizzazioni AFT

Se AFT esporta il piano JSON in questo bucket dipende dalla distribuzione Terraform:

- Community Edition (open source): AFT esporta il piano JSON nel bucket per impostazione predefinita a ogni esecuzione del solo piano.
- HCP Terraform (Terraform Cloud) e Terraform Enterprise: puoi visualizzare i risultati del piano nell'interfaccia utente di HCP Terraform run. Per esportare anche il piano JSON nel bucket, imposta la seguente variabile su nella configurazione di input della distribuzione AFT. `true`

```
aft_plan_output_export_enabled = true
```

Per impostazione predefinita, AFT conserva i piani esportati per 30 giorni. Per modificare la durata di conservazione, imposta la `aft_plan_output_retention_days` variabile nella configurazione di input della distribuzione AFT.

```
aft_plan_output_retention_days = 30
```

Note

La `aft_plan_output_export_enabled` variabile influisce solo sulle distribuzioni HCP Terraform (Terraform Cloud) e Terraform Enterprise. Nella distribuzione Community Edition (open source), AFT esporta il piano JSON per impostazione predefinita e questa variabile non ha alcun effetto.

Considerazioni sulle risorse per AWS Control Tower Account Factory for Terraform

Quando configuri una landing zone utilizzando AWS Control Tower Account Factory for Terraform, all'interno dei tuoi AWS account vengono creati diversi tipi di AWS risorse.

Cerca risorse

- È possibile utilizzare i tag per cercare l'elenco più aggiornato di risorse AFT. La coppia chiave-valore per la ricerca è:

Key: managed_by | Value: AFT

- Per i servizi dei componenti che non supportano i tag, è possibile individuare le risorse con una ricerca `aft` nei nomi delle risorse.

Note

AFT non crea alcuna risorsa AWS di Backup nell'account di gestione.

Tabelle delle risorse create inizialmente, per account

Account di gestione AWS Control Tower Account Factory per Terraform

AWS service	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	AWSAFTAdmin
		AWSAFTExecution
		AWSAFTService
		ct-aft-*
		aft-*
		codebuild_trigger_role
AWS Identity and Access Management	Policy	python-layer-builder-aft-common-*
		aft-*
CodeCommit	Repositories	aft-*

AWS service	Tipo di risorsa	Nome risorsa
CodeBuild	Progetti di compilazione	aft-* ct-aft-* python-layer-builder-aft-common-*
Codice Pipeline	Pipelines	<i>YourAccountId</i> -customizations-pipeline
Simple Storage Service (Amazon S3)	Bucket	aft-*
Simple Storage Service (Amazon S3)	Bucket	aft-plan-output-*
Lambda	Funzioni	aft-*
Lambda	Livelli	aft-common-*
DynamoDB	Tabelle	aft-request aft-request-audit aft-request-metadata aft-controltower-events
Step Functions	Macchine statali	aft-account-provisioning-customizations aft-account-provisioning-framework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc

AWS service	Tipo di risorsa	Nome risorsa
Amazon SNS	Argomenti	aft-notifications aft-failure-notifications
Amazon EventBridge	Bus di eventi	aft-events-from-ct-management
Amazon EventBridge	Regole dell'evento	aft-account-provisioning-customizations-trigger aft-account-request-codepipeline-trigger aft-lambda-account-request-processor aft-controltower-event-logger
Servizio di gestione delle chiavi (KMS)	Chiavi gestite dal cliente	aft-backend-*-kms-key aft
AWS Systems Manager	Archivio dei parametri	/aft/*
Amazon SQS	Queues	aft-account-request.fifo aft-account-request-dlg.fifo
CloudWatch	Gruppi di log	/aws/*/ct-aft-* /aws/*/aft-* /aws/codebuild/python-layer-builder-aft-common-*
AWS Backup	Vault	aft-controltower-backup-vault
AWS Backup	Piani	aft-controltower-backup-plan

AWS service	Tipo di risorsa	Nome risorsa
AWS Support Center (opzionale)	Piani di supporto	Enterprise

AWS account forniti tramite AWS Control Tower Account Factory per Terraform

AWS service	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	AWSAFTExecution
AWS Support Center (opzionale)	Piani di supporto	Enterprise

Account di gestione AWS Control Tower

AWS service	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	AWSAFTExecution
		AWSAFTService
		aft-controltower-events-rule
AWS Systems Manager	Archivio dei parametri	/aft/*
EventBridge	Regole degli eventi	aft-capture-ct-events
CloudTrail (Facoltativo)	Trail	aws-aft-CustomizationsCloudTrail
AWS Support Center (opzionale)	Piani di supporto	Enterprise

Account di archiviazione dei log AWS Control Tower

AWS service	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	AWSAFTExecution
		AWSAFTService
Servizio di gestione delle chiavi (KMS)	Chiavi gestite dal cliente	aft
Simple Storage Service (Amazon S3)	Bucket	aws-aft-logs-*
		aws-aft-s3-access-logs-*
AWS Support Center (opzionale)	Piani di supporto	Enterprise

Account di audit AWS Control Tower

AWS service	Tipo di risorsa	Nome risorsa
AWS Identity and Access Management	Roles	AWSAFTExecution
		AWSAFTService
AWS Support Center (opzionale)	Piani di supporto	Enterprise

Ruoli richiesti

In generale, i ruoli e le policy fanno parte della gestione delle identità e degli accessi (IAM) in AWS. Per ulteriori informazioni, consulta la [AWS IAM User Guide](#).

AFT crea diversi ruoli e policy IAM negli account di gestione AFT e AWS Control Tower per supportare le operazioni della pipeline AFT. Questi ruoli vengono creati in base al modello di accesso con privilegi minimi, che limita l'autorizzazione alle serie minime di azioni e risorse richieste per ciascun ruolo e policy. A questi ruoli e politiche viene assegnata una `key:value` coppia di AWS tag, per l'identificazione. `managed_by:AFT`

Oltre a questi ruoli IAM, AFT crea tre ruoli essenziali:

- il AWSAFTAdmin ruolo
- il AWSAFTExecution ruolo
- il AWSAFTService ruolo

Questi ruoli sono spiegati nelle sezioni seguenti.

Il ruolo AWSAFTAdmin, spiegato

Quando si distribuisce AFT, il AWSAFTAdmin ruolo viene creato nell'account di gestione AFT. Questo ruolo consente alla pipeline AFT di assumere il AWSAFTExecution ruolo in AWS Control Tower e negli account con provisioning AFT, quindi di eseguire azioni relative al provisioning e alla personalizzazione degli account.

Ecco la policy in linea (artefatto JSON) associata al ruolo: AWSAFTAdmin

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::*:role/AWSAFTExecution",
        "arn:aws:iam::*:role/AWSAFTService"
      ]
    }
  ]
}
```

Il seguente elemento JSON mostra la relazione di fiducia per il ruolo. AWSAFTAdmin Il numero segnaposto 012345678901 viene sostituito dal numero ID dell'account di gestione AFT.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Il ruolo di AWSAFTExecution, spiegato

Quando si distribuisce AFT, il AWSAFTExecution ruolo viene creato negli account di gestione AFT e di gestione di AWS Control Tower. Successivamente, la pipeline AFT crea il AWSAFTExecution ruolo in ogni account con provisioning AFT durante la fase di provisioning dell'account AFT.

AFT utilizza inizialmente il AWSControlTowerExecution ruolo per creare il AWSAFTExecution ruolo in account specifici. Il AWSAFTExecution ruolo consente alla pipeline AFT di eseguire i passaggi eseguiti durante le fasi di provisioning e personalizzazione del provisioning del framework AFT, per gli account con provisioning AFT e per gli account condivisi.

Ruoli distinti aiutano a limitare l'ambito

Come best practice, mantieni le autorizzazioni di personalizzazione separate dalle autorizzazioni consentite durante la distribuzione iniziale delle risorse. Ricorda che il AWSAFTEService ruolo è destinato al provisioning dell'account e alla personalizzazione dell'AWSAFTExecutionaccount. Questa separazione limita l'ambito delle autorizzazioni consentite durante ogni fase della pipeline. Questa distinzione è particolarmente importante se si personalizzano gli account condivisi di AWS Control Tower, poiché gli account condivisi possono contenere informazioni sensibili, come dettagli di fatturazione o informazioni sugli utenti.

Autorizzazioni per il AWSAFTExecution ruolo: AdministratorAccess — una policy gestita da AWS

Il seguente artefatto JSON mostra la policy IAM (relazione di fiducia) associata al ruolo.

AWSAFTExecution Il numero segnaposto 012345678901 è sostituito dal numero ID dell'account di gestione AFT.

Politica di fiducia per AWSAFTExecution

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Il ruolo di AWSAFTService, spiegato

Il AWSAFTService ruolo distribuisce le risorse AFT in tutti gli account registrati e gestiti, inclusi gli account condivisi e l'account di gestione. In precedenza le risorse venivano distribuite solo dal ruolo. AWSAFTExecution

Il AWSAFTService ruolo è destinato all'uso da parte dell'infrastruttura di servizio per distribuire le risorse durante la fase di provisioning e deve essere utilizzato AWSAFTExecution solo per implementare le personalizzazioni. Assumendo i ruoli in questo modo, è possibile mantenere un controllo degli accessi più granulare durante ogni fase.

Autorizzazioni per il AWSAFTService ruolo: AdministratorAccess — una policy gestita da AWS

Il seguente artefatto JSON mostra la policy IAM (relazione di fiducia) associata al ruolo.

AWSAFTService Il numero segnaposto 012345678901 è sostituito dal numero ID dell'account di gestione AFT.

Politica di fiducia per AWSAFTService

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Servizi relativi ai componenti

Quando si implementa AFT, i componenti vengono aggiunti all' AWS ambiente da ciascuno di questi AWS servizi.

- [AWS Control Tower](#) — AFT utilizza AWS Control Tower Account Factory nell'account di gestione di AWS Control Tower per il provisioning degli account.
- [Amazon DynamoDB](#) — AFT crea tabelle Amazon DynamoDB nell'account di gestione AFT, che memorizzano le richieste di account, la cronologia di controllo degli aggiornamenti degli account, i metadati degli account e gli eventi del ciclo di vita di AWS Control Tower. AFT crea anche trigger DynamoDB Lambda per avviare processi a valle, come l'avvio del flusso di lavoro di provisioning degli account AFT.
- [Amazon Simple Storage Service](#) — AFT crea bucket Amazon Simple Storage Service (S3) nell'account di gestione AFT e nell'account di archivio dei log di AWS Control Tower, che memorizzano i log generati dai servizi richiesti dalla pipeline AFT. AWS AFT crea anche un bucket S3 backend Terraform, primario e secondario, per archiviare gli stati Terraform generati durante i flussi di Regioni AWS lavoro della pipeline AFT.
- [Amazon Simple Notification Service](#) — AFT crea argomenti Amazon Simple Notification Service (SNS) nell'account di gestione AFT, che memorizza le notifiche di esito positivo e negativo dopo l'elaborazione di ogni richiesta di account AFT. Puoi ricevere questi messaggi utilizzando il protocollo che preferisci.

- [Amazon Simple Queuing Service](#) : AFT crea una coda FIFO di Amazon Simple Queuing Service (Amazon SQS) nell'account di gestione AFT. La coda consente di inviare più richieste di account in parallelo, ma invia una richiesta alla volta ad AWS Control Tower Account Factory, per l'elaborazione sequenziale.
- [AWS CodeBuild](#) — AFT crea progetti di CodeBuild compilazione AWS nell'account di gestione AFT per inizializzare, compilare, testare e applicare i piani Terraform per il codice sorgente AFT in varie fasi di compilazione.
- [AWS CodePipeline](#) — AFT crea CodePipeline pipeline AWS nell'account di gestione AFT per integrarsi con il provider di CodeStar connessioni AWS selezionato e supportato per il codice sorgente AFT e per attivare processi di compilazione in AWS. CodeBuild
- [AWS Lambda](#) — AFT crea funzioni e livelli AWS Lambda nell'account di gestione AFT per eseguire le fasi durante la richiesta dell'account, il provisioning dell'account AFT e i processi di personalizzazione degli account.
- [AWS Systems Manager Parameter Store](#) — AFT configura AWS Systems Manager Parameter Store nell'account di gestione AFT, per memorizzare i parametri di configurazione richiesti per i processi della pipeline AFT.
- [Amazon CloudWatch](#) — AFT crea gruppi di CloudWatch log Amazon nell'account di gestione AFT per archiviare i log generati dai servizi AWS utilizzati dalla pipeline AFT. Il periodo di conservazione dei CloudWatch log è impostato su `Never Expire`
- [Amazon VPC](#) — AFT crea un Amazon Virtual Private Cloud (VPC) per isolare i servizi e le risorse nell'account di gestione AFT in un ambiente di rete separato, per una maggiore sicurezza.
- [AWS KMS](#) — AFT utilizza AWS Key Management Service (KMS) nell'account di gestione AFT e nell'account di archivio dei log di AWS Control Tower. AFT crea chiavi per crittografare gli stati di Terraform, i dati archiviati nelle tabelle DynamoDB e gli argomenti SNS. Questi log e artefatti vengono generati quando le risorse e i servizi AWS vengono distribuiti da AFT. Le chiavi KMS create da AFT hanno la rotazione annuale abilitata per impostazione predefinita.
- [AWS Identity and Access Management \(IAM\)](#) : AFT segue il modello Least Privilege consigliato. Crea ruoli e policy di AWS Identity and Access Management (IAM) nell'account di gestione AFT, negli account AWS Control Tower e negli account assegnati a AFT, se necessario, per eseguire le azioni richieste durante il flusso di lavoro della pipeline AFT.
- [AWS Step Functions](#) : AFT crea macchine a stati AWS Step Functions nell'account di gestione AFT. Queste macchine a stati orchestrano e automatizzano il processo e le fasi per il framework di provisioning e le personalizzazioni degli account AFT.

- [Amazon EventBridge](#) — AFT crea un bus di EventBridge eventi Amazon nell'account di gestione AFT e AWS Control Tower per acquisire e archiviare gli eventi del ciclo di vita di AWS Control Tower a lungo termine nella tabella DynamoDB dell'account di gestione AFT. AFT crea regole per gli CloudWatch eventi Amazon negli account di gestione AFT e AWS Control Tower, che attivano più passaggi necessari durante l'esecuzione del flusso di lavoro della pipeline AFT
- [AWS CloudTrail \(Facoltativo\)](#) : quando questa funzionalità è abilitata, AFT crea un percorso AWS CloudTrail organizzativo nell'account di gestione di AWS Control Tower, per registrare gli eventi di dati per i bucket Amazon S3 e le funzioni Lambda. AWS AFT invia questi log a un bucket S3 centrale nell'account di archivio dei log di AWS Control Tower.
- [AWS Supporto \(opzionale\)](#) : quando questa funzionalità è abilitata, AFT attiva il piano AWS Enterprise Support per gli account forniti da AFT. Per impostazione predefinita, AWS gli account vengono creati con il piano AWS di supporto di base abilitato.

Pipeline di provisioning degli account AFT

Una volta completata la fase di provisioning degli account della pipeline, il framework AFT continua. Esegue automaticamente una serie di passaggi per garantire che i nuovi account forniti dispongano dei dettagli necessari, prima dell'inizio della [Personalizzazioni dell'account](#) fase.

Ecco i passaggi successivi eseguiti dalla pipeline AFT.

1. Convalida l'input della richiesta di account.
2. Recupera le informazioni sull'account assegnato, ad esempio l'ID dell'account.
3. Memorizza i metadati dell'account in una tabella DynamoDB nell'account di gestione AFT.
4. Crea il ruolo IAM `AWSAFTExecution` nell'account appena eseguito il provisioning. AFT assume questo ruolo per eseguire la fase di personalizzazione dell'account, poiché questo ruolo concede l'accesso al portafoglio dell'account factory.
5. Applica i tag dell'account forniti come parte dei parametri di input della richiesta di account.
6. Applica le opzioni della funzionalità AFT scelte al momento dell'implementazione di AFT.
7. Applica le personalizzazioni di provisioning degli account AFT fornite. La sezione successiva spiega di più su come configurare queste personalizzazioni con una macchina a stati AWS Step Functions, in un repository. `git` Questa fase viene talvolta definita fase del framework di provisioning degli account. Fa parte del processo di provisioning di base, ma in precedenza hai impostato un framework che fornisce integrazioni personalizzate come parte del flusso di lavoro di

- provisioning degli account, prima di aggiungere ulteriori personalizzazioni agli account nella fase successiva.
8. Per ogni account di cui è stato effettuato il provisioning, crea un AWS CodePipeline account di gestione AFT, che verrà eseguito per eseguire la fase (successiva, globale). [Personalizzazioni dell'account](#)
 9. Richiama la pipeline di personalizzazione dell'account per ogni account fornito (e mirato).
 10. Invia una notifica di esito positivo o negativo all'argomento SNS, da cui è possibile recuperare i messaggi.

Configura le personalizzazioni del framework di provisioning degli account con una macchina a stati

Se configuri integrazioni personalizzate non Terraform prima di eseguire il provisioning dei tuoi account, queste personalizzazioni sono incluse nel flusso di lavoro di provisioning degli account AFT. Ad esempio, potresti richiedere alcune personalizzazioni per garantire che tutti gli account creati da AFT siano conformi agli standard e alle politiche della tua organizzazione, come gli standard di sicurezza, e questi standard possono essere aggiunti agli account prima di ulteriori personalizzazioni. Queste personalizzazioni del framework di provisioning degli account vengono implementate su ogni account di cui è stato eseguito il provisioning, prima che inizi la fase di personalizzazione globale dell'account.

Note

La funzionalità AFT descritta in questa sezione è destinata agli utenti esperti che comprendono il funzionamento di AWS Step Functions. In alternativa, ti consigliamo di collaborare con gli helper globali nella fase di personalizzazione degli account.

Il framework di provisioning degli account AFT richiama una macchina a stati AWS Step Functions, definita dall'utente, per implementare le personalizzazioni. Fai riferimento alla documentazione di [AWS Step Functions](#) per saperne di più sulle possibili integrazioni tra macchine a stati.

Ecco alcune integrazioni comuni.

- AWS Lambda funziona nella lingua di tua scelta
- Attività AWS ECS o AWS Fargate, utilizzando contenitori Docker
- Attività di AWS Step Functions che utilizzano worker personalizzati, ospitati in AWS o in locale

- Integrazioni Amazon SNS o SQS

Se non viene definita alcuna macchina a stati AWS Step Functions, la fase viene interrotta senza alcuna operazione. Per creare una macchina a stati per il provisioning delle personalizzazioni di un account AFT, segui le istruzioni in [Crea la tua macchina a stati per il provisioning delle personalizzazioni dell'account AFT](#). Prima di aggiungere personalizzazioni, assicurati di disporre dei prerequisiti.

Questi tipi di integrazioni non fanno parte di AWS Control Tower e non possono essere aggiunti durante la fase globale di pre-API della personalizzazione dell'account AFT. La pipeline AFT consente invece di impostare queste personalizzazioni come parte del processo di provisioning e vengono eseguite nel flusso di lavoro di provisioning. È necessario implementare queste personalizzazioni creando la macchina a stati in anticipo, prima di dare il via alla fase di provisioning dell'account AFT, come descritto nelle sezioni seguenti.

Prerequisiti per la creazione di una macchina a stati

- Un AFT completamente implementato. [Implementa AWS Control Tower Account Factory per Terraform \(AFT\)](#) Per ulteriori informazioni sull'implementazione di AFT, vedere.
- Configura un git repository nel tuo ambiente per le personalizzazioni del provisioning degli account AFT. Per ulteriori informazioni, consulta [Post-deployment passaggi](#).

Crea la tua macchina a stati per il provisioning delle personalizzazioni dell'account AFT

Fase 1: Modificare la definizione della macchina a stati

Modificare la definizione della macchina a `customizations.asl.json` stati di esempio. L'esempio è disponibile nel git repository che hai impostato per archiviare le personalizzazioni del provisioning degli account AFT, nelle fasi successive all'implementazione. <https://docs.aws.amazon.com/controltower/latest/userguide/aft-post-deployment.html> Fai riferimento alla [AWS Step Functions Developer Guide](#) per saperne di più sulle definizioni delle macchine a stati.

Passaggio 2: includi la configurazione Terraform corrispondente

Includi i file Terraform con l'.tf estensione nello stesso git repository con la definizione della macchina a stati per la tua integrazione personalizzata. Ad esempio, se scegli di chiamare una funzione Lambda nella definizione del task della tua macchina a stati, includerai il `lambda.tf` file nella stessa directory. Assicurati di includere i ruoli e le autorizzazioni IAM richiesti per le tue configurazioni personalizzate.

Quando fornisci l'input appropriato, la pipeline AFT richiama automaticamente la tua macchina a stati e implementa le tue personalizzazioni come parte della fase del framework di provisioning degli account AFT.

Per riavviare il framework di provisioning e le personalizzazioni degli account AFT

AFT esegue il framework di provisioning degli account e le fasi di personalizzazione per ogni account distribuito tramite la pipeline AFT. Per riavviare le personalizzazioni del provisioning degli account, puoi utilizzare uno di questi due metodi:

1. Apporta qualsiasi modifica a un account esistente nel repository per le richieste di account.
2. Crea un nuovo account con AFT.

Personalizzazioni dell'account

AFT può implementare configurazioni standard o personalizzate negli account assegnati.

Nell'account di gestione AFT, AFT fornisce una pipeline per ogni account. Con questa pipeline, puoi implementare le tue personalizzazioni in tutti gli account, in un set di account o in singoli account.

Puoi eseguire script Python, script bash e configurazioni Terraform oppure puoi interagire con la CLI AWS come parte della fase di personalizzazione dell'account.

Panoramica di

Dopo aver specificato le personalizzazioni nei git repository prescelti, quello in cui memorizzi le personalizzazioni globali o in cui memorizzi le personalizzazioni dell'account, la fase di personalizzazione dell'account viene completata automaticamente dalla pipeline AFT. Per personalizzare gli account in modo retroattivo, vedere. [Re-invoke personalizzazioni](#)

Personalizzazioni globali (facoltative)

È possibile scegliere di applicare determinate personalizzazioni a tutti gli account forniti da AFT. Ad esempio, se è necessario creare un particolare ruolo IAM o implementare un controllo personalizzato in ogni account, la fase di personalizzazione globale della pipeline AFT consente di farlo automaticamente.

Personalizzazioni dell'account (facoltative)

Per personalizzare un singolo account, o un insieme di conti, in modo diverso dagli altri account forniti da AFT, puoi sfruttare la parte dedicata alle personalizzazioni degli account della pipeline AFT per

implementare configurazioni specifiche dell'account. Ad esempio, solo un determinato account può richiedere l'accesso a un gateway Internet.

Prerequisiti di personalizzazione

Prima di iniziare a personalizzare gli account, assicurati che questi prerequisiti siano soddisfatti.

- Un AFT completamente distribuito. Per informazioni su come eseguire la distribuzione, vedere [Configura e avvia il tuo AWS Control Tower Account Factory per Terraform](#)
- Pre-populated git repository per personalizzazioni globali e personalizzazioni degli account nell'ambiente in uso. Per ulteriori informazioni, consulta [Compilare ogni repository](#). [Post-deployment passaggi](#)

Applica personalizzazioni globali

Per applicare personalizzazioni globali, devi inserire una struttura di cartelle specifica nel repository prescelto.

- Se le configurazioni personalizzate sono sotto forma di programmi o script Python, inseriscile nella cartella del tuo `api_helpers/pythonrepository`.
- Se le tue configurazioni personalizzate sono sotto forma di script Bash, inseriscile nella cartella `api_helpers` del tuo repository.
- Se le tue configurazioni personalizzate sono sotto forma di Terraform, inseriscile nella cartella `terraform` del tuo repository.
- Fai riferimento al file README delle personalizzazioni globali per maggiori dettagli sulla creazione di configurazioni personalizzate.

Note

Le personalizzazioni globali vengono applicate automaticamente, dopo la fase del framework di provisioning degli account AFT nella pipeline AFT.

Applica le personalizzazioni dell'account

Puoi applicare personalizzazioni all'account inserendo una struttura di cartelle specifica nel repository prescelto. Le personalizzazioni degli account vengono applicate automaticamente nella pipeline

AFT e dopo la fase di personalizzazione globale. Puoi anche creare più cartelle che contengono diverse personalizzazioni dell'account nel tuo repository di personalizzazioni dell'account. Per ogni personalizzazione dell'account richiesta, utilizza i seguenti passaggi.

Per applicare le personalizzazioni dell'account

1. Passaggio 1: creare una cartella per la personalizzazione dell'account

Nel repository prescelto, copia la `ACCOUNT_TEMPLATE` cartella fornita da AFT in una nuova cartella. Il nome della nuova cartella deve corrispondere a `account_customizations_name` quello fornito nella richiesta dell'account.

2. Aggiungi le configurazioni alla cartella di personalizzazione dell'account specifica

Puoi aggiungere configurazioni alla cartella delle personalizzazioni dell'account in base al formato delle configurazioni.

- Se le tue configurazioni personalizzate sono sotto forma di programmi o script Python, inseriscile nella cartella `api_helpers/python/` che si **`[account_customizations_name]`** trova nel tuo repository.
- Se le tue configurazioni personalizzate sono sotto forma di script Bash, inseriscile nella cartella **`[account_customizations_name]/api_helpers/`** che si trova nel tuo repository.
- Se le tue configurazioni personalizzate sono sotto forma di Terraform, inseriscile nella cartella `/terraform` che si trova nel tuo repository. **`[account_customizations_name]`**

Per ulteriori informazioni sulla creazione di configurazioni personalizzate, consulta il file `README` per le personalizzazioni dell'account.

3. Fai riferimento al **`account_customizations_name`** parametro specifico nel file di richiesta dell'account

Il file di richiesta dell'account AFT include il parametro di `inputaccount_customizations_name`. Immettete il nome della personalizzazione dell'account come valore per questo parametro.

 Note

È possibile inviare più richieste di account per gli account presenti nel proprio ambiente. Quando desideri applicare personalizzazioni dell'account diverse o simili, specifica le

personalizzazioni dell'account utilizzando il parametro di `account_customizations_name` input nelle richieste dell'account. Per ulteriori informazioni, consulta [Inviare](#) più richieste di account.

Re-invoke personalizzazioni

AFT fornisce un modo per richiamare nuovamente le personalizzazioni nella pipeline AFT. Questo metodo è utile quando è stata aggiunta una nuova fase di personalizzazione o quando si apportano modifiche a una personalizzazione esistente. Quando si richiama nuovamente, AFT avvia la pipeline di personalizzazioni per apportare modifiche all'account fornito da AFT. Un reinvoke basato sull'origine degli eventi consente di applicare personalizzazioni a singoli account, a tutti gli account, agli account in base alla relativa unità organizzativa o agli account selezionati in base ai tag.

Segui questi tre passaggi per richiamare nuovamente le personalizzazioni per gli account. AFT-provisioned

Passaggio 1: invia le modifiche agli archivi di personalizzazione globali o degli account **git**

Puoi aggiornare le personalizzazioni globali e dell'account secondo necessità e inviare le modifiche ai tuoi repository. `git` A questo punto, non succede nulla. La pipeline di personalizzazioni deve essere richiamata da una fonte di eventi, come spiegato nei due passaggi successivi.

Fase 2: Avvia un'esecuzione di AWS Step Function per richiamare nuovamente le personalizzazioni

AFT fornisce una AWS Step Function richiamata `aft-invoke-customizations` nell'account di gestione AFT. Lo scopo di tale funzione è richiamare nuovamente la pipeline di personalizzazione degli account. AFT-provisioned

Ecco un esempio di schema di eventi (formato JSON) che puoi creare per passare l'input a `aft-invoke-customizations` AWS Step Function.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
```

```

    "target_value": [ "ou1","ou2"]
  },
  {
    "type": "tags",
    "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
  },
  {
    "type": "accounts",
    "target_value": [ "acc1_ID","acc2_ID"]
  }
],

"exclude": [
  {
    "type": "ous",
    "target_value": [ "ou1","ou2"]
  },
  {
    "type": "tags",
    "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
  },
  {
    "type": "accounts",
    "target_value": [ "acc1_ID","acc2_ID"]
  }
]
}

```

Lo schema di eventi di esempio mostra che puoi scegliere gli account da includere o escludere dal processo di reinvoke. È possibile filtrare per unità organizzativa (OU), tag di account e ID account. Se non applichi alcun filtro e includi l'estratto conto `"type": "all"`, viene richiamata nuovamente la personalizzazione per tutti AFT-provisioned gli account.

È possibile includere un `bypass_steps` parametro nell'input Step Functions per saltare fasi di provisioning specifiche durante la reinvocazione.

bypass_steps value	Comportamento
<code>["provisioning_bootstrap"]</code>	Salta le fasi di provisioning e bootstrap dell'account; esegue solo le pipeline di personalizzazione globali e dell'account.

bypass_steps value	Comportamento
[](vuoto)	Esegue l'intero flusso, incluso il provisioning (impostazione predefinita).

L'esempio seguente mostra un input Step Functions che richiama nuovamente le personalizzazioni per un account specifico ignorando i passaggi di provisioning e bootstrap.

```
{
  "include": [
    {
      "type": "accounts",
      "target_value": ["123456789012"]
    }
  ],
  "bypass_steps": ["provisioning_bootstrap"]
}
```

Note

Se la tua versione di AWS Control Tower Account Factory for Terraform (AFT) è 1.6.5 o successiva, puoi scegliere come target le unità organizzative annidate con la sintassi `OU Name (ou-id-1234`. Per ulteriori informazioni, consulta il seguente argomento su [GitHub](#).

Per visualizzare in anteprima le modifiche che AFT apporterebbe a un account senza applicarle, utilizzate un'esecuzione solo per il piano. Per avviarne uno, includi un `plan_only` parametro impostato su `true` nell'input Step Functions. Quando lo impostate `"plan_only": true`, AFT viene eseguito `terraform plan` per le personalizzazioni globali e degli `terraform apply` account anziché. È quindi possibile rivedere le modifiche che un account riceverebbe prima di applicarle. Plan-only funziona su tutte le distribuzioni Terraform supportate, tra cui Community Edition, HCP Terraform (Terraform Cloud) e Terraform Enterprise.

L'esempio seguente mostra un input Step Functions che esegue un'esecuzione solo del piano per un account specifico `plan_only` impostando `true` e specificando l'ID dell'account nel blocco `include`

```
{
  "include": [
```

```
{
  "type": "accounts",
  "target_value": ["123456789012"]
},
"plan_only": true
}
```

Nell'esempio precedente, sostituite il seguente valore con le vostre informazioni:

- 123456789012— Sostituisci questo valore con l'ID dell'account AWS che desideri utilizzare come target per l'esecuzione solo del piano.

Dopo aver esaminato l'output del piano, esegui nuovamente la pipeline di personalizzazioni senza il `plan_only` parametro (esecuzione normale) per applicare le modifiche ai tuoi account.

Note

Nella distribuzione Community Edition (open source), AFT esporta l'output JSON di ogni piano nel bucket Amazon S3 crittografato con output del piano nell'account di gestione AFT. Questa esportazione avviene solo per ogni esecuzione del piano. Nelle distribuzioni HCP Terraform (Terraform Cloud) e Terraform Enterprise, puoi visualizzare i risultati del piano nell'interfaccia utente di HCP Terraform run. Facoltativamente, puoi anche esportare l'output JSON di ogni piano nel bucket. Per ulteriori informazioni, consulta [Esporta l'output del piano Terraform su Amazon S3](#).

Dopo aver compilato i parametri dell'evento, Step Functions viene eseguito e richiama le personalizzazioni corrispondenti. AFT può richiamare un massimo di 5 personalizzazioni alla volta. Step Functions attende e si ripete fino al completamento di tutti gli account che soddisfano i criteri dell'evento.

Fase 3: Monitora l'output di AWS Step Function e guarda AWS CodePipeline in esecuzione

- L'output Step Function risultante contiene ID di account che corrispondono alla fonte dell'evento di input di Step Function.
- Accedi ad AWS CodePipeline in Developer Tools e visualizza le pipeline di personalizzazione corrispondenti per l'ID dell'account.

Risoluzione dei problemi relativi al tracciamento delle richieste di personalizzazione dell'account AFT

Flussi di lavoro di personalizzazione degli account basati su AWS Lambda registri di emissione contenenti l'account di destinazione e gli ID delle richieste di personalizzazione. AFT ti consente di tracciare e risolvere i problemi delle richieste di personalizzazione con Amazon CloudWatch Logs fornendoti le query di CloudWatch Logs Insights che puoi utilizzare per filtrare i CloudWatch log relativi alla tua richiesta di personalizzazione in base all'account di destinazione o all'ID della richiesta di personalizzazione. Per ulteriori informazioni, consulta [Analyzing log data with Amazon CloudWatch Logs nella Amazon CloudWatch Logs User Guide](#).

Per utilizzare CloudWatch Logs Insights for AFT

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Dal riquadro di navigazione, scegli Logs, quindi seleziona Logs insights.
3. Scegli Query.
4. In Query di esempio, scegli Account Factory for Terraform, quindi seleziona una delle seguenti query:

- Registri di personalizzazione per ID account

Note

Assicurati di sostituirlo **"YOUR-ACCOUNT-ID"** con l'ID dell'account di destinazione.

```
fields @timestamp, log_message.account_id as target_account_id,  
log_message.customization_request_id as customization_request_id,  
log_message.detail as detail, @logStream  
| sort @timestamp desc  
| filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /  
customization_request_id/
```

- Registri di personalizzazione in base all'ID della richiesta di personalizzazione

Note

Assicurati di sostituirlo **"YOUR-CUSTOMIZATION-REQUEST-ID"** con l'ID della richiesta di personalizzazione. È possibile trovare l'ID della richiesta di

personalizzazione nell'output della macchina a stati del framework di provisioning dell'AFT Account Provisioning Framework AWS Step Functions . Per ulteriori informazioni sull'AFT Account Provisioning Framework, vedete [AFT Account Provisioning Pipeline](#)

```
fields @timestamp, log_message.account_id as target_account_id,  
  log_message.customization_request_id as customization_request_id,  
  log_message.detail as detail, @logStream  
| sort @timestamp desc  
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. Dopo aver selezionato una query, assicuratevi di selezionare un intervallo di tempo, quindi scegliete Esegui query.

Trigger di personalizzazione

I trigger di personalizzazione di Account Factory for Terraform (AFT) automatizzano la riesecuzione degli account e delle personalizzazioni globali quando gli account si spostano tra le unità organizzative (OU). Man mano che l'organizzazione si evolve, gli account passano spesso da un'unità organizzativa all'altra per riflettere i cambiamenti nella proprietà del team, nei requisiti di conformità o nella classificazione dei carichi di lavoro. Senza fattori di personalizzazione, ogni mossa richiede un intervento manuale per riapplicare le personalizzazioni in linea con il nuovo contesto organizzativo dell'account.

Con i trigger di personalizzazione abilitati, AFT rileva le modifiche all'unità organizzativa e richiama automaticamente le pipeline di personalizzazione per gli account interessati. Ciò garantisce che gli account eseguano sempre le personalizzazioni appropriate alla loro attuale collocazione delle unità organizzative, riducendo il sovraccarico operativo e minimizzando il rischio di deviazioni della configurazione. Ad esempio, quando un account passa da un'unità organizzativa di sviluppo a un'unità organizzativa di produzione, i trigger di personalizzazione possono applicare automaticamente controlli di sicurezza e politiche di conformità specifici della produzione senza l'intervento manuale.

Important

Gli account aggiornati tramite la funzionalità Auto Enroll nella landing zone di AWS Control Tower non emettono l'evento del UpdateManagedAccount ciclo di vita. I trigger di

personalizzazione non si attivano per tali operazioni. Se ti affidi ad Auto Enroll per portare gli account sotto la gestione di AWS Control Tower, devi richiamare manualmente le personalizzazioni per tali account.

Come funzionano i trigger di personalizzazione

Quando i trigger di personalizzazione sono abilitati e AFT elabora un evento di provisioning dell'account, valuta se l'unità organizzativa dell'account è cambiata e intraprende le azioni appropriate.

1. AFT rileva una modifica dell'unità organizzativa confrontando l'unità organizzativa corrente dell'account con quella registrata in precedenza.
2. Se l'unità organizzativa viene modificata, AFT arricchisce l'esecuzione con il contesto del trigger, incluse l'unità organizzativa di origine e di destinazione.
3. AFT richiama la pipeline di personalizzazione, ignorando le fasi di provisioning e bootstrap già completate. Per i dettagli sulla configurazione del bypass, vedere. [the section called “Re-invoke personalizzazioni”](#)
4. AFT registra una voce di controllo con gli account di origine e destinazione del trigger.

Se la funzionalità è disabilitata o se l'unità organizzativa non è stata modificata, il provisioning standard continua senza attivare la riesecuzione della personalizzazione.

Configurazione dei trigger di personalizzazione

Per abilitare i trigger di personalizzazione, imposta la `aft_customization_triggers` variabile nel tuo modulo di distribuzione AFT:

```
module "aft" {  
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"  
  
  aft_customization_triggers = ["account_move"]  
  
  # ... other variables  
}
```

L'unico valore valido è "account_move". Per disabilitare i trigger di personalizzazione, imposta la variabile su un elenco vuoto (). [] La funzionalità è disattivata per impostazione predefinita.

Per escludere un account specifico dall'elaborazione automatica dei trigger, imposta l'`account_skip_customization_triggers` attributo su `"true"` per l'account di destinazione nel file Terraform di richiesta dell'account. Quando questo attributo è impostato, AFT salta la chiamata di personalizzazione per quell'account anche quando rileva una modifica dell'unità organizzativa. Ciò è utile per gli account sottoposti a migrazioni pianificate in cui non è richiesta la ripersonalizzazione automatica.

Percorsi di eventi supportati

Il `account_move` trigger si attiva quando AFT riceve un evento del ciclo di vita di `UpdateManagedAccount` AWS Control Tower. Questo evento viene emesso quando:

- L'unità organizzativa di un account viene modificata tramite il file di richiesta dell'account AFT (aggiornamento del `ManagedOrganizationalUnit` parametro Terraform).
- Un account viene aggiornato tramite la console AWS Control Tower.
- Un account viene spostato utilizzando le operazioni Register OU o Account Factory (console o API Service Catalog).

Important

Gli account aggiornati tramite la funzionalità Auto Enroll nella landing zone di AWS Control Tower non emettono l'evento del `UpdateManagedAccount` ciclo di vita. Il trigger di personalizzazione non si attiva per tali operazioni.

Per ulteriori informazioni sugli eventi del ciclo di vita di AWS Control Tower, consulta gli eventi del ciclo di [vita di AWS Control Tower nella Guida](#) per l'utente di AWS Control Tower.

Monitoraggio e tracciabilità

Ogni esecuzione di personalizzazione (attivata da una modifica dell'unità organizzativa, da una chiamata manuale o da una richiesta di account) scrive un record di controllo in una tabella DynamoDB. È possibile utilizzare questi record per capire perché è stata eseguita una personalizzazione, quali account sono stati interessati e in che modo l'esecuzione è correlata ad altre attività della pipeline.

Campo	Description
execution_id	L'ID di esecuzione di Step Functions
timestamp	Quando è stato creato il record
target_accounts	Elenco degli ID degli account di destinazione
bypass_steps	Fasi di provisioning che sono state saltate
customization_triggers	Contesto di attivazione (unità organizzativa di origine e destinazione)
trigger_source	Perché l'esecuzione è stata eseguita: account_move manual, o account_request
customization_request_id	Collega le esecuzioni di provisioning e personalizzazione per una correlazione end-to-end

customization_request_id consente di correlare l'evento di attivazione con l'esecuzione della pipeline a valle su entrambe le macchine a stati Step Functions. È possibile utilizzare questo identificatore per tracciare il passaggio di un singolo account dal rilevamento iniziale al completamento della personalizzazione.

Example Interroga i record di controllo per fonte di attivazione

```
aws dynamodb scan \  
  --table-name aft-customizations-audit \  
  --filter-expression "trigger_source = :ts" \  
  --expression-attribute-values '{"ts": {"S": "account_move"}}'
```

Alternative per il controllo della versione del codice sorgente in AFT

AFT utilizza un sistema AWS CodeCommit di controllo della versione del codice sorgente (VCS) e ne consente altri [AWS CodeConnections](#) che soddisfano i requisiti aziendali o l'architettura esistente.

Se state implementando AFT per la prima volta e non disponete di un CodeCommit repository esistente, dovete specificare un provider VCS esterno, come parte dei prerequisiti per la distribuzione di AFT.

AFT supporta le seguenti alternative di controllo del codice sorgente:

- GitHub
- GitHub Enterprise Server
- BitBucket
- GitLab
- GitLab Self-managed
- Azure DevOps

 Note

Se si specifica AWS CodeCommit come VCS, non sono necessari passaggi aggiuntivi. AFT crea i `git` repository necessari nell'ambiente, con nomi predefiniti. Tuttavia, è possibile sovrascrivere i nomi dei repository predefiniti per conformarsi CodeCommit, se necessario, agli standard organizzativi.

Configurate un sistema di controllo della versione del codice sorgente alternativo (VCS personalizzato) con AFT

Per configurare un sistema di controllo della versione del codice sorgente alternativo per la tua implementazione AFT, segui questi passaggi.

Passaggio 1: creare **git** repository in un sistema di controllo delle versioni (VCS) di terze parti supportato.

Se non si utilizza AWS CodeCommit, è necessario creare `git` repository nell'ambiente di provider VCS di terze parti per i seguenti elementi. AFT-supported

- Richieste di account AFT. [Codice di esempio disponibile](#). Per ulteriori informazioni sulle richieste di account AFT, vedere [Effettua il provisioning di un nuovo account con AFT](#).
- Personalizzazioni del provisioning degli account AFT. [Codice di esempio disponibile](#). Per ulteriori informazioni sulle personalizzazioni del provisioning degli account AFT, vedere. [Crea la tua macchina a stati per il provisioning delle personalizzazioni dell'account AFT](#)
- Personalizzazioni globali AFT. [Codice di esempio disponibile](#). Per ulteriori informazioni sulle personalizzazioni globali AFT, vedere [Personalizzazioni dell'account](#).

- Personalizzazioni dell'account AFT. [Codice di esempio disponibile](#). Per ulteriori informazioni sulle personalizzazioni degli account AFT, vedere [Personalizzazioni dell'account](#).

Fase 2: Specificare i parametri di configurazione VCS necessari per l'implementazione di AFT

I seguenti parametri di input sono necessari per configurare il provider VCS come parte della distribuzione AFT.

- `vcs_provider`: se non lo utilizzi AWS CodeCommit, specifica il provider VCS come,,, o "bitbucket" "github" "githubenterprise" "gitlab" "gitlabselfmanaged" "azuredevops", in base al tuo caso d'uso.
- `github_enterprise_url`: solo per i clienti Enterprise, specifica l'URL. GitHub GitHub
- `account_request_repo_name`: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-request` In un ambiente di provider VCS di terze parti AFT-supported, aggiorna questo valore di input con il nome effettivo del repository. Per BitBucket Github, GitHub Enterprise e Azure GitLab GitLab Self-managed DevOps, il nome del repository deve avere il formato. `[Org]/[Repo]`
- `account_customizations_repo_name`: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-customizations` In un ambiente di provider VCS di terze parti AFT-supported, aggiorna questo valore di input con il nome del repository. Per BitBucket Github, GitHub Enterprise e Azure GitLab GitLab Self-managed DevOps, il nome del repository deve avere il formato. `[Org]/[Repo]`
- `account_provisioning_customizations_repo_name`: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-provisioning-customizations` In un ambiente di provider VCS di terze parti AFT-supported, aggiorna questo valore di input con il nome del repository. Per BitBucket Github, GitHub Enterprise e Azure GitLab GitLab Self-managed DevOps, il nome del repository deve avere il formato. `[Org]/[Repo]`
- `global_customizations_repo_name`: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-global-customizations` In un ambiente di provider VCS di terze parti AFT-supported, aggiorna questo valore di input con il nome del repository. Per BitBucket Github, GitHub Enterprise e Azure GitLab GitLab Self-managed DevOps, il nome del repository deve avere il formato. `[Org]/[Repo]`
- `account_request_repo_branch`: il ramo è predefinito, ma il valore può essere sovrascritto. `main`

Per impostazione predefinita, AFT proviene dal ramo di ogni repository. `main` `git` È possibile sovrascrivere il valore del nome del ramo con un parametro di input aggiuntivo. Per ulteriori informazioni sui parametri di input, fare riferimento al file README nel modulo [AFT Terraform](#).

 Per esistente AWS CodeCommit clienti

Se si crea un CodeCommit repository con un nuovo nome per AFT, è possibile aggiornare il nome del repository aggiornando i valori di questi parametri di input.

Fase 3: Completare la AWS CodeCommit connessione per i provider VCS di terze parti

Quando la distribuzione viene eseguita, AFT crea i AWS CodeCommit repository richiesti oppure crea una AWS CodeCommit connessione per il provider VCS di terze parti scelto. In quest'ultimo caso, è necessario accedere manualmente alla console dell'account di gestione AFT per completare la connessione in sospeso CodeCommit . Consulta [la AWS CodeCommit documentazione](#) per ulteriori istruzioni sul completamento della CodeCommit connessione.

Sposta AFT da AWS CodeCommit a un altro provider VCS

Questa sezione fornisce una panoramica su come spostare AWS Control Tower Account Factory for Terraform (AFT) da AWS CodeCommit sistema di controllo della versione (VCS) a un altro provider VCS.

Fase 1: Configura nuovi repository nel VCS di tua scelta.

Fase 2. Aggiungete questi repository come nuovi telecomandi. `git`

Fase 3. Esegui `git push` sul nuovo provider VCS.

 Note

La struttura del repository che crei dovrebbe essere la stessa di. AWS CodeCommit La modifica della struttura impedisce a AFT di eseguire il codice desiderato.

Struttura del repository:

- `aft-account-request`
- `personalizzazioni aft-account-`
- `personalizzazioni aft-global-`

- personalizzazioni `aft-account-provisioning`

Fase 4. Nel tuo account di gestione AWS Control Tower, aggiorna il modulo Terraform (bootstrap) in modo che punti al tuo provider VCS, come mostrato nell'esempio seguente:

Esempio: [GitLab con Terraform OSS](#)

— Esegui quindi `terraform plan` e `terraform apply` per visualizzare in anteprima le modifiche.

Fase 5: Completa i passaggi per completare la configurazione di CodeConnection (precedentemente noto come CodeStar):

1. Accedi al tuo account di gestione AFT
2. Individua e completa i dati in sospeso AWS CodeConnections per il nuovo provider VCS, come descritto in [Aggiornamento di una connessione in sospeso o nella AWS console](#), []. `https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`
3. Riferimento: passaggi [Post-deployment](#)

Note

Le pipeline degli account conservano la fonte precedente fino a quando non viene *aft-invoke-customizations* richiamato Step Functions. Questa chiamata può essere eseguita come parte dell'aggiornamento o come parte delle successive chiamate di personalizzazione.

Per maggiori informazioni, consulta questo blog: [Come migrare il tuo AWS CodeCommit repository su un altro provider Git.](#)

Protezione dei dati

Il modello di responsabilità [AWS condivisa](#) si applica alla protezione dei dati in AFT. Ai fini della protezione dei dati, consigliamo le seguenti best practice per la sicurezza.

- Segui le linee guida sulla protezione dei dati fornite da AWS Control Tower. Per informazioni dettagliate, vedi [Protezione dei dati in AWS Control Tower](#).

- Conserva la configurazione dello stato di Terraform generata al momento della distribuzione AFT. Per informazioni dettagliate, vedi [Implementa AWS Control Tower Account Factory per Terraform \(AFT\)](#).
- Ruota periodicamente le credenziali sensibili come indicato dalla politica di sicurezza della tua organizzazione. Esempi di segreti sono i token Terraform, i token e git così via.

Crittografia dei dati inattivi

AFT crea bucket Amazon S3, argomenti Amazon SNS, code Amazon SQS e database Amazon DynamoDB crittografati a riposo con chiavi del servizio di gestione delle chiavi. AWS Per impostazione predefinita, le chiavi KMS create da AFT hanno la rotazione annuale abilitata. Se scegli le distribuzioni HCP Terraform o Terraform Enterprise di Terraform, AFT include un SecureString parametro AWS Systems Manager per memorizzare i valori dei token Terraform sensibili.

AFT utilizza i AWS servizi descritti in [Servizi relativi ai componenti](#) che, per impostazione predefinita, sono crittografati a riposo. Per i dettagli, consulta la AWS documentazione per ciascun AWS servizio componente di AFT e scopri le pratiche di protezione dei dati seguite da ciascun servizio.

Crittografia in transito

AFT si basa sui AWS servizi descritti in [Servizi relativi ai componenti](#) che utilizzano la crittografia in transito, per impostazione predefinita. Per i dettagli, consulta la AWS documentazione relativa a ciascun AWS servizio componente di AFT e scopri le pratiche di protezione dei dati seguite da ciascun servizio.

Per le distribuzioni HCP Terraform o Terraform Enterprise, AFT chiama un'API endpoint HTTPS per accedere alla tua organizzazione Terraform. Se scegli un provider VCS di terze parti supportato da AWS CodeStar connessioni, AFT chiama un'API endpoint HTTPS per accedere alla tua organizzazione di provider VCS.

Rimuovere un account da AFT

Questo argomento descrive come rimuovere un account da AFT, in modo che la pipeline AFT interrompa la distribuzione e l'aggiornamento dell'account.

Important

La rimozione di un account dalla pipeline AFT è irreversibile e può comportare una perdita di stato.

È possibile rimuovere un account da AFT quando si desidera chiudere un account per un'applicazione ritirata, isolare un account compromesso o spostare un account da un'organizzazione a un'altra organizzazione.

 Note

La rimozione di un account da AFT è diversa dall'eliminazione di un account AWS Control Tower o Account AWS. Quando rimuovi un account da AFT, AWS Control Tower continua a gestirlo. Per eliminare un account AWS Control Tower oppure Account AWS, consulta quanto segue:

- [Annulla la gestione di un account](#) nella AWS Control Tower User Guide.
- [Chiusura di un account](#) nella Guida per l'AWS Billing utente.

Per rimuovere un account dalle pipeline AFT

La procedura seguente descrive come rimuovere un account da AFT.

1. Rimuovi l'account dal **git** repository che memorizza le richieste di account

Nell'**git** archivio in cui memorizzate le richieste di account, eliminate la richiesta di account per l'account che desiderate rimuovere da AFT.

Quando rimuovi una richiesta di account dall'archivio delle richieste di account, AFT elimina la pipeline di personalizzazione e i metadati dell'account. Per ulteriori informazioni, consultate le note di rilascio della versione [1.8.0](#) per AFT on. GitHub

2. Elimina l'area di lavoro Terraform (solo per i clienti HCP Terraform e Terraform Enterprise)

Elimina gli spazi di lavoro per le personalizzazioni globali e le personalizzazioni degli account per l'account che desideri rimuovere da AFT.

3. Elimina lo stato Terraform dal backend di Amazon S3

Nell'account di gestione AFT, elimina tutte le cartelle pertinenti all'interno dei bucket Amazon S3 per l'account che desideri rimuovere da AFT.

 Tip

Negli esempi seguenti, sostituiscilo **012345678901** con il numero ID dell'account di gestione AFT.

Esempio: Terraform OSS

Quando scegli Terraform OSS, trovi 3 cartelle per ogni account nei bucket `aft-backend-012345678901-primary-region` e `aft-backend-012345678901-secondary-region` Amazon S3. Queste cartelle sono correlate allo stato delle personalizzazioni dell'account, allo stato della pipeline di personalizzazione e allo stato delle personalizzazioni globali

Esempio: HCP Terraform o Terraform Enterprise

Quando scegli HCP Terraform o Terraform Enterprise, trovi una cartella per ogni account nei bucket Amazon `aft-backend-012345678901-primary-region` S3 `aft-backend-012345678901-secondary-region` e Amazon. Queste cartelle sono correlate allo stato della pipeline di personalizzazione.

Parametri operativi

Per impostazione predefinita, Account Factory for Terraform (AFT) invia metriche operative anonime a AWS. Utilizziamo questi dati per capire in che modo i clienti utilizzano AFT in modo da poter migliorare la qualità e le funzionalità della soluzione. È possibile disattivare la raccolta dei dati modificando un parametro durante l'implementazione di AFT. Quando la raccolta è abilitata, i seguenti dati vengono inviati a AWS:

- Soluzione: l'identificatore specifico di AFT
- Versione: la versione di AFT
- Identificatore univoco universale (UUID): identificatore univoco generato casualmente per ogni implementazione AFT
- Timestamp: marcatura temporale di raccolta dati
- Dati: configurazione AFT e azioni intraprese dal cliente

AWS possiede i dati raccolti. La raccolta dei dati è soggetta all'[AWS Informativa sulla privacy](#).

Note

Le versioni di AFT precedenti alla 1.6.0 non riportano le metriche di utilizzo a. AWS

Per disattivare le metriche di rendicontazione:

- Imposta il valore di input `aft_metrics_reporting` to `false` nel tuo file di configurazione di input Terraform, come mostrato nell'esempio che segue, e ridistribuisce AFT. Questo valore è impostato su di `true` default, se non lo impostate in modo esplicito.

Se copi l'esempio, ricordati di sostituire i valori ID e Region effettivi con gli elementi forniti nelle stringhe con. x

```
module "control_tower_account_factory" {  
  source = "aws-ia/control_tower_account_factory/aws"  
  
  # Required Vars  
  ct_management_account_id      = "xxxxxxxxxxxx"  
  log_archive_account_id       = "xxxxxxxxxxxx"  
  audit_account_id             = "xxxxxxxxxxxx"  
  aft_management_account_id     = "xxxxxxxxxxxx"  
  ct_home_region               = "xx-xxxx-x"  
  tf_backend_secondary_region = "xx-xxxx-x"  
  
  # Optional Vars  
  aft_metrics_reporting = false    # to opt out, set this value to false  
}
```

Guida alla risoluzione dei problemi di Account Factory for Terraform (AFT)

Questa sezione può aiutarti a risolvere i problemi più comuni che potresti riscontrare quando usi Account Factory for Terraform (AFT).

Argomenti

- [Problemi generali](#)

- [Problemi relativi all'account provisioning/registration](#)
- [Problemi relativi all'invocazione delle personalizzazioni](#)
- [Problemi relativi al flusso di lavoro per la personalizzazione degli account](#)

Problemi generali

- Quote di risorse superate AWS

Se i gruppi di log indicano che hai superato le quote di AWS risorse, contatta l'assistenza. [AWS Account Factory](#) utilizza Servizi AWS con quote di risorse che includono AWS CodeBuild, e AWS Organizations. AWS Systems Manager Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Che cos'è AWS CodeBuild?](#) nella Guida CodeBuild per l'utente.
 - [Che cos'è AWS Organizations?](#) nella Guida per l'utente delle organizzazioni.
 - [Che cos'è AWS Systems Manager?](#) nella Guida per l'utente di Systems Manager.
- Versione obsoleta di Account Factory

Se riscontri un problema e ritieni che si tratti di un bug, assicurati di disporre della versione più recente di Account Factory. Per ulteriori informazioni, consulta [Aggiornamento della versione di Account Factory](#).

- Sono state apportate modifiche locali al codice sorgente di Account Factory

Account Factory è un progetto open source. AWS Control Tower supporta il codice di base di Account Factory. Se apporti una modifica locale al codice di base di Account Factory, AWS Control Tower supporta l'implementazione di Account Factory solo nel migliore dei modi.

- Autorizzazioni per i ruoli Account Factory insufficienti

Account Factory crea ruoli e policy IAM per gestire le implementazioni e le personalizzazioni degli account venduti. Se modifichi questi ruoli o politiche, la pipeline di Account Factory potrebbe non essere in grado di eseguire determinate azioni. Per ulteriori informazioni, consulta Ruoli <https://docs.aws.amazon.com/controltower/latest/userguide/aft-required-roles.html> obbligatori.

- Gli archivi degli account non sono stati compilati correttamente

Assicurati di seguire i passaggi <https://docs.aws.amazon.com/controltower/latest/userguide/aft-post-deployment.html> successivi all'implementazione prima di effettuare il provisioning degli account.

- Non viene rilevata alcuna deriva dopo aver modificato manualmente l'unità organizzativa

 Note

AWS Control Tower rileva automaticamente la deriva. Per informazioni sulla risoluzione della deriva, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

La deriva non viene rilevata quando l'unità organizzativa (OU) viene modificata manualmente. Ciò è dovuto alla natura di Account Factory basata sugli eventi. Quando viene inviata una richiesta di account, la risorsa gestita da Terraform è un articolo Amazon DynamoDB, non un account diretto. Dopo la modifica di un elemento, la richiesta viene messa in coda, dove AWS Control Tower la elabora tramite Service Catalog (il servizio che gestisce i dettagli dell'account). Se modifichi l'unità organizzativa manualmente, la deriva non viene rilevata perché la richiesta dell'account non è cambiata.

Problemi relativi all'account provisioning/registration

- La richiesta di account (email address/name) esiste già

Il problema si traduce in genere in un errore di un prodotto Service Catalog durante il provisioning o `asConditionalCheckFailedException`.

È possibile trovare ulteriori informazioni sul problema effettuando una delle seguenti operazioni:

- Controlla i tuoi gruppi di CloudWatch log Terraform o Logs.
- Esamina gli errori che vengono generati nell'argomento Amazon SNS. `aft-failure-notifications`
- Richiesta di account non valida

Assicurati che la richiesta dell'account segua lo schema previsto. Per esempi, vedi https://github.com/aws-ia/terraform-aws-control_tower_account_factory/tree/main/sources/aft-customizations-repos/aft-account-request/examples terraform-aws-control_tower_account_factory on. GitHub

- AWS Quote di risorse delle organizzazioni superate

Assicurati che la richiesta del tuo account non superi le quote di AWS Organizations risorse. Per ulteriori informazioni, consulta [Quote per AWS le organizzazioni](#).

Problemi relativi all'invocazione delle personalizzazioni

- Account di destinazione non inserito in Account Factory

Assicurati che tutti gli account inclusi in una richiesta di personalizzazione siano stati inseriti in Account Factory. Per ulteriori informazioni, consulta [Aggiornare un account esistente](#).

- L'account a cui sono destinate le richieste di personalizzazione è presente nella tabella **DynamoDBaft-request-metadata**, ma non nell'archivio delle richieste di account

Formatta la richiesta di richiamo della personalizzazione per escludere l'account incriminato effettuando una delle seguenti operazioni:

- Nella tabella **DynamoDBaft-request-metadata**, elimina la voce che fa riferimento all'account che non è più presente nell'archivio delle richieste di account.
 - Non utilizzare «tutti» come destinazione.
 - Non è indirizzato all'unità organizzativa a cui appartiene l'account.
 - Non indirizzato direttamente all'account.
- Token errato utilizzato per HCP Terraform

Assicurati di aver impostato il token corretto. HCP Terraform supporta solo token basati sul team, non token basati sull'organizzazione.

- Creazione dell'account non riuscita prima della creazione della pipeline di personalizzazione dell'account; impossibile personalizzare l'account

Apporta una modifica alle specifiche dell'account nell'archivio delle richieste di account. Quando apporti una modifica, ad esempio la modifica del valore di un tag per un account, Account Factory segue il percorso che tenta di creare la pipeline, anche se la pipeline non esiste.

Problemi relativi al flusso di lavoro per la personalizzazione degli account

Se riscontri problemi relativi al flusso di lavoro di personalizzazione degli account, assicurati che la tua versione di AFT sia 1.8.0 o successiva e di eliminare tutte le istanze di metadati relativi all'account dalla tabella delle richieste di DynamoDB.

Per informazioni sulla versione 1.8.0 di AFT, consulta la versione 1.8.0 in poi. https://github.com/aws-ia/terraform-aws-control_tower_account_factory/releases/tag/1.8.0 GitHub

Per informazioni su come controllare e aggiornare la tua versione di AFT, vedi quanto segue:

- [Controllate la versione AFT](#)
- [Aggiorna la versione AFT](#)

Puoi anche tracciare e risolvere i problemi delle richieste di personalizzazione utilizzando le query di Amazon CloudWatch Logs Insights per filtrare i log contenenti l'account di destinazione e gli ID delle richieste di personalizzazione. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi al tracciamento delle richieste di personalizzazione degli account AFT](#).

Rileva e risolvi la deriva in AWS Control Tower

Identificare e risolvere la deriva è un'attività operativa regolare per gli amministratori degli account di gestione di AWS Control Tower. Risolvere la deriva aiuta a garantire la conformità ai requisiti di governance.

Quando crei la landing zone, la landing zone e tutte le unità organizzative (OU), gli account e le risorse sono conformi alle regole di governance applicate dai controlli scelti. Man mano che tu e i membri della tua organizzazione utilizzate la landing zone, potrebbero verificarsi cambiamenti in questo stato di conformità. Alcune modifiche potrebbero essere accidentali mentre altre potrebbero essere apportate intenzionalmente per rispondere a eventi operativi prioritari.

Il rilevamento della deviazione aiuta a identificare le risorse che richiedono modifiche o aggiornamenti di configurazione per risolvere la deviazione.

Rilevamento della deriva

AWS Control Tower rileva automaticamente la deriva. Per rilevare la deriva, il `AWSControlTowerAdmin` ruolo richiede un accesso persistente all'account di gestione in modo che AWS Control Tower possa effettuare chiamate API di sola lettura verso AWS Organizations. Queste chiamate API vengono visualizzate come eventi. AWS CloudTrail

La deriva per un account membro viene evidenziata nelle notifiche di Amazon Simple Notification Service (Amazon SNS) aggregate nell'account di controllo. Le notifiche in ogni account membro inviano avvisi a un argomento locale di Amazon SNS e a una funzione Lambda.

Note

Quando la funzionalità di registrazione automatica per gli account è abilitata in Impostazioni, queste notifiche SNS non sono disponibili.

Per i controlli che fanno parte dello AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower, la deriva viene mostrata nelle pagine dei dettagli dell'account e dell'account nella console AWS Control Tower, nonché tramite una notifica Amazon SNS.

Gli amministratori degli account membri possono (e, come best practice, devono) sottoscrivere le notifiche di deriva SNS per account specifici. Ad esempio, l'argomento `aws-controltower-`

AggregateSecurityNotifications SNS fornisce notifiche di deviazione. La console AWS Control Tower indica agli amministratori degli account di gestione quando si è verificata una deriva. Per ulteriori informazioni sugli argomenti SNS relativi al rilevamento e alla notifica delle deviazioni, consulta Prevenzione e notifica delle [deviazioni](#).

Deduplicazione delle notifiche Drift

Se lo stesso tipo di deriva si verifica più volte sullo stesso set di risorse, AWS Control Tower invia una notifica SNS solo per l'istanza iniziale di drift. Se AWS Control Tower rileva che questa istanza di deriva è stata risolta, invia un'altra notifica solo se la deriva si ripresenta per quelle risorse identiche.

Esempio: la deriva da SCP viene gestita nel modo seguente

- Se modifichi lo stesso SCP gestito più volte, ricevi una notifica per la prima volta che lo modifichi.
- Se modifichi un SCP gestito, quindi correggi una deriva e poi lo modifichi nuovamente, riceverai due notifiche.

Tipi di deviazione dell'account

- Account spostato tra unità organizzative (vedi [Deriva dell'ereditarietà sulle linee di base abilitate](#) e [Modifica dell'ereditarietà sui controlli abilitati](#))
- Account rimosso dall'organizzazione

Note

Quando si sposta un account da un'unità organizzativa all'altra, i controlli dell'unità organizzativa precedente non vengono rimossi. Se si abilita un nuovo controllo basato su hook sull'unità organizzativa di destinazione, il vecchio il controllo basato su hook viene rimosso dall'account e il nuovo controllo lo sostituisce. I controlli implementati con SCP e AWS Config le regole devono sempre essere rimossi manualmente quando un account cambia unità organizzativa.

Esempi di deriva politica

- SCP aggiornato
- SCP si è staccato da OU

Per ulteriori informazioni, vedere [Types of Governance](#) Drift.

Visualizzazione della deriva

È possibile visualizzare lo stato di deviazione degli account e delle unità organizzative tramite la console o le API e identificare quando le configurazioni di account e unità organizzative sono diverse o non sincronizzate. Lo stato di drift viene comunicato anche tramite messaggi SNS. Per ulteriori informazioni sulla ricezione di questi messaggi SNS, consulta la [Guida alla sottoscrizione agli argomenti](#) SNS.

Per visualizzare lo stato delle unità organizzative e delle variazioni dell'account nella console, vai alla pagina Organizzazione, quindi seleziona le unità organizzative o gli account che desideri controllare.

Per visualizzare lo stato di deviazione delle unità organizzative e degli account a livello di codice, chiama l'[ListEnabledBaselines](#) API per visualizzare gli stati delle linee di base abilitate. Per visualizzare gli stati dei singoli account in modo programmatico con l'API, utilizza il flag. `ListEnabledBaselines includeChildren` Puoi filtrare in base a questi stati e visualizzare solo gli account e le unità organizzative che richiedono la tua attenzione.

Note

AWS Control Tower genera un [evento del ciclo](#) di vita al termine di ogni operazione di correzione della deriva.

Risolvere la deriva

Sebbene il rilevamento sia automatico, i passaggi per risolvere la deriva devono essere eseguiti manualmente tramite la console o con le API. (Tranne in alcuni casi in cui la registrazione automatica è abilitata per gli account che vengono spostati.)

Ad esempio, puoi risolvere la divergenza delle politiche per i controlli a livello di codice, chiamando l'API. [ResetEnabledControl](#)

Per risolvere la deviazione della linea di base della configurazione per un'unità organizzativa, è possibile scegliere Re-register l'unità organizzativa nella console. Se la deriva è causata da un singolo account, puoi scegliere Aggiorna account nella console. Per risolvere la deriva di base con le API, puoi chiamare l'[ResetEnabledBaseline](#) API sull'unità organizzativa.

Riepilogo

- Molti tipi di deriva possono essere risolti tramite la pagina delle impostazioni della zona di atterraggio. Puoi scegliere il pulsante Ripristina nella sezione Versioni per risolvere questi tipi di deriva.
- Se l'unità organizzativa ha meno di 1000 account, è possibile risolvere la deriva negli account forniti da Account Factory, o deriva da SCP, selezionando Re-registerOU nella pagina Organizzazione o nella pagina dei dettagli dell'unità organizzativa.
- È possibile risolvere il problema della deriva dell'account, ad esempio aggiornando un singolo [Account membro trasferito](#) account. Per ulteriori informazioni, consulta [Aggiorna l'account nella console](#).
- [Per quanto riguarda i controlli, è possibile risolvere molti tipi di deviazioni chiamando l'ResetEnabledControlAPI.](#)
- La deviazione di base delle unità Re-register organizzative e degli account può essere risolta chiamando l'[ResetEnabledBaselineAPI](#) o scegliendo l'unità organizzativa o l'account Update nella console AWS Control Tower.
- Per risolvere il problema della deriva ereditaria che si verifica quando gli account vengono spostati tra le unità organizzative, è possibile abilitare la funzionalità di registrazione automatica. Quando la registrazione automatica è abilitata, AWS Control Tower corregge automaticamente la deriva dell'ereditarietà applicando le risorse di base e le configurazioni di controllo dall'unità organizzativa di destinazione all'account spostato. Puoi abilitare la registrazione automatica nella pagina Impostazioni della landing zone nella console o chiamando l'[UpdateLandingZoneAPI](#) con il **RemediationType** parametro impostato su Inheritance Drift. Per ulteriori informazioni, consulta [Sposta e registra gli account con la registrazione automatica](#).

 Quando si interviene per risolvere il problema della deriva in una versione con landing zone, il comportamento dipende dalla versione corrente.

- Se utilizzi la versione 3.1 o successiva della landing zone, puoi scegliere Aggiorna per modificare la configurazione della landing zone senza aggiornare le versioni, oppure scegliere Ripristina per riapplicare le configurazioni salvate alle risorse della tua drifted landing zone. La deriva viene risolta come parte del processo di aggiornamento.
- Se utilizzi una versione di landing zone precedente alla 3.1, non puoi scegliere Reset. Devi scegliere Aggiorna e aggiornare la tua landing zone almeno alla versione 3.1.

Considerazioni sulla deriva e sulla scansione delle politiche

AWS Control Tower analizza quotidianamente gli SCP, gli RCP e le policy dichiarative gestiti per verificare che i controlli corrispondenti siano applicati correttamente e che non abbiano subito variazioni. Per recuperare queste risorse ed eseguire controlli su di esse, AWS Control Tower chiama AWS Organizations per tuo conto, utilizzando un ruolo nel tuo account di gestione.

Se una scansione di AWS Control Tower rileva una deriva, riceverai una notifica. AWS Control Tower invia una sola notifica per problema di deriva, quindi se la tua landing zone è già in stato di deriva, non riceverai notifiche aggiuntive a meno che non venga trovato un nuovo elemento di drift.

AWS Organizations limita la frequenza con cui ciascuna delle sue API può essere chiamata. Questo limite è espresso in transazioni al secondo (TPS) ed è noto come limite TPS, velocità di limitazione o frequenza di richiesta API. Quando AWS Control Tower verifica i tuoi SCP, RCP e policy dichiarative chiamando AWS Organizations, le chiamate API effettuate da AWS Control Tower vengono conteggiate ai fini del limite TPS, poiché AWS Control Tower utilizza l'account di gestione per effettuare le chiamate.

In rare situazioni, questo limite può essere raggiunto chiamando ripetutamente le stesse API, tramite una soluzione di terze parti o uno script personalizzato scritto da te. Ad esempio, se tu e AWS Control Tower chiamate le stesse AWS Organizations API nello stesso momento (entro 1 secondo) e vengono raggiunti i limiti TPS, le chiamate successive vengono limitate. Cioè, queste chiamate restituiscono un errore come `Rate exceeded`.

Se viene superata la frequenza di una richiesta API

- Se AWS Control Tower raggiunge il limite e viene rallentato, sospendiamo l'esecuzione dell'audit e la riprendiamo in un secondo momento.
- Se il carico di lavoro raggiunge il limite e viene limitato, il risultato può variare da una leggera latenza fino a un errore fatale nel carico di lavoro, a seconda di come è configurato il carico di lavoro. Questo caso limite è qualcosa di cui essere consapevoli.

Una scansione SCP giornaliera è composta da

1. Recupero delle unità organizzative attive di recente.
2. Per ogni unità organizzativa registrata, recupero di tutti gli SCP gestiti da AWS Control Tower collegati all'unità organizzativa. Gli SCP gestiti hanno identificatori che iniziano con `aws-guardrails`

3. Per ogni controllo preventivo abilitato sull'unità organizzativa, verifica che la dichiarazione politica del controllo sia presente negli SCP gestiti dall'OU.

Un'unità organizzativa può avere uno o più SCP gestiti.

Tipi di deriva da risolvere immediatamente

La maggior parte dei tipi di deviazione può essere risolta dagli amministratori. Alcuni tipi di deriva devono essere risolti immediatamente, inclusa la cancellazione di un'unità organizzativa richiesta dalla landing zone di AWS Control Tower. Ecco alcuni esempi di deriva grave che potresti voler evitare:

- Non eliminare l'unità organizzativa di sicurezza: l'unità organizzativa originariamente denominata Security durante la configurazione della landing zone da parte di AWS Control Tower non deve essere eliminata. Se la elimini, vedrai un messaggio di errore che ti chiede di reimpostare immediatamente la landing zone. Non potrai intraprendere altre azioni in AWS Control Tower fino al completamento del ripristino.
- Non eliminare i ruoli richiesti: AWS Control Tower verifica determinati ruoli AWS Identity and Access Management (IAM) quando accedi alla console per rilevare eventuali variazioni dei ruoli IAM. Se questi ruoli sono mancanti o inaccessibili, vedrai una pagina di errore che ti chiederà di reimpostare la landing zone. Questi ruoli sono: `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole`

Per ulteriori informazioni su questi ruoli, consulta [Autorizzazioni necessarie per utilizzare la console AWS Control Tower](#).

- Non eliminare tutte le unità organizzative aggiuntive: è necessaria almeno un'unità organizzativa aggiuntiva per il funzionamento di AWS Control Tower, ma non deve essere necessariamente l'unità organizzativa Sandbox.
- Non rimuovere gli account condivisi: se rimuovi account condivisi dalle unità organizzative Foundational con la AWS Organizations console o le API, ad esempio rimuovendo l'account di registrazione dall'unità organizzativa di sicurezza. Lo spostamento di questi account crea un tipo di deriva da Move Account a cui è necessario porre rimedio. Per porre rimedio a questo tipo di deriva, è necessario aggiornare la landing zone.

 Note

È consigliabile non spostare questi account condivisi dall'unità organizzativa Foundational.

Modifiche riparabili alle risorse

Di seguito è riportato un elenco di modifiche alle risorse AWS Control Tower consentite, sebbene creino una deriva risolvibile. I risultati di queste operazioni consentite sono visualizzabili nella console AWS Control Tower, sebbene possa essere necessario un aggiornamento.

Per ulteriori informazioni su come risolvere la deriva risultante, consulta [Managing Resources Outside of AWS Control Tower](#).

Modifiche consentite al di fuori della console AWS Control Tower

- Cambia il nome di un'unità organizzativa registrata.
- Modificare il nome dell'unità organizzativa di sicurezza.
- Modifica il nome degli account dei membri nelle unità organizzative non di base.
- Eliminare un'unità organizzativa non fondamentale.
- Eliminare un account registrato da un'unità organizzativa non fondamentale.
- Modifica l'indirizzo e-mail di un account condiviso nell'unità organizzativa di sicurezza.
- Modifica l'indirizzo e-mail di un account membro in un'unità organizzativa registrata.

 Note

Lo spostamento di account tra le unità organizzative è considerato una deriva e deve essere risolto.

Drift e fornitura di nuovi account

Se la tua landing zone è in uno stato di deriva, la funzionalità di registrazione dell'account in AWS Control Tower non funzionerà. In tal caso, devi fornire nuovi account tramite AWS Service Catalog. Per istruzioni, consulta l'argomento [Esegui il provisioning degli account nella console Service Catalog, con Account Factory](#).

In particolare, se hai apportato alcune modifiche ai tuoi account tramite Service Catalog, come cambiare il nome del tuo portafoglio, la funzione di registrazione dell'account non funzionerà.

Tipi di deriva della governance

La deriva della governance, chiamata anche deriva organizzativa, si verifica quando le unità organizzative, gli SCP e gli account dei membri vengono modificati o aggiornati. I tipi di deviazione della governance che possono essere rilevati in AWS Control Tower sono i seguenti:

- Diversità nella governance di account e unità organizzative
- Deriva della zona di atterraggio
- Controlla la deriva per i controlli non SCP
- Deriva ereditaria per linee di base e controlli

Le sezioni successive forniscono dettagli su questi tipi di deriva segnalati da AWS Control Tower e su come risolverli.

Note

AWS Control Tower interromperà l'invio di notifiche di drift all'argomento SNS per i clienti LZ4.0 + e inizierà invece a inviare notifiche di drift EventBridge all'account di gestione. Per vedere esempi di eventi e linee guida su come ricevere notifiche di drift, EventBridge consulta la sezione seguente sulla creazione. EventBridge

Cambiamenti nella governance di account e unità organizzative

- [Account membro trasferito](#)
- [Account membro rimosso](#)
- [Aggiornamento non pianificato a SCP gestito](#)
- [SCP scollegato dall'unità organizzativa gestita](#)

Deriva della zona di atterraggio

Un altro tipo di deriva è la deriva delle landing zone, che può essere trovata tramite l'account di gestione. La deriva della zona di atterraggio consiste nella deriva dei ruoli IAM o in qualsiasi tipo di

deriva organizzativa che influisca specificamente sulle unità organizzative di base e sugli account condivisi.

- [Foundational OU eliminata](#)
- [Accesso affidabile disabilitato](#)

Un caso particolare di deriva delle landing zone è la deriva dei ruoli, che viene rilevata quando un ruolo richiesto non è disponibile. Se si verifica questo tipo di deriva, la console visualizza una pagina di avviso e alcune istruzioni su come ripristinare il ruolo. La landing zone non è disponibile finché non viene risolto il problema del ruolo. Per ulteriori informazioni sulla deriva dei ruoli, consulta [Non eliminare i ruoli obbligatori nella sezione chiamata. Tipi di deriva da risolvere immediatamente](#)

Control drift per i controlli non SCP

AWS Control Tower segnala la deriva del controllo per quanto riguarda i controlli implementati con le policy di controllo delle risorse (RCP), le politiche dichiarative e i controlli che fanno parte dello AWS Security Hub CSPM Service-managed Standard: AWS Control Tower.

- [Deriva di controllo CSPM del Security Hub](#)
- [Controlla la deriva delle politiche](#)

Variazione dell'ereditarietà per linee di base e controlli

- Deriva della linea di base abilitata

Quando le configurazioni di base su un account membro sono diverse da quelle applicate all'unità organizzativa principale, AWS Control Tower segnala lo spostamento dell'ereditarietà per le baseline abilitate (configurazioni delle risorse) su tali unità organizzative e account. [Per ulteriori informazioni sulle linee di base, consulta Tipi di linee di base.](#)

- [Deriva dell'ereditarietà sulle linee di base abilitate](#)
- Control drift abilitato

Quando le configurazioni di controllo abilitate su un account membro sono diverse da quelle applicate all'unità organizzativa principale, AWS Control Tower segnala una variazione di ereditarietà per i controlli abilitati su tali unità organizzative e account.

- [Modifica dell'ereditarietà sui controlli abilitati](#)

Deriva non segnalata

- AWS Control Tower non rileva differenze rispetto ad altri servizi che funzionano con l'account di gestione AWS CloudTrail, tra cui Amazon CloudWatch, IAM Identity Center e così via. CloudFormation AWS Config
- AWS Control Tower non rileva la deriva delle risorse o altri tipi di deriva che può verificarsi se si modificano le risorse contenute in una baseline.

Account membro trasferito

Note

Per i clienti con LZ 4.0+, AWS Control Tower non invierà notifiche di spostamento dell'account per gli account Account Factory sprovvisti di. `AWSControlTowerBaseline`

Questo tipo di deviazione si verifica sull'account anziché sull'unità organizzativa. Questo tipo di deriva può verificarsi quando un account membro di AWS Control Tower, l'account di audit o l'account di archiviazione dei log viene spostato da un'unità organizzativa AWS Control Tower registrata a qualsiasi altra unità organizzativa. In molti casi, puoi evitare questo tipo di deriva attivando la funzione di registrazione automatica per gli account, nella pagina Impostazioni. Per ulteriori dettagli, consultare [Sposta e registra gli account con la registrazione automatica](#).

Di seguito è riportato un esempio di notifica di deriva quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more than 1000 accounts, you must update the provisioned product in Account Factory.",
}
```

```
"AccountId" : "012345678909",  
"SourceId" : "012345678909",  
"DestinationId" : "ou-3210-1EXAMPLE"  
}
```

Risoluzioni

Quando si verifica questo tipo di deviazione per un account fornito da Account Factory in un'unità organizzativa con un massimo di 1000 account, è possibile risolverlo nei seguenti modi:

- Accedere alla pagina Organizzazione nella console AWS Control Tower, selezionare l'account e scegliere **Aggiorna account** in alto a destra (l'opzione più veloce per i singoli account).
- Accedere alla pagina Organizzazione nella console AWS Control Tower, quindi scegliere **Re-register** l'unità organizzativa che contiene l'account (l'opzione più veloce per più account). Per ulteriori informazioni, consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#).
- Aggiornamento del prodotto fornito in Account Factory. Per ulteriori informazioni, consulta [Aggiorna e sposta gli account con AWS Control Tower](#).

Note

Se hai diversi account individuali da aggiornare, consulta anche questo metodo per effettuare aggiornamenti con uno script: [Fornisci e aggiorna gli account utilizzando l'automazione](#).

- Quando si verifica questo tipo di deriva in un'unità organizzativa con più di 1000 account, la risoluzione della deriva può dipendere dal tipo di account spostato, come spiegato nei paragrafi successivi. Per ulteriori informazioni, consulta [Aggiorna la tua landing zone](#).
- Se un account dotato di Account Factory viene spostato: in un'unità organizzativa con meno di 1000 account, puoi risolvere il problema aggiornando il prodotto di cui hai effettuato il provisioning in Account Factory, registrando nuovamente l'unità organizzativa o aggiornando la landing zone.

In un'unità organizzativa con più di 1000 account, è necessario risolvere il problema aggiornando ogni account spostato, tramite la console AWS Control Tower o il prodotto fornito, poiché l'Re-register unità organizzativa non eseguirà l'aggiornamento. Per ulteriori informazioni, consulta [Aggiorna e sposta gli account con AWS Control Tower](#).

- Se viene spostato un account condiviso: puoi risolvere il problema derivante dallo spostamento dell'account di controllo o dell'archivio dei log aggiornando la landing zone. Per ulteriori informazioni, consulta [Aggiorna la tua landing zone](#).

Nome di campo obsoleto

Il nome del campo `MasterAccountID` è stato modificato in conformità `ManagementAccountID` alle linee guida. AWS Il vecchio nome è obsoleto. Dal 2022, gli script che contengono il nome di campo obsoleto non funzionano più.

Account membro rimosso

Questo tipo di deriva può verificarsi quando un account membro viene rimosso da un'unità organizzativa AWS Control Tower registrata. L'esempio seguente mostra la notifica di deriva quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has been removed from organization o-123EXAMPLE. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory provisioned product",
  "AccountId" : "012345678909"
}
```

Risoluzione

- Quando si verifica questo tipo di deviazione in un account membro, puoi risolverla aggiornando l'account nella console AWS Control Tower o in Account Factory. Ad esempio, è possibile aggiungere l'account a un'altra unità organizzativa registrata dalla procedura guidata di aggiornamento di Account Factory. Per ulteriori informazioni, consulta [Aggiorna e sposta gli account con AWS Control Tower](#).

- Se un account condiviso viene rimosso da un'unità organizzativa Foundational, devi risolvere il problema reimpostando la landing zone. Fino a quando questa deriva non sarà risolta, non sarà possibile utilizzare la console AWS Control Tower.
- Per ulteriori informazioni sulla risoluzione della deviazione per gli account e le unità di gestione, vedere [Se gestisci risorse all'esterno di AWS Control Tower](#).

Note

In Service Catalog, il prodotto fornito da Account Factory che rappresenta l'account non viene aggiornato per rimuovere l'account. Al contrario, il prodotto sottoposto a provisioning viene visualizzato come TAIANTED e in uno stato di errore. Per eseguire la pulizia, vai al Service Catalog, scegli il prodotto fornito, quindi scegli Termina.

Aggiornamento non pianificato a SCP gestito

Questo tipo di deriva può verificarsi quando un SCP per un controllo viene aggiornato nella AWS Organizations console o a livello di codice utilizzando uno degli SDK AWS CLI AWS. Di seguito è riportato un esempio di notifica di deriva quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Risoluzione

Quando si verifica questo tipo di deriva in un'unità organizzativa con un massimo di 1000 account, è possibile risolverlo nei seguenti modi:

- Accedere alla pagina Organizzazione nella console AWS Control Tower per registrare nuovamente l'unità organizzativa (opzione più rapida). Per ulteriori informazioni, consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#).
- Aggiornamento della landing zone (opzione più lenta). Per ulteriori informazioni, consulta [Aggiorna la tua landing zone](#).

Se si verifica questo tipo di deriva in un'unità organizzativa con più di 1000 account, risolverlo aggiornando la landing zone. Per ulteriori informazioni, consulta [Aggiorna la tua landing zone](#).

SCP scollegato dall'unità organizzativa gestita

Questo tipo di deriva può verificarsi quando un SCP per un controllo è stato scollegato da un'unità organizzativa gestita da AWS Control Tower. Questo evento è particolarmente comune quando lavori dall'esterno della console AWS Control Tower. Di seguito è riportato un esempio di notifica di deriva quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Risoluzione

Quando si verifica questo tipo di deriva in un'unità organizzativa con un massimo di 1000 account, è possibile risolverlo nei seguenti modi:

- Accedere all'unità organizzativa nella console AWS Control Tower per registrare nuovamente l'unità organizzativa (opzione più rapida). Per ulteriori informazioni, consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#).

- Aggiornamento della landing zone (opzione più lenta). Se la deriva influisce su un controllo obbligatorio, il processo di aggiornamento crea una nuova policy di controllo del servizio (SCP) e la collega all'unità organizzativa per risolvere la deriva. Per ulteriori informazioni su come aggiornare la landing zone, consulta [Aggiorna la tua landing zone](#).

Se si verifica questo tipo di deriva in un'unità organizzativa con più di 1000 account, risolvi il problema aggiornando la landing zone. Se la deriva influisce su un controllo obbligatorio, il processo di aggiornamento crea una nuova policy di controllo del servizio (SCP) e la collega all'unità organizzativa per risolvere la deriva. Per ulteriori informazioni su come aggiornare la landing zone, consulta [Aggiorna la tua landing zone](#).

Foundational OU eliminata

Questo tipo di deriva si applica solo alle unità organizzative AWS Control Tower Foundational, come l'unità organizzativa Security. Può verificarsi se un'unità organizzativa Foundational viene eliminata al di fuori della console AWS Control Tower. Le unità organizzative di base non possono essere spostate senza creare questo tipo di deriva, perché spostare un'unità organizzativa equivale a eliminarla e aggiungerla altrove. Quando risolvi la deriva aggiornando la landing zone, AWS Control Tower sostituisce l'unità organizzativa Foundational nella posizione originale. L'esempio seguente mostra una notifica di deriva che potresti ricevere quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

Risoluzione

Poiché questa deriva si verifica solo per le unità organizzative fondamentali, la risoluzione è quella di aggiornare la landing zone. Quando vengono eliminati altri tipi di unità organizzative, AWS Control Tower viene aggiornato automaticamente.

Per ulteriori informazioni sulla risoluzione della deviazione per gli account e le unità di gestione, vedere [Se gestisci risorse all'esterno di AWS Control Tower](#).

Deriva di controllo CSPM del Security Hub

Questo tipo di deriva si verifica quando un controllo che fa parte dello AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower segnala uno stato di deriva. Il AWS Security Hub CSPM servizio stesso non segnala uno stato di deriva per questi controlli. Il servizio invia invece i risultati ad AWS Control Tower.

La deriva di controllo di Security Hub CSPM può essere rilevata anche se AWS Control Tower non riceve un aggiornamento di stato da Security Hub CSPM da più di 24 ore. Se tali risultati non vengono ricevuti come previsto, AWS Control Tower verifica che il controllo stia andando alla deriva. L'esempio seguente mostra una notifica di deriva che potresti ricevere quando viene rilevato questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that an AWS Security Hub control
    was removed in your account example-account@amazon.com <mailto:example-
    account@amazon.com>. The artifact deployed on the target OU and accounts does not match
    the expected template and configuration for the control. This mismatch indicates that
    configuration changes were made outside of AWS Control Tower. For more information,
    view Security Hub standard",
  "MasterAccountId" : "123456789XXX",
  "ManagementAccountId" : "123456789XXX",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
  "RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
    and enable it again. If the problem persists, contact AWS support.",
  "AccountId" : "7876543219XXX",
  "ControlId" : "SH.XXXXXXX.1",
  "ControlName" : "EBS snapshots should not be publicly restorable",
  "ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
  "EnabledControlIdentifier": "arn:aws:controltower:us-
    east-1::enabledcontrol/<UNIQUE_ID>".
  "Region" : "us-east-1"
}
```

Risoluzione

Per le unità organizzative con meno di 1000 account, la soluzione consigliata consiste nel chiamare l'ResetEnabledControlAPI per il controllo della deriva. Nella console, è possibile selezionare Re-register l'unità organizzativa, che ripristina il controllo allo stato originale. In alternativa, per qualsiasi unità organizzativa, puoi rimuovere e riattivare il controllo tramite la console o le API AWS Control Tower, che ripristinano anche il controllo.

Per ulteriori informazioni sulla risoluzione della deviazione per gli account e le unità di gestione, vedere [Se gestisci risorse all'esterno di AWS Control Tower](#).

Controlla la deriva delle politiche

Questo tipo di deriva si verifica quando un controllo implementato con politiche di controllo delle risorse (RCP) o politiche dichiarative segnala uno stato di deriva. Restituisce uno stato diCONTROL_INEFFECTIVE, che è possibile visualizzare nella console AWS Control Tower e nel messaggio drift. Il messaggio di deriva per questo tipo di deriva include anche il messaggio EnabledControlIdentifier relativo al controllo interessato.

Questo tipo di deriva non viene segnalato per i controlli. SCP-based

L'esempio seguente mostra una notifica di deriva che potresti ricevere quando viene rilevato questo tipo di deriva.

```
{
  "Message": "AWS Control Tower detects that a policy it owns was updated unexpectedly. This mismatch indicates that configuration changes were made outside of AWS Control Tower.",
  "MasterAccountId": "123456789XXX",
  "ManagementAccountId": "123456789XXX",
  "OrganizationId": "o-123EXAMPLE",
  "DriftType": "CONTROL_INEFFECTIVE",
  "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if permitted or Re-register the OU. If the problem persists, contact AWS support.",
  "TargetIdentifier": "arn:aws::organizations/o-123456/ou-1234-4567",
  "ControlId": "CT.XXXXXXX.PV.1",
  "ControlName": "EBS snapshots should not be publicly restorable",
  "ApiControlIdentifier": "arn:aws:controlcatalog::control/<UNIQUE_ID>",
  "EnabledControlIdentifier": "arn:aws:controltower:us-east-1::enabledcontrol/<UNIQUE_ID>"
}
```

Risoluzione

La soluzione più semplice per la deriva delle policy di controllo sui controlli RCP, sui controlli delle policy dichiarative e sui controlli CSPM Security Hub abilitati in AWS Control Tower è chiamare l'API `ResetEnabledControl`.

Per le unità organizzative con meno di 1000 account, un'altra soluzione della console o dell'API riguarda l'unità organizzativa, che ripristina Re-registeril controllo allo stato originale.

Per ogni singola unità organizzativa, puoi rimuovere e riattivare il controllo tramite la console o le API AWS Control Tower, che ripristinano anche il controllo.

Per ulteriori informazioni sulla risoluzione della deviazione per gli account e le unità di gestione, vedere [Se gestisci risorse all'esterno di AWS Control Tower](#).

Accesso affidabile disabilitato

Questo tipo di deriva si applica alle zone di atterraggio di AWS Control Tower. Si verifica quando disabiliti l'accesso affidabile ad AWS Control Tower AWS Organizations dopo aver configurato la landing zone di AWS Control Tower.

Quando l'accesso affidabile è disabilitato, AWS Control Tower non riceve più eventi di modifica da AWS Organizations. AWS Control Tower si affida a questi eventi di modifica per rimanere sincronizzato. AWS Organizations Di conseguenza, AWS Control Tower potrebbe non rilevare modifiche organizzative negli account e nelle unità organizzative. Ecco perché è importante registrare nuovamente ogni unità organizzativa ogni volta che si aggiorna la landing zone.

Esempio: notifica di deriva

Di seguito è riportato un esempio della notifica di deriva che si riceve quando si verifica questo tipo di deriva.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
  AWS Organizations. For more information, including steps to resolve this issue, see
  https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
  access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
```

```
}
```

Risoluzione

AWS Control Tower ti avvisa quando si verifica questo tipo di deriva nella console AWS Control Tower. La soluzione è reimpostare la landing zone di AWS Control Tower. Per ulteriori informazioni, consulta [Resolving drift](#).

Deriva dell'ereditarietà sulle linee di base abilitate

Questo tipo di deriva può verificarsi nelle unità organizzative e negli account AWS Control Tower.

Risoluzione

AWS Control Tower ti avvisa quando si verifica questo tipo di deriva. Per quasi tutti i casi di modifica dell'ereditarietà, riceverai una notifica di deviazione per la modifica dell'account membro di Moved. Questo perché questo tipo di deviazione si verifica in genere quando un account viene spostato o quando un account non riesce a registrarsi.

Visualizza e risolvi il problema del drift nella console

Nella console AWS Control Tower, puoi visualizzare questo stato di deriva ereditato nella colonna Baseline state della pagina Organizations. La soluzione dalla console è rivolta all'unità organizzativa o all'aggiornamento dell'Re-registeraccount.

Visualizza e risolvi la deriva a livello di codice

Per visualizzare lo stato della deriva a livello di codice, puoi chiamare l'[ListEnabledBaselinesAPI](#) per visualizzare gli stati delle linee di base abilitate sulle tue unità organizzative. Per visualizzare gli stati dei singoli account in modo programmatico con l'API, utilizza il flag. `ListEnabledBaselines includeChildren`

Puoi risolvere questo tipo di deriva a livello di codice, chiamando l'API. [ResetEnabledBaseline](#)

Previeni la deriva ereditaria con la registrazione automatica

Per evitare che ciò influisca sui futuri trasferimenti di account, attiva la registrazione automatica. Quando la registrazione automatica è attiva, AWS Control Tower applica le linee di base e le configurazioni di controllo dell'unità organizzativa di destinazione a un account spostato quando si aggiorna l'account per spostarlo su un'unità organizzativa diversa. Per ulteriori informazioni, consulta. [Sposta e registra gli account con la registrazione automatica](#) Auto-enrollment non

risolve la deriva della linea di base già esistente rispetto a una mossa precedente. Per risolvere la deriva esistente, utilizzate uno dei metodi di risoluzione descritti in precedenza in questa sezione. È possibile registrare nuovamente l'unità organizzativa, aggiornare l'account o chiamare l'`ResetEnabledBaselineAPI`.

Modifica dell'ereditarietà sui controlli abilitati

Questo tipo di deriva può verificarsi nelle unità organizzative e negli account AWS Control Tower.

Risoluzione

AWS Control Tower ti avvisa quando si verifica questo tipo di deriva. Per quasi tutti i casi di modifica dell'ereditarietà, ricevi una notifica di deviazione per la modifica dell'account membro di Moved. Questo tipo di deriva si verifica in genere quando si sposta un account tra le unità organizzative mentre la registrazione automatica è disattivata. In questo caso, AWS Control Tower applica i controlli dell'unità organizzativa di destinazione all'account, ma non rimuove automaticamente i controlli che l'account ha ereditato dall'unità organizzativa precedente. Di conseguenza, i controlli Detective e i controlli Proattivi dell'unità organizzativa precedente possono rimanere sull'account in uno stato diverso. I controlli preventivi non sono soggetti a questo tipo di deriva ereditaria.

Note

Non è possibile rimediare a questa deriva ereditaria aggiornando l'account, registrando nuovamente l'unità organizzativa o chiamando l'API `ResetEnabledControl`. Queste azioni risolvono solo la deriva della configurazione. Non rimuovono il controllo che un account trasferito eredita ancora dall'unità organizzativa precedente. Per rimuovere il controllo residuo, è necessario disabilitarlo con l'`DisableControlAPI`, come descritto in questa sezione.

Visualizza drift nella console

Nella console AWS Control Tower, puoi vedere quale controllo abilitato ha lo stato Drifted. Queste informazioni vengono visualizzate solo nella pagina dei dettagli dell'account interessato. La console non mostra `EnabledControlIdentifier` (l'ARN del controllo abilitato) necessario per disabilitare un controllo alla deriva. Per ottenerlo `EnabledControlIdentifier`, utilizza l'API AWS Control Tower, come descritto in questa sezione.

Visualizza e risolvi la deriva utilizzando il AWS CLI

Per trovare il controllo modificato sull'account interessato, elenca i controlli abilitati per quell'account. Imposta l'identificatore di destinazione sull'account e includi il `--include-children` flag in modo che vengano restituiti i controlli ereditati:

```
aws controltower list-enabled-controls --target-identifier <account ARN> --include-children
```

Nell'output, trova il controllo abilitato il cui tipo di `inheritance` deriva mostra uno stato. `DRIFTED`. Nota il `arn` valore di quel controllo abilitato. Questo valore è quello `EnabledControlIdentifier` che usi per disabilitare il controllo. Ad esempio:

```
{
  "arn": "arn:aws:controltower:<Region>:<management account ID>:enabledcontrol/<enabled control ID>",
  "controlIdentifier": "arn:aws:controlcatalog::control/<control ID>",
  "targetIdentifier": "arn:aws:organizations::<management account ID>:account/<organization ID>/<member account ID>",
  "driftStatusSummary": {
    "driftStatus": "DRIFTED",
    "types": {
      "inheritance": { "status": "DRIFTED" },
      "resource": { "status": "IN_SYNC" }
    }
  }
}
```

Per rimuovere il controllo alla deriva, disabilitalo passando il comando `EnabledControlIdentifier` al `disable-control` comando:

```
aws controltower disable-control --enabled-control-identifier <EnabledControlIdentifier>
```

Per ulteriori informazioni, consulta [ListEnabledControls](#) e [DisableControl](#) consulta l'AWS Control Tower API Reference.

Previene la deriva ereditaria con la registrazione automatica

Per evitare che ciò influisca sui futuri trasferimenti di account, attiva la registrazione automatica. Per ulteriori informazioni, consulta [Sposta e registra gli account con la registrazione automatica](#). Quando la registrazione automatica è attiva, AWS Control Tower applica le linee di base e le configurazioni di controllo dell'unità organizzativa di destinazione a un account spostato e rimuove i controlli dell'unità

organizzativa precedente. Tuttavia, la registrazione automatica non rimuove i controlli che erano già rimasti da uno spostamento eseguito prima dell'attivazione. Per rimuovere questi controlli, utilizza l'API. `DisableControl`

EventBridge creazione

Note

EventBridge è abilitato solo per LZ4.0 + clienti.

EventBridge Formato di esempio per AWS Control Tower

```
{
  "version": "0",
  "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
  "detail-type": "Drift Detected",
  "source": "aws.controltower",
  "account": "111122223333",
  "time": "2018-03-22T00:38:11Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "message" : "AWS Control Tower has detected that your member account 'account-email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/move-account'",
    "managementAccountId" : "012345678912",
    "organizationId" : "o-123EXAMPLE",
    "driftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
    "remediationStep" : "Re-register this organizational unit (OU), or if the OU has more than 1000 accounts, you must update the provisioned product in Account Factory.",

    "accountId" : "012345678909",
    "sourceId" : "012345678909",
    "destinationId" : "ou-3210-1EXAMPLE"
  }
}
```

Guida alla creazione di EventBridge regole per ricevere notifiche di deviazione:

Per creare una EventBridge regola per le notifiche di deriva

1. Apri la EventBridge console Amazon:
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.
5. Per Tipo di regola, scegli Regola con un modello di eventi.
6. Definisci l'origine dell'evento:
 - Per «Origine evento», seleziona AWS i servizi come origine dell'evento.
 - Per "nome AWS del servizio», seleziona AWS Control Tower.
 - Per «Tipo di evento», seleziona Drift Detected
7. Seleziona il bersaglio:
 - Per i tipi di destinazione, scegli il AWS servizio e per Seleziona una destinazione, scegli una destinazione come un argomento di notifica di deriva o una funzione Lambda. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.
 - A seconda della destinazione selezionata, fornisci i dettagli di configurazione necessari, come il nome della funzione Lambda o l'argomento ARN per la notifica delle deviazioni.
8. Rivedi e crea la regola:
 - Rivedi i dettagli della regola e apporta le modifiche necessarie.
 - Quando sei soddisfatto, fai clic su Crea regola per salvare la nuova EventBridge regola.

Dopo aver creato la regola, inizierà il monitoraggio degli eventi AWS Control Tower specificati e attiverà l'azione target selezionata quando si verificano eventi di deriva.

Se gestisci risorse all'esterno di AWS Control Tower

AWS Control Tower configura account, unità organizzative e altre risorse per tuo conto, ma tu sei il proprietario di queste risorse. Puoi modificare queste risorse all'interno di AWS Control Tower o al di fuori di esso. Il luogo più comune in cui modificare le risorse all'esterno di AWS Control Tower è la

AWS Organizations console. Questo argomento descrive come riconciliare le modifiche alle risorse di AWS Control Tower quando le apporti all'esterno di AWS Control Tower.

La ridenominazione, l'eliminazione e lo spostamento delle risorse all'esterno della console AWS Control Tower causa la perdita di sincronizzazione della console. Molte modifiche possono essere riconciliate automaticamente. Alcune modifiche richiedono il ripristino della zona di destinazione, per aggiornare le informazioni visualizzate nella console AWS Control Tower.

In generale, le modifiche apportate all'esterno della console AWS Control Tower alle risorse di AWS Control Tower creano uno stato di deriva *risolvibile* nella zona di atterraggio. Per ulteriori informazioni su queste modifiche, vedi [Modifiche riparabili alle risorse](#).

Attività che richiedono il ripristino della zona di atterraggio

- Eliminazione dell'unità organizzativa di sicurezza (un caso speciale, da non fare alla leggera).
- Rimozione di un account condiviso dall'unità organizzativa di sicurezza (scelta non consigliata).
- Aggiornamento, collegamento o scollegamento di un SCP associato all'unità organizzativa di sicurezza.

Modifiche che vengono aggiornate automaticamente da AWS Control Tower

- Modifica dell'indirizzo email di un account registrato
- Ridenominazione di un account registrato
- Creazione di una nuova unità organizzativa (OU) di primo livello
- Ridenominazione di un'unità organizzativa registrata
- Eliminazione di un'unità organizzativa registrata (ad eccezione dell'unità organizzativa di sicurezza, che richiede un aggiornamento).
- Eliminazione di un account registrato (ad eccezione di un account condiviso nell'unità organizzativa di sicurezza)

Note

AWS Service Catalog gestisce le modifiche in modo diverso rispetto ad AWS Control Tower. AWS Service Catalog può creare un cambiamento nella posizione di governance quando riconcilia le modifiche. Per ulteriori informazioni sull'aggiornamento di un prodotto fornito, vedere [Aggiornamento dei prodotti forniti nella documentazione](#). AWS Service Catalog

Facendo riferimento a risorse esterne a AWS Control Tower

Quando crei nuove OU e account all'esterno di AWS Control Tower, questi non sono governati da AWS Control Tower, anche se possono essere visualizzati.

Creazione di una UO

Le unità organizzative (OU) create all'esterno di AWS Control Tower vengono definite **non registrate**. Sono visualizzate nella pagina **Organizzazione**, ma non sono regolate dai controlli AWS Control Tower.

Creazione di un account

Gli account creati al di fuori di AWS Control Tower vengono definiti **non registrati**. Gli account registrati e non registrati che appartengono a un'unità organizzativa registrata con AWS Control Tower vengono visualizzati nella pagina **Organizzazione**. Gli account che non appartengono a un'unità organizzativa registrata possono essere invitati utilizzando la console **AWS Organizations**. Questo invito a partecipare non registra l'account in AWS Control Tower né estende la governance di AWS Control Tower all'account. Per estendere la governance registrando l'account, vai alla pagina **Organizzazione** o alla pagina dei dettagli dell'account in AWS Control Tower e scegli **Registra account**.

Modifica esterna dei nomi delle risorse di AWS Control Tower

Puoi modificare i nomi delle unità organizzative (OU) e degli account all'esterno della console AWS Control Tower e la console si aggiorna automaticamente per riflettere tali modifiche.

Ridenominazione di una UO

In AWS Organizations, puoi modificare il nome di un'unità organizzativa utilizzando l' **AWS Organizations API** o la console. Quando si modifica il nome di un'unità organizzativa all'esterno di AWS Control Tower, la console di AWS Control Tower riflette automaticamente la modifica del nome. Tuttavia, se esegui il provisioning dei tuoi account utilizzando **AWS Service Catalog**, devi anche reimpostare la zona di destinazione per garantire che AWS Control Tower rimanga coerente con AWS Organizations. Il flusso di lavoro **Reset** garantisce la coerenza tra i servizi per le unità organizzative fondamentali e aggiuntive. Puoi risolvere questo tipo di deriva dalla pagina delle impostazioni della zona di destinazione. Vedi la sezione chiamata «Resolving Drift» in [Rileva e risolvi la deriva in AWS Control Tower](#)

AWS Control Tower mostra i nomi delle unità organizzative nella pagina **Organizzazione** nella dashboard di AWS Control Tower. Puoi vedere quando l'operazione di ripristino della zona di atterraggio è riuscita.

Ridenominazione di un account registrato

Ogni AWS account ha un nome visualizzato che può essere modificato dall'utente root dell'account nella **Gestione costi e fatturazione AWS console**. Quando si rinomina un account registrato in AWS Control Tower, la modifica del nome si riflette automaticamente in AWS Control Tower. Per ulteriori informazioni sulla modifica del nome di un account, consulta [Gestire un AWS account](#) nella AWS Billing User Guide.

Eliminazione dell'unità organizzativa di sicurezza

Questo tipo di deviazione è un caso speciale. Se elimini l'unità organizzativa di sicurezza, verrà visualizzata una pagina con un messaggio di errore che ti chiede di reimpostare la zona di atterraggio. È necessario reimpostare la zona di destinazione prima di poter intraprendere qualsiasi altra azione in AWS Control Tower.

- Non sarai in grado di eseguire alcuna azione nella console AWS Control Tower e non potrai creare nuovi account AWS Service Catalog fino al completamento del ripristino.
- Non potrai visualizzare la pagina delle impostazioni della zona di destinazione dove è presente il pulsante **Reset**.

In questa situazione, il processo di ripristino della zona di destinazione crea una nuova unità organizzativa di sicurezza e sposta i due account condivisi nella nuova unità organizzativa di sicurezza. AWS Control Tower contrassegna gli account Log Archive e Audit come modificati. Lo stesso processo risolve la deriva in questi account.

Se decidi di dover eliminare l'unità organizzativa di sicurezza, ecco cosa devi sapere:

Prima di poter eliminare l'unità organizzativa di sicurezza, devi assicurarti che non contenga account. In particolare, è necessario rimuovere gli account Log Archive e Audit dall'unità organizzativa. Si consiglia di spostare questi account in un'altra unità organizzativa.

 Note

L'azione di eliminazione dell'unità organizzativa di sicurezza non deve essere eseguita senza la dovuta considerazione. L'azione potrebbe creare problemi di conformità se la registrazione viene sospesa temporaneamente e perché alcuni controlli potrebbero non essere applicati.

Per informazioni generali sulla deviazione, consultare “Risoluzione della deviazione” in [Rileva e risolvi la deriva in AWS Control Tower](#).

Rimozione di un account dall'unità organizzativa di sicurezza

Non è consigliabile rimuovere nessuno degli account condivisi dall'organizzazione o spostarli fuori dall'unità organizzativa di sicurezza. Se hai rimosso accidentalmente un account condiviso, puoi seguire la procedura di correzione in questa sezione per ripristinare l'account.

- Dalla console di AWS Control Tower: per avviare il processo di riparazione, segui i passaggi di riparazione semi-manuali. Assicurati che l'utente o il ruolo che utilizzi per accedere alla console AWS Control Tower disponga delle autorizzazioni per l'esecuzione. `organizations:InviteAccountToOrganization` Se non disponi di tali autorizzazioni, segui i passaggi di riparazione manuale, che utilizzano sia la console AWS Control Tower che la console AWS Organizations
- A partire dalla AWS Organizations console: questo processo di riparazione è una procedura leggermente più lunga e completamente manuale. Quando segui i passaggi di riparazione manuale, passerai dalla AWS Organizations console alla console AWS Control Tower. Quando lavori in AWS Organizations, avrai bisogno di un utente o di un ruolo con la policy `AWSOrganizationsFullAccess` gestita o equivalente. Quando lavori nella console AWS Control Tower, avrai bisogno di un utente o ruolo con la policy `AWSControlTowerServiceRolePolicy` gestita o equivalente e dell'autorizzazione per eseguire tutte le azioni di AWS Control Tower (`controltower: *`).
- Se i passaggi correttivi non consentono di ripristinare l'account, contatta il Supporto AWS

I risultati della rimozione di un account condiviso tramite AWS Organizations:

- L'account non è più protetto dai controlli obbligatori di AWS Control Tower con politiche di controllo dei servizi (SCP). Risultato: le risorse create da AWS Control Tower nell'account possono essere modificate o eliminate.

- L'account non è più incluso nell'account AWS Organizations di gestione. Risultato: l'amministratore dell'account di AWS Organizations gestione non ha più visibilità sulle spese dell'account.
- Non è più garantito che l'account venga monitorato da AWS Config. Risultato: l'amministratore dell'account di AWS Organizations gestione potrebbe non essere in grado di rilevare le modifiche alle risorse.
- L'account non è più nell'organizzazione. Risultato: gli aggiornamenti e il ripristino di AWS Control Tower falliranno.

Per ripristinare un account condiviso utilizzando la console AWS Control Tower (procedura semi-manuale)

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>. Devi accedere come utente IAM, utente in IAM Identity Center o ruolo con autorizzazioni per l'esecuzione `organizations:InviteAccountToOrganization`. Se non disponi di tali autorizzazioni, utilizza la procedura di riparazione manuale descritta più avanti in questo argomento.
2. Nella pagina **Landing zone drift detected**, scegli di porre rimedio **Re-Invite** alla rimozione dell'account condiviso invitando nuovamente l'account condiviso nell'organizzazione. Un'e-mail generata automaticamente viene inviata all'indirizzo e-mail dell'account.
3. Accetta l'invito a riportare l'account condiviso nell'organizzazione. Esegui una delle seguenti operazioni:
 - Accedi all'account condiviso che è stato rimosso, quindi vai su <https://console.aws.amazon.com/organizations/home#/invite>
 - Se hai accesso al messaggio email inviato quando hai nuovamente invitato l'account, accedi all'account rimosso, quindi fai clic sul link nel messaggio per accedere direttamente all'invito all'account.
 - Se l'account condiviso che è stato rimosso non appartiene a un'altra organizzazione, accedi all'account, apri la AWS Organizations console e vai su **Inviti**.
4. Accedi nuovamente all'account di gestione o ricarica la console AWS Control Tower se è già aperta. Vedrai la pagina **Landing zone drift**. Scegli **Ripristina** per riparare la zona di atterraggio.
5. Attendi il completamento del processo di ripristino.

Se la riparazione ha esito positivo, l'account condiviso appare in uno stato e conforme normali.

Se i passaggi correttivi non consentono di ripristinare l'account, contatta. Supporto AWS

Per ripristinare un account condiviso utilizzando AWS Control Tower e AWS Organizations console (riparazione manuale)

1. Accedi alla AWS Organizations console all'indirizzo. <https://console.aws.amazon.com/organizations/> Devi accedere come utente IAM, utente in IAM Identity Center o ruolo con la policy `AWSOrganizationsFullAccess` gestita o equivalente.
2. Invita l'account condiviso a tornare nell'organizzazione. Per informazioni sui requisiti, i prerequisiti e la procedura per invitare un account a AWS Organizations, consulta [Invitare un AWS account nella tua organizzazione](#) nella Guida per l'AWS Organizations utente.
3. Accedi all'account condiviso che è stato rimosso, quindi vai su <https://console.aws.amazon.com/organizations/home#/invite> per accettare l'invito.
4. Accedi nuovamente all'account di gestione.
5. Accedi alla console di AWS Control Tower come utente o ruolo con la policy `AWSControlTowerServiceRolePolicy` gestita o equivalente e le autorizzazioni per eseguire tutte le azioni di AWS Control Tower (`controltower: *`).
6. Verrà visualizzata la pagina di destinazione della zona di destinazione con un'opzione per reimpostare la zona di atterraggio. Scegli **Ripristina** per riparare la zona di atterraggio.
7. Attendi il completamento del processo di ripristino.

Se la riparazione ha esito positivo, l'account condiviso appare in uno stato e conforme normali.

Se i passaggi correttivi non consentono di ripristinare l'account, contatta. Supporto AWS

Modifiche esterne che vengono aggiornate automaticamente

Le modifiche apportate agli indirizzi e-mail del tuo account vengono aggiornate automaticamente da AWS Control Tower, ma Account Factory non le aggiorna automaticamente.

Modifica dell'indirizzo email di un account sottoposto a governance

AWS Control Tower recupera e visualizza gli indirizzi e-mail come richiesto dall'esperienza sulla console. Pertanto, gli indirizzi e-mail condivisi e di altro tipo vengono aggiornati e visualizzati in modo coerente in AWS Control Tower dopo la modifica.

 Note

In AWS Service Catalog, Account Factory mostra i parametri specificati nella console al momento della creazione di un prodotto su cui è stato effettuato il provisioning. Tuttavia, l'indirizzo email dell'account originale non viene aggiornato automaticamente quando l'indirizzo email dell'account cambia. Questo perché l'account è concettualmente contenuto all'interno del prodotto di cui è stato eseguito il provisioning; non è lo stesso del prodotto di cui è stato eseguito il provisioning. Per aggiornare questo valore, è necessario aggiornare il prodotto con provisioning, che può causare una modifica nella governance.

Applicazione di regole esterne AWS Config

AWS Control Tower mostra lo stato di conformità di tutte AWS Config le regole distribuite nelle unità organizzative registrate con AWS Control Tower, incluse le regole attivate all'esterno della console AWS Control Tower.

Eliminazione delle risorse AWS Control Tower all'esterno di AWS Control Tower

Puoi eliminare OU e account in AWS Control Tower e non devi intraprendere ulteriori azioni per visualizzare gli aggiornamenti. Account Factory viene aggiornato automaticamente quando si elimina un'unità organizzativa, ma non quando si elimina un account.

Eliminazione di un'unità organizzativa registrata (ad eccezione dell'unità organizzativa di sicurezza)

All'interno AWS Organizations, puoi rimuovere le unità organizzative (OU) vuote utilizzando l'API o la console. Le unità organizzative che contengono account non possono essere eliminate.

AWS Control Tower riceve una notifica AWS Organizations quando un'unità organizzativa viene eliminata. Aggiorna l'elenco delle unità organizzative in Account Factory, in modo che l'elenco delle unità organizzative registrate rimanga coerente.

 Note

In AWS Service Catalog, l'Account Factory viene aggiornato per rimuovere l'unità organizzativa eliminata dall'elenco delle unità organizzative disponibili in cui è possibile eseguire il provisioning di un account.

Eliminazione di un account registrato da un'unità organizzativa

Quando elimini un account registrato, AWS Control Tower riceve una notifica e apporta aggiornamenti, in modo che le informazioni rimangano coerenti.

 Note

In AWS Service Catalog, il prodotto fornito da Account Factory che rappresenta l'account gestito non viene aggiornato per eliminare l'account. Al contrario, il prodotto sottoposto a provisioning viene visualizzato come Tainted e in uno stato di errore. Per eseguire la pulizia, passare a AWS Service Catalog, scegliere il prodotto di cui è stato eseguito il provisioning, quindi scegliere **Terminate** (Termina).

Gestisci organizzazioni e account con AWS Control Tower

Tutte le unità organizzative (OU) e gli account creati in AWS Control Tower sono governati automaticamente da AWS Control Tower. Inoltre, se disponi di unità organizzative e account esistenti creati all'esterno di AWS Control Tower, puoi inserirli nella governance di AWS Control Tower.

Per AWS gli account esistenti AWS Organizations e quelli esistenti, la maggior parte dei clienti preferisce registrare gruppi di account registrando l'intera unità organizzativa (OU) che contiene gli account. Puoi anche registrare gli account singolarmente. Per ulteriori informazioni sulla registrazione di singoli account, vedere. [Informazioni sulla registrazione degli account esistenti](#)

Terminologia

- Quando si inserisce un'organizzazione esistente in AWS Control Tower, si parla di **registrazione dell'organizzazione** o **estensione della governance** all'organizzazione.
- Quando si inserisce un AWS account in AWS Control Tower, si chiama **registrazione dell'account**.

Visualizza le tue unità organizzative e i tuoi account

Nella **pagina AWS Control Tower Organization**, puoi visualizzare tutte le unità organizzative presenti AWS Organizations, incluse le unità organizzative registrate presso AWS Control Tower e quelle non registrate. Puoi visualizzare le unità organizzative annidate come parte della gerarchia. Un modo semplice per visualizzare le unità organizzative nella **pagina Organizzazione** è selezionare **Unità organizzative solo** dal menu a discesa in alto a destra.

La **pagina Organizzazione** elenca tutti gli account dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di iscrizione in AWS Control Tower. Un modo semplice per visualizzare gli account nella **pagina Organizzazione** è selezionare **Account solo** dal menu a discesa in alto a destra. È possibile visualizzare, aggiornare e registrare gli account singolarmente all'interno delle unità organizzative, se gli account soddisfano i prerequisiti per l'iscrizione.

Se non si seleziona alcun filtro, nella **pagina Organizzazione** vengono visualizzati gli account e le unità organizzative in una gerarchia. È una posizione centrale per il monitoraggio e l'esecuzione di azioni su tutte le risorse di AWS Control Tower. Per ulteriori informazioni sulla **pagina Organizzazione**, puoi visualizzare la procedura dettagliata video.

 Note

Quando abiliti l'accesso affidabile all'organizzazione che contiene la tua zona di destinazione, AWS Control Tower può creare ruoli, gestire risorse e leggere i dati per tutti gli account dell'organizzazione. Tramite l'accesso affidabile, qualsiasi account o unità organizzativa dell'organizzazione è disponibile per AWS Control Tower, sia esso registrato e iscritto o meno registrato e non iscritto.

Procedura guidata: video

Questo video (4:01) descrive come lavorare con la pagina Organizzazione in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sull'utilizzo della pagina dell'organizzazione in AWS Control Tower.](#)

Argomenti

- [Registra un'unità organizzativa esistente con AWS Control Tower](#)
- [Informazioni sulla registrazione degli account esistenti](#)
- [Trasferire un account a un'altra organizzazione](#)

Estendere la governance a un'organizzazione esistente

Puoi aggiungere la governance di AWS Control Tower a un'organizzazione esistente configurando una zona di destinazione (LZ) come indicato nella Guida per l'utente di AWS Control Tower in [Getting Started, Step 2](#).

Ecco cosa aspettarti quando configuri la tua landing zone di AWS Control Tower in un'organizzazione esistente.

- Puoi avere una zona di atterraggio per AWS Organizations organizzazione.
- AWS Control Tower utilizza l'account di gestione AWS Organizations dell'organizzazione esistente come account di gestione. Non è necessario un nuovo account di gestione.
- AWS Control Tower configura due nuovi account in un'unità organizzativa registrata: un account di controllo e un account di registrazione.

- I limiti di servizio dell'organizzazione devono consentire la creazione di questi due account aggiuntivi.
- Dopo aver avviato la zona di destinazione o registrato un'unità organizzativa, i controlli di AWS Control Tower si applicano automaticamente a tutti gli account registrati in tale unità organizzativa.
- Puoi registrare altri AWS account esistenti in un'unità organizzativa governata da AWS Control Tower, in modo che i controlli si applichino a tali account.
- Puoi aggiungere altre unità organizzative in AWS Control Tower e registrare le unità organizzative esistenti.

Per verificare altri prerequisiti per la registrazione e l'iscrizione, consulta [Getting Started with AWS Control Tower](#).

Ecco ulteriori dettagli su come i controlli AWS Control Tower non si applicano alle unità organizzative nelle organizzazioni AWS che non dispongono di zone di destinazione di AWS Control Tower configurate:

- I nuovi account creati al di fuori di AWS Control Tower Account Factory non sono vincolati dai controlli dell'unità organizzativa registrata.
- I nuovi account creati nelle unità organizzative non registrate presso AWS Control Tower non sono vincolati dai controlli, a meno che non si registrino specificamente tali account in AWS Control Tower. Per ulteriori informazioni sulla registrazione degli account, consulta [Informazioni sulla registrazione degli account esistenti](#).
- Le organizzazioni aggiuntive esistenti, gli account esistenti e le nuove unità organizzative o gli account creati all'esterno di AWS Control Tower non sono vincolati dai controlli di AWS Control Tower, a meno che non si registri separatamente l'unità organizzativa o si registri l'account.

Per ulteriori informazioni su come applicare AWS Control Tower a unità organizzative e account esistenti, consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#).

Per una panoramica del processo di configurazione di una landing zone di AWS Control Tower nell'organizzazione esistente, guarda il video nella sezione successiva.

Note

Durante la configurazione, AWS Control Tower esegue controlli preliminari per evitare problemi comuni. Tuttavia, se stai utilizzando la soluzione AWS Landing Zone per AWS

Organizations, consulta il tuo architetto di AWS soluzioni prima di provare ad abilitare AWS Control Tower nella tua organizzazione per determinare se AWS Control Tower può interferire con l'attuale distribuzione della zona di destinazione. Inoltre, consulta [Se l'account non soddisfa i prerequisiti](#) la sezione per informazioni sullo spostamento degli account da una zona di atterraggio all'altra.

Video: abilita una zona di atterraggio esistente AWS Organizations

Questo video (7:48) descrive come configurare e abilitare una zona di atterraggio di AWS Control Tower in strutture esistenti AWS Organizations . Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Abilita AWS Control Tower per le organizzazioni esistenti](#)

Considerazioni per IAM Identity Center e le organizzazioni esistenti

- Se Centro identità AWS IAM (IAM Identity Center) è già configurato, la regione principale di AWS Control Tower deve essere la stessa della regione IAM Identity Center.
- AWS Control Tower non elimina una configurazione esistente.
- Se IAM Identity Center è già abilitato e si utilizza IAM Identity Center Directory, AWS Control Tower aggiunge risorse come set di autorizzazioni, gruppi e così via e procede come al solito.
- Se è impostata un'altra directory (esterna, AD, Managed AD), AWS Control Tower non modifica la configurazione esistente. Per ulteriori dettagli, consultare [Considerazioni per Centro identità AWS IAM clienti \(IAM Identity Center\)](#).

Accesso ad altri AWS services

Dopo aver inserito la tua organizzazione nella governance di AWS Control Tower, hai ancora accesso a tutti AWS i servizi disponibili tramite AWS Organizations, tramite la AWS Organizations console e le API. Per ulteriori informazioni, consulta [Servizi AWS correlati](#).

Unità organizzative annidate in AWS Control Tower

Questo capitolo elenca le aspettative e le considerazioni di cui dovresti essere a conoscenza quando lavori con unità organizzative annidate in AWS Control Tower. Nella maggior parte dei casi, lavorare

con unità organizzative annidate equivale a lavorare con una struttura di unità organizzative piatta. Il registro e Re-register le funzionalità funzionano con le unità organizzative annidate, ad eccezione dei comportamenti modificati descritti in questo capitolo.

Procedura guidata: video

Questo video (4:46) descrive come gestire le distribuzioni di unità organizzative annidate in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sulla gestione delle unità organizzative annidate in AWS Control Tower.](#)

Per indicazioni sulle best practice per le unità organizzative annidate e la tua zona di destinazione, consulta il post del blog [Organizzare la tua zona di atterraggio AWS Control Tower con le unità organizzative annidate.](#)

Espandi da una struttura OU piatta a una struttura OU annidata

Se hai creato la tua landing zone di AWS Control Tower con una struttura OU piatta, puoi espanderla in una struttura OU annidata.

Questo processo prevede quattro fasi principali:

1. Crea la struttura di unità organizzativa annidata desiderata in AWS Control Tower.
2. Accedi alla AWS Organizations console e usa la loro funzionalità di spostamento in blocco per spostare gli account dall'unità organizzativa di origine (fissa) all'unità organizzativa di destinazione (annidata). Ecco come:
 - a. Vai all'unità organizzativa da cui desideri spostare gli account.
 - b. Seleziona tutti gli account nell'unità organizzativa.
 - c. Scegli Sposta.

Note

Questo passaggio deve essere eseguito nella AWS Organizations console interna perché AWS Control Tower non dispone della funzionalità Move.

3. Vai all'unità organizzativa annidata in AWS Control Tower e registrati. Re-register Verranno registrati tutti gli account dell'unità organizzativa annidata.

- Se hai creato l'unità organizzativa in AWS Control Tower, Re-register l'unità organizzativa.
 - Se hai creato l'unità organizzativa in AWS Organizations, registra l'unità organizzativa per la prima volta.
4. Dopo lo spostamento e la registrazione degli account, elimina l'unità organizzativa di primo livello vuota dalla AWS Organizations console o dalla console di AWS Control Tower.

Controlli preliminari della registrazione dell'unità organizzativa Nested

Per supportare la corretta registrazione delle unità organizzative annidate e dei relativi account membri, AWS Control Tower esegue una serie di controlli preliminari. Questi stessi controlli preliminari vengono eseguiti quando si registra un'unità organizzativa di primo livello o un'unità organizzativa annidata. Per ulteriori informazioni, consulta Cause [comuni di errore durante la registrazione o la nuova registrazione](#).

- Se tutti i controlli preliminari vengono superati, AWS Control Tower inizia a registrare l'unità organizzativa automaticamente.
- Se i controlli preliminari falliscono, AWS Control Tower interrompe il processo di registrazione e fornisce un elenco di elementi che devono essere corretti prima di poter registrare l'unità organizzativa.

Unità organizzative e ruoli annidati

AWS Control Tower distribuisce il `AWSControlTowerExecution` ruolo agli account all'interno dell'unità organizzativa di destinazione e agli account di tutte le unità organizzative annidate nell'unità organizzativa di destinazione, anche quando l'intenzione è quella di registrare solo l'unità organizzativa di destinazione. Questo ruolo conferisce a qualsiasi utente dell'account di gestione le autorizzazioni di amministratore su qualsiasi account che ricopre il ruolo. `AWSControlTowerExecution` Il ruolo può essere utilizzato per eseguire azioni che normalmente non sarebbero consentite dai controlli AWS Control Tower.

Puoi eliminare questo ruolo dagli account non registrati che non intendi registrare. Se elimini questo ruolo, non puoi registrare l'account con AWS Control Tower o registrare le unità organizzative principali immediate, a meno che non ripristini il ruolo nell'account. Per eliminare il `AWSControlTowerExecution` ruolo da un account, è necessario accedere con il `AWSControlTowerExecution` ruolo, poiché nessun altro responsabile IAM è autorizzato a eliminare i ruoli gestiti da AWS Control Tower.

Per informazioni su come limitare l'accesso ai ruoli, consulta Condizioni [opzionali per le relazioni di fiducia tra](#) i ruoli.

Cosa succede durante la registrazione e la nuova registrazione delle unità organizzative e degli account annidati

Quando registri o registri nuovamente un'unità organizzativa annidata, AWS Control Tower registra tutti gli account non registrati dell'unità organizzativa di destinazione e aggiorna tutti gli account registrati. Ecco cosa aspettarsi.

AWS Control Tower esegue le seguenti attività

- Aggiunge il `AWSControlTowerExecution` ruolo a tutti gli account non registrati in questa unità organizzativa e a tutti gli account non registrati nelle relative unità organizzative annidate.
- Registra gli account dei membri che non sono iscritti.
- Re-enrolls gli account dei membri registrati.
- Crea un login IAM Identity Center per gli account dei membri appena registrati.
- Aggiorna gli account dei membri iscritti esistenti per riflettere le modifiche alla zona di atterraggio.
- Aggiorna i controlli configurati per questa unità organizzativa e i relativi account membri.

Considerazioni sulla registrazione dell'unità organizzativa annidata

- Non è possibile registrare un'unità organizzativa nell'unità organizzativa principale (unità organizzativa di sicurezza).
- Le unità organizzative annidate devono essere registrate separatamente.
- Non è possibile registrare un'unità organizzativa a meno che l'unità organizzativa principale non sia registrata.
- Non è possibile registrare un'unità organizzativa a meno che tutte le unità organizzative più in alto nell'albero non siano state registrate correttamente in un determinato momento (alcune potrebbero essere state eliminate).
- È possibile registrare un'unità organizzativa che si trova al di sotto di un'unità organizzativa più elevata, ma tale deviazione non viene riparata da tale azione.

Limiti dell'unità organizzativa annidata

- Le unità organizzative possono essere annidate a una profondità massima di 5 livelli sotto la radice.
- Le unità organizzative annidate nell'unità organizzativa di destinazione devono essere registrate o registrate nuovamente separatamente.
- Se l'unità organizzativa di destinazione è di livello 2 o inferiore nella gerarchia, ovvero se non è un'unità organizzativa di livello superiore, i controlli preventivi abilitati sulle unità organizzative superiori vengono applicati automaticamente a questa unità organizzativa e a tutte le unità organizzative inferiori.
- Gli errori di registrazione dell'unità organizzativa non si propagano verso l'alto nell'albero della gerarchia. Puoi visualizzare i dettagli sugli stati delle unità organizzative annidate nella pagina dei dettagli dell'unità organizzativa principale.
- Gli errori di registrazione dell'unità organizzativa non si propagano lungo l'albero della gerarchia.
- AWS Control Tower non modifica le impostazioni VPC per account nuovi o esistenti.

Unità organizzative annidate e conformità

Dalla console AWS Control Tower, puoi visualizzare le unità organizzative e gli account non conformi nella pagina **Organizzazione**, in modo da poter comprendere la conformità su una scala più ampia.

Considerazioni sulla conformità per le unità organizzative e gli account annidati

- La conformità di un'unità organizzativa non è determinata in base alla conformità delle unità organizzative annidate al suo interno.
- Lo stato di conformità di un controllo viene calcolato su tutte le unità organizzative su cui è abilitato il controllo, comprese le unità organizzative annidate. Visualizza lo [stato di conformità di AWS Control Tower per le unità organizzative e gli account](#).
- Un'unità organizzativa viene indicata come non conforme solo se ha account non conformi, indipendentemente dalla posizione dell'unità organizzativa nella gerarchia dell'unità organizzativa.
- Se un'unità organizzativa annidata non è conforme, l'unità organizzativa principale non viene automaticamente considerata non conforme.
- Nella pagina dei dettagli dell'unità organizzativa o dell'account, puoi visualizzare un elenco di risorse non conformi che potrebbero causare la visualizzazione dello stato di non conformità delle unità organizzative o degli account.

Unità organizzative annidate e deriva

In determinate situazioni, la deriva può impedire la registrazione delle unità organizzative annidate.

Aspettative per le unità organizzative drift e annidate

- È possibile abilitare i controlli sulle unità organizzative con unità madri diverse, ma non direttamente sulle unità organizzative derivate.
- Puoi attivare i controlli investigativi in un'unità organizzativa diversa, purché non si tratti di un'unità organizzativa derivata di primo livello.
- I controlli obbligatori sono abilitati solo sulle unità organizzative di primo livello. I controlli obbligatori vengono ignorati quando si registra un'unità organizzativa annidata.
- Un controllo obbligatorio protegge AWS Config le risorse; pertanto, tale controllo deve essere in uno stato non alterato per registrare le unità organizzative annidate. Se deviato, AWS Control Tower blocca la registrazione delle unità organizzative annidate.
- Se l'unità organizzativa di primo livello è alterata, il controllo che protegge le AWS Config risorse potrebbe essere in errore. In questa situazione, AWS Control Tower blocca qualsiasi azione che richieda la creazione o l'aggiornamento di AWS Config risorse, inclusa l'applicazione di controlli investigativi.

Unità operative e controlli annidati

Quando si abilita un controllo su un'unità organizzativa registrata, i controlli preventivi e investigativi hanno comportamenti diversi. Per le unità organizzative annidate, i controlli proattivi si comportano in modo simile ai controlli detective.

Controlli preventivi

- I controlli preventivi vengono applicati alle unità organizzative annidate.
- I controlli preventivi obbligatori vengono applicati a tutti gli account appartenenti all'unità organizzativa e alle relative unità organizzative annidate.
- I controlli preventivi riguardano tutti gli account e le unità organizzative annidati nell'unità organizzativa di destinazione, anche se tali account e unità organizzative non sono registrati.

Controlli investigativi e proattivi

- Le unità organizzative annidate non ereditano automaticamente i controlli detective o proattivi; questi devono essere abilitati separatamente.
- I controlli investigativi e proattivi vengono implementati solo sugli account registrati nelle regioni operative della zona di atterraggio.

Stati di controllo ed ereditarietà abilitati

È possibile visualizzare i controlli ereditati per ciascuna unità organizzativa nella pagina dei dettagli dell'unità organizzativa.

Tip

Puoi utilizzare l'ereditarietà dei controlli per rimanere entro la quota SCP di un'unità organizzativa. Ad esempio, puoi abilitare un controllo all'unità organizzativa di livello superiore di una gerarchia di unità organizzative, invece di abilitarlo direttamente per un'unità organizzativa annidata.

Status ereditato

- Lo stato **Ereditato** indica che il controllo è abilitato solo per ereditarietà e non è stato applicato direttamente all'unità organizzativa.
- Lo stato **Abilitato** indica che il controllo viene applicato su questa unità organizzativa, indipendentemente dal relativo stato sulle altre unità organizzative.
- Lo stato **Failed** indica che il controllo non viene applicato su questa unità organizzativa, indipendentemente dal relativo stato su altre unità organizzative.

Note

Lo stato **Ereditato** indica che il controllo è stato applicato a un'unità organizzativa più in alto nell'albero ed è applicato a questa unità organizzativa, ma non è stato aggiunto direttamente a questa unità organizzativa.

 Se la tua zona di atterraggio non è la versione corrente

Ogni riga della tabella Controlli abilitati rappresenta un controllo abilitato su una singola unità organizzativa.

Unità organizzative annidate e radice

La root non è un'unità organizzativa e non può essere registrata o registrata nuovamente. Inoltre, non puoi creare account direttamente nella root. La radice non può essere non conforme o avere uno stato del ciclo di vita, ad esempio registrata o in fase di sviluppo.

Tuttavia, la radice è il contenitore di primo livello per tutti gli account e le unità organizzative. Nel contesto delle unità organizzative annidate, è il nodo in cui sono annidate tutte le altre unità organizzative.

Registra un'unità organizzativa esistente con AWS Control Tower

Un modo efficace per inserire più AWS account esistenti in AWS Control Tower consiste nell'estendere la governance di AWS Control Tower a un'intera unità organizzativa (OU).

Per abilitare la governance di AWS Control Tower su un'unità organizzativa esistente creata con AWS Organizations e i relativi account, registra l'unità organizzativa nella tua zona di destinazione di AWS Control Tower. Puoi registrare unità organizzative che contengono fino a 1000 account. Se un'unità organizzativa contiene più di 1000 account, non è possibile registrarla in AWS Control Tower.

Quando registri un'unità organizzativa, gli account dei suoi membri vengono registrati nella zona di destinazione di AWS Control Tower. Sono regolati dai controlli che si applicano alle rispettive unità organizzative.

A partire dalla versione 4.0 di Landing Zone, puoi abilitare direttamente i controlli su un'unità organizzativa. I controlli investigativi richiedono la registrazione di AWS Config, che può essere attivata registrando l'unità organizzativa o abilitando la registrazione di AWS Config sull'unità organizzativa. Register OU abiliterà AWSControlTowerBaseline Abilita AWS Config, la registrazione verrà ConfigBaseline abilitata. Per ulteriori informazioni, consulta [Tipi di linee di base](#) e [La guida di riferimento di AWS Control Tower Controls](#).

 Note

Se non disponi già di una landing zone di AWS Control Tower, inizia configurando una zona di atterraggio, in una nuova organizzazione creata da AWS Control Tower o in un' AWS Organizations organizzazione esistente. Per ulteriori dettagli su come configurare una zona di atterraggio, consulta [Guida introduttiva a AWS Control Tower](#).

Cosa succede ai miei account quando registro la mia unità organizzativa?

AWS Control Tower richiede l'autorizzazione per stabilire un accesso affidabile tra AWS CloudFormation e AWS Organizations per tuo conto, in modo da AWS CloudFormation poter distribuire automaticamente il tuo stack negli account della tua organizzazione.

- Il `AWSControlTowerExecution` ruolo viene aggiunto a tutti gli account con lo stato `Non registrato`.
- I controlli obbligatori sono abilitati per impostazione predefinita nell'unità organizzativa e in tutti i relativi account al momento della registrazione dell'unità organizzativa.

Iscrizione parziale degli account dopo la registrazione di un'unità organizzativa

È possibile registrare un'unità organizzativa con successo, ma alcuni account potrebbero rimanere non registrati. In tal caso, questi account non soddisfano alcuni dei prerequisiti per l'iscrizione. Se la registrazione di un account nell'ambito del processo di registrazione OU non ha esito positivo, lo stato dell'account nella pagina degli account indica che l'iscrizione non è riuscita. Puoi anche visualizzare le informazioni sull'account nella tua pagina OU, ad esempio `4 di 5`, nel campo degli account.

Ad esempio, se visualizzi `4 su 5`, significa che l'unità organizzativa ha 5 account in totale e 4 di questi sono stati registrati correttamente, ma un account non è stato registrato durante la procedura di registrazione dell'unità organizzativa. `Re-Register` Puoi scegliere l'unità organizzativa per avviare la registrazione degli account, dopo esserti assicurato che gli account soddisfino i prerequisiti di iscrizione.

Prerequisiti utente IAM per la registrazione di un'unità organizzativa

La tua identità AWS Identity and Access Management (IAM) (utente o ruolo) o l'identità utente IAM Identity Center devono essere incluse nel portafoglio Account Factory appropriato quando esegui

l'operazione Register OU, anche se Admin disponi già delle autorizzazioni. In caso contrario, la creazione dei prodotti forniti fallirà durante la registrazione. L'errore si verifica perché AWS Control Tower si basa sulle credenziali dell'utente IAM o sull'identità dell'utente IAM Identity Center per la registrazione di un'unità organizzativa.

Il portafoglio pertinente è quello creato da AWS Control Tower, denominato AWS Control Tower Account Factory Portfolio. Accedi ad esso scegliendo Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. Quindi seleziona la scheda denominata Gruppi, ruoli e utenti per visualizzare la tua identità IAM o IAM Identity Center. Per ulteriori informazioni su come concedere l'accesso, consulta [la documentazione per AWS Service Catalog](#).

Registrare un'unità organizzativa esistente

Nella console di AWS Control Tower, nella pagina Organizzazione, puoi visualizzare tutte le unità organizzative e gli account dell'organizzazione in una gerarchia, comprese le unità organizzative registrate con AWS Control Tower e quelle non registrate.

In generale, le unità organizzative non registrate sono state create e non sono governate da nessun'altra zona di atterraggio. AWS Organizations Puoi registrare unità organizzative esistenti che contengono fino a 1000 account. Se un'unità organizzativa contiene più di 1000 account, non è possibile registrarla in AWS Control Tower.

Per registrare un'unità organizzativa esistente dalla console

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.
2. Nel menu di navigazione a sinistra, scegli Organizzazione.
3. Nella pagina Organizzazione, seleziona il pulsante di opzione accanto all'unità organizzativa che desideri registrare, quindi seleziona Registra unità organizzativa dal menu a discesa Azioni in alto a destra o, in alternativa, seleziona il nome dell'unità organizzativa in modo da poter visualizzare la pagina dei dettagli dell'unità organizzativa per tale unità organizzativa.
4. Nella pagina dei dettagli dell'unità organizzativa, in alto a destra, puoi selezionare Registra unità organizzativa dal menu a discesa Azioni.

Il processo di registrazione richiede un minimo di 10 minuti per estendere la governance all'unità organizzativa e fino a 2 minuti aggiuntivi per ogni account aggiuntivo.

Per registrare un'unità organizzativa esistente con le API

Per registrare un'unità organizzativa esistente con le API di AWS Control Tower, puoi chiamare l'EnableBaselineAPI con il `AWSControlTowerBaseline` `baselineIdentifier` campo. Per ulteriori informazioni, consulta [Registrazione un'unità organizzativa AWS Control Tower solo con API](#).

Risultati della registrazione di un'unità organizzativa esistente

Dopo aver registrato un'unità organizzativa esistente, il `AWSControlTowerExecution` ruolo consente ad AWS Control Tower di estendere la governance ai suoi singoli account. I guardrail vengono applicati e le informazioni sulle attività degli account vengono riportate negli account di controllo e registrazione.

Gli altri risultati includono quanto segue:

- `AWSControlTowerExecution` consente il controllo da parte dell'account di controllo AWS Control Tower.
- `AWSControlTowerExecution` consente di configurare la registrazione dell'organizzazione, in modo che tutti i registri per ogni account vengano inviati all'account di registrazione.
- `AWSControlTowerExecution` assicura che i controlli AWS Control Tower selezionati si applichino automaticamente a ogni singolo account delle unità organizzative e a ogni nuovo account creato in AWS Control Tower.

Per un'unità organizzativa registrata, puoi fornire report di conformità e sicurezza basati sulle funzionalità di controllo e registrazione incorporate nei controlli AWS Control Tower. I team di sicurezza e conformità possono verificare che tutti i requisiti siano soddisfatti e che non si sia verificata alcuna deriva organizzativa. Per ulteriori informazioni su drift, consulta [Rileva e risolvi la deriva in AWS Control Tower](#)

Note

Una situazione insolita può verificarsi quando AWS Control Tower visualizza le unità organizzative e i relativi account. Se hai creato un account in un'unità organizzativa registrata e successivamente sposti l'account registrato in un'altra unità organizzativa non registrata, in particolare se utilizzi l'unità organizzativa AWS Organizations per spostare l'account, puoi visualizzare il risultato «1 di 0» nella pagina dei dettagli dell'unità organizzativa. Inoltre, potresti aver creato un altro account non registrato in quell'unità organizzativa non registrata. Se è presente un account non registrato, la console potrebbe leggere «1 di 1» per l'unità

organizzativa. Sembrerà che il singolo account (appena creato) sia registrato, ma in realtà non lo è. È necessario registrare il nuovo account.

Crea una nuova unità organizzativa

Ecco come creare un'unità organizzativa o un'unità organizzativa annidata in AWS Control Tower.

Per creare una nuova unità organizzativa in AWS Control Tower

1. Vai alla [pagina dell'organizzazione](#).
2. Seleziona [Crea unità organizzativa](#) dal menu a discesa [Crea risorse](#) in alto a destra.
3. Specifica un nome nel campo [Nome dell'unità organizzativa](#).
4. Nel menu a discesa dell'unità organizzativa principale, puoi vedere la gerarchia delle unità organizzative registrate. Seleziona un'unità organizzativa principale per la nuova unità organizzativa che stai creando.
5. Scegliere [Aggiungi](#).

Tip

Per aggiungere un'unità organizzativa annidata in meno passaggi, seleziona il nome dell'unità organizzativa principale mostrato nella tabella nella [pagina Organizzazione](#), visualizza la [pagina dell'unità organizzativa principale](#), quindi scegli [Aggiungi un'unità organizzativa principale](#) dal menu a discesa [Azioni](#) in alto a destra. La nuova unità organizzativa viene creata automaticamente come unità organizzativa annidata sotto l'unità organizzativa selezionata.

Note

Se la tua zona di atterraggio non è aggiornata, nel menu a discesa vedrai un elenco semplice anziché una gerarchia. Anche se la tua zona di atterraggio include unità organizzative annidate, non vedrai le unità organizzative L5 nel menu a discesa, perché non puoi creare una nuova unità organizzativa al di sotto di una unità organizzativa L5. Per ulteriori informazioni sulle unità organizzative annidate in AWS Control Tower, consulta [Unità organizzative annidate in AWS Control Tower](#)

Rimuovere un'unità organizzativa

AWS Control Tower supporta azioni separate sulla console per annullare la registrazione di un'unità organizzativa ed eliminare un'unità organizzativa.

L'eliminazione di un'unità organizzativa è definitiva. Non può essere annullata.

Considerazioni

- Affinché le operazioni di eliminazione e annullamento della registrazione abbiano esito positivo, l'unità organizzativa deve essere priva di account.
- Tutti i controlli opzionali devono essere rimossi dall'unità organizzativa.
- È necessario annullare la registrazione dell'unità organizzativa prima di eliminarla.
- Puoi rimuovere un'unità organizzativa da AWS Control Tower annullando la registrazione, senza eliminarla.

Per rimuovere un'unità organizzativa da AWS Control Tower

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.
2. Vai alla pagina dell'organizzazione.
3. Seleziona il nome dell'unità organizzativa per visualizzare la pagina dei dettagli dell'unità organizzativa e assicurati che tutti gli account vengano rimossi dall'unità organizzativa.
4. Inoltre, nella pagina dei dettagli dell'unità organizzativa, assicurati che tutti i controlli opzionali siano stati rimossi dall'unità organizzativa.
5. Torna alla pagina Organizzazione e seleziona il pulsante di opzione accanto all'unità organizzativa.
6. Seleziona **Annulla registrazione unità organizzativa** dal menu a discesa **Azioni** in alto a destra.
7. Fermati qui se non desideri eliminare completamente l'unità organizzativa, ma solo per annullare la registrazione da AWS Control Tower. Per eliminare completamente l'unità organizzativa, continua con il passaggio successivo.
8. Per continuare, seleziona **Elimina** dal menu a discesa **Azioni** in alto a destra.

È necessario attendere il completamento del processo di annullamento della registrazione prima di poter annullare la registrazione di un'altra unità organizzativa.

 Note

Per rimuovere gli account gestiti da AWS Control Tower, puoi accedere ad **Account factory** dal riquadro di navigazione a sinistra nella console AWS Control Tower. Per rimuovere gli account nell'unità organizzativa che non sono gestiti da AWS Control Tower, accedi alla **AWS Organizations** console.

Per annullare la registrazione di un'unità organizzativa a livello di codice, chiama l'API.

[DisableBaseline](#)

Cause comuni di errore durante la registrazione o la nuova registrazione

In generale, quando registri o registri nuovamente un'unità organizzativa, tutti gli account all'interno di tale unità organizzativa vengono registrati in AWS Control Tower. Tuttavia, è possibile che alcuni account non riescano a registrarsi, anche se l'intera unità organizzativa viene registrata correttamente. In questi casi, è necessario risolvere l'errore di verifica preliminare relativo all'account e quindi provare a registrare nuovamente l'account o l'unità organizzativa.

Se la registrazione (o la nuova registrazione) di un'unità organizzativa o di uno dei suoi account membri fallisce, AWS Control Tower restituisce messaggi di errore per gli account membri interessati. Puoi visualizzare i messaggi di errore nella pagina dei dettagli dell'unità organizzativa, dove una tabella aggrega i controlli preliminari e i messaggi di errore dell'account. Se un'operazione di registrazione dell'unità organizzativa ha esito negativo, la tabella mostra tutti i messaggi di errore per tutti gli account appartenenti all'unità organizzativa. Se necessario, puoi anche visualizzare i messaggi di errore nella pagina dei dettagli dell'account per ciascun account.

Facoltativamente, puoi scaricare un file contenente un rapporto dettagliato che mostra quali controlli preliminari non sono stati superati, per l'analisi offline. Puoi completare il download scegliendo il pulsante **Download**, che appare in alto a destra nell'area di registrazione.

Questa sezione elenca i tipi di errori che potresti ricevere se i controlli preliminari falliscono e come correggerli.

Errore nella zona di atterraggio

- Zona di atterraggio non pronta

Reimposta la tua attuale zona di atterraggio o aggiornala alla versione più recente.

Errori OU

- Supera il numero massimo di SCP

Potresti aver superato il limite per le politiche di controllo del servizio (SCP) per unità organizzativa oppure potresti aver raggiunto un'altra quota. Un limite di 10 SCP per unità organizzativa si applica a tutte le unità organizzative presenti nella zona di destinazione di AWS Control Tower. Se hai più SCP di quanto consentito dalla quota, devi eliminare o combinare gli SCP.

- SCP in conflitto

Gli SCP esistenti possono essere applicati all'unità organizzativa o all'account, il che impedisce ad AWS Control Tower di registrare l'account. Controlla gli SCP applicati per eventuali policy che potrebbero impedire il funzionamento di AWS Control Tower. Assicurati di controllare gli SCP ereditati dalle unità organizzative più in alto nella gerarchia.

- Supera la quota dello stack impostato

La quota dello stack set potrebbe essere stata superata. Se hai più istanze di quante ne consenta la quota, devi eliminare alcune istanze dello stack. Per ulteriori informazioni, consultare [Quote di AWS CloudFormation](#) nella Guida per l'utente di AWS CloudFormation .

- Supera il limite dell'account

AWS Control Tower limita ogni unità organizzativa a 1000 account durante la registrazione.

Errori di account

- Pre-checks impediti sugli account

Un SCP esistente nell'unità organizzativa impedisce ad AWS Control Tower di effettuare controlli preliminari sugli account dei membri dell'unità organizzativa. Per risolvere questo errore di verifica preliminare, aggiorna o rimuovi l'SCP dall'unità organizzativa.

- Errore nell'indirizzo email

L'indirizzo email specificato per l'account non è conforme agli standard di denominazione. Ecco l'espressione regolare (regex) che specifica quali caratteri sono consentiti: `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Registratore di configurazione o canale di consegna abilitato

L'account può avere un registratore di AWS Config configurazione o un canale di distribuzione esistente. Questi devono essere eliminati o modificati AWS CLI in tutte le AWS regioni in cui l'account di gestione AWS Control Tower ha governato le risorse, prima di poter registrare un account.

- STS disabilitato

Servizio di token di sicurezza AWS (AWS STS) può essere disabilitato nell'account. AWS Gli endpoint STS devono essere attivati negli account di tutte le regioni supportate da AWS Control Tower.

- Conflitto IAM Identity Center

La regione principale di AWS Control Tower non è la stessa della regione Centro identità AWS IAM (IAM Identity Center). Se IAM Identity Center è già configurato, la regione principale di AWS Control Tower deve essere la stessa della regione IAM Identity Center.

- Argomento SNS in conflitto

L'account ha un nome di argomento Amazon Simple Notification Service (Amazon SNS) che AWS Control Tower deve utilizzare. AWS Control Tower crea risorse (ad esempio argomenti SNS) con nomi specifici. Se questi nomi sono già stati utilizzati, la configurazione di AWS Control Tower non riesce. Questa situazione potrebbe verificarsi se si riutilizza un account precedentemente registrato in AWS Control Tower.

- È stato rilevato un account sospeso

Questo account è stato sospeso. Non può essere registrato in AWS Control Tower. Rimuovi l'account da questa unità organizzativa e riprova.

- Utente IAM non presente nel portafoglio

Aggiungi l'utente AWS Identity and Access Management (IAM) al portafoglio di Service Catalog prima di registrare l'unità organizzativa. Questo errore riguarda solo l'account di gestione.

- L'account non soddisfa i prerequisiti

L'account non soddisfa i prerequisiti per la registrazione dell'account. Ad esempio, all'account potrebbero mancare i ruoli e le autorizzazioni necessari per registrarlo in AWS Control Tower. Le istruzioni per aggiungere un ruolo sono disponibili in. [Aggiungi manualmente il ruolo IAM richiesto a un ruolo IAM esistente Account AWS e iscrivilo](#)

Come promemoria, AWS CloudTrail si attiva automaticamente su tutti i tuoi AWS account quando li registri in AWS Control Tower. Se CloudTrail è abilitata su un account precedente alla registrazione, è possibile che si verifichi una doppia fatturazione a meno che non venga CloudTrail disattivata prima di iniziare il processo di registrazione.

Aggiorna le organizzazioni

Il modo più rapido per aggiornare un'unità organizzativa (OU) o aggiornare più account all'interno di un'unità organizzativa consiste nell'eseguire una delle seguenti azioni:

- Re-register l'unità organizzativa se `AWSControlTowerBaseline` è abilitata.
- Reimposta le linee di base abilitate o ripristina i controlli abilitati se non `AWSControlTowerBaseline` è abilitato.

Quando aggiornare le unità organizzative e gli account AWS Control Tower

Quando esegui un aggiornamento della landing zone, devi aggiornare gli account registrati per applicare nuovi controlli a tali account.

- È possibile eseguire un aggiornamento di tutti gli account di un'unità organizzativa utilizzando l'opzione Re-Register o Reimposta.
- Se hai più di un'unità organizzativa registrata nella tua landing zone, registra nuovamente o reimposta tutte le unità organizzative per aggiornare tutti i tuoi account.
- Per aggiornare un singolo account, puoi eseguire l'aggiornamento dalla console AWS Control Tower oppure puoi selezionare l'opzione Update provisioned product in AWS Service Catalog se `AWSControlTowerBaseline` è abilitata sull'account. Per informazioni, consulta [Aggiorna l'account nella console](#).

Aggiorna più account nella stessa unità organizzativa

Ripeti questi passaggi per ogni unità organizzativa della tua organizzazione AWS Control Tower, se devi aggiornare tutti gli account e le unità organizzative.

Per aggiornare più account in un'unica unità organizzativa, con un'unica azione

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.

2. Nel menu di navigazione a sinistra, scegli Organizzazione.
3. Nella pagina Organizzazione, scegli un'unità organizzativa qualsiasi per visualizzare la pagina dei dettagli dell'unità organizzativa.
4. Se **AWSControlTowerBaseline** è abilitata sull'unità organizzativa, seleziona Re-Register OU in Azioni. Se non **AWSControlTowerBaseline** è abilitato sull'unità organizzativa, seleziona Reset AWS Config baseline in Actions per resettare la baseline abilitata e seleziona i controlli abilitati e Reset control nella sezione «Enabled controls» per reimpostare i controlli abilitati.

In alternativa, puoi selezionare qualsiasi account che mostri lo stato di Update available e quindi scegliere Aggiorna account, per tutti gli account necessari.

Cosa succede durante la nuova registrazione

Quando registri nuovamente un'unità organizzativa:

- Il campo di stato della baseline di AWS Control Tower indica se **AWSControlTowerBaseline** è applicato all'account (Enabled), se la baseline non è stata applicata (Non abilitata) o se l'applicazione della baseline non è riuscita in precedenza (Failed).
- Quando registri nuovamente l'unità organizzativa, il **AWSControlTowerExecution** ruolo viene aggiunto a tutti gli account con lo stato Non abilitato o Fallito.
- AWS Control Tower crea un accesso Single Sign-On (IAM Identity Center) per i nuovi account registrati.
- Gli account abilitati vengono registrati nuovamente in AWS Control Tower.
- L'eventuale modifica dei controlli preventivi applicati all'unità organizzativa è fissa, poiché gli SCP vengono ripristinati alle definizioni predefinite.
- Tutti gli account vengono aggiornati in base alle ultime modifiche alle landing zone.

Per ulteriori informazioni, consulta [Informazioni sulla registrazione degli account esistenti](#).

Tip

Quando registri nuovamente un'unità organizzativa o quando aggiorni la versione della landing zone e gli account di più membri, potresti visualizzare un messaggio di errore che menziona il. `StackSet-AWSControlTowerExecutionRole` Questa operazione `StackSet` nell'account di gestione può fallire perché il ruolo `AWSControlTowerExecutionIAM` esiste già

in tutti gli account dei membri registrati. Questo messaggio di errore è un comportamento previsto e può essere ignorato.

Aggiorna un singolo account

Note

La fornitura, l'aggiornamento e la personalizzazione di un singolo account devono essere indirizzati a un'unità organizzativa (OU) con AWSControlTowerBaseline abilitato. Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare le ResetEnabledControl API su ResetEnabledBaseline EnabledBaselines e EnabledControls su quell'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControlTowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

Puoi aggiornare singoli account AWS Control Tower nella console AWS Control Tower o nella console Service Catalog.

Per aggiornare un singolo account nella console AWS Control Tower, consulta [Aggiorna l'account nella console](#).

Per aggiornare un singolo account in AWS Service Catalog

1. Passa a AWS Service Catalog.
2. Nel menu di navigazione del riquadro a sinistra, scegli Provisioned products.
3. Nella pagina Provisioned products, seleziona il pulsante di opzione accanto al prodotto fornito che desideri aggiornare.
4. In alto a destra, scegli il menu a discesa Azioni per aggiornare.

Per ulteriori informazioni sull'aggiornamento in AWS Service Catalog, consulta [Aggiornare il prodotto fornito in Service Catalog](#) la sezione [Aggiornamento dei prodotti](#) nella Service Catalog Administrator Guide.

Trasferire un account a un'altra organizzazione

Puoi trasferire un account membro registrato in AWS Control Tower a un'altra AWS Organizations organizzazione.

Prerequisiti

- L'account deve essere registrato in AWS Control Tower nell'organizzazione di origine. Cioè, all'account vengono applicate linee di base, controlli proattivi o controlli investigativi.
- L'account deve essere stato creato almeno 4 giorni prima del trasferimento.
- È necessario avere accesso all'account di gestione dell'organizzazione di origine e di destinazione.

Fase 1: Annullare la registrazione dell'account da AWS Control Tower

Prima di trasferire l'account, devi disabilitare tutte le risorse AWS Control Tower applicate direttamente all'account. L'account può continuare a ereditare i controlli preventivi.

Se si utilizza la registrazione automatica

Sposta l'account in una delle seguenti posizioni:

- La radice dell'organizzazione
- Un'unità organizzativa non gestita
- Con Landing Zone 4.0 o versione successiva, un'unità organizzativa con solo controlli preventivi abilitati

Se non utilizzi la registrazione automatica

I metodi seguenti sono disponibili anche se utilizzi la registrazione automatica.

- Per gli account con la linea di base AWS Control Tower and Backup, scegli Unmanage dalla console AWS Control Tower. È inoltre possibile interrompere il prodotto fornito tramite il AWS Service Catalog APIs o la console.
- Per gli account con la linea di base AWS Config, disabilita la linea di base AWS Config sull'unità organizzativa oppure sposta l'account su root e utilizza l'API. `DisableBaseline`

Fase 2: Trasferire l'account all'organizzazione di destinazione

Dopo che tutte le linee di base e i controlli di AWS Control Tower applicati all'account diversi dai controlli preventivi sono stati disabilitati, completa il trasferimento.

1. Dall'account di gestione dell'organizzazione di destinazione, invia un invito all'account membro.
2. Accetta l'invito dall'account del membro.
3. Dall'account di gestione dell'organizzazione di destinazione, sposta l'account nell'unità organizzativa desiderata.

Per istruzioni sul processo di migrazione, consulta [Migrazione AWS degli account verso un'altra organizzazione](#) nella Guida per l'AWS Organizations utente.

Fase 3: Registrare l'account nell'organizzazione di destinazione

Una volta che l'account è nell'organizzazione di destinazione, registralo in AWS Control Tower.

- Se Auto Enroll è abilitato nella landing zone di AWS Control Tower che governa l'organizzazione di destinazione, AWS Control Tower applica automaticamente le linee di base e i controlli all'account.
- Se non utilizzi Auto Enroll nell'organizzazione di destinazione, registra manualmente l'account in AWS Control Tower. Per ulteriori informazioni, consulta [Informazioni sulla registrazione degli account esistenti](#).

Ulteriori considerazioni

Periodo di attesa

Gli account creati AWS Organizations tramite Account Factory devono avere almeno 4 giorni prima di poterli trasferire o rimuovere da un'organizzazione. Per ulteriori informazioni, consulta [Rimuovere un account membro da un'organizzazione](#) nella Guida per l'AWS Organizations utente.

AWS Limiti dell'aggregatore Config

Quando trasferisci più account, potresti raggiungere il limite di AWS Config per il numero massimo di account aggiunti o eliminati a settimana per tutti gli aggregatori (1.000). Per richiedere un aumento del limite, consulta [AWS Config service limits](#). Puoi anche eseguire l'aggiornamento alla versione 4.0 della landing zone, che utilizza un aggregatore Config collegato al servizio. Per maggiori dettagli, consulta [AWS Config updates in landing zone versione 4.0](#).

Accesso all'account membro

Gli account non registrati non hanno alcun ruolo `AWSControlTowerExecution`. Quando disabiliti la baseline Config o AWS Control Tower, AWS Control Tower elimina il ruolo di esecuzione e aggiunge il `OrganizationsAccountAccessRole`. Puoi utilizzare questo ruolo per accettare un invito per l'organizzazione di destinazione.

Quando l'account è registrato nell'organizzazione di destinazione, il `AWSControlTowerExecution` ruolo viene creato. Questo ruolo sostituisce `OrganizationsAccountAccessRole` e considera attendibile il nuovo account di gestione.

AWS Service Catalog e registrazione automatica

La registrazione automatica non agisce sulle risorse in AWS Service Catalog. Tutti i prodotti forniti da Account Factory rimangono nell'account di gestione anche se i conti sottostanti non sono registrati. Per terminare questi prodotti forniti nell'account di gestione, vedere [Eliminazione dei prodotti forniti nella Guida per l'utente](#) del AWS Service Catalog. Tutti i blueprint di Account Factory Customization (AFC) rimangono nell'account.

Servizi integrati

AWS Control Tower è un servizio che si basa su altri AWS servizi, per assisterti nella configurazione di un ambiente ben progettato. Questo capitolo fornisce una breve panoramica di questi servizi, comprese le informazioni di configurazione sui servizi sottostanti e sul loro funzionamento in AWS Control Tower.

Per ulteriori informazioni su come misurare un ambiente ben progettato, scopri lo [AWS Well-Architected strumento](#). Consulta anche la [Management and Governance Cloud Environment Guide](#).

Argomenti

- [AWS Opzioni di backup disponibili](#)
- [Implementa ambienti con CloudFormation](#)
- [Monitora gli eventi con CloudTrail](#)
- [Monitora risorse e servizi con CloudWatch](#)
- [Gestisci le configurazioni delle risorse con AWS Config](#)
- [Gestisci le autorizzazioni per le entità con IAM](#)
- [AWS Key Management Service](#)
- [Esegui funzioni di calcolo serverless con Lambda](#)
- [Gestisci gli account tramite AWS Organizations](#)
- [Archivia oggetti con Amazon S3](#)
- [Monitora il tuo ambiente con Security Hub CSPM](#)
- [Fornisci gli account tramite AWS Service Catalog](#)
- [Tieni traccia degli avvisi tramite Amazon Simple Notification Service](#)
- [Crea applicazioni distribuite con AWS Step Functions](#)

AWS Opzioni di backup disponibili

AWS Backup consente di creare un piano di backup per la zona di destinazione di AWS Control Tower. Puoi incorporare un flusso di lavoro di backup e ripristino dei dati direttamente nella tua zona di destinazione. Il piano di backup include regole predefinite, come i giorni di conservazione, la frequenza dei backup e la finestra temporale durante la quale viene eseguito il backup. Per ulteriori informazioni, consulta [AWS Backup e AWS Control Tower](#).

Implementa ambienti con CloudFormation

CloudFormation consente di creare e fornire implementazioni AWS dell'infrastruttura in modo prevedibile e ripetuto. Ti aiuta a sfruttare AWS i prodotti per creare applicazioni altamente affidabili, altamente scalabili e convenienti nel cloud senza preoccuparti di creare e configurare l'infrastruttura sottostante. AWS CloudFormation consente di utilizzare un file modello per creare ed eliminare una raccolta di risorse insieme come una singola unità (uno stack). Per ulteriori informazioni, consulta la Guida per l'utente di [AWS CloudFormation](#).

AWS Control Tower utilizza CloudFormation StackSets per distribuire e gestire le risorse di base, come i ruoli e i AWS Config registratori IAM, nei tuoi account. Per ulteriori informazioni su come funzionano CloudFormation insieme AWS Control Tower, consulta [Crea AWS Control Tower risorse con AWS CloudFormation](#)

Monitora gli eventi con CloudTrail

AWS Control Tower si configura AWS CloudTrail per consentire la registrazione e l'audit centralizzati. Con CloudTrail, l'account di gestione può esaminare le azioni amministrative e gli eventi del ciclo di vita degli account dei membri.

CloudTrail ti aiuta a monitorare il tuo AWS ambiente nel cloud conservando una cronologia delle chiamate AWS API per i tuoi account. Ad esempio, puoi identificare gli utenti e gli account che hanno chiamato le AWS API per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state effettuate le chiamate e l'ora in cui sono avvenute le chiamate. Puoi integrarti CloudTrail nelle applicazioni utilizzando l'API, automatizzare la creazione di percorsi per la tua organizzazione, controllare lo stato dei percorsi e controllare in che modo gli amministratori attivano e disattivano CloudTrail l'accesso. Per ulteriori informazioni, consulta la Guida per l'utente di [AWS CloudTrail](#).

Monitora risorse e servizi con CloudWatch

Amazon CloudWatch offre una soluzione di monitoraggio affidabile, scalabile e flessibile che puoi iniziare a utilizzare in pochi minuti. Non sarà più necessario configurare, gestire e ridimensionare sistemi di monitoraggio propri e relativa infrastruttura. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

Per ulteriori informazioni su come Amazon CloudWatch funziona con AWS Control Tower, consulta [Monitoring](#).

Gestisci le configurazioni delle risorse con AWS Config

AWS Config fornisce una visione dettagliata delle risorse associate al tuo AWS account, incluso come sono configurate, come sono correlate tra loro e come le configurazioni e le loro relazioni sono cambiate nel tempo. Per ulteriori informazioni, consulta la Guida per sviluppatori di [AWS Config](#).

AWS Config le risorse fornite da AWS Control Tower sono contrassegnate automaticamente con `aws-control-tower` un valore di `managed-by-control-tower`

Per ulteriori informazioni su come AWS Config monitora e registra le risorse in AWS Control Tower e su come vengono fatturate, consulta. [Monitora le modifiche alle risorse con AWS Config](#)

AWS Control Tower utilizza Regole di AWS Config per implementare i controlli investigativi. Per ulteriori informazioni, consulta [Informazioni sui controlli in AWS Control Tower](#).

Integrazione di AWS Config nella Control Tower Landing Zone 4.0

Service-Linked Config Aggregator (SLCA)

AWS Control Tower ora implementa un Service-Linked Config Aggregator (SLCA) come parte di Landing Zone 4.0+. Questa modifica rappresenta un miglioramento significativo nel modo in cui i dati di AWS Config vengono aggregati e gestiti all'interno dell'organizzazione.

Modifiche chiave

Nuova implementazione di Service-Linked Config Aggregator

- Un Service-Linked Config Aggregator viene distribuito nell'account di integrazione AWS Config designato.
- Per i clienti esistenti, questo sarà il tuo account di controllo
- Per i nuovi clienti, questo sarà l'account specificato nel `config.accountId` campo del manifesto

Amministratore delegato

- L'account aggregatore AWS Config diventa l'amministratore delegato di AWS Config
- AWS Control Tower configura automaticamente le impostazioni degli amministratori delegati
- Ciò consente la gestione centralizzata di AWS Config in tutta l'organizzazione

Migrazione da Legacy Aggregators

Durante l'aggiornamento a Landing Zone 4.0:

- L'aggregatore dell'organizzazione nell'account di gestione verrà rimosso.
- L'aggregatore di account nell'account di controllo verrà rimosso.
- Questi vengono sostituiti dal nuovo Config Aggregator collegato al servizio nell'account di aggregazione di integrazione AWS Config.

Aggregazione avanzata dei dati

Il Config Aggregator collegato al servizio offre funzionalità migliorate per l'aggregazione dei dati di Config:

- Può aggregare dati da qualsiasi registratore AWS Config della tua organizzazione
- Include dati provenienti da account non gestiti da Control Tower
- Fornisce una visione completa degli elementi di configurazione in tutta l'organizzazione
- Supporta controlli avanzati del perimetro dei dati

Considerazioni importanti

Configurazione dell'amministratore delegato

- AWS Control Tower utilizzerà l'account specificato nel manifesto per l'integrazione con AWS Config
- Questo account verrà automaticamente configurato come amministratore delegato
- Per questa configurazione non è richiesta alcuna azione aggiuntiva da parte dei clienti
- Per i clienti esistenti, il precedente account di integrazione di Security Roles (account Audit) verrà configurato come account aggregatore centrale di AWS Config durante l'aggiornamento a Landing Zone 4.0

Ambito di aggregazione dei dati

- Service-Linked Config Aggregator può aggregare dati di configurazione da:
 - Account gestiti da Control Tower
 - Non-Control Account gestiti da Tower

- Qualsiasi account con un registratore di configurazione attivo nella tua organizzazione

Controlli di accesso

- L'accesso ai dati aggregati è gestito tramite politiche IAM
- L'account aggregatore centrale AWS Config ha un accesso centralizzato a tutti i dati aggregati
- Gli account membri gestiscono i propri registratori AWS Config individuali

Best practice

Selezione dell'account Config Central Aggregator

- Scegli un account dedicato al monitoraggio della sicurezza e della conformità
- Assicurati che siano in atto controlli di accesso appropriati
- Prendi in considerazione l'utilizzo di un account di controllo o sicurezza esistente

Gestione dei dati

- Rivedi regolarmente i dati di configurazione aggregati
- Implementa politiche di conservazione appropriate
- Monitora lo stato del registratore AWS Config su tutti gli account

Impatto della migrazione

Quando si esegue l'aggiornamento a Landing Zone 4.0:

Prima della migrazione

- Documenta le regole e gli aggregatori di AWS Config esistenti
- Rivedi gli attuali modelli di accesso ai dati di AWS Config
- Pianifica eventuali aggiornamenti delle policy IAM necessari

Durante la migrazione

- Gli aggregatori AWS Config precedenti verranno rimossi automaticamente

- Service-Linked Verrà distribuito Config Aggregator
- L'amministratore delegato verrà configurato

Dopo la migrazione

- Verifica che Service-Linked Config Aggregator funzioni correttamente
- Conferma l'aggregazione dei dati dagli account dei membri
- Aggiorna gli strumenti di monitoraggio e reporting secondo necessità

Gestisci le autorizzazioni per le entità con IAM

AWS Identity and Access Management (IAM) è un AWS servizio per il controllo dell'accesso ad altri AWS servizi. Con IAM, puoi gestire centralmente gli utenti, le credenziali di sicurezza, come le chiavi di accesso e le autorizzazioni, che designano le AWS risorse a cui gli utenti e le applicazioni hanno accesso.

Quando configuri la tua zona di destinazione, puoi creare Centro identità AWS IAM automaticamente una serie di gruppi, se selezioni IAM come provider di identità. Questi gruppi dispongono di set di autorizzazioni che sono politiche di autorizzazione predefinite di IAM. Gli utenti finali possono anche utilizzare IAM per definire l'ambito delle autorizzazioni per gli utenti IAM e altre entità all'interno degli account dei membri.

AWS Identity and Access Management (IAM) semplifica la gestione dell'accesso agli AWS account e alle applicazioni aziendali. Puoi controllare l'accesso all'IAM Identity Center e le autorizzazioni utente su tutti i tuoi AWS account in AWS Control Tower.

Per ulteriori informazioni, consulta la Guida per l'utente di [Centro identità AWS IAM](#).

Se risiedi in un paese Regione AWS che non supporta IAM, puoi rivolgerti a un altro provider di identità per configurare e gestire manualmente i tuoi utenti e gruppi.

AWS Key Management Service

AWS Key Management Service (AWS KMS) consente di creare e controllare chiavi che proteggono i dati. AWS Control Tower consente opzionalmente di crittografare i dati con chiavi di AWS KMS crittografia. Per informazioni su AWS KMS, consulta la [AWS KMS Developer Guide](#).

Per informazioni su come configurare le AWS KMS chiavi con AWS Control Tower, consulta Configurazione [AWS KMS opzionale delle chiavi](#).

Esegui funzioni di calcolo serverless con Lambda

Con AWS Lambda, puoi eseguire il codice senza fornire o gestire i server. È possibile eseguire codice per molti tipi di applicazioni o servizi di backend, senza la necessità di ulteriori costi amministrativi. Quando carichi il codice, Lambda può eseguire e scalare il codice con elevata disponibilità. Puoi configurare il codice in modo che venga attivato automaticamente da altri AWS servizi oppure puoi richiamarlo direttamente da qualsiasi app web o mobile.

Ad esempio, alcuni ruoli nell'account di audit di AWS Control Tower possono essere assunti a livello di programmazione, in modo da poter esaminare altri account utilizzando Lambda. Inoltre, puoi utilizzare gli eventi del ciclo di vita di AWS Control Tower per attivare le funzioni Lambda.

Gestisci gli account tramite AWS Organizations

AWS Organizations è un servizio di gestione degli account che consente di consolidare più AWS account in un'organizzazione creata e gestita centralmente. Con Organizations, puoi creare account membri e invitare account esistenti a entrare a far parte della tua organizzazione. Puoi organizzare questi account in gruppi e collegarvi controlli basati su policy. Per ulteriori informazioni, consulta la Guida per l'utente di [AWS Organizations](#).

In AWS Control Tower, Organizations aiuta a gestire centralmente la fatturazione, controllare l'accesso, la conformità e la sicurezza e condividere le risorse tra gli AWS account dei membri. Gli account vengono raggruppati in gruppi logici, denominati unità organizzative. Per ulteriori informazioni sulle organizzazioni, consulta la Guida [per](#) AWS Organizations l'utente.

AWS Control Tower utilizza le seguenti unità organizzative:

- **Root:** il contenitore principale per tutti gli account e tutte le altre unità organizzative nella tua zona di destinazione.
- **Sicurezza:** questa unità organizzativa contiene l'account di archiviazione dei log, l'account di controllo e le risorse di cui sono proprietarie.
- **Sandbox:** questa unità organizzativa viene creata quando si imposta la zona di atterraggio. Questa e altre unità organizzative secondarie nella tua zona di atterraggio contengono gli account dei tuoi membri. Questi sono gli account a cui gli utenti finali accedono per eseguire operazioni sulle AWS risorse.

 Note

Puoi aggiungere unità organizzative aggiuntive nella tua zona di destinazione tramite la console AWS Control Tower nella [pagina delle unità organizzative](#).

Considerazioni

Alle unità organizzative create tramite AWS Control Tower possono essere applicati dei controlli. Per impostazione predefinita, le unità organizzative create all'esterno di AWS Control Tower non possono. Tuttavia, è possibile registrare tali unità organizzative. Dopo aver registrato un'unità organizzativa, puoi applicarne i controlli e applicarne i controlli. Per informazioni sulla registrazione di un'unità organizzativa, consulta [Registrare un'unità organizzativa esistente con AWS Control Tower](#).

Archivia oggetti con Amazon S3

Amazon Simple Storage Service (Amazon S3) è un servizio di storage su Internet. È possibile utilizzare Amazon S3 per memorizzare e recuperare qualsiasi volume di dati, in qualunque momento e da qualunque luogo tramite il Web. Queste operazioni possono essere eseguite tramite l'interfaccia Web semplice e intuitiva della Console di gestione AWS. Per ulteriori informazioni, consulta la Guida per l'utente di [Amazon Simple Storage Service](#).

Quando configuri la tua zona di destinazione, viene creato un bucket Amazon S3 nel tuo account di archivio dei log per contenere tutti i log di tutti gli account nella tua zona di destinazione.

Monitora il tuo ambiente con Security Hub CSPM

AWS Control Tower è integrato con AWS Security Hub CSPM tramite lo standard Security Hub CSPM chiamato Service-Managed Standard: AWS Control Tower. Per ulteriori informazioni, consulta [lo standard Security Hub](#).

Fornisci gli account tramite AWS Service Catalog

AWS Service Catalog consente agli amministratori IT di creare, gestire e distribuire portafogli di prodotti approvati agli utenti finali, che hanno quindi accesso ai prodotti di cui hanno bisogno in un portale personalizzato. I prodotti tipici includono server, database, siti Web o applicazioni che vengono distribuiti utilizzando risorse AWS.

È possibile controllare gli utenti che hanno accesso a prodotti specifici, il che consente di imporre la conformità agli standard aziendali organizzativi, gestire i cicli di vita dei prodotti e aiutare gli utenti a trovare e lanciare prodotti con sicurezza. Per ulteriori informazioni, consultare la [Service Catalog Administrator Guide](#).

In AWS Control Tower, gli amministratori cloud centrali e gli utenti finali possono effettuare il provisioning di account personalizzati nella zona di destinazione utilizzando AWS Service Catalog prodotti, denominati progetti personalizzati. Per ulteriori informazioni, consulta [la Fase 2. Crea il AWS Service Catalog prodotto](#).

Puoi interagire con gli account AWS Control Tower tramite la AWS Service Catalog console e le API. Per ulteriori informazioni, consulta [Interagisci con gli account AWS Control Tower da AWS Service Catalog](#)

AWS Control Tower può anche utilizzare le API del Service Catalog per automatizzare ulteriormente il provisioning e l'aggiornamento degli account. Per informazioni dettagliate, consulta la [Developer Guide. AWS Service Catalog](#)

Tieni traccia degli avvisi tramite Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) è un servizio web che consente alle applicazioni, agli utenti finali e ai dispositivi di inviare e ricevere notifiche istantaneamente dal cloud. Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di Amazon Simple Notification Service](#).

AWS Control Tower utilizza Amazon SNS per inviare avvisi programmatici agli indirizzi e-mail del tuo account di gestione e del tuo account di controllo. Questi avvisi ti aiutano a prevenire la deriva all'interno della tua zona di atterraggio. Per ulteriori informazioni, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Utilizziamo anche Amazon Simple Notification Service per inviare notifiche di conformità da AWS Config

Tip

Uno dei modi migliori per ricevere notifiche di conformità al controllo di AWS Control Tower (nel tuo account di audit) è abbonarti a `AggregateConfigurationNotifications`. È un servizio che ti aiuta a verificare la conformità. Fornisce dati reali sulle AWS Config regole che non sono conformi. AWS Config mantiene automaticamente l'elenco degli account nell'unità organizzativa.

È necessario abbonarsi manualmente, tramite e-mail o qualsiasi tipo di abbonamento consentito da SNS. L'estratto conto `arn:aws:sns:homeregion:account:aws-controltower-AggregateSecurityNotifications` rimanda al tuo account di controllo.

Crea applicazioni distribuite con AWS Step Functions

AWS Step Functions semplifica il coordinamento dei componenti delle applicazioni distribuite in una serie di passaggi in un flusso di lavoro visivo. Si possono creare ed eseguire stati macchina che permettono di eseguire le fasi dell'applicazione in modo affidabile e scalabile. Per ulteriori informazioni, consulta la [AWS Step Functions Guida per sviluppatori](#).

Gestione delle identità e degli accessi in AWS Control Tower

Per eseguire qualsiasi operazione nella tua zona di destinazione, ad esempio il provisioning degli account in Account Factory o la creazione di nuove unità organizzative (OU) nella console AWS Control Tower, puoi scegliere AWS Identity and Access Management (IAM) o Centro identità AWS IAM richiedere l'autenticazione di essere un utente approvato AWS . Ad esempio, se utilizzi la console AWS Control Tower, autentichi la tua identità fornendo AWS le tue credenziali, fornite dall'amministratore.

Dopo aver autenticato la tua identità, IAM controlla il tuo accesso AWS con un set definito di autorizzazioni su un set specifico di operazioni e risorse. Se sei un amministratore di account, puoi utilizzare IAM per controllare l'accesso di altri utenti IAM alle risorse associate al tuo account.

Argomenti

- [Autenticazione](#)
- [Controllo accessi](#)
- [Lavorare con AWS IAM Identity Center e AWS Control Tower](#)
- [Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#)
- [Impedisce l'impersonificazione tra servizi](#)
- [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#)

Autenticazione

Puoi accedere AWS a uno dei seguenti tipi di identità:

- **AWS utente root dell'account:** quando si crea un AWS account per la prima volta, si inizia con un'identità che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è denominata utente root dell' AWS account. Puoi accedere a questa identità utilizzando l'indirizzo e-mail e la password usati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Segui invece la [best practice di utilizzare l'utente root solo per creare il tuo primo utente IAM Identity Center \(consigliato\) o utente IAM \(pratica non consigliata nella maggior parte dei casi d'uso\)](#). Quindi conservare al sicuro le credenziali dell'utente root e utilizzarle per eseguire solo alcune attività di gestione dell'account e del servizio. Per ulteriori informazioni, consulta [Quando accedere come utente root](#).

- **Utente IAM:** un utente [IAM](#) è un'identità all'interno del tuo AWS account che dispone di autorizzazioni specifiche e personalizzate. Puoi utilizzare le credenziali utente IAM per accedere a AWS pagine Web sicure come la Console di AWS gestione, i forum di AWS discussione o il AWS Centro assistenza. AWS Le best practice consigliano di creare un utente IAM Identity Center anziché un utente IAM, perché c'è un rischio maggiore per la sicurezza quando si crea un utente IAM con credenziali a lungo termine.

Se devi creare un utente IAM per un determinato scopo, oltre alle credenziali di accesso, puoi generare chiavi di accesso per ogni utente IAM. Puoi utilizzare queste chiavi quando AWS chiami i servizi in modo programmatico, tramite uno dei vari SDK o utilizzando l'interfaccia a riga di AWS comando (CLI). L'SDK e gli strumenti della CLI utilizzano le chiavi di accesso per firmare crittograficamente la tua richiesta. Se non utilizzi AWS strumenti, devi firmare tu stesso la richiesta. AWS Control Tower supporta Signature Version 4, un protocollo per l'autenticazione delle richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste, consulta [Signature Version 4 Signing Process](#) nella sezione General Reference. AWS

- **Ruolo IAM:** un [ruolo IAM](#) è un'identità IAM che è possibile creare nell'account e che dispone di autorizzazioni specifiche. Un ruolo IAM è simile a un utente IAM in quanto è un' AWS identità e dispone di politiche di autorizzazione che determinano cosa può e non può fare l'identità. AWS Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Inoltre, un ruolo non ha credenziali a lungo termine standard associate (password o chiavi di accesso). Tuttavia, quando assumi un ruolo, vengono fornite le credenziali di sicurezza provvisorie per la sessione del ruolo. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:
 - **Accesso utente federato:** anziché creare un utente IAM, puoi utilizzare le identità esistenti provenienti dalla Directory Service tua directory utente aziendale o da un provider di identità web. Questi sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando l'accesso viene richiesto tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta la sezione relativa a [utenti federati e ruoli](#) nella Guida per l'utente di IAM.
 - **AWS accesso al servizio:** un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni nel tuo account per tuo conto. Quando si configurano alcuni ambienti AWS di servizio, è necessario definire un ruolo che il servizio deve assumere. Questo ruolo di servizio deve includere tutte le autorizzazioni necessarie al servizio per accedere alle AWS risorse di cui ha bisogno. I ruoli del servizio variano da servizio a servizio, ma molti permettono di selezionare le autorizzazioni, a condizione di soddisfare i requisiti documentati per quel servizio. I ruoli del servizio forniscono l'accesso all'interno dell'account e non possono essere utilizzati per concedere l'accesso ai servizi in altri account. Puoi creare, modificare ed eliminare un ruolo del

servizio dall'interno di IAM. Ad esempio, puoi creare un ruolo che consente ad Amazon Redshift di accedere a un bucket Amazon S3 per tuo conto e quindi caricare i dati dal bucket in un cluster Amazon Redshift. Per ulteriori informazioni, consulta [Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio](#) nella IAM User Guide.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza Amazon EC2 e che AWS effettuano richieste CLI o API. AWS Questo è preferibile all'archiviazione delle chiavi di accesso all'interno dell'istanza Amazon EC2. Per assegnare un AWS ruolo a un'istanza Amazon EC2 e renderla disponibile per tutte le sue applicazioni, è necessario creare un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza Amazon EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.
- L'autenticazione degli utenti di IAM Identity Center al portale utenti di IAM Identity Center è controllata dalla directory che hai connesso a IAM Identity Center. Tuttavia, l'autorizzazione agli AWS account disponibili per gli utenti finali dall'interno del portale utente è determinata da due fattori:
 - A chi è stato assegnato l'accesso a tali AWS account nella console AWS IAM Identity Center. Per ulteriori informazioni, consulta [Single Sign-On Access](#) nella Guida Centro identità AWS IAM per l'utente.
 - Quale livello di autorizzazioni è stato concesso agli utenti finali nella console AWS IAM Identity Center per consentire loro l'accesso appropriato a tali account. AWS Per ulteriori informazioni, consulta [Permission Sets](#) nella Guida per l'Centro identità AWS IAM utente.

Controllo accessi

Per creare, aggiornare, eliminare o elencare le risorse AWS Control Tower o altre AWS risorse nella tua zona di destinazione, hai bisogno delle autorizzazioni per eseguire l'operazione e hai bisogno delle autorizzazioni per accedere alle risorse corrispondenti. Inoltre, per eseguire l'operazione a livello di codice, devi disporre di chiavi di accesso valide.

Le seguenti sezioni descrivono come gestire le autorizzazioni per AWS Control Tower:

Argomenti

- [Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#)

- [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#)

Lavorare con AWS IAM Identity Center e AWS Control Tower

In AWS Control Tower, IAM Identity Center consente agli amministratori centrali del cloud e agli utenti finali di gestire l'accesso a più AWS account e applicazioni aziendali. Per impostazione predefinita, AWS Control Tower utilizza questo servizio per configurare e gestire l'accesso agli account creati tramite Account Factory, a meno che tu non abbia selezionato l'opzione per la gestione automatica dell'identità e del controllo degli accessi.

Per ulteriori informazioni sulla selezione di un provider di identità, consulta [Linee guida per IAM Identity Center](#).

Per un breve tutorial su come configurare gli utenti e le autorizzazioni del tuo IAM Identity Center in AWS Control Tower, puoi guardare questo video (6:23). Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Guida video alla configurazione di AWS IAM Identity Center in AWS Control Tower.](#)

Informazioni sulla configurazione di AWS Control Tower con IAM Identity Center

Quando configuri inizialmente AWS Control Tower, solo l'utente root e tutti gli utenti IAM con le autorizzazioni corrette possono aggiungere utenti IAM Identity Center. Tuttavia, dopo che gli utenti finali sono stati aggiunti al AWSAccountFactorygruppo, possono creare nuovi utenti IAM Identity Center dalla procedura guidata Account Factory. Per ulteriori informazioni, consulta [Fornisci e gestisci gli account con Account Factory](#).

Se scegli l'impostazione predefinita consigliata, AWS Control Tower configura la tua landing zone con una directory preconfigurata che ti aiuta a gestire le identità degli utenti e il single sign-on, in modo che gli utenti abbiano accesso federato tra gli account. Quando configuri la landing zone, questa directory predefinita viene creata per contenere gruppi di utenti e set di autorizzazioni.

Note

Puoi delegare l'amministrazione della Centro identità AWS IAM tua organizzazione a un account diverso dall'account di gestione, utilizzando la funzionalità di amministratore delegato di IAM Identity Center. Se scegli di utilizzare questa funzionalità, tieni presente che gli

amministratori con accesso alla gestione dell'appartenenza ai gruppi possono gestire anche i gruppi assegnati all'account di gestione. Per ulteriori informazioni, consulta questo post del blog, intitolato [Guida introduttiva all'amministrazione delegata AWS SSO](#)

Gruppi di utenti, ruoli e set di autorizzazioni

I gruppi di utenti gestiscono ruoli specializzati definiti all'interno degli account condivisi. I ruoli stabiliscono set di autorizzazioni a cui appartengono. Tutti i membri di un gruppo ereditano i set di autorizzazioni o i ruoli associati al gruppo. È possibile creare nuovi gruppi per gli utenti finali degli account membri, in modo da poter assegnare solo i ruoli necessari per le attività specifiche eseguite da un gruppo.

I set di autorizzazioni disponibili coprono un'ampia gamma di requisiti di autorizzazione utente distinti, come l'accesso in sola lettura, l'accesso amministrativo ad AWS Control Tower e l'accesso al Service Catalog. Questi set di autorizzazioni consentono agli utenti finali di effettuare il provisioning AWS dei propri account nella landing zone in modo rapido e conforme alle linee guida aziendali.

Per suggerimenti su come pianificare le allocazioni di utenti, gruppi e autorizzazioni, fare riferimento a [Consigli per la configurazione di gruppi, ruoli e politiche](#)

Per ulteriori informazioni su come utilizzare questo servizio nel contesto di AWS Control Tower, consulta i seguenti argomenti nella Guida per l'Centro identità AWS IAM utente.

- Per aggiungere utenti, consulta [Aggiungi utenti](#).
- Per aggiungere utenti a gruppi, consulta [Aggiungi utente e gruppi](#).
- Per modificare le proprietà dell'utente, consulta [Modifica proprietà dell'utente](#).
- Per aggiungere un gruppo, consulta [Aggiungi gruppi](#).

Warning

AWS Control Tower configura la directory IAM Identity Center nella tua regione d'origine. Se configuri la landing zone in un'altra regione e poi accedi alla console IAM Identity Center, devi modificare la regione nella tua regione di origine. Non eliminare la configurazione di IAM Identity Center nella tua regione d'origine.

Cose da sapere sugli account IAM Identity Center e AWS Control Tower

Ecco alcune cose utili da sapere quando si lavora con gli account utente IAM Identity Center in AWS Control Tower.

- Se il tuo account utente AWS IAM Identity Center è disabilitato, riceverai un messaggio di errore quando provi a fornire nuovi account in Account Factory. Puoi riabilitare il tuo utente IAM Identity Center nella console IAM Identity Center.
- Se si specifica un nuovo indirizzo e-mail utente IAM Identity Center quando si aggiorna il prodotto fornito associato a un account fornito da Account Factory, AWS Control Tower crea un nuovo account utente IAM Identity Center. L'account utente creato in precedenza non viene rimosso. Se preferisci rimuovere l'indirizzo e-mail utente precedente di IAM Identity Center da AWS IAM Identity Center, consulta [Disabilitazione](#) di un utente.
- AWS IAM Identity Center è stato [integrato con Azure Active Directory](#) e puoi connettere il tuo Azure Active Directory esistente a AWS Control Tower.
- Per ulteriori informazioni su come il comportamento di AWS Control Tower interagisce con AWS IAM Identity Center e diverse fonti di identità, consulta [Considerations for Changing Your Identity Source nella documentazione](#) di AWS IAM Identity Center.

Gruppi IAM Identity Center per AWS Control Tower

AWS Control Tower offre gruppi preconfigurati per organizzare gli utenti che svolgono attività specifiche nei tuoi account. Puoi aggiungere utenti e assegnarli a questi gruppi direttamente in IAM Identity Center. In questo modo i set di autorizzazione corrispondono agli utenti in gruppi all'interno degli account. Per le linee guida e le best practice più recenti sulla configurazione dei gruppi, consulta [le Best practice](#) nella Guida per l'utente di IAM Identity Center.

I seguenti gruppi vengono creati quando configuri la landing zone.

AWSAccountFactory

Account	Set di autorizzazioni	Description
Gestione dell'account	AWSServiceCatalogE ndUserAccess	Questo gruppo viene utilizzato in questo account solo per fornire nuovi account utilizzando Account Factory.

AWSServiceCatalogAdmins

Account	Set di autorizzazioni	Description
Gestione dell'account	AWSServiceCatalogAdminFullAccess	Questo gruppo viene utilizzato solo in questo account per apportare modifiche amministrative a Account Factory. Gli utenti di questo gruppo non possono fornire nuovi account a meno che non facciano parte anche loro del AWSAccountFactorygruppo.

AWSControlTowerAdmins

Account	Set di autorizzazioni	Description
Gestione dell'account	AWSAdministratorAccess	Gli utenti di questo gruppo in questo account sono gli unici ad avere accesso alla console AWS Control Tower.
Account di archiviazione dei log	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.
Account di audit	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.
Account membri	AWSOrganizationsFullAccess	Gli utenti hanno pieno accesso a Organizations in questo account.

AWSSecurityAuditPowerUsers

Account	Set di autorizzazioni	Description
Gestione dell'account	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo AWS consapevole delle applicazioni.
Account di archiviazione dei log	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo AWS consapevole delle applicazioni.
Account di audit	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo di applicazioni AWS consapevoli.
Account membri	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo di applicazioni AWS consapevoli.

AWSSecurityAuditors

Account	Set di autorizzazioni	Description
Gestione dell'account	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS

Account	Set di autorizzazioni	Description
		servizi e le risorse di questo account.
Account di archiviazione dei log	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.
Account di audit	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.
Account membri	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.

AWSLogArchiveAdmins

Account	Set di autorizzazioni	Description
Account di archiviazione dei log	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.

AWSLogArchiveViewers

Account	Set di autorizzazioni	Description
Account di archiviazione dei log	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.

AWSAuditAccountAdmins

Account	Set di autorizzazioni	Description
Account di audit	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.

Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower

Ogni AWS risorsa è di proprietà di un Account AWS e le autorizzazioni per creare o accedere a una risorsa sono regolate da politiche di autorizzazione. Un amministratore dell'account è in grado di collegare le policy relative alle autorizzazioni alle identità IAM (ovvero utenti, gruppi e ruoli). Alcuni servizi (ad esempio AWS Lambda) supportano anche l'aggiunta di criteri di autorizzazione alle risorse.

Note

Un amministratore account (o un amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consulta [Best practice IAM](#) nella Guida per l'utente di IAM.

Quando si è responsabili della concessione delle autorizzazioni a un utente o ruolo, è necessario conoscere e tenere traccia degli utenti e dei ruoli che richiedono autorizzazioni, delle risorse per le quali ogni utente e ruolo richiede le autorizzazioni e delle azioni specifiche che devono essere consentite per il funzionamento di tali risorse.

Argomenti

- [Risorse e operazioni di AWS Control Tower](#)
- [Informazioni sulla proprietà delle risorse](#)
- [Gestisci l'accesso alle risorse](#)
- [Specifica gli elementi delle policy: azioni, effetti e principi](#)
- [Specifica delle condizioni in una policy](#)

Risorse e operazioni di AWS Control Tower

In AWS Control Tower, la risorsa principale è una zona di atterraggio. AWS Control Tower supporta anche un tipo di risorsa aggiuntivo, i controlli, a volte denominati guardrail. Tuttavia, per AWS Control Tower, puoi gestire i controlli solo nel contesto di una zona di atterraggio esistente. I controlli possono essere definiti una sottorisorsa.

Alle risorse e alle risorse secondarie in Amazon AWS sono associati nomi di risorse Amazon (ARN) univoci, come mostrato nell'esempio seguente.

AWS Control Tower fornisce una serie di operazioni API per lavorare con le risorse di AWS Control Tower. Per un elenco delle operazioni disponibili, consulta AWS Control Tower, [l'API Reference di AWS Control Tower](#).

Per ulteriori informazioni sulle CloudFormation risorse di AWS Control Tower, consulta [la Guida per AWS CloudFormation l'utente](#).

Informazioni sulla proprietà delle risorse

L' AWS account è il proprietario delle risorse create nell'account, indipendentemente da chi le ha create. In particolare, il proprietario della risorsa è l' AWS account dell'entità [principale](#) (ovvero l'utente Account AWS root, un utente IAM Identity Center, un utente IAM o un ruolo IAM) che autentica la richiesta di creazione della risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le AWS credenziali dell'utente root del tuo AWS account per configurare una zona di atterraggio, il tuo AWS account è il proprietario della risorsa.
- Se crei un utente IAM nel tuo AWS account e concedi a quell'utente le autorizzazioni per configurare una zona di atterraggio, l'utente può configurare una zona di atterraggio purché il suo account soddisfi i prerequisiti. Tuttavia, il tuo AWS account, a cui appartiene l'utente, possiede la risorsa della zona di atterraggio.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per configurare una zona di atterraggio, chiunque possa assumere il ruolo può configurare una zona di atterraggio. Il tuo AWS account, a cui appartiene il ruolo, possiede la risorsa della zona di atterraggio.

Gestisci l'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

Note

Questa sezione illustra l'utilizzo di IAM nel contesto di AWS Control Tower. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa, consulta [Che cos'è IAM?](#) nella Guida per l'utente di IAM. Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta [Riferimento alle policy IAM di AWS](#) nella Guida per l'utente di IAM.

Le policy associate a un'identità IAM sono denominate policy basate sull'identità (policy IAM). Le policy collegate a una risorsa vengono definite policy basate sulle risorse.

Note

AWS Control Tower supporta solo policy basate sull'identità (policy IAM).

Argomenti

- [Informazioni sulle politiche basate sull'identità \(politiche IAM\)](#)
- [Crea ruoli e assegna autorizzazioni](#)
- [Resource-based politiche](#)

Informazioni sulle politiche basate sull'identità (politiche IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo nel tuo account: per concedere a un utente le autorizzazioni per creare una risorsa AWS Control Tower, ad esempio per configurare una zona di destinazione, puoi allegare una politica di autorizzazioni a un utente o gruppo a cui appartiene l'utente.
- Collega una policy di autorizzazione a un ruolo (assegnazione di autorizzazioni tra account): per concedere autorizzazioni tra più account, è possibile collegare una policy di autorizzazione basata

su identità a un ruolo IAM. Ad esempio, un amministratore di un AWS account (Account A) può creare un ruolo che concede autorizzazioni tra account a un altro AWS account (Account B) oppure l'amministratore può creare un ruolo che concede autorizzazioni a un altro AWS servizio.

1. L'amministratore dell'Account A crea un ruolo IAM e allega una policy di autorizzazioni al ruolo che concede le autorizzazioni per gestire le risorse nell'Account A.
2. L'amministratore dell'Account A attribuisce una politica di fiducia al ruolo. La policy identifica l'Account B come principale che può assumere il ruolo.
3. In qualità di principale, l'amministratore dell'Account B può concedere a qualsiasi utente dell'Account B il permesso di assumere il ruolo. Assumendo il ruolo, gli utenti dell'Account B possono creare o accedere alle risorse nell'Account A.
4. Per concedere a un AWS servizio la capacità (autorizzazioni) di assumere il ruolo, il principale specificato nella politica di fiducia può essere un AWS servizio.

Crea ruoli e assegna autorizzazioni

I ruoli e le autorizzazioni consentono di accedere alle risorse, in AWS Control Tower e in altri AWS servizi, incluso l'accesso programmatico alle risorse.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in: Centro identità AWS IAM

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di Centro identità AWS IAM .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consulta [Access Management](#) nella IAM User Guide (Guida per l'utente di IAM).

 Note

Quando configuri una landing zone di AWS Control Tower, avrai bisogno di un utente o di un ruolo con la policy `AdministratorAccess` gestita. (`arn:aws:iam: :aws:) policy/ AdministratorAccess`

Per creare un ruolo per un Servizio AWS (console IAM)

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. Per Tipo di entità attendibile, seleziona Servizio AWS.
4. Per Servizio o caso d'uso, scegli un servizio, quindi scegli il caso d'uso. I casi d'uso sono definiti dal servizio per includere la politica di fiducia richiesta dal servizio.
5. Scegli Avanti.
6. Per Policy di autorizzazione, le opzioni dipendono dal caso d'uso selezionato:
 - Se il servizio definisce le autorizzazioni per il ruolo, le policy di autorizzazioni non possono essere selezionate.
 - Seleziona una policy da un set limitato di policy di autorizzazione.
 - Seleziona una policy tra tutte le policy di autorizzazione.
 - Non selezionare policy di autorizzazioni, crea le policy dopo la creazione del ruolo e quindi collegale al ruolo.
7. (Facoltativo) Impostare un [limite delle autorizzazioni](#). Questa è una funzionalità avanzata disponibile per i ruoli di servizio, ma non per i ruoli collegati ai servizi.
 - a. Apri la sezione Imposta limite delle autorizzazioni e seleziona Usa un limite delle autorizzazioni per controllare il numero massimo di autorizzazioni del ruolo.

IAM include un elenco delle politiche AWS gestite e gestite dal cliente nel tuo account.
 - b. Selezionare la policy da utilizzare per il limite delle autorizzazioni.
8. Scegli Avanti.

9. Per Nome del ruolo, le opzioni dipendono dal servizio:

- Se il servizio definisce il nome del ruolo, non puoi modificarlo.
- Se il servizio definisce un prefisso per il nome del ruolo, puoi inserire un suffisso facoltativo.
- Se il servizio non definisce il nome del ruolo, puoi assegnare un nome al ruolo.

 Important

Quando assegni un nome a un ruolo, tieni presente quanto segue:

- I nomi dei ruoli devono essere univoci all'interno del tuo Account AWS e non possono essere resi univoci per caso.

Ad esempio, non creare ruoli denominati **PRODRROLE** e **prodrole**. Quando il nome di un ruolo viene utilizzato in una policy o come parte di un ARN, il nome del ruolo fa distinzione tra maiuscole e minuscole, tuttavia quando un nome di ruolo viene visualizzato ai clienti nella console, ad esempio durante il processo di accesso, il nome del ruolo non fa distinzione tra maiuscole e minuscole.

- Non è possibile modificare il nome del ruolo dopo averlo creato, in quanto altre entità possono fare riferimento al ruolo.

10. (Facoltativo) In Descrizione, inserisci una descrizione per il ruolo.
11. (Facoltativo) Per modificare i casi d'uso e le autorizzazioni per il ruolo, in Fase 1: seleziona le entità attendibili o Fase 2: aggiungi autorizzazioni seleziona Modifica.
12. (Facoltativo) Per facilitare l'identificazione, l'organizzazione o la ricerca del ruolo, aggiungi i tag come coppie chiave-valore. Per ulteriori informazioni sull'uso dei tag in IAM, consulta [Tag for AWS Identity and Access Management resources](#) nella IAM User Guide.
13. Verificare il ruolo e quindi scegliere Create role (Crea ruolo).

Come utilizzare l'editor di policy JSON per creare una policy

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy).

Se è la prima volta che selezioni Policy, verrà visualizzata la pagina Benvenuto nelle policy gestite. Seleziona Inizia.

3. Nella parte superiore della pagina, scegli Crea policy.
4. Nella sezione Editor di policy, scegli l'opzione JSON.
5. Immettere o incollare un documento di policy JSON. Per dettagli sul linguaggio della policy IAM, consulta la [Documentazione di riferimento delle policy JSON IAM](#).
6. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la [convalida delle policy](#), quindi scegli Next (Successivo).

 Note

È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta [Modifica della struttura delle policy](#) nella Guida per l'utente di IAM.

7. (Facoltativo) Quando crei o modifichi una policy in Console di gestione AWS, puoi generare un modello di policy JSON o YAML che puoi usare nei modelli. CloudFormation

Per fare ciò, nell'editor delle politiche scegli Azioni, quindi scegli Genera modello.

CloudFormation Per saperne di più CloudFormation, consulta i riferimenti ai tipi di [AWS Identity and Access Management risorse](#) nella Guida AWS CloudFormation per l'utente.

8. Una volta terminata l'aggiunta delle autorizzazioni alla policy, scegli Successivo.
9. Nella pagina Rivedi e crea, immettere un valore in Nome policy e Descrizione (facoltativo) per la policy in fase di creazione. Rivedi Autorizzazioni definite in questa policy per visualizzare le autorizzazioni concesse dalla policy.
10. (Facoltativo) Aggiungere metadati alla policy collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'uso dei tag in IAM, consulta [Tag for AWS Identity and Access Management resources](#) nella IAM User Guide.
11. Seleziona Crea policy per salvare la nuova policy.

Per utilizzare l'editor visivo per creare una policy.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy).

Se è la prima volta che selezioni Policy, verrà visualizzata la pagina Benvenuto nelle policy gestite. Seleziona Inizia.

3. Scegli Crea policy.
4. Nella sezione Editor delle politiche, trova la sezione Seleziona un servizio, quindi scegli un Servizio AWS. È possibile utilizzare la casella di ricerca in alto per limitare i risultati nell'elenco di servizi. È possibile selezionare solo un servizio nel blocco di autorizzazione di un editor visivo. Per concedere l'accesso a più di un servizio, aggiungi più blocchi di autorizzazioni selezionando Aggiungi altre autorizzazioni.
5. In Operazioni consentite, scegli le operazioni da aggiungere alla policy. È possibile selezionare operazioni nei modi seguenti:
 - Selezionare la casella di controllo per tutte le azioni.
 - Scegli Aggiungi azioni per inserire il nome di un'azione specifica. È possibile utilizzare un carattere jolly (*) per specificare più azioni.
 - Selezionare uno dei gruppi di livelli di accesso per scegliere tutte le azioni per il livello di accesso, ad esempio Lettura, Scrittura o Elenco.
 - Espandere ciascuno dei gruppi Access level (Livello di accesso) per selezionare singole operazioni.

Come impostazione predefinita, la policy che si sta creando utilizza le operazioni selezionate. Per rifiutare invece le operazioni scelte, selezionare Switch to deny permissions (Passa a rifiuto autorizzazioni). Poiché [IAM rifiuta per impostazione predefinita](#), si consiglia come best practice di sicurezza di consentire le autorizzazioni solo alle operazioni e alle risorse necessarie per un utente. Crea un'istruzione JSON per negare le autorizzazioni solo se desideri sovrascrivere un'autorizzazione consentita separatamente da un'altra dichiarazione o politica. Si consiglia di limitare al minimo il numero di autorizzazioni di rifiuto perché possono aumentare la difficoltà di risoluzione dei problemi relative alle autorizzazioni.

6. Per Risorse, se il servizio e le azioni selezionati nei passaggi precedenti non supportano la scelta di [risorse specifiche](#), tutte le risorse sono consentite e non è possibile modificare questa sezione.

Se si selezionano una o più operazioni che supportano le [autorizzazioni a livello di risorsa](#), l'editor visivo elenca tali risorse. È possibile selezionare Risorse per specificare le risorse per la policy.

È possibile specificare le risorse nei seguenti modi:

- Seleziona Aggiungi ARN per specificare le risorse in base al loro nome della risorsa Amazon (ARN). È possibile utilizzare l'editor ARN visivo o elencare manualmente gli ARN. Per ulteriori informazioni sulla sintassi ARN, consulta [Amazon Resource Names \(ARNs\) nella IAM User Guide](#). Per informazioni sull'utilizzo degli ARN nell'elemento di una policy, consulta [IAM JSON policy elements: Resource](#) in the IAM User Guide.
 - Scegli Qualsiasi in questo account accanto a una risorsa per concedere autorizzazioni a qualsiasi risorsa di quel tipo.
 - Seleziona Tutto per selezionare tutte le risorse per quel servizio.
7. (Facoltativo) Scegli Condizioni di richiesta - opzionale per aggiungere condizioni alla policy che si sta creando. Le condizioni limitano l'effetto di una dichiarazione di policy JSON. Ad esempio, puoi specificare che un utente può eseguire le operazioni sulle risorse solo quando la richiesta dell'utente viene effettuata entro un determinato intervallo di tempo. Puoi anche utilizzare le condizioni di uso comune per limitare se un utente deve essere autenticato utilizzando un dispositivo di autenticazione a più fattori (MFA). In alternativa, è possibile richiedere che la richiesta provenga da un determinato intervallo di indirizzi IP. Per un elenco di tutte le chiavi di contesto che è possibile utilizzare in una condizione di policy, vedi [Azioni, risorse e chiavi di condizione per AWS i servizi](#) nel Service Authorization Reference.

È possibile selezionare le condizioni nei modi seguenti:

- Utilizzare le caselle di controllo per selezionare le condizioni di utilizzo comune.
- Seleziona Aggiungi altra condizione per specificare altre condizioni. Scegliete la chiave di condizione, il qualificatore e l'operatore della condizione, quindi immettete un valore. Per aggiungere più di un valore, seleziona Aggiungi. È possibile considerare i valori come connessi da un OR operatore logico. Una volta terminato, scegli Aggiungi condizione.

Per aggiungere più di una condizione, scegli di nuovo Aggiungi altra condizione. Ripetere come necessario. Ogni condizione si applica solo a questo blocco di autorizzazione di un editor visivo. Tutte le condizioni devono essere vere per il blocco di autorizzazioni per essere considerato una corrispondenza. In altre parole, considerate le condizioni che devono essere collegate da un AND operatore logico.

Per ulteriori informazioni sull'elemento Condition, consulta [IAM JSON policy elements: Condition](#) nella IAM User Guide.

8. Per aggiungere più blocchi di autorizzazioni, seleziona Aggiungi ulteriori autorizzazioni. Per ogni blocco, ripetere le fasi da 2 a 5.

 Note

È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta [Modifica della struttura delle policy](#) nella Guida per l'utente di IAM.

9. (Facoltativo) Quando crei o modifichi una policy in Console di gestione AWS, puoi generare un modello di policy JSON o YAML da utilizzare nei modelli. CloudFormation

Per fare ciò, nell'editor delle politiche scegli Azioni, quindi scegli Genera modello.

CloudFormation Per saperne di più CloudFormation, consulta i riferimenti ai tipi di [AWS Identity and Access Management risorse](#) nella Guida AWS CloudFormation per l'utente.

10. Una volta terminata l'aggiunta delle autorizzazioni alla policy, scegli Successivo.
11. Nella pagina Rivedi e crea, immettere un valore in Nome policy e Descrizione (facoltativo) per la policy in fase di creazione. Rivedi il campo Autorizzazioni definite in questa policy per accertarti di disporre delle autorizzazioni previste.
12. (Facoltativo) Aggiungere metadati alla policy collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'uso dei tag in IAM, consulta [Tag for AWS Identity and Access Management resources](#) nella IAM User Guide.
13. Seleziona Crea policy per salvare la nuova policy.

Per concedere l'accesso programmatico

Gli utenti hanno bisogno dell'accesso programmatico se vogliono interagire con persone AWS esterne a. Console di gestione AWS Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza le credenziali della console come credenziali temporanee per firmare richieste programmatiche a AWS SDK o AWS CLI API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> • Per saperne di più AWS CLI, consulta Login for AWS local development nella Guida per l'utente. AWS Command Line Interface • Per AWS gli SDK, consulta Login for AWS local development nella Guida di riferimento per AWS SDK and Tools.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Usa le credenziali temporanee e per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> • Per saperne di più AWS CLI, consulta Configurazione dell'uso Centro identità AWS IAM nella Guida AWS CLI per l'utente. AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento per AWS SDK e strumenti.
IAM	Usa le credenziali temporanee e per firmare le richieste	Seguendo le istruzioni in Uso delle credenziali temporanee

Quale utente necessita dell'accesso programmatico?	Per	Come
	programmatiche agli SDK o alle API AWS CLI. AWS AWS	con le AWS risorse nella IAM User Guide.
IAM	(Non consigliato) Usa le credenziali a lungo termine per firmare richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> • Per saperne di più AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente. AWS Command Line Interface • Per AWS SDK e strumenti, consulta Autenticare utilizzando credenziali a lungo termine nella Guida di riferimento per SDK e strumenti. AWS • Per le AWS API, consulta Gestire le chiavi di accesso per gli utenti IAM nella IAM User Guide.

Proteggiti dagli aggressori

Per ulteriori informazioni su come proteggersi dagli aggressori quando si concedono autorizzazioni ad altri responsabili del AWS servizio, consulta Condizioni [opzionali per le relazioni di fiducia tra ruoli](#). Aggiungendo determinate condizioni alle tue politiche, puoi contribuire a prevenire un tipo specifico di attacco, noto come attacco sostitutivo confuso, che si verifica se un'entità costringe un'entità con più privilegi a compiere un'azione, ad esempio con l'impersonificazione tra servizi. Per informazioni generali sulle condizioni delle polizze, consulta anche. [Specifica delle condizioni in una policy](#)

Per ulteriori informazioni sull'utilizzo di policy basate sull'identità con AWS Control Tower, consulta [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#). Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta [Identità \(utenti, gruppi e ruoli\)](#) nella Guida per l'utente di IAM.

Resource-based politiche

Anche altri servizi, ad esempio Amazon S3, supportano policy di autorizzazioni basate su risorse. Ad esempio, è possibile associare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. AWS Control Tower non supporta policy basate sulle risorse.

Specifica gli elementi delle policy: azioni, effetti e principi

Puoi configurare e gestire la tua zona di destinazione tramite la console AWS Control Tower o le API https://docs.aws.amazon.com/controltower/latest/APIReference/API_Operations.html della zona di destinazione. Per configurare la tua zona di destinazione, devi essere un utente IAM con autorizzazioni amministrative come definito in una policy IAM.

I seguenti elementi sono i più basilari che puoi identificare in una policy:

- **Risorsa:** in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa. Per ulteriori informazioni, consulta [Risorse e operazioni di AWS Control Tower](#).
- **Operazione:** utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Per informazioni sui tipi di azioni disponibili da eseguire, consulta [Azioni definite da AWS Control Tower](#).
- **Effetto:** l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USare non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- **Principal:** nelle policy basate sull'identità (politiche IAM), l'utente a cui è collegata la policy è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). AWS Control Tower non supporta policy basate sulle risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta [AWS Riferimento alle policy IAM](#) nella Guida per l'utente di IAM.

Specifica delle condizioni in una policy

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della policy IAM per specificare le condizioni in base a cui la policy deve essere applicata. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta la sezione [Condizione](#) nella Guida per l'utente di IAM.

Per esprimere le condizioni, puoi utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per AWS Control Tower. Tuttavia, esistono chiavi AWS di condizione estese che è possibile utilizzare in modo appropriato. Per un elenco completo delle chiavi AWS-wide, consulta [Available Keys for Conditions](#) nella IAM User Guide.

Impedisci l'impersonificazione tra servizi

Nel AWS, l'impersonificazione tra servizi può portare al confuso problema dei vice. Quando un servizio chiama un altro servizio, si verifica l'impersonificazione tra servizi se un servizio manipola un altro servizio per utilizzare le proprie autorizzazioni per agire sulle risorse di un cliente in un modo che non sarebbe altrimenti consentito. Per prevenire questo attacco, AWS fornisce strumenti per aiutarti a proteggere i tuoi dati, in modo che solo i servizi con autorizzazioni legittime possano accedere alle risorse del tuo account.

Ti consigliamo di utilizzare le `aws:SourceAccount` condizioni `aws:SourceArn` and nelle tue policy, per limitare le autorizzazioni che AWS Control Tower concede a un altro servizio per l'accesso alle tue risorse.

- Usalo `aws:SourceArn` se desideri associare una sola risorsa all'accesso tra servizi.
- Usa `aws:SourceAccount` se desideri consentire a qualsiasi risorsa di quell'account di essere associata all'uso tra servizi.
- Se il `aws:SourceArn` valore non contiene l'ID dell'account, ad esempio l'ARN per un bucket Amazon S3, devi utilizzare entrambe le condizioni per limitare le autorizzazioni.
- Se utilizzi entrambe le condizioni e se il `aws:SourceArn` valore contiene l'ID dell'account, il `aws:SourceAccount` valore e l'account nel `aws:SourceArn` valore devono mostrare lo stesso ID account se utilizzati nella stessa dichiarazione politica

Per maggiori informazioni ed esempi, consulta <https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html>.

Utilizzo di policy basate sull'identità (policy IAM) per AWS Control Tower

Questo argomento fornisce esempi di politiche basate sull'identità che dimostrano come un amministratore di account può associare politiche di autorizzazioni alle identità IAM (ovvero utenti, gruppi e ruoli) e quindi concedere le autorizzazioni per eseguire operazioni sulle risorse AWS Control Tower.

Important

Ti consigliamo di esaminare innanzitutto gli argomenti introduttivi che spiegano i concetti e le opzioni di base disponibili per gestire l'accesso alle tue risorse AWS Control Tower. Per ulteriori informazioni, consulta [Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#).

Autorizzazioni necessarie per utilizzare la console AWS Control Tower

AWS Control Tower crea automaticamente tre ruoli quando si configura una zona di atterraggio. Tutti e tre i ruoli sono necessari per consentire l'accesso alla console. AWS Control Tower suddivide le autorizzazioni in tre ruoli come best practice per limitare l'accesso ai set minimi di azioni e risorse.

Tre ruoli richiesti per l'accesso alla zona di atterraggio

- [AWS ControlTowerAdmin ruolo](#)
- [AWS ControlTowerStackSetRole](#)
- [AWSControlTowerCloudTrailRole](#)

Ti consigliamo di limitare l'accesso alle politiche di fiducia dei ruoli per questi ruoli. Per ulteriori informazioni, consulta Condizioni [opzionali per le relazioni di fiducia tra i ruoli](#).

Visualizza il Control Catalog nella console

Per visualizzare le informazioni di controllo nella console AWS Control Tower, devi aggiungere `controlcatalog` autorizzazioni aggiuntive alle tue policy IAM. Queste autorizzazioni sono le seguenti:

- `controlcatalog:GetControl`
- `controlcatalog:ListControls`
- `controlcatalog:ListControlMappings`
- `controlcatalog:ListCommonControls`

Ecco un esempio che mostra le autorizzazioni aggiornate nella policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "controlcatalog:GetControl",
        "controlcatalog:ListControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

È necessario aggiungere queste autorizzazioni perché AWS Control Tower chiama le `controlcatalog` API per recuperare determinati metadati di controllo, quindi le autorizzazioni di AWS Control Tower non sono sufficienti.

Per ulteriori informazioni su come aggiornare le autorizzazioni, consulta [Creare ruoli e assegnare autorizzazioni](https://docs.aws.amazon.com/controltower/latest/userguide/assign-permissions.html). <https://docs.aws.amazon.com/controltower/latest/userguide/assign-permissions.html>

Per ulteriori informazioni sulle azioni `controlcatalog` IAM, consulta [Azioni, risorse e chiavi di condizione per Control Catalog](#).

 Note

Le informazioni di controllo sono disponibili tramite le API <https://docs.aws.amazon.com/controlcatalog/latest/APIReference/Welcome.html> di Control Catalog.

AWS ControlTowerAdmin ruolo

Questo ruolo fornisce ad AWS Control Tower l'accesso all'infrastruttura fondamentale per la manutenzione della zona di atterraggio. Il `AWS ControlTowerAdmin` ruolo richiede una policy gestita allegata e una policy di fiducia dei ruoli per il ruolo IAM. Una politica di fiducia dei ruoli è una politica basata sulle risorse, che specifica quali presidi possono assumere il ruolo.

Ecco un esempio di questa politica di fiducia dei ruoli:

JSON

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

Per creare questo ruolo dalla AWS CLI e inserirlo in un file chiamato `trust.json`, ecco un esempio di comando CLI:

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-role-policy-document file:///trust.json
```

Questo ruolo richiede due policy IAM.

1. Una policy in linea, ad esempio:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeAvailabilityZones",
      "Resource": "*"
    }
  ]
}
```

2. La politica gestita che segue, che è la `AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

`AWS ControlTowerServiceRolePolicy` È una policy AWS gestita che definisce le autorizzazioni per creare e gestire risorse AWS Control Tower, come AWS CloudFormation stackset e istanze di stack, file di AWS CloudTrail log, un aggregatore di configurazione per AWS Control Tower, nonché AWS Organizations account e unità organizzative (OU) governati da AWS Control Tower.

Gli aggiornamenti a questa policy gestita sono riepilogati nella tabella,. [Policy gestite per AWS Control Tower](#)

Per ulteriori informazioni, consultare [AWS ControlTowerServiceRolePolicy](#) la AWS Managed Policy Reference Guide.

Politica di fiducia dei ruoli:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      }
    }
  ]
}
```



```

    ]
  },
  "Action": "sts:AssumeRole"
}
]
}

```

La politica in linea è `AWS ControlTowerAdminPolicy`:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:DescribeAvailabilityZones",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

AWS ControlTowerIdentityCenterManagementPolicy

Questa policy fornisce le autorizzazioni per configurare le risorse IAM Identity Center (iDC) negli account dei membri registrati con AWS Control Tower. Quando si seleziona IAM Identity Center come provider di identità durante la configurazione (o l'aggiornamento) della zona di destinazione in AWS Control Tower, questa policy viene associata al ruolo `AWS ControlTowerAdmin`.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS ControlTowerIdentityCenterManagementPolicy](#) nella Guida di riferimento alle policy gestite da AWS.

AWS ControlTowerStackSetRole

CloudFormation assume questo ruolo per distribuire set di stack negli account creati da AWS Control Tower. Policy inline:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AWSControlTowerExecution"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Policy di trust

JSON

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

AWS ControlTowerCloudTrailRolePolicy

AWS Control Tower CloudTrail lo abilita come best practice e fornisce questo ruolo a. CloudTrail CloudTrail assume questo ruolo per creare e pubblicare CloudTrail i log.

Politica gestita: AWS ControlTowerCloudTrailRolePolicy

Questo ruolo utilizza la policy AWS-managedAWS ControlTowerCloudTrailRolePolicy, che concede le autorizzazioni necessarie per pubblicare CloudTrail i log di controllo su Amazon CloudWatch Logs per conto di AWS Control Tower. Questa policy gestita sostituisce la policy in linea utilizzata in precedenza per questo ruolo, consentendo di AWS aggiornarla senza l'intervento del cliente.

Per ulteriori informazioni, consulta [AWS ControlTowerCloudTrailRolePolicy](#) la AWS Managed Policy Reference Guide.

Gli aggiornamenti a questa policy gestita sono riepilogati nella tabella, [Policy gestite per AWS Control Tower](#).

Note

Prima dell'introduzione della policy gestita, questo ruolo utilizzava una policy in linea con autorizzazioni equivalenti. La policy in linea è stata sostituita dalla policy gestita per consentire aggiornamenti senza interruzioni.

Politica in linea precedente (per riferimento):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "logs:CreateLogStream",
      "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
      "Effect": "Allow"
    },
    {
      "Action": "logs:PutLogEvents",
      "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
      "Effect": "Allow"
    }
  ]
}
```

```
}
```

Policy di trust

JSON

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

AWS ControlTowerBlueprintAccess requisiti di ruolo

AWS Control Tower richiede la creazione del AWS ControlTowerBlueprintAccess ruolo nell'account hub blueprint designato, all'interno della stessa organizzazione.

Role name (Nome ruolo)

Il nome del ruolo deve essere AWS ControlTowerBlueprintAccess.

Politica di fiducia dei ruoli

Il ruolo deve essere impostato in modo da fidarsi dei seguenti principi:

- Il principale che utilizza AWS Control Tower nell'account di gestione.
- Il AWS ControlTowerAdmin ruolo nell'account di gestione.

L'esempio seguente mostra una politica di fiducia con privilegi minimi. Quando crei la tua policy, sostituisci il termine *YourManagementAccountId* con l'ID account effettivo del tuo account di gestione AWS Control Tower e sostituisci il termine *YourControlTowerUserRole* con l'identificatore del ruolo IAM per il tuo account di gestione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/service-role/AWSControlTowerAdmin",
          "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

Autorizzazioni relative ai ruoli

È necessario allegare la policy gestita `AWSServiceCatalogAdminFullAccess` al ruolo.

AWSServiceRoleForAWSControlTower

Questo ruolo fornisce ad AWS Control Tower l'accesso all'account Log Archive, all'account Audit e agli account dei membri, per operazioni fondamentali per il mantenimento della zona di atterraggio, come la notifica della dispersione di risorse.

Il `AWS ServiceRoleFor AWS ControlTower` ruolo richiede una policy gestita allegata e una policy di fiducia dei ruoli per il ruolo IAM.

Politica gestita per questo ruolo: `AWS ControlTowerAccountServiceRolePolicy`

Politica di fiducia dei ruoli:

JSON

```
{
```

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

AWS ControlTowerAccountServiceRolePolicy

Questa policy AWS gestita consente ad AWS Control Tower di chiamare AWS servizi che forniscono la configurazione automatica degli account e la governance centralizzata per tuo conto.

La policy contiene le autorizzazioni minime per AWS Control Tower per implementare l'inoltro dei AWS Security Hub CSPM risultati per le risorse gestite dai controlli CSPM di Security Hub che fanno parte dello Service-managed standard Security Hub CSPM: AWS Control Tower e impedisce le modifiche che limitano la capacità di gestire gli account dei clienti. Fa parte del processo di rilevamento della AWS Security Hub CSPM deriva in background che non viene avviato direttamente da un cliente.

La policy fornisce le autorizzazioni per creare EventBridge regole Amazon, in particolare per i controlli CSPM di Security Hub, in ciascun account membro e queste regole devono specificarne una precisa. EventPattern Inoltre, una regola può funzionare solo sulle regole gestite dal nostro responsabile del servizio.

Responsabile del servizio: `controltower.amazonaws.com`

Per ulteriori informazioni, consulta [AWS ControlTowerAccountServiceRolePolicy](#) la AWS Managed Policy Reference Guide.

Gli aggiornamenti a questa policy gestita sono riepilogati nella tabella, [Policy gestite per AWS Control Tower](#).

Policy gestite per AWS Control Tower

AWS risolve molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da AWS. Le policy gestite concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non

dover cercare quali sono le autorizzazioni richieste. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento a una policy esistente	AWS Control Tower ha spostato l'cloudformation:BatchDescribeTypeConfiguration autorizzazione dall'istruzione resource-scoped hooks a una nuova dichiarazione conResource: "*", perché non CloudFormation supporta le autorizzazioni a livello di risorsa per questa API.	19 maggio 2026
AWS ControlTowerAccountServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate all'API del AWS CloudFormation servizio BatchDescribeTypeConfigurations per un miglioramento interno degli hook collegati ai servizi.	19 maggio 2026
AWS ControlTowerAccountServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiornato una policy esistente per migliorare la precisione di convalida delle condizioni delle EventBridge regole di Amazon. L'aggiornamento sposta la events:detail-type condizione da StringEquals a	30 dicembre 2025

Modifica	Descrizione	Data
	<p>ForAllValues:StringEquals per un migliore controllo della corrispondenza dei modelli di eventi mantenendo le stesse autorizzazioni funzionali.</p>	
<p>AWS ControlTowerAccountServiceRolePolicy: aggiornamento di una policy esistente</p>	<p>AWS Control Tower ha aggiunto una nuova policy che estende le seguenti autorizzazioni:</p> <ul style="list-style-type: none"> • AWS Config autorizzazioni per creare, etichettare, eliminare, gestire e leggere un aggregatore di configurazione collegato ai servizi • AWS Config autorizzazioni per descrivere tutti gli aggregatori di configurazione • AWS Organizations autorizzazione a elencare gli amministratori delegati per AWS Config • AWS Organizations autorizzazione a descrivere l'organizzazione • CloudFormation autorizzazioni per gestire gli hook collegati ai servizi 	10 novembre 2025

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy — Politica gestita aggiornata	<p>AWS Control Tower ha aggiornato il modello di risorse Amazon CloudWatch Logs in AWS ControlTowerServiceRolePolicy per supportare l'AWS CloudTrail l'integrazione opzionale di Landing Zone 4.0. Lo schema è cambiato da <code>aws-controltower/CloudTrailLogs:*</code> a <code>aws-controltower/CloudTrailLogs:*</code>, aggiungendo dopo un carattere jolly <code>CloudTrailLogs</code> per consentire la gestione di gruppi di log con qualsiasi suffisso.</p> <p>Questo aggiornamento abilita AWS CloudTrail l'integrazione opzionale di Landing Zone 4.0, che consente ai clienti di abilitare e disabilitare AWS CloudTrail l'integrazione più volte. Ogni volta che l'integrazione viene abilitata, i gruppi di CloudWatch log di Amazon Logs vengono ricreati con suffissi univoci per evitare conflitti di denominazione. L'aggiornamento è retrocompatibile con le distribuzioni esistenti.</p>	31 ottobre 2025

Modifica	Descrizione	Data
AWS ControlTowerCloudTrailRolePolicy — Nuova politica gestita	<p>AWS Control Tower ha introdotto la policy AWS ControlTowerCloudTrailRolePolicy gestita, che consente di CloudTrail creare flussi di log e pubblicare eventi di log nei gruppi di log di Control Tower-managed Amazon CloudWatch Logs.</p> <p>Questa policy gestita sostituisce la policy in linea precedentemente utilizzata da AWS ControlTowerCloudTrailRole, consentendo di AWS aggiornarla senza l'intervento del cliente. La policy ha lo scopo di registrare i gruppi con nomi corrispondenti al modello. aws-controltower/CloudTrail Logs*</p>	31 ottobre 2025

Modifica	Descrizione	Data
AWS ControlTowerIdentityCenterManagementPolicy — Una nuova politica	<p>AWS Control Tower ha aggiunto una nuova policy che consente ai clienti di configurare le risorse IAM Identity Center negli account registrati in AWS Control Tower e consente ad AWS Control Tower di porre rimedio ad alcuni tipi di deviazioni e durante la registrazione automatica degli account.</p> <p>Questa modifica è necessaria per consentire ai clienti di configurare IAM Identity Center in AWS Control Tower e per consentire ad AWS Control Tower di correggere la deriva delle iscrizioni automatiche.</p>	10 ottobre 2025
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove CloudFormation autorizzazioni che consentono ad AWS Control Tower di interrogare e distribuire risorse di stack set negli account dei membri durante la registrazione automatica degli account in AWS Control Tower.	10 ottobre 2025

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di abilitare e disabilitare le regole collegate ai servizi AWS Config .</p> <p>Questa modifica è necessari a per consentire ai clienti di gestire i controlli distribuiti dalle regole di configurazione.</p>	5 giugno 2025
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate alle API del AWS CloudFormation servizio e ActivateType DeactivateType attivarle. SetTypeConfiguration AWS::ControlTower types</p> <p>Questa modifica consente ai clienti di fornire controlli proattivi senza l'implementazione di tipi di Hook privati. CloudFormation</p>	10 dicembre 2024

Modifica	Descrizione	Data
AWS ControlTowerAccountServiceRolePolicy — Una nuova politica	<p>AWS Control Tower ha aggiunto un nuovo ruolo collegato ai servizi che consente ad AWS Control Tower di creare e gestire regole per gli eventi e, in base a tali regole, di gestire il rilevamento delle deviazioni per i controlli correlati a Security Hub CSPM.</p> <p>Questa modifica è necessaria per consentire ai clienti di visualizzare le risorse derivate nella console, quando tali risorse sono correlate ai controlli CSPM di Security Hub che fanno parte dello standard Security Hub CSPM: AWS Control Tower. Service-managed</p>	22 maggio 2023

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate al e le <code>EnableRegion</code> <code>GetRegionOptStatus</code> API implementate dal servizio AWS Account Management per rendere Regioni AWS disponibile l'opt-in per gli account dei clienti nella zona di destinazione (account di gestione, account di archiviazione dei log, account di controllo, account membri dell'unità organizzativa). <code>ListRegions</code></p> <p>Questa modifica è necessaria affinché i clienti possano avere la possibilità di espandere la governance delle regioni da parte di AWS Control Tower nelle regioni opt-in.</p>	6 aprile 2023

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di assumere il <code>AWSControlTowerBlueprintAccess</code> ruolo nell'account blueprint (hub), che è un account dedicato in un'organizzazione, contenente blueprint predefiniti archiviati in uno o più prodotti del Service Catalog. AWS Control Tower si assume il <code>AWSControlTowerBlueprintAccess</code> ruolo di eseguire tre attività: creare un portafoglio di Service Catalog, aggiungere il prodotto blueprint richiesto e condividere il portafoglio con un account membro richiesto al momento del provisioning dell'account.</p> <p>Questa modifica è necessaria affinché i clienti possano fornire account personalizzati tramite AWS Control Tower Account Factory.</p>	28 ottobre 2022

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di impostare AWS CloudTrail percorsi a livello di organizzazione, a partire dalla versione 3.0 della zona di destinazione.</p> <p>La CloudTrail funzionalità basata sull'organizzazione richiede che i clienti abbiano un accesso affidabile abilitato per il CloudTrail servizio e l'utente o il ruolo IAM deve disporre dell'autorizzazione e per creare un percorso a livello di organizzazione nell'account di gestione.</p>	20 giugno 2022

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	<p>AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di utilizzare la crittografia delle chiavi KMS.</p> <p>La funzionalità KMS consente ai clienti di fornire la propria chiave KMS per crittografare i propri log. CloudTrail I clienti possono inoltre modificar e la chiave KMS durante l'aggiornamento o la riparazio ne della zona di atterraggio. Quando si aggiorna la chiave KMS, sono necessarie AWS CloudFormation le autorizza zioni per chiamare l'API. AWS CloudTrail PutEventS elector La modifica alla policy serve a consentire al AWS ControlTowerAdmin ruolo di chiamare l' AWS CloudTrail PutEventS elector API.</p>	28 luglio 2021
AWS Control Tower ha iniziato a tracciare le modifiche	AWS Control Tower ha iniziato a tracciare le modifiche relative alle politiche AWS gestite.	27 maggio 2021

Sicurezza in AWS Control Tower

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [modello di responsabilità condivisa](#) descrive questo 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. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformità AWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano ad AWS Control Tower, consulta [AWS Services in Scope by Compliance Program](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata dai AWS servizi che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, nonché le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AWS Control Tower. I seguenti argomenti mostrano come configurare AWS Control Tower per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse AWS Control Tower.

Protezione dei dati in AWS Control Tower

Il modello di [responsabilità AWS condivisa \(modello di \)](#) si applica alla protezione dei dati in AWS Control Tower. 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, consulta [Domande frequenti sulla privacy dei dati](#) . Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il [Centro generale sulla protezione dei dati \(GDPR\)](#).

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare singoli utenti con Centro identità AWS IAM o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Sugeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. 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 con AWS Control Tower o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI 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 si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Note

La registrazione delle attività degli utenti con AWS CloudTrail viene gestita automaticamente in AWS Control Tower quando configuri la landing zone.

Per ulteriori informazioni sulla protezione dei dati, consulta il post del blog [AWS Modello di responsabilità condivisa e GDPR](#) su AWS Security Blog. AWS Control Tower offre le seguenti opzioni che puoi utilizzare per proteggere i contenuti presenti nella tua landing zone:

Argomenti

- [Crittografia dei dati inattivi](#)
- [Crittografia in transito](#)

- [Limitazione dell'accesso ai contenuti](#)

Crittografia dei dati inattivi

AWS Control Tower utilizza bucket Amazon S3 e database Amazon DynamoDB crittografati a riposo utilizzando Amazon S3-Managed Keys () a SSE-S3 supporto della landing zone. Questa crittografia è configurata di default quando configuri la landing zone. Facoltativamente, puoi configurare la tua landing zone per crittografare le risorse con chiavi di crittografia KMS. Puoi anche stabilire la crittografia a riposo per i servizi che utilizzi nella tua landing zone per i servizi che la supportano. Per ulteriori informazioni, consulta il capitolo sulla sicurezza della documentazione online del servizio.

Crittografia in transito

AWS Control Tower utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito a supporto della landing zone. Inoltre, l'accesso ad AWS Control Tower richiede l'utilizzo della console, a cui è possibile accedere solo tramite un endpoint HTTPS. Questa crittografia è configurata di default quando configuri la landing zone.

Limitazione dell'accesso ai contenuti

Come best practice, è consigliabile limitare l'accesso ai sottoinsiemi di utenti appropriati. Con AWS Control Tower, puoi farlo assicurandoti che gli amministratori del cloud centrale e gli utenti finali dispongano delle autorizzazioni IAM corrette o, nel caso degli utenti di IAM Identity Center, che siano nei gruppi corretti.

- Per ulteriori informazioni sui ruoli e le policy per le entità IAM, consulta la [IAM User Guide](#).
- Per ulteriori informazioni sui gruppi IAM Identity Center creati quando configuri la landing zone, consulta [Gruppi IAM Identity Center per AWS Control Tower](#).

Convalida della conformità per AWS Control Tower

AWS Control Tower è un servizio ben progettato che può aiutare la tua organizzazione a soddisfare le tue esigenze di conformità con controlli e best practice. Inoltre, revisori di terze parti valutano la sicurezza e la conformità di una serie di servizi che puoi utilizzare nella tua landing zone come parte di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformità](#). Per informazioni generali, consulta [Programmi di conformità di AWS](#).

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricare i report in AWS Artifact](#) nella AWS Artifact Guida per l'utente.

La tua responsabilità di conformità quando usi AWS Control Tower è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- [Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services](#): questo white paper descrive come le aziende possono utilizzare per creare applicazioni. AWS HIPAA-compliant
- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua area geografica.
- [AWS Config](#)— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub CSPM](#)— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in AWS Control Tower

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 tramite reti a bassa latenza, ad alto throughput e altamente ridondanti. Le zone di disponibilità consentono di progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta [In che modo AWS Le regioni funzionano con AWS Control Tower](#).

La tua regione d'origine è definita come la AWS regione in cui è stata configurata la tua landing zone.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta [Infrastruttura AWS globale](#).

Sicurezza dell'infrastruttura in AWS Control Tower

AWS Control Tower è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper [Amazon Web Services: Overview of Security Processes](#).

Utilizzi chiamate API AWS pubblicate per accedere ai AWS servizi e alle risorse all'interno della tua landing zone attraverso la rete. Richiediamo Transport Layer Security (TLS) 1.2 e consigliamo Transport Layer Security (TLS) 1.3 o versione successiva. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman 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. In alternativa è possibile utilizzare [Servizio di token di sicurezza AWS](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi configurare gruppi di sicurezza per fornire ulteriore sicurezza dell'infrastruttura di rete per i carichi di lavoro delle landing zone di AWS Control Tower. Per ulteriori informazioni, consulta [Procedura dettagliata: configura gruppi di sicurezza in AWS Control Tower con AWS Firewall Manager](#).

Registrazione e monitoraggio in AWS Control Tower

Il monitoraggio consente di pianificare e rispondere a potenziali incidenti. I risultati delle attività di monitoraggio vengono archiviati in file di registro. Pertanto, la registrazione e il monitoraggio sono concetti strettamente correlati e sono una parte importante della natura ben architettata di AWS Control Tower.

Quando configuri la landing zone, uno degli account condivisi creati è l'account di archiviazione dei log. È dedicato alla raccolta centralizzata di tutti i registri, compresi i registri di tutti gli account condivisi e dei membri. I file di log vengono archiviati in un bucket Amazon S3. Questi file di log consentono agli amministratori e ai revisori di esaminare le operazioni e gli eventi che si sono verificati.

Come best practice, è consigliabile raccogliere i dati di monitoraggio da tutte le parti della AWS configurazione nei log, in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. AWS fornisce diversi strumenti per monitorare le risorse e le attività nella landing zone.

Ad esempio, lo stato dei comandi viene monitorato costantemente. Puoi vedere il loro stato a colpo d'occhio nella console AWS Control Tower o in modo programmatico tramite [le API AWS Control Tower](#). Inoltre, lo stato e lo stato degli account che hai fornito in Account Factory vengono monitorati costantemente.

Visualizza le azioni registrate dalla pagina Attività

Nella console AWS Control Tower, la pagina Attività fornisce una panoramica delle azioni dell'account di gestione AWS Control Tower. Per accedere alla pagina delle attività di AWS Control Tower, seleziona Activities dalla barra di navigazione a sinistra.

Le attività mostrate nella pagina Attività sono le stesse riportate nel registro degli AWS CloudTrail eventi per AWS Control Tower, ma sono mostrate in formato tabellare. Per ulteriori informazioni su un'attività specifica, selezionare l'attività dalla tabella e quindi scegliere View details (Visualizza dettagli).

Puoi visualizzare le azioni e gli eventi degli account dei membri nei file di archivio dei log.

Le seguenti sezioni descrivono il monitoraggio e la registrazione in AWS Control Tower con maggiori dettagli:

Argomenti

- [Strumenti integrati per il monitoraggio](#)
- [Registrazione delle azioni di AWS Control Tower con AWS CloudTrail](#)
- [Eventi del ciclo di vita in AWS Control Tower](#)
- [Utilizzo AWS Notifiche utente con AWS Control Tower](#)

Informazioni sulla registrazione in AWS Control Tower

AWS Control Tower registra automaticamente le azioni e gli eventi, attraverso la sua integrazione con AWS CloudTrail e AWS Config, e li registra in CloudWatch. Tutte le azioni vengono registrate, incluse le azioni dall'account di gestione AWS Control Tower e dagli account dei membri dell'organizzazione. Le azioni e gli eventi dell'account di gestione sono visualizzabili nella pagina Attività della console. È possibile visualizzare le azioni e gli eventi dell'account membro nei file di archivio dei registri.

Organization-level sentieri

AWS Control Tower imposta un nuovo CloudTrail percorso quando configuri una landing zone. È un percorso a livello di organizzazione, il che significa che registra tutti gli eventi per l'account di gestione e tutti gli account dei membri dell'organizzazione. Questa funzionalità si basa su un accesso affidabile per concedere all'account di gestione le autorizzazioni per creare un percorso su ogni account membro.

Per ulteriori informazioni su AWS Control Tower e sugli itinerari CloudTrail organizzativi, consulta [Creazione di un percorso per un'organizzazione](#).

Note

Nelle versioni di AWS Control Tower precedenti alla versione 3.0 della landing zone, AWS Control Tower creava una traccia degli account dei membri in ogni account. Quando esegui l'aggiornamento alla versione 3.0, il CloudTrail percorso diventa un percorso organizzativo. Per le migliori pratiche quando ci si sposta da un percorso all'altro, consulta [le migliori pratiche per la modifica dei percorsi](#) nella Guida per l'utente CloudTrail.

Quando registri un account in AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso dell'organizzazione AWS Control Tower. Se disponi già di una distribuzione di un CloudTrail

trail in quell'account, potresti riscontrare addebiti duplicati a meno che non elimini il trail esistente per l'account prima di registrarlo in AWS Control Tower.

Note

Quando esegui l'aggiornamento alla versione 3.0 della landing zone, AWS Control Tower elimina i trail a livello di account (creati da AWS Control Tower) negli account registrati per tuo conto. I tuoi file di log esistenti a livello di account vengono conservati nel loro bucket Amazon S3.

Policy sui bucket di Amazon S3 per la registrazione

In AWS Control Tower, AWS e i servizi hanno accesso alle tue risorse solo quando la richiesta proviene dalla tua organizzazione o unità organizzativa (OU). È necessario soddisfare una `aws:SourceOrgID` condizione per qualsiasi autorizzazione di scrittura.

Puoi utilizzare la chiave di `aws:SourceOrgID` condizione e impostare il valore dell'ID della tua organizzazione nell'elemento condition della tua policy sui bucket di Amazon S3. Questa condizione garantisce che solo gli account all'interno dell'organizzazione possano scrivere log nel bucket Amazon S3. Impedisce agli account esterni all'organizzazione di scrivere log nel bucket Amazon S3 di AWS Control Tower.

Per ulteriori informazioni su questa chiave di condizione, consulta [IAM global condition context keys](#). Per un post sul blog sui controlli scalabili, consulta [Use scalable controls for AWS services access your resources](#).

Questa politica non influisce sulla funzionalità dei carichi di lavoro esistenti.

Landing zone versione 3.3 e precedenti

Nella versione 3.3 e precedenti della landing zone, AWS Control Tower distribuisce un singolo bucket Amazon S3 nell'account di archiviazione dei log che archivia sia i log che quelli. AWS CloudTrail AWS Config La bucket policy è mostrata nell'esempio seguente.

```
S3AuditBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref S3AuditBucket
    PolicyDocument:
```

Version: 2012-10-17

Statement:

- Sid: AllowSSLRequestsOnly
 - Effect: Deny
 - Principal: '*'
 - Action: s3:*
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${S3AuditBucket}"
 - !Sub "arn:\${AWS::Partition}:s3:::\${S3AuditBucket}/*"
 - Condition:
 - Bool:
 - aws:SecureTransport: false
- Sid: AWSS3BucketPermissionsCheck
 - Effect: Allow
 - Principal:
 - Service:
 - cloudtrail.amazonaws.com
 - config.amazonaws.com
 - Action: s3:GetBucketAcl
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${S3AuditBucket}"
- Sid: AWSConfigBucketExistenceCheck
 - Effect: Allow
 - Principal:
 - Service:
 - cloudtrail.amazonaws.com
 - config.amazonaws.com
 - Action: s3:ListBucket
 - Resource:
 - !Sub "arn:\${AWS::Partition}:s3:::\${S3AuditBucket}"
- Sid: AWSS3BucketDeliveryForConfig
 - Effect: Allow
 - Principal:
 - Service:
 - config.amazonaws.com
 - Action: s3:PutObject
 - Resource:
 - Fn::Join:
 - ""
 - - !Sub "arn:\${AWS::Partition}:s3:::"
 - !Ref "S3AuditBucket"
 - !Sub "\${AWSLogsS3KeyPrefix}/AWSLogs/*/*"

Condition:

```

    StringEquals:
      aws:SourceOrgID: !Ref OrganizationId
  - Sid: AWSBucketDeliveryForOrganizationTrail
    Effect: Allow
    Principal:
      Service:
        - cloudtrail.amazonaws.com
    Action: s3:PutObject
    Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
      [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
        ${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
        ${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
      [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
        ${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
    Condition:
      StringEquals:
        aws:SourceOrgID: !Ref OrganizationId

```

Landing zone versione 4.0 e successive

Nella versione 4.0 e successive della landing zone, AWS Config AWS CloudTrail utilizza bucket Amazon S3 dedicati separati anziché un bucket condiviso. Il bucket Amazon S3 per AWS Config i log si trova nell'account di AWS Config integrazione (in precedenza account Audit). Il bucket Amazon S3 per AWS CloudTrail i log si trova nell'account AWS CloudTrail amministratore (in precedenza account Log Archive). Per ulteriori informazioni, consulta [Aggiornamenti di AWS Config](#).

AWS CloudTrail politica bucket (AWS CloudTrail account amministratore)

L'esempio seguente mostra la policy del AWS CloudTrail bucket implementata nell' AWS CloudTrail account amministratore:

```

S3AuditBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref S3AuditBucket
    PolicyDocument:
      Version: 2012-10-17
      Statement:
        - Sid: AllowSSLRequestsOnly
          Effect: Deny
          Principal: '*'
          Action: s3:*

```

```

Resource:
  - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
  - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
Condition:
  Bool:
    aws:SecureTransport: false
- Sid: AWSS3BucketPermissionsCheck
  Effect: Allow
  Principal:
    Service:
      - cloudtrail.amazonaws.com
  Action: s3:GetBucketAcl
  Resource:
    - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
- Sid: AWSConfigBucketExistenceCheck
  Effect: Allow
  Principal:
    Service:
      - cloudtrail.amazonaws.com
  Action: s3:ListBucket
  Resource:
    - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
- Sid: AWSS3BucketDeliveryForOrganizationTrail
  Effect: Allow
  Principal:
    Service:
      - cloudtrail.amazonaws.com
  Action: s3:PutObject
  Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
    [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
    ${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
    ${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
    [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
    ${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
  Condition:
    StringEquals:
      aws:SourceOrgID: !Ref OrganizationId

```

AWS Config politica bucket (AWS Config account di integrazione)

L'esempio seguente mostra la policy AWS Config bucket implementata nell'account di AWS Config integrazione:

```
ConfigS3BucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref ConfigS3Bucket
    PolicyDocument:
      Version: 2012-10-17
      Statement:
        - Sid: AllowSSLRequestsOnly
          Effect: Deny
          Principal: '*'
          Action: s3:*
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
            - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/*"
          Condition:
            Bool:
              aws:SecureTransport: false
        - Sid: AWSConfigBucketPermissionsCheck
          Effect: Allow
          Principal:
            Service:
              - config.amazonaws.com
          Action: s3:GetBucketAcl
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
        - Sid: AWSConfigBucketExistenceCheck
          Effect: Allow
          Principal:
            Service:
              - config.amazonaws.com
          Action: s3:ListBucket
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
        - Sid: AWSConfigBucketDelivery
          Effect: Allow
          Principal:
            Service:
              - config.amazonaws.com
          Action: s3:PutObject
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/${ConfigS3KeyPrefix}/AWSLogs/*/*"
```

Condition:

```
StringEquals:  
aws:SourceOrgID: !Ref OrganizationId
```

Strumenti integrati per il monitoraggio

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Control Tower e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare AWS Control Tower, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. È possibile raccogliere e tenere traccia dei parametri, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- Amazon EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge abilita l'elaborazione automatizzata basata sugli eventi, poiché puoi scrivere regole che controllano determinati eventi e attivano azioni automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni, consulta la [Amazon CloudWatch Events User Guide](#).
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre CloudTrail fonti. CloudWatch Logs possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate.

Suggerimento: è possibile visualizzare e interrogare le CloudTrail attività su un account tramite CloudWatch Logs and CloudWatch Logs Insights. Questa attività include gli eventi del ciclo di vita di AWS Control Tower. CloudWatch Logs Insights ti consentono di eseguire query più granulari e precise di quelle che normalmente saresti in grado di eseguire utilizzando CloudTrail

Per ulteriori informazioni, consulta [Registrazione delle azioni di AWS Control Tower con AWS CloudTrail](#).

Registrazione delle azioni di AWS Control Tower con AWS CloudTrail

AWS Control Tower è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in AWS Control Tower. CloudTrail acquisisce le azioni per AWS Control Tower come eventi. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per AWS Control Tower.

Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad AWS Control Tower, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, incluso come configurarlo e abilitarlo, consulta la Guida per [l'AWS CloudTrail utente](#).

Informazioni su AWS Control Tower in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di eventi supportata in AWS Control Tower, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Note

Nelle versioni di AWS Control Tower precedenti alla versione 3.0 della zona di destinazione, AWS Control Tower ha creato un percorso di account per i membri. Quando esegui l'aggiornamento alla versione 3.0, il CloudTrail percorso viene aggiornato per diventare un percorso organizzativo. Per le migliori pratiche per gli spostamenti tra i percorsi, consulta [Creazione di un percorso organizzativo](#) nella Guida per l' CloudTrail utente.

Consigliato: creare un percorso

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per AWS Control Tower, crea un percorso. Un percorso 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 AWS . Il percorso registra gli eventi provenienti da tutte le regioni della AWS partizione e invia i file di registro al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un trail](#)
- [Preparati a creare un percorso](#)
- [Gestione dei CloudTrail costi](#)
- [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](#)

AWS Control Tower registra le seguenti azioni come eventi nei file di CloudTrail registro:

API pubbliche

- Per un elenco completo delle API pubbliche di AWS Control Tower e dettagli su ciascuna di esse, consulta [The AWS Control Tower API Reference](#). Le chiamate a queste API pubbliche vengono registrate da. AWS CloudTrail

Altre API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig

- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.
- Se la richiesta è stata rifiutata in quanto accesso negato o elaborata correttamente.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Esempio: voci del file di registro di AWS Control Tower

Un trail è una configurazione che consente la distribuzione di eventi come file di log a un bucket Amazon S3 specificato. CloudTrail i file di log contengono una o più voci di registro. Un evento

rappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail gli eventi non vengono visualizzati in un ordine specifico nei file di registro.

L'esempio seguente mostra una voce di CloudTrail registro che mostra la struttura di una tipica voce di file di registro per un evento SetupLandingZone AWS Control Tower, incluso un record dell'identità dell'utente che ha avviato l'azione.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE::assumed-role/AWSControlTowerTestAdmin/backend-test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

Monitora le modifiche alle risorse con AWS Config

AWS Control Tower è abilitato AWS Config su tutti gli account registrati, in modo da monitorare la conformità attraverso controlli investigativi, registrare le modifiche alle risorse e fornire i log delle modifiche delle risorse a un account centralizzato. AWS Control Tower centralizza questi AWS Config dati in modo da poter esaminare le modifiche alla configurazione delle risorse di tutti gli account registrati in un unico posto, il che ti aiuta a controllare il tuo ambiente e dimostrare la conformità.

Se la versione della tua landing zone è precedente alla 3.0: per gli account registrati, AWS Config registra tutte le modifiche alle risorse, per tutte le regioni in cui opera l'account. Ogni modifica è modellata come un elemento di configurazione (CI), che contiene informazioni come l'identificatore della risorsa, la regione, la data di registrazione di ogni modifica e se la modifica si riferisce a una risorsa nota o scoperta di recente.

Se la versione della tua landing zone è 3.0 o successiva: AWS Control Tower limita la registrazione per risorse globali, come utenti, gruppi, ruoli e policy gestite dai clienti IAM, solo alla tua regione di origine. Le copie delle modifiche globali alle risorse non vengono archiviate in tutte le regioni. Questa limitazione della registrazione delle risorse è conforme [alle AWS Config migliori pratiche](#). Un [elenco completo delle risorse globali](#) è disponibile nella AWS Config documentazione.

- Per ulteriori informazioni AWS Config, consulta [How AWS Config works](#).
- Per un elenco delle risorse che AWS Config possono supportare, consulta [Tipi di risorse supportati](#).
- Per ulteriori informazioni su come personalizzare il monitoraggio delle risorse nell'ambiente AWS Control Tower, consulta il post del blog intitolato [Personalizza il monitoraggio AWS Config delle risorse in AWS Control Tower](#).

AWS Control Tower configura un canale di AWS Config distribuzione in ogni account registrato. Il canale di distribuzione invia le modifiche registrate a un account centralizzato, dove le AWS Config archivia in un bucket Amazon Simple Storage Service. Il nome e la posizione del bucket Amazon S3 dipendono dalla versione della landing zone in uso:

- Per la versione 3.3 o precedente della landing zone, i log vengono archiviati nel bucket `aws-controltower-logs-*` Amazon S3 nell'account di archiviazione dei log.
- Per la versione 4.0 o successiva della landing zone, i log vengono archiviati nel bucket `aws-controltower-config-logs-*` Amazon S3 AWS Config nell'account di integrazione (precedentemente noto come account Audit). Per ulteriori informazioni, consulta [Aggiornamenti di AWS Config](#).

Manage (Gestione) AWS Config costi in AWS Control Tower

Questa sezione descrive come AWS Config registrare e fatturare le modifiche alle risorse nei tuoi account AWS Control Tower. Queste informazioni possono aiutarti a capire come gestire i costi associati a AWS Config, quando utilizzi AWS Control Tower. AWS Control Tower non comporta costi aggiuntivi.

Note

Se la versione della tua landing zone è 3.0 o successiva: AWS Control Tower limita AWS Config la registrazione per risorse globali, come utenti, gruppi, ruoli e policy gestite dai clienti IAM, solo alla tua regione di origine. Pertanto, alcune delle informazioni contenute in questa sezione potrebbero non essere applicabili alla tua landing zone.

AWS Config è progettato per registrare ogni modifica apportata a ciascuna risorsa, in ogni regione in cui opera un account, come elemento di configurazione (CI). AWS Config ti fattura per ogni elemento di configurazione che genera.

Come funziona AWS Config

AWS Config registra le risorse in ogni regione, separatamente. Alcune risorse globali, come i ruoli IAM, vengono registrate una volta per regione. Ad esempio, se crei un nuovo ruolo IAM in un account registrato che opera in cinque regioni, AWS Config genera cinque CI, uno per ogni regione. Altre risorse globali, come le zone ospitate da Route 53, vengono registrate una sola volta in tutte le regioni. Ad esempio, se crei una nuova zona ospitata su Route 53 in un account registrato, AWS

Config genera un CI, indipendentemente dal numero di regioni selezionate per quell'account. Per un elenco che ti aiuti a distinguere questi tipi di risorse, consulta [La stessa risorsa viene registrata più volte](#).

Note

Quando AWS Control Tower funziona con AWS Config, una regione può essere governata da AWS Control Tower o non governata e registrare AWS Config comunque le modifiche se l'account opera in quella regione.

AWS Config rileva due tipi di relazioni nelle risorse

AWS Config fa una distinzione tra relazioni dirette e indirette tra le risorse. Se una risorsa viene restituita nella chiamata API Descrivi di un'altra risorsa, tali risorse vengono registrate come relazione diretta. Quando si modifica una risorsa in relazione diretta con un'altra risorsa, AWS Config non crea un CI per entrambe le risorse.

Ad esempio, se crei un'istanza Amazon EC2 e l'API richiede la creazione di un'interfaccia di rete, AWS Config considera che l'istanza Amazon EC2 abbia una relazione diretta con l'interfaccia di rete. Di conseguenza, AWS Config genera un solo CI.

AWS Config registra le modifiche separate per le relazioni tra risorse che sono relazioni indirette. Ad esempio, AWS Config genera due CI se crei un gruppo di sicurezza e aggiungi un'istanza Amazon EC2 associata che fa parte del gruppo di sicurezza.

Per ulteriori informazioni sulle relazioni dirette e indirette, consulta [Cos'è una relazione diretta e indiretta rispetto a una risorsa?](#)

È possibile trovare [un elenco delle relazioni tra le risorse](#) nella AWS Config documentazione.

Visualizza il AWS Config dati del registratore sugli account registrati

AWS Config è integrato in CloudWatch modo da poter visualizzare gli IC in AWS Config una dashboard. Per ulteriori informazioni, consulta il post del blog intitolato [AWS Config support Amazon CloudWatch metrics](#).

A livello di programmazione, per visualizzare AWS Config i dati, puoi utilizzare la AWS CLI o utilizzare altri strumenti. AWS

Interroga il AWS Config dati del registratore su una risorsa specifica

È possibile utilizzare la AWS CLI per recuperare un elenco delle modifiche più recenti per una risorsa.

Comando di cronologia delle risorse:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Per ulteriori informazioni, consulta [la documentazione dell'API per get-config-history](#).

Visualizzare AWS Config dati con Quick

Puoi visualizzare e interrogare le risorse registrate da AWS Config tutta l'organizzazione. Per ulteriori informazioni, consulta [Config Resource Compliance Dashboard](#) e [Visualizzazione dei dati con AWS Config Amazon Athena](#) e Quick.

Risoluzione dei problemi AWS Config in AWS Control Tower

Questa sezione fornisce informazioni su alcuni problemi che potresti riscontrare durante l'utilizzo AWS Config con AWS Control Tower.

Elevata AWS Config costi

Se il flusso di lavoro include processi che creano, aggiornano o eliminano risorse frequentemente o se gestisce un gran numero di risorse, tale flusso di lavoro può generare un gran numero di CI. Se esegui questi processi in un account non di produzione, valuta la possibilità di annullare la registrazione dell'account. Potrebbe essere necessario disattivare manualmente il AWS Config registratore per quell'account.

Note

Dopo aver annullato la registrazione dell'account, AWS Control Tower non può applicare controlli investigativi o registrare gli eventi dell'account, come AWS Config le attività, per le risorse in quell'account.

Per ulteriori informazioni, consulta [Annullare la gestione](#) di un account registrato. Per informazioni su come disattivare il AWS Config registratore, vedere [Gestione](#) del registratore di configurazione.

La stessa risorsa viene registrata più volte

Verifica se la risorsa è una [risorsa globale](#). Per le zone di atterraggio di AWS Control Tower precedenti alla versione 3.0, AWS Config è possibile registrare determinate risorse globali una volta per ogni regione in cui opera. Ad esempio, se AWS Config è abilitato su otto regioni, ogni ruolo viene registrato otto volte.

Le seguenti risorse vengono registrate una volta per ogni regione in cui AWS Config è operativo:

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Le altre risorse globali vengono registrate una sola volta. Ecco alcuni esempi di risorse che vengono registrate una sola volta:

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config non ha registrato una risorsa

Alcune risorse hanno relazioni di dipendenza con altre risorse. Queste relazioni possono essere dirette o indirette. [Puoi trovare un elenco di relazioni indirette obsolete nelle domande frequenti. AWS Config](#)

Eventi del ciclo di vita in AWS Control Tower

Alcuni eventi registrati da AWS Control Tower sono eventi del ciclo di vita. Lo scopo di un evento del ciclo di vita è contrassegnare il completamento di determinate azioni di AWS Control Tower che

modificano lo stato delle risorse. Gli eventi del ciclo di vita si applicano alle risorse create o gestite da AWS Control Tower, come una zona di atterraggio, una baseline o un controllo, relative a un'unità organizzativa (OU) o a un account.

Caratteristiche degli eventi del ciclo di vita di AWS Control Tower

- Per ogni evento del ciclo di vita, il log eventi mostra se l'operazione originaria di Control Tower è stata completata correttamente o non è riuscita.
- AWS CloudTrail registra automaticamente ogni evento del ciclo di vita come evento di servizio non API. AWS Per ulteriori informazioni, consulta la Guida per [l' AWS CloudTrail utente](#).
- Ogni evento del ciclo di vita viene inoltre distribuito ai servizi Amazon EventBridge e Amazon CloudWatch Events. Nota: per ricevere gli eventi del ciclo di vita in EventBridge, devi avere un AWS CloudTrail percorso attivo con la registrazione abilitata. Per ulteriori informazioni sugli eventi di AWS servizio erogati tramite AWS CloudTrail, consulta gli eventi di servizio [AWS erogati tramite AWS CloudTrail](#) nella Amazon EventBridge User Guide.

Gli eventi del ciclo di vita in AWS Control Tower offrono due vantaggi principali:

- Poiché un evento del ciclo di vita registra il completamento di un'azione di AWS Control Tower, puoi creare una regola Amazon o una EventBridge regola Amazon CloudWatch Events in grado di attivare le fasi successive del flusso di lavoro di automazione, in base allo stato dell'evento del ciclo di vita.
- I log forniscono ulteriori dettagli per aiutare amministratori e revisori nell'esame di determinati tipi di attività nelle organizzazioni.

Come funzionano gli eventi del ciclo di vita

AWS Control Tower si affida a più servizi per implementare le sue azioni. Pertanto, ogni evento del ciclo di vita viene registrato solo dopo il completamento di una serie di operazioni. Ad esempio, quando abiliti un controllo su un'unità organizzativa, AWS Control Tower avvia una serie di passaggi secondari che implementano la richiesta. Il risultato finale dell'intera serie di fasi secondarie viene registrato nel log come stato dell'evento del ciclo di vita.

- Se ogni fase secondaria sottostante è stata completata correttamente, lo stato dell'evento del ciclo di vita viene registrato come Succeeded (Riuscito).
- Se una delle fasi secondarie sottostanti non è stata completata correttamente, lo stato dell'evento del ciclo di vita viene registrato come Failed (Non riuscito).

Ogni evento del ciclo di vita include un timestamp registrato che mostra quando è stata avviata l'azione di AWS Control Tower e un altro timestamp che mostra quando l'evento del ciclo di vita è completato, indicando il successo o il fallimento.

Visualizzazione degli eventi del ciclo di vita in Control Tower

Puoi visualizzare gli eventi del ciclo di vita dalla pagina Attività nella dashboard di AWS Control Tower.

- Per passare alla pagina Activities (Attività) selezionare Activities (Attività) dal riquadro di navigazione a sinistra.
- Per ottenere ulteriori dettagli su un evento specifico, selezionare l'evento e quindi scegliere il pulsante View details (Visualizza dettagli) in alto a destra.

Per ulteriori informazioni su come integrare gli eventi del ciclo di vita di AWS Control Tower nei flussi di lavoro, consulta questo post del blog, [Utilizzo degli eventi del ciclo di vita per tenere traccia delle azioni di AWS Control Tower e attivare flussi di lavoro automatizzati](#).

Comportamento previsto ed eventi del ciclo di vita CreateManagedAccount UpdateManagedAccount

Quando crei un account o registri un account in AWS Control Tower, queste due azioni richiamano la stessa API interna. Se si verifica un errore durante il processo, di solito si verifica dopo la creazione dell'account, ma il provisioning non è completo. Quando si riprova a creare l'account dopo l'errore o quando si tenta di aggiornare il prodotto fornito, AWS Control Tower rileva che l'account esiste già.

Poiché l'account esiste, AWS Control Tower registra l'evento del UpdateManagedAccount ciclo di vita anziché l'evento del CreateManagedAccount ciclo di vita alla fine della richiesta di nuovo tentativo. Potresti aspettarti di vedere un altro CreateManagedAccount evento a causa dell'errore. Tuttavia, l'evento del UpdateManagedAccount ciclo di vita è il comportamento previsto e desiderato.

Se prevedi di creare o registrare account in AWS Control Tower utilizzando metodi automatici, programma la funzione Lambda per cercare gli eventi del ciclo di vita e gli eventi UpdateManagedAccount del ciclo di vita. CreateManagedAccount

Nomi dell'evento del ciclo di vita

Ogni evento del ciclo di vita è denominato in modo da corrispondere all'azione originaria di AWS Control Tower, anch'essa registrata da AWS. CloudTrail Pertanto, ad esempio, viene denominato

un evento del ciclo di vita originato dall'evento AWS Control Tower. `CreateManagedAccount`
`CloudTrail CreateManagedAccount`

Ogni nome nell'elenco che segue è un collegamento a un esempio dei dettagli registrati in formato JSON. I dettagli aggiuntivi mostrati in questi esempi sono tratti dai registri degli eventi di Amazon CloudWatch .

Anche se JSON non supporta i commenti, alcuni commenti sono stati aggiunti negli esempi a scopo esplicativo. I commenti sono preceduti da `///` e appaiono sul lato destro degli esempi.

In questi esempi, alcuni nomi di account e nomi di organizzazione vengono oscurati. `accountId` è sempre una sequenza di 12 numeri, che negli esempi è stata sostituita con `"xxxxxxxxxxxxxx"`. `organizationalUnitID` è una stringa univoca di lettere e numeri. Il formato viene mantenuto negli esempi.

- [`CreateManagedAccount`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per creare e fornire un nuovo account utilizzando l'account factory.
- [`UpdateManagedAccount`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per aggiornare un prodotto con provisioning associato a un account creato in precedenza utilizzando l'account factory.
- [`EnableGuardrail`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per abilitare un controllo su un'unità organizzativa.
- [`DisableGuardrail`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per disabilitare un controllo su un'unità organizzativa.
- [`SetupLandingZone`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per configurare una zona di atterraggio.
- [`UpdateLandingZone`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per aggiornare la zona di atterraggio esistente.
- [`RegisterOrganizationalUnit`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per abilitare le sue funzionalità di governance su un'unità organizzativa.
- [`DeregisterOrganizationalUnit`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per disabilitare le sue funzionalità di governance su un'unità organizzativa.
- [`PrecheckOrganizationalUnit`](#): il registro registra se AWS Control Tower ha rilevato risorse che potrebbero impedire il corretto completamento dell'operazione di governance di `Extend`.
- [`EnableBaseline`](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per abilitare una nuova linea di base su un account membro di destinazione

nell'ambito di un'unità organizzativa. L'operazione di abilitazione può essere avviata utilizzando l'EnableBaselineAPI o la console.

- [ResetEnabledBaseline](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per reimpostare una baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. L'operazione di ripristino può essere avviata utilizzando l'ResetEnabledBaselineAPI o la console.
- [UpdateEnabledBaseline](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per aggiornare una baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. L'operazione di aggiornamento può essere avviata utilizzando l'UpdateEnabledBaselineAPI o la console.
- [DisableBaseline](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per disabilitare una baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. L'operazione di disabilitazione può essere avviata utilizzando l'DisableBaselineAPI o la console.
- [EnableControl](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per abilitare un controllo su un account di destinazione nell'ambito di un'unità organizzativa. L'operazione di abilitazione può essere avviata utilizzando l'EnableControlAPI o la console.
- [ResetEnabledControl](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per reimpostare un controllo abilitato esistente su un account di destinazione in un'unità organizzativa. L'operazione di ripristino può essere avviata utilizzando l'ResetEnabledControlAPI o la console.
- [UpdateEnabledControl](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per aggiornare un controllo abilitato esistente su un account di destinazione in un'unità organizzativa. L'operazione di aggiornamento può essere avviata utilizzando l'UpdateEnabledControlAPI o la console.
- [DisableControl](#): il registro registra se AWS Control Tower ha completato con successo tutte le azioni per disabilitare un controllo abilitato esistente su un account di destinazione in un'unità organizzativa. L'operazione di disabilitazione può essere avviata utilizzando l'DisableControlAPI o la console.

Le sezioni seguenti forniscono un elenco degli eventi del ciclo di vita di AWS Control Tower, con esempi dei dettagli registrati per ogni tipo di evento del ciclo di vita.

CreateManagedAccount

Questo evento del ciclo di vita registra se AWS Control Tower ha creato e fornito con successo un nuovo account utilizzando l'account factory. Questo evento corrisponde all'evento AWS Control Tower. CreateManagedAccount CloudTrail Il log eventi del ciclo di vita include accountName e accountId dell'account appena creato e organizationalUnitName e organizationalUnitId dell'unità organizzativa in cui è stato inserito l'account.

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX", // Management account
  ID.
  "time": "2018-08-30T21:42:18Z", // Format: yyyy-MM-
  dd'T'hh:mm:ssZ
  "region": "us-east-1", // AWS Control Tower
  home region.
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call
    was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
    "eventSource": "controltower.amazonaws.com",
    "eventName": "CreateManagedAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "createManagedAccountStatus": {
        "organizationalUnit":{
          "organizationalUnitName":"Custom",
          "organizationalUnitId":"ou-XXXX-l3zc8b3h"
```

```

    },
    "account":{
      "accountName":"LifeCycle1",
      "accountId":"XXXXXXXXXXXX"
    },
    "state":"SUCCEEDED",
    "message":"AWS Control Tower successfully created a managed account.",
    "requestedTimestamp":"2019-11-15T11:45:18+0000",
    "completedTimestamp":"2019-11-16T12:09:32+0000"}
  }
}
}

```

UpdateManagedAccount

Questo evento del ciclo di vita registra se AWS Control Tower ha aggiornato correttamente il prodotto fornito associato a un account creato in precedenza utilizzando account factory. Questo evento corrisponde all'evento AWS Control Tower. UpdateManagedAccount CloudTrail. Il log eventi del ciclo di vita include accountName e accountId dell'account associato e organizationalUnitName e organizationalUnitId dell'unità organizzativa in cui è stato inserito l'account aggiornato.

```

{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX", // AWS Control Tower
  "organization": "organization management account.",
  "time": "2018-08-30T21:42:18Z", // Format: yyyy-MM-
  "region": "us-east-1", // AWS Control Tower
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXX",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call
    "was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
  }
}

```

```

    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateManagedAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "updateManagedAccountStatus": {
        "organizationalUnit": {
          "organizationalUnitName": "Custom",
          "organizationalUnitId": "ou-XXXX-13zc8b3h"
        },
        "account": {
          "accountName": "LifeCycle1",
          "accountId": "XXXXXXXXXXXX"
        },
        "state": "SUCCEEDED",
        "message": "AWS Control Tower successfully updated a managed account.",
        "requestedTimestamp": "2019-11-15T11:45:18+0000",
        "completedTimestamp": "2019-11-16T12:09:32+0000"
      }
    }
  }
}

```

EnableGuardrail

Questo evento del ciclo di vita registra se AWS Control Tower ha abilitato con successo un controllo su un'unità organizzativa gestita da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower EnableGuardrail CloudTrail. Il registro degli eventi del ciclo di vita include la `guardrailId` fine `guardrailBehavior` del controllo e la fine `organizationalUnitId` dell'unità `organizationalUnitName` organizzativa su cui il controllo è abilitato.

```

{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX",
  "time": "2018-08-30T21:42:18Z", // End-time of action.
  "format": "yyyy-MM-dd'T'hh:mm:ssZ"
}

```

```

    "region": "us-east-1",                                     // AWS Control Tower
    home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "00000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                        "organizationalUnitName": "Custom",
                        "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                ],
                "guardrails": [
                    {
                        "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                        "guardrailBehavior": "DETECTIVE"
                    }
                ],
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully enabled a guardrail on an
organizational unit.",
                "requestTimestamp": "2019-11-12T09:01:07+0000",
                "completedTimestamp": "2019-11-12T09:01:54+0000"
            }
        }
    }
}

```

DisableGuardrail

Questo evento del ciclo di vita registra se AWS Control Tower ha disabilitato con successo un controllo su un'unità organizzativa gestita da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower DisableGuardrail CloudTrail . Il registro degli eventi del ciclo di vita include la guardrailId fine guardrailBehavior del controllo e la fine organizationalUnitId dell'unità organizationalUnitName organizzativa su cui il controllo è disabilitato.

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX",
  "time": "2018-08-30T21:42:18Z",
  "region": "us-east-1",
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableGuardrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "disableGuardrailStatus": {
        "organizationalUnits": [
          {
            "organizationalUnitName": "Custom",
            "organizationalUnitId": "ou-vwxy-18vy4yro"
          }
        ]
      },
      "guardrails": [
```



```

        {
            "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
            "guardrailBehavior": "DETECTIVE"
        }
    ],
    "state": "SUCCEEDED",
    "message": "AWS Control Tower successfully disabled a guardrail on an
organizational unit.",
    "requestTimestamp": "2019-11-12T09:01:07+0000",
    "completedTimestamp": "2019-11-12T09:01:54+0000"
}
    }
}
}

```

SetupLandingZone

Questo evento del ciclo di vita registra se AWS Control Tower ha impostato correttamente una zona di atterraggio. Questo evento corrisponde all'evento AWS Control Tower SetupLandingZone CloudTrail. Il registro degli eventi del ciclo di vita include `rootOrganizationalId` l'ID dell'organizzazione che AWS Control Tower crea dall'account di gestione. La voce di registro include anche `organizationalUnitName` e `organizationalUnitId` per ciascuna unità organizzativa e `accountName` e `accountId` per ciascun account, creati quando AWS Control Tower configura la zona di destinazione.

```

{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",           // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                             // Management account
    ID.
    "time": "2018-08-30T21:42:18Z",                         // Event time from
    CloudTrail.
    "region": "us-east-1",                                  // Management account
    CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                   // Management-account
            ID.

```

```

    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-08-30T21:42:18Z",           // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",                     // AWS Control Tower
home region.
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "CloudTrail_event_ID",             // This value is
generated by CloudTrail.
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "serviceEventDetails": {
    "setupLandingZoneStatus": {
      "state": "SUCCEEDED",                     // Status of entire
lifecycle operation.
      "message": "AWS Control Tower successfully set up a new landing zone.",

      "rootOrganizationalId" : "r-1234",
      "organizationalUnits" : [                 // Use a list.
        {
          "organizationalUnitName": "Security", // Security OU
name.
          "organizationalUnitId": "ou-adpf-302pk332" // Security OU ID.
        },
        {
          "organizationalUnitName": "Custom",    // Custom OU name.
          "organizationalUnitId": "ou-adpf-302pk332" // Custom OU ID.
        },
      ],
      "accounts": [                             // All created
accounts are here. Use a list of "account" objects.

        {
          "accountName": "Audit",
          "accountId": "XXXXXXXXXXXX"
        },
        {
          "accountName": "Log archive",
          "accountId": "XXXXXXXXXXXX"
        }
      ],
    },
  },

```

```

        "requestedTimestamp": "2018-08-30T21:42:18Z",
        "completedTimestamp": "2018-08-30T21:42:18Z"
    }
}
}
}

```

UpdateLandingZone

Questo evento del ciclo di vita registra se AWS Control Tower ha aggiornato correttamente la zona di atterraggio esistente. Questo evento corrisponde all'evento AWS Control Tower UpdateLandingZone CloudTrail. Il registro degli eventi del ciclo di vita include l'rootOrganizationalIdID dell'organizzazione (aggiornata) governata da AWS Control Tower. La voce di registro include anche l'organizationalUnitNameand organizationalUnitId per ciascuna unità organizzativa e l'accountNameand accountId per ciascun account, creato in precedenza, quando AWS Control Tower ha originariamente impostato la zona di atterraggio.

```

{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",           // Request ID.
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX",                             // Management account
  ID.
  "time": "2018-08-30T21:42:18Z",                         // Event time from
  CloudTrail.
  "region": "us-east-1",                                  // Management account
  CloudTrail region.
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",                       // Management account
      ID.
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z",                 // Timestamp when call
    was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateLandingZone",
    "awsRegion": "us-east-1",                             // AWS Control Tower
    home region.
  }
}

```

```

    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "CloudTrail_event_ID",           // This value is
generated by CloudTrail.

    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
        "updateLandingZoneStatus": {
            "state": "SUCCEEDED",               // Status of entire
operation.
            "message": "AWS Control Tower successfully updated a landing zone.",

            "rootOrganizationalId" : "r-1234",
            "organizationalUnits" : [           // Use a list.
                {
                    "organizationalUnitName": "Security",           // Security OU
name.
                    "organizationalUnitId": "ou-adpf-302pk332"      // Security OU ID.
                },
                {
                    "organizationalUnitName": "Custom",             // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"      // Custom OU ID.
                },
            ],
            "accounts": [                                           // All created
accounts are here. Use a list of "account" objects.
                {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                },
                {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
}

```

}

RegisterOrganizationalUnit

Questo evento del ciclo di vita registra se AWS Control Tower ha abilitato con successo le sue funzionalità di governance su un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower RegisterOrganizationalUnit CloudTrail . Il registro degli eventi del ciclo di vita include la fine organizationalUnitId dell'organizationalUnitNameunità organizzativa che AWS Control Tower ha sottoposto alla sua governance.

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "123456789012",
  "time": "2018-08-30T21:42:18Z",
  "region": "us-east-1",
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "RegisterOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "registerOrganizationalUnitStatus": {
        "state": "SUCCEEDED",

        "message": "AWS Control Tower successfully registered an organizational
unit.",

        "organizationalUnit" :
```

```

        {
            "organizationalUnitName": "Test",
            "organizationalUnitId": "ou-adpf-302pk332"
        }
        "requestedTimestamp": "2018-08-30T21:42:18Z",
        "completedTimestamp": "2018-08-30T21:42:18Z"
    }
}
}
}

```

DeregisterOrganizationalUnit

Questo evento del ciclo di vita registra se AWS Control Tower ha disabilitato con successo le sue funzionalità di governance su un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower DeregisterOrganizationalUnit CloudTrail. Il registro degli eventi del ciclo di vita include la fine dell'unità `organizationalUnitName` organizzativa su cui AWS Control Tower ha disabilitato le sue funzionalità di governance. `organizationalUnitId`

```

{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "00000000-0000-0000-1111-123456789012",
        "readOnly": false,
    }
}

```

```

    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "deregisterOrganizationalUnitStatus": {
        "state": "SUCCEEDED",
        "message": "AWS Control Tower successfully de-registered an
organizational unit.",
        "organizationalUnit" :
          {
            "organizationalUnitName": "Test",                // Foundational
OU name.
            "organizationalUnitId": "ou-adpf-302pk332"        // Foundational
OU ID.
          },
        "requestedTimestamp": "2018-08-30T21:42:18Z",
        "completedTimestamp": "2018-08-30T21:42:18Z"
      }
    }
  }
}

```

PrecheckOrganizationalUnit

Questo evento del ciclo di vita registra se AWS Control Tower ha eseguito con successo i controlli preliminari su un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower. `PrecheckOrganizationalUnit` CloudTrail Il registro degli eventi del ciclo di vita contiene un campo `per`, e `failedPrechecks` i valori `IdName`, per ogni risorsa su cui AWS Control Tower ha eseguito i controlli preliminari durante il processo di registrazione dell'unità organizzativa.

Il registro degli eventi contiene anche informazioni sugli account annidati su cui sono stati eseguiti i controlli preliminari, inclusi i `accountName` campi, e. `accountId` `failedPrechecks`

Se il `failedPrechecks` valore è vuoto, significa che tutti i controlli preliminari per quella risorsa sono stati superati correttamente.

- Questo evento viene emesso solo se si verifica un errore di precontrollo.
- Questo evento non viene emesso se si sta registrando un'unità organizzativa vuota.

Esempio di evento:

```

{
  "eventVersion": "1.08",

```

```
"userIdentity": {
  "accountId": "XXXXXXXXXXXX",
  "invokedBy": "AWS Internal"
},
"eventTime": "2021-09-20T22:45:43Z",
"eventSource": "controltower.amazonaws.com",
"eventName": "PrecheckOrganizationalUnit",
"awsRegion": "us-west-2",
"sourceIPAddress": "AWS Internal",
"userAgent": "AWS Internal",
"eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
"readOnly": false,
"eventType": "AwsServiceEvent",
"managementEvent": true,
"recipientAccountId": "XXXXXXXXXXXX",
"serviceEventDetails": {
  "precheckOrganizationalUnitStatus": {
    "organizationalUnit": {
      "organizationalUnitName": "Ou-123",
      "organizationalUnitId": "ou-abcd-123456",
      "failedPrechecks": [
        "SCP_CONFLICT"
      ]
    }
  },
  "accounts": [
    {
      "accountName": "Child Account 1",
      "accountId": "XXXXXXXXXXXX",
      "failedPrechecks": [
        "FAILED_TO_ASSUME_ROLE"
      ]
    },
    {
      "accountName": "Child Account 2",
      "accountId": "XXXXXXXXXXXX",
      "failedPrechecks": [
        "FAILED_TO_ASSUME_ROLE"
      ]
    },
    {
      "accountName": "Management Account",
      "accountId": "XXXXXXXXXXXX",
      "failedPrechecks": [
        "MISSING_PERMISSIONS_AF_PRODUCT"
      ]
    }
  ]
}
```



```

    ]
  },
  {
    "accountName": "Child Account 3",
    "accountId": "XXXXXXXXXXXX",
    "failedPrechecks": []
  },
  ...
],
"state": "FAILED",
"message": "AWS Control Tower failed to register an organizational unit due to
pre-check failures. Go to the OU details page to download a list of failed pre-checks
for the OU and accounts within.",
"requestedTimestamp": "2021-09-20T22:44:02+0000",
"completedTimestamp": "2021-09-20T22:45:43+0000"
}
},
"eventCategory": "Management"
}

```

EnableBaseline

Questo evento del ciclo di vita registra se AWS Control Tower ha abilitato con successo una baseline su un account membro di destinazione in un'unità organizzativa. Questo evento corrisponde allo o agli eventi di `AWS Control TowerRegisterOrganizationalUnit.EnableBaseline` CloudTrail. Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, la `baselineIdentifier` su cui è stata abilitata la baseline, la `parentIdentifier` baseline abilitata sull'unità organizzativa principale e la `statusSummary` visualizzazione dello stato SUCCEEDED o FAILED, insieme ai parametri aggiuntivi e al timestamp dell'operazione.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-02-10T17:14:57Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "EnableBaseline",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",

```

```

    "requestParameters": null,
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
      "enableBaselineStatus": {
        "enabledBaselineDetails": {
          "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "parentIdentifier": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-ern76xmzvf/XXXXXXXXXXXX",
          "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/XXXXXXXXXXXXXXXXXXXX",
          "baselineVersion": "4.0",
          "statusSummary": {
            "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
            "status": "SUCCEEDED"
          },
          "parameters": [
            {
              "key": "IdentityCenterEnabledBaselineArn",
              "value": {
                "untyped": {
                  "object": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX"
                }
              }
            }
          ]
        }
      },
      "requestedTimestamp": "2025-02-10T17:07:09+0000",
      "completedTimestamp": "2025-02-10T17:14:57+0000"
    },
    "eventCategory": "Management"
  }
}

```

ResetEnabledBaseline

Questo evento del ciclo di vita registra se AWS Control Tower ha ripristinato correttamente la baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. Questo evento corrisponde allo o agli eventi di AWS Control TowerRegisterOrganizationalUnit. ResetEnabledBaseline CloudTrail Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, la baseline targetIdentifier su cui è stata abilitata la baseline, la parentIdentifier baseline abilitata sull'unità organizzativa principale e la statusSummary visualizzazione dello stato SUCCEEDED o FAILED, insieme ai parametri aggiuntivi e al timestamp dell'operazione.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-02-10T21:17:55Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "ResetEnabledBaseline",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "resetEnabledBaselineStatus": {
      "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/XXXXXXXXXXXXXXXXXXXX",
        "baselineVersion": "1.0",
```

```

        "statusSummary": {
            "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
            "status": "SUCCEEDED"
        },
        "parameters": []
    },
    "requestedTimestamp": "2025-02-10T21:14:24Z",
    "completedTimestamp": "2025-02-10T21:17:54+0000"
}
},
"eventCategory": "Management"
}

```

UpdateEnabledBaseline

Questo evento del ciclo di vita registra se AWS Control Tower ha aggiornato correttamente la baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. Questo evento corrisponde allo o agli eventi di AWS Control Tower RegisterOrganizationalUnit. UpdateEnabledBaseline CloudTrail Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, la baseline targetIdentifier su cui è stata abilitata la baseline, la parentIdentifier baseline abilitata sull'unità organizzativa principale e la statusSummary visualizzazione dello stato SUCCEEDED o FAILED, insieme ai parametri aggiuntivi e al timestamp dell'operazione.

```

{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T19:45:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,

```

```

    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
      "updateEnabledBaselineStatus": {
        "enabledBaselineDetails": {
          "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "parentIdentifier": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-ern76xmzvf/XXXXXXXXXXXX",
          "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/XXXXXXXXXXXXXXXXXXXX",
          "baselineVersion": "4.0",
          "statusSummary": {
            "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
            "status": "SUCCEEDED"
          },
          "parameters": [
            {
              "key": "IdentityCenterEnabledBaselineArn",
              "value": {
                "untyped": {
                  "object": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX"
                }
              }
            }
          ]
        },
        "requestedTimestamp": "2025-02-10T19:39:35+0000",
        "completedTimestamp": "2025-02-10T19:45:28+0000"
      }
    },
    "eventCategory": "Management"
  }
}

```

DisableBaseline

Questo evento del ciclo di vita registra se AWS Control Tower ha disabilitato con successo la baseline abilitata esistente su un account membro di destinazione nell'ambito di un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower. DisableBaseline CloudTrail Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, la baseline targetIdentifier su cui è stata abilitata la baseline, la parentIdentifier

baseline abilitata sull'unità organizzativa principale e la statusSummary visualizzazione dello stato SUCCEEDED o FAILED, insieme ai parametri aggiuntivi e al timestamp dell'operazione.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-03-14T00:50:58Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "DisableBaseline",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "disableBaselineStatus": {
      "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/XXXXXXXXXXXXXXXXXXXX",
        "baselineVersion": "1.0",
        "statusSummary": {
          "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
          "status": "SUCCEEDED"
        },
        "parameters": []
      },
      "baselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
```

```

        "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXX",
        "baselineVersion": "1.0",
        "statusSummary": {
            "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
            "status": "SUCCEEDED"
        },
        "parameters": []
    },
    "requestedTimestamp": "2025-03-14T00:49:13Z",
    "completedTimestamp": "2025-03-14T00:50:58+0000"
}
},
"eventCategory": "Management"
}

```

EnableControl

Questo evento del ciclo di vita registra se AWS Control Tower ha abilitato con successo un controllo su un account di destinazione gestito da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower EnableControl CloudTrail e viene emesso quando un controllo viene abilitato utilizzando l'EnableControlAPI o la console. Il registro degli eventi del ciclo di vita include il controllo che è stato abilitato, il `arn` controllo abilitato risultante, il `parentIdentifier` controllo abilitato sull'unità organizzativa principale, quello `targetIdentifier` su cui è stato abilitato il controllo e la `state` visualizzazione dello stato SUCCEEDED o message FAILED, insieme a un timestamp dell'operazione.

Note

L'evento del EnableControl ciclo di vita corrisponde all'API. EnableControl AWS Control Tower emette anche l'evento del EnableGuardrail ciclo di vita precedente quando un controllo è abilitato. Se crei un'automazione che reagisce all'attivazione dei controlli, tieni conto di entrambi i nomi degli eventi.

```
{
```

```

    "eventVersion": "1.11",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T15:59:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a4f45d0d-ab6d-41c7-9f97-786d80ff23d2",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
      "enableControlStatus": {
        "arn": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
        "parentIdentifier": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TC0LC0JPSV6T",
        "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_LOGGING_ENABLED",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-k54j7iydcs/XXXXXXXXXXXX",
        "state": "SUCCEEDED",
        "message": "AWS Control Tower successfully enabled a control on the target.",
        "requestedTimestamp": "2026-01-07T15:59:24+0000",
        "completedTimestamp": "2026-01-07T15:59:28+0000"
      }
    },
    "eventCategory": "Management"
  }
}

```

ResetEnabledControl

Questo evento del ciclo di vita registra se AWS Control Tower ha ripristinato correttamente un controllo abilitato esistente su un account di destinazione gestito da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower `ResetEnabledControl` CloudTrail e viene

emesso quando un controllo abilitato viene ripristinato utilizzando l'`ResetEnabledControlAPI` o la console. Il registro degli eventi del ciclo di vita include i dati `controlIdentifier` del controllo, `arn` del controllo abilitato, `parentIdentifier` del controllo abilitato sull'unità organizzativa principale, quello `targetIdentifier` su cui è stato reimpostato il controllo e la `state` visualizzazione dello stato `SUCCEEDED` o `message FAILED`, insieme a un timestamp dell'operazione.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2026-01-07T16:10:42Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "ResetEnabledControl",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "c82d6f3a-4b9e-43ca-8d21-1a3f8d5b62e9",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "resetEnabledControlStatus": {
      "arn": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
      "parentIdentifier": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TC0LC0JPSV6T",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_LOGGING_ENABLED",
      "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-k54j7iydcs/XXXXXXXXXXXX",
      "state": "SUCCEEDED",
      "message": "AWS Control Tower has successfully reset the enabled control on the target.",
      "requestedTimestamp": "2026-01-07T16:10:36+0000",
      "completedTimestamp": "2026-01-07T16:10:42+0000"
    }
  },
  "eventCategory": "Management"
}
```

}

UpdateEnabledControl

Questo evento del ciclo di vita registra se AWS Control Tower ha aggiornato correttamente un controllo abilitato esistente su un account di destinazione gestito da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower UpdateEnabledControl CloudTrail e viene emesso quando un controllo abilitato viene aggiornato tramite l'UpdateEnabledControlAPI o la console. Il registro degli eventi del ciclo di vita include i dati controlIdIdentifier del controllo, arn del controllo abilitato, parentIdentifier del controllo abilitato sull'unità organizzativa principale, quello targetIdentifier su cui il controllo è stato aggiornato e la state visualizzazione dello stato SUCCEEDED o message FAILED, insieme a un timestamp dell'operazione.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2026-01-07T16:25:19Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "UpdateEnabledControl",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "d93e7a4b-5caf-44db-9e32-2b4a9e6c73fa",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "updateEnabledControlStatus": {
      "arn": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
      "parentIdentifier": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TC0LC0JPSV6T",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_LOGGING_ENABLED",
      "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-k54j7iydcs/XXXXXXXXXXXX",

```

```

        "state": "SUCCEEDED",
        "message": "AWS Control Tower successfully updated the enabled control on
the target.",
        "requestedTimestamp": "2026-01-07T16:25:13+0000",
        "completedTimestamp": "2026-01-07T16:25:19+0000"
    }
},
"eventCategory": "Management"
}

```

DisableControl

Questo evento del ciclo di vita registra se AWS Control Tower ha disabilitato con successo un controllo abilitato esistente su un account di destinazione gestito da AWS Control Tower. Questo evento corrisponde all'evento AWS Control Tower DisableControl CloudTrail e viene emesso quando un controllo viene disabilitato utilizzando l'DisableControlAPI o la console. Il registro degli eventi del ciclo di vita include i controlIdentifier dati del controllo, arn del controllo abilitato, parentIdentifier del controllo abilitato sull'unità organizzativa principale, quello targetIdentifier su cui il controllo è stato disabilitato e la state visualizzazione dello stato SUCCEEDED o message FAILED, insieme a un timestamp dell'operazione.

Note

AWS Control Tower emette anche l'evento del DisableGuardrail ciclo di vita precedente quando un controllo è disabilitato. Se crei un'automazione che reagisce alla disattivazione dei controlli, tieni conto di entrambi i nomi degli eventi.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2026-01-07T16:42:11Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "DisableControl",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",

```

```

    "requestParameters": null,
    "responseElements": null,
    "eventID": "e04f8b5c-6dba-45ec-af43-3c5b0f7d84ab",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
      "disableControlStatus": {
        "arn": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
        "parentIdentifier": "arn:aws:controltower:us-east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TC0LC0JPSV6T",
        "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_LOGGING_ENABLED",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-k54j7iydcs/XXXXXXXXXXXX",
        "state": "SUCCEEDED",
        "message": "AWS Control Tower successfully disabled the enabled control on the target.",
        "requestedTimestamp": "2026-01-07T16:42:05+0000",
        "completedTimestamp": "2026-01-07T16:42:11+0000"
      }
    },
    "eventCategory": "Management"
  }
}

```

Utilizzo AWS Notifiche utente con AWS Control Tower

Puoi utilizzare [le notifiche AWS utente](#) per configurare i canali di consegna per ricevere notifiche sugli AWS Control Tower eventi. L'utente riceverà una notifica quando un evento corrisponde a una regola specificata. Puoi ricevere notifiche relative agli eventi attraverso più canali, tra cui e-mail, [Amazon Q Developer in chat](#), [applicazioni di chat](#), notifiche chat o notifiche push [per app per dispositivi mobili per AWS console](#). È anche possibile visualizzare le notifiche nel Centro notifiche della console.

AWS Le notifiche utente supportano l'aggregazione, che può ridurre il numero di notifiche che ricevi durante eventi specifici. Le notifiche sono visibili anche nel Centro notifiche della console.

I vantaggi dell'iscrizione alle notifiche tramite Notifiche AWS utente invece di EventBridge includono:

- Un'interfaccia utente (UI) più intuitiva.
- Integrazione con la AWS console, nell' `bell/notifications` area della barra di navigazione globale.

- Supporto nativo per le notifiche e-mail, non è necessario configurare Amazon SNS.
- In particolare, il supporto per le notifiche push mobili, in esclusiva per le notifiche AWS utente.

Ad esempio, un tipo di notifica che potresti voler ricevere è in caso di rilevazioni critiche e di elevata gravità del CSPM di Security Hub. Un frammento di codice in JSON per configurare l'abbonamento alle notifiche può essere simile al seguente:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filtraggio degli eventi

- Puoi filtrare gli eventi per servizio e nome utilizzando i filtri disponibili nella console AWS User Notifications.
- Puoi filtrare gli eventi in base a proprietà specifiche se crei il tuo EventBridge filtro dal codice JSON.

Evento di esempio AWS Control Tower

Ecco un esempio generalizzato di evento per AWS Control Tower.

- È un EventBridge evento.
- Puoi iscriverti a EventBridge eventi (come questo) utilizzando le notifiche AWS utente.

```

{
  "version": "0",
  "id": "<id>", // alphanumeric string
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "<account ID>", // Management account ID.
  "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
  "region": "<region>", // AWS Control Tower home region.
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "121212121212",
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
    yyyy-MM-dd'T'hh:mm:ssZ.
    "eventSource": "controltower.amazonaws.com",
    "eventName": "<event name>", // one of the event names listed in https://
    docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
    "awsRegion": "<region>",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "<id>",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      // the contents of this object vary depending on the event subtype and
    event state
    }
  }
}

```

AWS Backup e AWS Control Tower

AWS Backup è un servizio che consente di creare piani per il backup automatico AWS delle risorse. Per configurare i backup per le risorse AWS Control Tower, devi seguire quattro passaggi principali:

1. Abilita AWS Backup per la tua landing zone. Puoi farlo nella pagina delle impostazioni della zona di atterraggio nella console AWS Control Tower. Quando si attiva AWS Backup, le risorse vengono create in diversi account. Per ulteriori informazioni, consulta [Risorse create per AWS Backup](#).
2. Opt-in ai backup per AWS Control Tower nella AWS Backup console. Per ulteriori informazioni, consulta [Working with supported services](#) nella AWS Backup Developer Guide.
3. AWS Backup Attivalo sulle singole unità organizzative che desideri includere. Puoi eseguire questa operazione nella pagina dei dettagli dell'unità organizzativa nella console, dopo aver abilitato AWS Backup a livello di landing zone. Quando si abilita AWS Backup su un'unità organizzativa, gli account di tale unità organizzativa ricevono gli AWS Backup archivi locali.
4. Etichetta le risorse selezionate da includere nei backup. Il tag indica la frequenza dei backup per quella risorsa. Il piano di backup segue la pianificazione specificata dai tag delle risorse su ciascuna risorsa.

Per ulteriori informazioni, consulta [la Guida per AWS Backup gli sviluppatori](#). Non è previsto alcun costo per la configurazione di AWS Backup con AWS Control Tower. Dovrai sostenere un costo da AWS Backup Per informazioni sui prezzi, consultare [Prezzi di AWS Backup](#).

Per ulteriori dettagli sulle AWS Backup risorse che AWS Control Tower crea nella tua landing zone di AWS Control Tower, consulta [Risorse create per AWS Backup](#)

Note

AWS Control Tower non supporta la configurazione di piani di backup per le risorse AWS Control Tower direttamente tramite il AWS Backup servizio, senza abilitarla anche nel servizio AWS Control Tower.

Prerequisiti

Prima di poter configurare AWS Backup le risorse AWS Control Tower, devi disporre di un' AWS Organizations organizzazione esistente. Se hai già configurato la landing zone di AWS Control Tower, questa funge da organizzazione esistente.

È necessario allocare o creare altri due AWS account che non sono registrati in AWS Control Tower. Questi account diventano l'account di backup centrale e l'account di amministratore di backup. Assegna un nome a questi account con questi nomi.

Inoltre, è necessario selezionare o creare una chiave multiregione AWS Key Management Service (KMS), in particolare per il Backup AWS .

Definizione dei prerequisiti

- L'account di backup centrale: l'account di backup centrale archivia il tuo archivio di backup AWS Control Tower e i tuoi backup. Questo vault viene creato in tutto ciò Regioni AWS che AWS Control Tower gestisce, all'interno di questo account. Cross-account le copie vengono archiviate in questo account, nel caso in cui un account sia compromesso e richieda il ripristino dei dati.
- L'account dell'amministratore di backup: l'account dell'amministratore di backup è l'account amministratore delegato per il AWS Backup servizio in AWS Control Tower. Memorizza i piani di report di Backup Audit Manager (BAM). Questo account aggrega tutti i dati di monitoraggio del backup, come i processi di ripristino e i processi di copia. I dati vengono archiviati in un bucket Amazon S3. Per ulteriori informazioni, consulta [Creazione di piani di report utilizzando la AWS Backup console nella Guida](#) per gli AWS Backup sviluppatori.
- Requisiti politici per la chiave multiregionale AWS KMS

La AWS KMS chiave richiede una politica chiave. Prendi in considerazione una politica chiave simile a questa, che limiti l'accesso ai responsabili (utenti e ruoli) che dispongono di autorizzazioni associate all'account di gestione della tua organizzazione:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "KMS key policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
```



```

        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:root"
        },
        "Action": "kms:*",
        "Resource": "*"
    },
    {
        "Sid": "Allow use of the KMS key for organization",
        "Effect": "Allow",
        "Principal": {
            "AWS": "*"
        },
        "Action": [
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:GenerateDataKey*",
            "kms:Encrypt",
            "kms:ReEncrypt*",
            "kms:GetKeyPolicy",
            "kms:CreateGrant",
            "kms:ListGrants",
            "kms:RevokeGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "ORGANIZATION-ID"
            }
        }
    }
]
}

```

Questa politica di esempio offre a tutti gli account dell'organizzazione l'accesso ai relativi dati di backup crittografati. Utilizza [le chiavi di condizione AWS globali](#) e [le chiavi di AWS KMS condizione](#) per perfezionare le autorizzazioni, a seconda dei principali che richiedono l'accesso ai backup.

Note

La tua AWS KMS chiave multiregionale deve essere replicata per ogni operazione Regione AWS che intendi gestire con AWS Control Tower. È necessario impostare una policy chiave

su ogni chiave di replica multiregionale. Per informazioni su come creare chiavi di replica, consulta [Creare chiavi di replica multiregionali](#).

Abilitare i backup

Puoi abilitare i backup delle risorse nei tuoi account registrati in AWS Control Tower, durante la configurazione della landing zone o quando aggiorni la landing zone.

Come [Prerequisiti](#), è necessario fornire i seguenti elementi

- E Account AWS per fungere da account AWS Backup amministratore
- E Account AWS per fungere da account di Backup AWS Backup Centrale
- Una AWS KMS chiave multiregionale gestita dall'utente, per i backup su più account

Come abilitare i backup

Il processo di abilitazione prevede due parti principali: in primo luogo, abilita i backup per la landing zone, quindi abilita i backup per ogni unità organizzativa registrata che richiede backup.

Prima parte: configura i backup per la tua landing zone

Console: puoi configurare i backup per la tua landing zone nella console AWS Control Tower, nella pagina delle impostazioni della zona di atterraggio. Vedrai questa opzione durante l'operazione di configurazione iniziale della landing zone e potrai rivisitarla in seguito con un aggiornamento della landing zone.

API: puoi abilitare i backup con le API AWS Control Tower chiamando l'[UpdateLandingZoneAPI](#), se disponi già di una landing zone di AWS Control Tower, oppure l'[CreateLandingZoneAPI](#) se stai configurando AWS Control Tower per la prima volta. (Suggerimento: dopo di che, chiama l'[EnableBaselineAPI](#) per stabilire i backup per ogni unità organizzativa di cui hai bisogno.)

Fuori dalla console AWS Control Tower

Parte dell'abilitazione dei backup per la tua landing zone include un passaggio all'esterno della console AWS Control Tower. Devi accedere alla AWS Backup console per esaminare le tue risorse.

Per esaminare i tipi di risorse che hai scelto o attivare tipi di risorse aggiuntivi

1. Apri la console all' AWS Backup indirizzo. <https://console.aws.amazon.com/backup>

2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Attivazione del servizio scegliere Configura risorse.
4. Utilizza gli interruttori a levetta per abilitare o disabilitare i servizi in cui desideri includere. AWS BackupAssicurati che le risorse di cui desideri eseguire il backup siano selezionate, come RDS, EC2, DDB e così via, indipendentemente dal fatto che facciano parte del tuo ambiente AWS Control Tower o meno.

Per maggiori dettagli, [consulta Accetta la gestione dei servizi con](#) AWS Backup

Considerazioni sui nuovi tipi di risorse

Prima di affidarsi AWS Backup alla gestione della protezione dei dati per le risorse di qualsiasi AWS servizio, è necessario eseguire la procedura precedente e attivare AWS Backup tale servizio. Inoltre, poiché il AWS Backup servizio aggiungerà il supporto per servizi aggiuntivi e i relativi tipi di risorse in futuro, è necessario ripetere questa procedura e attivare ogni tipo di risorsa aggiuntivo AWS Backup prima di poter eseguire il backup di quel tipo di risorsa in AWS Control Tower. L'etichettatura di un tipo di risorsa non supportato può causare il fallimento del backup.

Quando attivi i backup per la tua landing zone, AWS Control Tower stabilisce i due account che hai fornito rispettivamente come account Central Backup e account Backup Administrator. AWS Control Tower crea [risorse](#) in questi account e in altri account.

Important

Per abilitare i backup per gli account AWS Control Tower Audit e Log Archive, devi configurare i backup per l'unità organizzativa di sicurezza chiamando l'EnableBaselineAPI. Questa impostazione è consigliata.

La serie di piani e di conservazione consigliata è la seguente:

- Backup orari = 2 settimane di conservazione nel deposito locale, nessuna copia nell'archivio di backup centrale
- Backup giornalieri = 2 settimane di conservazione nel vault locale, 1 mese di conservazione nell'archivio di backup centrale

- Backup settimanali = 1 mese di conservazione nel vault locale, 3 mesi nel vault centrale
- Backup mensili = 3 mesi di conservazione nel vault locale, 3 mesi di conservazione nel deposito di backup centrale

Per informazioni su come creare i piani di backup, consulta [Creazione di piani di report](#) utilizzando la console. AWS Backup

Parte successiva: abilitare i backup sulle unità organizzative

Dopo aver abilitato AWS Backup nelle impostazioni della landing zone, devi eseguire il passaggio aggiuntivo per abilitare il backup sulle unità organizzative specifiche di cui desideri eseguire il backup. Se l'opzione è abilitata AWS Backup per la landing zone, nella pagina dei dettagli dell'unità organizzativa della console verrà visualizzata una sezione che consente di scegliere Abilita il backup per l'unità organizzativa. Se il backup non è abilitato a livello di landing zone, questa sezione non verrà visualizzata nella pagina dei dettagli dell'unità organizzativa.

Per abilitarlo BackupBaseline su un'unità organizzativa, tale unità deve averla già AWSControlTowerBaseline abilitata. Per gli account registrati in ogni unità organizzativa è AWSControlTowerBaseline abilitato.

Negli account e nelle unità organizzative selezionati, AWS Control Tower configura risorse aggiuntive

- Un archivio di Backup locale

AWS Control Tower crea un vault di backup locale nei tuoi account, con quattro possibili tipi di piani di backup collegati al vault. I piani di Backup creati tramite AWS Control Tower sono contrassegnati con un prefisso.

```
BackupPlanTags:
  aws-control-tower: 'managed-by-control-tower'
```

- Quattro tipi di piani di backup: orari, giornalieri, settimanali, mensili.

Ogni piano è associato a un'assegnazione di risorse basata su tag. Ad esempio, qualsiasi risorsa etichettata con `aws-control-tower-backuphourly: true` è protetta con un piano di backup orario.

- Un ruolo di backup locale nei tuoi account

AWS Control Tower crea un ruolo IAM, che viene utilizzato per i backup. Il ruolo richiede quattro autorizzazioni specifiche.

```
"backup:UpdateGlobalSettings", "organizations:RegisterDelegatedAdministrator", "organizations:E
```

Il ruolo ha una relazione di fiducia con il responsabile del servizio di AWS Backup. The role is named `aws-controltower-backup-role` e gli sono associate le seguenti autorizzazioni gestite:

- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)

Tagga le risorse per il backup

Parte del processo di configurazione dei backup in AWS Control Tower consiste nell'etichettare le risorse che desideri includere nel tuo piano di backup. I tag specificano la frequenza dei backup. Questi sono i tag possibili.

- `aws-control-tower-backuphourly : true`
- `aws-control-tower-backupdaily: true`
- `aws-control-tower-backupweekly: true`
- `aws-control-tower-backupmonthly: true`

Considerazioni

- Quando AWS Backup è attivo su un'unità organizzativa, vedrai il valore `Enabled` nel campo `Status` nella pagina dei dettagli dell'unità organizzativa nella console AWS Control Tower. Alcuni altri valori possibili del campo `Status` includono `Not enabled`, `In progress` e `Failed`. Se viene visualizzato lo stato `Non riuscito`, scegli `Re-register OU` per riapplicare la AWS Backup configurazione all'unità organizzativa.
- Se l'opzione è stata AWS Backup attivata su un'unità organizzativa, i nuovi account forniti tramite `Account Factory` in base a cui l'unità organizzativa AWS Backup includerà.

Disattiva i backup

Puoi disattivare i backup delle tue risorse negli account registrati in AWS Control Tower, durante la configurazione della landing zone o quando aggiorni la landing zone.

Per disattivare i backup sono necessari due passaggi principali: prima, disattiva la AWS Backup linea di base su ogni unità organizzativa che ha i backup abilitati, quindi disattiva i backup per la tua landing zone.

Primo passaggio: disattivare i backup sulle unità organizzative

Se AWS Backup è abilitata, devi disabilitare la AWS Backup linea di base di tutte le unità organizzative prima di disattivarla AWS Backup per entrare nella tua landing zone.

Se hai unità organizzative annidate, disabilita la linea di base di AWS Backup sulle unità organizzative secondarie prima dell'unità organizzativa principale. Sebbene la baseline di AWS Backup sia ancora abilitata su un'unità organizzativa secondaria, AWS Control Tower non può disabilitarla sull'unità organizzativa principale.

Puoi disabilitare la baseline di AWS Backup su un'unità organizzativa utilizzando le API AWS Control Tower o la console AWS Control Tower.

Per disabilitare la linea di base (API) di AWS Backup

Innanzitutto, trova l'ARN della baseline di AWS Backup. Chiama l'`ListBaselinesAPI` e richiedi la baseline che `BackupBaseline` deve ottenere il nome suo ARN.

```
aws controltower list-baselines --query 'baselines[?name==`BackupBaseline`]'
```

Quindi, utilizzando quell'ARN, identifica quali unità organizzative hanno abilitato la linea di base di AWS Backup. Chiama l'`ListEnabledBaselinesAPI`, filtrando in base all'identificatore di base, per trovare ogni `BackupBaseline` baseline abilitata e il relativo `enabledBaselineIdentifier` ARN da disabilitare.

```
aws controltower list-enabled-baselines --filter baselineIdentifiers=BackupBaseline-ARN
```

Per disabilitare la baseline di AWS Backup su un'unità organizzativa, puoi chiamare l'`DisableBaselineAPI`.

Comando di esempio:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

Per disabilitare la linea di base di AWS Backup (console)

1. Accedi alla console AWS Control Tower e vai alla pagina Organizzazione.
2. Scegli l'unità organizzativa il cui stato di base di AWS Backup è abilitato per aprire la pagina dei dettagli dell'unità organizzativa.
3. Nella sezione Integrazioni su questa unità organizzativa - opzionale, in AWS Backup, scegli Modifica.
4. Nella finestra di dialogo che appare, seleziona Disabilita, quindi scegli Conferma.

Quando disabiliti la linea di AWS Backup base, AWS Control Tower pulisce le seguenti risorse:

- Tutti gli stackset relativi a AWS Backup
- Tutti i controlli relativi a AWS Backup

Note

Il vault locale viene mantenuto anche se gli stackset vengono eliminati, poiché la politica di conservazione sul vault locale è impostata su. Retain Conserva i tuoi dati.

Passaggio successivo: spegnere AWS Backup per la tua landing zone

Dopo aver soddisfatto il prerequisito disattivando i backup sulle unità organizzative, per disattivare i backup dalla console AWS Control Tower, vai alla pagina delle impostazioni della zona di destinazione. Scegli Disabilita il backup.

Quando disattivi AWS Backup, AWS Control Tower modifica le seguenti risorse:

- Rimuove tutti gli stackset relativi a AWS Backup
- Disattiva tutti i controlli relativi all'unità organizzativa di sicurezza AWS Backup
- De-registers l'account amministratore delegato per l'amministrazione AWS Backup
- Rimuove la governance di AWS Control Tower (per CloudTrail e così via) dagli account AWS Backup Administrator e Central Backup AWS Config

- AWS Control Tower conserva i AWS Backup vault e le risorse del bucket Amazon S3 contenenti i tuoi dati

Dopo aver disabilitato i backup, non vengono creati nuovi backup, ma i backup esistenti non vengono rimossi.

Abilita il backup sugli account spostati

Se sposti un account in un'unità organizzativa AWS Control Tower AWS Backup abilitata e l'account non è registrato in AWS Control Tower, il piano di backup non si applica automaticamente all'account.

Console: AWS Backup per abilitare un singolo account dalla console AWS Control Tower, puoi scegliere **Aggiorna account** nella pagina dei dettagli dell'account oppure puoi scegliere **Re-register OU** nella pagina dei dettagli dell'unità organizzativa per aggiornare più account contemporaneamente.

API: dall'API, se si sposta un account in un'unità organizzativa con la baseline di backup abilitata, è possibile richiamare l'`ResetEnabledBaselineAPI` su tale unità organizzativa, specificando la `EnabledBaseline` risorsa dell'unità organizzativa come destinazione, per attivare i backup sull'account tramite ereditarietà dall'unità organizzativa.

Comando di esempio:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/X0SD0RW8HDB5ZNWEE --region us-
east-1
```

Risposta di esempio:

```
{
  "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

La deriva del backup in AWS Control Tower

La deriva non viene segnalata per AWS Backup le configurazioni in AWS Control Tower. Per ulteriori informazioni sulla deriva in AWS Control Tower, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Se elimini o modifichi il AWS Backup piano, quest'ultimo può entrare in uno stato di deriva. Ecco alcune modifiche da evitare.

- Non spostare l'account Backup Administrator dall'unità organizzativa di sicurezza.
- Non spostare l'account Central Backup dall'unità organizzativa di sicurezza.
- Non rimuovere l'account Backup Administrator dall'organizzazione.
- Non rimuovere l'account Central Backup dall'organizzazione.
- Non scollegare, collegare o aggiornare l' AWS Backup SCP applicato all'unità organizzativa di sicurezza.
- Non scollegare, collegare o aggiornare l' AWS Backup SCP applicato ad altre unità organizzative.
- Non rimuovere l'autorizzazione dell'account Backup Administrator per AWS Backup.
- Non aggiornate le impostazioni di backup tra account per disattivare i backup su più account. Per ulteriori informazioni sui backup tra account, consulta [UpdateGlobalSettings](#) l'API Reference.AWS Backup
- Non eliminare la chiave. AWS KMS
- Non modificate la politica AWS KMS delle chiavi dopo averla impostata.
- Non disabilitate l'accesso affidabile del servizio per AWS Backup.

Note

Drift viene segnalato sullo stato dei SCP-based controlli che proteggono AWS Backup le risorse in AWS Control Tower.

Risorse create per AWS Backup

Le tabelle in questa pagina mostrano le risorse che vengono create negli account AWS Control Tower quando abilitate AWS Backup.

La tabella seguente mostra le risorse che AWS Control Tower crea nell'account AWS Control Tower Central Backup quando abiliti AWS Backup l'organizzazione della landing zone.

Descrizione	Risorse per l'account Central Backup
Quale unità organizzativa contiene l'account?	Unità organizzativa di sicurezza

Descrizione	Risorse per l'account Central Backup
Quale azione ha creato la risorsa?	Zona di atterraggio: creazione o aggiornamento
Quali risorse vengono create?	Cassaforte di Backup centrale— <code>aws-controltower-central-backupvault-*</code>
Quali regioni sono incluse?	Tutte le regioni governate
Quali controlli sono correlati a queste risorse?	<code>CT.BACKUP.PV.3</code>

La tabella seguente mostra le risorse che AWS Control Tower crea nell'account AWS Control Tower Backup Administrator quando abiliti AWS Backup l'organizzazione della landing zone.

Descrizione	Risorse per l'account Backup Administrator: questo è l'account amministratore delegato per AWS Backup
Quale unità organizzativa contiene l'account?	Unità organizzativa di sicurezza
Quale azione ha creato la risorsa?	Zona di atterraggio: creazione o aggiornamento
Quali risorse vengono create?	<p>Backup Audit Manager (BAM)</p> <ul style="list-style-type: none"> <code>aws-controltower_copy_report</code> <code>aws-controltower_backup_report</code> <code>aws-controltower_restore_report</code> <p>Bucket Amazon S3 per l'archiviazione dei log BAM— <code>aws-controltower-backup-reports-<i>{accountId}</i>-*</code></p> <p>Bucket di registrazione degli accessi Amazon S3— <code>aws-controltower-backup-reports-log-<i>{accountId}</i>-*</code></p>

Descrizione	Risorse per l'account Backup Administrator: questo è l'account amministratore delegato per AWS Backup
Quali regioni sono incluse?	Regione di origine
Quali controlli sono correlati a queste risorse?	<ul style="list-style-type: none"> • CT.BACKUP.PV.2 • CT.S3.PV.1 • CT.S3.PV.1

La tabella seguente mostra le risorse che AWS Control Tower crea nell'account AWS Control Tower Audit e nell'account AWS Control Tower Log Archive quando abiliti AWS Backup l'unità organizzativa di sicurezza.

Descrizione	Risorse per gli account Audit e Log Archive
Quale unità organizzativa contiene l'account?	Unità organizzativa di sicurezza
Quale azione ha creato la risorsa?	Abilitare il BackupBaseline
Quali risorse vengono create?	<ul style="list-style-type: none"> • Vault di Backup locale— <code>aws-controltower-local-backupvault-*</code> • Ruolo di Backup locale: <code>aws-controltower-BackupRole</code> • Quattro piani di Backup locali (orario, settimanale, mensile, giornaliero) <ul style="list-style-type: none"> • <code>aws-controltower-hourly-backup-plan</code> • <code>aws-controltower-daily-backup-plan</code> • <code>aws-controltower-weekly-backup-plan</code> • <code>aws-controltower-monthly-backup-plan</code>

Descrizione	Risorse per gli account Audit e Log Archive
	<ul style="list-style-type: none"> Un ruolo IAM— <code>aws-controltower-BackupRole</code>
Quali regioni sono incluse?	Tutte le regioni governate
Quali controlli sono correlati a queste risorse?	<ul style="list-style-type: none"> <code>CT.BACKUP.PV.3</code> <code>CT.IAM.PV.1</code> <code>CT.BACKUP.PV.3</code> <code>CT.BACKUP.PV.1</code>

Note

Quando si BackupBaseline applica l'unità organizzativa di sicurezza, tutti gli account membri di quell'unità organizzativa ricevono le AWS Backup risorse, non solo gli account Audit e Log Archive.

La tabella seguente mostra le risorse che AWS Control Tower crea negli account dei membri dell'unità organizzativa AWS Control Tower quando abiliti AWS Backup su un'unità organizzativa di destinazione.

Descrizione	Risorse per gli account dei membri in altri OUs
In quale unità organizzativa è contenuto l'account?	Qualsiasi unità organizzativa diversa dall'unità organizzativa di sicurezza
Quale azione ha creato la risorsa?	Abilitare il BackupBaseline
Quali risorse vengono create?	<ul style="list-style-type: none"> Vault di Backup locale— <code>aws-controltower-local-backupvault-*</code> Ruolo di Backup locale: <code>aws-controltower-BackupRole</code> Quattro piani di Backup locali (orario, settimanale, mensile, giornaliero)

Descrizione	Risorse per gli account dei membri in altri OUs
	<ul style="list-style-type: none"> • aws-controltower-hourly-backup-plan • aws-controltower-daily-backup-plan • aws-controltower-weekly-backup-plan • aws-controltower-monthly-backup-plan • Un ruolo IAM— aws-controltower-BackupRole
Quali regioni sono incluse?	Tutte le regioni governate
Quali controlli sono correlati a queste risorse?	<ul style="list-style-type: none"> • CT.BACKUP.PV.3 • CT.IAM.PV.1 • CT.BACKUP.PV.3 • CT.BACKUP.PV.1

Controlli per AWS Backup

Quando abiliti AWS Backup nella landing zone di AWS Control Tower, vengono attivati alcuni controlli preventivi nel tuo ambiente. Questi controlli proteggono le risorse AWS Backup necessarie per operare con AWS Control Tower. Non puoi abilitare questi controlli se non AWS Backup sono abilitati per la tua landing zone.

Per ulteriori informazioni, consulta [Controlli per AWS Backup](#).

Smantellamento di una landing zone di AWS Control Tower

AWS Control Tower consente di configurare e gestire AWS ambienti sicuri con più account, noti come landing zone. Il processo di pulizia di tutte le risorse allocate da AWS Control Tower viene definito decommissioning di una landing zone.

Se non desideri più utilizzare AWS Control Tower, lo strumento di smantellamento automatico pulisce le risorse allocate da AWS Control Tower. Per iniziare il processo di disattivazione automatica, vai alla pagina Impostazioni della zona di atterraggio, seleziona la scheda Disattivazione e scegli Decommission landing zone.

Per un elenco delle azioni eseguite durante la disattivazione, consulta. [Panoramica del processo di smantellamento](#)

Warning

L'eliminazione manuale di tutte le risorse AWS Control Tower non equivale alla disattivazione. Non ti permetterà di creare una nuova landing zone.

I tuoi dati e quelli esistenti non AWS Organizations vengono modificati dal processo di smantellamento, nei seguenti modi.

- AWS Control Tower non rimuove i dati, ma rimuove solo parti della landing zone creata.
- Una volta completato il processo di smantellamento, rimangono alcuni artefatti di risorse, come i bucket Amazon S3 e i gruppi di log Amazon Logs. CloudWatch Queste risorse devono essere eliminate manualmente prima di impostare un'altra landing zone e per evitare possibili costi associati alla gestione di determinate risorse.
- Non è possibile utilizzare la disattivazione automatica per rimuovere una landing zone parzialmente configurata. Se il processo di configurazione della landing zone non riesce, è necessario risolvere lo stato di errore e configurarla fino in fondo per rendere possibile la disattivazione automatica oppure eliminare manualmente le risorse singolarmente.

La disattivazione di una landing zone è un processo con conseguenze significative e non può essere annullata. Le azioni di smantellamento intraprese da AWS Control Tower e gli artefatti che rimangono dopo la disattivazione sono descritti nelle sezioni seguenti.

⚠ Important

Si consiglia vivamente di eseguire questo processo di disattivazione solo se si intende interrompere l'utilizzo della landing zone. Non è possibile ricreare la landing zone esistente dopo averla disattivata.

Panoramica del processo di smantellamento

Quando richiedi la disattivazione della tua landing zone, AWS Control Tower esegue le seguenti azioni.

- Disattiva ogni controllo investigativo abilitato nella landing zone. AWS Control Tower elimina le CloudFormation risorse che supportano il controllo.
- Disattiva ogni controllo preventivo rimuovendo le policy di controllo dei servizi (SCP) da AWS Organizations. Se una policy è vuota (cosa che dovrebbe succedere dopo aver rimosso tutti gli SCP gestiti da AWS Control Tower), AWS Control Tower rimuove ed elimina completamente la policy.
- Elimina tutti i blueprint distribuiti come CloudFormation StackSets
- Elimina tutti i blueprint distribuiti come stack in tutte le regioni. CloudFormation
- Per ogni account fornito, AWS Control Tower esegue le seguenti azioni durante il processo di smantellamento.
 - Elimina i record di ogni account factory dell'account.
 - Revoca le autorizzazioni AWS Control Tower all'account rimuovendo il ruolo IAM creato da AWS Control Tower (a meno che non siano state aggiunte politiche aggiuntive) e ricrea il ruolo IAM standard. `OrganizationAccountAccessRole`
 - Rimuove i record dell'account da AWS Service Catalog
 - Rimuove il prodotto di account factory e il portfolio da AWS Service Catalog.
- Elimina i blueprint per gli account condivisi (Audit e Log Archive).
- Revoca le autorizzazioni AWS Control Tower dagli account condivisi rimuovendo il ruolo IAM creato da AWS Control Tower (a meno che non siano state aggiunte politiche aggiuntive) e ricrea il ruolo IAM. `OrganizationAccountAccessRole`
- Elimina i record relativi agli account condivisi.
- Elimina i record relativi alle OU create dal cliente.
- Elimina i record interni che identificano la regione di origine.

 Note

Dopo la disattivazione, è possibile rimuovere il blueprint VPC Account Factory (BP_ACCOUNT_FACTORY_VPC) per ripulire le route e i gateway NAT, se il VPC non era vuoto.

Come disattivare una landing zone

Per disattivare la landing zone di AWS Control Tower dalla console, segui la procedura indicata qui.

 Note

Ti consigliamo di annullare la gestione degli account registrati prima della disattivazione.

1. Se la baseline di AWS Backup è abilitata su qualsiasi unità organizzativa registrata, disabilitala su tutte le unità organizzative in cui è abilitata prima di disattivare la landing zone. Altrimenti, la disattivazione fallisce. Per istruzioni, consulta l'argomento [the section called “Primo passaggio: disattivare i backup sulle unità organizzative”](#).

Se la disattivazione non è già riuscita per questo motivo, puoi disabilitare la baseline di AWS Backup ed eseguire nuovamente la disattivazione.

2. Vai alla pagina delle impostazioni della zona di atterraggio nella console AWS Control Tower.
3. Scegli Disattiva la tua landing zone all'interno della sezione Disattiva la tua landing zone .
4. Viene visualizzata una finestra di dialogo che spiega l'azione che stai per eseguire, con un processo di conferma obbligatorio. Per confermare l'intenzione di disattivare, è necessario selezionare ogni casella e digitare la conferma come richiesto.

 Important

Il processo di disattivazione non può essere annullato.

5. Se confermi l'intenzione di disattivare la landing zone, verrai reindirizzato alla home page di AWS Control Tower durante la disattivazione. Il processo può richiedere fino a due ore.

Non chiudere gli account dei membri della tua organizzazione mentre è in corso la disattivazione. La disattivazione potrebbe fallire.

6. Una volta completata la disattivazione, è necessario eliminare le risorse rimanenti manualmente prima di configurare una nuova landing zone dalla console AWS Control Tower. Queste risorse rimanenti includono alcuni bucket, organizzazioni e gruppi di CloudWatch log di Amazon S3 specifici.

Note

Queste azioni possono avere conseguenze significative per le tue attività di fatturazione e conformità. Ad esempio, la mancata eliminazione di queste risorse può comportare addebiti imprevisti.

Per ulteriori informazioni sull'eliminazione manuale delle risorse, vedere [Informazioni sulla rimozione delle risorse AWS Control Tower](#).

7. Se intendi configurare una nuova landing zone in una nuova AWS regione, segui questo passaggio aggiuntivo. Immettete il seguente comando tramite la CLI:

```
aws organizations disable-aws-service-access --service-principal  
controltower.amazonaws.com
```

Disattiva la tua landing zone con le API

Il processo di pulizia di tutte le risorse di una landing zone è denominato smantellamento di una landing zone.

Important

Si consiglia vivamente di eseguire questo processo di disattivazione solo se si intende interrompere l'utilizzo della landing zone. Non è possibile ricreare la landing zone esistente dopo averla disattivata.

Per maggiori dettagli sulla disattivazione di una landing zone, incluse informazioni importanti su come AWS Control Tower gestisce i tuoi dati e quelli esistenti AWS Organizations, consulta la pagina.

[Smantellamento di una landing zone di AWS Control Tower](#)

Per disattivare una landing zone, chiama l'`DeleteLandingZoneAPI`. Questa API restituisce un `operationIdentifier`, che puoi quindi utilizzare quando chiami l'`GetLandingZoneOperationAPI` per verificare lo stato dell'operazione di eliminazione.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Output:

```
{
  "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXXX"
}
```

Attività di pulizia manuale necessarie dopo la disattivazione

Questa sezione elenca le attività di pulizia manuale da eseguire dopo la fase iniziale di smantellamento.

- È necessario specificare indirizzi e-mail diversi per gli account Log archive e Audit se si crea una nuova landing zone dopo la disattivazione di una, oppure si segue la procedura per aggiungere i propri account Log Archive o Audit esistenti.
- Il gruppo CloudWatch Logs log, `aws-controltower/CloudTrailLogs`, deve essere eliminato manualmente prima di configurare un'altra landing zone.
- I due bucket Amazon S3 con nomi riservati per i log devono essere rimossi o rinominati manualmente.
- È necessario eliminare o rinominare manualmente le unità organizzative Security e Sandbox esistenti.

Note

Prima di poter eliminare l'organizzazione dell'unità organizzativa AWS Control Tower Security, è necessario eliminare gli account di registrazione e controllo, ma non l'account di gestione. Per eliminare questi account, è necessario [Quando accedere come utente root](#) all'account di controllo e all'account di registrazione ed eliminarli singolarmente.

- Potresti voler eliminare manualmente la configurazione Centro identità AWS IAM (IAM Identity Center) per AWS Control Tower, ma puoi procedere con la configurazione IAM Identity Center esistente.
- Potresti voler rimuovere il VPC creato da AWS Control Tower e rimuovere il set di AWS CloudFormation stack associato.
- Prima di poter configurare una nuova landing zone in una nuova AWS regione, devi seguire questi passaggi aggiuntivi.
 - Immettete il seguente comando tramite la CLI:

```
aws organizations disable-aws-service-access --service-principal  
controltower.amazonaws.com
```

- Elimina la regola gestita rimanente, chiamata `AWSControlTowerManagedRule`, dagli account condivisi e membri per tutte le regioni governate. `AWSControlTowerManagedRule` è una EventBridge regola di Amazon.

Risorse non rimosse durante la disattivazione

La disattivazione di una landing zone non inverte completamente il processo di configurazione di AWS Control Tower. Restano alcune risorse, che possono essere rimosse manualmente.

AWS Organizations

Per i clienti senza AWS Organizations organizzazioni esistenti, AWS Control Tower configura un'organizzazione con una o più unità organizzative (OU). L'unità organizzativa di sicurezza designata e l'unità organizzativa Sandbox creata opzionalmente. Quando si disattiva la landing zone, la gerarchia dell'organizzazione viene mantenuta, come segue:

- Le unità organizzative (OU) create dalla console AWS Control Tower non vengono rimosse.
- Le unità organizzative Security e Sandbox non vengono rimosse.
- L'organizzazione non viene eliminata da AWS Organizations.
- Nessun account AWS Organizations (condiviso, assegnato o di gestione) viene spostato o rimosso.

Centro identità AWS IAM (COSI)

Per i clienti che non dispongono di una directory IAM Identity Center esistente, AWS Control Tower configura IAM Identity Center e configura una directory iniziale. Quando disattivi la landing zone,

AWS Control Tower non apporta modifiche a IAM Identity Center. Se necessario, puoi eliminare manualmente le informazioni dell'IAM Identity Center memorizzate nel tuo account di gestione. In particolare, queste aree sono invariate dalla disattivazione:

- Gli utenti creati con Account Factory non vengono rimossi.
- I gruppi creati dalla configurazione di AWS Control Tower non vengono rimossi.
- I set di autorizzazioni creati da AWS Control Tower non vengono rimossi.
- Le associazioni tra AWS account e set di autorizzazioni IAM Identity Center non vengono rimosse.
- Le directory di IAM Identity Center non vengono modificate.
- Queste policy di IAM Identity Center per AWS Control Tower non vengono rimosse:
 - `AWSControlTowerAdminPolicy`
 - `AWSControlTowerCloudTrailRolePolicy`
 - `AWSControlTowerStackSetRolePolicy`

Roles

Durante la configurazione, AWS Control Tower crea determinati ruoli per te se usi la console o ti chiede di creare questi ruoli se configuri la landing zone tramite le API. Quando disattivi la vostra landing zone, i seguenti ruoli non vengono rimossi:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Note

Il `AWSControlTowerExecution` ruolo negli account dei membri verrà eliminato quando la landing zone viene eliminata, indipendentemente dal fatto che AWS Control Tower abbia creato il ruolo per tuo conto o se lo hai creato manualmente. Tuttavia, se hai associato policy aggiuntive a questo ruolo o modificato le policy associate a questo ruolo, AWS Control Tower potrebbe non essere in grado di eliminare questo ruolo durante l'eliminazione della Landing Zone. In questi casi, l'eliminazione della Landing Zone avrà esito positivo, ma il ruolo verrà mantenuto nell'account membro.

Bucket Amazon S3

Durante la configurazione, AWS Control Tower crea bucket nell'account di archiviazione dei log per AWS CloudTrail e nell'account di aggregazione centrale di configurazione per l'integrazione con AWS Config. AWS Control Tower crea bucket per la registrazione e per la registrazione degli accessi in ciascuno di questi account. Quando si disattiva la landing zone, le seguenti risorse non vengono rimosse:

- I bucket S3 di accesso alla registrazione e alla registrazione nell'account di archivio dei registri non vengono rimossi.
- I bucket S3 di registrazione e accesso alla registrazione nell'account di aggregazione centrale di configurazione non vengono rimossi.
- I contenuti dei bucket di accesso alla registrazione e alla registrazione in ciascuno di questi account non vengono rimossi.

Account di integrazione dei servizi

AWS Control Tower richiede che ogni configurazione di integrazione del servizio disponga di un account centrale. Questo account può essere creato o meno durante la configurazione di AWS Control Tower in base alla versione landing zone. Quando si disattiva la landing zone:

- Gli account di integrazione dei servizi creati durante la configurazione di AWS Control Tower non vengono chiusi.
- Il ruolo `OrganizationAccountAccessRole` IAM viene ricreato per allinearli alla configurazione standard AWS Organizations .
- Il ruolo `AWSControlTowerExecution` viene rimosso.

Account di cui è stato eseguito il provisioning

I clienti di AWS Control Tower possono utilizzare account factory per creare nuovi AWS account. Quando si disattiva la landing zone:

- Gli account di provisioning creati con account factory non vengono chiusi.
- I prodotti forniti non AWS Service Catalog vengono rimossi. Se li ripulisci chiudendoli, i relativi account vengono spostati nell'unità organizzativa principale.
- Il VPC creato da AWS Control Tower non viene rimosso e lo AWS CloudFormation stack set associato (`BP_ACCOUNT_FACTORY_VPC`) non viene rimosso.

- Il ruolo `OrganizationAccountAccessRole` IAM viene ricreato per allinearli alla configurazione standard. AWS Organizations
- Il ruolo `AWSControlTowerExecution` viene rimosso.

CloudWatch Registri (Log Group)

- Un gruppo di CloudWatch log dei registri, `aws-controltower/CloudTrailLogs`, viene creato come parte del blueprint denominato `AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER`. Questo gruppo di log non viene rimosso. Al contrario, il blueprint viene eliminato e le risorse vengono mantenute.

Note

I clienti della landing zone 3.0 e versioni successive non devono eliminare i CloudTrail CloudTrail registri e i ruoli di registro dei singoli account registrati, poiché questi vengono creati solo nell'account di gestione, per il percorso a livello di organizzazione.

A partire dalla versione 3.2 della landing zone, AWS Control Tower crea una EventBridge regola Amazon, chiamata `AWSControlTowerManagedRule`. Questa regola viene creata in ogni account membro, per tutte le regioni governate. La regola non viene eliminata automaticamente durante la disattivazione, quindi è necessario eliminarla manualmente dagli account di integrazione del servizio e dagli account dei membri di tutte le regioni governate prima di poter configurare una landing zone in una nuova regione.

Le procedure per eliminare le risorse di AWS Control Tower sono riportate in [Rimuovi le risorse AWS Control Tower](#).

Rimuovi le risorse AWS Control Tower

Questo documento fornisce istruzioni su come rimuovere singolarmente le risorse AWS Control Tower, nell'ambito di normali attività amministrative e di manutenzione. Le procedure fornite in questo capitolo sono destinate esclusivamente alla rimozione di singole risorse, o di alcune risorse, quando necessario. Non è la stessa cosa che disattivare la landing zone.

La rimozione di risorse può richiedere la rimozione di risorse per due tipi di attività:

- Eliminare le risorse mentre viene gestita la landing zone in situazioni ordinarie.

- Per ripulire le risorse rimaste dopo lo smantellamento automatico.

Warning

La rimozione manuale delle risorse non ti consentirà di configurare una nuova landing zone. Non è la stessa cosa dello smantellamento. Se intendi smantellare la landing zone di AWS Control Tower, segui le istruzioni [Smantellamento di una landing zone di AWS Control Tower](#) prima di intraprendere qualsiasi azione descritta in questo capitolo. Le istruzioni contenute in questo capitolo possono aiutarti a ripulire le risorse rimaste dopo il completamento dello smantellamento automatico. Anche se elimini manualmente tutte le risorse della landing zone, non è come disattivarla e potresti incorrere in addebiti imprevisti.

Se devi rimuovere un account da AWS Control Tower, consulta le seguenti sezioni per chiudere un account:

- [Annullare la gestione di un account](#)
- [Chiudere un account creato in Account Factory](#)

Ho bisogno della disattivazione anziché dell'eliminazione?

Se non intendi più utilizzare AWS Control Tower per la tua azienda o se hai bisogno di una ridistribuzione importante delle risorse organizzative, potresti voler smantellare le risorse create durante la configurazione iniziale della landing zone.

- Una volta completato il processo di smantellamento, rimangono alcuni artefatti di risorse, come i bucket Amazon S3 e i gruppi di log Amazon Logs. CloudWatch
- Devi ripulire manualmente le risorse rimanenti nei tuoi account prima di configurare un'altra landing zone ed evitare la possibilità di addebiti imprevisti. Per ulteriori informazioni, consulta [Risorse non rimosse durante la disattivazione](#).

Warning

Ti consigliamo vivamente di eseguire una procedura di smantellamento solo se intendi smettere di usare la tua landing zone. Questo processo non può essere annullato.

Informazioni sulla rimozione delle risorse AWS Control Tower

Le singole procedure in questo capitolo ti guidano attraverso i metodi manuali per rimuovere le risorse AWS Control Tower. Queste procedure possono essere seguite quando è necessario eliminare una risorsa specifica dalla landing zone.

Prima di eseguire queste procedure, salvo diversa indicazione, devi aver effettuato l'accesso alla Console di gestione AWS nella regione di origine della tua landing zone e devi aver effettuato l'accesso come utente IAM o utente in IAM Identity Center con autorizzazioni amministrative per l'account di gestione che contiene la tua landing zone.

Warning

Si tratta di azioni distruttive che possono introdurre una deriva di governance nella configurazione di AWS Control Tower. Non possono essere annullate.

Argomenti

- [Eliminare SCPs](#)
- [Elimina e impila StackSets](#)
- [Eliminare i bucket Amazon S3 nell'account Log Archive](#)
- [Rimuovi un portafoglio e un prodotto Account Factory](#)
- [Rimuovi i ruoli e le policy di AWS Control Tower](#)
- [Guida alle risorse AWS Control Tower](#)

Eliminare SCPs

AWS Control Tower utilizza le policy di controllo dei servizi (SCPs) per i propri controlli. Questa procedura spiega come eliminare i file SCPs specificamente correlati ad AWS Control Tower.

Eliminare AWS Organizations SCPs

1. Apri la console Organizations all'indirizzo <https://console.aws.amazon.com/organizations/>.
2. Apri la scheda Policies e trova le Service Control Policies (SCPs) che hanno il prefisso aws-guardrails e procedi come segue per ogni SCP:

- a. Scollegare l'SCP dall'unità organizzativa associata.
- b. Eliminare l'SCP.

Elimina e impila StackSets

AWS Control Tower utilizza StackSets e distribuisce i controlli Regole di AWS Config relativi ai controlli nella landing zone. Le seguenti procedure illustrano come eliminare queste risorse specifiche.

Per eliminare CloudFormation StackSets

1. Apri la CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Dal menu di navigazione a sinistra, scegli. StackSets
3. Per ognuno StackSet con il prefisso AWSControlTower, procedi come segue. Se hai molti account in un account StackSet, l'operazione può richiedere del tempo.
 - a. Scegli lo specifico StackSet dalla tabella nella dashboard. Si apre la relativa pagina delle proprietà StackSet.
 - b. Nella parte inferiore della pagina, nella tabella Stacks, registrate l' AWS account IDs per tutti gli account della tabella. Copiare l'elenco di tutti gli account.
 - c. In Azioni, scegli Elimina pile da. StackSet
 - d. In Imposta le opzioni di distribuzione, da Posizioni di distribuzione, scegli Distribuisci gli stack negli account.
 - e. Nel campo di testo, inserisci l' AWS account di IDs cui hai registrato al passaggio 3.b, separato da virgole. Ad esempio: **123456789012**, **098765431098** e così via.
 - f. Da Specify regions (Specifica regioni), scegliere Add all (Aggiungi tutti), lasciare le impostazioni predefinite per il resto dei parametri nella pagina e selezionare Next (Successivo).
 - g. Nella pagina Review (Revisione), rivedere le scelte, quindi selezionare Delete stacks (Elimina stack).
 - h. Nella pagina delle StackSet proprietà, puoi ricominciare questa procedura per l'altro utente. StackSets
4. Il processo è completo quando i record nella tabella Stacks delle diverse pagine delle StackSets proprietà sono vuoti.

5. Quando i record nella tabella Stacks sono vuoti, scegli Elimina. StackSet

Per eliminare le pile CloudFormation

1. Apri la CloudFormation console in <https://console.aws.amazon.com/cloudformation>.
2. Dalla dashboard Stacks, cerca tutti gli stack con il prefisso Tower. AWSControl
3. Per ogni stack nella tabella, eseguire le operazioni seguenti:
 - a. Selezionare la casella di controllo accanto al nome dello stack.
 - b. Dal menu Actions (Operazioni), scegliere Delete Stack (Elimina stack).
 - c. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere Yes, Delete (Sì, Elimina).

Eliminare i bucket Amazon S3 nell'account Log Archive

Le seguenti procedure ti guidano su come accedere all'account di archiviazione dei log come utente IAM Identity Center nel AWSControlTowerExecutiongruppo e quindi eliminare i bucket Amazon S3 nel tuo account di archivio dei log.

Per effettuare l'accesso all'account di archivio dei log con le autorizzazioni corrette

1. Apri la console Organizations all'indirizzo <https://console.aws.amazon.com/organizations/>.
2. Nella scheda Accounts (Account), individuare l'account Log archive (Archivio di log).
3. Dal riquadro destro visualizzato, creare un record del numero dell'account di archivio dei log.
4. Dalla barra di navigazione, scegliere il nome account per aprire il menu account.
5. Seleziona Switch Role (Cambia ruolo).
6. Nella pagina visualizzata, indicare il numero di account per l'account di archivio dei log in Account.
7. Per Ruolo, inserisci AWSControlTowerExecution.
8. Il campo Display Name (Nome visualizzato) viene compilato con testo.
9. Scegliere l'opzione Color (Colore) preferita.
10. Seleziona Switch Role (Cambia ruolo).

Per eliminare i bucket Amazon S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Cercare i nomi dei bucket che contengono aws-controlltower.
3. Per ogni bucket nella tabella, eseguire le operazioni seguenti:
 - a. Selezionare la casella di controllo per il bucket nella tabella.
 - b. Scegli Elimina.
 - c. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate, immettere il nome del bucket per confermare, quindi scegliere Confirm (Conferma).

Rimuovi un portafoglio e un prodotto Account Factory

La procedura seguente illustra come accedere come utente IAM Identity Center nel AWSServiceCatalogAdminsgruppo e quindi ripulire il portafoglio e i prodotti Account Factory.

Per accedere al tuo account di gestione con le autorizzazioni corrette

1. Vai all'URL del tuo portale utente all'indirizzo *directory-id*.awsapps.com/start
2. In Account, trova l'AWS account di gestione.
3. Da AWSServiceCatalogAdminFullAccess, scegli Console di gestione per accedere a Console di gestione AWS As this role.

Per ripulire Account Factory

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Dal menu di navigazione a sinistra, scegliere Portfolios list (Elenco portafogli).
3. Nella tabella Local Portfolios, cercate un portafoglio denominato AWS Control Tower Account Factory Portfolio.
4. Scegliere il nome di tale portafoglio per passare alla pagina dei dettagli.
5. Espandi la sezione Vincoli della pagina e scegli il pulsante di opzione per il vincolo con il nome del prodotto Control Tower AWS Account Factory.
6. Scegliere REMOVE CONSTRAINTS (RIMUOVI VINCOLI).

7. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere CONTINUE (CONTINUA).
8. Dalla sezione Prodotti della pagina, scegli il pulsante di opzione per il prodotto denominato AWS Control Tower Account Factory.
9. Scegliere REMOVE PRODUCT (RIMUOVI PRODOTTO).
10. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere CONTINUE (CONTINUA).
11. Espandere la sezione Users, Groups, and Roles (Utenti, gruppi e ruoli) della pagina e selezionare le caselle di controllo per tutti i record in questa tabella.
12. Scegliere REMOVE USERS, GROUP OR ROLE (RIMUOVI UTENTI, GRUPPO O RUOLI).
13. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere CONTINUE (CONTINUA).
14. Dal menu di navigazione a sinistra, scegliere Portfolios list (Elenco portafogli).
15. Nella tabella Local Portfolios, cercate un portafoglio denominato AWS Control Tower Account Factory Portfolio.
16. Scegliere il pulsante di opzione per tale portafoglio, quindi selezionare DELETE PORTFOLIO (ELIMINA PORTAFOGLIO).
17. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere CONTINUE (CONTINUA).
18. Dal menu di navigazione a sinistra, scegliere Product list (Elenco prodotti).
19. Nella pagina dei prodotti di amministrazione, cerca il prodotto denominato AWS Control Tower Account Factory.
20. Scegliere il prodotto per aprire la pagina Admin product details (Dettagli prodotto amministratore).
21. Da Actions (Operazioni), scegliere Delete product (Elimina prodotto).
22. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere CONTINUE (CONTINUA).

Rimuovi i ruoli e le policy di AWS Control Tower

Queste procedure illustrano come ripulire i ruoli e le policy che AWS Control Tower ha creato al momento della configurazione della landing zone o successivamente.

Per eliminare il AWSService CatalogEndUserAccess ruolo IAM Identity Center

1. Apri la Centro identità AWS IAM console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. Cambia la tua AWS regione con la tua regione di residenza, che è la regione in cui hai inizialmente configurato AWS Control Tower.
3. Dal menu di navigazione a sinistra, scegli AWS account.
4. Scegli il link del tuo account di gestione.
5. Scegli il menu a discesa relativo ai set di autorizzazioni AWSServiceCatalogEndUserAccess, seleziona e quindi scegli Rimuovi.
6. Scegli AWS gli account dal pannello di sinistra.
7. Aprire la scheda Permission sets (Set di autorizzazioni).
8. Selezionalo AWSServiceCatalogEndUserAccessed eliminalo.

Per eliminare i ruoli IAM

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Dal menu di navigazione a sinistra, scegliere Roles (Ruoli).
3. Nella tabella, cerca i ruoli con il nome AWSControlTower.
4. Per ogni ruolo nella tabella, procedere nel modo seguente:
 - a. Selezionare la casella di controllo per il ruolo.
 - b. Scegli Delete role (Elimina ruolo).
 - c. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate e scegliere Yes, Delete (Sì, Elimina).

Per eliminare le policy IAM

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Dal menu di navigazione a sinistra, scegliere Policies (Policy).
3. Nella tabella, cerca le politiche con il nome AWSControlTower.
4. Per ogni policy nella tabella, procedere nel modo seguente:
 - a. Selezionare la casella di controllo per la policy.

- b. Scegliere Policy actions (Operazioni policy) e Delete (Elimina) dal menu a discesa.
- c. Nella finestra di dialogo visualizzata, rivedere le informazioni per assicurarsi che siano accurate, quindi scegliere Delete (Elimina).

Guida alle risorse AWS Control Tower

Se riscontri problemi che non riesci a risolvere quando rimuovi le risorse AWS Control Tower, contatta [AWS Support](#).

Configurazione dopo la disattivazione di una landing zone

Dopo aver disattivato la landing zone, non è possibile eseguire nuovamente l'installazione fino al completamento della pulizia manuale. Inoltre, senza la pulizia manuale di queste risorse rimanenti, è possibile che vengano addebitati costi di fatturazione imprevisti. È necessario occuparsi di questi problemi:

- L'account di gestione AWS Control Tower fa parte dell'unità organizzativa AWS Control Tower Root. Assicurati che questi ruoli IAM e le policy IAM vengano rimossi dall'account di gestione:
 - Ruoli:
 - `AWSControlTowerAdmin`
 - `AWSControlTowerCloudTrailRole`
 - `AWSControlTowerStackSetRole`
 - Policy:
 - `AWSControlTowerAdminPolicy`
 - `AWSControlTowerCloudTrailRolePolicy`
 - `AWSControlTowerStackSetRolePolicy`
- Potresti voler eliminare o aggiornare la configurazione esistente di IAM Identity Center per AWS Control Tower prima di configurare nuovamente una landing zone, ma non è necessario eliminarla.
- Potresti voler rimuovere il VPC creato da AWS Control Tower.
- La configurazione fallisce se gli indirizzi e-mail specificati per gli account di registrazione o di controllo sono associati a un account esistente AWS . Puoi chiudere gli AWS account o utilizzare

indirizzi e-mail diversi per configurare nuovamente una landing zone. In alternativa, puoi riutilizzare questi account condivisi esistenti, con la funzione che ti consente di creare i tuoi account di registrazione e controllo. Per ulteriori informazioni, consulta [Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti](#).

- L'installazione non riesce se nell'account di registrazione sono già presenti bucket Amazon S3 con i seguenti nomi riservati:
 - `aws-controltower-logs-{accountId}-{region}` (utilizzato per il bucket di registrazione).
 - `aws-controltower-s3-access-logs-{accountId}-{region}` (utilizzato per il bucket di accesso alla registrazione).

È necessario rinominare o rimuovere questi bucket oppure utilizzare un account diverso per l'account di registrazione.

- L'installazione fallisce se l'account di gestione ha il gruppo di log esistente, `aws-controltower/CloudTrailLogs`, in Logs. CloudWatch È necessario rinominare o rimuovere il gruppo di log.

Prima di eseguire la configurazione in un nuovo Regione AWS

Se intendi configurare una nuova landing zone in una nuova AWS regione, segui questi passaggi aggiuntivi.

- Immettete il seguente comando tramite la CLI:

```
aws organizations disable-aws-service-access --service-principal  
controltower.amazonaws.com
```

- Elimina la EventBridge regola Amazon rimanente, chiamata `AWSControlTowerManagedRule`, dagli account condivisi e membri per tutte le regioni governate.

Procedure guidate

Questo capitolo contiene procedure dettagliate che possono aiutarti nell'uso di AWS Control Tower.

Argomenti

- [Procedura dettagliata: passaggio da ALZ a AWS Control Tower](#)
- [Procedura dettagliata: configura AWS Control Tower senza un VPC](#)
- [Rimuovi le risorse AWS Control Tower](#)
- [Procedura dettagliata: configura gruppi di sicurezza in AWS Control Tower con AWS Firewall Manager](#)
- [Smantellamento di una landing zone di AWS Control Tower](#)

Procedura dettagliata: passaggio da ALZ a AWS Control Tower

Molti AWS clienti hanno adottato la soluzione [AWS Landing Zone \(ALZ\)](#) per configurare un ambiente sicuro, conforme e con più account. AWS Per ridurre l'onere della gestione di una zona di atterraggio, AWS ha creato il servizio gestito chiamato AWS Control Tower.

Non sono previste funzionalità aggiuntive per ALZ; è disponibile solo con supporto a lungo termine. Pertanto, ti consigliamo di passare al servizio AWS Control Tower da ALZ. Il blog collegato in questo capitolo illustra diverse considerazioni relative al passaggio e spiega come pianificare con successo una migrazione da ALZ ad AWS Control Tower.

Blog: [Migra la soluzione AWS Landing Zone su AWS Control Tower](#)

AWS Prescriptive Guidance offre una documentazione più completa, inclusi i passaggi per la transizione da ALZ ad AWS Control Tower. In sostanza, abiliterai la governance di AWS Control Tower nella tua organizzazione esistente che esegue ALZ, in base a una serie di prerequisiti. Per informazioni, consulta [Transitioning from AWS Landing Zone a AWS Control Tower](#).

Procedura dettagliata: configura AWS Control Tower senza un VPC

Questo argomento illustra come configurare gli account AWS Control Tower senza un VPC.

Se il carico di lavoro non richiede un VPC, puoi procedere come segue:

- Puoi eliminare il cloud privato virtuale (VPC) di AWS Control Tower. Questo VPC è stato creato al momento della configurazione della zona di atterraggio.
- Puoi modificare le impostazioni di Account Factory in modo da creare nuovi account AWS Control Tower senza un VPC associato.

Important

Se esegui il provisioning di account Account Factory con le impostazioni di accesso a Internet VPC abilitate, tale impostazione di Account Factory ha la precedenza sul controllo [Disallow internet access per un'istanza Amazon VPC gestita da un cliente](#). Per evitare di abilitare l'accesso a Internet per i nuovi account di cui è stato effettuato il provisioning, è necessario modificare l'impostazione in Account Factory.

Elimina il VPC di AWS Control Tower

Al di fuori di AWS Control Tower, ogni AWS cliente dispone di un VPC predefinito, che può visualizzare sulla console Amazon Virtual Private Cloud (Amazon VPC) all'indirizzo. <https://console.aws.amazon.com/vpc/> Riconoscerai il VPC predefinito perché il suo nome include sempre il suffisso (default).

Quando configuri una landing zone di AWS Control Tower, AWS Control Tower elimina il tuo VPC AWS predefinito e crea un nuovo VPC predefinito di AWS Control Tower. Il nuovo VPC è associato al tuo account di gestione AWS Control Tower. Questo argomento si riferisce a quel nuovo VPC come Control Tower VPC.

Quando visualizzi il tuo AWS Control Tower VPC nella console Amazon VPC, non vedrai la parola (impostazione predefinita) alla fine del nome. Se disponi di più di un VPC, devi utilizzare l'intervallo CIDR assegnato per identificare il VPC AWS Control Tower corretto.

Puoi eliminare il VPC di AWS Control Tower, ma se in seguito ti servirà un VPC in AWS Control Tower, dovrai crearlo tu stesso.

Per eliminare il VPC di AWS Control Tower

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Cerca **VPC** o seleziona **VPC** dalle opzioni del Service Catalog. Viene quindi visualizzato il VPC Dashboard (Pannello di controllo VPC).

3. Dal menu a sinistra, scegliere Your VPCs (I tuoi VPC). Viene quindi visualizzato un elenco di tutti i tuoi VPC.
4. Identifica AWS Control Tower VPC in base alla sua gamma CIDR.
5. Seleziona il VPC, scegli Actions (Operazioni) e quindi Delete VPC (Elimina VPC).

In ogni regione esiste già un VPC AWS (predefinito) per l'account di gestione di AWS Control Tower. Per seguire le migliori pratiche di sicurezza, se scegli di eliminare il VPC di AWS Control Tower, è consigliabile eliminare anche il VPC AWS predefinito associato all'account di gestione da tutte le regioni. AWS Pertanto, per proteggere l'account di gestione, rimuovi il VPC predefinito da ciascuna regione e rimuovi il VPC creato da Control Tower nella tua regione principale di AWS Control Tower.

Facoltativamente, pulisci la risorsa VPC nell'account

Facoltativamente, per ripulire la risorsa VPC di AWS Control Tower `aws-controltower-VPC`, da un account esistente, puoi rimuovere l'istanza dello stack dal AWS CloudFormation `StackSetAWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`, dopo esserti assicurato che non vi siano risorse o dipendenze di risorse esistenti nel VPC.

Crea un account in AWS Control Tower senza un VPC

Se i carichi di lavoro degli utenti finali non richiedono VPC, puoi utilizzare questo metodo per configurare account utente finale per i quali non sono stati creati VPC automaticamente.

Dalla dashboard di AWS Control Tower, puoi visualizzare e modificare le impostazioni delle configurazioni di rete. Dopo aver modificato le impostazioni in modo che gli account AWS Control Tower vengano creati senza un VPC associato, tutti i nuovi account vengono creati senza un VPC fino a quando non modifichi nuovamente le impostazioni.

Per configurare Account Factory per la creazione di account senza VPC

1. Apri un browser web e accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>.
2. Scegli Account Factory dal menu a sinistra.
3. Viene quindi visualizzata la pagina Account Factory con la sezione Configurazione di rete.
4. Annota le impostazioni correnti qualora desiderassi ripristinarle in un secondo momento.

5. Scegli il pulsante Edit (Modifica) nella sezione Network Configuration (Configurazione di rete).
6. Nella pagina Edit account factory network configuration (Modifica configurazione rete Factory Account), vai alla sezione VPC Configuration options for new accounts (Opzioni di configurazione VPC per i nuovi account).

Puoi seguire l'opzione 1 o l'opzione 2, o entrambe, per assicurarti che AWS Control Tower non crei un VPC durante il provisioning di un account.

a. Opzione 1: rimozione delle sottoreti

- Disattiva l'interruttore a levetta della Internet-accessible sottorete.
- Imposta il valore Maximum number of private subnets (Numero massimo di sottoreti private) a 0.

b. Opzione 2: rimozione AWS Regioni

- Deseleziona tutte le caselle di controllo nella colonna Regions for VPC creation (Regioni per la creazione di VPC).

7. Selezionare Salva.

Possibili errori

Fai attenzione a questi possibili errori che potrebbero verificarsi quando elimini il tuo AWS Control Tower VPC o riconfiguri Account Factory per creare account senza VPC.

- Il tuo account di gestione esistente potrebbe avere dipendenze o risorse nel VPC di AWS Control Tower, il che può causare un errore di cancellazione.
- Se lasci il CIDR predefinito impostato durante la configurazione per l'avvio di nuovi account senza un VPC, la richiesta ha esito negativo con un errore indicante che il CIDR non è valido.

Procedura dettagliata: configura gruppi di sicurezza in AWS Control Tower con AWS Firewall Manager

Il video mostra come utilizzare il servizio AWS Firewall Manager per migliorare la sicurezza della rete per AWS Control Tower. Puoi designare un account amministratore della sicurezza abilitato per impostare i gruppi di sicurezza. Vedrai come configurare le politiche di sicurezza e applicare le regole di sicurezza per le tue organizzazioni AWS Control Tower e come porre rimedio alle risorse

non conformi applicando le policy automaticamente. Puoi visualizzare i gruppi di sicurezza in vigore per ogni account e risorsa (ad esempio un'istanza Amazon EC2) nella tua organizzazione.

Puoi creare policy di firewall personalizzate oppure sottoscrivere le regole di fornitori attendibili.

Configura i gruppi di sicurezza con AWS Firewall Manager

Questo video (8:02) descrive come configurare una migliore sicurezza dell'infrastruttura di rete per le risorse e i carichi di lavoro in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sulla configurazione del firewall in AWS Control Tower.](#)

Per ulteriori informazioni, consulta la [documentazione su come configurare il AWS WAF.](#)

Risoluzione dei problemi

Se riscontri problemi durante l'utilizzo di AWS Control Tower, puoi utilizzare le seguenti informazioni per risolverli secondo le nostre best practice. Se i problemi riscontrati non rientrano nell'ambito delle seguenti informazioni o se persistono dopo aver cercato di risolverli, contatta il servizio di [AWS assistenza](#).

Argomenti

- [Avvio della landing zone non riuscito](#)
- [Aggiornamento della zona di atterraggio non riuscito con errore KMS](#)
- [Impossibile aggiornare la zona di atterraggio](#)
- [Errore relativo alla zona di atterraggio non aggiornata](#)
- [Provisioning del nuovo account non riuscito](#)
- [Registrazione di un account esistente non riuscita](#)
- [Impossibile aggiornare un account di Factory Account](#)
- [Errore, errore che menziona AWS Config](#)
- [Errore nel portafoglio AWS Control Tower Account Factory](#)
- [È stato ricevuto un errore di autorizzazioni insufficienti](#)
- [I controlli investigativi non hanno effetto sugli account](#)
- [Frequenza superata \(errore restituito dal AWS Organizations "Hello, World!"\)](#)
- [Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower](#)
- [AWS Supporto](#)

Avvio della landing zone non riuscito

Cause comuni di fallimento del lancio della landing zone:

- Mancanza di risposta a un messaggio di posta elettronica di conferma.
- CloudFormation StackSet fallimento.

Messaggi e-mail di conferma: se il tuo account di gestione ha meno di un'ora, potresti riscontrare problemi durante la creazione degli account aggiuntivi.

Operazione da eseguire

Se si verifica questo problema, controllare la propria e-mail. Potrebbe essere stata inviata un'e-mail di conferma in attesa di risposta. In alternativa, consigliamo di attendere un'ora, quindi riprovare. Se il problema persiste, contatta l'[AWS assistenza](#).

Fallito StackSets: un'altra possibile causa del fallimento del lancio della landing zone è il CloudFormation StackSet fallimento. AWS Le regioni Security Token Service (STS) devono essere abilitate nell'account di gestione per tutte le AWS regioni governate da AWS Control Tower, in modo che il provisioning possa avere successo; in caso contrario, i set di stack non verranno avviati.

Operazione da eseguire

Assicurati di abilitare tutte le [regioni endpoint AWS Security Token Service \(STS\)](#) richieste prima di avviare AWS Control Tower.

Per correggere i set di stack non riusciti e riprovare la configurazione

1. Accedere alla CloudFormation console nell'area appropriata. Regione AWS
2. Pulisci lo stack fallito con il nome AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER.
3. Attendi il completamento del processo di eliminazione dello stack.
4. Torna alla pagina AWS Control Tower.
5. Seleziona nuovamente Configura landing zone.

Per visualizzare un elenco di Regioni AWS quelli supportati da AWS Control Tower, consulta [In che modo AWS Le regioni funzionano con AWS Control Tower](#).

Aggiornamento della zona di atterraggio non riuscito con errore KMS

La causa più comune di un errore di aggiornamento delle landing zone è una politica AWS KMS chiave non valida.

Motivi comuni per cui una politica chiave KMS non è valida:

- Errore di battitura nella policy.
- Ho dimenticato di aggiungere la dichiarazione politica richiesta.

- AWS Partizione errata.
- Numero di conto errato nella polizza.
- Hai dimenticato di rimuovere i segnaposto nella politica di esempio.

Operazione da eseguire

Rivedi la tua politica per verificare la presenza di questi errori.

Per ulteriori informazioni sulle politiche AWS KMS chiave, consulta [Configurazione delle chiavi KMS](#) e [Prerequisiti di Backup](#).

Impossibile aggiornare la zona di atterraggio

AWS Control Tower non torna a una versione precedente di landing zone se un aggiornamento fallisce. Potresti trovare la tua landing zone in uno stato indeterminato. In tal caso, contatta l' AWS assistenza.

Gli aggiornamenti delle zone di atterraggio potrebbero non riuscire per diversi motivi.

- Prerequisiti non soddisfatti
- AWS Config esistono risorse in determinati account
- esistono conti chiusi

Prerequisiti non soddisfatti

Un aggiornamento della landing zone deve soddisfare gli stessi prerequisiti della configurazione di una landing zone. Prima di effettuare l'aggiornamento, esamina i controlli effettuati [prima del lancio](#).

AWS Config esistono risorse negli account Security OU

Non aggiungere AWS Config risorse agli account Audit e Log Archive. Il processo di aggiornamento delle landing zone non può essere completato con queste risorse presenti. Queste restrizioni sono simili a quelle relative alla registrazione di un account o alla configurazione di una landing zone per la prima volta. Per ulteriori informazioni, consulta [Registrare account che dispongono di risorse esistenti AWS Config](#).

Esistono account chiusi

Quando un account è in uno stato Chiuso o Sospeso, potresti riscontrare un problema quando tenti di aggiornare la tua landing zone. È necessario eliminare il prodotto fornito su ogni account chiuso prima di eseguire un aggiornamento della landing zone.

Nella pagina del prodotto AWS Service Catalog fornito, è possibile che venga visualizzato un messaggio di errore simile al seguente:

```
AWSControlTowerExecution role can't be assumed on the account.
```

Causa comune: hai sospeso un account senza eliminare il prodotto fornito.

Azione da intraprendere: se visualizzi questo errore, hai due opzioni:

1. Contatta l'AWS assistenza e riapri l'account, elimina il prodotto fornito, quindi chiudi nuovamente l'account.
2. Rimuovi le risorse StackSets che sono rimaste orfane a causa della chiusura dell'account.
(Questa opzione è disponibile solo se StackSets hanno istanze nello stato Corrente che non stai rimuovendo).

Per rimuovere le risorse da StackSets, procedi nel seguente modo per ogni account chiuso:

- Accedi a ciascuna delle AWS Control Tower StackSets e rimuovi StackInstances da ogni regione, per l'account che è stato chiuso.
- **IMPORTANTE:** scegli l'opzione Retain Stack in modo da StackSet rimuovere solo le istanze dello stack. StackSet non può assumere un ruolo dall'account chiuso, quindi fallirà se tenta di assumere il AWSControlTowerExecution ruolo, il che porta al messaggio di errore che hai ricevuto.

Errore relativo alla zona di atterraggio non aggiornata

Se non hai aggiornato la tua landing zone di recente, potresti ricevere un errore quando tenti di riottenere l'accesso ad AWS Control Tower. Potresti visualizzare un messaggio di errore simile a questo:

```
Unable to access Control Tower
```

Il tuo account è inattivo da troppo tempo. A causa dell'inattività, è necessario aggiornare la landing zone per accedere ad AWS Control Tower.

Tuttavia, l'aggiornamento della landing zone potrebbe non riuscire.

Passaggi da eseguire

Accedi all'account di gestione della tua organizzazione e accedi come utente root. Il tuo utente IAM o utente in IAM Identity Center deve disporre delle autorizzazioni di amministratore di AWS Control Tower e far parte del AWSControlTowerAdminsgruppo. Quindi riprova a eseguire l'aggiornamento.

Provisioning del nuovo account non riuscito

Se si verifica questo problema, controlla queste cause comuni.

Quando hai compilato il modulo di provisioning dell'account, potresti aver:

- specificato tagOptions,
- abilitato notifiche SNS,
- abilitato le notifiche dei prodotti sottoposti a provisioning.

Riprova a effettuare il provisioning del tuo account, senza specificare nessuna di queste opzioni. Per ulteriori informazioni, consulta [Esegui il provisioning degli account nella console Service Catalog, con Account Factory](#).

Altre cause comuni di errore:

- Se hai creato il piano di un prodotto sottoposto a provisioning (per visualizzare le modifiche alle risorse), il provisioning dell'account potrebbe rimanere nello stato In progress (In corso) a tempo indeterminato.
- La creazione di un nuovo account in Account Factory avrà esito negativo mentre sono in corso altre modifiche alla configurazione di AWS Control Tower. Ad esempio, mentre è in esecuzione un processo per aggiungere un controllo a un'unità organizzativa, Account Factory visualizzerà un messaggio di errore se si tenta di effettuare il provisioning di un account.

Per verificare lo stato di un'azione precedente in AWS Control Tower

- Vai a AWS CloudFormation > StackSets
- Controlla ogni set di stack relativo ad AWS Control Tower (prefisso: "«AWSControlTower)
- Cerca CloudFormation StackSets le operazioni ancora in esecuzione.

Se il provisioning dell'account richiede più di un'ora, è consigliabile terminare il processo di provisioning e riprovare.

Registrazione di un account esistente non riuscita

Se provi una volta a registrare un AWS account esistente e l'iscrizione fallisce, quando provi una seconda volta, il messaggio di errore potrebbe indicare che lo stack set esiste. Per continuare, è necessario rimuovere il prodotto fornito da Account Factory.

Se il motivo del primo errore di registrazione è stato la mancata creazione del ruolo `AWSControlTowerExecution` nell'account in anticipo, il messaggio di errore che verrà visualizzato correttamente indica di creare il ruolo. Tuttavia, quando si tenta di creare il ruolo, è probabile che venga visualizzato un altro messaggio di errore che indica che AWS Control Tower non è in grado di creare il ruolo. Questo errore si verifica perché il processo è stato parzialmente completato.

In questo caso, è necessario eseguire due passaggi di ripristino prima di poter procedere con la registrazione dell'account esistente. Innanzitutto, è necessario terminare il prodotto fornito da Account Factory tramite la AWS Service Catalog console. Successivamente, è necessario utilizzare la AWS Organizations console per spostare manualmente l'account dall'unità organizzativa e riportarlo alla directory principale. Al termine, creare il ruolo `AWSControlTowerExecution` nell'account, quindi compilare nuovamente il modulo Enroll account (Registra account).

Un'altra possibile causa di errore di registrazione è che l'account dispone di risorse Config esistenti. AWS In tal caso, consulta [Registrazione account che dispongono di AWS Config risorse esistenti](#) per istruzioni su come modificare le risorse esistenti.

Impossibile aggiornare un account di Factory Account

Quando uno stato dell'account non è coerente, non può essere aggiornato correttamente da Account Factory o AWS Service Catalog.

Caso 1: È possibile che venga visualizzato un messaggio di errore simile a questo:

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

Causa comune: AWS Control Tower rimuove sempre il VPC AWS predefinito durante il provisioning iniziale. Per avere un VPC AWS predefinito in un account, devi aggiungerlo dopo la creazione

dell'account. AWS Control Tower dispone di un proprio VPC predefinito che sostituisce il AWS VPC predefinito, a meno che non si configuri Account Factory come mostrato nella procedura dettagliata, in modo che AWS Control Tower non fornisca affatto un VPC. Pertanto l'account non avrà il VPC. È necessario aggiungere nuovamente il VPC AWS predefinito se si desidera utilizzare quello.

Tuttavia, AWS Control Tower non supporta il AWS VPC predefinito. La distribuzione fa sì che l'account entri in uno stato Tainted. Quando si trova in quello stato, non è possibile aggiornare l'account tramite AWS Service Catalog.

Operazione da eseguire: è necessario eliminare il VPC predefinito aggiunto e quindi sarà possibile aggiornare l'account.

Note

Lo Tainted stato causa un problema successivo: un account non aggiornato può impedire l'attivazione dei controlli sull'unità organizzativa di cui fa parte.

Caso 2: è possibile che venga visualizzato un messaggio di errore simile a questo:

`AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.`

Causa comune: si è tentato di spostare un account da un'unità organizzativa registrata a un'altra, ma le vecchie regole di AWS Config rimangono invariate. Lo stato dell'account non è coerente.

Azioni da intraprendere:

Se lo spostamento dell'account era previsto:

- Chiudi l'account in Service Catalog.
- Registralo di nuovo.
- Context/impact: le regole di AWS configurazione distribuite non corrispondono alla configurazione dettata dall'unità organizzativa di destinazione.
- AWS Le regole di Config possono rimanere quelle dell'unità organizzativa precedente, causando spese indesiderate.
- I tentativi di registrare nuovamente o aggiornare l'account falliranno a causa di conflitti di denominazione delle risorse.

Se lo spostamento dell'account non è stato intenzionale:

- Riporta l'account alla sua unità organizzativa originale.
- Aggiorna l'account da Service Catalog.
- Nei parametri di avvio, inserisci l'unità organizzativa in cui si trovava originariamente l'account.
- Context/impact: Se l'account non viene riportato alla sua unità organizzativa originale, il suo stato non sarà coerente con i controlli dettati dalla nuova unità organizzativa in cui si trova.
- L'aggiornamento di un account non è una soluzione valida, in quanto non elimina AWS Config le regole associate all'unità organizzativa precedente.

Errore, errore che menziona AWS Config

Se AWS Config è abilitato in qualsiasi AWS regione supportata da AWS Control Tower, potresti ricevere un messaggio di errore perché un controllo preliminare non è riuscito. Il messaggio potrebbe non spiegare adeguatamente il problema, a causa di alcuni comportamenti di base di AWS Config

È possibile che venga visualizzato un messaggio di errore analogo a uno dei seguenti:

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again`
.
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again`
.

Causa comune: quando il AWS Config servizio è abilitato su un AWS account, crea un registratore di configurazione e un canale di distribuzione con un nome predefinito. Se si disabilita il AWS Config servizio tramite la console, il registratore di configurazione o il canale di distribuzione non vengono eliminati. È necessario eliminarli tramite la CLI o modificarli per l'utilizzo di AWS Control Tower. Se il AWS Config servizio è abilitato in una qualsiasi delle regioni supportate da AWS Control Tower, può verificarsi questo errore.

Se l'account dispone di risorse AWS Config esistenti, consulta [Registrazione account che dispongono di AWS Config risorse esistenti](#) per istruzioni su come modificare le risorse esistenti.

Operazione da intraprendere: eliminare il recorder di configurazione e il canale di distribuzione in tutte le regioni supportate. La disabilitazione di AWS Config non è sufficiente, il registratore di configurazione e il canale di consegna devono essere eliminati tramite la CLI. Dopo aver eliminato il registratore di configurazione e il canale di distribuzione dalla CLI, puoi riprovare ad avviare AWS Control Tower e registrare l'account.

Se stai distribuendo un prodotto fornito, devi eliminarlo prima di riprovare. In caso contrario, è possibile che venga visualizzato un messaggio di errore simile a questo:

- An error occurred (**InvalidParametersException**) when calling the **ProvisionProduct** operation: A stack named *Stackname* already exists.

Nel messaggio, *Stackname* specifica il nome dello stack.

Ecco alcuni esempi di comandi AWS Config CLI che è possibile utilizzare per determinare lo stato del registratore di configurazione e del canale di distribuzione.

Comandi di visualizzazione:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- The normal response is something like "name": "default"

Elimina comandi:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Per ulteriori informazioni, consulta il AWS Config documentazione

- [Gestione del Configuration Recorder \(AWS CLI\)](#)

-

Gestione del Canale di Distribuzione

Errore nel portafoglio AWS Control Tower Account Factory

Quando cerchi di creare, registrare o aggiornare un account, potresti visualizzare uno dei seguenti messaggi di errore:

```
Your AWS IAM identity does not have access to the AWS Control Tower Account Factory portfolio in AWS Service Catalog. To resolve this, an administrator must associate your AWS IAM identity with the portfolio.
```

or

```
No launch paths found for resource: prod-xxxx
```

Cause comuni:

- È possibile che tu abbia effettuato l'accesso come utente root. AWS Control Tower non supporta la creazione di account quando si effettua l'accesso come utente root.
- Il tuo utente IAM Identity Center non è stato aggiunto al gruppo di autorizzazioni appropriato. Potrebbe essere necessario aggiungere il tuo utente IAM Identity Center a uno di questi gruppi di autorizzazioni: AWSAccountFactory(per l'accesso da parte dell'utente finale) o AWSServiceCatalogAdmins(per l'accesso da amministratore).
- Se sei autenticato come utente IAM, devi [aggiungerlo al AWS Service Catalog portafoglio in modo che disponga delle](#) autorizzazioni corrette.
- Questo problema si verifica anche se disponi delle autorizzazioni corrette, ma viene rilevata una deriva da AWS Control Tower ed è necessaria una riparazione della deriva. Per riparare la maggior parte dei tipi di deriva, scegli Ripristina nella pagina delle impostazioni della zona di atterraggio.

È stato ricevuto un errore di autorizzazioni insufficienti

È possibile che il tuo account non disponga delle autorizzazioni necessarie per eseguire determinate operazioni in alcuni casi. AWS Organizations Se riscontri il seguente tipo di errore, controlla tutte le aree di autorizzazione, ad esempio le autorizzazioni IAM o IAM Identity Center, per assicurarti che l'autorizzazione non venga negata da quelle aree:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

[Se ritieni che il tuo lavoro richieda l'azione che stai tentando e non riesci a individuare alcuna restrizione pertinente, contatta l'amministratore di sistema o il servizio di assistenza AWS .](#)

I controlli investigativi non hanno effetto sugli account

Se hai recentemente esteso la distribuzione di AWS Control Tower in una nuova AWS regione, i nuovi controlli investigativi applicati non hanno effetto sui nuovi account creati in nessuna regione finché i singoli account all'interno delle unità organizzative governate da AWS Control Tower non vengono aggiornati. I controlli investigativi esistenti sugli account esistenti sono ancora in vigore.

Se provi ad attivare un controllo investigativo prima di aggiornare i tuoi account, potresti visualizzare un messaggio di errore simile al seguente:

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Azione da intraprendere: aggiorna gli account.

Per aggiornare i tuoi account dalla console AWS Control Tower, consulta [Quando aggiornare le unità organizzative e gli account AWS Control Tower](#).

Per aggiornare più account individuali in modo programmatico, puoi utilizzare le API e la AWS Service Catalog AWS CLI per automatizzare gli aggiornamenti. Per ulteriori informazioni su come affrontare il processo di aggiornamento, vedere questo [Procedura guidata: video](#). Puoi sostituire l'API con l'UpdateProvisionedProductAPI mostrata nel ProvisionProductvideo.

Se hai ulteriori difficoltà ad abilitare i controlli investigativi sui tuoi account, contatta il [AWS servizio clienti](#).

Frequenza superata (errore restituito dal AWS Organizations "Hello, World!")

Possibile causa

Il tuo carico di lavoro era in esecuzione mentre AWS Control Tower eseguiva una scansione giornaliera per verificare se i tuoi SCP fossero andati alla deriva.

Passaggi da seguire

Se riscontri una limitazione o un `rate exceeded` errore dell'API, prova questi passaggi:

- Esegui i tuoi carichi di lavoro in un momento diverso. (Fai riferimento alla pianificazione della scansione dell'invarianza SCP di AWS Control Tower per regione per scoprire quando AWS Control Tower esegue le sue scansioni di audit.)
- Se chiami le API direttamente tramite HTTP: utilizza l' AWS SDK, che riprova automaticamente le azioni non riuscite
- Richiedi un aumento del limite tramite [Service Quotas and Support](#) AWS

Un esempio di istruzioni per la risoluzione dei problemi relativi alla limitazione delle API in Elastic Beanstalk è disponibile qui: <https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/>

Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower

Warning

Questa pratica non soddisfa i prerequisiti per la registrazione di account idonei, poiché gli account idonei devono far parte della stessa AWS Organization generale e ogni organizzazione può avere una sola landing zone. Se hai provato a eseguire questa azione e ti accorgi di ricevere più messaggi di errore, ecco alcune informazioni che potrebbero esserti utili.

Per spostare un account di cui hai effettuato il provisioning tramite Account Factory in un'altra landing zone gestita da AWS Control Tower, con un altro account di gestione, devi rimuovere tutti i ruoli IAM e gli stack associati a quell'account dall'unità organizzativa originale. Rimuovi queste risorse da ogni regione in cui è distribuito l'account.

Note

Il modo migliore per rimuovere le risorse consiste nel deprovisioning dell'account nell'unità organizzativa originale prima di provare a spostarlo.

Se non si rimuovono le risorse, l'iscrizione alla nuova unità organizzativa fallirà, in modo alquanto spettacolare. È possibile che vengano visualizzati uno o più messaggi di errore e continuerai a ricevere messaggi di errore simili fino a quando i ruoli e gli stack rimanenti non verranno rimossi da ogni regione in cui è stato distribuito l'account.

Ogni volta che si riceve un messaggio di errore, è necessario rimuovere l'account dalla nuova unità organizzativa, eliminare la vecchia risorsa oggetto del messaggio di errore e quindi tentare di riportare l'account nella nuova unità organizzativa. Questo processo di rimozione ed eliminazione deve essere ripetuto per ogni risorsa rimanente, per ogni regione in cui è stato distribuito l'account, possibilmente 10 o 20 volte. Questi errori ripetuti si verificano perché l'account è stato assegnato a un'unità organizzativa con un SCP che impedisce l'eliminazione del ruolo IAM. Puoi abbreviare il processo di ripristino eliminando tutte le risorse dell'account prima di riprovare.

Gli esempi seguenti rappresentano i tipi di messaggi di errore che potresti ricevere se rimangono ruoli e stack non eliminati. Molto probabilmente vedrai uno di questi messaggi alla volta, per ogni volta che tenti di registrare l'account, purché rimangano risorse obsolete.

I valori delle stringhe ID delle risorse sono stati modificati per gli esempi. I loro valori non saranno gli stessi in un messaggio di errore che potresti ricevere. È possibile che venga visualizzato un messaggio simile ai seguenti esempi:

- AWS Control Tower cannot create the IAM role *aws-controltower-AdministratorExecutionRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ConfigRecorderRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ForwardSnsNotificationRole* because the role already exists. To continue, delete the existing IAM role and try again.

Oppure potresti visualizzare un messaggio di errore relativo a un errore di stack set, simile a questo:

```
"Error\":"StackSetFailState",
"Cause\":"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
```

```

here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
    stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
    stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.

```

Una volta rimosse tutte le risorse rimanenti dalla prima unità organizzativa, sarà possibile invitare, fornire o registrare correttamente l'account nella nuova unità organizzativa.

AWS Supporto

Se desideri spostare gli account membro esistenti in un piano di supporto diverso, puoi accedere a ciascun account con le credenziali dell'account root, [confrontare i piani](#) e impostare il livello di supporto desiderato.

Si consiglia di aggiornare l'MFA e i contatti per la sicurezza dell'account quando si apportano modifiche al piano di supporto.

Tipi di linee di base

Una linea di base in AWS Control Tower è un gruppo di risorse e configurazioni specifiche che puoi applicare a un target. L'obiettivo di base più comune può essere un'unità organizzativa (OU). Ad esempio, puoi abilitare una linea di base con un'unità organizzativa selezionata come destinazione, per registrarla in AWS Control Tower.

Durante la configurazione della landing zone, AWS Control Tower abilita automaticamente determinate linee di base sugli account di integrazione dei servizi. Abilita e aggiorna queste linee di base in base alle impostazioni e alle configurazioni della landing zone. AWS Control Tower crea e distribuisce le risorse sull'obiettivo nel modo specificato dalla baseline.

Quando abiliti una linea di base su una destinazione, la baseline viene rappresentata come una risorsa AWS, chiamata `risorsaEnabledBaseline`.

AWS Control Tower include due tipi generali di linee di base:

- Linee di base che possono essere abilitate su un'unità organizzativa.
- Linee di base che possono essere abilitate sugli account di integrazione dei servizi, durante la configurazione delle landing zone.

Tipi di base applicabili a livello di unità organizzativa

Note

Solo le linee di base applicabili a livello di unità organizzativa possono essere abilitate direttamente con l'API. `EnableBaseline`

- Nome: `AWSControlTowerBaseline`

Descrizione: questa baseline imposta le risorse e i controlli per gli account dei membri all'interno dell'unità organizzativa di destinazione, necessari per il monitoraggio della conformità, il controllo, il monitoraggio della sicurezza e, facoltativamente, la gestione degli accessi. Questa linea di base è abilitata quando registri un'unità organizzativa in AWS Control Tower.

Prerequisito: l'integrazione con AWS Config deve essere abilitata nella landing zone di AWS Control Tower.

Considerazione: questa linea di base mantiene le impostazioni della landing zone Region deny control. In altre parole, se una regione non è autorizzata a livello di landing zone, tale regione non è autorizzata per quell'unità organizzativa quando si chiama l'EnableBaselineAPI per registrare un'unità organizzativa.

Note

La OU-level Region nega il controllo non ha modo di autorizzare le Regioni che la landing zone Region nega il controllo non consente.

Per ulteriori informazioni, vedi [Come funzionano gli SCP con deny](#) nella documentazione. AWS Organizations

Raccomandazione: ti consigliamo di confermare le regioni in cui l'unità organizzativa di destinazione potrebbe eseguire carichi di lavoro e di confrontare i risultati con la landing zone Region deny control prima di chiamare l'EnableBaselineAPI per l'unità organizzativa, altrimenti potresti perdere l'accesso alle risorse in determinate regioni.

- Nome: ConfigBaseline

Descrizione: questa linea di base configura le risorse relative ad AWS Config per gli account dei membri all'interno dell'unità organizzativa di destinazione necessarie per l'abilitazione di Detective Controls. Le risorse impostate sono un sottoinsieme di risorse di. AWSControlTowerBaseline

Prerequisito: l'integrazione con AWS Config deve essere abilitata nella landing zone di AWS Control Tower.

Considerazione: questa linea di base non mantiene le impostazioni della landing zone Region deny control. Il Region Deny Control non verrà abilitato come parte dell'attivazione. ConfigBaseline

Limitazione: AWSControlTowerBaseline e ConfigBaseline non può essere abilitato sulla stessa unità organizzativa. Solo una di esse è consentita su un'unità organizzativa.

ConfigBaseline stato di «Non abilitato»

Se l'unità organizzativa è AWSControlTowerBaseline abilitata, lo ConfigBaseline stato viene visualizzato come «Non abilitato». Si tratta di un comportamento previsto. AWSControlTowerBaseline include AWS Config funzionalità. Non è necessario

abilitarlo separatamente ConfigBaseline su unità organizzative che lo hanno già fattoAWSControlTowerBaseline.

- Nome: BackupBaseline

Descrizione: questa linea di base imposta risorse e controlli per gli account dei membri all'interno dell'unità organizzativa di destinazione. Questi sono necessari affinché l'integrazione con AWS Backup possa automatizzare il backup dei dati e centralizzare Servizi AWS la gestione delle policy di backup.

Prerequisiti:

- L'integrazione con AWS Backup deve essere abilitata nella landing zone di AWS Control Tower.
- L'integrazione con AWS Config deve essere abilitata nella landing zone di AWS Control Tower.
- AWSControlTowerBaseline deve essere abilitato sull'unità organizzativa di destinazione.

Considerazione: prima di abilitare l'BackupBaseline unità organizzativa di destinazione, assicurati che AWSControlTowerBaseline sia abilitata sull'unità organizzativa di destinazione. Cioè, l'unità organizzativa di destinazione deve essere registrata in AWS Control Tower.

- Puoi scegliere di attivarla AWS Backup durante il processo di creazione della landing zone AWS Control Tower o durante un processo di aggiornamento della landing zone.
- BackupBaseline È compatibile con le versioni 3.1 e successive della landing zone.
- Non BackupBaseline viene applicato all'account di gestione.

Tipi di base che si applicano agli account di integrazione dei servizi durante la configurazione delle landing zone

AWS Control Tower abilita determinate linee di base sugli account di integrazione dei servizi, come parte del processo di configurazione e aggiornamento delle landing zone. Le linee di base per la tua landing zone possono cambiare man mano che modifichi le impostazioni della landing zone. Ad esempio, se opti per IAM Identity Center, AWS Control Tower può abilitare l'ultima versione della IdentityCenterBaseline baseline sulla tua landing zone.

Puoi visualizzare le linee di base abilitate per la tua landing zone con la chiamata ListEnabledBaselines API.

 Note

A partire dalla versione 4.0 di Landing Zone, AuditBaseline viene sostituita da due linee di base distinte: e. CentralSecurityRolesBaseline CentralConfigBaseline

- Nome: CentralConfigBaseline

Descrizione: configura risorse centrali per il monitoraggio e il controllo della conformità all'interno dell'organizzazione utilizzando AWS Config.

- Nome: CentralSecurityRolesBaseline

Descrizione: configura risorse centrali per il monitoraggio della sicurezza all'interno dell'organizzazione.

- Nome: AuditBaseline

Descrizione: configura le risorse per monitorare la sicurezza e la conformità degli account dell'organizzazione.

- Nome: LogArchiveBaseline

Descrizione: configura un archivio centrale per i registri delle attività delle API e delle configurazioni delle risorse degli account dell'organizzazione.

- Nome: IdentityCenterBaseline

Descrizione: configura risorse condivise per IAM Identity Center, che prepara l'accesso AWSControlTowerBaseline a Identity Center per gli account.

Considerazione: questa linea di base funziona solo se hai selezionato IAM Identity Center come provider di identità al momento della configurazione iniziale della landing zone, o se successivamente modifichi le impostazioni della landing zone per abilitare IAM Identity Center per la tua landing zone. Se utilizzi un provider di identità diverso, non avrai accesso per abilitare questa linea di base.

- Nome: BackupCentralVaultBaseline

Descrizione: configura il AWS Backup vault centrale dell'organizzazione.

- Nome: BackupAdminBaseline

Descrizione: configura l'amministratore delegato e l' AWS Backup Audit Manager.

Registrazione parziale degli account

Quando si utilizzano le linee di base, è possibile inserire un account in uno stato denominato Registrato parzialmente.

Questo stato può verificarsi se registri nuovamente un'unità organizzativa chiamando l'`ResetEnabledBaselineAPI`, poiché AWS Control Tower applica solo le risorse obbligatorie agli account nell'unità organizzativa di destinazione. Un account a cui mancano le risorse (controlli) opzionali per l'unità organizzativa principale è contrassegnato come Parzialmente registrato.

Se sposti un account non registrato in un'unità organizzativa registrata e poi richiami l'`ResetEnabledBaselineAPI` sull'unità organizzativa per registrare quell'account, AWS Control Tower applica le risorse associate `AWSControlTowerBaseline` all'account appena registrato. Tuttavia, i controlli opzionali abilitati per questa unità organizzativa non vengono applicati all'account. L'account rimane in uno stato di registrazione parziale.

Per registrare completamente l'account, scegli Re-registro aggiorna l'account nella console. Quando selezioni queste operazioni dalla console, AWS Control Tower applica tutte le risorse di quell'unità organizzativa all'account appena registrato, inclusi i controlli opzionali attivati per quell'unità organizzativa.

Variazione nelle operazioni tra la console AWS Control Tower e le API per le linee di base

Quando modifichi lo stato di governance di un'unità organizzativa, la console AWS Control Tower esegue automaticamente più operazioni per te, rispetto alla modifica della governance tramite le API per le linee di base.

Differenze

- Registrazione e fornitura di prodotti

Quando registri un'unità organizzativa tramite la console, AWS Control Tower crea prodotti Service Catalog per gli account dei membri dell'unità organizzativa, come parte della registrazione di ciascun account. Quando si registra un'unità organizzativa tramite l'`EnableBaselineAPI` e `AWSControlTowerBaseline`, AWS Control Tower non crea prodotti forniti per gli account dei membri nell'unità organizzativa.

- Annullare la registrazione di un'unità organizzativa

Ogni volta che annulli la registrazione di un'unità organizzativa, devi prima rimuovere tutti gli account membro e le OU annidate. Quindi, AWS Control Tower rimuove tutti i controlli applicati all'unità organizzativa.

- Se si seleziona Elimina l'unità organizzativa dalla console, AWS Control Tower procede all'annullamento della registrazione e quindi all'eliminazione dell'unità organizzativa dall'organizzazione.
- Tuttavia, se annulli la registrazione dell'unità organizzativa chiamando l'`DisableBaselineAPI` per rimuoverla `AWSControlTowerBaseline` dall'unità organizzativa, AWS Control Tower non elimina l'unità organizzativa dall'organizzazione, ma è ancora presente nell'organizzazione, non registrata.

Linee di base e account dei membri abilitati

Quando si abilita una baseline su un'unità organizzativa, tale configurazione viene ereditata dagli account membri dell'unità organizzativa. A causa del fatto di ereditarietà, quando ci riferiamo all'account la chiamiamo baseline abilitata ai figli. La linea di base applicata all'unità organizzativa è denominata baseline abilitata ai genitori. La baseline abilitata al genitore controlla la configurazione delle relative linee di base abilitate per i figli. È simile al modo in cui un controllo, quando abilitato su un'unità organizzativa, si applica a ogni account all'interno dell'unità organizzativa.

Visualizza lo stato di base di un account

AWS Control Tower non consente di indirizzare gli account direttamente con linee di base. Tuttavia, puoi monitorare lo stato di attivazione e di deviazione di ciascun account membro utilizzando le linee di base ereditate relative all'abilitazione dei figli. Per visualizzare lo stato dei tuoi account, puoi chiamare l'API con il [ListEnabledBaselines](#) flag di funzionalità. `includeChildren`

Disattiva la linea di base di un account

AWS Control Tower non consente di disabilitare una baseline abilitata per i figli collegata a una baseline abilitata per i genitori. Una linea di base abilitata ai figli può essere disabilitata se è stata modificata in base all'ereditarietà e non è più collegata a una linea di base abilitata ai genitori.

Linee di base e impostazioni predefinite per il controllo delle versioni

Se la tua landing zone AWS Control Tower è già configurata e scegli di abilitare una landing zone di base, AWS Control Tower abilita la versione più recente della linea di base compatibile con la versione della tua landing zone. Se scegli di abilitare una baseline per un'unità organizzativa che non è già registrata presso AWS Control Tower, AWS Control Tower fornisce automaticamente l'ultima versione compatibile della linea di base per quell'unità organizzativa.

Compatibilità delle versioni di base delle unità organizzative e delle landing zone

Le linee di base di AWS Control Tower ti consentono di impostare uno standard di governance a livello di unità organizzativa, anziché a livello di landing zone, se la tua azienda lo richiede. La linea di base chiamata `AWSControlTowerBaseline` è disponibile per aiutarti a registrare le unità organizzative con AWS Control Tower.

Note

Una baseline è un gruppo di controlli e risorse che collaborano per stabilire un ambiente di governance stabile all'interno della landing zone.

Quando abiliti una baseline su un'unità organizzativa, richiamando l'`EnableBaselineAPI` in AWS Control Tower, devi specificare una versione di base compatibile con la versione corrente della landing zone di AWS Control Tower. Dopo aver specificato una linea di base, tutti gli account dei membri di un'unità organizzativa seguono la linea di base fornita per l'unità organizzativa. In altre parole, ai nuovi account viene fornita la linea di base aggiornata e gli account dei membri esistenti vengono regolati in base alla nuova linea di base.

Se non si seleziona una linea di base per le unità organizzative e gli account esistenti, la versione della landing zone determina l'intero assetto di governance, per impostazione predefinita. Tuttavia, a ciascuna unità organizzativa registrata nella zona di atterraggio viene assegnata una versione di base, che è la versione di base più recente compatibile con la versione corrente della landing zone. Pertanto, a ciascuna unità organizzativa e a ogni account membro registrato è associata una linea di base, anche se non viene mai assegnata una linea di base specifica.

Per quanto riguarda la OU-level linea di base `AWSControlTowerBaseline`, la tabella che segue mostra la compatibilità delle linee di base con le versioni delle landing zone di AWS Control Tower.

Versione di base	Versioni della zona di atterraggio	Progetti inclusi	Modifica rispetto alla linea di base precedente		
1.0	Da 2,0 a 2,7	BP_BASELI NE_CLOUDT RAIL, BP_BASELI NE_CLOUDW ATCH, BP_BASELI NE_CONFIG , BP_BASELI NE_ROLES, BP_BASELI NE_SERVIC E_ROLES, risorse IAM	Nessuno		
2.0	da 2,8 a 2,9	BP_BASELI NE_CLOUDT RAIL, BP_BASELI NE_CLOUDW ATCH, BP_BASELI NE_CONFIG , BP_BASELI NE_ROLES, BP_BASELI NE_SERVIC E_ROLES,	Aggiunto il ruolo AWS Config collegato al servizio (SLR) e nuovo blueprint Config per utilizzare la SLR		

Versione di base	Versioni della zona di atterraggio	Progetti inclusi	Modifica rispetto alla linea di base precedente		
		Config SLR, risorse IAM			
3.0	Da 3.0 a 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, risorse IAM	Nuovo AWS Config progetto. Passa alla registrazione delle risorse globali solo nella regione d'origine. CloudTrail I Blueprint rimosso		
4.0	da 3.2 a 3.3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, risorse IAM	Nuovo modello SLR		

Versione di base	Versioni della zona di atterraggio	Progetti inclusi	Modifica rispetto alla linea di base precedente		
5.0	4.0	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, risorse IAM	Autorizzazioni di aggregazione AWS Config rimosse. L'autorizzazione di AWS Config Aggregation da ciascun account membro non è necessaria poiché la LandingZone versione 4.0 ha adottato AWS Organizations Config Aggregator, che ha accesso a tutti gli account dei membri all'interno dell'organizzazione.		

Per ulteriori informazioni sulle risorse specifiche create negli account quando configuri la landing zone, consulta [Risorse create negli account condivisi](#).

Se aggiorni la tua landing zone a una versione che supporta una versione di **AWSControlTowerBaseline** base più recente e la nuova versione della landing zone è compatibile con la versione di base esistente, lo stato dell'unità organizzativa cambia in Update available.

- È possibile continuare a utilizzare Account Factory e altre funzionalità senza aggiornare immediatamente la baseline dell'unità organizzativa (OU).
- I nuovi account registrati in questa unità organizzativa ricevono risorse basate sulla versione di base esistente fino all'aggiornamento della versione di base (con la funzionalità Extend governance nella console o tramite l'API). UpdateEnabledBaseline
- Dopo aver aggiornato la versione di base, tutti gli account all'interno di quell'unità organizzativa ricevono risorse in base alla nuova versione di base.

Note

Dopo aver aggiornato la versione della landing zone di AWS Control Tower, se le unità organizzative mostrano lo stato di Aggiornamento richiesto nella console, è necessario aggiornare la versione di base su tali unità organizzative.

Considerazioni per le linee di base

- Se l'unità organizzativa richiede un aggiornamento di base, non è possibile fornire nuovi account o registrare account esistenti in tale unità organizzativa.
- Dopo un aggiornamento della landing zone, se prevedi di aggiornare anche una baseline dell'unità organizzativa, devi registrare nuovamente l'unità organizzativa o aggiornare la versione di base dell'unità organizzativa a livello di codice.
- Ti consigliamo di eseguire l'aggiornamento alla versione di base più compatibile per la versione di landing zone che stai utilizzando, in modo da ottenere tutti i vantaggi della landing zone e della baseline combinati. Ad esempio, se esegui l'aggiornamento alla versione 3.3 della landing zone, puoi continuare a utilizzare la baseline 3.0, ma non otterrai tutti i vantaggi della versione 3.3 della landing zone a meno che non esegui anche l'aggiornamento alla baseline 4.0.
- Gli aggiornamenti di base non possono essere ripristinati.

- L'abilitazione di base si rivolge a un'unità organizzativa alla volta. Pertanto, le unità organizzative nidificate non vengono aggiornate automaticamente quando viene aggiornata l'unità organizzativa principale. Si consiglia di aggiornare l'unità organizzativa principale prima di aggiornare le unità organizzative nidificate.
- Quando si chiama l'UpdateEnabledBaselineAPI o si registra nuovamente un'unità organizzativa dalla console, l'unità organizzativa conserva tutti i controlli abilitati prima dell'aggiornamento di base.
- Se più versioni di base sono compatibili con la versione della landing zone, è necessario utilizzare la versione di base più recente se si abilita una linea di base su un'unità organizzativa non gestita.

Esempi: registrazione di un'unità organizzativa AWS Control Tower solo con API

Questa panoramica di esempi è un documento complementare. Per spiegazioni, avvertenze e ulteriori informazioni, vedere. [Tipi di linee di base](#)

Prerequisiti

Devi disporre di un'unità organizzativa esistente che non sia registrata presso AWS Control Tower e che desideri registrare. In alternativa, è necessario disporre di un'unità organizzativa registrata che desideri registrare nuovamente per scopi di aggiornamento.

Registra un'unità organizzativa

1. Controlla se IdentityCenterBaseline è abilitato per la zona di atterraggio. In tal caso, ottieni l'identificativo Identity Center Enabled Baseline.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].  
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?  
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Ottieni l'ARN dell'unità organizzativa di destinazione.

```
aws organizations describe-organizational-unit --organizational-unit-id  
<Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Ottieni l'ARN della linea di base. `AWSControlTowerBaseline`

```
aws controltower list-baselines --query 'baselines[?name=='AWSControlTowerBaseline'].
[arn]'
```

4. Crea la `AWSControlTowerBaseline` baseline sull'unità organizzativa di destinazione.

Se l'Identity Center Baseline è abilitata:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
' [{"key": "IdentityCenterEnabledBaselineArn", "value": "<Identity Center Enabled
Baseline ARN>"} ]'
```

Se l'Identity Center Baseline non è abilitato, ometti il `parameters` flag, come segue:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Re-register un'unità organizzativa

Dopo aver aggiornato le impostazioni della zona di atterraggio o aver aggiornato la versione della zona di atterraggio, è necessario che le Re-register unità organizzative forniscano le modifiche più recenti. Segui questi passaggi per registrare nuovamente un'unità organizzativa a livello di programmazione, reimpostando la `EnabledBaseline` risorsa associata e tutte le risorse associate. `EnabledControl`

Important

Se l'unità organizzativa ha i controlli opzionali abilitati, devi anche chiamare l'[ResetEnabledControl](#) API per ogni controllo opzionale abilitato dopo aver reimpostato la baseline. Questo passaggio garantisce che i controlli opzionali rimangano coerenti con l'ultima configurazione della zona di atterraggio. Se salti questo passaggio, i controlli opzionali sull'unità organizzativa potrebbero non riflettere le ultime modifiche alla zona di atterraggio. Se non hai abilitato alcun controllo opzionale, questo passaggio non è obbligatorio.

1. Ottieni l'ARN dell'unità organizzativa di destinazione da registrare nuovamente.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --query 'OrganizationalUnit.[Arn]'
```

2. Ottieni l'ARN della EnabledBaseline risorsa per l'unità organizzativa di destinazione.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?targetIdentifier==`<OUARN>`].[arn]'
```

3. Reimposta la baseline abilitata.

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier <EnabledBaselineArn>
```

4. Se l'unità organizzativa ha i controlli opzionali abilitati, elenca i controlli abilitati per l'unità organizzativa e ripristina ciascuno di essi in modo che rimangano coerenti con l'ultima configurazione della zona di atterraggio.

Elenca i controlli abilitati sull'unità organizzativa di destinazione:

```
aws controltower list-enabled-controls --target-identifier <OU ARN>
```

Per ogni controllo opzionale abilitato restituito, reimpostalo chiamando:

```
aws controltower reset-enabled-control --enabled-control-identifier <EnabledControlArn>
```

Per ulteriori informazioni, consulta [ResetEnabledControl](#) l'AWS Control Tower API Reference.

Esempi di utilizzo delle API di base

Questa sezione contiene esempi di parametri di input e output per le API di base di AWS Control Tower.

DisableBaseline

Per ulteriori informazioni sul funzionamento di questa API, consulta [DisableBaseline](#)

DisableBaselineingresso:


```
{
  "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaselineuscita:

```
{
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

Esempi di DisableBaseline CLI:

```
aws controltower disable-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
  --region us-west-2
```

EnableBaseline

Per ulteriori informazioni su questo funzionamento dell'API, consulta [EnableBaseline](#).

EnableBaselineingresso:

```
{
  "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
  "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjq1",
  "baselineVersion": "3.0",
  "parameters": [
    {
      "key": "IdentityCenterEnabledBaselineArn",
      "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ"
    }
  ]
}
```

EnableBaselineoutput, restituendo una nuova risorsa:

```
{
```

```

    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TN0HRD7ES5VV"
  }

```

Esempi di EnableBaseline CLI:

Questo esempio mostra l'abilitazione di una linea di base per un' AWS Organizations organizzazione che ha la landing zone abilitata all'accesso a AWS IAM Identity Center, gestito da AWS Control Tower. Per recuperare l'EnabledBaselineidentificatore dell'Identity Center, puoi chiamare l>ListEnabledBaselinesAPI, filtrando in base alla linea di base di Identity Center: (arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)

```

aws controltower list-enabled-baselines \
  --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
  --region us-west-2

```

La risposta mostrerà il EnabledBaseline dettaglio, che mostra il relativo identificatore.

```

{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
      "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
      "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    }
  ]
}

```

Note

Prendi nota del valore ARN della risposta e passa questo valore come parametro per abilitare la linea di base predefinita.

```
aws controltower enable-baseline \  
  --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \  
  --baseline-version 3.0 \  
  --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-1k87jh65 \  
  --parameters  
  ' [{"key": "IdentityCenterEnabledBaselineArn", "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"} ]' \  
  --region us-west-2
```

Per un'organizzazione con la landing zone disattivata dalla gestione di AWS Control Tower di IAM Identity Center, abilita la linea di base senza il parametro.

```
aws controltower enable-baseline \  
  --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \  
  --baseline-version 3.0 \  
  --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-1k87jh65 \  
  --region us-west-2
```

GetBaseline

Per ulteriori informazioni su questo funzionamento dell'API, consulta [GetBaseline](#)

GetBaselineingresso:

```
{  
  "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"  
}
```

GetBaselineuscita:

```
{  
  "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",  
  "name": "AWSControlTowerBaseline",  
  "description": "Sets up resources and mandatory controls for member accounts within the target OU, required for AWS Control Tower governance.",  
}
```

Esempi di GetBaseline CLI:

```
aws controltower get-baseline \  
  --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \  
  --region us-west-2
```

GetBaselineOperation

Per ulteriori informazioni su questo funzionamento dell'API, consulta [GetBaselineOperation](#).

GetBaselineOperationingresso:

```
{  
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"  
}
```

GetBaselineOperationuscita:

```
{  
  "baselineOperation": {  
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",  
    "operationType": "DISABLE_BASELINE",  
    "status": "FAILED",  
    "startTime": "2023-01-12T19:05:00Z",  
    "endTime": "2023-01-12T19:45:00Z",  
    "statusMessage": "Can't perform DisableBaseline on a parent target with  
governed child OUs"  
  }  
}
```

Esempi di GetBaselineOperation CLI:

```
aws controltower get-baseline-operation \  
  --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \  
  --region us-west-2
```

GetEnabledBaseline

Per ulteriori informazioni su questo funzionamento dell'API, consulta [GetEnabledBaseline](#).

GetEnabledBaselineingresso:

```
{
  "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaselineuscita:

```
{
  "enabledBaselineDetails": {
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
    "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
    "baselineVersion": "3.0",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjq1",
    "statusSummary": {
      "status": "SUCCEEDED",
      "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
    },
    "parameters": [
      {
        "key": "IdentityCenterEnabledBaselineArn",
        "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
      }
    ]
  }
}
```

Esempi di GetEnabledBaseline CLI:

```
aws controltower get-enabled-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EYC \
  --region us-west-2
```

ListBaselines

Per ulteriori informazioni su questo funzionamento dell'API, consulta [ListBaselines](#).

ListBaselinesinput (utilizzando input opzionali):

```
{
  "nextToken": "AbCd1234",
  "maxResults": "4"
}
```

ListBaselinesuscita:

```
{
  "baselines": [
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KM010S6311",
      "name": "AuditBaseline",
      "description": "Sets up resources to monitor security and compliance of accounts in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
      "name": "LogArchiveBaseline",
      "description": "Sets up a central repository for logs of API activities and resource configurations from accounts in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
      "name": "IdentityCenterBaseline",
      "description": "Sets up shared resources for AWS Identity Center, which prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
      "name": "AWSControlTowerBaseline",
      "description": "Sets up resources and mandatory controls for member accounts within the target OU, required for AWS Control Tower governance."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9A0MU2",
      "name": "BackupCentralVaultBaseline",
      "description": "Sets up central AWS Backup vault in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
      "name": "BackupAdminBaseline",
      "description": "Sets up delegated admin and AWS Backup Audit Manager."
    }
  ]
}
```

```
{
  "arn": "arn:aws:controltower:us-east-1::baseline/AP09ATVPBKFRRLK",
  "name": "BackupBaseline",
  "description": "Sets up local Backup vault and attach Backup policy."
}
```

Esempi di ListBaselines CLI:

```
aws controltower list-baselines \
  --region us-west-2
```

ListEnabledBaselines

L'ListEnabledBaselinesAPI dispone di un parametro opzionale che consente di visualizzare le linee di base applicate agli account membri di un'unità organizzativa. Gli esempi che seguono mostrano alcuni comandi CLI che è possibile utilizzare per visualizzare le linee di base di un account. AWS Control Tower fa riferimento a queste linee di base, che sono abilitate sull'unità organizzativa, ma si applicano a ciascun account all'interno dell'unità organizzativa, come linee di base abilitate ai bambini, poiché derivano la loro configurazione di governance dalle linee di base applicate all'unità organizzativa.

Per ulteriori informazioni sul funzionamento di questa API, consulta [ListEnabledBaselines](#)

ListEnabledBaselinesinput per mostrare le linee di base abilitate ai bambini:

```
aws controltower list-enabled-baselines --include-children
```

ListEnabledBaselinesoutput per visualizzare le linee di base abilitate ai bambini:

```
{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/X02UQ1PC6BB5085S5",
      "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/AP09ATVPBKFRRLK",
      "baselineVersion": "1.0",
      "statusSummary": {
        "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
```

```

        "status": "SUCCEEDED"
      },
      "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/ou-k86y-ld9k8vpu"
    },
    {
      "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/XAFPKQQX0JB50ZWQH",
      "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/AP09ATVPBKFRRLK",
      "baselineVersion": "1.0",
      "parentIdentifier": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/X0IZ4G08CWB50ZWON",
      "statusSummary": {
        "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
        "status": "SUCCEEDED"
      },
      "targetIdentifier": "arn:aws:organizations::666355521292:account/o-vaex10vaey/183295447314"
    }
  ]

```

Note

Nell'esempio precedente, il `parentIdentifier` campo mostra la linea di base abilitata dell'unità organizzativa principale per questa baseline abilitata al figlio.

Visualizza tutte le linee di base applicate a un obiettivo specifico (unità organizzativa o account):

```

aws controltower list-enabled-baselines \
  --filter '{
    "targetIdentifiers": ["TARGET_ARN"]
  }'

```

Visualizza tutte le unità organizzative con una linea di base specifica:

```

aws controltower list-enabled-baselines \
  --filter '{
    "baselineIdentifiers": ["BASELINE_ARN"]
  }'

```


Visualizza tutte le unità organizzative e gli account con una linea di base specifica:

```
aws controltower list-enabled-baselines \
  --filter '{
    "baselineIdentifiers": ["BASELINE_ARN"]
  }' \
  --include-children
```

Visualizza tutti gli account in un'unità organizzativa con Baseline B abilitata:

```
### First fetch the enabled baseline record for Baseline B on the OU
aws controltower list-enabled-baselines \
  --filter '{
    "targetIdentifiers": ["OU_TARGET_ARN"],
    "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
  }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
enabled baseline record on the OU
aws controltower list-enabled-baselines \
  --filter '{
    "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
  }' \
  --include-children
```

Ulteriori informazioni sulle linee di base abilitate ai bambini

- È possibile utilizzare l'GetEnabledBaselineAPI per visualizzare informazioni dettagliate su una specifica baseline abilitata ai bambini
- È possibile utilizzare l'GetBaselineOperationAPI per visualizzare un'operazione eseguita sulla baseline abilitata ai figli
- Non è possibile chiamare alcuna API di scrittura, ad esempio, ResetEnabledBaseline or EnableBaseline UpdateEnabledBaselineDisableBaseline, direttamente su una baseline abilitata per i figli.
- Le risorse di base abilitate ai bambini possono essere modificate solo tramite il servizio AWS Control Tower, tramite operazioni eseguite sull'unità organizzativa principale o tramite Account Factory.

Esempi di utilizzo dei filtri:

ListEnabledBaselinesinput (senza filtri):

```
{
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}
```

ListEnabledBaselinesinput (solo baselineIdentifiers filtro):

```
{
  "filter": {
    "baselineIdentifiers": ['arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-east-1::baseline/12GZU8CKZKVMS2AW']
  },
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}
```

ListEnabledBaselinesinput (solo targetIdentifiers filtro):

```
{
  "filter": {
    "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
  },
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 2
}
```

ListEnabledBaselinesinput (baselineIdentifiers e targetIdentifiers filtri):

```
{
  "filter": {
    "baselineIdentifiers": ['arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2']
    "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-fex1u317']
  },
  "nextToken": "bde7-XX0c6fXXXXXX",
}
```

```
"maxResults": 5
}
```

ListEnabledBaselinesuscita:

```
{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ",
      "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
      "baselineVersion": "3.0",
      "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhp/
ou-r9mj-4j3mzjql",
      "statusSummary": {
        "status": "SUCCEEDED",
        "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
      "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
      "baselineVersion": "4.0",
      "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
      "statusSummary": {
        "status": "FAILED",
        "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
      }
    }
  ],
  "nextToken": "e2bXXXXX6cab"
}
```

Esempio di CLI con un tipo di filtro (baselineIdentifiersfiltro):

```
aws controltower list-enabled-baselines \
  --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
```

```
--region us-west-2
```

Esempio di CLI che utilizza più filtri (baselineIdentifier e targetIdentifier filtri):

```
aws controltower list-enabled-baselines \  
  --filter targetIdentifier=arn:aws:organizations::123456789012:ou/o-  
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifier=arn:aws:controltower:us-  
west-2::baseline/17BSJV3IGJ2QSGA2 \  
  --region us-west-2
```

ResetEnabledBaseline

Per ulteriori informazioni su questo funzionamento dell'API, vedere [ResetEnabledBaseline](#).

ResetEnabledBaselineingresso:

```
{  
  "enabledBaselineIdentifier": "arn:aws:controltower:us-  
west-2:123456789012:enabledbaseline/XAJ9NkW88AA4W9CLL"  
}
```

ResetEnabledBaselineuscita:

```
{  
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"  
}
```

Esempi di ResetEnabledBaseline CLI:

```
aws controltower reset-enabled-baseline \  
  --enabled-baseline-identifier arn:aws:controltower:us-  
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \  
  --region us-west-2
```

UpdateEnabledBaseline

Per ulteriori informazioni su questo funzionamento dell'API, consulta [UpdateEnabledBaseline](#).

UpdateEnabledBaselineingresso:

```
{
  "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NkW88AA4W9CLL",
  "baselineVersion": "4.0",
  "parameters": [
    {
      "key": "IdentityCenterEnabledBaselineArn",
      "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJT5I4W07MZ"
    }
  ]
}
```

UpdateEnabledBaselineuscita:

```
{
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

Esempi di UpdateEnabledBaseline CLI:

```
aws controltower update-enabled-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
  --baseline-version 4.0
  --parameters
  '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
  --region us-west-2
```

Informazioni e link aggiuntivi

Questo argomento include collegamenti a post di blog pertinenti, documentazione tecnica e informazioni correlate che possono aiutarti a lavorare con AWS Control Tower. Le fonti riguardano alcuni casi d'uso comuni e le best practice per le funzionalità di AWS Control Tower e alcuni miglioramenti aggiuntivi.

Tutorial e laboratori

- [Laboratorio AWS Control Tower](#): questi laboratori forniscono una panoramica di alto livello delle attività comuni relative ad AWS Control Tower.
- Nella dashboard di AWS Control Tower, scegli [Ottieni una guida personalizzata](#) se hai in mente un caso d'uso ma non sai da dove iniziare.
- Prova a visitare questa YouTube playlist di [AWS Cloud Operations](#) e cerca in AWS Control Tower per trovare video che spiegano di più su come utilizzare le funzionalità di AWS Control Tower.

Rete

Imposta modelli ripetibili e gestibili per le reti in AWS. Scopri di più sulla progettazione, l'automazione e le apparecchiature comunemente utilizzate dai clienti.

- [AWS Architettura VPC Quick Start](#): questa guida rapida fornisce una base di rete basata sulle AWS migliori pratiche per la tua infrastruttura AWS cloud. Crea un AWS Virtual Private Network ambiente con sottoreti pubbliche e private in cui è possibile avviare AWS servizi e altre risorse.
- [Self-service VPC in AWS Control Tower utilizzando AWS Service Catalog](#): questo post del blog descrive un modo per configurare Account Factory in modo da poter effettuare il provisioning degli account con VPC personalizzati.
- [Implementazione di Serverless Transit Network Orchestrator \(STNO\) in AWS Control Tower](#): questo post del blog dimostra come automatizzare l'accesso alla connettività di rete tra gli account. Questo blog è destinato agli amministratori di AWS Control Tower o ai responsabili della gestione delle reti all'interno del loro ambiente. AWS

Sicurezza, identità e registrazione

Estendi il tuo livello di sicurezza, integra con provider di identità esterni o esistenti e centralizza i sistemi di registrazione.

Sicurezza

- [Automazione AWS Security Hub CSPM degli avvisi con gli eventi del ciclo di vita di AWS Control Tower](#): questo post del blog descrive come automatizzare l'abilitazione e la configurazione di Security Hub CSPM in un ambiente multi-account AWS Control Tower su account esistenti e nuovi.
- [Abilitazione AWS Identity and Access Management](#): questo post del blog descrive come migliorare la visibilità della sicurezza organizzativa abilitando e centralizzando i risultati di IAM Access Analyzer.
- [AWS Systems Manager Parameter Store](#) fornisce uno storage gerarchico sicuro per la gestione dei dati di configurazione e la gestione dei segreti. Puoi usarlo per condividere le informazioni di configurazione in un luogo sicuro, per l'utilizzo da parte di AWS Systems Manager e di AWS CloudFormation. Ad esempio, puoi memorizzare un elenco di regioni in cui desideri distribuire i pacchetti di conformità.

Identità

- [Collega l'identità utente di Azure AD AWS agli account e alle applicazioni per il Single Sign-on](#): questo post del blog descrive come usare Azure AD con IAM Identity Center e AWS Control Tower.
- [Gestisci l'accesso ad AWS centralmente per gli utenti di Okta con Centro identità AWS IAM](#): questo post del blog descrive come usare Okta con IAM Identity Center e AWS Control Tower.

Registrazione di log

- [AWS Soluzione di registrazione centralizzata](#): questo post della soluzione descrive la soluzione di registrazione centralizzata che consente alle organizzazioni di raccogliere, analizzare e visualizzare i log su AWS più account e regioni. AWS
- Per informazioni sulla visualizzazione delle AWS Config risorse, consulta il [Config Resource Compliance Dashboard](#).

Distribuzione delle risorse e gestione dei carichi di lavoro

Implementa e gestisci risorse e carichi di lavoro.

- [Getting Started Integrazione con la libreria](#): questo post del blog descrive i portafogli Getting Started che puoi utilizzare.
- [Distribuzione continua di Cloud Custodian su AWS Control Tower](#)

Lavorare con organizzazioni e account esistenti

Collabora con AWS organizzazioni e account esistenti.

- [Registrazione di un account](#): questo argomento della guida per l'utente descrive come registrare un AWS account esistente in AWS Control Tower.
- [Crea un account in AWS Control Tower](#): questo post del blog descrive come implementare AWS Control Tower nelle tue organizzazioni esistenti. AWS
- [Estendi la governance di AWS Control Tower utilizzando i pacchetti di conformità AWS Config](#): questo post del blog descrive come distribuire i pacchetti di AWS Config conformità per aiutare a portare gli account e le organizzazioni esistenti alla governance di AWS Control Tower.
- [Come rilevare e mitigare le violazioni del Guardrail con AWS Control Tower](#): questo post del blog descrive come aggiungere controlli e come iscriversi alle notifiche SNS in modo da poter ricevere notifiche via e-mail delle violazioni della conformità dei controlli.

Automazione e integrazione

Automatizza la creazione di account e integra gli eventi del ciclo di vita con AWS Control Tower.

- [Eventi del ciclo di vita](#): questo post del blog descrive come utilizzare gli eventi del ciclo di vita con AWS Control Tower.
- [Creazione automatica degli account](#): questo post del blog descrive come configurare la creazione automatica di account in AWS Control Tower.
- [Automazione dei log di flusso di Amazon VPC](#): questo post del blog descrive come automatizzare e centralizzare Amazon VPC Flow Logs in un ambiente con più account.

- [Automatizza la codifica dei VPC con gli eventi del ciclo di vita di AWS Control Tower](#): questo post del blog descrive come automatizzare l'etichettatura delle risorse per i VPC, tramite eventi del ciclo di vita in AWS Control Tower.
- [Gestione automatizzata degli account](#): questo post del blog descrive come automatizzare le attività di gestione degli account dopo la configurazione dell'ambiente AWS Control Tower.

Migrazione dei carichi di lavoro

Utilizza altri AWS servizi con AWS Control Tower per facilitare la migrazione dei carichi di lavoro.

- [CloudEndure migrazione](#): questo post del blog descrive come combinare CloudEndure altri AWS servizi con AWS Control Tower per facilitare la migrazione dei carichi di lavoro.

Servizi AWS correlati

AWS Control Tower funge da livello di orchestrazione per AWS Organizations. Pertanto, tramite la console e le API di AWS Organizations, hai accesso a oltre 20 altri servizi AWS che funzionano con AWS Control Tower. Questi servizi aggiuntivi non sono accessibili direttamente tramite la console AWS Control Tower.

- Per un elenco completo dei servizi disponibili per AWS Control Tower tramite AWS Organizations, consulta i servizi [AWS che puoi utilizzare con AWS Organizations](#).
- Per abilitare le funzionalità multi-account per questi servizi AWS correlati, devi abilitare l'accesso affidabile. Per ulteriori informazioni, consulta [Utilizzo di AWS Organizations con altri servizi](#) AWS.

Note

Ricorda che AWS IAM Identity Center e IAM AWS CloudTrail sono configurati per te in AWS Control Tower e completamente integrati. AWS Config Non è necessario modificare le impostazioni di accesso attendibile o di amministrazione delegata per questi servizi.

- Alcuni AWS servizi disponibili tramite AWS Organizations possono utilizzare l'amministrazione delegata, tra cui AWS Systems Manager e AWS Firewall Manager. Per ulteriori informazioni, consulta [Configurazione di un amministratore delegato](#) e [Abilitazione di un account amministratore delegato per Firewall Manager](#). Guarda anche questo video, [Configurare gruppi di sicurezza con AWS Firewall Manager](#).

Marketplace AWS soluzioni

Scopri le soluzioni di Marketplace AWS.

- [AWS Control Tower Marketplace](#): Marketplace AWS offre un'ampia gamma di soluzioni per AWS Control Tower per aiutarti a integrare software di terze parti. Queste soluzioni aiutano a risolvere i principali casi d'uso operativi e infrastrutturali, tra cui gestione delle identità, sicurezza per un ambiente con più account, reti centralizzate, intelligenza operativa e gestione delle informazioni e degli eventi di sicurezza (SIEM).

Note di rilascio di AWS Control Tower

Le seguenti sezioni mostrano i dettagli sulle versioni di AWS Control Tower, sin dall'inizio del servizio. Alcune versioni richiedono un aggiornamento per una landing zone di AWS Control Tower, mentre altre versioni vengono incorporate automaticamente nel servizio.

Le funzionalità e le versioni sono elencate in ordine cronologico inverso (prima la più recente) in base alla data in cui sono state annunciate ufficialmente al pubblico.

Argomenti

- [gennaio 2026 - Presente](#)
- [gennaio 2025 - dicembre 2025](#)
- [gennaio - dicembre 2024](#)
- [gennaio - dicembre 2023](#)
- [gennaio - dicembre 2022](#)
- [gennaio - dicembre 2021](#)
- [gennaio - dicembre 2020](#)
- [giugno - dicembre 2019](#)

gennaio 2026 - Presente

Da gennaio 2026, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Account Factory for Terraform \(AFT\) supporta le esecuzioni di personalizzazione solo in base al piano](#)
- [AWS Control Tower disponibile nel cloud sovrano europeo](#)

Account Factory for Terraform (AFT) supporta le esecuzioni di personalizzazione solo in base al piano

16 settembre 2026

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Il framework di personalizzazione degli account AWS Control Tower, Account Factory for Terraform (AFT), ora supporta esecuzioni di personalizzazione in modalità solo piano (sola lettura). Puoi passare l'`plan_only` input alla macchina a `aft-invoke-customizations` stati per visualizzare in anteprima le modifiche Terraform che un account riceverebbe. Ciò consente di rivedere le modifiche senza applicarle. AFT viene eseguito `terraform plan` invece che `terraform apply` su tutte le distribuzioni Terraform supportate. AFT può esportare l'output JSON del piano in un bucket Amazon S3 crittografato nell'account di gestione AFT. Nella distribuzione Community Edition (open source), AFT esporta l'output per impostazione predefinita. Su Terraform Cloud e Terraform Enterprise, l'esportazione è attivabile e puoi anche visualizzare i risultati nell'interfaccia utente di HCP Terraform run. `aft_plan_output_export_enabled`

[Per ulteriori informazioni, consulta Personalizzazioni dell'account.](#)

AWS Control Tower disponibile nel cloud sovrano europeo

13 gennaio 2026

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower è ora disponibile nel cloud sovrano europeo. Per ulteriori informazioni su AWS Control Tower nel cloud sovrano europeo, consulta la [Guida per l'utente di AWS Control Tower per il cloud sovrano europeo](#).

gennaio 2025 - dicembre 2025

Da gennaio 2025, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Zona di destinazione di AWS Control Tower versione 4.0](#)
- [AWS Control Tower ne aggiunge altri 279 AWS Config controlli per Control Catalog](#)
- [AWS Control Tower è disponibile nella regione Asia Pacifico \(Nuova Zelanda\)](#)
- [AWS Control Tower supporta la registrazione automatica degli account](#)
- [AWS Control Tower aggiorna la versione Python](#)
- [AWS Control Tower supporta gli indirizzi IPv6](#)
- [AWS Control Tower riduce la deriva](#)

[Disponibile la versione 1.15.0 di Account Factory per Terraform](#)

- [Controlli aggiornati con tipi di istanza Nitro](#)

- [AWS Control Tower è disponibile nella regione Asia Pacifico \(Taipei\)](#)
- [AWS Control Tower supporta PrivateLink](#)
- [Supporto per framework di settore aggiuntivi, metadati aggiornati](#)
- [Service-linked AWS Config controlli](#)
- [La visualizzazione della console dei controlli abilitati offre una visibilità centralizzata](#)
- [the section called “Account Factory for Terraform \(AFT\) supporta nuove configurazioni in fase di distribuzione”](#)
- [AWS Control Tower introduce la reportistica a livello di account per le API di base](#)
- [the section called “AWS Control Tower è disponibile in AWS Regioni dell'Asia Pacifico \(Thailandia\) e del Messico \(centrale\)”](#)
- [Aggiuntivo AWS Config controlli disponibili](#)
- [Annulla la registrazione e l'eliminazione delle azioni per le unità organizzative](#)
- [the section called “Control Catalog supporta gli indirizzi IPv6”](#)

Zona di destinazione di AWS Control Tower versione 4.0

17 novembre 2025

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 4.0. Per informazioni, consulta [Aggiorna la tua landing zone](#)).

AWS Control Tower landing zone 4.0 è un importante aggiornamento che introduce un' Controls-Only esperienza flessibile, consentendo ai clienti di personalizzare il modo in cui implementare e gestire il proprio ambiente AWS con più account. Questa versione cambia in modo significativo il modo in cui AWS Control Tower si integra con i servizi AWS e gestisce le risorse organizzative. Per informazioni sulle modifiche principali, consulta [Guida alla migrazione di Landing Zone v4.0](#).

Modifiche e caratteristiche principali

- Integrazioni di servizi opzionali: la zona di destinazione 4.0 ti consente di scegliere quali integrazioni di servizi abilitare nel tuo ambiente. La disattivazione di un'integrazione eliminerà le risorse distribuite da AWS Control Tower specifiche per tale integrazione negli account gestiti e negli account centrali di integrazione dei servizi. Ora puoi abilitare o disabilitare selettivamente le integrazioni dei servizi:
 - AWS Config

- AWS CloudTrail
- Ruoli di sicurezza
- AWS Backup

Importante: se desideri disabilitare l'integrazione con AWS Config, devi disabilitare anche i ruoli di sicurezza, IAM Identity Center e le integrazioni AWS Backup.

- Risorse dedicate invece di utilizzare risorse condivise: la zona di atterraggio 4.0 ora crea risorse dedicate per i servizi chiave. Questa separazione offre un migliore isolamento delle risorse e un controllo più granulare sulle risorse specifiche del servizio:
 - Bucket S3 separati per AWS Config
 - Bucket S3 separati per AWS CloudTrail
 - Argomenti SNS individuali per ogni servizio
- Struttura organizzativa flessibile: la landing zone 4.0 elimina i precedenti requisiti della struttura organizzativa:
 - Non è più necessario utilizzare un'unità organizzativa di sicurezza
 - È possibile definire la propria struttura organizzativa
 - L'unico requisito è che tutti gli account hub si trovino nella stessa unità organizzativa
- Esperienza di controllo dedicata: ora puoi creare una configurazione minima della zona di atterraggio che includa:
 - Integrazione di base con AWS Organizations
 - Capacità di abilitare i controlli senza abilitare la linea di `AWSControlTowerBaseline` base
 - Configurazioni di governance personalizzate in base alle tue esigenze
- AWS Config Changes - Landing Zone 4.0 introduce diversi miglioramenti all'implementazione dell'integrazione di AWS Config:
 - Una nuova linea di base di Config Spoke specifica per i controlli investigativi
 - Service-linked Config aggregator (SLCA) nell'account Config hub
 - Sostituzione degli aggregatori tradizionali di organizzazioni e account
- Manifesto opzionale:
 - Il campo manifest è ora opzionale e consente di:
 - Crea zone di atterraggio senza integrazioni di servizi

- Maggiore flessibilità nella configurazione iniziale
- Opzioni di implementazione personalizzate

AWS Control Tower ne aggiunge altri 279 AWS Config controlli per Control Catalog

14 novembre 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora include 279 AWS Config controlli aggiuntivi come parte del Control Catalog. È possibile visualizzare i controlli nella console di AWS Control Tower e tramite le API.

Alcuni controlli hanno relazioni con altri controlli. Queste relazioni sono espresse anche nella console AWS Control Tower e nelle API. I tipi di relazione includono Complementare, Mutuamente esclusivo e Alternativo.

AWS Control Tower è disponibile nella regione Asia Pacifico (Nuova Zelanda)

28 ottobre 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è ora disponibile nella regione Asia Pacifico (Nuova Zelanda).

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

AWS Control Tower supporta la registrazione automatica degli account

15 ottobre 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Per i clienti che utilizzano la landing zone di AWS Control Tower versione 3.1 o successiva, AWS Control Tower ora consente la registrazione automatica degli account nelle unità organizzative. Se si opta per la registrazione automatica degli account, AWS Control Tower applica le risorse e i

controlli di base abilitati di un'unità organizzativa a un account, quando lo si sposta in una nuova unità organizzativa. I controlli e le linee di base della precedente unità organizzativa vengono rimossi. Nella maggior parte dei casi, questa azione non crea alcuna deriva.

Per attivare la registrazione automatica: puoi selezionare la registrazione automatica degli account nella pagina delle impostazioni della zona di destinazione nella console AWS Control Tower o chiamando AWS Control Tower o le UpdateLandingZone API, con il valore del parametro CreateLandingZone impostato su Inheritance Drift. RemediationType

Per applicare la registrazione automatica: dopo aver selezionato questa opzione nella pagina Impostazioni, puoi spostare un account tramite la console, l'API o la console AWS Control Tower. AWS Organizations AWS Organizations MoveAccount

Per annullare la registrazione di un account con registrazione automatica: se sposti un account al di fuori di un'unità organizzativa registrata, AWS Control Tower rimuove automaticamente tutte le risorse e i controlli di base distribuiti.

Per ulteriori informazioni sulla registrazione automatica, consulta. [Facoltativamente, configura la registrazione automatica per gli account](#)

Questa versione include anche un aggiornamento a una politica gestita e a una nuova politica gestita. Abbiamo aggiornato [AWS ControlTowerServiceRolePolicy](#) e aggiunto il nuovo [AWS ControlTowerIdentityCenterManagementPolicy](#).

Abbiamo aggiornato AWS Control Tower CreateLandingZone e le UpdateLandingZone API per aggiungere una nuova RemediationType, chiamata Inheritance Drift.

AWS Control Tower aggiorna la versione Python

3 settembre 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

La versione 3.9 di Python è obsoleta. AWS Control Tower ha aggiornato le versioni di Python nei tuoi ambienti AWS Control Tower. Non è richiesta alcuna azione e questo aggiornamento non influisce sui carichi di lavoro esistenti.

AWS Control Tower riduce la deriva

20 agosto 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiornato la funzionalità di Service Control Policy (SCP) drift. Con questa versione, due tipi di deriva della governance vengono gestiti direttamente da AWS Control Tower e non causano più deviazioni nel tuo ambiente.

Sono stati rimossi due tipi di deriva di governance

- SCP collegato a un'unità organizzativa gestita: questo tipo di deriva si verificava quando un SCP per un controllo era collegato a qualsiasi altra unità organizzativa. Questo evento era particolarmente comune quando si aggiornavano le unità organizzative dall'esterno della console AWS Control Tower.
- SCP collegato all'account membro: questo tipo di deriva si verificava in genere quando un SCP per un controllo veniva collegato a un account dall'esterno della console AWS Control Tower.

Per ulteriori informazioni sulla deriva, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

AWS Control Tower supporta gli indirizzi IPv6

18 agosto 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

L'API AWS Control Tower ora supporta gli indirizzi Internet Protocol versione 6 (IPv6) tramite i nostri nuovi endpoint dual-stack. Gli endpoint esistenti che supportano IPv4 rimangono disponibili per la compatibilità con le versioni precedenti. I nuovi domini dual-stack sono disponibili [da Internet](#) o all'interno di un Amazon Virtual Private [Cloud \(VPC\) utilizzando](#) [AWS PrivateLink](#)

Disponibile la versione 1.15.0 di Account Factory per Terraform

28 luglio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

È disponibile la versione 1.15.0 di AWS Control Tower Account Factory for Terraform (AFT). Per ulteriori informazioni, consulta il repository AFT. [GitHub](#)

Controlli aggiornati con tipi di istanza Nitro

24 luglio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiornato gli otto controlli proattivi nel Control Catalog (precedentemente chiamato Control Library) che applicano i tipi di istanze Amazon EC2. Questo aggiornamento consente di creare un'istanza di alcuni nuovi tipi di istanze Nitro e rimuove alcuni tipi di istanze della serie U obsoleti.

Controlli aggiornati

- [CT.AUTOSCALING.PR.10](#)
- [CT.AUTOSCALING.PR.11](#)
- [CT.EC2.PR.15](#)
- [CT.EC2.PR.16](#)
- [CT.EC2.PR.17](#)
- [CT.EC2.PR.18](#)
- [CT.EC2.PR.19](#)
- [CT.EC2.PR.20](#)

Nuovi tipi di istanze disponibili

- c8gd
- c8gn
- i7i
- m8gd
- p6-b200
- r8gd

Tipi di istanza rimossi

- u-12tb1
- u-18tb1
- u-24tb1
- u-9tb1

I controlli aggiornati sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle regioni in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower è disponibile nella regione Asia Pacifico (Taipei)

23 luglio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è ora disponibile nella regione Asia Pacifico (Taipei):

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

AWS Control Tower supporta PrivateLink

30 giugno 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta [AWS PrivateLink](#). Puoi richiamare le API di AWS Control Tower e Control Catalog dall'interno del tuo Amazon Virtual Private Cloud (VPC) senza accedere alla rete Internet pubblica. AWS PrivateLink fornisce connettività privata tra cloud privati virtuali (VPC), servizi e risorse supportati e reti locali. AWS PrivateLink il supporto per AWS Control Tower è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower.

Supporto per framework di settore aggiuntivi, metadati aggiornati

12 giugno 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Con questa versione, AWS Control Tower si espande per includere il supporto per 10 framework di settore. Per un elenco dei framework, consulta Frameworks supportati. <https://docs.aws.amazon.com/controltower/latest/controlreference/frameworks-supported.html>

Ad esempio, puoi iniziare accedendo alla pagina del Control Catalog nella console di AWS Control Tower e cercando un framework, ad esempio per visualizzare tutti i controlli relativi a quel framework. PCI-DSS-v4.0 Oppure puoi esaminare i controlli e i framework a livello di codice, chiamando la nuova API. [ListControlMappings](#)

Le definizioni dei metadati associate ai controlli stanno cambiando, per supportare meglio questi framework di settore aggiuntivi. Le modifiche ai metadati possono influire sul modo in cui valutate i controlli per l'abilitazione. Ad esempio, i valori per i metadati NIST, PCI e CIS potrebbero essere cambiati. Ti consigliamo di rivedere le mappature per i controlli abilitati nella pagina dei dettagli del controllo della console.

Nella console e nell'API, abbiamo introdotto 3 nuovi campi di metadati. Collettivamente, questi campi descrivono una gerarchia che aiuta a capire come classificare e abilitare i controlli. I campi sono: Dominio, Obiettivo e [Controllo comune](#). Abbiamo ridefinito i nostri obiettivi [di controllo](#) per allinearli meglio all'ambito più ampio dei framework di settore disponibili. Per ulteriori informazioni su questa gerarchia, consulta la panoramica di Ontology. <https://docs.aws.amazon.com/controlcatalog/latest/userguide/ontology-overview.html>

- Queste modifiche ai metadati si riflettono nella console AWS Control Tower e l'esperienza della console è coerente su tutta la AWS Control Tower e le console. AWS Config
- Per visualizzare le informazioni di controllo nella console AWS Control Tower, devi aggiungere `controlcatalog` autorizzazioni aggiuntive alle politiche IAM. Per ulteriori informazioni, consulta [Autorizzazioni richieste per utilizzare la console AWS Control Tower](#).
- Ogni controllo ora ha un nuovo campo chiamato `GovernedResources`, che mostra i tipi di risorse che il controllo governa. In alcuni casi, questo campo mostra il prefisso di servizio per le risorse e in altri casi può essere vuoto. Per ulteriori informazioni, consulta [GetControl](#) e [ListControls](#).

Con questa versione, abbiamo rinominato la `Controls Library` in `Control Catalog`, per coerenza con altra terminologia.

Service-linked AWS Config controlli

12 giugno 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower annuncia il supporto per i controlli investigativi di AWS Control Tower da distribuire come regole collegate ai servizi. AWS Config

Con questa versione, AWS Control Tower ora distribuisce le regole di configurazione collegate ai servizi direttamente negli account registrati, sostituendo il precedente metodo di distribuzione con stack set. AWS CloudFormation Questa modifica migliora significativamente la velocità di distribuzione. Inoltre, queste regole di configurazione collegate ai servizi aiutano a garantire una

governance coerente delle risorse, poiché impediscono la deriva involontaria della configurazione che potrebbe essere causata da modifiche manuali agli stack set o alle regole di configurazione. CloudFormation

In futuro, tutti i controlli AWS Control Tower implementati dalle AWS Config regole verranno implementati con questo meccanismo, che richiama direttamente le API. AWS Config

Important

Prima di adottare regole di configurazione collegate ai servizi, rivedi le personalizzazioni esistenti, ad esempio le correzioni, che hai apportato alle regole di Config all'esterno di AWS Control Tower, poiché queste personalizzazioni verranno rimosse durante la transizione. Le AWS Config API non supportano l'aggiunta di configurazioni di correzione per le regole collegate ai servizi. AWS Config Consulta [PutRemediationConfigurations](#).

Dettagli e azioni richieste

- Quando aggiorni o ripristini la tua zona di destinazione, AWS Control Tower aggiorna i controlli obbligatori che regolano l'unità organizzativa di sicurezza. Per completare l'aggiornamento, è inoltre necessario reimpostare ciascuno dei controlli di rilevamento implementati con AWS Config regole o l'unità organizzativa. Re-register
- L'intero ambito di questo aggiornamento si applica a te se la tua versione della zona di destinazione di AWS Control Tower è 3.2 o successiva. Quando applichi questo aggiornamento, le AWS Config regole esistenti vengono modificate per diventare regole di configurazione gestite dal servizio, insieme al nuovo metodo di distribuzione.
- Se la tua zona di destinazione è la versione 3.1 o precedente, tutte le nuove regole di configurazione verranno implementate con il nuovo metodo, non più con Stack Sets. Le regole di configurazione esistenti NON vengono aggiornate per diventare regole di configurazione gestite dal servizio. Rimarranno del tipo standard.
- È possibile identificare le regole di configurazione collegate ai servizi tramite la relativa risorsa ARN, che ha il formato:

```
arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*
```

La funzionalità prevista dei controlli, se implementata da regole collegate ai servizi, non è AWS Config cambiata. Le regole di configurazione detective e collegate ai servizi in AWS Control Tower

possono identificare le risorse non conformi all'interno degli account, come le violazioni delle policy, e fornire avvisi tramite la dashboard. Per mantenere la coerenza, evitare deviazioni nella configurazione e semplificare l'esperienza utente complessiva, queste regole ora possono essere modificate solo tramite AWS Control Tower.

Come parte di questa versione, abbiamo aggiunto quattro nuove autorizzazioni alla policy per il ruolo collegato ai servizi (SLR) [AWSServiceRoleForAWSControlTower](#), in modo da poter abilitare e disabilitare le regole collegate ai servizi AWS Config per gli account registrati.

```
config:DescribeConfigRules
config:TagResource
config:PutConfigRule
config>DeleteConfigRule
```

La visualizzazione della console dei controlli abilitati offre una visibilità centralizzata

21 maggio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto una nuova pagina nella console che mostra tutti i controlli abilitati in un'unica vista centralizzata. In precedenza, i controlli erano visualizzabili solo con l'account o l'unità organizzativa su cui erano abilitati. La visualizzazione consolidata consente di identificare più facilmente le lacune nella governance dei controlli, su larga scala.

Nella pagina Controlli abilitati, puoi filtrare i controlli in base al comportamento: Preventivo, Detective o Proattivo. Puoi anche filtrare in base all'implementazione del controllo, ad esempio SCP. Per ogni controllo, puoi vedere quante unità organizzative hanno questo controllo abilitato.

Per visualizzare la pagina dei controlli abilitati, accedi alla sezione Controlli nella console AWS Control Tower.

Account Factory for Terraform (AFT) supporta nuove configurazioni in fase di distribuzione

13 maggio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Il framework di personalizzazione degli account AWS Control Tower, Account Factory for Terraform (AFT), ora supporta tre configurazioni opzionali aggiuntive al momento della distribuzione. Puoi distribuire AFT in un cloud privato virtuale (VPC) personalizzato, specificare il nome del progetto Terraform per la tua distribuzione AFT e contrassegnare le risorse create da AFT.

Per ulteriori informazioni, consulta [Deploy AWS Control Tower Account Factory for Terraform \(AFT\)](#).

AWS Control Tower introduce la reportistica a livello di account per le API di base

12 maggio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Ora puoi visualizzare la deriva e lo stato di registrazione degli account in modo programmatico per i tuoi account gestiti, richiamando le API di base. Grazie a questa funzionalità, puoi identificare quando le configurazioni di base dell'account e dell'unità organizzativa sono alterate o non sincronizzate. Per visualizzare lo stato di deriva a livello di codice, puoi chiamare l'API per le baseline abilitate. [ListEnabledBaselines](#) Per visualizzare gli stati dei singoli account in modo programmatico con l'API, usa il flag. `ListEnabledBaselines includeChildren` Puoi filtrare in base a questi stati e visualizzare solo gli account e le unità organizzative che richiedono la tua attenzione.

[AWS ControlTowerBaseline](#) Imposta le configurazioni, i controlli e le risorse ottimali necessari per la governance. Quando abiliti questa linea di base su un'unità organizzativa (OU), gli account dei membri all'interno dell'unità organizzativa vengono registrati automaticamente in AWS Control Tower. Le API di base di AWS Control Tower includono il CloudFormation supporto, che consente di creare automazioni che gestiscono le unità organizzative e gli account con Infrastructure as code (IaC).

Per ulteriori informazioni su queste API, consulta le [linee di base](#) nella Guida per l'utente di AWS Control Tower. Le API di base e le funzionalità di reporting appena lanciate per la deriva e lo stato di registrazione degli account sono disponibili ovunque sia disponibile AWS Control Tower. Regioni AWS Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la tabella. [Regione AWS](#)

AWS Control Tower è disponibile in AWS Regioni dell'Asia Pacifico (Thailandia) e del Messico (centrale)

9 maggio 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è ora disponibile nelle seguenti AWS regioni:

- Asia Pacifico (Thailandia)
- Messico (centrale)

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

Aggiuntivo AWS Config controlli disponibili

11 aprile 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta altre 223 AWS Config regole gestite per vari casi d'uso, come sicurezza, costi, durata e operazioni. Con questo lancio, ora puoi usare AWS Control Tower per cercare e scoprire le AWS Config regole di cui hai bisogno per governare il tuo ambiente con più account; quindi abilitare e gestire i controlli direttamente da AWS Control Tower.

Per iniziare dalla console AWS Control Tower, vai al Control Catalog e cerca i controlli con il filtro di implementazione AWS Config. Puoi abilitare i controlli direttamente dalla console AWS Control Tower.

Per maggiori dettagli, consulta AWS Config Controlli [integrati disponibili in AWS Control Tower](#).

Con questo lancio, abbiamo aggiornato le `GetControl` API `ListControls` and per supportare tre nuovi campi: `CreateTime` `Severity` e `Implementation`, che puoi utilizzare quando cerchi un controllo in Control Catalog. Ad esempio, ora puoi trovare a livello di codice AWS Config le regole ad alta severità create dopo l'ultima valutazione.

Puoi cercare le nuove AWS Config regole Regioni AWS ovunque sia disponibile AWS Control Tower. Per distribuire una regola, consulta l'elenco delle regole supportate Regioni AWS per quella regola, per vedere dove può essere abilitata.

Annulla la registrazione e l'eliminazione delle azioni per le unità organizzative

8 aprile 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta azioni separate sulla console per annullare la registrazione di un'unità organizzativa ed eliminarla. È necessario annullare la registrazione dell'unità organizzativa prima di eliminarla. Puoi rimuovere un'unità organizzativa da AWS Control Tower annullando la registrazione.

Per ulteriori informazioni, consulta [Rimuovere un'unità organizzativa](#).

Control Catalog supporta gli indirizzi IPv6

2 aprile 2025

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

L'API AWS Control Tower Control Catalog ora supporta gli indirizzi Internet Protocol version 6 (IPv6) tramite i nostri nuovi endpoint dual-stack. Gli endpoint Control Catalog esistenti che supportano IPv4 rimangono disponibili per la compatibilità con le versioni precedenti. I nuovi domini dual-stack sono disponibili [da Internet](#) o all'interno di un Amazon Virtual Private [Cloud \(VPC\) utilizzando](#) [AWS PrivateLink](#)

gennaio - dicembre 2024

Nel 2024, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Supporti GitHub AWS Control Tower cFCT e RCP](#)
- [AWS Control Tower aggiunge controlli preventivi con policy dichiarative](#)
- [AWS Control Tower aggiunge opzioni di piano di backup prescrittive](#)
- [AWS Control Tower si integra AWS Config controlli](#)
- [AWS Control Tower migliora la gestione degli hook e aggiunge regioni di controllo proattive](#)
- [AWS Control Tower lancia politiche di controllo delle risorse gestite](#)
- [AWS Control Tower segnala una deriva delle politiche di controllo](#)
- [Nuova API ResetEnabledControl](#)
- [API di controllo degli aggiornamenti del catalogo GetControl](#)
- [AWS Control Tower AFT supporta GitLab](#)
- [AWS Control Tower è disponibile in AWS Regione Asia Pacifico \(Malesia\)](#)
- [AWS Control Tower supporta fino a 1000 account per unità organizzativa](#)

- [AWS Control Tower aggiunge la selezione della versione della zona di destinazione](#)
- [API di controllo descrittiva disponibile, accesso esteso a regioni e controlli](#)
- [AWS Control Tower supporta AFT e cFCT nelle regioni opt-in](#)
- [AWS Control Tower aggiunge l'API ListLandingZoneOperations](#)
- [AWS Control Tower supporta fino a 100 operazioni di controllo simultanee](#)
- [AWS Control Tower è disponibile in AWS Canada occidentale \(Calgary\)](#)
- [AWS Control Tower supporta l'adeguamento delle quote in modalità self-service](#)
- [AWS Control Tower rilascia il Guida di riferimento ai controlli](#)
- [AWS Control Tower aggiorna e rinomina due controlli proattivi](#)
- [I controlli obsoleti non sono più disponibili](#)
- [AWS Control Tower supporta l'etichettatura EnabledControl delle risorse in CloudFormation](#)
- [AWS Control Tower supporta le API per la registrazione e la configurazione delle unità organizzative con linee di base](#)

Supporti GitHub AWS Control Tower cFCT e RCP

9 dicembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta GitHub TM™ come opzione per un sistema di controllo della versione (VCS) di terze parti e fonte di configurazione per Customizations for AWS Control Tower (CFCT). Per ulteriori informazioni, consulta [Imposta GitHub come fonte di configurazione](#).

AWS Control Tower ora supporta le politiche di controllo delle risorse (RCP) per le personalizzazioni per AWS Control Tower (CFCT). Per ulteriori informazioni, consulta [Guida alla personalizzazione cFCT](#).

AWS Control Tower aggiunge controlli preventivi con policy dichiarative

1 dicembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta i controlli preventivi implementati da AWS Organizations politiche dichiarative di. Le policy dichiarative vengono applicate direttamente a livello di servizio. Questo approccio garantisce l'applicazione della configurazione specificata, anche quando il servizio

introduce nuove funzionalità o API. Per ulteriori informazioni, consulta Controlli implementati con politiche dichiarative. <https://docs.aws.amazon.com/controltower/latest/controlreference/declarative-controls.html>

AWS Control Tower aggiunge opzioni di piano di backup prescrittive

25 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta AWS Backup piani prescrittivi che consentono di incorporare un flusso di lavoro di backup e ripristino dei dati direttamente nella zona di destinazione. Il piano di backup include regole predefinite, come i giorni di conservazione, la frequenza dei backup e la finestra temporale durante la quale viene eseguito il backup. Queste regole definiscono come eseguire il backup AWS delle risorse su tutti gli account membri gestiti. Quando applichi un piano di backup alla zona di destinazione, AWS Control Tower garantisce che il piano sia coerente per tutti gli account dei membri e in linea con le raccomandazioni sulle migliori pratiche di AWS Backup.

Per ulteriori informazioni, consulta [AWS Backup e AWS Control Tower](#).

AWS Control Tower si integra AWS Config controlli

21 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha integrato alcuni AWS Config controlli, in modo che possano essere visualizzati e gestiti da AWS Control Tower.

Per ulteriori informazioni, consulta AWS Config Controlli [integrati disponibili in AWS Control Tower](#)

AWS Control Tower migliora la gestione degli hook e aggiunge regioni di controllo proattive

20 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Con questa versione, puoi utilizzare tutta la capacità degli CloudFormation hook, senza restrizioni di AWS Control Tower. Inoltre, i controlli proattivi sono disponibili nella regione Canada occidentale (Calgary) e nella regione Asia Pacifico (Malesia).

In precedenza, tutti gli CloudFormation hook presenti nell'ambiente dovevano essere protetti dal CT.CLOUDFORMATION.PR.1 controllo, in modo che solo AWS Control Tower potesse modificarli. Con questa versione, puoi distribuire CloudFormation hook e modificarli, senza le restrizioni precedentemente richieste dal servizio AWS Control Tower.

Se attualmente utilizzi controlli proattivi, puoi passare a questa funzionalità di hook migliorata. Per reimpostare tutti i controlli proattivi su un'unità organizzativa, reimposta ogni singolo controllo proattivo attivo su tale unità organizzativa. Puoi eseguire il ripristino chiamando l'`ResetEnabledControlAPI` o aggiornando il controllo dalla console, con la funzionalità `Reset`. Quando completi questa attività di ripristino per qualsiasi controllo proattivo, AWS Control Tower sposta tutti gli hook di controllo proattivi sull'unità organizzativa nella nuova funzionalità. Ripeti questa procedura per ogni unità organizzativa che implementa controlli proattivi.

Dopo aver ripristinato qualsiasi controllo proattivo, rimuovi il controllo sulle unità organizzative di AWS CT.CLOUDFORMATION.PR.1 Control Tower, a meno che tu non abbia abilitato quel controllo per un altro scopo. Se non disattivi il CT.CLOUDFORMATION.PR.1 controllo, non sarai in grado di creare e modificare gli altri CloudFormation hook.

Per ulteriori informazioni, consulta [Aggiornare gli hook di controllo proattivi](#).

AWS Control Tower lancia politiche di controllo delle risorse gestite

15 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower offre un nuovo tipo di controllo preventivo, implementato con politiche di controllo delle risorse (RCP). Questi controlli ti aiutano a stabilire un perimetro di dati nell'ambiente AWS Control Tower, per proteggere le tue risorse da accessi non intenzionali.

Ad esempio, puoi abilitare RCP-based i controlli per Amazon S3, Servizio di token di sicurezza AWS AWS Key Management Service, Amazon SQS e i servizi. AWS Secrets Manager Un RCP-based controllo può imporre un requisito come «Richiedi che le risorse Amazon S3 dell'organizzazione siano accessibili solo dai principali IAM che appartengono all'organizzazione o da un AWS servizio», indipendentemente dalle autorizzazioni concesse sulle singole policy dei bucket.

È possibile configurare i nuovi RCP-based controlli e alcuni controlli SCP-based preventivi esistenti per specificare le esenzioni AWS IAM per i principali e le risorse. Se non desideri che un principale o una risorsa siano governati dal controllo, puoi configurare un'esenzione.

Combinando i controlli preventivi, proattivi e investigativi in AWS Control Tower, puoi monitorare se il tuo AWS ambiente multi-account è sicuro e gestito secondo le migliori pratiche, come lo standard [AWS Foundational Security Best Practices](#).

Questi nuovi controlli RCP-based preventivi sono disponibili Regioni AWS laddove è disponibile AWS Control Tower. Per un elenco completo dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower segnala una deriva delle politiche di controllo

15 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora segnala una variazione delle politiche di controllo, per i controlli implementati con politiche di controllo delle risorse (RCP) e per i controlli che fanno parte dello Service-managed standard Security Hub CSPM: AWS Control Tower. Questo tipo di deriva può essere corretto tramite la nuova API. `ResetEnabledControl` Per ulteriori informazioni, consulta [Tipi di deriva della governance](#).

Nuova API `ResetEnabledControl`

14 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower annuncia una nuova API per aiutarti a gestire la deriva del controllo in modo programmatico. Puoi riparare il control drift e ripristinare un controllo alla configurazione prevista. L'`ResetEnabledControl` API funziona con i controlli AWS Control Tower opzionali, inclusi i controlli fortemente consigliati ed elettivi.

Eccezioni di controllo

- I controlli implementati con le politiche di controllo del servizio (SCP) non possono essere ripristinati con questa API. Per ulteriori informazioni, consulta [ResetEnabledControl](#).
- I controlli obbligatori non possono essere ripristinati perché proteggono le risorse di AWS Control Tower.
- La regione che nega il controllo della zona di atterraggio deve essere ripristinata tramite la console.

La deriva del controllo si verifica quando un controllo AWS Control Tower viene modificato all'esterno di AWS Control Tower, ad esempio dalla AWS Organizations console. La risoluzione della deriva aiuta a garantire la conformità ai requisiti di governance.

API di controllo degli aggiornamenti del catalogo **GetControl**

8 novembre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta un'GetControlAPI aggiornata che include due nuovi campi: `Implementation` tipi per tutti i controlli e `Parameters` per determinati controlli che possono essere configurati.

L'GetControlAPI fa parte dello spazio dei `controlcatalog` nomi di AWS Control Tower.

Per ulteriori informazioni, consulta l'[GetControlAPI](#) nel Control Catalog API Reference.

Questa versione include le modifiche correlate mostrate nella console AWS Control Tower.

- Il valore dei `Implementation` parametri di tutti i AWS Security Hub CSPM controlli esistenti è cambiato da AWS Config regola a AWS Security Hub CSPM. Il pannello di aiuto della console corrispondente viene modificato per riflettere questa modifica.
- Il valore del `Implementation` parametro di tutti i controlli Hook esistenti è cambiato da CloudFormation guard rule a CloudFormation hook. Il pannello di aiuto della console corrispondente viene modificato per riflettere questa modifica.

AWS Control Tower AFT supporta GitLab

23 ottobre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta la GitLab TM™ e GitLab Self-managed come opzioni per un sistema di controllo della versione (VCS) di terze parti e una fonte di configurazione per Account Factory for Terraform (AFT).

AWS Control Tower è disponibile in AWS Regione Asia Pacifico (Malesia)

21 ottobre 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è disponibile nella regione AWS Asia Pacifico (Malesia).

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

AWS Control Tower supporta fino a 1000 account per unità organizzativa

30 agosto 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aumentato il numero massimo di account consentiti per unità organizzativa (OU) da 300 a 1000. Ora puoi iscrivere fino a 1000 Account AWS alla governance di AWS Control Tower contemporaneamente, senza modificare la struttura dell'unità organizzativa. I processi di registrazione e ri-registrazione dell'unità organizzativa sono inoltre più efficienti e richiedono molto meno tempo per distribuire le risorse di base di AWS Control Tower nei tuoi account.

Alcune limitazioni degli account si applicano ancora a causa delle limitazioni sul numero di CloudFormation stack set disponibili. In particolare, il numero massimo di account che puoi iscrivere in un'unità organizzativa può variare a seconda del numero di regioni che hai sotto la governance. Per ulteriori informazioni, consulta la sezione [Limitazioni basate sui AWS servizi sottostanti](#) nella Guida [per l'utente di](#) AWS Control Tower. Per un elenco completo dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge la selezione della versione della zona di destinazione

15 agosto 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Se utilizzi AWS Control Tower landing zone versione 3.1 e successive, puoi aggiornare o riparare la zona di destinazione nella versione corrente oppure puoi passare a una versione a tua scelta. In precedenza, qualsiasi aggiornamento o riparazione della zona di atterraggio richiedeva un aggiornamento alla versione più recente.

Con la selezione della versione della zona di destinazione, hai una maggiore flessibilità per pianificare gli aggiornamenti della versione mentre valuti le potenziali modifiche al tuo ambiente. Non è necessario scegliere tra la riparazione della deriva per mantenere la conformità, l'aggiornamento

delle configurazioni della zona di atterraggio o l'aggiornamento alla versione più recente della zona di atterraggio. Se utilizzi la versione 3.1 o successiva della zona di atterraggio, puoi scegliere di rimanere sulla versione corrente o passare a una versione più recente quando aggiorni o ripristini le configurazioni della zona di atterraggio.

API di controllo descrittiva disponibile, accesso esteso a regioni e controlli

6 agosto 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto due nuove operazioni API che consentono di trovare ulteriori informazioni sui controlli disponibili, a livello di programmazione. Questa funzionalità semplifica l'implementazione dei controlli con l'automazione.

- L'[GetControl](#) API restituisce i dettagli su un controllo abilitato, tra cui l'identificatore di destinazione, un riepilogo delle informazioni di controllo, un elenco di regioni di destinazione e lo stato di deriva.
- L'[ListControls](#) API restituisce un elenco suddiviso in pagine di tutti i controlli disponibili nella libreria di controlli AWS Control Tower.

Queste API sono raggiungibili tramite il namespace [AWS Control Catalog](#). Il AWS Control Catalog fa parte di AWS Control Tower, che include controlli che aiutano a gestire altri AWS servizi, non solo AWS Control Tower. Questo catalogo esteso consolida i controlli di diversi AWS servizi, in modo da poter visualizzare AWS i controlli in base ad alcuni casi d'uso comuni, come: sicurezza, costi, durata e operazioni. Per ulteriori informazioni, consulta [il riferimento](#) alle API di Control Catalog.

Disponibilità estesa nelle regioni

A partire da questa versione, puoi estendere la governance di AWS Control Tower Regioni AWS laddove alcuni dei tuoi controlli (già) abilitati non siano disponibili. Inoltre, ora puoi abilitare determinati controlli in più regioni, anche se il controllo non è supportato in tutte le regioni governate.

In precedenza, AWS Control Tower impediva di estendere la governance alle regioni o di abilitare i controlli, mentre non offriva coerenza tra tutti i controlli abilitati e le regioni governate. Con questa versione, hai maggiore flessibilità e maggiore responsabilità nell'assicurare che la configurazione sia corretta per tutti i controlli abilitati e tutte le regioni governate. Le API di controllo di [AWS Control Tower](#) e le API del catalogo di [controllo](#) possono aiutarti a ottenere informazioni sulle AWS regioni in cui sei protetto dai controlli abilitati e sulle regioni in cui possono essere distribuiti controlli

aggiuntivi. Le informazioni su regioni e controlli sono disponibili anche nella console AWS Control Tower.

AWS Control Tower supporta AFT e cFCT nelle regioni opt-in

18 luglio 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Oggi, i framework di personalizzazione di AWS Control Tower Account Factory for Terraform (AFT) e Customizations for AWS Control Tower (cFCT) sono disponibili in altri cinque Regioni AWS: Asia Pacifico (Hyderabad, Jakarta e Osaka), Israele (Tel Aviv) e Medio Oriente (Emirati Arabi Uniti).

Account Factory for Terraform (AFT) crea una pipeline Terraform per aiutarti a fornire e personalizzare gli account in AWS Control Tower. Customizations for AWS Control Tower (cFCT) ti aiuta a personalizzare la zona di destinazione e gli account di AWS Control Tower con CloudFormation modelli e policy di controllo dei servizi (SCP).

Per saperne di più, visita le pagine Account Factory for Terraform e Customizations for AWS Control Tower, nella Guida per l'utente di AWS Control Tower. Potresti anche voler consultare le note di rilascio sulla pagina Github di AFT e sulla pagina Github di cFCT. AFT e cFCT sono supportati in tutte AWS le regioni, con alcune eccezioni. Per informazioni specifiche, consulta [Limitazioni regionali](#).

AWS Control Tower aggiunge l'API **ListLandingZoneOperations**

26 giugno 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto un'API che consente di recuperare un elenco delle operazioni applicate di recente alla zona di atterraggio e delle operazioni attualmente in corso. L'API può restituire la cronologia delle operazioni sulle zone di atterraggio e i relativi identificatori per un massimo di 90 giorni. Per esempi di utilizzo, consulta [Visualizzare lo stato delle operazioni nella zona di atterraggio](#).

Per ulteriori informazioni sull'`ListLandingZoneOperations` API, consulta [ListLandingZoneOperations](#) l'AWS Control Tower API Reference.

AWS Control Tower supporta fino a 100 operazioni di controllo simultanee

20 maggio 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta più operazioni di controllo con una maggiore concorrenza. Puoi inviare fino a 100 operazioni di controllo di AWS Control Tower, su più unità organizzative (OU), contemporaneamente, dalla console o con le API. È possibile eseguire fino a dieci (10) operazioni contemporaneamente e quelle aggiuntive vengono messe in coda. In questo modo, è possibile impostare una configurazione più standardizzata su più configurazioni Account AWS, senza l'onere operativo di operazioni di controllo ripetitive.

Per monitorare lo stato delle operazioni di controllo in corso e in coda, puoi accedere alla nuova pagina Operazioni recenti nella console AWS Control Tower oppure puoi chiamare la nuova API.

[ListControlOperations](#)

La libreria AWS Control Tower contiene più di 500 controlli, mappati a diversi obiettivi, framework e servizi di controllo. Per un obiettivo di controllo specifico, come Encrypt data at rest, puoi abilitare più controlli con una singola operazione di controllo, per aiutarti a raggiungere l'obiettivo. Questa funzionalità facilita lo sviluppo accelerato, consente un'adozione più rapida dei controlli basati sulle best practice e attenua le complessità operative.

AWS Control Tower è disponibile in AWS Canada occidentale (Calgary)

3 maggio 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

A partire da oggi, puoi attivare AWS Control Tower nella regione Canada occidentale (Calgary). Se hai già implementato AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione, puoi farlo con le API delle zone di [destinazione di AWS Control Tower](#). Oppure dalla console, vai alla pagina delle impostazioni nella dashboard di AWS Control Tower, seleziona le regioni e aggiorna la tua zona di destinazione.

La regione Canada West (Calgary) non supporta AWS Service Catalog. Per questo motivo, alcune funzionalità di AWS Control Tower sono diverse. La modifica di funzionalità più importante è che Account Factory non è disponibile. Se scegli Canada West (Calgary) come regione di residenza, le procedure per l'aggiornamento degli account, l'impostazione delle automazioni degli account e qualsiasi altro processo che coinvolge Service Catalog sono diverse rispetto alle altre regioni.

Account di provisioning

Per creare ed effettuare il provisioning di un nuovo account nella regione Canada West (Calgary), ti consigliamo di creare un account al di fuori di AWS Control Tower e quindi di registrarlo in un'unità

organizzativa registrata. Per ulteriori informazioni, consulta [Registrare un account esistente](#) e [Procedure per registrare un account](#).

Le API del Service Catalog non sono disponibili nella regione Canada occidentale (Calgary). Lo script di esempio mostrato in [Automate il provisioning degli account in AWS Control Tower tramite le API di Service Catalog non è utilizzabile](#).

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) e Customizations for AWS Control Tower (cFCT) non sono disponibili in Canada occidentale (Calgary), a causa della mancanza di altre dipendenze sottostanti per AWS Control Tower. Se estendi la governance alla regione Canada West (Calgary), puoi continuare a gestire i blueprint AFC in tutte le regioni supportate da AWS Control Tower, purché Service Catalog sia disponibile nella tua regione di origine.

Controlli

Controlli e controlli proattivi per lo AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower non sono disponibili nella regione Canada occidentale (Calgary). Il controllo preventivo non CT.CLOUDFORMATION.PR.1 è disponibile in Canada West (Calgary) perché è richiesto solo per attivare i controlli proattivi basati su hook. Alcuni controlli investigativi basati su non sono disponibili. AWS Config Per informazioni dettagliate, vedi [Limitazioni di controllo](#).

Provider di identità

L'IAM Identity Center non è disponibile in Canada West (Calgary). La procedura consigliata è quella di impostare la zona di atterraggio in una regione in cui è disponibile IAM Identity Center. In alternativa, hai la possibilità di gestire automaticamente la configurazione dell'accesso all'account se utilizzi un provider di identità esterno in Canada West (Calgary).

L'indisponibilità di Service Catalog nella regione Canada occidentale (Calgary) non ha alcun effetto sulle altre regioni supportate da AWS Control Tower. Queste differenze si applicano solo se la tua regione di residenza è Canada occidentale (Calgary).

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

AWS Control Tower supporta l'adeguamento delle quote in modalità self-service

25 aprile 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta l'adeguamento self-service delle quote tramite la console Service Quotas. Per ulteriori informazioni, consulta [Richiesta di un aumento della quota](#).

AWS Control Tower rilascia il Guida di riferimento ai controlli

21 aprile 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha rilasciato la Controls Reference Guide, un nuovo documento in cui è possibile trovare informazioni dettagliate sui controlli specifici dell'ambiente AWS Control Tower. In precedenza, questo materiale era incluso nella Guida per l'utente di AWS Control Tower. La Controls Reference Guide descrive i controlli in un formato esteso. Per ulteriori informazioni, consulta la Guida di riferimento di [AWS Control Tower Controls](#).

AWS Control Tower aggiorna e rinomina due controlli proattivi

26 marzo 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha rinominato due controlli proattivi per allinearli agli aggiornamenti di Amazon Service. OpenSearch

- [\[CT.OPENSEARCH.PR.8\] Richiedi un dominio Elasticsearch Service da utilizzare TLSv1.2](#)
- [\[CT.OPENSEARCH.PR.16 \] Richiedi un dominio Amazon OpenSearch Service da utilizzare TLSv1.2](#)

Abbiamo aggiornato i nomi dei controlli e gli artefatti di questi due controlli per allinearli alla recente versione di Amazon OpenSearch Service, che [ora supporta la versione 1.3 di Transport Layer Security \(TLS\)](#) tra le sue opzioni di sicurezza di trasporto per la sicurezza degli endpoint di dominio.

Per aggiungere il supporto TLSv1.3 per questi controlli, abbiamo aggiornato l'artefatto e il nome dei controlli in modo che riflettano l'intento del controllo. Ora valutano la versione TLS minima del dominio del servizio. Per effettuare questo aggiornamento nel tuo ambiente, devi **disabilitare e abilitare** i controlli per distribuire l'artefatto più recente.

Nessun altro controllo proattivo è interessato da questa modifica. Ti consigliamo di rivedere questi controlli per assicurarti che soddisfino i tuoi obiettivi di controllo.

Per domande o dubbi, contatta l'[AWS assistenza](#).

I controlli obsoleti non sono più disponibili

12 marzo 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower).

AWS Control Tower ha reso obsoleti alcuni controlli. Questi controlli non sono più disponibili.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower supporta l'etichettatura **EnabledControl** delle risorse in CloudFormation

22 febbraio 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Questa versione di AWS Control Tower aggiorna il comportamento della **EnabledControl** risorsa, per allinearla meglio ai controlli configurabili e per migliorare la capacità di gestire l'ambiente AWS Control Tower con l'automazione. Con questa versione, puoi aggiungere tag alle **EnabledControl** risorse configurabili tramite modelli. CloudFormation In precedenza, era possibile aggiungere tag solo tramite la console e le API di AWS Control Tower.

Le operazioni di AWS Control Tower **GetEnabledControl** e **ListTagsForResource** API vengono aggiornate con questa versione, poiché si basano sulla funzionalità delle **EnabledControl** risorse. **EnableControl**

Per ulteriori informazioni, consulta le **EnabledControl** risorse relative ai [tag in AWS Control Tower](#) e [EnabledControl](#) nella Guida per l'CloudFormation utente.

AWS Control Tower supporta le API per la registrazione e la configurazione delle unità organizzative con linee di base

14 febbraio 2024

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Queste API supportano la registrazione programmatica dell'unità organizzativa durante la `EnableBaseline` chiamata. Quando abiliti una linea di base su un'unità organizzativa, gli account dei membri all'interno dell'unità organizzativa vengono registrati nella governance di AWS Control Tower. Potrebbero essere applicate alcune avvertenze. Ad esempio, la registrazione dell'unità organizzativa tramite la console AWS Control Tower consente controlli opzionali e controlli obbligatori. Quando si chiamano le API, potrebbe essere necessario completare un passaggio aggiuntivo per abilitare i controlli opzionali.

Una linea di base di AWS Control Tower include le migliori pratiche per la governance di AWS Control Tower di un'unità organizzativa e degli account dei membri. Ad esempio, quando si abilita una baseline su un'unità organizzativa, gli account dei membri all'interno dell'unità organizzativa ricevono un gruppo definito di risorse AWS CloudTrail AWS Config, tra cui IAM Identity Center e i ruoli IAM richiesti AWS .

Le linee di base specifiche sono compatibili con specifiche versioni delle zone di destinazione di AWS Control Tower. AWS Control Tower può applicare la linea di base compatibile più recente alla tua zona di atterraggio, quando modifichi le impostazioni della zona di atterraggio. Per ulteriori informazioni, consulta [Compatibilità delle versioni di base delle unità organizzative e delle landing zone](#).

Questa versione include quattro elementi essenziali [Tipi di linee di base](#)

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Con le nuove API e le linee di base definite, puoi registrare le unità organizzative e automatizzare il flusso di lavoro di provisioning delle unità organizzative. Le API possono anche gestire le unità organizzative che sono già soggette alla governance di AWS Control Tower, in modo da poter registrare nuovamente le unità organizzative dopo gli aggiornamenti delle zone di destinazione. Le

API includono il supporto per una CloudFormation EnabledBaseline risorsa, che consente di gestire le unità organizzative con Infrastructure as code (IaC).

API di base

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Agire sulla base di una linea di base per un'unità organizzativa.
- GetEnabledBaseline, ListEnabledBaselines: Scopri le configurazioni per le tue baseline abilitate.
- GetBaselineOperation: visualizza lo stato di una particolare operazione di base.
- ResetEnabledBaseline: corregge la deriva delle risorse su un'unità organizzativa con una baseline abilitata (incluse le unità organizzative annidate e la deriva dei controlli obbligatoria). Inoltre, corregge la deriva a livello di zona di atterraggio e nega il controllo
- GetBaseline, ListBaselines: Scopri i contenuti delle linee di base di AWS Control Tower.

Per ulteriori informazioni su queste API, consulta le [linee di base nella Guida per l'utente di AWS Control Tower e](#) nell'API Reference. https://docs.aws.amazon.com/controltower/latest/APIReference/API_Operations.html Le nuove API sono disponibili Regioni AWS dove è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la Regione AWS tabella.

gennaio - dicembre 2023

Nel 2023, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno \(fase 3\)](#)
- [Zona di destinazione di AWS Control Tower versione 3.3](#)
- [Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno \(fase 2\)](#)
- [AWS Control Tower annuncia i controlli per agevolare la sovranità digitale](#)
- [API per le zone di destinazione di AWS Control Tower](#)
- [API di tagging di controllo di AWS Control Tower](#)
- [AWS Control Tower è disponibile in AWS Asia Pacifico \(Melbourne\)](#)
- [Transizione verso una nuova AWS Service Catalog Tipo di prodotto esterno \(fase 1\)](#)
- [AWS Control Tower aggiunge una nuova API di controllo](#)
- [AWS Control Tower aggiunge nuovi controlli](#)

- [AWS Control Tower rileva una deriva attendibile degli accessi](#)
- [AWS Control Tower è disponibile in quattro versioni aggiuntive Regioni AWS](#)
- [AWS Control Tower è disponibile in AWS Israele \(Tel Aviv\)](#)
- [AWS Control Tower aggiunge 28 nuovi controlli proattivi](#)
- [AWS Control Tower rende obsoleti due controlli](#)
- [Zona di destinazione di AWS Control Tower versione 3.2](#)
- [AWS Control Tower aggiunge la mappatura da email a ID per IAM Identity Center](#)
- [AWS Control Tower ne aggiunge altre AWS Security Hub CSPM controlli](#)
- [AWS Control Tower pubblica metadati per AWS Security Hub CSPM controlli](#)
- [AWS Control Tower aggiunge Account Factory Customization \(AFC\) per Terraform](#)
- [AWS Control Tower aggiunge un centro di identità IAM autogestito](#)
- [AWS Control Tower aggiunge una nota di governance mista](#)
- [AWS Control Tower aggiunge nuovi controlli proattivi](#)
- [AWS Control Tower aggiorna i controlli Amazon EC2](#)
- [AWS Control Tower è disponibile in sette versioni aggiuntive Regioni AWS](#)
- [AWS Control Tower Account Factory Customization \(AFC\) e tracciamento delle richieste sono generalmente disponibili](#)
- [Zona di destinazione di AWS Control Tower versione 3.1](#)
- [I controlli proattivi di AWS Control Tower sono generalmente disponibili](#)

Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 3)

14 dicembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower non supporta più Terraform Open Source come tipo di prodotto (modello) durante la creazione di nuovi prodotti. Account AWS Per ulteriori informazioni e istruzioni sull'aggiornamento dei blueprint dell'account, consulta la sezione Transition to the External ([Transizione al tipo di prodotto AWS Service Catalog esterno](#)).

Se non aggiorni i blueprint del tuo account per utilizzare il tipo di prodotto esterno, puoi aggiornare o chiudere solo gli account di cui hai effettuato il provisioning utilizzando i blueprint Open Source Terraform.

Zona di destinazione di AWS Control Tower versione 3.3

14 dicembre 2023

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower alla versione 3.3. Per informazioni, consulta [Aggiorna la tua landing zone](#)).

Aggiornamenti alla policy dei bucket S3 nell'account AWS Control Tower Audit

Abbiamo modificato la policy dei bucket di Amazon S3 Audit che AWS Control Tower implementa negli account, in modo che sia soddisfatta una `aws:SourceOrgID` condizione per qualsiasi autorizzazione di scrittura. Con questa versione, AWS i servizi hanno accesso alle tue risorse solo quando la richiesta proviene dalla tua organizzazione o unità organizzativa (OU).

È possibile utilizzare la chiave di `aws:SourceOrgID` condizione e impostare il valore sull'ID dell'organizzazione nell'elemento di condizione della policy del bucket S3. Questa condizione garantisce che CloudTrail solo i log per conto degli account all'interno dell'organizzazione possano essere scritti nel bucket S3; impedisce che i CloudTrail log esterni all'organizzazione vengano scritti nel bucket S3 di AWS Control Tower.

Abbiamo apportato questa modifica per rimediare a una potenziale vulnerabilità di sicurezza, senza influire sulla funzionalità dei carichi di lavoro esistenti. Per visualizzare la policy aggiornata, consulta [Policy sui bucket di Amazon S3 per la registrazione](#)

Per ulteriori informazioni sulla nuova chiave di condizione, consulta la documentazione IAM e il post sul blog IAM intitolato "Usa controlli scalabili per i AWS servizi che accedono alle tue risorse».

Aggiornamenti alla policy nell'argomento AWS Config SNS

Abbiamo aggiunto la nuova chiave `aws:SourceOrgID` condizionale alla policy per l'argomento AWS Config SNS. Per visualizzare la politica aggiornata, vedi [La politica sull'argomento SNS. AWS Config](#)

Aggiornamenti alla zona di atterraggio Region Deny control

- Rimosso `discovery-marketplace:`. Questa azione è coperta dall'`aws-marketplace:*esenzione`.
- Aggiunto `quicksight:DescribeAccountSubscription`

Modello aggiornato CloudFormation

Abbiamo aggiornato il CloudFormation modello per lo stack denominato BASELINE-CLLOUDTRAIL-MASTER in modo che non mostri deviazioni quando non viene utilizzata AWS KMS la crittografia.

Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 2)

7 dicembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

HashiCorp hanno aggiornato le loro licenze Terraform. Di conseguenza, AWS Service Catalog ha modificato il supporto per i prodotti Terraform Open Source e ha fornito i prodotti a un nuovo tipo di prodotto, chiamato External.

Per evitare interruzioni dei carichi di lavoro e AWS delle risorse esistenti nei tuoi account, segui le fasi di transizione di AWS Control Tower nella sezione [Transizione al tipo di prodotto AWS Service Catalog esterno](#) entro il 14 dicembre 2023.

AWS Control Tower annuncia i controlli per agevolare la sovranità digitale

27 novembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower annuncia 65 nuovi controlli AWS gestiti, per aiutarti a soddisfare i tuoi requisiti di sovranità digitale. Con questa versione, puoi scoprire questi controlli sotto un nuovo gruppo di sovranità digitale nella console AWS Control Tower. Puoi utilizzare questi controlli per prevenire azioni e rilevare modifiche alle risorse riguardanti la residenza dei dati, la restrizione granulare dell'accesso, la crittografia e le funzionalità di resilienza. Questi controlli sono progettati per semplificare la gestione dei requisiti su larga scala. Per ulteriori informazioni sui controlli della sovranità digitale, vedi [Controlli che migliorano la protezione della sovranità digitale](#).

Ad esempio, puoi scegliere di abilitare i controlli che aiutano a far rispettare le tue strategie di crittografia e resilienza, come Richiedi una cache AWS AppSync API per avere la crittografia in transito abilitata o Richiedi l'implementazione di un firewall di AWS rete in più zone di disponibilità. Puoi anche personalizzare il sistema di negazione del controllo della regione AWS Control Tower per applicare le restrizioni regionali che meglio si adattano alle tue esigenze aziendali specifiche.

Questa versione offre funzionalità di negazione delle regioni AWS Control Tower ben migliorate. Puoi applicare un nuovo controllo di negazione regionale parametrizzato a livello di unità organizzativa, per una maggiore granularità della governance, mantenendo al contempo una governance regionale aggiuntiva a livello di zona di destinazione. Questo controllo dei rifiuti regionali personalizzabile ti

aiuta ad applicare le restrizioni regionali che meglio si adattano alle tue esigenze aziendali specifiche. Per ulteriori informazioni sul nuovo controllo di negazione regionale configurabile, consulta Controllo di rifiuto [regionale applicato all'unità organizzativa](#).

Come nuovo strumento del nuovo potenziamento Region Deny, questa versione include una nuova API che consente di ripristinare `UpdateEnabledControl` i controlli abilitati alle impostazioni predefinite. Questa API è particolarmente utile nei casi d'uso in cui è necessario risolvere rapidamente la deriva o per garantire a livello di codice che un controllo non sia in uno stato di deriva. Per ulteriori informazioni sulla nuova API, consulta l'AWS Control Tower API [Reference](#)

Nuovi controlli proattivi

- CT.APIGATEWAY.PR.6: richiedi a un dominio REST Amazon API Gateway di utilizzare una policy di sicurezza che specifichi una versione minima del protocollo TLS di TLSv1.2
- CT.APPSYNC.PR.2: richiede un'API AWS AppSync GraphQL da configurare con visibilità privata
- CT.APPSYNC.PR.3: richiede che un'API AWS AppSync GraphQL non sia autenticata con le chiavi API
- CT.APPSYNC.PR.4: richiede una cache dell'API AWS AppSync GraphQL per abilitare la crittografia in transito.
- CT.APPSYNC.PR.5: richiede una cache dell'API AWS AppSync GraphQL per abilitare la crittografia a riposo.
- CT.AUTOSCALING.PR.9: richiedi un volume Amazon EBS configurato tramite una configurazione di avvio di Amazon EC2 Auto Scaling per crittografare i dati inattivi
- CT.AUTOSCALING.PR.10: richiedi a un gruppo Amazon EC2 Auto Scaling di utilizzare solo i tipi di istanze AWS Nitro quando sovrascrive un modello di avvio
- CT.AUTOSCALING.PR.11: richiedi solo i tipi di istanze AWS Nitro che supportano la crittografia del traffico di rete tra le istanze da aggiungere a un gruppo Amazon EC2 Auto Scaling, quando si sovrascrive un modello di avvio
- CT.DAX.PR.3: richiedi un cluster DynamoDB Accelerator per crittografare i dati in transito con Transport Layer Security (TLS)
- CT.DMS.PR.2: Richiede un endpoint AWS Database Migration Service (DMS) per crittografare le connessioni per gli endpoint di origine e di destinazione
- CT.EC2.PR.15: richiedi che un'istanza Amazon EC2 utilizzi un tipo di istanza AWS Nitro durante la creazione dal tipo di risorsa `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: richiedi che un'istanza Amazon EC2 utilizzi un tipo di istanza AWS Nitro quando viene creata utilizzando il tipo di risorsa `AWS::EC2::Instance`

- CT.EC2.PR.17: richiedi un host dedicato Amazon EC2 per utilizzare un tipo di istanza AWS Nitro
- CT.EC2.PR.18: richiedi a una flotta Amazon EC2 di sovrascrivere solo i modelli di avvio con tipi di istanze Nitro AWS
- CT.EC2.PR.19: richiedi a un'istanza Amazon EC2 di utilizzare un tipo di istanza nitro che supporti la crittografia in transito tra le istanze quando viene creata utilizzando il tipo di risorsa `AWS::EC2::Instance`
- CT.EC2.PR.20: richiedi a una flotta Amazon EC2 di sovrascrivere solo i modelli di avvio con tipi di istanze AWS Nitro che supportano la crittografia in transito tra le istanze
- CT.ELASTICACHE.PR.8: richiedi un gruppo di ElastiCache replica Amazon di versioni successive di Redis per attivare l'autenticazione RBAC
- CT.MQ.PR.1: richiedi a un broker Amazon MQ ActiveMQ di utilizzare la modalità di distribuzione per l'alta disponibilità active/standby
- CT.MQ.PR.2: richiedi a un broker Amazon MQ Rabbit MQ di utilizzare la modalità Multi-AZ cluster per l'alta disponibilità
- CT.MSK.PR.1: richiedi un cluster Amazon Managed Streaming for Apache Kafka (MSK) per applicare la crittografia in transito tra i nodi del cluster broker
- CT.MSK.PR.2: richiedi la configurazione di un cluster Amazon Managed Streaming for Apache Kafka (MSK) con la disattivazione PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Richiedi la distribuzione di un firewall AWS Network Firewall in più zone di disponibilità
- CT.RDS.PR.26: Richiedi un proxy DB Amazon RDS per richiedere connessioni Transport Layer Security (TLS)
- CT.RDS.PR.27: Richiede un gruppo di parametri del cluster Amazon RDS DB per richiedere connessioni Transport Layer Security (TLS) per i tipi di motore supportati
- CT.RDS.PR.28: richiede un gruppo di parametri Amazon RDS DB per richiedere connessioni Transport Layer Security (TLS) per i tipi di motore supportati
- CT.RDS.PR.29: Richiede che un cluster Amazon RDS non sia configurato per essere accessibile pubblicamente tramite la proprietà " PubliclyAccessible
- CT.RDS.PR.30: richiedi che un'istanza di database Amazon RDS abbia la crittografia a riposo configurata per utilizzare una chiave KMS specificata per i tipi di motore supportati
- CT.S3.PR.12: richiedi che un punto di accesso Amazon S3 abbia una configurazione Block Public Access (BPA) con tutte le opzioni impostate su true

Nuovi controlli preventivi

- CT.APPSYNC.PV.1Richiede che un'API AWS AppSync GraphQL sia configurata con visibilità privata
- CT.EC2.PV.1Richiedi la creazione di un'istanza Amazon EBS da un volume EC2 crittografato
- CT.EC2.PV.2Richiedi che un volume Amazon EBS collegato sia configurato per crittografare i dati inattivi
- CT.EC2.PV.3Richiedi che uno snapshot di Amazon EBS non sia ripristinabile pubblicamente
- CT.EC2.PV.4Richiedi che le API dirette di Amazon EBS non vengano chiamate
- CT.EC2.PV.5Non consentire l'uso dell'importazione ed esportazione di macchine virtuali Amazon EC2
- CT.EC2.PV.6Non consentire l'uso di azioni Amazon EC2 e API obsolete RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1Richiedi una policy AWS KMS chiave per contenere una dichiarazione che limiti la creazione di sovvenzioni ai servizi AWS KMS AWS
- CT.KMS.PV.2Richiedere che una chiave AWS KMS asimmetrica con materiale chiave RSA utilizzato per la crittografia non abbia una lunghezza della chiave di 2048 bit
- CT.KMS.PV.3Richiedi che una AWS KMS chiave sia configurata con la politica di bypass e il controllo di sicurezza del blocco abilitato
- CT.KMS.PV.4Richiedi che una chiave AWS KMS gestita dal cliente (CMK) sia configurata con materiale chiave proveniente da CloudHSM AWS
- CT.KMS.PV.5Richiedi che una chiave AWS KMS gestita dal cliente (CMK) sia configurata con materiale chiave importato
- CT.KMS.PV.6Richiedere che una chiave AWS KMS gestita dal cliente (CMK) sia configurata con materiale chiave proveniente da un key store esterno (XKS)
- CT.LAMBDA.PV.1Richiedi un URL di funzione per utilizzare l'autenticazione AWS Lambda AWS IAM-based
- CT.LAMBDA.PV.2Richiedi che l'URL di una AWS Lambda funzione sia configurato per l'accesso solo da parte dei principali all'interno del tuo Account AWS

API per le zone di destinazione di AWS Control Tower

26 novembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora offre API che ti aiutano a gestire la tua zona di atterraggio in modo programmatico. Queste API consentono di creare, aggiornare e reimpostare la zona di atterraggio, nonché di recuperare informazioni sulla configurazione e sulle operazioni della zona di atterraggio. Per ulteriori informazioni, consulta Esempi di API per le zone di [destinazione](#).

Le API delle zone di destinazione sono disponibili in tutti i paesi in Regioni AWS cui è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

API di tagging di controllo di AWS Control Tower

10 novembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora offre API che consentono di etichettare i controlli abilitati in modo programmatico. Queste API consentono di aggiungere, rimuovere ed elencare i tag per i controlli abilitati. Per ulteriori informazioni, consulta [Tagging delle risorse di AWS Control Tower](#).

Le API di control tagging sono disponibili in tutti i paesi in Regioni AWS cui è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower è disponibile in AWS Asia Pacifico (Melbourne)

3 novembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è disponibile nell'Asia Pacifico (Melbourne). Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

Transizione verso una nuova AWS Service Catalog Tipo di prodotto esterno (fase 1)

31 ottobre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

HashiCorp hanno aggiornato le loro licenze Terraform. Di conseguenza, AWS Service Catalog ha modificato il supporto per i prodotti Terraform Open Source e ha fornito i prodotti a un nuovo tipo di prodotto, chiamato External.

Per evitare interruzioni dei carichi di lavoro e AWS delle risorse esistenti nei tuoi account, segui le fasi di transizione di AWS Control Tower nella sezione [Transizione al tipo di prodotto AWS Service Catalog esterno](#) entro il 14 dicembre 2023.

AWS Control Tower aggiunge una nuova API di controllo

27 ottobre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower offre ora una nuova API che consente di aggiornare i controlli abilitati. `UpdateEnabledControl` Questa API è particolarmente utile nei casi d'uso in cui è necessario risolvere rapidamente la deriva o garantire a livello di programmazione che un controllo non sia in uno stato di deriva. Per ulteriori informazioni sulla nuova API, consulta l'AWS Control Tower API [Reference](#).

L'`UpdateEnabledControlAPI` è disponibile in tutti i paesi in Regioni AWS cui è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge nuovi controlli

20 ottobre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto 22 nuovi controlli alla libreria di controlli AWS Control Tower. Questi controlli ti aiutano ad applicare le migliori pratiche per le tue AWS risorse. Per ulteriori informazioni sui nuovi controlli, consulta [Categorie https://docs.aws.amazon.com/controltower/latest/userguide/control-categories.html](https://docs.aws.amazon.com/controltower/latest/userguide/control-categories.html) di controllo.

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower rileva una deriva attendibile degli accessi

13 ottobre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora rileva e segnala la deriva delle impostazioni di accesso attendibili. Le impostazioni di accesso attendibili consentono ad AWS Control Tower di interagire con altri AWS servizi per tuo conto. Se queste impostazioni vengono modificate all'esterno di AWS Control Tower, AWS Control Tower rileverà la deriva e la segnalerà nella console AWS Control Tower. Per ulteriori informazioni sulla deriva degli accessi affidabili, consulta [Tipi di deriva della governance](#).

Il rilevamento affidabile della deriva degli accessi è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower è disponibile in quattro versioni aggiuntive Regioni AWS

29 settembre 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è disponibile in altre quattro aree Regioni AWS: Asia Pacifico (Hyderabad), Asia Pacifico (Jakarta), Europa (Spagna) ed Europa (Zurigo). Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella. [Regione AWS](#)

AWS Control Tower è disponibile in AWS Israele (Tel Aviv)

1 agosto 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è disponibile in Israele (Tel Aviv). Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge 28 nuovi controlli proattivi

27 luglio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto 28 nuovi controlli proattivi alla libreria di controlli AWS Control Tower. Questi controlli ti aiutano ad applicare le migliori pratiche per le tue AWS risorse. Per ulteriori

informazioni sui nuovi controlli, consulta Categorie <https://docs.aws.amazon.com/controltower/latest/userguide/control-categories.html> di controllo.

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower rende obsoleti due controlli

27 luglio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha reso obsoleti due controlli: CT.CLOUDFORMATION.PR.2 e CT.CLOUDFORMATION.PR.3. Questi controlli non sono più disponibili nella libreria di controlli AWS Control Tower. Per ulteriori informazioni sui controlli obsoleti, consulta Categorie di [controllo](#).

I controlli obsoleti non sono più disponibili in nessuno. Regione AWS

Zona di destinazione di AWS Control Tower versione 3.2

16 giugno 2023

(È richiesto un aggiornamento per la landing zone di AWS Control Tower alla versione 3.2. Per informazioni, consulta [Aggiorna la tua landing zone](#)).

La versione 3.2 della landing zone di AWS Control Tower porta i controlli che fanno parte dello AWS Security Hub CSPM Service-Managed Standard: AWS Control Tower alla disponibilità generale. Introduce la possibilità di visualizzare lo stato di deriva dei controlli che fanno parte di questo standard nella console AWS Control Tower.

Questo aggiornamento include un nuovo ruolo collegato ai servizi (SLR), chiamato. `AWSServiceRoleForAWSControlTower`. Questo ruolo assiste AWS Control Tower creando una regola EventBridge gestita, denominata `AWSControlTowerManagedRule` in ogni account membro. Questa regola gestita raccoglie gli eventi di AWS Security Hub CSPM ricerca e, con AWS Control Tower, può determinare la deriva del controllo.

Questa regola è la prima regola gestita creata da AWS Control Tower. La regola non viene distribuita da uno stack, ma direttamente dalle EventBridge API. È possibile visualizzare la regola nella

EventBridge console o tramite le API. EventBridge Se il managed-by campo è compilato, mostrerà l'entità del servizio AWS Control Tower.

In precedenza, AWS Control Tower assumeva il `AWSControlTowerExecution` ruolo di eseguire operazioni negli account dei membri. Questo nuovo ruolo e questa nuova regola sono meglio allineati al principio delle best practice di concedere il privilegio minimo quando si eseguono operazioni in un ambiente con più AWS account. Il nuovo ruolo fornisce autorizzazioni limitate che consentono specificamente: creare la regola gestita negli account dei membri, mantenere la regola gestita, pubblicare notifiche di sicurezza tramite SNS e verificare la deriva. Per ulteriori informazioni, consulta [AWSServiceRoleForAWSControlTower](#).

L'aggiornamento della zona di destinazione 3.2 include anche una nuova StackSet risorsa nell'account di gestione, `BP_BASELINE_SERVICE_LINKED_ROLE` che inizialmente implementa il ruolo collegato al servizio.

Quando si segnala la deriva del controllo di Security Hub CSPM (nella zona di atterraggio 3.2 e versioni successive), AWS Control Tower riceve un aggiornamento giornaliero dello stato da Security Hub CSPM. Sebbene i controlli siano attivi in ogni regione governata, AWS Control Tower invia gli eventi AWS Security Hub CSPM Finding solo alla regione principale di AWS Control Tower. Per ulteriori informazioni, consulta [Security Hub control drift reporting](#).

Aggiornamento al controllo Region Deny

Questa versione della zona di atterraggio include anche un aggiornamento del controllo Region Deny.

Sono stati aggiunti servizi e API globali

- Gestione costi e fatturazione AWS (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) per consentire la visibilità degli eventi globali negli account dei membri.
- AWS Fatturazione consolidata (`consolidatedbilling:*`)
- AWS Applicazione mobile Management Console (`consoleapp:*`)
- AWS Livello gratuito (`freetier:*`)
- Fatturazione AWS (`invoicing:*`)
- AWS QI (`iq:*`)
- AWS Notifiche utente (`notifications:*`)
- AWS Notifiche utente Contatti (`notifications-contacts:*`)

- Amazon Payments (`payments:*`)
- AWS Impostazioni fiscali (`tax:*`)

Servizi e API globali rimossi

- Rimosso `s3:GetAccountPublic` perché non è un'azione valida.
- Rimossa `s3:PutAccountPublic` perché non è un'azione valida.

AWS Control Tower aggiunge la mappatura da email a ID per IAM Identity Center

13 luglio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta la mappatura da e-mail a ID per IAM Identity Center. Questa funzionalità consente di mappare gli indirizzi e-mail agli ID utente di IAM Identity Center, semplificando la gestione dell'accesso degli utenti all'ambiente AWS Control Tower. Per ulteriori informazioni sulla mappatura da e-mail a ID, consulta [Integrazione con IAM Identity Center](#).

Email-to-ID la mappatura è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower ne aggiunge altre AWS Security Hub CSPM controlli

29 giugno 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto altri AWS Security Hub CSPM controlli alla libreria di controlli AWS Control Tower. Questi controlli ti aiutano ad applicare le migliori pratiche per le tue AWS risorse. Per ulteriori informazioni sui nuovi controlli, consulta Categorie <https://docs.aws.amazon.com/controltower/latest/userguide/control-categories.html> di controllo.

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower pubblica metadati per AWS Security Hub CSPM controlli

22 giugno 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora pubblica i metadati per i controlli. AWS Security Hub CSPM Questi metadati includono informazioni sul controllo, come l'ID del controllo, il titolo del controllo e la descrizione del controllo. Per ulteriori informazioni sui metadati, consulta Metadati di controllo. <https://docs.aws.amazon.com/controltower/latest/userguide/control-metadata.html>

I metadati di controllo sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei Regioni AWS luoghi in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge Account Factory Customization (AFC) per Terraform

15 giugno 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta l'Account Factory Customization (AFC) per Terraform. Questa funzionalità consente di utilizzare Terraform per personalizzare gli account AWS Control Tower. Per ulteriori informazioni su AFC for Terraform, consulta [Account Factory Customization for Terraform](#).

AFC for Terraform è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge un centro di identità IAM autogestito

8 giugno 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta il centro di identità IAM autogestito. Questa funzionalità consente di utilizzare il proprio provider di identità con AWS Control Tower. Per ulteriori informazioni sul centro di identità IAM autogestito, consulta [IAM identity center](#).

Self-managed Il centro di identità IAM è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge una nota di governance mista

1 giugno 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora include una nota sulla governance mista. Questa nota spiega come AWS Control Tower collabora con altri AWS servizi per fornire la governance AWS delle tue risorse. Per ulteriori informazioni sulla governance mista, consulta Governance [mista](#).

La nota sulla governance mista è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiunge nuovi controlli proattivi

25 maggio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiunto nuovi controlli proattivi alla libreria di controlli AWS Control Tower. Questi controlli ti aiutano ad applicare le migliori pratiche per le tue AWS risorse. Per ulteriori informazioni sui nuovi controlli, consulta Categorie <https://docs.aws.amazon.com/controltower/latest/userguide/control-categories.html> di controllo.

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower aggiorna i controlli Amazon EC2

18 maggio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ha aggiornato i controlli Amazon EC2 nella libreria di controlli AWS Control Tower. Questi aggiornamenti migliorano la sicurezza e l'affidabilità del tuo ambiente AWS Control Tower. Per ulteriori informazioni sui controlli aggiornati, consulta Categorie [di controllo](#).

I controlli aggiornati sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower è disponibile in sette versioni aggiuntive Regioni AWS

11 maggio 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower è disponibile in altre sette aree Regioni AWS: Asia Pacifico (Osaka), Canada (Centrale), Europa (Milano), Europa (Stoccolma), Medio Oriente (Bahrain), Medio Oriente (Emirati Arabi Uniti) e Sud America (San Paolo). Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la tabella. [Regione AWS](#)

AWS Control Tower Account Factory Customization (AFC) e tracciamento delle richieste sono generalmente disponibili

27 aprile 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower Account Factory Customization (AFC) e il tracciamento delle richieste sono ora disponibili a livello generale. AFC consente di personalizzare gli account AWS Control Tower e il tracciamento delle richieste consente di monitorare lo stato delle richieste AWS Control Tower. Per ulteriori informazioni su AFC e sul tracciamento delle richieste, consulta [Account Factory Customization e Request tracing](#). <https://docs.aws.amazon.com/controltower/latest/userguide/request-tracing.html>

L'AFC e il tracciamento delle richieste sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

Zona di destinazione di AWS Control Tower versione 3.1

9 febbraio 2023

(Aggiornamento richiesto per la zona di destinazione di AWS Control Tower alla versione 3.1. Per informazioni, consulta [Aggiorna la tua landing zone](#))

La versione 3.1 della landing zone di AWS Control Tower include i seguenti aggiornamenti:

- Con questa versione, AWS Control Tower disattiva la registrazione degli accessi non necessaria per il bucket di registrazione degli accessi, che è il bucket Amazon S3 in cui i log di accesso sono archiviati nell'account Log Archive, continuando ad abilitare la registrazione degli accessi al server per i bucket S3. Questa versione include anche aggiornamenti al controllo Region Deny che consentono azioni aggiuntive per i servizi globali, come Piani e. Supporto AWS Artifact
- La disattivazione della registrazione degli accessi al server per il bucket di registrazione degli accessi di AWS Control Tower fa sì che Security Hub CSPM crei un risultato per il bucket di registrazione degli accessi dell'account Log Archive, a causa di una AWS Security Hub CSPM regola, [\[S3.9\] la registrazione degli accessi al server bucket S3 deve essere abilitata](#). In linea con Security Hub CSPM, ti consigliamo di eliminare questo particolare risultato, come indicato nella descrizione di questa regola nel Security Hub CSPM. Per ulteriori informazioni, consulta le informazioni sui risultati eliminati. <https://docs.aws.amazon.com/securityhub/latest/userguide/finding-workflow-status.html>
- La registrazione degli accessi per il bucket di registrazione (normale) nell'account Log Archive è invariata nella versione 3.1. In linea con le migliori pratiche, gli eventi di accesso per quel bucket vengono registrati come voci di registro nel bucket di registrazione degli accessi. Per ulteriori informazioni sulla registrazione degli accessi, consulta Registrazione delle richieste tramite la [registrazione degli accessi al server nella documentazione di Amazon S3](#).
- Abbiamo effettuato un aggiornamento del controllo Region Deny. Questo aggiornamento consente azioni da parte di più servizi globali. Per informazioni dettagliate su questo SCP, consulta [Negare l'accesso in AWS base a quanto richiesto Regione AWS](#) e [Controlli che migliorano la protezione della residenza dei dati](#).

Servizi globali aggiunti:

- Gestione dell'account AWS (account:*)
- AWS Attiva (activate:*)
- AWS Artifact (artifact:*)
- AWS Billing Conductor (billingconductor:*)
- AWS Compute Optimizer (compute-optimizer:*)
- AWS Data Pipeline (datapipeline:GetAccountLimits)
- AWS Device Farm(devicefarm:*)
- Marketplace AWS (discovery-marketplace:*)
- Amazon ECR () ecr-public:*

- AWS License Manager (license-manager:ListReceivedLicenses)
- AWS vela leggera () lightsail:Get*
- Esploratore di risorse AWS (resource-explorer-2:*)
- Amazon S3 (,) s3:CreateMultiRegionAccessPoint s3:GetBucketPolicyStatus s3:PutMultiRegionAccessPointPolicy
- AWS Piani di risparmio () savingsplans:*
- IAM Identity Center (sso:*)
- AWS Support App (supportapp:*)
- Supporto Piani (supportplans:*)
- AWS Sostenibilità (sustainability:*)
- AWS Resource Groups Tagging API (tag:GetResources)
- Marketplace AWS Informazioni sui fornitori () vendor-insights:ListEntitledSecurityProfiles

I controlli proattivi di AWS Control Tower sono generalmente disponibili

13 aprile 2023

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

I controlli proattivi di AWS Control Tower sono ora disponibili a livello generale. I controlli proattivi ti aiutano ad applicare le migliori pratiche per le tue risorse. AWS Per ulteriori informazioni sui controlli proattivi, consulta [Controlli proattivi](#).

I controlli proattivi sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco dei paesi Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

gennaio - dicembre 2022

Nel 2022, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Operazioni simultanee sugli account](#)
- [Personalizzazione dell'account di fabbrica \(AFC\)](#)
- [I controlli completi aiutano a AWS approvvigionamento e gestione delle risorse](#)

- [Stato di conformità visualizzabile per tutti AWS Config rules](#)
- [API per i controlli e una nuova CloudFormation risorsa](#)
- [cFCT supporta l'eliminazione di set di stack](#)
- [Conservazione personalizzata dei log](#)
- [È disponibile la riparazione di Role Drift](#)
- [Zona di destinazione AWS Control Tower versione 3.0](#)
- [La pagina Organizzazione combina le visualizzazioni delle unità organizzative e degli account](#)
- [Creazione e registrazione dell'account semplificate](#)
- [AFT supporta la personalizzazione automatica per gli account AWS Control Tower condivisi](#)
- [Operazioni simultanee per tutti i controlli opzionali](#)
- [Account di sicurezza e registrazione esistenti](#)
- [Zona di destinazione di AWS Control Tower versione 2.9](#)
- [Zona di destinazione di AWS Control Tower versione 2.8](#)

Operazioni simultanee sugli account

16 dicembre 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta azioni simultanee in account factory. Puoi creare, aggiornare o registrare fino a cinque (5) account alla volta. Invia fino a cinque azioni in successione e visualizza lo stato di completamento di ogni richiesta, mentre la creazione degli account viene completata in background. Ad esempio, non è più necessario attendere il completamento di ogni processo prima di aggiornare un altro account o prima di registrare nuovamente un'intera unità organizzativa (OU).

Personalizzazione dell'account di fabbrica (AFC)

28 novembre 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

La personalizzazione dell'account factory consente di personalizzare account nuovi ed esistenti dall'interno della console AWS Control Tower. Queste nuove funzionalità di personalizzazione

offrono la flessibilità di definire i blueprint degli account, che sono CloudFormation modelli contenuti in un prodotto specializzato di Service Catalog. I blueprint forniscono risorse e configurazioni completamente personalizzate. Puoi anche scegliere di utilizzare blueprint predefiniti, creati e gestiti dai AWS partner, che ti aiutano a personalizzare gli account per casi d'uso specifici.

In precedenza, AWS Control Tower Account Factory non supportava la personalizzazione degli account nella console. Con questo aggiornamento di account factory, puoi predefinire i requisiti dell'account e implementarli come parte di un flusso di lavoro ben definito. Puoi applicare i blueprint per creare nuovi account, iscrivere altri account in AWS Control Tower e aggiornare AWS gli account AWS Control Tower esistenti.

Quando effettui il provisioning, registri o aggiorni un account in account factory, selezionerai il blueprint da distribuire. Il provisioning delle risorse specificate nel blueprint viene effettuato nel tuo account. Una volta completata la creazione dell'account, tutte le configurazioni personalizzate sono immediatamente disponibili per l'uso.

Per iniziare a personalizzare gli account, puoi definire le risorse per il caso d'uso previsto in un prodotto Service Catalog. È inoltre possibile selezionare soluzioni gestite dai partner dalla AWS Getting Started Library. Per ulteriori informazioni, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

I controlli completi aiutano a AWS approvvigionamento e gestione delle risorse

28 novembre 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta una gestione completa dei controlli, inclusi nuovi controlli proattivi opzionali, implementati tramite CloudFormation hook. Questi controlli sono definiti proattivi perché controllano le risorse, prima che le risorse vengano distribuite, per determinare se le nuove risorse saranno conformi ai controlli attivati nel tuo ambiente.

Oltre 130 nuovi controlli proattivi ti aiutano a raggiungere obiettivi politici specifici per il tuo ambiente AWS Control Tower, a soddisfare i requisiti dei framework di conformità standard del settore e a governare le interazioni di AWS Control Tower tra più di venti altri servizi. AWS

La libreria di controlli AWS Control Tower classifica questi controlli in base ai servizi e alle risorse associati. AWS Per maggiori dettagli, consulta Controlli [proattivi](#).

Con questa versione, AWS Control Tower è inoltre integrato AWS Security Hub CSPM, tramite il nuovo standard CSPM Security Hub: AWS Control Tower, che supporta Service-Managed lo standard AWS Foundational Security Best Practices (FSBP). Puoi visualizzare oltre 160 controlli CSPM di Security Hub insieme ai controlli AWS Control Tower nella console e ottenere un punteggio di sicurezza Security Hub CSPM per il tuo ambiente AWS Control Tower. Per ulteriori informazioni, consulta [Controlli Security Hub](#).

Stato di conformità visualizzabile per tutti AWS Config rules

18 novembre 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora mostra lo stato di conformità di tutte le AWS Config regole distribuite nelle unità organizzative registrate con AWS Control Tower. Puoi visualizzare lo stato di conformità di tutte le AWS Config regole che riguardano i tuoi account in AWS Control Tower, iscritti o non registrati, senza uscire dalla console di AWS Control Tower. I clienti possono scegliere di impostare le regole di configurazione, chiamate controlli investigativi, in AWS Control Tower o di configurarle direttamente tramite il servizio. AWS Config AWS Config Vengono visualizzate le regole distribuite da, insieme alle regole distribuite da AWS Control Tower.

In precedenza, AWS Config le regole distribuite tramite il AWS Config servizio non erano visibili nella console AWS Control Tower. I clienti dovevano accedere al AWS Config servizio per identificare le regole non AWS Config conformi. Ora puoi identificare qualsiasi AWS Config regola non conforme all'interno della console AWS Control Tower. Per visualizzare lo stato di conformità di tutte le regole di configurazione, accedi alla pagina dei dettagli dell'account nella console AWS Control Tower. Verrà visualizzato un elenco che mostra lo stato di conformità dei controlli gestiti da AWS Control Tower e delle regole Config distribuite all'esterno di AWS Control Tower.

API per i controlli e una nuova CloudFormation risorsa

1 settembre 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta la gestione programmatica dei controlli, noti anche come guardrail, tramite una serie di chiamate API. Una nuova CloudFormation risorsa supporta la funzionalità API per i controlli. Per ulteriori dettagli, consulta [Automatizza le attività in AWS Control Tower](#) e [Crea AWS Control Tower risorse con AWS CloudFormation](#).

Queste API consentono di abilitare, disabilitare e visualizzare lo stato dell'applicazione dei controlli nella libreria AWS Control Tower. Le API includono il supporto per CloudFormation, in modo da poter gestire AWS le risorse come infrastructure-as-code (IaC). AWS Control Tower fornisce controlli preventivi e investigativi opzionali che esprimono le intenzioni politiche relative a un'intera unità organizzativa (OU) e a ogni account all'interno dell'unità organizzativa. AWS Queste regole rimangono in vigore quando crei nuovi account o apporti modifiche agli account esistenti.

API incluse in questa versione

- **EnableControl**— Questa chiamata API attiva un controllo. Avvia un'operazione asincrona che crea AWS risorse sull'unità organizzativa specificata e sugli account in essa contenuti.
- **DisableControl**— Questa chiamata API disattiva un controllo. Avvia un'operazione asincrona che elimina AWS le risorse sull'unità organizzativa specificata e gli account in essa contenuti.
- **GetControlOperation**— Restituisce lo stato di una particolare operazione o operazione.
EnableControl DisableControl
- **ListEnabledControls**— Elenca i controlli abilitati da AWS Control Tower sull'unità organizzativa specificata e gli account in essa contenuti.

Per visualizzare un elenco di nomi di controllo per i controlli opzionali, consulta Identificatori di [risorse per API e controlli](#), nella Guida per l'utente di AWS Control Tower.

cFCT supporta l'eliminazione di set di stack

26 agosto 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

Le personalizzazioni per AWS Control Tower (cFCT) ora supportano l'eliminazione di set di stack, impostando un parametro nel file `manifest.yaml`. Per ulteriori informazioni, consulta [Eliminazione di un set di stack](#).

Important

Quando si imposta inizialmente il valore di `enable_stack_set_deletion` to `true`, la prossima volta che si richiama cFCT, TUTTE le risorse che iniziano con il prefisso `CustomControlTower-`, che hanno il tag chiave associato e che non sono dichiarate nel file `manifestKey:AWS_Solutions, Value: CustomControlTowerStackSet`, vengono eliminate gradualmente.

Conservazione personalizzata dei log

15 agosto 2022

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower. Per informazioni, consulta [Aggiorna la tua landing zone](#))

AWS Control Tower offre ora la possibilità di personalizzare la politica di conservazione per i bucket Amazon S3 che archiviano i log di AWS Control Tower CloudTrail. Puoi personalizzare la tua politica di conservazione dei log di Amazon S3, in incrementi di giorni o anni, fino a un massimo di 15 anni.

Se scegli di non personalizzare la conservazione dei log, le impostazioni predefinite sono 1 anno per la registrazione standard dell'account e 10 anni per la registrazione degli accessi.

Questa funzionalità è disponibile per i clienti esistenti tramite AWS Control Tower quando si aggiorna o si ripara la zona di destinazione e per i nuovi clienti tramite la configurazione di AWS Control Tower

È disponibile la riparazione di Role Drift

11 agosto 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora supporta la riparazione della deriva dei ruoli. È possibile ripristinare un ruolo richiesto senza una riparazione completa della zona di atterraggio. Se è necessario questo tipo di riparazione del drift, la pagina di errore della console fornisce i passaggi per ripristinare il ruolo, in modo che la zona di atterraggio sia nuovamente disponibile.

Zona di destinazione AWS Control Tower versione 3.0

29 luglio 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.0. Per informazioni, consulta [Aggiorna la tua landing zone](#))

La versione 3.0 della landing zone di AWS Control Tower include i seguenti aggiornamenti:

- La possibilità di scegliere percorsi a livello di organizzazione o di disattivare i AWS CloudTrail CloudTrail percorsi gestiti da AWS Control Tower.

- Due nuovi controlli investigativi per determinare se AWS CloudTrail sta registrando l'attività nei tuoi account.
- L'opzione per aggregare AWS Config informazioni sulle risorse globali solo nella tua regione di origine.
- Un aggiornamento della Regione nega il controllo.
- Un aggiornamento della politica gestita, `AWSControlTowerServiceRolePolicy`.
- Non creiamo più il ruolo IAM `aws-controltower-CloudWatchLogsRole` e il gruppo di CloudWatch log `aws-controltower/CloudTrailLogs` in ogni account registrato. In precedenza, li creavamo in ogni account per la cronologia degli account. Con i percorsi organizzativi, ne creiamo solo uno nell'account di gestione.

Le sezioni seguenti forniscono maggiori dettagli su ogni nuova funzionalità.

Organization-level CloudTrail percorsi in AWS Control Tower

Con la versione 3.0 della zona di destinazione, AWS Control Tower ora supporta i percorsi a livello di organizzazione AWS CloudTrail .

Quando aggiorni la zona di destinazione di AWS Control Tower alla versione 3.0, hai la possibilità di selezionare percorsi a livello di organizzazione come preferenza di registrazione o di CloudTrail disattivare i AWS CloudTrail percorsi gestiti da AWS Control Tower. Quando esegui l'aggiornamento alla versione 3.0, AWS Control Tower elimina i percorsi esistenti a livello di account per gli account registrati dopo un periodo di attesa di 24 ore. AWS Control Tower non elimina i percorsi a livello di account per gli account non registrati. Nel caso improbabile che l'aggiornamento della zona di destinazione non abbia esito positivo, ma l'errore si verifichi dopo che AWS Control Tower ha già creato il percorso a livello di organizzazione, potresti incorrere in addebiti duplicati per i percorsi a livello di organizzazione e a livello di account, fino a quando l'operazione di aggiornamento non sarà completata correttamente.

Passando dalla landing zone 3.0, AWS Control Tower non supporta più i percorsi gestiti a livello di account. AWS AWS Control Tower crea invece un percorso a livello di organizzazione, attivo o inattivo, a seconda della selezione.

Note

Dopo l'aggiornamento alla versione 3.0 o successiva, non è possibile continuare con i CloudTrail percorsi a livello di account gestiti da AWS Control Tower.

Nessun dato di registrazione viene perso dai log aggregati degli account, poiché i log rimangono nel bucket Amazon S3 esistente in cui sono archiviati. Vengono eliminati solo i percorsi, non i log esistenti. Se selezioni l'opzione per aggiungere percorsi a livello di organizzazione, AWS Control Tower apre un nuovo percorso verso una nuova cartella all'interno del bucket Amazon S3 e continua a inviare le informazioni di registrazione a quella posizione. Se scegli di disattivare i percorsi gestiti da AWS Control Tower, i log esistenti rimangono nel bucket, invariati.

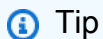
Convenzioni di denominazione dei percorsi per l'archiviazione dei log

- I log degli account trail vengono archiviati con un percorso del seguente formato: `/org id/AWSLogs/...`
- I log degli itinerari organizzativi vengono archiviati con un percorso del seguente formato: `/org id/AWSLogs/org id/...`

Il percorso creato da AWS Control Tower per i CloudTrail percorsi a livello di organizzazione è diverso dal percorso predefinito per un percorso a livello di organizzazione creato manualmente, che avrebbe il seguente formato:

- `/AWSLogs/org id/...`

Per ulteriori informazioni sulla denominazione dei percorsi, consulta [Finding your log CloudTrail file](#).



Tip

Se prevedi di creare e gestire percorsi a livello di account, ti consigliamo di creare i nuovi percorsi prima di completare l'aggiornamento alla versione 3.0 della landing zone di AWS Control Tower, per iniziare subito la registrazione.

In qualsiasi momento, puoi scegliere di creare nuovi percorsi a livello di account o organizzazione e gestirli autonomamente CloudTrail. L'opzione di scegliere CloudTrail percorsi a livello di organizzazione gestiti da AWS Control Tower è disponibile durante qualsiasi aggiornamento della zona di destinazione alla versione 3.0 o successiva. Puoi attivare e disattivare i percorsi a livello di organizzazione ogni volta che aggiorni la tua zona di atterraggio.

Se i tuoi log sono gestiti da un servizio di terze parti, assicurati di assegnare il nuovo nome di percorso al tuo servizio.

 Note

Per le zone di atterraggio alla versione 3.0 o successive, i AWS CloudTrail percorsi a livello di account non sono supportati da AWS Control Tower. Puoi creare e gestire i tuoi percorsi a livello di account in qualsiasi momento oppure puoi scegliere i percorsi a livello di organizzazione gestiti da AWS Control Tower.

Registra le AWS Config risorse solo nella regione d'origine

Nella versione 3.0 della zona di destinazione, AWS Control Tower ha aggiornato la configurazione di base in AWS Config modo da registrare le risorse globali solo nella regione di origine. Dopo l'aggiornamento alla versione 3.0, la registrazione delle risorse globali è abilitata solo nella regione di origine.

Questa configurazione è considerata una best practice. È consigliata da AWS Security Hub CSPM e e AWS Config consente di risparmiare sui costi riducendo il numero di elementi di configurazione creati quando le risorse globali vengono create, modificate o eliminate. In precedenza, ogni volta che una risorsa globale veniva creata, aggiornata o eliminata, da un cliente o da un AWS servizio, veniva creato un elemento di configurazione per ogni elemento in ciascuna regione governata.

Due nuovi controlli investigativi per la registrazione AWS CloudTrail

Come parte della modifica ai AWS CloudTrail percorsi a livello di organizzazione, AWS Control Tower sta introducendo due nuovi controlli di rilevamento che verificano se è abilitato. CloudTrail Il primo controllo ha una guida obbligatoria ed è abilitato sull'unità organizzativa di sicurezza durante la configurazione o gli aggiornamenti della zona di destinazione della versione 3.0 e successive. Il secondo controllo è basato su linee guida fortemente consigliate e viene applicato facoltativamente a qualsiasi unità organizzativa diversa dall'unità organizzativa di sicurezza, a cui è già applicata la protezione di controllo obbligatoria.

Controllo obbligatorio: [rileva se gli account condivisi dell'unità organizzativa di sicurezza sono abilitati AWS CloudTrail o CloudTrail Lake sono abilitati](#)

Controllo fortemente consigliato: [rileva se un account è abilitato AWS CloudTrail o se CloudTrail Lake è abilitato](#)

Per ulteriori informazioni sui nuovi controlli, consulta [la libreria di controlli AWS Control Tower](#).

Un aggiornamento della regione nega il controllo

Abbiamo aggiornato l'NotActionelenco nella sezione Regioni in cui è stato negato il controllo per includere le azioni intraprese da alcuni servizi aggiuntivi, elencati di seguito:

```
"chatbot:*",
"s3:GetAccountPublic",
"s3:DeleteMultiRegionAccessPoint",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:ListMultiRegionAccessPoints",
"s3:GetStorageLensConfiguration",
"s3:GetStorageLensDashboard",
"s3:ListStorageLensConfigurations",
"s3:GetAccountPublicAccessBlock",
"s3:PutAccountPublic",
"s3:PutAccountPublicAccessBlock",
```

Procedura guidata: video

Questo video (3:07) descrive come aggiornare la zona di destinazione di AWS Control Tower esistente alla versione 3. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

[Video dettagliato sull'aggiornamento di una Landing Zone di AWS Control Tower esistente alla Landing Zone 3.](#)

La pagina Organizzazione combina le visualizzazioni delle unità organizzative e degli account

18 luglio 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

La nuova pagina Organizzazione in AWS Control Tower mostra una visualizzazione gerarchica (ad albero) di tutte le unità organizzative (OU) e gli account. Combina le informazioni delle pagine delle unità organizzative e degli account, che esistevano in precedenza.

Nella nuova pagina, è possibile visualizzare le relazioni tra le unità organizzative principali e le relative unità organizzative e account annidate. È possibile intervenire sui raggruppamenti di risorse.

È possibile configurare la visualizzazione della pagina. Ad esempio, è possibile espandere o comprimere la visualizzazione gerarchica, filtrare la visualizzazione per visualizzare solo gli account o le unità organizzative, scegliere di visualizzare solo gli account registrati e le unità organizzative registrate oppure è possibile visualizzare gruppi di risorse correlate. È più facile assicurarsi che l'intera organizzazione sia aggiornata correttamente.

Creazione e registrazione dell'account semplificate

30 giugno 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower offre ora un flusso di lavoro semplificato per la creazione e la registrazione degli account. Puoi creare un nuovo account o registrare un account esistente in un unico flusso di lavoro, senza accedere alla console di Service Catalog. Per ulteriori informazioni, consulta [Registra un account esistente dalla console AWS Control Tower](#).

AFT supporta la personalizzazione automatica per gli account AWS Control Tower condivisi

27 maggio 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

Account Factory for Terraform (AFT) ora può personalizzare e aggiornare in modo programmatico qualsiasi account gestito da AWS Control Tower, inclusi l'account di gestione, l'account di audit e l'account di archivio dei log, insieme agli account registrati. Puoi centralizzare la personalizzazione dell'account e la gestione degli aggiornamenti, proteggendo al contempo la sicurezza delle configurazioni degli account, poiché stabilisci il ruolo che svolge il lavoro.

Il ruolo `AWSAFTExecution` esistente ora implementa le personalizzazioni in tutti gli account. È possibile configurare le autorizzazioni IAM con limiti che limitano l'accesso al ruolo `AWSAFTExecution` in base ai requisiti aziendali e di sicurezza. Puoi anche delegare a livello di codice le autorizzazioni di personalizzazione approvate in quel ruolo, per utenti fidati. Come procedura consigliata, si consiglia di limitare le autorizzazioni a quelle necessarie per implementare le personalizzazioni richieste.

AFT ora crea il nuovo ruolo `AWSAFTService` per distribuire le risorse AFT in tutti gli account gestiti, inclusi gli account condivisi e l'account di gestione. Le risorse in precedenza venivano distribuite dal ruolo `AWSAFTExecution`.

Il provisioning degli account condivisi e di gestione di AWS Control Tower non viene eseguito tramite account factory, quindi non contengono i prodotti corrispondenti. AWS Service Catalog Pertanto, non è possibile aggiornare gli account condivisi e di gestione in Service Catalog.

Operazioni simultanee per tutti i controlli opzionali

18 maggio 2022

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora supporta operazioni simultanee per i controlli preventivi e per i controlli investigativi.

Con questa nuova funzionalità, qualsiasi controllo opzionale ora può essere applicato o rimosso contemporaneamente, migliorando così la facilità d'uso e le prestazioni di tutti i controlli opzionali. È possibile abilitare più controlli opzionali senza attendere il completamento delle singole operazioni di controllo. Gli unici momenti limitati sono quelli in cui AWS Control Tower è in fase di configurazione della zona di destinazione o quando sta estendendo la governance a una nuova organizzazione.

Funzionalità supportate per i controlli preventivi:

- Applica e rimuovi diversi controlli preventivi sulla stessa unità organizzativa.
- Applica e rimuovi diversi controlli preventivi su diverse unità organizzative, contemporaneamente.
- Applica e rimuovi lo stesso controllo preventivo su più unità organizzative contemporaneamente.
- È possibile applicare e rimuovere contemporaneamente qualsiasi controllo preventivo e investigativo.

Puoi riscontrare questi miglioramenti della concorrenza dei controlli in tutte le versioni rilasciate di AWS Control Tower.

Quando si applicano controlli preventivi alle unità organizzative annidate, i controlli preventivi riguardano tutti gli account e le unità organizzative annidati nell'unità organizzativa di destinazione, anche se tali account e unità organizzative non sono registrati presso AWS Control Tower. I controlli preventivi vengono implementati utilizzando le Service Control Policies (SCP), che ne fanno parte. AWS Organizations I controlli investigativi vengono implementati utilizzando AWS Config regole. I guardrail rimangono attivi quando crei nuovi account o apporti modifiche agli account esistenti e AWS Control Tower fornisce un rapporto riepilogativo di come ciascun account è conforme alle politiche abilitate. Per un elenco completo dei controlli disponibili, consulta [la libreria di controlli AWS Control Tower](#).

Account di sicurezza e registrazione esistenti

16 maggio 2022

(Disponibile durante la configurazione iniziale.)

AWS Control Tower offre ora la possibilità di specificare un AWS account esistente come account di sicurezza o di registrazione di AWS Control Tower, durante il processo di configurazione iniziale della zona di destinazione. Questa opzione elimina la necessità per AWS Control Tower di creare nuovi account condivisi. L'account di sicurezza, chiamato di default `account Audit`, è un account con restrizioni che consente ai team addetti alla sicurezza e alla conformità di accedere a tutti gli account nella zona di destinazione. L'account di registrazione, che per impostazione predefinita è denominato `account Log Archive`, funziona come un repository. Memorizza i registri delle attività delle API e delle configurazioni delle risorse di tutti gli account nella zona di destinazione.

Integrando gli account di sicurezza e registrazione esistenti, è più facile estendere la governance di AWS Control Tower alle organizzazioni esistenti o passare ad AWS Control Tower da una zona di destinazione alternativa. L'opzione per utilizzare gli account esistenti viene visualizzata durante la configurazione iniziale della zona di destinazione. Include controlli durante il processo di configurazione, che garantiscono il successo dell'implementazione. AWS Control Tower implementa i ruoli e i controlli necessari sugli account esistenti. Non rimuove o unisce le risorse o i dati esistenti in questi account.

Limitazione: se prevedi di inserire AWS account esistenti in AWS Control Tower come account di audit e di archiviazione dei log e se tali account dispongono di AWS Config risorse esistenti, devi eliminare le AWS Config risorse esistenti prima di poter registrare gli account in AWS Control Tower.

Zona di destinazione di AWS Control Tower versione 2.9

22 aprile 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.9. Per informazioni, consulta [Aggiorna la tua landing zone](#))

La versione 2.9 della landing zone di AWS Control Tower aggiorna il server di notifica Lambda per utilizzare il runtime di Python versione 3.9. Questo aggiornamento risolve la deprecazione della versione 3.6 di Python, prevista per luglio 2022. Per le informazioni più recenti, consulta la pagina sulla deprecazione di [Python](#).

Zona di destinazione di AWS Control Tower versione 2.8

10 febbraio 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.8. Per informazioni, consulta [Aggiorna la tua landing zone](#))

La versione 2.8 della landing zone di AWS Control Tower aggiunge funzionalità in linea con i recenti aggiornamenti delle [AWS Foundational Security Best Practices](#).

In questa versione:

- La registrazione degli accessi è configurata per il bucket dei log di accesso nell'account Log Archive, per tenere traccia degli accessi al bucket del log di accesso S3 esistente.
- È stato aggiunto il supporto per la politica del ciclo di vita. Il log di accesso per il bucket di log di accesso S3 esistente è impostato su un tempo di conservazione predefinito di 10 anni.
- Inoltre, questa versione aggiorna AWS Control Tower per utilizzare il AWS Service Linked Role (SLR) fornito da AWS Config, in tutti gli account gestiti (escluso l'account di gestione), in modo da poter impostare e gestire le regole di configurazione in base alle best practice. AWS Config I clienti che non effettuano l'upgrade continueranno a utilizzare il ruolo esistente.
- Questa versione semplifica il processo di configurazione di AWS Control Tower KMS per la crittografia AWS Config dei dati e migliora la relativa messaggistica di stato in CloudTrail
- La versione include un aggiornamento al Region Deny Control, per consentire la funzionalità in. `route53-application-recovery us-west-2`
- Aggiornamento: il 15 febbraio 2022, abbiamo rimosso la coda di lettere morte per AWS le funzioni Lambda.

Ulteriori dettagli:

- Se disattivi la tua zona di atterraggio, AWS Control Tower non rimuove il ruolo collegato al servizio. AWS Config
- Se rimuovi il provisioning di un account Account Factory, AWS Control Tower non rimuove il ruolo collegato al servizio. AWS Config

Per aggiornare la zona di destinazione a 2.8, vai alla [pagina delle impostazioni della zona di destinazione](#), seleziona la versione 2.8, quindi scegli **Aggiorna**. Dopo aver aggiornato la zona di

atterraggio, devi aggiornare tutti gli account gestiti da AWS Control Tower, come indicato in [Gestione degli aggiornamenti di configurazione in AWS Control Tower](#).

gennaio - dicembre 2021

Nel 2021, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Funzionalità di negazione delle regioni](#)
- [Funzionalità di residenza dei dati](#)
- [AWS Control Tower introduce il provisioning e la personalizzazione degli account Terraform](#)
- [È disponibile un nuovo evento sul ciclo di vita](#)
- [AWS Control Tower abilita le unità organizzative annidate](#)
- [Concorrenza del controllo investigativo](#)
- [Sono disponibili due nuove regioni](#)
- [Deselezione della regione](#)
- [AWS Control Tower funziona con AWS Sistemi di gestione delle chiavi](#)
- [Controlli rinominati, funzionalità invariata](#)
- [AWS Control Tower esegue quotidianamente la scansione degli SCP per verificare eventuali deviazioni](#)
- [Nomi personalizzati per unità organizzative e account](#)
- [Zona di atterraggio AWS Control Tower versione 2.7](#)
- [Tre nuovi AWS Regioni disponibili](#)
- [Governa solo le regioni selezionate](#)
- [AWS Control Tower ora estende la governance alle unità organizzative esistenti nel tuo AWS organizations](#)
- [AWS Control Tower fornisce aggiornamenti in blocco degli account](#)

Funzionalità di negazione delle regioni

30 novembre 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower.)

AWS Control Tower ora offre funzionalità Region Deny, che ti aiutano a limitare l'accesso ai AWS servizi e alle operazioni per gli account registrati nel tuo ambiente AWS Control Tower. La

funzionalità Region Deny integra le funzionalità di selezione e deselezionazione delle regioni esistenti in AWS Control Tower. Insieme, queste funzionalità aiutano a risolvere i problemi di conformità e normativi, bilanciando al contempo i costi associati all'espansione in regioni aggiuntive.

Ad esempio, AWS i clienti in Germania possono negare l'accesso ai AWS servizi nelle regioni al di fuori della regione di Francoforte. Puoi selezionare regioni con restrizioni durante il processo di configurazione di AWS Control Tower o nella pagina delle impostazioni della zona di destinazione. La funzione Region deny è disponibile quando si aggiorna la versione della zona di destinazione di AWS Control Tower. Alcuni AWS servizi sono esenti dalla funzionalità Region Deny. Per saperne di più, consulta [Configurare il controllo di negazione della regione](#).

Funzionalità di residenza dei dati

30 novembre 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower offre ora controlli personalizzati per garantire che i dati dei clienti caricati AWS sui servizi si trovino solo nelle AWS regioni specificate. Puoi selezionare la AWS regione o le regioni in cui i dati dei clienti vengono archiviati ed elaborati. Per un elenco completo delle AWS regioni in cui è disponibile AWS Control Tower, consulta la tabella delle [AWS regioni](#).

Per un controllo granulare, puoi applicare controlli aggiuntivi, come Disabilitare le connessioni Amazon Virtual Private Network (VPN) o Disallow l'accesso a Internet per un'istanza Amazon VPC. Puoi visualizzare lo stato di conformità dei controlli nella console AWS Control Tower. Per un elenco completo dei controlli disponibili, consulta [la libreria di controlli AWS Control Tower](#).

AWS Control Tower introduce il provisioning e la personalizzazione degli account Terraform

29 novembre 2021

(Aggiornamento opzionale per la zona di atterraggio di AWS Control Tower)

Ora puoi utilizzare Terraform per fornire e aggiornare account personalizzati tramite AWS Control Tower, con AWS Control Tower Account Factory for Terraform (AFT).

AFT fornisce un'unica pipeline Terraform Infrastructure as code (IaC), che esegue il provisioning degli account gestiti da AWS Control Tower. Le personalizzazioni durante il provisioning aiutano a soddisfare le politiche aziendali e di sicurezza, prima di fornire gli account agli utenti finali.

La pipeline di creazione automatica degli account AFT monitora fino al completamento del provisioning dell'account, quindi continua, attivando moduli Terraform aggiuntivi che migliorano l'account con le personalizzazioni necessarie. Come parte aggiuntiva del processo di personalizzazione, puoi configurare la pipeline per installare i tuoi moduli Terraform personalizzati e puoi scegliere di aggiungere una qualsiasi delle opzioni di funzionalità AFT, fornite da per le personalizzazioni comuni. AWS

Inizia a usare AWS Control Tower Account Factory for Terraform seguendo i passaggi forniti nella Guida per l'utente di AWS Control Tower e scaricando AFT per la tua istanza Terraform. [Implementa AWS Control Tower Account Factory per Terraform \(AFT\)](#) AFT supporta le distribuzioni open source Terraform Cloud, Terraform Enterprise e Terraform.

È disponibile un nuovo evento sul ciclo di vita

18 novembre 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

L'evento `PrecheckOrganizationalUnit` registra se ci sono risorse che bloccano il successo dell'attività di governance `Extend`, incluse le risorse nelle unità organizzative annidate. Per ulteriori informazioni, consulta [PrecheckOrganizationalUnit](#).

AWS Control Tower abilita le unità organizzative annidate

16 novembre 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora ti consente di includere unità organizzative annidate come parte della tua zona di atterraggio.

AWS Control Tower fornisce supporto per unità organizzative (OU) annidate, consentendo di organizzare gli account in più livelli gerarchici e di applicare i controlli preventivi in modo gerarchico. Puoi registrare unità organizzative contenenti unità organizzative annidate, creare e registrare unità organizzative sotto unità organizzative principali e abilitare i controlli su qualsiasi unità organizzativa registrata, indipendentemente dalla profondità. Per supportare questa funzionalità, la console mostra il numero di account e unità organizzative gestiti.

Con le unità organizzative annidate, puoi allineare le unità organizzative di AWS Control Tower alla strategia AWS multi-account e ridurre il tempo necessario per abilitare i controlli su più unità organizzative applicando i controlli a livello di unità organizzativa principale.

Considerazioni chiave

1. Puoi registrare le unità organizzative multilivello esistenti con AWS Control Tower un'unità organizzativa alla volta, iniziando dall'unità organizzativa di livello superiore e procedendo lungo l'albero. Per ulteriori informazioni, consulta [Espandi da una struttura OU piatta a una struttura OU annidata](#).
2. Gli account che fanno capo direttamente a un'unità organizzativa registrata vengono registrati automaticamente. Gli account più in basso nell'albero possono essere registrati registrando l'unità organizzativa principale immediata.
3. I controlli preventivi (SCP) vengono ereditati automaticamente nella gerarchia; gli SCP applicati all'unità principale vengono ereditati da tutte le unità organizzative annidate.
4. I controlli investigativi (regole di AWS configurazione) NON vengono ereditati automaticamente.
5. La conformità ai controlli investigativi viene segnalata da ciascuna unità organizzativa.
6. La deriva di SCP su un'unità organizzativa influisce su tutti gli account e le unità organizzative ad essa collegate.
7. Non è possibile creare nuove unità organizzative annidate nell'unità organizzativa di sicurezza (unità organizzativa principale).

Concorrenza del controllo investigativo

5 novembre 2021

(Aggiornamento opzionale per la zona di atterraggio di AWS Control Tower)

I controlli investigativi di AWS Control Tower ora supportano operazioni simultanee per i controlli investigativi, migliorando la facilità d'uso e le prestazioni. Puoi abilitare più controlli investigativi senza attendere il completamento delle singole operazioni di controllo.

Funzionalità supportate:

- Abilita diversi controlli di rilevamento sulla stessa unità organizzativa (ad esempio, rileva se l'MFA per l'utente root è abilitato e rileva se è consentito l'accesso pubblico in scrittura ai bucket Amazon S3).
- Abilita controlli di rilevamento diversi su diverse unità organizzative, contemporaneamente.
- La messaggistica di errore Guardrail è stata migliorata per fornire indicazioni aggiuntive per le operazioni di controllo simultanee supportate.

Non supportato in questa versione:

- L'attivazione contemporanea dello stesso controllo investigativo su più unità organizzative non è supportata.
- La concorrenza dei controlli preventivi non è supportata.

Puoi riscontrare i miglioramenti della concorrenza del controllo investigativo in tutte le versioni di AWS Control Tower. Si consiglia ai clienti che non utilizzano attualmente la versione 2.7 di eseguire un aggiornamento della zona di destinazione per sfruttare altre funzionalità, come la selezione e la deselezionazione delle regioni, disponibili nella versione più recente.

Sono disponibili due nuove regioni

29 luglio 2021

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower è ora disponibile in due AWS regioni aggiuntive: Sud America (San Paolo) ed Europa (Parigi). Questo aggiornamento estende la disponibilità di AWS Control Tower a 15 AWS regioni.

Se non conosci AWS Control Tower, puoi avviarlo subito in una qualsiasi delle regioni supportate. Durante il lancio, puoi selezionare le regioni in cui desideri che AWS Control Tower crei e gestisca il tuo ambiente con più account.

Se disponi già di un ambiente AWS Control Tower e desideri estendere o rimuovere le funzionalità di governance di AWS Control Tower in una o più regioni supportate, vai alla [pagina delle impostazioni della zona di destinazione](#) nella dashboard di AWS Control Tower, quindi seleziona le regioni. Dopo aver aggiornato la tua zona di destinazione, devi quindi [aggiornare tutti gli account governati da AWS Control Tower](#).

Deselezione della regione

29 luglio 2021

(Aggiornamento opzionale per la zona di atterraggio di AWS Control Tower)

La deselezione della regione AWS Control Tower migliora la capacità di gestire l'impronta geografica delle risorse AWS Control Tower. Puoi deselezionare le regioni che non desideri più governare da

AWS Control Tower. Questa funzionalità offre la possibilità di risolvere i problemi di conformità e normativi bilanciando al contempo i costi associati all'espansione in regioni aggiuntive.

La deselezionazione delle regioni è disponibile quando si aggiorna la versione della zona di destinazione di AWS Control Tower.

Quando usi Account Factory per creare un nuovo account o registrare un account membro preesistente, o quando selezioni **Extend Governance** per registrare gli account in un'unità organizzativa preesistente, AWS Control Tower implementa le sue funzionalità di governance, che includono registrazione, monitoraggio e controlli centralizzati, nelle regioni scelte negli account. La scelta di deselezionare una regione e rimuovere la governance di AWS Control Tower da quella regione rimuove tale funzionalità di governance, ma non inibisce la capacità degli utenti di distribuire AWS risorse o carichi di lavoro in quelle regioni.

AWS Control Tower funziona con AWS Sistemi di gestione delle chiavi

28 luglio 2021

(Aggiornamento opzionale per la zona di atterraggio di AWS Control Tower)

AWS Control Tower offre la possibilità di utilizzare una AWS chiave Key Management Service (AWS KMS). Una chiave viene fornita e gestita dall'utente per proteggere i servizi distribuiti da AWS Control Tower AWS CloudTrail AWS Config, inclusi i dati Amazon S3 associati. AWS La crittografia KMS è un livello di crittografia avanzato rispetto alla SSE-S3 crittografia utilizzata da AWS Control Tower per impostazione predefinita.

L'integrazione del supporto AWS KMS in AWS Control Tower è in linea con le AWS Foundational Security Best Practices, che consigliano un ulteriore livello di sicurezza per i file di registro sensibili. È necessario utilizzare le chiavi AWS gestite da KMS (SSE-KMS) per la crittografia a riposo. AWS Il supporto per la crittografia KMS è disponibile quando si configura una nuova zona di atterraggio o quando si aggiorna la zona di destinazione AWS Control Tower esistente.

Per configurare questa funzionalità, puoi selezionare **KMS Key Configuration** durante la configurazione iniziale della zona di atterraggio. Puoi scegliere una chiave KMS esistente oppure puoi selezionare un pulsante che ti reindirizza alla console AWS KMS per crearne una nuova. Hai anche la flessibilità di passare dalla crittografia predefinita a SSE-KMS o a una SSE-KMS chiave diversa.

Per una landing zone di destinazione di AWS Control Tower esistente, puoi eseguire un aggiornamento per iniziare a utilizzare le chiavi AWS KMS.

Controlli rinominati, funzionalità invariata

26 luglio 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower sta rivedendo alcuni nomi e descrizioni dei controlli per riflettere meglio le intenzioni politiche del controllo. I nomi e le descrizioni modificati ti aiutano a comprendere in modo più intuitivo i modi in cui i controlli incorporano le politiche dei tuoi account. Ad esempio, abbiamo cambiato parte dei nomi dei controlli investigativi da «Disallow» a «Detective» perché il controllo investigativo stesso non impedisce un'azione specifica, ma rileva solo le violazioni delle policy e fornisce avvisi tramite la dashboard.

La funzionalità di controllo, le linee guida e l'implementazione rimangono invariate. Sono stati modificati solo i nomi e le descrizioni dei controlli.

AWS Control Tower esegue quotidianamente la scansione degli SCP per verificare eventuali deviazioni

11 maggio 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora esegue scansioni automatiche giornaliere dei tuoi SCP gestiti per verificare che i controlli corrispondenti siano applicati correttamente e che non siano stati modificati. Se una scansione rileva una deviazione, riceverai una notifica. AWS Control Tower invia solo una notifica per problema di deriva, quindi se la tua zona di atterraggio è già in stato di deriva, non riceverai notifiche aggiuntive a meno che non venga trovato un nuovo elemento di deriva.

Nomi personalizzati per unità organizzative e account

16 aprile 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora consente di personalizzare la denominazione delle zone di destinazione. Puoi mantenere i nomi consigliati da AWS Control Tower per le unità organizzative (OU) e gli account principali oppure puoi modificare questi nomi durante il processo iniziale di configurazione della zona di destinazione.

I nomi predefiniti forniti da AWS Control Tower per le unità organizzative e gli account principali corrispondono alle linee guida sulle best practice per AWS più account. Tuttavia, se la tua azienda ha politiche di denominazione specifiche o se hai già un'unità organizzativa o un account esistente con lo stesso nome consigliato, la nuova funzionalità di denominazione dell'unità organizzativa e degli account ti offre la flessibilità necessaria per affrontare tali vincoli.

A prescindere dalla modifica del flusso di lavoro durante la configurazione, l'unità organizzativa precedentemente nota come unità organizzativa principale è ora denominata unità organizzativa di sicurezza e l'unità organizzativa precedentemente nota come unità organizzativa personalizzata è ora denominata unità organizzativa Sandbox. Abbiamo apportato questa modifica per migliorare l'allineamento con le linee guida generali AWS sulle migliori pratiche per la denominazione.

I nuovi clienti vedranno questi nuovi nomi delle unità organizzative. I clienti esistenti continueranno a vedere i nomi originali di queste unità organizzative. Potresti riscontrare alcune incongruenze nella denominazione delle unità organizzative mentre stiamo aggiornando la nostra documentazione con i nuovi nomi.

Per iniziare a usare AWS Control Tower dalla Console di AWS gestione, vai alla console AWS Control Tower e seleziona **Configura zona di destinazione** in alto a destra. Per ulteriori informazioni, puoi leggere come pianificare la tua zona di atterraggio di AWS Control Tower.

Zona di atterraggio AWS Control Tower versione 2.7

8 aprile 2021

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower alla versione 2.7. Per informazioni, consulta [Aggiorna la tua landing zone](#))

Con la versione 2.7 di AWS Control Tower, AWS Control Tower introduce quattro nuovi controlli preventivi obbligatori per l'archiviazione dei log che implementano le policy esclusivamente sulle risorse di AWS Control Tower. Abbiamo modificato le linee guida su quattro controlli Log Archive esistenti da obbligatori a facoltativi, poiché stabiliscono le policy per le risorse esterne ad AWS Control Tower. Questa modifica ed espansione dei controlli offre la possibilità di separare la governance degli archivi di log per le risorse all'interno di AWS Control Tower dalla governance delle risorse esterne ad AWS Control Tower.

I quattro controlli modificati possono essere utilizzati insieme ai nuovi controlli obbligatori per fornire la governance a un set più ampio di archivi di AWS log. Gli ambienti AWS Control Tower esistenti manterranno questi quattro controlli modificati abilitati automaticamente, per la coerenza

dell'ambiente; tuttavia, questi controlli opzionali ora possono essere disabilitati. I nuovi ambienti AWS Control Tower devono abilitare tutti i controlli opzionali. Gli ambienti esistenti devono disabilitare i controlli precedentemente obbligatori prima di aggiungere la crittografia ai bucket Amazon S3 non distribuiti da AWS Control Tower.

Nuovi controlli obbligatori:

- Disabilita le modifiche alla configurazione della crittografia per AWS Control Tower: bucket S3 creati nell'archivio di log
- Non consentire modifiche alla configurazione di registrazione per i bucket S3 creati da AWS Control Tower in Log Archive
- Non consentire modifiche alla politica dei bucket per i bucket S3 creati da AWS Control Tower nell'archivio di log
- Non consentire modifiche alla configurazione del ciclo di vita per i bucket S3 creati da AWS Control Tower nell'archivio di log

Le linee guida sono cambiate da obbligatorie a elettive:

- Disabilita le modifiche alla configurazione della crittografia per tutti i bucket Amazon S3 [In precedenza: abilitare la crittografia a riposo per l'archiviazione dei log]
- Disabilita le modifiche alla configurazione di registrazione per tutti i bucket Amazon S3 [In precedenza: abilitare la registrazione degli accessi per l'archiviazione dei log]
- Disabilita le modifiche alla policy dei bucket per tutti i bucket Amazon S3 [In precedenza: non consentire le modifiche alle policy all'archivio di log]
- Non consentire modifiche alla configurazione del ciclo di vita per tutti i bucket Amazon S3 [In precedenza: impostazione di una politica di conservazione per l'archiviazione dei log]

La versione 2.7 di AWS Control Tower include modifiche al blueprint delle zone di destinazione di AWS Control Tower che possono causare incompatibilità con le versioni precedenti dopo l'aggiornamento alla 2.7.

- In particolare, la versione 2.7 di AWS Control Tower si abilita `BlockPublicAccess` automaticamente sui bucket S3 distribuiti da AWS Control Tower. Puoi disattivare questa impostazione predefinita se il carico di lavoro richiede l'accesso a più account. Per ulteriori informazioni su ciò che accade quando `BlockPublicAccess` è abilitato, consulta [Bloccare l'accesso pubblico allo storage Amazon S3](#).

- La versione 2.7 di AWS Control Tower include un requisito per HTTPS. Tutte le richieste inviate ai bucket S3 distribuiti da AWS Control Tower devono utilizzare Secure Socket Layer (SSL). È consentito il passaggio solo delle richieste HTTPS. Se utilizzi HTTP (senza SSL) come endpoint per inviare le richieste, questa modifica genera un errore di accesso negato, che può potenzialmente interrompere il flusso di lavoro. Questa modifica non può essere annullata dopo l'aggiornamento 2.7 della tua zona di atterraggio.

Ti consigliamo di modificare le tue richieste per utilizzare TLS anziché HTTP.

Tre nuovi AWS Regioni disponibili

8 aprile 2021

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower è disponibile in tre AWS regioni aggiuntive: regione Asia Pacifico (Tokyo), regione Asia Pacifico (Seoul) e regione Asia Pacifico (Mumbai). È necessario un aggiornamento della zona di destinazione alla versione 2.7 per espandere la governance in queste regioni.

La tua zona di atterraggio non viene espansa automaticamente in queste regioni quando esegui l'aggiornamento alla versione 2.7, devi visualizzarle e selezionarle nella tabella Regioni per l'inclusione.

Governa solo le regioni selezionate

19 febbraio 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

La selezione della regione di AWS Control Tower offre una migliore capacità di gestire l'impronta geografica delle risorse AWS Control Tower. Per espandere il numero di regioni in cui ospitare AWS risorse o carichi di lavoro, per motivi di conformità, normativi, di costo o di altro tipo, ora puoi selezionare le regioni aggiuntive da gestire.

La selezione della regione è disponibile quando si configura una nuova zona di destinazione o si aggiorna la versione della zona di destinazione di AWS Control Tower. Quando usi Account Factory per creare un nuovo account o registrare un account membro preesistente, oppure quando usi Extend Governance per registrare account in un'unità organizzativa preesistente, AWS Control Tower implementa le sue funzionalità di governance di registrazione, monitoraggio e controlli

centralizzati nelle regioni scelte negli account. Per ulteriori informazioni sulla selezione delle regioni, consulta. [Configura le tue regioni AWS Control Tower](#)

AWS Control Tower ora estende la governance alle unità organizzative esistenti nel tuo AWS organizations

28 gennaio 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

Estendi la governance alle unità organizzative (OU) esistenti (quelle non presenti in AWS Control Tower) dall'interno della console AWS Control Tower. Con questa funzionalità, puoi portare le unità organizzative di alto livello e gli account inclusi nella governance di AWS Control Tower. Per informazioni sull'estensione della governance a un'intera unità organizzativa, consulta. [Registra un'unità organizzativa esistente con AWS Control Tower](#)

Quando registri un'unità organizzativa, AWS Control Tower esegue una serie di controlli per garantire la corretta estensione della governance e della registrazione degli account all'interno dell'unità organizzativa. Per ulteriori informazioni sui problemi comuni associati alla registrazione iniziale di un'unità organizzativa, consulta. [Cause comuni di errore durante la registrazione o la nuova registrazione](#)

Puoi anche visitare la pagina web del [prodotto AWS Control Tower](#) o YouTube visitare questo video su [come iniziare a usare AWS Control Tower per AWS Organizations](#).

AWS Control Tower fornisce aggiornamenti in blocco degli account

28 gennaio 2021

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

Con la funzionalità di aggiornamento in blocco, ora puoi aggiornare tutti gli account in un'unità AWS Organizations organizzativa registrata (OU) contenente fino a 300 account, con un solo clic, dalla dashboard di AWS Control Tower. Ciò è particolarmente utile nei casi in cui aggiorni la zona di destinazione di AWS Control Tower e devi anche aggiornare gli account registrati per allinearli alla versione corrente della zona di destinazione.

Questa funzionalità ti aiuta anche a mantenere aggiornati i tuoi account quando aggiorni la zona di atterraggio di AWS Control Tower per espanderla in nuove regioni o quando desideri registrare nuovamente un'unità organizzativa per assicurarti che a tutti gli account in quell'unità organizzativa

siano applicati i controlli più recenti. L'aggiornamento in blocco degli account elimina la necessità di aggiornare un account alla volta o di utilizzare uno script esterno per eseguire l'aggiornamento su più account.

Per informazioni sull'aggiornamento di una zona di atterraggio, vedere [Aggiorna la tua landing zone](#).

Per informazioni sulla registrazione o sulla nuova registrazione di un'unità organizzativa, vedere [Registra un'unità organizzativa esistente con AWS Control Tower](#)

gennaio - dicembre 2020

Nel 2020, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [La console AWS Control Tower ora si collega a siti esterni AWS Regole di configurazione](#)
- [AWS Control Tower è ora disponibile in regioni aggiuntive](#)
- [Aggiornamento Guardrail](#)
- [La console AWS Control Tower mostra ulteriori dettagli sulle unità organizzative e sugli account](#)
- [Usa AWS Control Tower per configurare nuovi account multipli AWS ambienti in AWS Organizations](#)
- [Personalizzazioni per la soluzione AWS Control Tower](#)
- [Disponibilità generale della versione 2.3 di AWS Control Tower](#)
- [Single-step provisioning degli account in AWS Control Tower](#)
- [Strumento di smantellamento di AWS Control Tower](#)
- [Notifiche degli eventi del ciclo di vita di AWS Control Tower](#)

La console AWS Control Tower ora si collega a siti esterni AWS Regole di configurazione

29 dicembre 2020

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.6. Per informazioni, consulta [Aggiorna la tua landing zone](#))

AWS Control Tower ora include un aggregatore a livello di organizzazione, che aiuta a rilevare le regole di configurazione esterne. AWS Ciò offre visibilità nella console di AWS Control Tower per verificare l'esistenza di regole di AWS configurazione create esternamente oltre a quelle create da

AWS Control Tower. AWS L'aggregatore consente ad AWS Control Tower di rilevare regole esterne e fornire un collegamento alla console AWS Config senza che AWS Control Tower debba accedere ad account non gestiti.

Con questa funzionalità, ora hai una visione consolidata dei controlli investigativi applicati ai tuoi account in modo da poter monitorare la conformità e determinare se hai bisogno di controlli aggiuntivi per il tuo account. Per informazioni, consulta [Come AWS Control Tower aggrega AWS Config le regole nelle unità organizzative e negli account non gestiti.](#)

AWS Control Tower è ora disponibile in regioni aggiuntive

18 novembre 2020

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.5. Per informazioni, consulta [Aggiorna la tua landing zone](#))

AWS Control Tower è ora disponibile in 5 AWS regioni aggiuntive:

- Regione Asia Pacifico (Singapore)
- Regione Europa (Francoforte)
- Regione Europa (Londra)
- Regione Europa (Stoccolma)
- Regione Canada (Centrale)

L'aggiunta di queste 5 AWS regioni è l'unica modifica introdotta per la versione 2.5 di AWS Control Tower.

AWS Control Tower è disponibile anche nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda) e Asia Pacifico (Sydney). Con questo lancio AWS Control Tower è ora disponibile in 10 regioni. AWS

Questo aggiornamento della zona di destinazione include tutte le regioni elencate e non può essere annullato. Dopo aver aggiornato la zona di destinazione alla versione 2.5, è necessario aggiornare manualmente tutti gli account registrati affinché AWS Control Tower possa governare nelle 10 regioni supportate. AWS Per informazioni, consulta [Configura le tue regioni AWS Control Tower.](#)

Aggiornamento Guardrail

8 ottobre 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

È stata rilasciata una versione aggiornata per il controllo obbligatorio AWS-GR_IAM_ROLE_CHANGE_PROHIBITED.

Questa modifica al controllo è necessaria perché gli account che vengono registrati automaticamente in AWS Control Tower devono avere il `AWSControlTowerExecution` ruolo abilitato. La versione precedente del controllo impedisce la creazione di questo ruolo.

Per ulteriori informazioni, consulta [Disallow Changes to AWS IAM Roles Set Up by AWS Control Tower e CloudFormation](#) nella AWS Control Tower Controls Reference Guide.

La console AWS Control Tower mostra ulteriori dettagli sulle unità organizzative e sugli account

22 luglio 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

Puoi visualizzare le organizzazioni e gli account non registrati in AWS Control Tower, insieme alle organizzazioni e agli account registrati.

Nella console di AWS Control Tower, puoi visualizzare maggiori dettagli sui tuoi AWS account e sulle unità organizzative (OU). La pagina Account ora elenca tutti gli account dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di iscrizione in AWS Control Tower. Ora puoi cercare, ordinare e filtrare in tutte le tabelle.

Usa AWS Control Tower per configurare nuovi account multipli AWS ambienti in AWS Organizations

22 aprile 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Organizations i clienti possono ora utilizzare AWS Control Tower per gestire unità organizzative (OU) e account di nuova creazione sfruttando queste nuove funzionalità:

- AWS Organizations I clienti esistenti possono ora configurare una nuova zona di destinazione per nuove unità organizzative (OU) nel loro account di gestione esistente. Puoi creare nuove

unità organizzative in AWS Control Tower e creare nuovi account in tali unità organizzative con la governance di AWS Control Tower.

- AWS Organizations i clienti possono registrare account esistenti utilizzando il processo di registrazione degli account o tramite script.

AWS Control Tower fornisce un servizio di orchestrazione che utilizza altri servizi. AWS È progettato per organizzazioni con più account e team che cercano il modo più semplice per configurare un AWS ambiente multi-account nuovo o esistente e governare su larga scala. Con un'organizzazione governata da AWS Control Tower, gli amministratori del cloud sanno che gli account dell'organizzazione sono conformi alle politiche stabilite. I builder ne traggono vantaggio perché possono effettuare il provisioning di nuovi AWS account rapidamente, senza preoccupazioni indebite sulla conformità.

Per informazioni sulla creazione di una zona di atterraggio, vedere. [Pianifica la tua landing zone di AWS Control Tower](#) Puoi anche visitare la pagina web del [prodotto AWS Control Tower](#) o YouTube visitare questo video su [come iniziare a usare AWS Control Tower per AWS Organizations](#).

Oltre a questa modifica, la funzionalità di provisioning rapido degli account in AWS Control Tower è stata rinominata account Enroll. Ora consente la registrazione di AWS account esistenti e la creazione di nuovi account. Per ulteriori informazioni, consulta [Registra un account esistente dalla console AWS Control Tower](#).

Personalizzazioni per la soluzione AWS Control Tower

17 marzo 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower include ora una nuova implementazione di riferimento che semplifica l'applicazione di modelli e policy personalizzati alla zona di destinazione di AWS Control Tower.

Con le personalizzazioni per AWS Control Tower, puoi utilizzare CloudFormation i modelli per distribuire nuove risorse su account esistenti e nuovi all'interno della tua organizzazione. Puoi anche applicare policy di controllo dei servizi (SCP) personalizzate a tali account in aggiunta agli SCP già forniti da AWS Control Tower. Le personalizzazioni per la pipeline di AWS Control Tower si integrano con gli eventi e le notifiche del ciclo di vita di AWS Control Tower ([Eventi del ciclo di vita in AWS Control Tower](#)) per garantire che le distribuzioni delle risorse rimangano sincronizzate con la tua zona di destinazione.

La documentazione di distribuzione per questa architettura di soluzioni AWS Control Tower è disponibile nella pagina web delle soluzioni. [AWS](#)

Disponibilità generale della versione 2.3 di AWS Control Tower

5 marzo 2020

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower. Per informazioni, consulta [Aggiorna la tua landing zone.](#))

AWS Control Tower è ora disponibile nella AWS regione Asia Pacifico (Sydney), oltre alle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon) ed Europa (Irlanda). L'aggiunta della regione Asia Pacifico (Sydney) è l'unica modifica introdotta per la versione 2.3 di AWS Control Tower.

Se non hai mai utilizzato AWS Control Tower in precedenza, puoi avviarlo oggi stesso in una qualsiasi delle regioni supportate. Se stai già utilizzando AWS Control Tower e desideri estenderne le funzionalità di governance alla regione Asia Pacifico (Sydney) nei tuoi account, vai alla pagina delle impostazioni nella dashboard di AWS Control Tower. Da lì, aggiorna la tua zona di destinazione alla versione più recente. Quindi, aggiorna i tuoi account singolarmente.

Note

L'aggiornamento della zona di atterraggio non aggiorna automaticamente i tuoi account. Se disponi di più account, gli aggiornamenti richiesti possono richiedere molto tempo. Per questo motivo, ti consigliamo di evitare di espandere la zona di destinazione di AWS Control Tower in regioni in cui non è necessario eseguire i carichi di lavoro.

Per informazioni sul comportamento previsto dei controlli investigativi a seguito di una distribuzione in una nuova regione, consulta [Configurare le regioni AWS Control Tower.](#)

Single-step provisioning degli account in AWS Control Tower

2 marzo 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora supporta il provisioning degli account in un'unica fase tramite la console AWS Control Tower. Questa funzionalità consente di effettuare il provisioning di nuovi account dalla console AWS Control Tower.

Per utilizzare il modulo semplificato, accedi ad **Account Factory** nella console AWS Control Tower e scegli **Quick account provisioning**. AWS Control Tower assegna lo stesso indirizzo email all'account fornito e all'utente **Single Sign-on (IAM Identity Center)** creato per l'account. Se desideri che questi due indirizzi email siano diversi, devi effettuare il provisioning del tuo account tramite **Service Catalog**.

Aggiorna gli account creati tramite un rapido provisioning degli account utilizzando **Service Catalog** e **AWS Control Tower account factory**, proprio come gli aggiornamenti di qualsiasi altro account.

Note

Nell'aprile 2020, la funzionalità di provisioning rapido degli account è stata rinominata **account Enroll**. Nel giugno 2022, la possibilità di creare e aggiornare account nella console AWS Control Tower è stata separata dalla possibilità di registrare account. AWS Per ulteriori informazioni, consulta [Registra un account esistente dalla console AWS Control Tower](#).

Strumento di smantellamento di AWS Control Tower

28 febbraio 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora supporta uno strumento di smantellamento automatico per aiutarti a ripulire le risorse allocate da AWS Control Tower. Se non intendi più utilizzare AWS Control Tower per la tua azienda o se hai bisogno di una ridistribuzione importante delle tue risorse organizzative, potresti voler ripulire le risorse create durante la configurazione iniziale della zona di destinazione.

Per disattivare la tua zona di destinazione utilizzando un processo per lo più automatizzato, contatta **Supporto AWS** per ricevere assistenza con i passaggi aggiuntivi necessari. Per ulteriori informazioni sullo smantellamento, vedere. [Smantellamento di una landing zone di AWS Control Tower](#)

Notifiche degli eventi del ciclo di vita di AWS Control Tower

22 gennaio 2020

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower annuncia la disponibilità delle notifiche degli eventi del ciclo di vita. Un evento del [ciclo di vita](#) segna il completamento di un'azione di AWS Control Tower in grado di modificare

lo stato di risorse quali unità organizzative (OU), account e controlli creati e gestiti da AWS Control Tower. Gli eventi del ciclo di vita vengono registrati come AWS CloudTrail eventi e trasmessi ad Amazon come eventi. EventBridge

AWS Control Tower registra gli eventi del ciclo di vita al completamento delle seguenti azioni che possono essere eseguite utilizzando il servizio: creazione o aggiornamento di una zona di destinazione; creazione o eliminazione di un'unità organizzativa; attivazione o disattivazione di un controllo su un'unità organizzativa; utilizzo dell'account factory per creare un nuovo account o spostare un account in un'altra unità organizzativa.

AWS Control Tower utilizza diversi AWS servizi per creare e gestire un ambiente con più account con best practice. AWS Il completamento di un'azione di AWS Control Tower può richiedere diversi minuti. Puoi tenere traccia degli eventi del ciclo di vita nei CloudTrail log per verificare se l'azione originaria di AWS Control Tower è stata completata correttamente. Puoi creare una EventBridge regola per notificarti quando viene CloudTrail registrato un evento del ciclo di vita o per attivare automaticamente la fase successiva del flusso di lavoro di automazione.

giugno - dicembre 2019

Dal 24 giugno al 31 dicembre 2019, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- [Disponibilità generale della versione 2.2 di AWS Control Tower](#)
- [Nuovi controlli elettivi in AWS Control Tower](#)
- [Nuovi controlli investigativi in AWS Control Tower](#)
- [AWS Control Tower accetta indirizzi e-mail per account condivisi con domini diversi rispetto all'account di gestione](#)
- [Disponibilità generale della versione 2.1 di AWS Control Tower](#)

Disponibilità generale della versione 2.2 di AWS Control Tower

13 novembre 2019

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower. Per informazioni, consulta [Aggiorna la tua landing zone.](#))

La versione 2.2 di AWS Control Tower fornisce tre nuovi controlli preventivi che impediscono la deviazione degli account:

- [Non consentire modifiche ai gruppi di CloudWatch log di Amazon Logs configurati da AWS Control Tower](#)
- [Disabilita l'eliminazione delle autorizzazioni di AWS Config aggregazione create da AWS Control Tower](#)
- [Disabilita l'eliminazione dell'archivio di log](#)

Un controllo è una regola di alto livello che fornisce una governance continua per l'intero ambiente. AWS Quando crei la tua landing zone di AWS Control Tower, la zona di atterraggio e tutte le unità organizzative (OU), gli account e le risorse sono conformi alle regole di governance applicate dai controlli scelti. Quando tu e i membri della tua organizzazione utilizzate la zona di atterraggio, possono verificarsi modifiche (accidentali o intenzionali) a questo stato di conformità. Il rilevamento della deriva consente di identificare le risorse che necessitano di modifiche o aggiornamenti di configurazione per risolvere la deriva. Per ulteriori informazioni, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Nuovi controlli elettivi in AWS Control Tower

05 settembre 2019

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora include i seguenti quattro nuovi controlli opzionali:

- [Impedisci le azioni di eliminazione sui bucket Amazon S3 senza MFA](#)
- [Non consentire modifiche alla configurazione di replica per i bucket Amazon S3](#)
- [Non consentire azioni come utente root](#)
- [Impedisci la creazione di chiavi di accesso per l'utente root](#)

Un controllo è una regola di alto livello che fornisce una governance continua per l'intero AWS ambiente. I guardrail consentono di esprimere le intenzioni di policy. Per ulteriori informazioni, consulta [Informazioni sui controlli in AWS Control Tower](#).

Nuovi controlli investigativi in AWS Control Tower

25 agosto 2019

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

AWS Control Tower ora include i seguenti otto nuovi controlli investigativi:

- [Rileva se il controllo delle versioni per i bucket Amazon S3 è abilitato](#)
- [Rileva se l'MFA è abilitato per gli utenti IAM della console AWS](#)
- [Rileva se l'MFA è abilitato per gli utenti IAM](#)
- [Rileva se l'ottimizzazione di Amazon EBS è abilitata per le istanze Amazon EC2](#)
- [Rileva se i volumi Amazon EBS sono collegati alle istanze Amazon EC2](#)
- [Rileva se l'accesso pubblico alle istanze di database Amazon RDS è abilitato](#)
- [Rileva se l'accesso pubblico alle istantanee del database Amazon RDS è abilitato](#)
- [Rileva se la crittografia dello storage è abilitata per le istanze di database Amazon RDS](#)

Un controllo è una regola di alto livello che fornisce una governance continua per l'intero ambiente. AWS Un controllo investigativo rileva la non conformità delle risorse all'interno degli account, come le violazioni delle policy, e fornisce avvisi tramite la dashboard. Per ulteriori informazioni, consulta [Informazioni sui controlli in AWS Control Tower](#).

AWS Control Tower accetta indirizzi e-mail per account condivisi con domini diversi rispetto all'account di gestione

1 agosto 2019

(Nessun aggiornamento richiesto per la zona di atterraggio di AWS Control Tower)

In AWS Control Tower, ora puoi inviare indirizzi e-mail per account condivisi (archivio di log e membri di audit) e account secondari (distribuiti utilizzando account factory) i cui domini sono diversi dall'indirizzo email dell'account di gestione. Questa funzionalità è disponibile solo quando crei una nuova zona di destinazione e quando esegui il provisioning di nuovi account secondari.

Disponibilità generale della versione 2.1 di AWS Control Tower

24 giugno 2019

(Aggiornamento richiesto per la zona di atterraggio di AWS Control Tower. Per informazioni, consulta [Update Your Landing Zone](#).)

AWS Control Tower è ora disponibile a livello generale e supportato per l'uso in produzione. AWS Control Tower è destinato alle organizzazioni con più account e ai team che cercano il modo più

semplice per configurare il loro nuovo AWS ambiente con più account e governare su larga scala. Con AWS Control Tower, puoi contribuire a garantire che gli account della tua organizzazione siano conformi alle policy stabilite. Gli utenti finali dei team distribuiti possono effettuare rapidamente il provisioning di nuovi AWS account.

Utilizzando AWS Control Tower, puoi [configurare una zona di destinazione](#) che utilizza best practice come la configurazione di una struttura [multi-account](#) utilizzando AWS Organizations, la gestione delle identità degli utenti e dell'accesso federato con Centro identità AWS IAM, l'abilitazione del provisioning degli account tramite Service Catalog e la creazione di un archivio di log centralizzato utilizzando e. AWS CloudTrail AWS Config

Per una governance continua, puoi abilitare i controlli preconfigurati, che sono regole chiaramente definite per la sicurezza, le operazioni e la conformità. I guardrail aiutano a prevenire l'implementazione di risorse non conformi alle policy e monitorano continuamente le risorse impiegate per individuare eventuali non conformità. La dashboard di AWS Control Tower offre una visibilità centralizzata in un AWS ambiente che include gli account assegnati, i controlli abilitati e lo stato di conformità degli account.

Puoi configurare un nuovo ambiente con più account con un solo clic nella console di AWS Control Tower. Non sono previsti costi aggiuntivi o impegni anticipati per l'utilizzo di AWS Control Tower. Paghi solo per i AWS servizi che hai abilitato per configurare una zona di atterraggio e implementare controlli selezionati.

Cronologia dei documenti

- Ultimo aggiornamento della documentazione: 30 dicembre 2025

La tabella seguente descrive importanti modifiche alla AWS Control Tower User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Account Factory for Terraform (AFT) supporta le esecuzioni di personalizzazione solo in base al piano	AFT ora supporta la personalizzazione solo in base al piano (sola lettura) che avviene attraverso l'input alla macchina a stati. <code>plan_only</code> <code>aft-invoke-customizations</code> Per impostazione predefinita, AFT esporta l'output del piano in un bucket Amazon S3 crittografato nella distribuzione Community Edition (open source). L'esportazione è opzionale su Terraform Cloud e Terraform Enterprise.	16 settembre 2026
Aggiornamento della politica gestita	Aggiornato AWS ControlTowerServiceRolePolicy .	19 maggio 2026
Aggiornamento della politica gestita	Aggiornato AWS ControlTowerAccountServiceRolePolicy .	19 maggio 2026
Aggiornamento della politica gestita	Aggiornato AWS ControlTowerAccountServiceRolePolicy .	30 dicembre 2025
AWS Control Tower landing zone versione 4.0 con ambiente di controllo dedicato	La versione 4.0 della landing zone di AWS Control Tower è ora disponibile con integrazioni	17 novembre 2025

oni di servizi opzionali e un ambiente di controllo dedicato.

[AWS Control Tower include 279 AWS Config controlli aggiuntivi](#)

Catalogo di controllo aggiornato per includere 279 AWS Config controlli aggiuntivi.

14 novembre 2025

[Aggiornamento della politica gestita](#)

Aggiornato [AWS ControlTowerAccountServiceRolePolicy](#).

10 novembre 2025

[Policy gestite e aggiornate](#)

Aggiornato [AWS ControlTowerServiceRolePolicy](#) per supportare l'AWS CloudTrail integrazione opzionale di Landing Zone 4.0. Il modello di risorse di Amazon CloudWatch Logs è cambiato da `aws-controltower/CloudTrailLogs:*` a `aws-controltower/CloudTrailLogs*:*` per consentire la gestione di gruppi di log con suffissi univoci. Questo aggiornamento è compatibile con le versioni precedenti e consente ai clienti di abilitare e disabilitare AWS CloudTrail l'integrazione più volte, con gruppi di log ricreati ogni volta con suffissi unici per evitare conflitti di denominazione.

5 novembre 2025

Nuova politica gestita	Documentazione aggiunta per la politica AWS ControlTowerCloudTrailRolePolicy gestita. Questa politica gestita sostituisce la politica in linea precedentemente utilizzata da AWS ControlTowerCloudTrailRole, consentendo di AWS aggiornare la politica senza l'intervento del cliente.	5 novembre 2025
AWS Control Tower disponibile nella regione Asia Pacifico (Nuova Zelanda)	AWS Control Tower è disponibile nella regione di Auckland, Nuova Zelanda.	28 ottobre 2025
AWS Control Tower supporta la registrazione automatica degli account	Registrazione automatica degli account e spostamento tra le unità organizzative.	15 ottobre 2025
Aggiornamento alla politica gestita, nuova politica gestita	Aggiornato AWS ControlTowerServiceRolePolicy aggiunto di nuovi AWS ControlTowerIdentityCenterManagementPolicy .	14 ottobre 2025
AWS Control Tower aggiorna la versione Python	Versioni Python aggiornate negli ambienti AWS Control Tower	3 settembre 2025
AWS Control Tower supporta IPv6	AWS Control Tower aggiunge il supporto per gli endpoint IPv6.	18 agosto 2025
Account Factory per Terraform versione 1.15.0	È disponibile la versione 1.15.0 di AFT.	28 luglio 2025

<u>Controlli aggiornati con i tipi di istanze Nitro</u>	Sono stati aggiornati otto controlli proattivi per aggiungere e nuovi tipi di istanze.	24 luglio 2025
<u>AWS Control Tower disponibile in Asia Pacifico (Taipei)</u>	AWS Control Tower aggiunge il supporto per l'Asia Pacifico (Taipei).	23 luglio 2025
<u>AWS Control Tower supporta AWS PrivateLink</u>	AWS Control Tower aggiunge il supporto per AWS PrivateLink.	30 giugno 2025
<u>Service-linked AWS Config controlli</u>	AWS Control Tower distribuisce controlli collegati ai servizi AWS Config .	12 giugno 2025
<u>Metadati migliorati. Controlli aggiuntivi, nuovi framework</u>	AWS Control Tower introduce controlli integrati aggiuntivi da AWS Config, con metadati migliorati per tutti i controlli nel Control Catalog e supporto per altri framework di settore.	12 giugno 2025
<u>Visualizzazione dei controlli abilitati</u>	AWS Control Tower introduce una visualizzazione completa da console dei controlli abilitati .	21 maggio 2025
<u>AFT supporta nuove configurazioni</u>	AWS Control Tower AFT supporta tre configurazioni opzionali aggiuntive al momento della distribuzione.	13 maggio 2025
<u>Linee di base migliorate</u>	AWS Control Tower ora segnala la variazione di base.	12 maggio 2025

AWS Control Tower disponibili nelle regioni di AWS Asia Pacifico (Tailandia) e Messico (Centrale)	Sono disponibili le seguenti regioni: Asia Pacifico (Tailandia) e Messico (Centrale).	9 maggio 2025
AWS Control Tower aggiunge 233 AWS Config controlli	Aggiunti nuovi controlli Config, tabelle di metadati rinnovate, tabelle Region, pagina identificatore globale.	11 aprile 2025
AWS Control Tower aggiorna un ruolo collegato al servizio	Aggiornamenti a. AWSControlTowerAccountServiceRolePolicy	10 dicembre 2024
AWS Control Tower cFCT supporta GitHub	Una nuova opzione per una fonte di configurazione di terze parti.	9 dicembre 2024
Controlli preventivi di AWS Control Tower con policy dichiarative	Un nuovo tipo di policy implementa un nuovo tipo di controllo preventivo.	1 dicembre 2024
AWS Control Tower si integra con Backup AWS	Puoi configurare piani per il backup delle risorse AWS Control Tower.	25 novembre 2024
AWS Control Tower integra i AWS Config controlli	AWS Control Tower integra AWS Config controlli selezionati.	21 novembre 2024
AWS Control Tower migliora la gestione degli hook	AWS Control Tower ora gestisce gli hook per i controlli proattivi.	20 novembre 2024
Segnalata una variazione delle politiche di controllo	AWS Control Tower segnala un nuovo tipo di deriva.	15 novembre 2024

AWS Control Tower lancia politiche di controllo delle risorse gestite	Un nuovo tipo di controlli preventivi, implementato con RCP.	15 novembre 2024
AWS Control Tower aggiunge ResetEnabledControl l'API	Una nuova API per gestire la deriva del controllo.	14 novembre 2024
API aggiornata GetControl	Due nuovi campi di controllo perGetControl .	8 novembre 2024
AWS Control Tower AFT supporta Gitlab	Una nuova opzione per una fonte di configurazione di terze parti.	23 ottobre 2024
AWS Control Tower disponibile nella regione AWS Asia Pacifico (Malesia)	È disponibile una nuova regione, Malesia (Kuala Lumpur).	21 ottobre 2024
AWS Control Tower supporta fino a 1000 account per unità organizzativa	Un aumento del limite di account per unità organizzativa.	30 agosto 2024
AWS Control Tower aggiunge la selezione della versione della landing zone	Aggiorna o ripara la landing zone senza passare alla versione più recente, se utilizzi la versione 3.1 o successiva.	15 agosto 2024
GetControl e operazioni ListControls API disponibili	Due nuove operazioni del Control Catalog consentono di trovare ulteriori informazioni sui controlli.	6 agosto 2024
AWS Control Tower supporta AFT e cFCT nelle regioni opt-in	AFT e cFCT sono disponibili in aggiunta. Regioni AWS	18 luglio 2024
AWS Control Tower aggiunge l'ListLandingZoneOperations API	Una nuova API che ti consente di recuperare le operazioni recenti per la tua landing zone.	26 giugno 2024

<u>AWS Control Tower supporta fino a 100 operazioni di controllo simultanee</u>	Un aumento della quota delle operazioni di controllo simultanee a 100.	20 maggio 2024
<u>AWS Control Tower disponibile nella AWS regione di Calgary West (Canada)</u>	AWS Control Tower è disponibile nella regione Canada occidentale (Calgary).	3 maggio 2024
<u>AWS Control Tower supporta l'aggiustamento delle quote in modalità self-service</u>	AWS Control Tower è integrato con AWS Service Quotas nella console.	25 aprile 2024
<u>La documentazione relativa ai controlli è stata spostata in una nuova guida</u>	AWS Control Tower ha pubblicato la Controls Reference Guide.	21 aprile 2024
<u>Etichettare EnabledControl le risorse in CloudFormation</u>	AWS Control Tower supporta l'aggiunta di tag alle EnabledControl risorse tramite CloudFormation modelli.	22 febbraio 2024
<u>API di base disponibili</u>	AWS Control Tower ha rilasciato nuove API per la registrazione programmatica delle unità organizzative.	14 febbraio 2024
<u>Landing zone di AWS Control Tower versione 3.3</u>	Disponibile la versione 3.3 della landing zone di AWS Control Tower.	14 dicembre 2023
<u>AWS Control Tower annuncia i controlli per favorire la sovranità digitale</u>	AWS Control Tower ha rilasciato un gruppo di controlli per aiutare i clienti con requisiti di sovranità digitale.	27 novembre 2023

<u>AWS Control Tower supporta le API delle landing zone</u>	AWS Control Tower supporta la configurazione e il lancio di landing zone utilizzando nuove API.	26 novembre 2023
<u>AWS Control Tower supporta i controlli abilitati all'etichettatura</u>	AWS Control Tower supporta l'etichettatura dei controlli abilitati, in console e con nuove API.	10 novembre 2023
<u>AWS Control Tower disponibile in Asia Pacifico (Melbourne) Regione AWS</u>	Disponibile nella regione Asia Pacifico (Melbourne).	3 novembre 2023
<u>Nuova API di controllo disponibile</u>	AWS Control Tower ha rilasciato una nuova API di controllo.	14 ottobre 2023
<u>AWS Control Tower lancia nuovi controlli</u>	AWS Control Tower ha rilasciato nuovi controlli proattivi e investigativi.	5 ottobre 2023
<u>I report di AWS Control Tower derivano dalla disabilitazione dell'accesso affidabile</u>	AWS Control Tower avvisa i clienti quando si verifica una deriva, se i clienti disattivano l'accesso affidabile ad AWS Control Tower in. AWS Organizations	21 settembre 2023
<u>AWS Control Tower disponibile in quattro versioni aggiuntive e Regioni AWS</u>	Disponibile in Asia Pacifico (Hyderabad), Europa (Spagna e Zurigo) e Medio Oriente (Emirati Arabi Uniti).	13 settembre 2023
<u>AWS Control Tower disponibile nella regione di Tel Aviv</u>	AWS Control Tower è disponibile nella regione di Tel Aviv, il-central-1.	28 agosto 2023

<u>AWS Control Tower lancia 28 nuovi controlli proattivi</u>	AWS Control Tower ha rilasciato 28 nuovi controlli proattivi.	24 luglio 2023
<u>AWS Control Tower rende obsoleti 2 controlli</u>	AWS Control Tower rimuoverà due controlli dalla libreria dei controlli a partire dal 18 agosto 2023.	18 luglio 2023
<u>Disponibile la landing zone 3.2 di AWS Control Tower</u>	È disponibile la versione 3.2 della landing zone di AWS Control Tower.	16 giugno 2023
<u>AWS Control Tower gestisce gli account in base all'ID</u>	AWS Control Tower tiene traccia AWS dell'ID dell'account, anziché dell'indirizzo e-mail dell'account.	14 giugno 2023
<u>Sono disponibili controlli di rilevamento CSPM aggiuntivi di Security Hub</u>	AWS Control Tower aggiunge dieci nuovi controlli alla libreria di controlli, per lo Service-Managed standard CSPM di Security Hub: AWS Control Tower.	12 giugno 2023
<u>AWS Control Tower pubblica tabelle di metadati di controllo</u>	AWS Control Tower ora fornisce tabelle di metadati di controllo come parte della documentazione pubblicata.	7 giugno 2023
<u>Supporto Terraform per la personalizzazione di Account Factory</u>	Single-region supporto per i progetti open source Terraform in AFC.	6 giugno 2023
<u>AWS Autogestione IAM disponibile per la landing zone</u>	AWS Control Tower ora supporta i clienti nella scelta del proprio provider di identità per una landing zone.	6 giugno 2023

Nuovo ruolo aggiunto	AWS Control Tower ha aggiunto un nuovo ruolo collegato ai servizi e una policy associata. <code>AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy</code>	1 giugno 2023
Aggiornamento misto sulla governance	Aggiornamento per consigliare i clienti in merito alla governance mista.	1 giugno 2023
Sono disponibili controlli proattivi aggiuntivi	I nuovi controlli proattivi ti aiutano a gestire l'ambiente multi-account e a raggiungere obiettivi di controllo specifici.	19 maggio 2023
Sono disponibili sette regioni aggiuntive	AWS Control Tower è ora disponibile in sette paesi aggiuntivi Regioni AWS: California settentrionale (San Francisco), Asia Pacifico (Hong Kong, Giacarta e Osaka), Europa (Milano), Medio Oriente (Bahrein) e Africa (Città del Capo).	19 aprile 2023
Passa a una policy gestita	Abbiamo modificato il <code>AWSControlTowerServiceRolePolicy</code> in modo che AWS Control Tower possa chiamare le <code>EnableRegion</code> , <code>ListRegions</code> , <code>GetRegionOptStatus</code> API implementate dal servizio di gestione degli AWS account.	6 aprile 2023

Il tracciamento delle richieste di personalizzazione dell'account è generalmente disponibile	AWS Control Tower ora supporta la possibilità di tracciare le richieste di personalizzazione degli account utilizzando il flusso di lavoro Account Factory for Terraform (AFT).	16 febbraio 2023
Aggiornamento delle best practice di IAM	Guida aggiornata per allinearsi alle raccomandazioni sulle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM .	15 febbraio 2023
Disponibile la landing zone 3.1 di AWS Control Tower	È disponibile la landing zone 3.1 di AWS Control Tower.	9 febbraio 2023
Controlli proattivi generalmente disponibili	I controlli proattivi vengono avviati dallo stato di anteprima alla disponibilità generale.	24 gennaio 2023
Operazioni simultanee sull'account	AWS Control Tower ora supporta fino a cinque (5) azioni simultanee in Account Factory. Puoi creare, aggiornare o registrare fino a cinque account alla volta.	16 dicembre 2022
I controlli proattivi aiutano nell'approvvigionamento delle risorse	AWS Control Tower ora supporta controlli proattivi , implementati tramite CloudFormation hook.	28 novembre 2022

[È disponibile la personalizzazione dell'account di fabbrica](#)

AWS Control Tower ora supporta il provisioning degli account con modelli di account personalizzabili, chiamati blueprint, direttamente dalla console AWS Control Tower.

28 novembre 2022

[Lo stato di conformità è visualizzabile per tutte le regole AWS Config](#)

AWS Control Tower ora mostra lo stato di conformità di tutte le AWS Config regole distribuite nelle unità organizzative registrate con AWS Control Tower.

18 novembre 2022

[Passa a una policy gestita](#)

Abbiamo modificato il codice `AWSControlTowerServiceRolePolicy` in modo che AWS Control Tower possa assumere il `AWSControlTowerBlueprintAccess` ruolo necessario per le personalizzazioni di Account Factory.

28 ottobre 2022

[API per controlli e risorse CloudFormation](#)

AWS Control Tower ora supporta l'attivazione e la disattivazione dei controlli tramite una serie di chiamate API e una nuova CloudFormation risorsa.

1 settembre 2022

[cFct supporta l'eliminazione di set di stack](#)

cFct supporta l'eliminazione degli stack set, impostando un parametro nel file manifest.

26 agosto 2022

[Conservazione personalizzata dei log](#)

Puoi personalizzare la politica di conservazione per i bucket Amazon S3 che archiviano i CloudTrail log di AWS Control Tower, in incrementi di giorni o anni, fino a un massimo di 15 anni.

15 agosto 2022

[È disponibile la riparazione di Role Drift](#)

AWS Control Tower supporta la riparazione per la deriva dei ruoli, senza una riparazione completa della landing zone.

11 agosto 2022

[Disponibile la versione 3.0](#)

La versione 3.0 della landing zone di AWS Control Tower passa dai AWS CloudTrail percorsi basati sull'account ai percorsi basati sull'organizzazione e aggiorna la policy gestita per abilitare percorsi a livello di organizzazione. Ti consente di AWS Config aggregare le informazioni solo nella tua regione d'origine. La versione 3.0 include anche un aggiornamento alla Region Deny Control e due nuovi controlli investigativi.

29 luglio 2022

[La pagina Organizzazione combina le visualizzazioni delle unità organizzative e degli account](#)

La nuova pagina Organization in AWS Control Tower mostra una visualizzazione gerarchica di tutte le unità organizzative (OU) e gli account.

18 luglio 2022

<u>Passa a una policy gestita</u>	Abbiamo modificato l'impostazione AWSControlTowerServiceRolePolicyin modo che i clienti possano disporre di AWS CloudTrail percorsi a livello di organizzazione per aggregare i log. AWS CloudTrail	20 giugno 2022
<u>Registrazione e aggiornamento più semplici per gli account dei membri</u>	AWS Control Tower ora ti offre la possibilità di registrare e aggiornare gli account dei membri individualmente, dall'interno della tua landing zone. Ogni account mostra quando è disponibile per un aggiornamento. Abbiamo separato il pulsante Registra account dal flusso di lavoro Crea account in Account Factory.	31 maggio 2022
<u>AFT supporta la personalizzazione per gli account condivisi</u>	AWS Control Tower Account Factory for Terraform ora supporta la personalizzazione per l'account di gestione AWS Control Tower, l'archivio dei log e gli account di audit.	27 maggio 2022
<u>Operazioni simultanee per tutti i controlli opzionali</u>	AWS Control Tower ora consente di applicare e rimuovere contemporaneamente protezioni preventive opzionali e controlli investigativi.	18 maggio 2022

Account di sicurezza e registrazione esistenti	AWS Control Tower ora supporta la possibilità di utilizzare gli account di sicurezza e registrazione esistenti, anziché crearne di nuovi durante la configurazione delle landing zone.	16 maggio 2022
Disponibile la versione 2.9	La versione 2.9 della landing zone di AWS Control Tower aggiorna il server di inoltro di notifiche Lambda per utilizzare il runtime Python versione 3.9.	22 aprile 2022
Supporto aggiornato per le migliori pratiche, disponibile la AWS versione 2.8	La versione 2.8 della landing zone di AWS Control Tower fornisce supporto aggiuntivo per garantire che i carichi di lavoro e AWS gli account siano in linea con AWS le migliori pratiche.	10 febbraio 2022
Region nega il controllo	AWS Control Tower ora include un controllo che ti aiuta a limitare l'accesso alle AWS regioni, per risolvere problemi di conformità e normative.	30 novembre 2021
Controlli sulla residenza dei dati	AWS Control Tower ora supporta controlli che aiutano a gestire la residenza dei dati con un controllo granulare.	30 novembre 2021
AWS Control Tower Account Factory per Terraform	AWS Control Tower ora supporta Terraform per il provisioning e l'aggiornamento automatizzati degli account.	29 novembre 2021

È disponibile un nuovo evento sul ciclo di vita	L'PrecheckOrganizationalUnit evento registra se alcune risorse impediscono il successo dell'attività di governance Extend, incluse le risorse nelle unità organizzative annidate.	18 novembre 2021
Unità organizzative annidate disponibili	AWS Control Tower ora consente alla landing zone di contenere strutture di unità organizzative annidate.	16 novembre 2021
Detective controlla la concorrenza	I controlli investigativi di AWS Control Tower ora supportano operazioni di abilitazione e disabilitazione simultanee.	5 novembre 2021
Sono disponibili due nuove regioni	AWS Control Tower è ora disponibile in due nuove AWS regioni, la regione Europa (Parigi) e la regione Sud America (San Paolo).	29 luglio 2021
Deselezione della regione	Puoi deselezionare AWS le regioni che non desideri più governare tramite AWS Control Tower.	29 luglio 2021
Chiavi KMS disponibili	Facoltativamente, puoi creare o scegliere le chiavi KMS da gestire per crittografare dati e risorse.	28 luglio 2021

[Passa a una politica gestita](#)

Abbiamo modificato l'impostazione AWSControlTowerServiceRolePolicyin modo che i clienti possano utilizzare le proprie chiavi di crittografia KMS per i AWS CloudTrail log.

28 luglio 2021

[I nomi dei controlli sono cambiati, la funzionalità è rimasta invariata](#)

Alcuni nomi e descrizioni dei controlli sono stati aggiornati per riflettere meglio le intenzioni politiche del controllo, senza modifiche nelle funzionalità.

26 luglio 2021

[Scansioni automatiche degli SCP gestiti](#)

AWS Control Tower esegue scansioni automatiche giornaliere degli SCP gestiti per verificare eventuali deviazioni.

11 maggio 2021

[Nomi personalizzati per unità organizzative e account](#)

AWS Control Tower ti consente di fornire nomi personalizzati durante il processo di configurazione delle landing zone, per le unità organizzative e gli account essenziali, senza creare deviazioni.

16 aprile 2021

[La disattivazione di una landing zone è self-service](#)

AWS Control Tower ora consente di disattivare una landing zone senza contattare l'AWS assistenza. La disattivazione è un processo semiautomatico che non può essere annullato. Non è la stessa cosa che eliminare manualmente tutte le risorse AWS Control Tower.

09 aprile 2021

[Tre regioni aggiuntive](#)

AWS Control Tower è ora disponibile in tre AWS regioni aggiuntive: regione Asia Pacifico (Tokyo), regione Asia Pacifico (Seoul) e regione Asia Pacifico (Mumbai).

8 aprile 2021

[Nuovi controlli Log Archive, disponibile la versione 2.7 della landing zone](#)

Quattro nuovi controlli Log Archive forniscono la governance di Log Archive sulle risorse AWS Control Tower, separatamente dalla governance delle risorse esterne ad AWS Control Tower. Le linee guida su quattro controlli esistenti sono passate da obbligatorie a facoltative. La versione 2.7 della landing zone di AWS Control Tower include un requisito per HTTPS, che non può essere annullato dopo l'aggiornamento.

8 aprile 2021

[Selezione della regione](#)

La selezione della regione AWS Control Tower offre una migliore capacità di gestire l'impronta geografica delle risorse AWS Control Tower. Per ampliare il numero di regioni in cui ospitare AWS risorse o carichi di lavoro, per motivi di conformità, normative, di costo o per altri motivi, ora puoi selezionare le regioni aggiuntive da governare.

19 febbraio 2021

[Registra un'unità organizzativa e gestisci tutti i suoi account con AWS Control Tower contemporaneamente](#)

AWS Control Tower aggiunge la possibilità di registrare un'unità organizzativa, un modo per portare più account alla governance contemporaneamente.

28 gennaio 2021

[Aggiornamenti multipli degli account nelle unità organizzative registrate](#)

Ora puoi aggiornare tutti gli account in qualsiasi unità AWS Organizations organizzativa (OU) registrata contenente fino a 300 account, con un solo clic, dalla dashboard di AWS Control Tower. La funzionalità di aggiornamento di più account, nota anche come aggiornamento in blocco, elimina la necessità di aggiornare un account alla volta o di utilizzare uno script esterno per eseguire l'aggiornamento su più account contemporaneamente.

28 gennaio 2021

[Nuovo ruolo per l'aggregazione di unità organizzative e account non gestiti](#)

Un nuovo ruolo aiuta a rilevare AWS Config le regole esterne, quindi AWS Control Tower non ha bisogno di accedere agli account non gestiti.

29 dicembre 2020

[AWS Control Tower è disponibile in altre AWS regioni.](#)

AWS Control Tower è ora disponibile per essere distribuito nella regione Asia Pacifico (Singapore), nella regione Europa (Francoforte), nella regione Europa (Londra), nella regione Europa (Stoccolma) e nella regione del Canada (centrale). Con questo lancio, AWS Control Tower è ora disponibile in 10 AWS regioni. Questo aggiornamento della landing zone include tutte le regioni elencate e non può essere annullato. Dopo aver aggiornato la landing zone alla versione 2.5, devi aggiornare manualmente tutti gli account registrati affinché AWS Control Tower gestisca le 10 regioni supportate AWS .

18 novembre 2020

[Controlla l'aggiornamento](#)

È stata rilasciata una versione aggiornata per il controllo obbligatorioAWS-GR_IAM_ROLE_CHANGE_PROHIBITED . Il controllo aggiornato consente una registrazione automatica più semplice degli account.

8 ottobre 2020

[La pagina di informazioni correlate è ora disponibile per AWS Control Tower](#)

La pagina informativa correlata semplifica la ricerca di attività comuni che possono essere utili dopo aver configurato la landing zone di AWS Control Tower.

18 settembre 2020

[La console AWS Control Tower mostra maggiori dettagli su unità organizzative e account.](#)

All'interno della console AWS Control Tower, puoi visualizzare maggiori dettagli sui tuoi AWS account e unità organizzative (OU). La pagina «Account» ora elenca tutti gli account dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di registrazione in AWS Control Tower. Ora puoi cercare, ordinare e filtrare su tutte le tabelle.

22 luglio 2020

[AWS Control Tower consente alle organizzazioni esistenti di configurare una landing zone](#)

Ora puoi lanciare una landing zone per AWS Control Tower in un'organizzazione esistente , per portare l'organizzazione alla governance. La funzionalità Quick Account Provisioning in AWS Control Tower è stata rinominata account Enroll e ora consente la registrazione di AWS account esistenti e la creazione di nuovi account.

16 aprile 2020

[AWS Control Tower è ora disponibile in Asia Pacifico](#)

AWS Control Tower è ora disponibile per essere distribuito nella AWS regione Asia Pacifico (Sydney). Questa versione richiede aggiornamenti manuali agli account dei fornitori, esegui l'aggiornamento solo se prevedi di eseguire carichi di lavoro in Asia Pacifico (Sydney).

3 marzo 2020

[È possibile smantellare una landing zone di AWS Control Tower](#)

AWS Support può aiutarvi a smantellare definitivamente una landing zone attraverso un processo per lo più automatizzato che preserva le vostre organizzazioni, anche se sono necessarie alcune operazioni di pulizia manuale.

27 febbraio 2020

[Il provisioning rapido degli account è disponibile in AWS Control Tower](#)

Il provisioning rapido degli account semplifica l'avvio di nuovi account membri quando la landing zone è aggiornata, con la funzione Enroll account (Registra account).

20 febbraio 2020

[Gli eventi del ciclo di vita vengono tracciati in AWS Control Tower](#)

Gli eventi del ciclo di vita forniscono dettagli aggiuntivi per determinati eventi AWS Control Tower, per semplificare l'automazione del flusso di lavoro.

12 dicembre 2019

[Le pagine Impostazioni e attività sono disponibili per AWS Control Tower](#)

Le pagine Impostazioni e Attività semplificano l'aggiornamento della landing zone e la visualizzazione degli eventi registrati.

30 novembre 2019

[Sono disponibili controlli preventivi aggiuntivi per AWS Control Tower](#)

I controlli preventivi in AWS Control Tower mantengono l'organizzazione e le risorse allineate all'ambiente.

6 settembre 2019

[Sono disponibili controlli investigativi aggiuntivi per AWS Control Tower](#)

I controlli investigativi in AWS Control Tower forniscono informazioni sullo stato dell'organizzazione e delle risorse.

27 agosto 2019

[AWS Control Tower è ora disponibile a livello generale](#)

AWS Control Tower è un servizio che offre il modo più semplice per configurare e gestire un AWS ambiente multi-account su larga scala.

24 giugno 2019

AWS Glossario

Per la AWS terminologia più recente, consultate il [AWS glossario](#) nella sezione Reference. Glossario AWS

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.