



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 altri servizi AWS	2
Sei un utente per la prima volta di AWS Control Tower?	3
Come funziona	3
Struttura di una zona di atterraggio di AWS Control Tower	3
Cosa succede quando configuri una landing zone	4
Cosa sono gli account condivisi?	5
Come funzionano i controlli	6
Come funziona AWS Control Tower con StackSets	7
Terminologia	8
Prezzi	12
Configurazione	13
Registrati per AWS	13
Registrati per un Account AWS	13
Crea un utente con accesso amministrativo	14
Approfondimenti	15
Nozioni di base	16
Guida rapida di avvio	16
Controlli prima del lancio	18
Considerazioni per i clienti AWS IAM Identity Center (IAM Identity Center)	19
Configura l'ambiente dedicato ai controlli	20
Nozioni di base	20
Considerazioni su AWS Config	21
Processo di implementazione	21
Note importanti	21
Inizia dalla console	22
Aspettative per la configurazione delle landing zone	22
Passaggio 1: crea gli indirizzi email del tuo account condiviso	23
Passaggio 2. Configura e avvia la tua landing zone	25
Fase 3. Rivedi e configura la landing zone	34
Inizia a usare APIs	34
Aspettative per la configurazione della landing zone con APIs	35
Fase 1: Configura la tua landing zone	36

Fase 2: Avvia la landing zone utilizzando AWS Control Tower APIs	40
Identifica la tua landing zone	43
Aggiorna la tua landing zone	44
Reimposta la landing zone per risolvere la deriva	46
Visualizza i dettagli del file manifest della tua landing zone	47
Visualizza lo stato delle operazioni nelle tue landing zone	50
Esempi: configura una landing zone di AWS Control Tower APIs solo con	53
Schemi delle zone di atterraggio	60
Avvia una landing zone usando CloudFormation	83
Fasi successive	89
Limitazioni e quote	91
Limitazioni note in AWS Control Tower	91
Richiesta di un aumento della quota	94
Limitazioni di controllo	95
Trova i controlli e le regioni disponibili	97
Limitazioni basate sui servizi sottostanti AWS	97
Differenze regionali	98
La guida di riferimento ai controlli	101
Le migliori pratiche per gli amministratori	102
Spiegazione dell'accesso agli utenti	102
Spiegazione dell'accesso alle risorse	102
Spiegazione dei controlli preventivi	103
Pianifica la tua landing zone	104
Confronta le funzionalità	105
Avvia AWS Control Tower in un'organizzazione esistente	106
Lancio di AWS Control Tower in una nuova organizzazione	107
Procedure consigliate: configurare una landing AWS zone con più account	107
Allineati alle linee guida relative a più account AWS	108
Linee guida per configurare un ambiente ben progettato	109
Esempio di AWS Control Tower con una struttura di unità organizzativa multi-account completa	112
Informazioni sul Root	113
Suggerimenti amministrativi per la configurazione delle landing zone	113
Guida alla migrazione di Landing Zone v4.0	115
Modifiche chiave	115
Aggiornamenti di AWS Config	117

Consigli per la configurazione di gruppi, ruoli e politiche	120
Linee guida sulle risorse AWS Control Tower	121
Quando accedere come utente root	124
AWS Organizations guida	125
Linee guida per IAM Identity Center	126
Guida Account Factory	128
Linee guida sulla sottoscrizione a SNS Topics	129
Guida per le chiavi KMS	130
Aggiornamenti della zona di atterraggio	130
Politiche per i servizi basati sull'intelligenza artificiale	133
Gestione degli aggiornamenti della configurazione	134
Informazioni sugli aggiornamenti	136
Aggiorna la tua landing zone	137
Procedura di aggiornamento standard	138
Seleziona una versione di landing zone	138
Aggiornamenti dell'account, versioni delle landing zone e linee di base	140
Conserva i percorsi degli account	140
Risolvi la deriva con Reset and Re-register	142
Esegui il provisioning e aggiorna gli account utilizzando l'automazione	143
Automatizza le attività	145
AWS CloudShell e il AWS CLI	147
Ottieni le autorizzazioni IAM per AWS CloudShell	148
Interagisci con AWS Control Tower AWS CloudShell	149
AWS CloudFormation risorse	152
AWS Control Tower e CloudFormation modelli	152
Scopri di più su CloudFormation	152
Personalizza la tua landing zone	154
Personalizzazione dalla console AWS Control Tower	154
Automatizza le personalizzazioni all'esterno della console AWS Control Tower	156
AWS Control Tower e LZA	156
Vantaggi delle personalizzazioni per AWS Control Tower (cFCT)	157
Esempi cFCT aggiuntivi	158
Panoramica sulle personalizzazioni per AWS Control Tower (cFCT)	158
Architecture	159
Costo	162
Servizi per i componenti	162

AWS CodeCommit	162
AWS CodePipeline	163
AWS Key Management Service	163
AWS Lambda	163
Amazon Simple Notification Service	163
Amazon Simple Storage Service	164
Amazon Simple Queue Service	164
AWS Step Functions	164
AWS Archivio parametri Systems Manager	165
Considerazioni sull'implementazione	165
Preparati per la distribuzione	165
Per aggiornare le personalizzazioni per AWS Control Tower	167
Modello e codice sorgente	167
Codice sorgente	167
Implementa cFCT	167
Prerequisiti	168
Fasi della distribuzione	168
Fase 1: Avvio dello stack	168
Fase 2: Crea un pacchetto personalizzato	172
Aggiorna lo stack	173
Eliminazione di un set di stack	174
Configura Amazon S3 come origine di configurazione	175
Configura GitHub come origine di configurazione	176
Prepara un repository GitHub	176
Crea la connessione GitHub	177
Distribuisci lo stack CloudFormation	177
Parametri operativi	177
Guida alla personalizzazione cFCT	179
Panoramica della pipeline del codice	179
Definire una configurazione personalizzata	181
Unità organizzativa root	188
OU annidata	190
Crea le tue personalizzazioni	190
Aggiornamenti di versione per il manifesto cFct	198
Rete	201
VPCs e AWS regioni in AWS Control Tower	201

Panoramica di AWS Control Tower e VPCs	202
CIDR e peering per VPC e AWS Control Tower	203
AWS PrivateLink	205
Considerazioni	205
Creazione di un endpoint di interfaccia	206
Creazione di una policy dell'endpoint	206
Ruoli e autorizzazioni	208
Ruoli e account	209
Ruoli e creazione di account	209
AWSControlTowerExecution ruolo	209
Condizioni opzionali per il ruolo, le relazioni di fiducia	211
In che modo AWS Control Tower aggrega AWS Config le regole negli account e negli account non gestiti OUs	214
Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower	217
Effettuazione del provisioning automatico degli account con ruoli IAM	221
Gestione delle risorse	223
Configura le regioni	224
Configura le tue regioni AWS Control Tower	225
Evita una governance mista durante la configurazione delle regioni	227
Informazioni sulle regioni che accettano l'adesione	229
Configura il Region Deny Control	232
Considerazioni relative alla regione a livello di unità organizzativa negano il controllo	233
Informazioni sugli account	234
Cosa succede quando AWS Control Tower crea un account	234
Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti	235
Informazioni sugli account condivisi	236
Gestione dell'account	236
Account di archiviazione dei log	236
Account di audit	237
Risorse per account condivisi	238
Risorse dell'account di gestione	239
Registra e archivia le risorse dell'account	243
Controlla le risorse dell'account	246
Informazioni sugli account dei membri	249
Interagisci con gli account AWS Control Tower da AWS Service Catalog	249
Crea ed esegui il provisioning di un account	250

Automatizza il provisioning degli account in AWS Control Tower by Service Catalog APIs ...	251
Aggiornare il prodotto fornito in Service Catalog	255
Annullare la registrazione di un account in Service Catalog	257
Fornisci e gestisci gli account	259
Autorizzazioni richieste	259
Metodi di approvvigionamento	260
Esegui il provisioning degli account nella console	262
Visualizza i tuoi account	263
Informazioni sulla registrazione degli account	264
Cosa succede durante la registrazione dell'account	265
Registra gli account esistenti con VPCs	266
Registra account con risorse AWS Config	267
Prerequisiti per l'iscrizione	267
Opzione di registrazione automatica	269
Registrazione dalla console	271
Se l'account non soddisfa i prerequisiti	275
Aggiungi manualmente il ruolo IAM richiesto a un ruolo esistente Account AWS e registrarlo	277
Registrare account che dispongono di risorse esistenti AWS Config	280
Passaggio 1: contatta l'assistenza per aggiungere account all'elenco degli account consentiti	282
Fase 2: Crea un nuovo ruolo IAM nell'account del membro	283
Fase 3: Identifica le AWS regioni con risorse preesistenti	284
Fase 4: Identifica le AWS regioni prive di AWS Config risorse	284
Fase 5: Modifica le risorse esistenti in ogni AWS regione	284
Fase 5a. AWS Config risorse del registratore	284
Fase 5b. Modifica le risorse del canale AWS Config di distribuzione	285
Fase 5c. Modifica le risorse di AWS Config autorizzazione all'aggregazione	286
Fase 6: Creare risorse dove non esistono, nelle regioni governate da AWS Control Tower ..	286
Fase 7: Registrazione dell'unità organizzativa con AWS Control Tower	288
Factory account	288
Permissions	289
Considerazioni sull'account	289
Aggiorna e sposta gli account	290
Modifica l'indirizzo e-mail di un account registrato	291
Cambia il nome di un account registrato	292

Configurazione delle impostazioni di Amazon VPC	293
Annullare la registrazione di un account	294
Chiudi un account	296
Risorse Account Factory	298
Personalizzazione Account Factory (AFC)	300
Configura per la personalizzazione	302
Crea un account personalizzato a partire da un blueprint	309
Personalizza gli account con AFC man mano che li registri	310
Aggiungi un blueprint a un account AWS Control Tower	310
Aggiorna un blueprint	311
Rimuovere un blueprint da un account	312
Progetti per i partner	312
Considerazioni sulle personalizzazioni di Account Factory (AFC)	312
In caso di errore del blueprint	313
Personalizzazione del documento di policy per i blueprint AFC in base a CloudFormation ...	315
Autorizzazioni aggiuntive necessarie per creare un prodotto Service Catalog basato su Terraform	316
Transizione al tipo di prodotto esterno	317
Account Factory di AWS Control Tower per Terraform (AFT)	319
Prerequisiti	319
Panoramica di AFT	320
Implementa AFT	323
Fornisci un nuovo account	333
Richieste multiple di account	334
Aggiorna un account esistente	335
Versioni supportate	337
Abilita le opzioni delle funzionalità	341
Risorse per AFT	344
Ruoli richiesti	349
Servizi per i componenti	353
Pipeline di fornitura degli account AFT	355
Personalizzazioni dell'account	358
VCS alternativo	364
Protezione dei dati	368
Rimuovere un account	369
Parametri operativi	371

Guida alla risoluzione dei problemi	372
Deviazione	376
Rilevamento della deriva	376
Visualizzazione della deriva	378
Risolvere la deriva	378
Considerazioni sulla deriva e sulla scansione delle politiche	380
Tipi di deriva da risolvere immediatamente	381
Modifiche riparabili alle risorse	382
Drift e fornitura di nuovi account	382
Tipi di deriva della governance	383
Account membro trasferito	385
Account membro rimosso	387
Aggiornamento non pianificato a SCP gestito	388
SCP scollegato dall'unità organizzativa gestita	389
Foundational OU eliminata	390
Deriva di controllo CSPM del Security Hub	391
Controlla la deriva delle politiche	392
Accesso affidabile disabilitato	393
Deriva dell'ereditarietà sulle linee di base abilitate	394
Variazione dell'ereditarietà sui controlli abilitati	394
EventBridge creazione	395
Se gestisci risorse al di fuori di AWS Control Tower	397
Riferimento a risorse esterne a AWS Control Tower	398
Modifica esterna dei nomi delle risorse AWS Control Tower	398
Eliminazione dell'unità organizzativa di sicurezza	399
Rimozione di un account dall'unità organizzativa di sicurezza	400
Modifiche esterne che vengono aggiornate automaticamente	402
Organizations	405
Procedura guidata: video	406
Argomenti	406
Estendi la governance a un'organizzazione esistente	406
Video: Attivazione di una zona di atterraggio esistente AWS Organizations	408
Considerazioni per IAM Identity Center e le organizzazioni esistenti	408
Accesso ad altri AWS servizi	408
Annidato OUs	408
Procedura guidata: video	409

Espandi da una struttura OU piatta a una struttura di unità organizzative annidata	409
Controlli preliminari della registrazione delle unità organizzative annidate	410
Nested e ruoli OUs	410
Cosa succede durante la registrazione e la nuova registrazione degli account nested OUs and	411
Considerazioni sulla registrazione di unità organizzative annidate	411
Limitazioni dell'unità organizzativa annidata	411
Nested e conformità OUs	412
Annidato e alla deriva OUs	412
Nested OUs e controlli	413
Nidato OUs e radice	415
Registra un'unità organizzativa per registrare più account	415
Registrare un'unità organizzativa esistente	417
Crea una nuova unità organizzativa	418
Rimuovere un'unità organizzativa	419
Cause comuni di errore durante la registrazione o la nuova registrazione	420
Aggiorna le organizzazioni	423
Quando effettuare l'aggiornamento OUs e gli account	424
Aggiorna più account in un'unica unità organizzativa	424
Cosa succede durante la nuova registrazione	425
Aggiorna un singolo account	425
Servizi integrati	427
AWS Backup	427
CloudFormation	428
CloudTrail	428
CloudWatch	428
AWS Config	429
Integrazione di AWS Config nella Control Tower Landing Zone 4.0	429
AWS Identity and Access Management	432
AWS Key Management Service	432
AWS Lambda	433
AWS Organizations	433
Considerazioni	434
Simple Storage Service (Amazon S3)	434
Security Hub CSPM	434
AWS Service Catalog	434

Amazon SNS	435
Step Functions	436
Gestione dell'identità e degli accessi	437
Autenticazione	437
Controllo accessi	439
IAM Identity Center e AWS Control Tower	440
Gruppi di utenti, ruoli e set di autorizzazioni	441
Cose da sapere sugli account IAM Identity Center e AWS Control Tower	441
Gruppi IAM Identity Center per AWS Control Tower	442
Panoramica della gestione dell'accesso alle risorse con IAM	446
Risorse e operazioni di AWS Control Tower	447
Informazioni sulla proprietà delle risorse	447
Gestisci l'accesso alle risorse	447
Specificate gli elementi della policy: azioni, effetti e principi	458
Specifica delle condizioni in una policy	458
Evita i confusi attacchi dei vice agenti	459
Policy IAM per AWS Control Tower	460
Autorizzazioni necessarie per utilizzare la console AWS Control Tower	460
AWS ControlTowerAdmin ruolo	462
AWS ControlTowerServiceRolePolicy	463
AWS ControlTowerIdentityCenterManagementPolicy	464
AWS ControlTowerStackSetRole	464
AWS ControlTowerCloudTrailRolePolicy	465
AWS ControlTowerBlueprintAccess requisiti di ruolo	467
AWSServiceRoleForAWSControlTorre	468
AWS ControlTowerAccountServiceRolePolicy	469
Policy gestite per AWS Control Tower	469
Sicurezza	481
Protezione dei dati	481
Crittografia dei dati inattivi	483
Crittografia in transito	483
Limitazione dell'accesso ai contenuti	483
Convalida della conformità	483
Resilienza	484
Sicurezza dell'infrastruttura	485
Registrazione di log e monitoraggio	486

Informazioni sulla registrazione in AWS Control Tower	487
Policy del bucket S3	488
Panoramica del monitoraggio	490
Registrazione delle azioni di AWS Control Tower con AWS CloudTrail	491
Informazioni su AWS Control Tower in CloudTrail	491
Esempio: voci dei file di log di AWS Control Tower	494
Monitora le modifiche alle risorse con AWS Config	495
Gestisci i costi di Config	496
Visualizza i dati del AWS Config registratore sugli account registrati	497
Risoluzione dei problemi AWS Config in AWS Control Tower	498
Eventi del ciclo di vita	500
CreateManagedAccount	503
UpdateManagedAccount	505
EnableGuardrail	506
DisableGuardrail	507
SetupLandingZone	509
UpdateLandingZone	510
RegisterOrganizationalUnit	512
DeregisterOrganizationalUnit	513
PrecheckOrganizationalUnit	515
EnableBaseline	517
ResetEnabledBaseline	518
UpdateEnabledBaseline	520
DisableBaseline	521
Notifiche all'utente	523
Backup	526
Prerequisiti	527
Abilita i backup	529
Prima parte: configura i backup per la tua landing zone	529
Parte successiva: abilitare i backup su OUs	531
Disattiva i backup	533
Primo passaggio: disattivare i backup OUs	533
Passaggio successivo: disattivate AWS Backup la vostra landing zone	533
Account spostati	534
Deriva di Backup	535
Risorse di Backup	536

Controlli per il AWS Backup	539
Smantellamento di una landing zone	540
Panoramica del processo di smantellamento	541
Come disattivare una landing zone	542
Smonta la tua landing zone con APIs	543
Attività di pulizia manuale necessarie dopo la disattivazione	544
Risorse non rimosse durante la disattivazione	545
Rimuovi le risorse AWS Control Tower	548
Ho bisogno della disattivazione anziché dell'eliminazione?	549
Informazioni sulla rimozione delle risorse AWS Control Tower	550
Eliminare SCPs	550
Elimina e impila StackSets	551
Eliminare i bucket Amazon S3 nell'account Log Archive	552
Rimuovi un portafoglio e un prodotto Account Factory	553
Rimuovi i ruoli e le policy di AWS Control Tower	554
Guida alle risorse AWS Control Tower	556
Configurazione dopo la disattivazione di una landing zone	556
Procedure guidate	558
Procedura dettagliata: passaggio da ALZ a AWS Control Tower	558
Procedura dettagliata: configura AWS Control Tower senza un VPC	558
Eliminare il VPC AWS Control Tower	559
Facoltativamente, pulisci la risorsa VPC nell'account	560
Crea un account in AWS Control Tower senza un VPC	560
Procedura dettagliata: configurazione di gruppi di sicurezza in AWS Control Tower con AWS Firewall Manager	561
Configurazione di gruppi di sicurezza con AWS Firewall Manager	562
Risoluzione dei problemi	563
Avvio della landing zone non riuscito	563
Aggiornamento della zona di atterraggio non riuscito con errore KMS	564
Impossibile aggiornare la zona di atterraggio	565
Errore relativo alla zona di atterraggio non aggiornata	566
Provisioning del nuovo account non riuscito	567
Registrazione di un account esistente non riuscita	568
Impossibile aggiornare un account di Factory Account	568
Errore, errore che menziona AWS Config	570
Nessun errore trovato nei percorsi di avvio	572

È stato ricevuto un errore di autorizzazioni insufficienti	572
I controlli investigativi non hanno effetto sugli account	573
Frequenza superata (errore restituito dall' AWS Organizations API)	573
Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower	574
AWS Support	576
Baseline	577
Tipi di base applicabili a livello di unità organizzativa	577
Tipi di base che possono essere applicati all'account condiviso durante la configurazione della landing zone	579
Iscrizione parziale	580
Confronta console e API	581
Linee di base e account dei membri abilitati	582
Linee di base e impostazioni predefinite per il controllo delle versioni	582
AWSControlTowerBaseline tabella	583
Esempi: registra un'unità organizzativa AWS Control Tower APIs solo con	588
Esempi di API di base	590
DisableBaseline	590
EnableBaseline	591
GetBaseline	593
GetBaselineOperation	594
GetEnabledBaseline	594
ListBaselines	595
ListEnabledBaselines	597
ResetEnabledBaseline	602
UpdateEnabledBaseline	602
Informazioni aggiuntive	604
Tutorial e laboratori	604
Rete	201
Sicurezza, identità e registrazione	604
Implementazione delle risorse e gestione dei carichi di lavoro	605
Collaborazione con organizzazioni e account esistenti	606
Automazione e integrazione	606
Migrazione dei carichi di lavoro	606
Servizi AWS correlati	607
Marketplace AWS soluzioni	607

Note di rilascio	608
gennaio 2026 - Presente	608
AWS Control Tower disponibile nel cloud sovrano europeo	608
gennaio 2025 - dicembre 2025	609
Landing zone di AWS Control Tower versione 4.0	609
AWS Control Tower aggiunge 279 AWS Config controlli aggiuntivi a Control Catalog	611
AWS Control Tower disponibile nella regione Asia Pacifico (Nuova Zelanda)	611
AWS Control Tower supporta la registrazione automatica degli account	612
AWS Control Tower aggiorna la versione Python	612
AWS Control Tower riduce la deriva	613
AWS Control Tower supporta IPv6 gli indirizzi	613
Account Factory per Terraform versione 1.15.0 disponibile	613
Controlli aggiornati con i tipi di istanze Nitro	614
AWS Control Tower disponibile nella regione Asia Pacifico (Taipei)	615
AWS Control Tower supporta PrivateLink	615
Support per framework di settore aggiuntivi, metadati aggiornati	615
Controlli collegati ai servizi AWS Config	616
La visualizzazione della console dei controlli abilitati offre visibilità centralizzata	618
Account Factory for Terraform (AFT) supporta nuove configurazioni al momento dell'implementazione	619
AWS Control Tower introduce la reportistica a livello di account come riferimento APIs	619
AWS Control Tower disponibile nelle regioni di AWS Asia Pacifico (Tailandia) e Messico (Centrale)	620
AWS Config Controlli aggiuntivi disponibili	620
Annulla registrazione ed eliminazione delle azioni per OUs	621
Control Catalog supporta gli indirizzi IPv6	621
gennaio - dicembre 2024	621
AWS Control Tower cFCT supporta GitHub e RCPs	622
AWS Control Tower aggiunge controlli preventivi con policy dichiarative	623
AWS Control Tower aggiunge opzioni di piano di backup prescrittivo	623
AWS Control Tower integra i AWS Config controlli	623
AWS Control Tower migliora la gestione degli hook e aggiunge regioni di controllo proattivo	624
AWS Control Tower lancia politiche di controllo delle risorse gestite	624
AWS Control Tower segnala variazioni nelle policy di controllo	625
Nuova API ResetEnabledControl	625

API di controllo degli aggiornamenti del catalogo GetControl	626
AWS Control Tower AFT supporta GitLab	626
AWS Control Tower disponibile nella regione AWS Asia Pacifico (Malesia)	627
AWS Control Tower supporta fino a 1000 account per unità organizzativa	627
AWS Control Tower aggiunge la selezione della versione della landing zone	627
API di controllo descrittivo disponibile, accesso esteso a regioni e controlli	628
AWS Control Tower supporta AFT e cFCT nelle regioni opt-in	629
AWS Control Tower aggiunge l'ListLandingZoneOperationsAPI	629
AWS Control Tower supporta fino a 100 operazioni di controllo simultanee	630
AWS Control Tower disponibile nel AWS Canada occidentale (Calgary)	630
AWS Control Tower supporta l'aggiustamento delle quote in modalità self-service	632
AWS Control Tower rilascia la Controls Reference Guide	632
AWS Control Tower aggiorna e rinomina due controlli proattivi	632
I controlli obsoleti non sono più disponibili	633
AWS Control Tower supporta l'etichettatura EnabledControl delle risorse in CloudFormation	633
AWS Control Tower supporta APIs la registrazione e la configurazione delle unità organizzative con linee di base	634
gennaio - dicembre 2023	635
Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 3)	636
Landing zone di AWS Control Tower versione 3.3	637
Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 2)	638
AWS Control Tower annuncia i controlli per favorire la sovranità digitale	638
Zona di atterraggio AWS Control Tower APIs	642
Etichettatura di controllo di AWS Control Tower APIs	642
AWS Control Tower disponibile in AWS Asia Pacifico (Melbourne)	643
Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 1)	643
AWS Control Tower aggiunge una nuova API di controllo	643
AWS Control Tower aggiunge nuovi controlli	644
AWS Control Tower rileva la deriva di accessi affidabili	644
AWS Control Tower disponibile in quattro versioni aggiuntive Regioni AWS	644
AWS Control Tower disponibile in AWS Israele (Tel Aviv)	645
AWS Control Tower aggiunge 28 nuovi controlli proattivi	645
AWS Control Tower rende obsoleti due controlli	645
Landing zone di AWS Control Tower versione 3.2	645
AWS Control Tower aggiunge la email-to-ID mappatura per IAM Identity Center	647

AWS Control Tower aggiunge ulteriori AWS Security Hub CSPM controlli	647
AWS Control Tower pubblica i metadati per i controlli AWS Security Hub CSPM	648
AWS Control Tower aggiunge Account Factory Customization (AFC) per Terraform	648
AWS Control Tower aggiunge un centro di identità IAM autogestito	649
AWS Control Tower aggiunge una nota di governance mista	649
AWS Control Tower aggiunge nuovi controlli proattivi	649
AWS Control Tower aggiorna i controlli di Amazon EC2	650
AWS Control Tower disponibile in sette versioni aggiuntive Regioni AWS	650
AWS Control Tower Account Factory Customization (AFC) e tracciamento delle richieste sono generalmente disponibili	650
Landing zone di AWS Control Tower versione 3.1	651
Controlli proattivi AWS Control Tower generalmente disponibili	652
gennaio - dicembre 2022	652
Operazioni simultanee sull'account	653
Personalizzazione Account Factory (AFC)	653
I controlli completi facilitano l'approvvigionamento e AWS la gestione delle risorse	654
Lo stato di conformità è visualizzabile per tutte le AWS Config regole	655
API per i controlli e una nuova risorsa CloudFormation	655
cFct supporta l'eliminazione di set di stack	656
Conservazione personalizzata dei log	657
È disponibile la riparazione della deriva dei ruoli	657
Landing zone di AWS Control Tower versione 3.0	657
La pagina Organizzazione combina visualizzazioni e account OUs	661
Creazione e registrazione semplificate dell'account	662
AFT supporta la personalizzazione automatizzata per gli account AWS Control Tower condivisi	662
Operazioni simultanee per tutti i controlli opzionali	663
Account di sicurezza e registrazione esistenti	664
Landing zone di AWS Control Tower versione 2.9	664
Landing zone di AWS Control Tower versione 2.8	665
gennaio - dicembre 2021	666
Funzionalità di negazione della regione	666
Funzionalità di residenza dei dati	667
AWS Control Tower introduce il provisioning e la personalizzazione degli account Terraform	667
Nuovo evento sul ciclo di vita disponibile	668

AWS Control Tower abilita il nested OUs	668
Detective controlla la concorrenza	669
Sono disponibili due nuove regioni	670
Deselezione della regione	670
AWS Control Tower funziona con i sistemi di gestione delle AWS chiavi	671
Controlli rinominati, funzionalità invariata	672
AWS Control Tower esegue scansioni SCPs giornaliere per verificare eventuali deviazioni .	672
Nomi e account personalizzati OUs	672
Landing zone di AWS Control Tower versione 2.7	673
Tre nuove AWS regioni disponibili	675
Governa solo le regioni selezionate	675
AWS Control Tower ora estende la governance OUs alle AWS organizzazioni esistenti	676
AWS Control Tower fornisce aggiornamenti in blocco degli account	676
gennaio - dicembre 2020	677
La console AWS Control Tower ora si collega a regole AWS Config esterne	677
AWS Control Tower ora disponibile in regioni aggiuntive	678
Aggiornamento Guardrail	678
La console AWS Control Tower mostra maggiori dettagli sugli OUs account	679
Usa AWS Control Tower per configurare nuovi AWS ambienti multi-account in AWS Organizations	679
Personalizzazioni per la soluzione AWS Control Tower	680
Disponibilità generale di AWS Control Tower versione 2.3	680
Provisioning degli account in un'unica fase in AWS Control Tower	681
Strumento di smantellamento di AWS Control Tower	682
Notifiche degli eventi relativi al ciclo di vita di AWS Control Tower	682
giugno - dicembre 2019	683
Disponibilità generale di AWS Control Tower versione 2.2	683
Nuovi controlli opzionali in AWS Control Tower	684
Nuovi controlli investigativi in AWS Control Tower	684
AWS Control Tower accetta indirizzi e-mail per account condivisi con domini diversi dall'account di gestione	685
Disponibilità generale di AWS Control Tower versione 2.1	685
Cronologia dei documenti	687
AWS Glossario	710
.....	dccxi

Cos'è AWS Control Tower?

AWS Control Tower offre un modo semplice per configurare e gestire un ambiente AWS multi-account, seguendo le best practice prescrittive. AWS Control Tower orchestra le funzionalità di diversi altri [AWS servizi](#), tra cui AWS Organizations, AWS Service Catalog, e AWS IAM Identity Center, per costruire una landing zone 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 cambino, ossia divergenza 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 gestisci 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 effettuare il provisioning di account e infrastrutture. Con AWS Control Tower, puoi aderire più facilmente agli standard aziendali, soddisfare i requisiti normativi e seguire le best practice.

AWS Control Tower consente agli utenti finali dei team distribuiti di fornire nuovi AWS account rapidamente, tramite modelli di account configurabili in Account Factory. Nel frattempo, gli amministratori cloud centrali 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 multi-account basato sulle best practice stabilite collaborando con migliaia di aziende. Per ulteriori informazioni sull'utilizzo di AWS Control Tower e sulle best practice delineate nella strategia AWS multi-account, consulta [AWS strategia multi-account: linee guida sulle migliori pratiche](#)

Funzionalità

AWS Control Tower ha le seguenti caratteristiche:

- Zona di atterraggio: una landing zone è un [ambiente multi-account](#) ben progettato, basato sulle migliori pratiche di sicurezza e conformità. È il contenitore a livello aziendale che contiene tutte le unità organizzative (OUs), 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: obbligatorie, fortemente raccomandate o facoltative. 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 la fornitura 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 [Fornitura e gestione degli account con Account Factory](#).
- **Dashboard:** la dashboard offre una supervisione continua della landing zone al team di amministratori cloud centrali. Utilizza la dashboard per visualizzare gli account assegnati in tutta l'azienda, i controlli abilitati per l'applicazione delle policy, i controlli abilitati per il rilevamento continuo della non conformità delle policy e le risorse non conformi organizzate per account e. OUs

In che modo AWS Control Tower interagisce con altri servizi AWS

AWS Control Tower si basa su AWS servizi affidabili e affidabili AWS Service Catalog, tra cui AWS IAM Identity Center, 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»), che è costruito 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 politiche a tali account. Per ulteriori informazioni sulla creazione e il provisioning degli account, vedere [Metodi](#) di approvvigionamento.
- **Governance centralizzata:** utilizzando le funzionalità di AWS Organizations, AWS Control Tower configura un framework che garantisce conformità e governance coerenti in tutto l'ambiente multi-account. Il AWS Organizations servizio fornisce funzionalità essenziali per la gestione di un

ambiente multi-account, tra cui governance e gestione centralizzate degli account, creazione di account, politiche di AWS Organizations APIs controllo dei servizi (SCPs) e politiche di controllo delle risorse (RCPs).

- **Estensibilità:** puoi creare o estendere il tuo ambiente AWS Control Tower lavorando direttamente all'interno AWS Organizations e nella console AWS Control Tower. Puoi vedere le tue modifiche riflesse in AWS Control Tower dopo aver registrato le tue organizzazioni esistenti e registrato i tuoi account esistenti in AWS Control Tower. Puoi aggiornare la landing zone di AWS Control Tower in base alle modifiche. Se i tuoi carichi di lavoro richiedono ulteriori funzionalità avanzate, puoi sfruttare altre soluzioni AWS partner oltre ad AWS Control Tower.

Sei un utente per la prima volta 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 maggiori informazioni su come pianificare e organizzare la tua landing zone, 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 delle landing zone 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 di AWS Control Tower

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

- **Root:** il genitore che contiene tutti gli altri elementi OUs nella tua landing zone.
- **Security OU:** questa unità organizzativa contiene gli account Log Archive e Audit. Questi account vengono spesso definiti account condivisi. Quando avvii la tua landing zone, puoi scegliere nomi personalizzati per questi account condivisi e hai la possibilità di trasferire gli AWS account esistenti in AWS Control Tower per motivi di sicurezza e registrazione. Tuttavia, questi non possono essere rinominati in un secondo momento e gli account esistenti non possono essere aggiunti per motivi di sicurezza e registrazione dopo il lancio iniziale.
- **Sandbox OU:** l'OU Sandbox viene creata all'avvio della landing zone, se la abiliti. Questo e altri account registrati OUs contengono gli account registrati con cui gli utenti lavorano per eseguire i loro 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:

- Crea due unità AWS Organizations organizzative (OUs): Security e Sandbox (opzionale), contenute nella struttura principale dell'organizzazione.
- Crea o aggiunge due account condivisi nell'unità organizzativa di sicurezza: l'account Log Archive e l'account Audit.
- 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 la gestione OUs 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 [Account di archiviazione dei log](#).

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 di audit](#).

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 dalla AWS Control Tower APIs. 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 (SCPs) e policy di controllo delle risorse (RCPs). I controlli investigativi sono implementati con AWS Config delle 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 rassegna di alcuni termini che vedrai nella documentazione di AWS Control Tower.

Innanzitutto, è bene 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 sulle organizzazioni e OUs, consulta la [AWS Organizations terminologia e i 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 su cui scalare i carichi di lavoro. AWS AWS Control Tower si affida AWS Organizations alla creazione di account, all'applicazione di controlli preventivi a livello di unità organizzative e alla fatturazione centralizzata.
- Un [AWS account Account Factory](#) è un AWS account fornito utilizzando Account Factory in AWS Control Tower. A volte, Account Factory viene definita informalmente come un «distributore automatico» per gli account.
- La tua [regione principale](#) di AWS Control Tower è la AWS regione in cui è stata distribuita la tua landing zone di AWS Control Tower. Puoi visualizzare la tua regione d'origine nelle impostazioni della landing zone.
- [AWS Service Catalog](#) consente di gestire centralmente i servizi IT più diffusi. Nel contesto di questo documento, Account Factory utilizza AWS Service Catalog per fornire nuovi AWS account, inclusi gli account provenienti da progetti personalizzati.
- [AWS CloudFormation StackSets](#) sono un tipo di risorsa che estende la funzionalità degli stack in modo da poter creare, aggiornare o eliminare gli stack su più account e regioni con un'unica operazione e un unico modello. CloudFormation
- Un'[istanza stack](#) è un riferimento a uno stack in un account di destinazione all'interno di una regione.
- Uno [stack](#) è una raccolta di AWS risorse che puoi gestire come singola unità.
- Un [aggregatore](#) è un tipo di AWS Config risorsa che raccoglie i dati di AWS Config configurazione e conformità da più account e regioni all'interno dell'organizzazione, consentendoti 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 all'interno

di 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 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, la linea di base chiamata `AWSControlTowerBaseline` è disponibile per aiutarti a registrarti OUs con AWS Control Tower. Durante la configurazione e l'aggiornamento della landing zone, l'obiettivo di base può essere un account condiviso o un'impostazione specifica per la landing zone nel suo insieme.
- Blueprint: un blueprint è un artefatto che incapsula alcuni metadati e descrive i componenti dell'infrastruttura che vengono 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.
- Risorsa non conforme: 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 configuri la landing zone: l'account di gestione, l'account di archiviazione dei log e l'account di audit. Puoi 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 registrati e non registrati:
 - I controlli preventivi attivati sull'unità organizzativa (o ereditati da) si applicano a tutti gli account al suo interno, compresi quelli non registrati. Ciò è vero perché i controlli preventivi vengono applicati mediante RCPS o politiche dichiarative a livello di unità organizzativa, non a livello di account. SCPs Per ulteriori informazioni, consulta [Inheritance for service control policies](#) nella documentazione. AWS Organizations
 - I controlli Detective abilitati sull'unità organizzativa non si applicano agli account non registrati.
 - I controlli proattivi sono implementati tramite hook. 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 mediante 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 vengono implementati con SCPs. I controlli investigativi sono implementati con AWS Config regole. 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. APIs In precedenza si chiamava Control Library. Abbiamo allineato la terminologia al nome del namespace, controlcatalog.
- **Zona di atterraggio:** una 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.
- **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, consulta la panoramica sull'[ontologia](#) di Control Catalog.
- **Unità organizzativa annidata:** un'unità organizzativa nidificata in AWS Control Tower è un'unità organizzativa contenuta all'interno di 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. Annidato: OUs crea una gerarchia. Quando si associa una politica a uno degli elementi della OUs gerarchia, questa viene spostata verso il basso e ha effetto su tutti gli account OUs 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 molti figli OUs.
- **Gerarchia delle unità organizzative:** in AWS Control Tower, la gerarchia di nested OUs può avere fino a cinque livelli. L'ordine di nidificazione è denominato Livelli. La parte superiore della gerarchia è designata come Livello 1.

- **Unità organizzativa di primo livello:** un'unità organizzativa di primo livello è qualsiasi unità organizzativa che si trova direttamente sotto la radice, non la radice stessa. La radice 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 dall'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 governata:** le regioni che mostrano lo stato Non governato non sono controllate o monitorate da AWS Control Tower. Di Regioni AWS solito non rispettano le stesse politiche di governance applicate da AWS Control Tower. Puoi creare risorse in queste regioni, ma tali risorse non sono protette dai controlli di AWS Control Tower.
- **Negata:** una regione negata viene bloccata specificamente da AWS Control Tower. All'interno del tuo ambiente AWS Control Tower, non puoi 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 per i AWS servizi abilitati da AWS Control Tower e i servizi che usi nella tua landing zone. Ad esempio, paghi per Service Catalog per il provisioning degli account con Account Factory e AWS CloudTrail per gli eventi monitorati nella tua landing zone. Per informazioni sui prezzi e le tariffe 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 notare 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 ulteriori informazioni 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 addebiti duplicati, se opti anche per 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 aderire durante la configurazione o l'aggiornamento della landing zone, AWS Control Tower configura e attiva un CloudTrail percorso a livello di organizzazione per te 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

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.

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

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

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

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

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Accedere come utente root](#) nella Guida per l'utente di Accedi ad AWS .

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

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

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

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

2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

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

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

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

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

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

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

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

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 per configurare la tua landing zone utilizzando la console AWS Control Tower oppure APIs.

Se AWS al momento sei un cliente, ma non conosci AWS Control Tower, prima di procedere [Pianifica la tua landing zone di AWS Control Tower](#), ti consigliamo di consultare la sezione chiamata.

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 APIs](#)
- [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 landing zone](#).

Note

AWS Control Tower configura servizi a pagamento AWS CloudTrail AWS Config, come Amazon CloudWatch, Amazon S3 e Amazon VPC. [Se utilizzi, questi servizi possono comportare costi, come mostrato 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

tui 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 una tantum sono elencate nella sezione chiamata [Aspettative per la configurazione delle landing zone](#).

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 Configura landing zone.
5. Segui le istruzioni nella console, accettando tutti i valori predefiniti. Dovrai digitare l'indirizzo e-mail del tuo account, un account di archiviazione dei log e un account di controllo.
6. Conferma le tue scelte e scegli Configura landing zone.
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 di configurare la landing zone, AWS Control Tower esegue automaticamente una serie di controlli pre-lancio sul 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 tua landing zone. Ecco i controlli che AWS Control Tower esegue prima di configurare una landing zone:

- I limiti di servizio esistenti per il Account AWS devono essere sufficienti per il lancio di AWS Control Tower. Per ulteriori informazioni, consulta [Limitazioni e quote in AWS Control Tower](#).
- Account AWS Devono essere abbonati 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 i clienti AWS IAM Identity Center (IAM Identity Center)

- Se AWS IAM Identity Center (IAM Identity Center) è già configurato, la regione principale di AWS Control Tower deve essere la stessa della regione IAM Identity Center.
- IAM Identity Center può essere installato solo nell'account di gestione di un'organizzazione.
- Alla directory IAM Identity Center si applicano tre opzioni, 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 (IdP) esterno, 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 dal tuo IdP esterno in Account Factory durante la creazione dell'account e AWS Control Tower consente a questo utente di accedere all'account appena fornito 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 assegni utenti a questi gruppi, questi utenti avranno accesso ai tuoi account registrati.

Per ulteriori informazioni sull'utilizzo di IAM Identity Center e AWS Control Tower, consulta [Cose da sapere sugli account IAM Identity Center e AWS Control Tower](#)

Considerazioni per AWS Config e clienti AWS CloudTrail

- L'accesso attendibile Account AWS non può essere abilitato nell'account di gestione dell'organizzazione per AWS Config. Per informazioni su come disabilitare l'accesso affidabile, consulta [la AWS Organizations documentazione su come abilitare o disabilitare l'accesso affidabile](#).
- Se disponi di un AWS Config registratore, un canale di distribuzione o una configurazione di aggregazione 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 la configurazione della landing zone. Questo controllo preliminare non si applica all'account

di gestione AWS Control Tower durante il lancio della landing zone. Per ulteriori informazioni, consulta [Registrazione account che dispongono di risorse esistenti AWS Config](#).

- Se esegui carichi di lavoro temporanei da account in AWS Control Tower, potresti notare un aumento dei costi associati a Config. AWS Contatta il rappresentante del tuo AWS 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 hai già una distribuzione di un CloudTrail trail nell'account, potresti riscontrare addebiti duplicati, a meno che non elimini il trail 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 di soli controlli senza implementare una landing zone 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 framework di conformità associati e i metadati di controllo. Per abilitare

questa esperienza su AWS Control Tower, seleziona Ho un ambiente esistente e voglio abilitare i controlli gestiti da AWS 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 trasferiti da una all'altra. OUs

Considerazioni su AWS Config

È possibile abilitarla 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 specificazione dei periodi di conservazione dei log di Amazon S3 per la registrazione.

Processo di implementazione

Se si procede senza procedere 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 attivare AWS Config la registrazione mentre il nuovo controllo ConfigBaseline viene abilitato sull'obiettivo OUs. Si tratta di una procedura di configurazione unica per unità organizzativa e prevede AWS Config prezzi basati sul numero di account per unità organizzativa e di risorse per account, per regione AWS.

Note importanti

La creazione di un ambiente AWS Control Tower stabilisce una relazione di fiducia con AWS Organizations, abilita il rilevamento delle deviazioni per i controlli preventivi e il monitoraggio delle modifiche all'account e all'unità organizzativa. Durante la configurazione, AWS Control Tower crea una configurazione di landing zone che funge da base per l'ambiente di controllo gestito.

Per creare il tuo ambiente dedicato ai controlli tramite, APIs consulta: [Inizia a usare AWS Control Tower utilizzando APIs](#) Nota che il campo manifest è ora opzionale con la landing zone 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 per configurare la tua landing zone 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 non conosci AWS Control Tower, prima di procedere [Pianifica la tua landing zone di AWS Control Tower](#), ti consigliamo di consultare la sezione chiamata.

Argomenti

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

Aspettative per la configurazione delle 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. 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 configurato la landing zone. Per impostazione predefinita, i livelli superiori OUs sono denominati 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, puoi facoltativamente specificare AWS account esistenti per AWS Control Tower da utilizzare come account di controllo e 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. (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.
- Facoltativamente, puoi specificare un blueprint 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 disponi di un blueprint disponibile. Per informazioni, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

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 Account Factory con VPCs, il CIDRs VPC non può essere modificato dopo la loro creazione.

Passaggio 1: crea gli indirizzi email del tuo account condiviso

Se stai configurando la tua landing zone in una nuova Account AWS, consulta [Configurazione](#).

- Per configurare la tua landing zone con nuovi account condivisi, AWS Control Tower richiede due indirizzi e-mail 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 account di sicurezza e archiviazione dei log esistenti in AWS Control Tower, puoi inserire gli indirizzi e-mail correnti degli AWS account esistenti.

Gli indirizzi e-mail sono necessari per:

- Account di audit: questo account è per il 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 devono accedere a tutte le informazioni di registrazione di tutti gli account registrati OUs all'interno della tua landing zone.

Questi account vengono configurati nella Security OU quando crei la landing zone. Come best practice, quando esegui azioni in questi account, ti consigliamo di utilizzare un utente IAM Identity Center con le autorizzazioni appropriate.

Note

Se specifichi 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 landing zone potrebbe non avere successo. 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: log archive e audit. Mentre leggi questo documento, ricordati di sostituire inizialmente i nomi personalizzati che dai a questi account, se scegli di personalizzarli. Puoi visualizzare i tuoi account con i loro nomi personalizzati nella pagina dei dettagli dell'account.

Note

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

Passaggio 2. Configura e avvia la tua landing zone

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

Important

La modifica della regione di residenza dopo aver implementato la landing zone di AWS Control Tower richiede la disattivazione e l'assistenza di Support. AWS Questa pratica non è consigliata.

Scopri come configurare e avviare la tua landing zone utilizzando AWS CLI in [Inizia a usare AWS Control Tower utilizzando APIs](#).

Per configurare e avviare la landing zone 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 di residenza desiderata per AWS Control Tower. Quindi scegli Configura la tua landing zone.

Fase 2a. Controlla e seleziona le tue AWS regioni

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

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

Per selezionare altre AWS regioni da governare

1. Il pannello mostra le attuali selezioni 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 passare alla governance da parte di AWS Control Tower. La selezione della tua 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 nega il controllo. Per impostazione predefinita, l'impostazione per questo controllo è **Non abilitata**.

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

Se ne accetti i nomi predefiniti OUs, non devi intraprendere alcuna azione per continuare la configurazione. Per modificare i nomi di OUs, inserisci i nuovi nomi direttamente nel campo del modulo.

- **Unità organizzativa fondamentale:** AWS Control Tower si basa su un'unità organizzativa di base 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 archivio dei registri** e **account di controllo**.
- **Unità organizzative aggiuntive:** AWS Control Tower può configurare una o più unità organizzative aggiuntive OUs per te. 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, si consiglia di denominarla **Sandbox OU**, come indicato nella [Linee guida per configurare un ambiente ben progettato](#). Se disponi già di un'unità organizzativa esistente in 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 landing zone. Non spostate o eliminate questi account condivisi. È possibile scegliere nomi personalizzati per gli account di controllo e di archiviazione dei registri durante la configurazione. In alternativa, è disponibile un'unica opzione per specificare AWS gli account esistenti come account condivisi.

È necessario fornire indirizzi e-mail univoci per l'archivio dei registri 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 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 landing zone. Non è possibile creare account separati per la fatturazione e per le autorizzazioni di amministratore in AWS Control Tower.

L'indirizzo e-mail mostrato per l'account di gestione non è modificabile durante questa fase di configurazione. Viene visualizzato come conferma, in modo da poter verificare che si stia modificando l'account di gestione corretto, nel caso in cui si disponga di 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 di fare in modo che AWS Control Tower crei nuovi account condivisi per te, gli indirizzi e-mail 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 chiamato inizialmente 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 chiamato inizialmente account di controllo. Molti clienti scelgono di chiamarlo account di sicurezza.
4. Fornisci un indirizzo email univoco per questo account.

Configura facoltativamente la conservazione dei registri

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 aggiorni o ripristini la landing zone.

Facoltativamente, gestisci automaticamente l'accesso Account AWS

Puoi scegliere se AWS Control Tower configurare Account AWS l'accesso con AWS Identity and Access Management (IAM) o se gestirlo automaticamente Account AWS , con utenti, ruoli e autorizzazioni di AWS IAM Identity Center che puoi configurare e personalizzare da solo, o con un altro metodo come un IdP esterno, per la federazione diretta degli account o la federazione su 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 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 alle normative in settori o paesi specifici o Regioni AWS laddove AWS IAM Identity Center non è disponibile.

La selezione di provider di identità a livello di account non è supportata. Questa opzione si applica solo alla landing zone nel suo insieme.

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

Configura facoltativamente i percorsi AWS CloudTrail

Come procedura consigliata, si consiglia 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 Opt in. Se desideri gestire la registrazione con i tuoi CloudTrail percorsi o 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 landing zone.

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

Configurare facoltativamente 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 landing zone.

Quando selezioni Set up landing zone, AWS Control Tower esegue un controllo preliminare per convalidare la tua chiave KMS. La chiave deve soddisfare questi requisiti:

- Abilitato
- Simmetria
- Non è una chiave multiregionale
- Alla politica sono state aggiunte le autorizzazioni corrette
- 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 di autorizzazione della chiave, come descritto nella sezione successiva.

Aggiorna la politica delle chiavi KMS

Prima di poter aggiornare una politica delle chiavi 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 aggiorni una policy chiave KMS, puoi 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 istruzioni di policy che consentono AWS Config e utilizzano 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 configurato AWS Control Tower.
- **YOUR-HOME-REGION**— la regione di residenza che selezionerai durante la configurazione di AWS Control Tower.
- **YOUR-KMS-KEY-ID**— l'ID della chiave KMS che verrà utilizzata con la policy.

Per aggiornare la politica delle chiavi KMS

1. Apri la AWS KMS console all'indirizzo <https://console.aws.amazon.com//kms>
2. Dal riquadro di navigazione, scegli Customer managed keys.

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:aws: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:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
    }
  },
}
```

```

    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/*"
    }
  }
}

```

6. Scegli **Save changes** (Salva modifiche).

Esempio di politica chiave KMS

La seguente politica di esempio mostra come potrebbe apparire la politica delle chiavi KMS dopo aver aggiunto le dichiarazioni di policy che concedono e le autorizzazioni AWS Config minime CloudTrail richieste. La politica di esempio non include la politica delle chiavi 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 altre politiche di esempio, consulta le seguenti pagine:

- [Concessione delle autorizzazioni di crittografia nella Guida](#) per l'AWS CloudTrail utente.
- [Autorizzazioni richieste per la chiave KMS \(quando si utilizza il servizio Role3 Bucket Delivery\) nella Guida](#) per gli sviluppatori.AWS Config

Proteggiti dagli aggressori

Aggiungendo determinate condizioni alle politiche, è possibile contribuire a prevenire un tipo specifico di attacco, noto come attacco secondario confuso, che si verifica se un'entità costringe un'entità con più privilegi a eseguire un'azione, ad esempio con l'impersonificazione tra servizi diversi. 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 multiregione e chiavi asimmetriche; tuttavia, AWS Control Tower non supporta chiavi multiregione 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 ulteriori informazioni in merito 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.

Configurare facoltativamente la registrazione automatica per gli account

Quando abiliti questa funzionalità durante la configurazione o successivamente, gli account che vengono spostati tra due account registrati OUs o spostati nel tuo ambiente AWS Control Tower per la prima volta, non mostrano più uno stato di deriva ereditaria. Gli account ereditano automaticamente le linee di base e i controlli abilitati sulla nuova unità organizzativa. I controlli e le linee di base dell'unità organizzativa precedente vengono rimossi.

Per attivare la registrazione automatica in qualsiasi momento dopo la configurazione, vai alla pagina delle impostazioni della landing zone e scegli Update landing zone o chiama l'API AWS Control Tower. `UpdateLandingZone`

Puoi spostare un account OUs da un account all'altro 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. In sostanza annulla la registrazione dell'account da AWS Control Tower.

Note

Se scegli di abilitare la funzionalità di registrazione automatica dopo la configurazione iniziale della landing zone, AWS Control Tower non risolve retroattivamente la deriva ereditaria causata dallo spostamento di account da un'altra OUs prima che la funzionalità di registrazione automatica fosse abilitata. La risoluzione automatica della deriva entra in vigore per gli account che vengono spostati dopo aver abilitato questa impostazione.

Facoltativamente, configura e crea account utente personalizzati

Quando segui il flusso di lavoro Crea account per aggiungere i tuoi account membro, puoi facoltativamente specificare un blueprint 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 disponi di un blueprint disponibile. Per informazioni, consulta [Personalizza gli account con Account Factory Customization \(AFC\)](#).

Fase 3. Rivedi e configura la landing zone

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

Per finalizzare

1. Sulla console, esamina 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 landing zone**.

Questa serie di passaggi avvia il processo di configurazione della landing zone, che può richiedere circa trenta minuti per essere completato. Durante la configurazione, AWS Control Tower crea il livello di 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 e-mail di AWS notifica e conferma dell'abbonamento da ogni AWS regione supportata 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 APIs

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

In questa procedura, APIs utilizzerai AWS Control Tower e altri AWS servizi per configurare e avviare una landing zone. Questi APIs 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 della landing zone con APIs](#)
- [Fase 1: Configura la tua landing zone](#)
- [Fase 2: Avvia la landing zone utilizzando AWS Control Tower APIs](#)
- [Identifica la tua landing zone](#)
- [Aggiorna la tua landing zone](#)
- [Reimposta la landing zone per risolvere la deriva](#)
- [Visualizza i dettagli del file manifest della tua landing zone](#)
- [Visualizza lo stato delle operazioni nelle tue landing zone](#)
- [Esempi: configura una landing zone di AWS Control Tower APIs solo con](#)
- [Schemi delle zone di atterraggio](#)
- [Avvia una landing zone usando CloudFormation](#)

Aspettative per la configurazione della landing zone con APIs

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, i Foundational OUs sono denominati 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 APIs, 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 VPCs, il CIDRs VPC non può essere modificato dopo la loro creazione.

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

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 la landing zone di AWS Control Tower APIs, devi prima chiamare APIs da 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 richieste per chiamare la landing zone APIs.

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 uno o più componenti aggiuntivi OUs. 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 la landing zone APIs 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 Organizations APIs. 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](#)

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 landing zone APIs. 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 AWS Control Tower APIs

Puoi usare AWS Control Tower APIs 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)
- L'account IDs deve essere valido a 12 cifre AWS . IDs
- La chiave KMS ARNs deve essere una chiave valida. AWS KMS ARNs
- 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-44XXXXXXXXXX"
```

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. ARNs
Le zone di atterraggio sono uniche a livello regionale.

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

Per [le regioni opt-in](#), l'`ListLandingZonesAPI` 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'`UpdateLandingZoneAPI` 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'`GetLandingZoneOperationAPI` 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
```

Esempio di `LandingZoneManifest file.json`, 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/
e84XXXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
    },
    "enabled": true
  },
  "securityRoles": {
    "accountId": "SECURITY ACCOUNT ID"
  },
  "accessManagement": {
    "enabled": true
  }
}
```

Output:

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


-  Facoltativamente, registrare nuovamente l'unità organizzativa per aggiornare gli account
- Per le AWS Control Tower registrate OUs con meno di 1000 account, puoi utilizzare la console AWS Control Tower, accedere alla pagina OU nella dashboard e selezionare Re-register OU 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 (OUs), 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 utilizzi l'ultima versione di landing zone disponibile. Puoi chiamare l'GetLandingZoneAPI e confrontare la versione della tua landing zone con l'ultima versione disponibile. Se necessario, puoi fare [Aggiorna la tua landing zone](#) in modo che la tua landing zone utilizzi l'ultima versione disponibile. In questi esempi, utilizziamo la versione 3.3 come versione più recente.

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 manifest della tua landing zone

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

Per vedere un esempio completo di schema di landing zone, vedi [Schemi delle zone di atterraggio](#).

Regioni governate: regioni da sottoporre a governance

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

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

Struttura organizzativa: seleziona i nomi della sicurezza e della sandbox OUs da creare nell'organizzazione

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

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

CentralizedLogging — Configurazione per AWS CloudTrail

- Tipo: oggetto
- Obbligatorio: sì
- Proprietà:
 - AccountId - a rappresenta String l' AWS account in cui deve essere distribuita la risorsa di registrazione
 - configurazioni: un uomo con tre proprietà Object
 - loggingBucket- un oggetto con una proprietàretentionDays, che richiede un Number
 - accessLoggingBucket- un oggetto con una proprietàretentionDays, che richiede un Number
 - kmsKeyArn- un opzionale String
 - abilitato: un opzionale Boolean
- 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
}
```

```
}
```

SecurityRoles: scegli dove distribuire la risorsa di registrazione

- Tipo: oggetto
- Obbligatorio: sì
- Proprietà: accountId - un String che rappresenta l' AWS account in cui deve essere distribuita la risorsa di registrazione
- Esempio:

```
"securityRoles": {  
    "accountId": "333333333333"  
}
```

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: un uomo Object con tre proprietà
 - centralBackup- un oggetto con una proprietàaccountId, che richiede un String
 - backupAdmin- un oggetto con una proprietàaccountId, che richiede 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
}
```

Visualizza lo stato delle operazioni nelle tue landing zone

L'`ListLandingZoneOperationsAPI` consente di visualizzare lo stato delle operazioni di AWS Control Tower che eseguono azioni sulla landing zone.

Per ulteriori informazioni su questo funzionamento dell'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_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0Vfmj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4Hs1NtPE8-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_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0Vfmj1wdl4J2nwnHI-

```

UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB021ihD4Mdcbm3SJg
 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 APIs solo con

Questa guida dettagliata 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 obbligatori.

```
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. Crea un account IDs e genera il file manifest delle landing zone.

I primi due comandi dell'esempio seguente memorizzano l'account IDs per gli account creati nel passaggio 1 in variabili. Queste variabili aiutano quindi a generare il file manifest delle landing zone.

```

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 landing zone con l'ultima versione.

È necessario configurare la landing zone 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 landing zone 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"  
  }  
}
```

È possibile utilizzare il seguente script di esempio per configurare un ciclo, 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 landing zone

Fase 1: Trova l'ARN della landing zone

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

L'output includerà l'identificatore della landing zone, 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/4B3H0ULNUOL2AXXX
```

Ecco un esempio del tipo di output che potresti vedere:

```
{
  "landingZone": {
    "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "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'**ListLandingZoneOperations**API per visualizzare lo stato di tutte le operazioni che modificano la tua landing zone.

Per monitorare lo stato di qualsiasi operazione di landing zone, puoi chiamare l'[ListLandingZoneOperations](#)API.

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 [Landing zone 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 APIs through 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: Array
    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 landing zone è configurata, 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 di 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 [Governare](#) le organizzazioni e gli account esistenti.
- Gli utenti finali possono effettuare il provisioning AWS dei propri account nella landing zone utilizzando Account Factory. Per ulteriori informazioni, consulta [Autorizzazioni per la configurazione e il provisioning degli account](#).
- Per garantire la sicurezza [Convalida della conformità per AWS Control Tower](#), gli amministratori cloud centrali possono esaminare gli archivi di log nell'account Log Archive e i revisori di terze parti designati possono esaminare le informazioni di controllo nell'account Audit (condiviso), che fa parte dell'unità organizzativa di sicurezza.
- Per ulteriori informazioni sulle funzionalità di AWS Control Tower, consulta [Informazioni correlate](#).
- Di tanto in tanto, potrebbe essere necessario aggiornare la landing zone per ottenere gli ultimi aggiornamenti del backend, i controlli più recenti e mantenere la landing zone up-to-date. 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'MFA per l'utente root del tuo account, fallo ora. Per ulteriori informazioni sulle migliori pratiche per l'utente root, consulta [Procedure ottimali per proteggere l'utente root dell'account](#).

Limitazioni e quote in AWS Control Tower

Questo capitolo descrive le limitazioni e le quote del AWS servizio da tenere a mente quando usi AWS Control Tower. Se non riesci a configurare la landing zone 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 ai controlli

Informazioni dettagliate sui controlli di 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 dei limiti complessivi in termini di concorrenza. In generale, è consentita un'operazione alla volta. Sono consentite due eccezioni a questa limitazione:
 - I controlli opzionali possono essere attivati e disattivati contemporaneamente, tramite un processo asincrono. In totale, possono essere in corso fino a cento (100) operazioni relative al controllo alla volta, indipendentemente dal fatto che vengano richiamate dalla console o da un'API.
 - Gli account possono essere forniti, aggiornati e registrati contemporaneamente in Account Factory, tramite un processo asincrono, con un massimo di cinque (5) operazioni relative agli account in corso contemporaneamente. La cancellazione degli account deve essere eseguita un account alla volta.
- Account Factory for Terraform (AFT) dispone di parametri di concorrenza aggiuntivi configurati durante la distribuzione. AWS ha testato AFT con questi valori predefiniti:
 - `concurrent_account_factory_actions`: 5 (fornitura di 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 landing zone per visualizzare queste modifiche nella console AWS Control Tower.
- OUs Nella landing zone di AWS Control Tower si applica un limite di cinque (5) SCPs per unità organizzativa.
- AWS Control Tower supporta fino a 10.000 account nell'organizzazione della tua landing zone, suddivisi tra tutti i tuoi OUs.
- Gli account esistenti OUs con oltre 1000 account annidati direttamente non possono essere registrati o registrati nuovamente in AWS Control Tower. Per ulteriori informazioni sulle limitazioni relative alla registrazione OUs, consulta. [Limitazioni basate sui servizi sottostanti AWS](#)
- 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

Puoi distribuire e gestire risorse in queste regioni con cFCT, se distribuisce cFCT nella tua regione di origine 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 versioni Regioni AWS, poiché 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

- AWS Control Tower Account Factory for Terraform (AFT) non può essere distribuito dai nuovi clienti AFT nelle seguenti regioni, perché non AWS CodeConnections è disponibile per la connessione a un sistema di controllo della versione (VCS) di terze parti:
 - Asia Pacifico (Hong Kong), Africa (Città del Capo), Medio Oriente (Bahrein), Europa (Zurigo), Asia Pacifico (Giacarta), Asia Pacifico (Hyderabad), Asia Pacifico (Osaka), Asia Pacifico (Melbourne), Israele (Tel Aviv), Europa (Spagna), Medio Oriente (Emirati Arabi Uniti), Asia Pacifico (Thailandia), Messico (Centrale)
- Le seguenti regioni non supportano. AWS Service Catalog
 - Canada occidentale (Calgary), ca-west-1
 - Asia Pacifico (Malesia), ap-sutheast-5
 - Asia Pacifico (Tailandia), ap-southeast-7
 - Messico (Centrale), mx-central-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 lo supportano AWS Service Catalog, consulta [AWS Control Tower disponibile nel AWS Canada occidentale \(Calgary\)](#).

- Quando si richiama un'API di controllo per attivare o disattivare un controllo, il limite per `DisableControl` gli aggiornamenti `EnableControl` e gli aggiornamenti in AWS Control Tower è di cento (100) operazioni simultanee. È possibile eseguire dieci operazioni (10) contemporaneamente, con le operazioni rimanenti 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. È possibile 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 al valore predefinito di 10 account.

Le seguenti quote possono essere visualizzate tramite la console Service Quotas

- Quota di operazioni simultanee sull'account: il numero massimo di operazioni simultanee sull'account che possono essere eseguite contemporaneamente. Impostazione predefinita: 5, massima: 10, regolabile
- Numero di account in una singola unità organizzativa: il numero massimo di account gestiti AWS Control Tower che possono essere presenti in un'unica 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 sui servizi sottostanti AWS](#) di AWS Control Tower. Impostazione predefinita: 1000, non regolabile.
- Operazioni simultanee per le unità organizzative (OUs): il numero massimo di operazioni simultanee relative all'unità organizzativa che possono essere eseguite contemporaneamente. Impostazione predefinita: 1, non regolabile.

Ad esempio, puoi richiedere un aumento della quota da cinque a un massimo di dieci operazioni simultanee relative all'account. Alcune caratteristiche prestazionali di AWS Control Tower possono cambiare dopo un aumento della quota. Ad esempio, potrebbe essere necessario più tempo per aggiornare un'unità organizzativa quando sono presenti più account. In alternativa, il completamento di un'azione su un'unità organizzativa con cinque unità potrebbe richiedere più tempo SCPs rispetto a tre SCPs.

 Note

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

In alternativa, puoi contattare [AWS Support](#) 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 al supporto Enterprise per la tua 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.

[Video dettagliato sugli aumenti delle quote in AWS Control Tower.](#)

Quando effettui il provisioning di nuovi account in questo ambiente, puoi utilizzare gli eventi del ciclo di vita per attivare richieste automatiche di aumenti delle quote di servizio, se necessario. Regioni AWS

[Ulteriori informazioni sulle AWS quote sono disponibili nella Guida generale.AWS](#)

Limitazioni di controllo

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

 La guida di riferimento ai controlli

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

Se modifichi le risorse di AWS Control Tower, ad esempio un SCP, o rimuovi qualsiasi AWS Config risorsa, come un registratore o un aggregatore di Config, AWS Control Tower non può più garantire che i controlli funzionino come previsto. Pertanto, la sicurezza del tuo ambiente multi-account potrebbe essere compromessa. Il [modello di sicurezza a responsabilità AWS condivisa](#) è applicabile a tutte le modifiche apportate dall'utente.

Note

AWS Control Tower aiuta a mantenere l'integrità dell'ambiente ripristinando i SCPs controlli preventivi alla loro configurazione standard quando aggiorni la landing zone. Le modifiche che potresti aver apportato SCPs vengono sostituite dalla versione standard del controllo, in base alla progettazione.

Limitazioni per regione

Alcuni controlli in AWS Control Tower non funzionano in alcune aree in Regioni AWS cui è disponibile AWS Control Tower, perché tali regioni non supportano le funzionalità sottostanti richieste. Di conseguenza, quando distribuisce quel controllo, potrebbe non funzionare in tutte le regioni governate con AWS Control Tower. Questa limitazione riguarda alcuni controlli investigativi, alcuni controlli proattivi e determinati controlli nel Security Hub CSPM Service-managed Standard: AWS Control Tower. Per ulteriori informazioni sulla disponibilità regionale, consulta i [controlli del Security Hub](#). Vedi anche la documentazione dell'[elenco dei servizi regionali e la documentazione di riferimento dei controlli CSPM di Security Hub](#).

Il comportamento di controllo è inoltre limitato 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 i limiti delle regioni e dei controlli, consulta [Considerazioni sull'attivazione delle regioni opt-in AWS](#).

Note

Per le informazioni più aggiornate sui controlli e sul supporto regionale, ti consigliamo di chiamare le operazioni [GetControle](#) e le [ListControlsAPI](#).

Trova i controlli e le regioni disponibili

Puoi visualizzare le regioni disponibili per ogni controllo nella console AWS Control Tower. Puoi visualizzare le regioni disponibili a livello di codice con [GetControlle](#) e [ListControls](#) APIs da AWS Control Catalog.

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

Limitazioni basate sui servizi sottostanti AWS

Questa pagina descrive le limitazioni che potresti incontrare a causa delle limitazioni di altri AWS servizi e come 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 sulla tua unità organizzativa sono abilitati più o meno controlli, i limiti degli account per unità organizzativa saranno diversi al momento della registrazione.

- Con 15 regioni governate, OUs sono supportati fino a 1000 account.
- Con 16 e 21 regioni governate, la dimensione massima delle unità organizzative supportate è compresa tra 600 e 1000 account.
- Con 22 regioni governate, sono OUs supportati fino a 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 a registrare nuovamente l'unità organizzativa. Inoltre, è possibile ridurre le dimensioni dell'unità organizzativa utilizzando un'unità organizzativa annidata o spostando gli account su 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 limiti dello stack set

Se prevedi di registrare un numero elevato di account su più account Regioni AWS, potresti riscontrare dei limiti creati dai set di CloudFormation stack sulla dimensione complessiva 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 regolate 15 regioni e sono abilitati 15 controlli opzionali, il limite per la registrazione dell'unità organizzativa è di 1000 account. Tuttavia, se è necessario registrarsi OUs con più di 1000 account o se è abilitato un gran numero di controlli opzionali, è necessario 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 registrarti OUs con un numero elevato di account, potresti incontrare dei limiti [al numero massimo di account che AWS Config puoi creare o eliminare ogni settimana](#), in tutti gli aggregatori. Gli account registrati non rientrano in questo limite: puoi registrare fino a 1000 nuovi account in AWS Control Tower ogni settimana.

Limitazioni introdotte per la prima volta per gli account e le regioni opt-in

Se prevedi di registrarti per la prima volta OUs con un gran numero di account in più regioni che hanno aderito all'iniziativa, potresti riscontrare delle limitazioni dovute alle [quote di gestione degli account](#), che possono portare a una latenza prolungata. È possibile che si verifichino errori durante la registrazione delle unità organizzative a causa della latenza.

Differenze regionali per la funzionalità di AWS Control Tower

Esistono alcune differenze nel comportamento di AWS Control Tower tra di loro Regioni AWS, poiché AWS Control Tower orchestra il comportamento di altri AWS servizi. Esempio:

- AWS Service Catalog non è disponibile in tutte le Regioni AWS ovunque sia 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 completamente disponibili in tutte le Regioni AWS causa della mancanza di funzionalità di base.
- AFT e cFCT non sono completamente disponibili in tutte le 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 ulteriori dettagli, consulta [Limitazioni e quote in AWS Control Tower](#).

- È AWS Service Catalog disponibile nella regione di residenza desiderata?
- Sono disponibili i controlli di cui hai bisogno? Vedi [Limitazioni del 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 chiamando `and.ListControls.GetControl` APIs. 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 governate dalla tua 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. Ma una volta 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 che distribuisce e le regioni in cui gestisci i carichi di lavoro in AWS Control Tower, in modo da non riscontrare lacune nella protezione delle tue 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 puoi distribuire il controllo in modo efficace, non le regioni non distribuibili.

La guida di riferimento ai controlli di AWS Control Tower

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 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 delle policy basate su IAM e 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 (SCPs), politiche di controllo delle risorse (RCPs) o politiche dichiarative. In confronto, un controllo investigativo ti informa di vari eventi o stati esistenti, mediante regole definite AWS Config .

Alcuni dei vostri utenti, come gli AWS sviluppatori, potrebbero aver bisogno di conoscere i controlli preventivi che si applicano a tutti gli account e che OUs 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 nella tua landing zone e almeno un AWS IAM Identity Center 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. Dalla tabella, scegli il nome di uno dei controlli OUs 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 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 non esistenti AWS Organizations OUs e agli account.

Note

Se disponi già di una AWS Organizations landing zone, puoi estendere la governance di AWS Control Tower dalla landing zone esistente ad alcuni o a tutti i tuoi account esistenti OUs e 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 a OUs e 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 gli account OUs e all'interno dell'organizzazione esistente.

Informazioni su Extending Governance: l'estensione della governance si applica a account specifici OUs e 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 allo specifico OUs e agli account 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 OUs creazioni all'interno AWS Organizations rimangono invariate, perché non sono registrate con AWS Control Tower. Puoi continuare a utilizzare quelli OUs 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 altri account OUs 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 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 (OUs) 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 (OUs)
- 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 tra loro, 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 (OUs), a fini di governance e controllo. OUs sono progettati per gestire l'applicazione delle politiche su più account.

Il nostro consiglio è di creare almeno un ambiente di riproduzione (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 account separati e fatturati come OUs account separati. Inoltre, potresti voler configurare un'unità organizzativa Sandbox per il test del codice.

Usa una struttura ben pianificata per la OUs tua landing zone

AWS Control Tower ne configura alcuni OUs automaticamente. 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 la tua OUs 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, la Security OU, ti consigliamo di crearne altre OUs 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 al posto tuo durante la creazione di landing zone, se la selezioni.

Altre due unità organizzative OUs consigliate possono essere configurate 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, denominata Workloads OU. Puoi aggiungerne altri OUs nella tua landing zone tramite la console AWS Control Tower nella pagina Unità organizzative.

Consigliato OUs oltre a quelli configurati 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 [Production starter organization with AWS Control Tower](#).

Esempio di AWS Control Tower con una struttura di unità organizzativa multi-account completa

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.

Puoi anche creare una struttura di unità organizzativa più semplice e piatta che funzioni bene e sia in linea con le AWS linee guida per più account. Il fatto che sia possibile creare una struttura di unità organizzative gerarchica non significa che sia necessario farlo.

- Per visualizzare un diagramma che mostra un set di esempi OUs in un ambiente AWS Control Tower espanso e piatto con indicazioni per AWS più account, consulta [Esempio: carichi di lavoro in una struttura di unità organizzativa piatta](#).
- Per ulteriori informazioni su come AWS Control Tower funziona con strutture di unità organizzative annidate, consulta [Annidato OUs in AWS Control Tower](#).
- Per ulteriori informazioni su come AWS Control Tower si allinea alle AWS linee guida, consulta il AWS white paper [Organizing Your AWS Environment Using Multiple Accounts](#).

Il diagramma nella pagina collegata mostra che OUs sono stati creati più elementi fondamentali OUs e altri aggiuntivi. Questi OUs soddisfano le esigenze aggiuntive di un'implementazione più ampia.

Nella OUs colonna Foundational, due OUs sono state aggiunte alla struttura di base:

- Security_Prod OU: fornisce un'area di sola lettura per le politiche di sicurezza, nonché un'area di controllo di sicurezza infrangibile.
- Infrastructure OU: è possibile separare l'unità organizzativa dell'infrastruttura, consigliata in precedenza, in due OUs, Infrastructure_Test (per l'infrastruttura di preproduzione) e Infrastructure_Prod (per l'infrastruttura di produzione).

Nell' OUs area Aggiuntiva, ne sono state aggiunte molte altre alla struttura di base. OUs I seguenti sono i seguenti che consigliamo OUs di creare man mano che l'ambiente cresce:

- Workload OU: l'unità organizzativa Workloads, consigliata in precedenza ma facoltativa, è stata suddivisa in due OUs, Workloads_Test (per carichi di lavoro di preproduzione) e Workloads_Prod (per carichi di lavoro di produzione).
- PolicyStaging OU: consente agli amministratori di sistema di testare le modifiche apportate ai controlli e alle politiche prima di applicarle completamente.
- Unità organizzativa sospesa: offre un'ubicazione per gli account che potrebbero essere stati temporaneamente disabilitati.

Informazioni sul Root

The Root non è un'unità organizzativa. È un contenitore per l'account di gestione e per tutti OUs gli account dell'organizzazione. Concettualmente, il Root contiene tutti i. OUs 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 del tuo. OUs [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 [Etichettatura di controllo di AWS Control Tower APIs](#).
- 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 su VPCs

- 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](#)

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.
- I ruoli collegati ai servizi vengono mantenuti in tutte le versioni di landing zone e non vengono più eliminati quando OUs diventano «non registrati»
- I ruoli collegati ai servizi possono essere eliminati manualmente dai clienti solo dopo la disattivazione della landing zone

- Prerequisito 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 anziché la politica in linea esistente. `AWSControlTowerCloudTrailRolePolicy` [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 alle unità organizzative di sicurezza e agli account di integrazione. 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.
- Notifiche di drift: AWS Control Tower interromperà l'invio di notifiche di drift all'argomento SNS per tutti i clienti sulla landing zone 4.0 senza l'`AWSControlTowerBaseline` opzione abilitata e inizierà invece a inviare notifiche di drift all'account EventBridge di gestione. [Per esaminare esempi di eventi e linee guida su come ricevere notifiche di drift EventBridge, consulta questa guida.](#)

- 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 opzionalmente richiesti 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:
 - CentralConfigBaselinepuò essere disabilitato solo se CentralSecurityRolesBaselineIdentityCenterBaseline, BackupAdminBaseline e le BackupCentralVaultBaseline linee di base vengono disabilitate per prime.
 - CentralSecurityRolesBaselinepuò essere disabilitato solo se IdentityCenterBaseline BackupAdminBaseline e le BackupCentralVaultBaseline linee di base vengono disabilitate per prime.
 - IdentityCenterBaselinepuò essere disabilitato indipendentemente.
 - BackupAdminBaselinee le BackupCentralVaultBaseline linee di base possono essere disabilitate indipendentemente
 - LogArchiveBaselinepuò essere disabilitato indipendentemente

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 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 [Registrazione account che dispongono di risorse esistenti AWS Config](#).
- 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 () verranno eliminati. `aws-controltower-GuardRailsComplianceAggregator`
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": "*"
}
]
}

```

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 l'accesso per AWS Config la gestione dei controlli investigativi. SCPs

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. Le risorse non conformi possono 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. Se lo fai, non sarai in grado di registrare questi account con AWS Control Tower o registrare il loro genitore OUs diretto.
- Non impedire l'utilizzo Regioni AWS tramite SCPs o AWS Security Token Service (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. SCPs 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 sugli account e OUs

- 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 di nuova registrazione dell'unità organizzativa 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 account 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 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 aggiornare le policy di controllo del servizio esistenti (SCPs) collegate a un'unità organizzativa registrata con AWS Control Tower. In questo modo i controlli potrebbero entrare in uno stato sconosciuto, che richiederà la reimpostazione della landing zone o la registrazione nuovamente dell'unità organizzativa in AWS Control Tower. Puoi invece utilizzarli AWS Organizations per crearne di nuovi SCPs e collegarli a quelli creati da AWS Control Tower OUs anziché modificare SCPs quelli creati da AWS Control Tower.
- Lo spostamento di singoli account già registrati in AWS Control Tower, dall'esterno di un'unità organizzativa registrata, causa deviazioni che devono essere risolte. Per informazioni, 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 tutti OUs nella console AWS Control Tower, anche se non sono autorizzati a recuperarli direttamente. 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. SCPs 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.

Per interrompere AWS IAM Identity Center in AWS Control Tower o iniziare a utilizzare AWS IAM Identity Center

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 AWS IAM Identity Center i clienti nella sezione Controlli pre-lancio](#) 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](#).
- [Utilizzo di 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. AWSControl TowerBaseline Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare ResetEnabledBaseline e attivare EnabledBaselines e ResetEnabledControl APIs EnabledControls attivare l'unità organizzativa per registrare gli account. Per i dettagli di, vedere:. AWSControl TowerBaseline [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 [Nessun errore trovato nei percorsi di avvio](#) la [sezione Risoluzione dei problemi](#) della AWS Control Tower User Guide.

Note

È possibile effettuare il provisioning di fino a cinque account alla volta.

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 drift 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. 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.](#)

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 delle chiavi 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 avanzati
- 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 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 ai tuoi account di carico di lavoro o. OUs 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 della landing zone di AWS Control Tower, nonché eventuali modifiche apportate alle policy di controllo del servizio (SCPs), 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 azioni SCPs non di proprietà di AWS Control Tower non `AWSControlTowerExecution` impediscano al ruolo di eseguire azioni negli account dei membri o azioni nell'account di gestione per il ruolo amministrativo che esegue l'aggiornamento.

Servizi basati sull'intelligenza artificiale e AWS Control Tower

È possibile creare politiche di controllo dei servizi (SCPs) che consentono di disattivare l'archiviazione dei dati da parte dei servizi basati sull'intelligenza artificiale. AWS Queste politiche SCP specificano che i servizi basati sull'intelligenza artificiale, come Amazon Rekognition o CodeWhisperer Amazon, non possono archiviare e utilizzare i tuoi dati per migliorare altri servizi basati sull'intelligenza artificiale. 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](#).

Quando aggiorni la landing zone, hai la possibilità di cancellare le mappature AWS dell'Identity Center (precedentemente chiamate AWS SSO) non utilizzate. 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 essere aggiornati anche 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 nel tuo account registrato OUs. 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 OUs un numero di account pari o inferiore a 1000, è possibile scegliere **Registra nuovamente l'unità organizzativa** per aggiornare tutti gli account all'interno dell'unità organizzativa e ripetere il comando **Re-register OU** 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 in <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, registra nuovamente OU per aggiornare gli account

Per le AWS Control Tower registrate OUs con meno di 1000 account, puoi andare alla pagina dell'unità organizzativa nella dashboard e selezionare Registra nuovamente l'unità organizzativa 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 AWS Control Tower APIs.

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 aver aggiornato la landing zone, potresti dover aggiornare i tuoi account. Il modo più semplice per aggiornare l'account consiste nel ripetere la procedura di registrazione OU per ciascuno dei tuoi utenti registrati OUs.

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 one-to-one mappatura 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 and 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 ti SCPs 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 di registrare nuovamente 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 la deriva in una versione con landing zone, sono possibili due comportamenti.

- Se utilizzi la versione più recente della landing zone, quando scegli Reset e poi scegli Confirm, le risorse della tua drifted landing zone vengono ripristinate alla configurazione AWS Control Tower salvata. La versione landing zone rimane la stessa.

- Se non utilizzi la versione più recente, devi scegliere Aggiorna. La landing zone viene aggiornata alla versione più recente della landing zone. La deriva viene risolta come parte di questo processo.

Esegui il provisioning 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 AWSControl TowerBaseline abilitato. Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare ResetEnabledBaseline e attivare EnabledBaselines e ResetEnabledControl APIs EnabledControls attivare l'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControl TowerBaseline [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 in AWS Control Tower by Service Catalog APIs](#).

 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:

- [Utilizzare AWS CloudShell per lavorare con 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 del controllo e l'audit. Puoi configurare queste azioni automatizzate con chiamate a:

- [AWS Service Catalog APIs](#)
- [AWS Organizations APIs](#)
- [AWS Control Tower APIs](#)
- [la AWS CLI](#)

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 seguenti forniscono collegamenti alle aree di questa AWS Control Tower User Guide che possono aiutarti ad automatizzare le attività.

Automatizzazione delle attività di controllo

Puoi 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'[API di riferimento di AWS Control Tower](#).

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

Automatizzazione delle attività relative alle landing zone

La landing zone di AWS Control Tower ti APIs aiuta ad automatizzare determinate attività relative alla tua landing zone. Per i dettagli, consulta l'[API di riferimento di AWS Control Tower](#).

Automatizzazione della registrazione delle unità organizzative

La baseline di AWS Control Tower ti APIs aiuta ad automatizzare determinate attività, come la registrazione di un'unità organizzativa. Per i dettagli, consulta l'[API di riferimento di AWS Control Tower](#).

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 [Chiudere un account membro AWS Control Tower tramite AWS Organizations](#).

Fornitura 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 puoi creare nuovi account e aggiornarli 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 [Esegui il provisioning degli account con AWS Control Tower Account Factory for Terraform \(AFT\)](#).

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, politiche di controllo dei servizi (SCPs) e politiche di controllo delle risorse (). RCPs Per ulteriori informazioni, consulta [Panoramica sulle personalizzazioni per AWS Control Tower \(cFCT\)](#).

Per ulteriori informazioni e un video sul provisioning automatico degli account, consulta la [procedura dettagliata: Provisioning automatizzato degli account in AWS Control Tower e Provisioning automatizzato](#) con ruoli IAM.

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

Controllo programmatico 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](#).

Automatizzazione di altre attività

Per informazioni su come aumentare determinate quote del servizio AWS Control Tower con un metodo di richiesta automatizzato, guarda questo video: [Automate Service Limit](#) Acrees.

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

Sono disponibili due esempi open source GitHub per aiutarti con determinate attività di automazione relative 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 best practice di sicurezza utilizzando Step Functions, durante il provisioning e la configurazione di nuovi account. Questo esempio include l'aggiunta di principi ai AWS Service Catalog portafogli condivisi a livello organizzativo e l'associazione automatica di gruppi IAM Identity Center a livello di organizzazione a nuovi account. 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 with AWS CloudShell, un AWS servizio che semplifica l'utilizzo della AWS CLI, [AWS CloudShell consulta e la AWS CLI](#).

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

Utilizzare AWS CloudShell per lavorare con 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 AWS Control Tower altri AWS servizi e utilizzerai la AWS CLI versione 2, preinstallata nell'ambiente di calcolo 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 autorizzazioni di accesso agli utenti IAM e agli utenti di IAM Identity Center. 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 allegata alle identità IAM:

- `AWSCloudShellFullAccess`: concede l'autorizzazione all'uso AWS CloudShell con accesso completo a tutte le funzionalità.

Se desideri limitare l'ambito di azioni che 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 l'autorizzazione a 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 avviarlo 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 necessari per lavorare. AWS Control Tower Ad esempio, puoi controllare il tuo AWS Config stato.

Interagisci con AWS Control Tower AWS CloudShell

Dopo l'avvio AWS CloudShell da Console di gestione AWS, puoi iniziare immediatamente a interagire 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 è necessario configurare le credenziali prima di effettuare chiamate.

Usalo AWS CloudShell per facilitare la configurazione AWS Control Tower

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 Identity Center o utente IAM con autorizzazioni amministrative per l'account di gestione che contiene la tua landing zone.

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

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-records`
 - La risposta normale è qualcosa del genere "name": "default"
2. Se disponi di un AWS Config registratore o di un canale di distribuzione esistente che devi eliminare prima di configurare la AWS Control Tower landing zone, 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 l'ingresso in uno stato incoerente.

Per ulteriori informazioni, consulta la documentazione AWS Config

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

-

[Gestione del Canale di Distribuzione](#)

3. Questo esempio mostra i comandi AWS CLI da cui inserire 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, questo è solo un esempio. Tuttavia, potrebbe essere necessario abilitare o disabilitare l'accesso affidabile per altri AWS servizi se si stanno automatizzando o personalizzando le azioni in. AWS Control Tower

Esempio: abilitare o disabilitare l'accesso affidabile ai servizi

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

Esempio: creare un bucket Amazon S3 con AWS CloudShell

Nell'esempio seguente, puoi utilizzare AWS CloudShell per creare un bucket Amazon S3 e quindi utilizzare il PutObjectmetodo 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 rispettate [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 dell' CreateBucket operazione: Il bucket specificato non è valido.

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

```
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 visualizza una risposta dal servizio simile al seguente output:

```
{
  "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebee56\""
}
```

ETagÈ l'hash dell'oggetto che è stato archiviato. Può essere usato 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 consente di modellare e configurare le AWS risorse in modo da 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 fornisce e configura tali risorse per te.

Quando si utilizza CloudFormation, è possibile riutilizzare il modello per configurare le AWS Control Tower risorse in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS regioni.

AWS Control Tower e CloudFormation modelli

Per fornire 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 che desideri fornire negli CloudFormation stack. Se non conosci JSON o YAML, puoi usare CloudFormation Designer per iniziare a usare i modelli. CloudFormation Per ulteriori informazioni, consulta [Che cos'è CloudFormation Designer?](#) nella Guida per l'utente di AWS CloudFormation .

AWS Control Tower supporta la creazione di `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` e `DisableControl` gli aggiornamenti AWS Control Tower è di 100 operazioni simultanee.

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

Scopri di più su CloudFormation

Per ulteriori informazioni 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 landing zone di AWS Control Tower sono configurabili nella console, come la selezione di regioni e controlli opzionali. Altre modifiche possono essere apportate all'esterno della console, con automazione.

Ad esempio, puoi creare personalizzazioni più ampie della tua landing zone con la funzionalità Customizations for AWS Control Tower, un framework di personalizzazione in GitOps stile che funziona con AWS CloudFormation modelli ed eventi del ciclo di vita di AWS Control Tower.

Personalizzazione dalla console AWS Control Tower

Per apportare queste personalizzazioni alla tua landing zone, 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 il tuo OUs in qualsiasi momento utilizzando la AWS Organizations console, ma apportare modifiche al tuo OUs in AWS Organizations potrebbe causare problemi riparabili.](#)
- È possibile selezionare i nomi degli account condivisi di Audit e Log Archive, ma non è possibile modificare i nomi dopo la configurazione. (Questa è una selezione una tantum).

Suggerimento

Ricorda che la ridenominazione di un'unità organizzativa AWS Organizations non aggiorna il prodotto fornito corrispondente in Account Factory. Per aggiornare automaticamente il prodotto fornito (ed evitare deviazioni), è necessario eseguire l'operazione dell'unità organizzativa tramite AWS Control Tower, inclusa la creazione, l'eliminazione o la registrazione di un'unità organizzativa.

Seleziona regioni AWS

- Puoi personalizzare la tua landing zone selezionando AWS regioni specifiche per la governance. Segui i passaggi nella console AWS Control Tower.

- Puoi selezionare e deselectare AWS le regioni per la governance quando aggiorni la landing zone.
- 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 su Regioni AWS dove cFct presenta limitazioni di implementazione, vedere.

[Limitazioni di controllo](#)

Personalizza aggiungendo controlli opzionali

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

Personalizza i tuoi percorsi AWS CloudTrail

- Quando aggiorni la tua landing zone 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 tua landing zone. AWS Control Tower crea un percorso a livello di organizzazione nel tuo account di gestione e tale percorso passa allo stato attivo o inattivo, in base alla tua scelta. Landing zone 3.0 non supporta 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 membri AWS Control Tower personalizzati e aggiornare gli account membro 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. Esempio:

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

[AFT viene distribuito con un modulo Terraform, disponibile nel repository AFT.](#)

- 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 policy di controllo dei servizi (SCPs). Puoi distribuire modelli e policy personalizzati su singoli account e unità organizzative (OUs) 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 con Landing Zone Accelerator (LZA) attivo. 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 landing zone di base e quindi di potenziare le funzionalità della landing zone con LZA, se necessario. Per ulteriori informazioni, consulta [AWS Control Tower and Landing zone Accelerator](#).

AWS Control Tower e acceleratore di zona di atterraggio

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

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

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

LZA configura automaticamente un ambiente cloud adatto per ospitare carichi di lavoro sicuri. Questa soluzione può essere implementata ovunque Regioni AWS, per aiutarvi a mantenere la coerenza delle operazioni e della governance. La soluzione LZA è progettata per allinearsi alle AWS migliori pratiche e per conformarsi a diversi framework di conformità globali.

Ti consigliamo di implementare AWS Control Tower come landing zone di base e quindi di potenziare le funzionalità della tua landing zone con LZA, se necessario. La combinazione di LZA e AWS Control Tower offre una soluzione completa e senza codice che aiuta a gestire e governare un ambiente multi-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 predisposizione della piattaforma, incluse sicurezza, conformità e capacità 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 denominato Customizations for AWS Control Tower (cFCT) ti aiuta a creare personalizzazioni per la tua landing zone più ampie di quelle che puoi creare nella console AWS Control Tower. Offre un processo automatizzato GitOps in stile. Puoi rimodellare la landing zone per soddisfare le tue esigenze aziendali.

Questo processo di infrastructure-as-code personalizzazione integra AWS CloudFormation modelli con le policy di controllo dei AWS servizi (SCPs) e [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 si crea 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 OUs la tua landing zone distribuendo risorse da te specificate.

Note

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

Vantaggi

- Espandi un AWS ambiente personalizzato e sicuro: puoi espandere il tuo ambiente AWS Control Tower multi-account più rapidamente e incorporare le AWS best practice in un flusso di lavoro di personalizzazione ripetibile.
- Crea un'istanza dei tuoi requisiti: puoi personalizzare la landing zone di AWS Control Tower in base alle tue esigenze aziendali, con AWS CloudFormation modelli e policy 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 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 agli account e, in modo automatico. OUs
- Estendi l'architettura di rete: puoi implementare architetture di rete personalizzate che migliorano e proteggono la connettività, come un gateway di transito.

Esempi cFCT aggiuntivi

- Un esempio di utilizzo del networking con Customizations for AWS Control Tower (cFCT) è fornito nel post del blog AWS Architecture, [Deploy consistent DNS with Service Catalog and AWS Control Tower](#) customizations.
- Un esempio specifico [relativo a cFCT e Amazon GuardDuty](#) è disponibile GitHub nel [aws-samplesrepository](#).
- [Ulteriori esempi di codice riguardanti 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, consultate 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 e politiche di controllo dei servizi (). SCPs

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 (OUs) all'interno dell'organizzazione.

Note

L'unità organizzativa (OU) di destinazione configurata in cFCT deve essere AWSControl TowerBaseline 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 file [ChangeLog.md](#) 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.

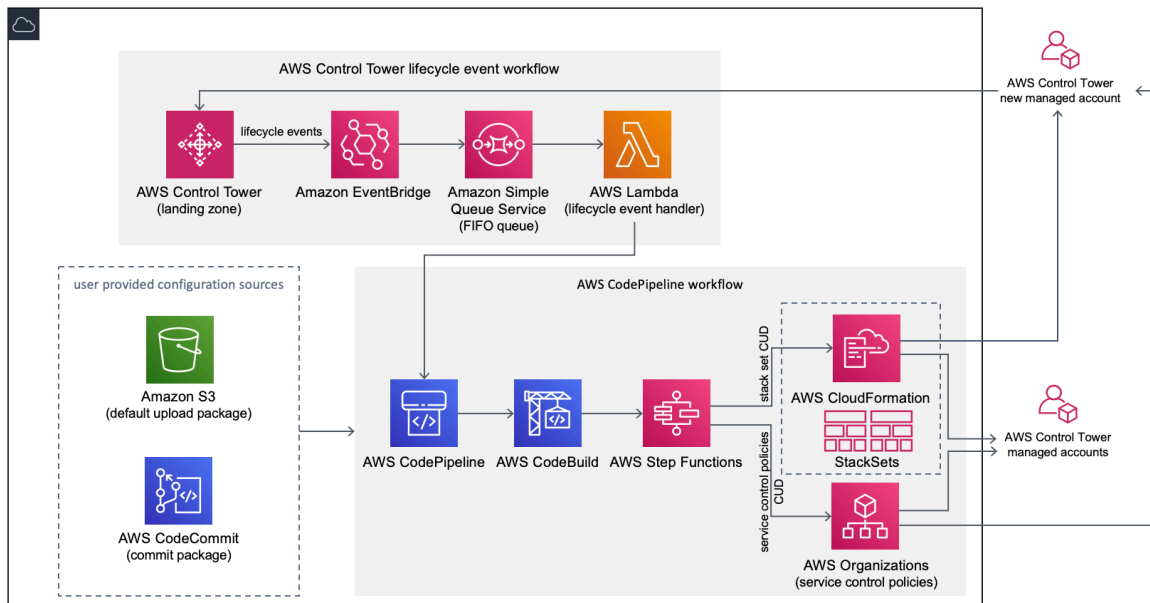


Figura 1: Personalizzazioni per l'architettura AWS Control Tower

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 del servizio (SCPs) e la [AWS CloudFormation StackSets](#) macchina a stati per distribuirle a livello di unità organizzativa o per distribuire SCPs istanze stack a livello di unità organizzativa o a livello 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 dell'organizzazione AWS CloudFormation StackSets e all'SCP interno di essa.

Quando caricate il pacchetto di configurazione, cFct richiama la pipeline di codice per eseguire tre 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'API per la AWS Organizations creazione. SCPs
- CloudFormation Stage: [richiama lo stack set state machine per distribuire le risorse specificate nell'elenco degli account o quelle fornite nel OUs file manifest](#).

In ogni fase, la pipeline di codice richiama le funzioni stack set e SCP step, che distribuiscono set di stack personalizzati e ai singoli account interessati o SCPs 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 set di stack e. SCPs

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

Il bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) AWS CodeCommit e le risorse del repository basato su Git 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 per i 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 origine per la tua pipeline, in alternativa ad Amazon S3.

In base al tuo input nel CloudFormation modello, cFct può creare un [AWS CodeCommit](#) repository con la stessa configurazione di esempio illustrata nella sezione Amazon Simple Storage Service.

[Per clonare il AWS CodeCommit repository cFCT sul tuo computer locale, devi creare credenziali che ti consentano l'accesso temporaneo al repository, come spiegato nella Guida per l'utente.](#)[AWS CodeCommit](#) [Per informazioni sulla compatibilità delle versioni, vedere Configurazione per.](#) [AWS CodeCommit](#)

 Note

Se non lo utilizzi 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 si distribuisce 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 [Utilizzo di Amazon S3 come sorgente di configurazione](#). La pipeline include fasi per convalidare e gestire i file e i modelli di configurazione, gli account principali, le politiche di controllo AWS Organizations del servizio e AWS CloudFormation StackSets Per ulteriori informazioni sulle fasi della pipeline, fare riferimento a [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 forniti 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 politica. 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 e la distribuzione iniziali AWS CloudFormation StackSets o AWS Organizations SCPs durante un evento del ciclo di vita di AWS Control Tower.

Amazon Simple Notification Service

cFct può pubblicare notifiche, come l'approvazione della pipeline, su 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 di cartelle necessaria. Questi esempi ti aiutano a sviluppare un pacchetto di configurazione per personalizzare la tua landing zone di AWS Control Tower. Il manifesto di esempio identifica le configurazioni richieste per i set di stack e le policy di controllo dei servizi (SCPs) di cui avrai bisogno per implementare le tue personalizzazioni.

È possibile utilizzare questo pacchetto di configurazione di esempio come modello per sviluppare e caricare il 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 Amazon Simple Queue Service (Amazon SQS) per acquisire gli eventi del ciclo di vita da Amazon. EventBridge Attiva una funzione, che richiama la distribuzione o AWS Lambda . AWS CodePipeline AWS CloudFormation StackSets SCPs Per ulteriori informazioni su, vedere. SCPs [AWS Organizations](#)

AWS Step Functions

CFct crea Step Functions per orchestrare le implementazioni di personalizzazione. Queste Step Functions traducono i file di configurazione per implementare le personalizzazioni necessarie in tutti gli ambienti.

AWS Archivio parametri Systems Manager

[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 ogni account per registrare AWS CloudTrail i dati in un bucket Amazon S3 centralizzato. Inoltre, Systems Manager Parameter Store offre 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 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, esamina i seguenti parametri e modificateli 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 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

Configurazione della pipeline		
Parametro	Predefinito	Descrizione
		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 Nome del repository	custom-control-tower-configuration	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 Configurazione AWS

Parametro	Predefinito	Descrizione
CodeCommit Nome del ramo	main	Il ramo Git in cui è archiviato il pacchetto di personalizzazione. Per utilizzare questo parametro, è necessario impostare il parametro CodePipeline Source su AWS CodeCommit.

CloudFormation StackSets Configurazione

Parametro	Predefinito	Descrizione
Tipo di concorrenza regionale	PARALLEL	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 SEQUENTIAL.
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 .

CloudFormation StackSets Configurazione		
Parametro	Predefinito	Descrizione
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 .

- Scegli Next (Successivo).
- Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
- 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.
- 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

Configura GitHub come origine di configurazione

Questa sezione spiega come distribuire personalizzazioni per AWS Control Tower (cFCT) utilizzando GitHub come sorgente. Il processo prevede tre fasi principali:

- Preparare un GitHub repository
- Crea la connessione di GitHub codice
- Distribuisci lo stack CloudFormation

Prepara 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 cFct](#) fornisce indicazioni dettagliate sulla creazione di un `manifest.yaml` file per configurare le personalizzazioni.

Crea la connessione GitHub

Dall'istanza Developer Tools --Connections per Github, esegui i seguenti passaggi:

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 un nome qualsiasi
3. Seleziona Connetti GitHub a, 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 repository, quindi seleziona il repository che hai creato in precedenza e Salva il tuo lavoro.
6. Nota l'ARN Code Connections: ti servirà per distribuire lo stack. CloudFormation

Distribuisci lo stack CloudFormation

- 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, fornire l'ARN di Code Connection
 - per GitHub Utente o Organizzazione, fornite il nome dell' GitHub utente o dell'organizzazione con cui avete creato il repository
 - Per GitHub Repository Name, inserisci il nome del repository (il valore predefinito è) `custom-control-tower-configuration`
 - Per GitHub Branch Name, inserisci il nome del ramo (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 rivolta 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 seguenti sezioni descrivono il processo in dettaglio.

Panoramica della pipeline del codice

Il pacchetto di configurazione richiede Amazon Simple Storage Service (Amazon S3) e AWS CodePipeline. Il pacchetto di configurazione contiene questi 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 utilizza questa impostazione predefinita. Se disponi di un AWS CodeCommit repository esistente, puoi cambiarne la posizione di origine. AWS

CodeCommit 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 utilizzare per personalizzare la tua landing zone. CodePipeline svolge queste attività:

- estrae il file manifest, il relativo set di modelli e altri file JSON
- esegue convalide di manifesti e modelli
- [richiama sezioni nel file manifest 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, il pacchetto 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. 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 di origine è la fase iniziale. Il pacchetto di configurazione personalizzato avvia questa fase della pipeline. L'origine di AWS CodePipeline può essere un bucket Amazon S3 o un AWS CodeCommit repository, in cui è possibile ospitare 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 `and. CloudFormation validate-template cfn_nag`. Se il file manifesto e i CloudFormation modelli superano i test, la pipeline passa alla fase successiva. Se i test falliscono, puoi esaminare CodeBuild i 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. Sospende la pipeline durante la distribuzione, fino a quando non viene fornita un'approvazione. Puoi attivare l'approvazione manuale modificando il parametro `Pipeline Approval Stage` su `Sì` all'avvio dello stack.

4. Fase politica

La fase della politica richiama la macchina a stati della policy di controllo dei servizi (SCP) o della politica di controllo delle risorse (RCP) per chiamare AWS Organizations APIs quella macchina a stati create o. SCPs RCPs

5. CloudFormation fase delle risorse

La fase CloudFormation delle risorse richiama lo stack set state machine per distribuire le risorse specificate nell'elenco degli account o delle unità organizzative (OUs), fornito nel file manifesto. La macchina a stati crea le CloudFormation risorse nell'ordine in cui sono specificate nel file manifesto. Per specificare una dipendenza dalle risorse, organizzate 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 manifesto `cFCT`, il set di modelli di accompagnamento e altri file JSON. Impacchetterai 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 storage di origine. Se scegli Amazon S3 come storage di origine, comprimi tutte le cartelle e i file in un file e carica solo il `custom-control-tower-configuration.zip` .zip file nel bucket Amazon S3 designato.

Note

Se lo utilizzi AWS CodeCommit, inserisci i file nel repository senza comprimerli.

Il file manifest 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 manifest 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 manifest specificano i valori della regione e le parole chiave della versione. Di seguito sono riportate le definizioni di tali parole chiave.

region: 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`, `oap-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 di AWS risorse, che verranno distribuite automaticamente dalla pipeline cFCT. Queste descrizioni delle risorse e dei relativi parametri disponibili sono fornite nella sezione successiva.

La sezione delle risorse del file manifesto cFCT

Questo argomento descrive la sezione risorse del file manifesto cFCT, in cui definirete le risorse necessarie per le personalizzazioni. Questa sezione del file manifesto cFct inizia con le parole chiave `resources` e continua fino alla fine del file.

La sezione `resources` del file manifesto specifica i CloudFormation StackSet o AWS Organizations SCPs and RCPs che cFCT distribuisce automaticamente tramite la pipeline del codice. È possibile elencare OUs, account e regioni per distribuire istanze stack.

Le istanze dello stack vengono distribuite a livello di account anziché a livello di unità organizzativa. SCPs e RCPs vengono distribuite a livello di unità organizzativa. Per ulteriori informazioni, consulta [Crea le tue personalizzazioni](#).

Il modello di esempio seguente 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 un set di stack.

- **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 manifest, un URI o URL di Amazon S3 che punta a un CloudFormation modello o a una politica di controllo del AWS Organizations servizio in JSON per la creazione di risorse, oppure CloudFormation SCPs RCPs

- **Tipo:** stringa
- **Obbligatorio:** sì

1. L'esempio seguente mostra `resource_file`, fornita 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 bucket policy consenta l'accesso in lettura per l'account di gestione AWS Control Tower da cui stai distribuendo cFCT. Se fornisci un URL HTTPS Amazon S3, verifica che il percorso utilizzi la notazione a punti. Ad esempio, `S3.us-west-1`. cFct non supporta endpoint che contengono un trattino tra S3 e la regione, ad esempio. `S3-us-west-2`

4. L'esempio seguente mostra una policy per i bucket di 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 ulteriori esempi, consulta gli [esempi di policy di Bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.

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 descrive la sezione dei parametri.

```
parameters:  
  - parameter_key: [String]  
    parameter_value: [String]
```

- parameter_key — La chiave associata al parametro.
 - Tipo: stringa
 - Obbligatorio: Sì (nella proprietà parameters)
 - Valori validi: a-z, A-Z e 0-9
- parameter_value — Il valore di input associato al parametro.
 - Tipo: stringa
 - Obbligatorio: Sì (nella proprietà parameters)

deploy_method — Il metodo di distribuzione per distribuire le risorse nell'account. Attualmente, deploy_method supporta la distribuzione di risorse utilizzando l'option stack_set per la distribuzione delle risorse tramite CloudFormation StackSets, l'option se si sta distribuendo o l'option scp se si sta distribuendo SCPs. rcp RCPs

- Tipo: stringa
- Valori validi: stack_set | scp | rcp
- Obbligatorio: sì

deployment_targets — Elenco di account o unità organizzative (OUs), in cui cFct distribuirà le risorse, specificate come account o organizational_units. CloudFormation

Note

Se si desidera implementare un SCP o RCP, la destinazione 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 di unità organizzative 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 si fornisce un'unità organizzativa che non contiene account e la proprietà `accounts` non viene aggiunta, cFct crea solo il set di stack.

Note

L'ID dell'account di gestione dell'organizzazione non è un valore consentito. Per impostazione predefinita, cFCT non supporta la distribuzione di istanze stack nell'account di gestione dell'organizzazione. [Se hai un caso d'uso speciale, vedi Root OU.](#)

`export_outputs` — Elenco di name/value coppie che denotano le chiavi dei parametri SSM. Queste chiavi dei parametri SSM consentono di memorizzare gli output dei modelli nell'archivio dei parametri SSM. L'output è destinato ad essere utilizzato come riferimento da altre risorse, definite in precedenza nel file manifest.

```
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 `[/org/member/audit/vpc_id]` variabile in cui `CfnOutput-Logical-ID` corrisponde alla variabile di output del modello. Per ulteriori informazioni sulla sezione Output di un CloudFormation modello, consulta [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.

- Tipo: 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 root

CFct supporta Root come valore per un'unità organizzativa (OU) `organizational_units` nella versione manifest V2 (2021-03-15).

- Se scegli il metodo di distribuzione `scp` o `orcp`, quando aggiungi Root `underorganizational_units`, AWS Control Tower applica le policy a tutti gli elementi OUs sotto Root. Se scegli il metodo di distribuzione `stack_set`, quando aggiungi Root

`underorganizational_units`, cFCT distribuisce gli stack set in tutti gli account sotto Root 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 AWS Control Tower.

In conformità alle linee guida sulle best practice, la distribuzione di AWS Control Tower colloca l'account di gestione nell'unità organizzativa principale, in modo che abbia accesso completo e non utilizzi 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 obiettivo 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, includi accounts come obiettivo di distribuzione e specifica l'account di gestione. Altrimenti, non includere gli account come obiettivo 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 aggiungerne nessun'altra. OUs

OU annidata

cFct supporta l'elenco di uno o più annidati OUs 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 due. OUs Per il metodo di distribuzione `scp` o `rcp`, AWS Control Tower distribuisce l'unità organizzativa SCPs o RCPs l'ultima unità organizzativa nel percorso dell'unità organizzativa annidata. Per quanto riguarda il metodo di distribuzione `stack_set`, AWS Control Tower distribuisce i set di stack 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 i set SCPs or RCPs to `OUname3` e stack solo su tutti gli account `OUname3` direttamente da,.

```
---
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 personalizzazioni personalizzate, è possibile modificare il `manifest.yaml` file cfCT aggiungendo o aggiornando le politiche di controllo del servizio (SCPs), le politiche di controllo delle risorse (RCPs) e le risorse. CloudFormation Per le risorse che devono essere distribuite, è possibile aggiungere o rimuovere account e. OUs È possibile aggiungere o modificare i modelli nelle

cartelle del pacchetto, creare cartelle personalizzate e fare riferimento ai modelli o alle cartelle del `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 dei servizi
- come configurare il proprio pacchetto di configurazione per i set di AWS CloudFormation stack

Imposta un pacchetto di configurazione per SCPs o RCPs

Questa sezione spiega come creare un pacchetto di configurazione per le politiche di controllo dei servizi (SCPs) o le politiche di controllo delle risorse (RCPs). Le due parti principali di questo processo sono (1) preparare il file manifest cFCT e (2) preparare la struttura delle cartelle.

Passaggio 1: modifica il file `manifest.yaml`

Usa il `manifest.yaml` file di esempio come punto di partenza. Immettete tutte le configurazioni necessarie. Aggiungi i `deployment_targets` dettagli `resource_file` e.

Il seguente frammento mostra il file manifesto predefinito.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

Il valore di `region` viene aggiunto automaticamente durante la distribuzione. Deve corrispondere alla regione in cui è stato distribuito cFCT. Questa regione deve essere la stessa della regione AWS Control Tower.

Per aggiungere un SCP o RCP personalizzato `example-configuration` nella cartella del pacchetto zip archiviato nel bucket Amazon S3, apri `example-manifest.yaml` il 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...

Il seguente frammento mostra un esempio di file manifest personalizzato. È possibile aggiungere più di una politica 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
```

Fase 2: Creare una struttura di cartelle

Puoi saltare questo passaggio se utilizzi un URL Amazon S3 per il file di risorse e utilizzi parametri key/value con coppie.

È necessario includere una policy SCP o una policy RCP in formato JSON per supportare il manifest, poiché il file manifest fa riferimento al file JSON. Assicuratevi che i percorsi dei file corrispondano alle informazioni sul percorso fornite nel file manifest.

- Un file JSON di policy contiene SCPs o RCPs su cui distribuire. OUs

Il seguente frammento mostra la struttura delle cartelle per il file manifest di esempio.

```
- manifest.yaml
- policies/
  - block-s3-public.json
```

Il seguente frammento 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:::*"
    }
  ]
}
```

Configurare 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 manifesto e (2) aggiornare la struttura delle cartelle.

Fase 1: Modificare il file manifesto esistente

Aggiungi le nuove CloudFormation StackSets informazioni al file manifesto che hai modificato in precedenza.

Solo a titolo di revisione, il seguente frammento contiene lo stesso file manifesto personalizzato mostrato in precedenza per impostare un pacchetto di configurazione per SCPs o. RCPs 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

```

Il frammento seguente mostra un file manifesto di esempio modificato che contiene i `resources` dettagli. L'ordine di `resources` determina l'ordine di esecuzione per la creazione `resources` delle dipendenze. 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 manifest.

```

---
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: Aggiornare la struttura delle cartelle

Quando aggiorni la struttura delle cartelle, puoi 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 OUs e gli 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'helper 'alfred' e i file dei parametri CloudFormation

cFct fornisce un meccanismo noto come alfred helper per ottenere il valore di una chiave [SSM Parameter Store](#) definita nel modello. CloudFormation Utilizzando l'helper alfred, è possibile utilizzare i valori archiviati 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'aiutante alfred ha due limitazioni. I parametri sono disponibili solo nella regione principale dell'account di gestione AWS Control Tower. Come best practice, prendi in considerazione l'utilizzo di valori che non cambiano da istanza stack a istanza stack. Quando l'helper 'alfred' recupera i parametri, sceglie un'istanza di stack casuale dal set di stack 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 VPC ID e subnet ID deve essere passato allo stack set 2 come valori dei parametri. Prima di *subnet ID* poter passare l'*VPC ID* and allo stack set 2, *subnet ID* deve essere archiviato nello stack set 1 utilizzando `VPC ID AWS::SSM::Parameter` Per ulteriori informazioni, consulta [AWS::SSM::Parameter](#) nella Guida per l'utente di CloudFormation .

CloudFormation set di pila 1:

Nel seguente frammento, l'helper alfred può ottenere il valore per VPC ID e 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 set di pila 2:

Lo snippet mostra i parametri specificati nel file CloudFormation stack 2. `manifest.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 set di pila 2.1:

Lo snippet mostra che è possibile elencare `alfred_ssm` le proprietà per supportare 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: $[alfred_ssm/stack_1/subnet/id']
  - parameter_key: AvailablityZones # Type: CommaDelimitedList
    parameter_value:
      - "$[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 sulla versione più recente di Customizations for AWS Control Tower (cFCT), consulta il [CHANGELOG.md](#) nel repository GitHub.

Warning

La versione 2.2.0 di Customizations for AWS Control Tower (cFCT) ha introdotto uno schema manifest cFCT (versione 2021-03-15) per allinearli al servizio correlato. AWS APIs. Lo schema manifest consente a un singolo file `manifest.yaml` di gestire le risorse supportate (modelli e) tramite flussi di lavoro disaccoppiati. CloudFormation SCPs RCPs DevOps. Ti consigliamo vivamente di aggiornare lo schema manifest cFCT dalla versione 2020-01-01 alla versione 2021-03-15 o successiva. cFct continua a supportare la versione 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 alla fine 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 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 cFCT

Quando si esegue l'aggiornamento alla versione dello schema manifesto cFCT 2021-03-15, ecco le modifiche che è necessario apportare per aggiornare i file. Le sezioni successive descrivono le modifiche obbligatorie e consigliate per la transizione.

Politiche di Organizations

1. Sposta la SCPs o RCPs in `organization_policies` nelle nuove risorse di proprietà.
2. Modificate la proprietà `policy_file` nella nuova proprietà `resource_file`.
3. Modificate `apply_to_accounts_in_ou` nella 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. Cambia `deploy_to_accounts` nella nuova proprietà `deployment_targets`. L'elenco degli account deve essere definito negli account delle proprietà secondarie.
5. Modificate la proprietà `ssm_parameters` nella nuova proprietà `export_outputs`.

Passaggi di aggiornamento cFCT altamente consigliati

CloudFormation parametri

1. Modificate la proprietà `parameter_file` con nuovi parametri di proprietà.
2. Rimuove il percorso del file nel valore della proprietà `parameter_file`.
3. Copiate la chiave del parametro e il valore del parametro dal file JSON del parametro 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 cFct 2021-03-15.

Rete in AWS Control Tower

AWS Control Tower fornisce supporto di base per il networking tramite VPCs.

Se la configurazione o le funzionalità predefinite del VPC AWS Control Tower non soddisfano le tue esigenze, puoi utilizzare altri AWS servizi per configurare il tuo VPC. Per ulteriori informazioni su come lavorare con VPCs AWS Control Tower, consulta [Creazione di un'infrastruttura di rete multi-VPC AWS scalabile e sicura](#).

Supporti IPv4 e IPv6 protocolli AWS Control Tower, tramite indirizzi IP dual-stack. Per ulteriori informazioni, consulta [Endpoint e quote di AWS Control Catalog e Endpoint e quote AWS Control Tower](#).

Argomenti correlati

- Per informazioni su come funziona AWS Control Tower quando registri account esistenti VPCs, consulta [Registra gli account esistenti con VPCs](#).
- Con Account Factory, puoi effettuare il provisioning di account che includono un VPC AWS Control Tower oppure puoi effettuare il provisioning di account senza un VPC. Per informazioni su come eliminare il VPC AWS Control Tower 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 dell'account VPCs, consulta la [documentazione di Account Factory](#) sull'aggiornamento di un account.
- Per ulteriori informazioni sull'utilizzo delle reti e VPCs su AWS Control Tower, consulta la sezione sulle [reti](#) nella pagina di informazioni correlate di questa Guida per l'utente.

VPCs 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 gestisci con AWS Control Tower. Questo VPC predefinito non è lo stesso di un VPC creato da AWS Control Tower per un account fornito, ma il AWS VPC 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 Region Deny Control, vai alla pagina delle impostazioni della zona di destinazione e seleziona Modifica impostazioni.

La Region deny control blocca le chiamate API verso la maggior parte dei servizi non governati. 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 l' AWS impostazione predefinita VPCs nelle regioni non governate. Per elencare il VPC predefinito in una regione puoi usare 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 VPCs

Ecco alcuni dati essenziali su AWS Control Tower VPCs:

- 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.
- Quando AWS Control Tower configura un nuovo account in una AWS regione supportata, AWS Control Tower elimina automaticamente il AWS VPC predefinito e configura un nuovo VPC configurato da AWS Control Tower.
- A ogni account AWS Control Tower è consentito un VPC creato da AWS Control Tower. Un account può averne altri AWS VPCs 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 VPCs, 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 un massimo di 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(non IPs al di fuori dell'192.168intervallo)

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 nessuna delle tue AWS Control Tower VPCs 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 VPCs utenti. Tuttavia, per impostazione predefinita, tutte le AWS Control Tower VPCs 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, puoi creare un account, quindi modificare l'intervallo CIDR e creare un nuovo account, e gli account VPCs allocati a questi due account possono essere sottoposti a 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 usarlo 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 dai richiedenti 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](#) nella AWS PrivateLink Guida.

AWS Control Tower supporta l'esecuzione di chiamate a tutte le sue 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 dell'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 per gli endpoint consente l'accesso completo a AWS Control Tower tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito ad AWS Control Tower dal tuo VPC, collega una policy personalizzata per gli 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 dell'API 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 [How AWS Control Tower aggrega AWS Config le regole negli account unmanaged and OUs](#).
- [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 su Account AWS 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 StackSet-AWSCo`n`trolTowerExecutionRole 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 `AWSControlTowerExecution` ruolo, indipendentemente dal fatto che sia stato creato manualmente o dalla stessa AWS Control Tower.

Scopo del ruolo: `AWSControlTowerExecution`

- `AWSControlTowerExecution` consente di creare e registrare account, automaticamente, con script e funzioni Lambda.
- `AWSControlTowerExecution` consente di configurare la registrazione delle organizzazioni, in modo che tutti i registri di ogni account vengano inviati all'account di registrazione.
- `AWSControlTowerExecution` consente di registrare un account individuale in AWS Control Tower. Innanzitutto, devi aggiungere il `AWSControlTowerExecution` ruolo a quell'account. Per istruzioni su come aggiungere il ruolo, consulta [Aggiungi manualmente il ruolo IAM richiesto a un ruolo esistente Account AWS e registralo](#).

Come funziona il `AWSControlTowerExecution` ruolo con OUs:

Il `AWSControlTowerExecution` 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.

In che modo AWS Control Tower aggrega AWS Config le regole negli account e negli account non gestiti OUs

- 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 `AWSControlTowerConfigAggregatorRoleForOrganizations`:

```
{
  "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: `AWSCloudFormationStackSetRoleForOrganizations` `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-AWSCoontrolTowerBP-BASELINE-ROLES` crea questi ruoli IAM solo programmatici e multiaccount nell'account di audit:

- `aws-controltower- AdministratorExecutionRole`
- `aws-controltower- ReadOnlyExecutionRole`

Lo stack AWS Control Tower `StackSet-AWSCoontrolTowerSecurityResources` 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: policy AWS gestita
2. AssumeRole-aws-controltower- AuditAdministratorRole — politica 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: policy AWS gestita
2. AssumeRole-aws-controltower- AuditReadOnlyRole — politica 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-AuditAdministratorRole

```
{
  "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`

JSON

```
{  
  "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:GetPeregrineStatus",  
        "sso:GetApplicationInstance",  
        "sso:ListDirectoryAssociations",  
        "sso:ListPermissionSets",  
        "sso:GetPermissionSet",  
        "sso:ProvisionApplicationInstanceForAWSAccount",  
      ]  
    }  
  ]  
}
```



```

        "sso:ProvisionApplicationProfileForAWSAccountInstance",
        "sso:ProvisionSAMLProvider",
        "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": "*"
}
]
}

```

Le autorizzazioni `sso:GetPeregrineStatus`, `sso:ProvisionApplicationInstanceForAWSAccount`, `sso:ProvisionApplicationProfileForAWSAccount` e `sso:ProvisionSAMLProvider` sono richieste da AWS Control Tower Account Factory per interagire con AWS IAM Identity Center.

Risorse in AWS Control Tower

- Per informazioni generali sulla proprietà delle risorse in AWS Control Tower, consulta [Panoramica della gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#).
- Per informazioni sulle risorse che AWS Control Tower crea negli account condivisi, consulta [Informazioni sugli account condivisi](#).
- 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 [AWS Control Tower APIs](#), consulta il [riferimento al tipo di risorsa AWS Control Tower](#) nella Guida per l'AWS CloudFormation utente.

Come funzionano AWS le regioni 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 d'origine

Quando crei una landing zone, la regione che utilizzi per accedere alla console di AWS gestione diventa la tua AWS regione di origine per AWS Control Tower. Durante il processo di creazione, alcune risorse vengono fornite nella regione di origine. Altre risorse, come OUs gli AWS account, sono globali.

Dopo aver selezionato una regione d'origine, non puoi cambiarla.

Controlli e regioni

Attualmente, tutti i controlli preventivi funzionano a livello globale. I controlli Detective e proattivi, tuttavia, funzionano solo nelle regioni in cui è supportato AWS Control Tower. Per ulteriori informazioni sul comportamento dei controlli quando attivi 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 tua landing zone di AWS Control Tower in una nuova AWS regione o rimuovi una regione dalla configurazione della tua landing zone. In genere, questa azione viene eseguita tramite la funzione Update della console AWS Control Tower.

Note

Ti consigliamo di evitare di espandere la landing zone di AWS Control Tower in AWS regioni in cui non è necessario eseguire i 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 landing zone, il che significa che definisce come base la tua landing zone:

- operare attivamente in tutte le nuove regioni selezionate, e
- cessare di amministrare le risorse nelle regioni deselezionate.

I singoli account all'interno delle unità organizzative (OUs) gestiti da AWS Control Tower non vengono aggiornati come parte di questo processo di aggiornamento delle landing zone. Pertanto, devi aggiornare i tuoi account registrando nuovamente i tuoi OUs

Durante la configurazione delle 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 landing zone per nuove regioni, i controlli investigativi di AWS Control Tower rispettano le seguenti regole:

- Ciò che esiste rimane uguale. Il comportamento di controllo, sia investigativo che preventivo, rimane invariato per gli account esistenti, nelle regioni esistenti e nelle OUs regioni esistenti.
- Non puoi applicare nuovi controlli investigativi agli account OUs contenenti account esistenti che non vengono aggiornati. Dopo aver configurato la landing zone di AWS Control Tower in una nuova regione (aggiornando la landing zone), devi aggiornare gli account esistenti in quella esistente OUs prima di poter abilitare nuovi controlli investigativi su quelle OUs e sugli account.
- I controlli investigativi esistenti iniziano a funzionare nelle nuove regioni configurate non appena aggiorni gli account. Quando aggiorni la landing zone di AWS Control Tower per configurare nuove regioni e quindi aggiorni un account, i controlli investigativi già abilitati sull'unità organizzativa inizieranno a funzionare su quell'account nelle nuove regioni configurate.

Configurazione delle regioni AWS Control Tower

1. Accedi alla console AWS Control Tower all'indirizzo <https://console.aws.amazon.com/controltower>
2. Nel menu di navigazione del riquadro a sinistra, scegli Impostazioni della zona di atterraggio.

3. Nella pagina delle impostazioni della zona di atterraggio, nella sezione Dettagli, scegli il pulsante Modifica impostazioni in alto a destra. Verrai indirizzato al flusso di lavoro di aggiornamento delle landing zone, poiché la gestione di nuove regioni o la rimozione delle regioni dalla governance richiedono l'aggiornamento alla versione più recente della landing zone.
4. In AWS Regioni aggiuntive per la governance, cerca le regioni che desideri governare (o smettere di governare). La colonna Stato indica quali regioni governi attualmente e quali no.
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 landing zone, registrati nuovamente OUs per aggiornare gli account nelle nuove regioni. Per ulteriori informazioni, consulta [Quando aggiornare AWS Control Tower OUs e gli account](#).

Un metodo alternativo per fornire o aggiornare i 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 [Esegui il provisioning 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 e dopo aver rimosso la governance di AWS Control Tower da una regione.

La governance mista è una situazione indesiderata che può verificarsi se i controlli che governano un'unità organizzativa non corrispondono completamente ai controlli che regolano 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 estende la governance a una nuova Regione AWS o la rimuove.

In questa situazione, alcuni account all'interno di un'unità organizzativa possono avere controlli diversi applicati in diverse regioni, rispetto ad altri account dell'unità organizzativa o rispetto alla posizione di governance generale della zona di destinazione.

In un'unità organizzativa con governance mista, se si effettua il provisioning di un nuovo account, tale nuovo account riceve la stessa regione (aggiornata) e la stessa posizione di governance dell'unità organizzativa della landing zone. Tuttavia, gli account esistenti che non sono ancora stati aggiornati non ricevono la posizione di governance aggiornata della regione.

In generale, una governance mista può creare indicatori di stato contraddittori o imprecisi nella console AWS Control Tower. Ad esempio, durante la governance mista, per gli account che non sono ancora stati aggiornati, le regioni che hanno scelto di aderire vengono mostrate con lo stato Non governato nella lista registrata OUs.

Note

AWS Control Tower non consente l'attivazione 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) nelle regioni che l'unità organizzativa già mostra come governate, poiché alcuni account nell'unità organizzativa non sono stati aggiornati. Potresti ricevere un messaggio di FAILED_TO_ENABLE errore.
- Durante la governance mista, se si estende la governance della zona di atterraggio a una regione che ha aderito all'iniziativa mentre uno degli account dell'unità organizzativa non è ancora stato aggiornato, il funzionamento dell'EnableControlAPI sull'unità organizzativa non riesce per i controlli investigativi e proattivi. Riceverai un messaggio FAILED_TO_ENABLE di errore, poiché gli account dei membri non aggiornati all'interno dell'unità organizzativa non sono ancora stati inseriti in tali regioni.
- Durante la governance mista, i controlli che fanno parte del Security Hub CSPM Service-managed Standard: AWS Control Tower non possono riportare la conformità in modo accurato nelle regioni in cui c'è una mancata corrispondenza tra la configurazione della landing zone e gli account che non vengono aggiornati.

- La governance mista non modifica il comportamento dei controlli basati su SCP (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 è la stessa cosa della deriva e non viene segnalata come deriva.

Riparare la governance mista

- I clienti sono ora in grado di riparare una 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 soggetta a una governance mista tramite un banner di avviso.

Considerazioni sull'attivazione delle regioni opt-in AWS

Sebbene la Regioni AWS maggior parte 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 opzionali. Al contrario, le regioni che sono attive per impostazione predefinita, non appena Account AWS vengono create, vengono chiamate regioni commerciali, regioni predefinite o semplicemente regioni.

Il termine opt-in ha una base storica. Tutte le Regioni AWS regioni introdotte dopo il 20 marzo 2019 vengono utilizzate come regioni opt-in. In una regione che prevede l'iscrizione, il tuo account non è abilitato all'interno di quella regione e la tua identità non viene replicata nella regione, a meno che tu non scelga di attivare l'uso di quella 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 firma X.509 o credenziali specifiche del contesto) e altre impostazioni a livello di account, come la politica delle password e l'alias dell'account.

Puoi attivare automaticamente le regioni opt-in durante la configurazione della landing zone, selezionandole. La tua landing zone 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 opzionale, attiva prima manualmente quella 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 (Giacarta), ap-southeast-3
- Regione Europa (Milano), eu-south-1
- Regione Africa (Città del Capo), af-south-1
- Regione del Medio Oriente (Bahrein), me-south-1
- Israele (Tel Aviv), il-central-1
- Regione del Medio Oriente (EAU), 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 del 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 distribuisce carichi di lavoro in regioni che richiedono l'adesione.

Governare o attivare?

Ricorda che governare 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 governare le Regioni che aderiscono all'iniziativa, ti consigliamo di non disattivare (disattivare) nessuna delle Regioni che aderiscono all'iniziativa, poiché ciò può comportare il fallimento dei tuoi 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 a AWS Control Tower, come la console di AWS fatturazione o l'SDK. AWS
- Quando AWS Control Tower estende la governance a una regione con consenso esplicito, attiva (opts-in) la regione in tutti gli account dei membri. Quando rimuovi una regione dalla governance, AWS Control Tower non disattiva (esclude) la regione negli account dei membri.
- Durante la deselezionazione della 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 AWS fatturazione o l'SDK. 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 landing zone viene disattivata, AWS Control Tower ripulisce le risorse in tutte le regioni governate, incluse le regioni opt-in. Tuttavia, AWS Control Tower non disattiva le regioni opt-in. Puoi disattivare le regioni opt-in come passaggio aggiuntivo dopo la disattivazione.
- Se la tua regione d'origine è una regione che accetta l'iscrizione 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 origine per la tua landing zone. Vedi [Abilitazione](#) di una regione.
- Se AWS Control Tower è configurato con una regione opt-in come regione di residenza e se accedi al servizio AWS Control Tower dalla AWS console in un'altra regione, la console non ti reindirizza automaticamente alla regione di origine.
- L'API sottostante ha 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, scegli solo quelle Regioni AWS in cui verranno eseguiti i carichi di lavoro e scegli una regione alla volta.

Limitazioni importanti per la governance e la contabilità

- Se sono regolamentate 16 o più regioni commerciali in cui è disponibile AWS Control Tower, incluse le regioni con adesione, 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](#).

Configura il Region Deny Control

AWS Control Tower offre due Region Deny Control. Un controllo `GRREGIONDENY`, quando attivato, si applica all'intera landing zone. Un altro controllo `CTMULTISERVICEPV1`, se attivato, può essere applicato a uno specifico OUs controllo specificato dall'utente. Per ulteriori informazioni, consulta [Negare l'accesso a in AWS base alla richiesta Regione AWS](#) e [Region Deny control applicato all'unità organizzativa](#).

Considerazioni sulla regione nega il controllo della landing zone

La Region Deney Control `GRREGIONDENY` è unica, perché si applica alla landing zone nel suo insieme, piuttosto che a una specifica UO. Per configurare il Region Deny Control, vai alla pagina delle impostazioni della zona di atterraggio e seleziona Modifica impostazioni.

- Questa impostazione può essere modificata in un secondo momento.
- Se abilitato, questo controllo si applica a tutti i registrati OUs.
- Questo controllo non può essere configurato per singoli utenti OUs.

Note

Prima di abilitare il Region Deny Control, assicurati di non disporre di risorse esistenti in queste aree, perché non avrai accesso alle tue risorse dopo aver applicato il controllo. Mentre il controllo è abilitato, non sarai in grado di distribuire risorse nelle regioni negate.

Quando si abilita il controllo, viene applicato a tutti i livelli superiori OUs registrati della gerarchia e viene ereditato dai livelli OUs inferiori della catena. Quando rimuovi il controllo, viene rimosso da tutte le regioni registrate OUs e non governate in AWS Control Tower che rimangono nello stato Non governato e puoi distribuire risorse in regioni al di fuori della disponibilità di AWS Control Tower.

Eccezioni

Non puoi negare l'accesso alla tua regione d'origine. Alcuni AWS servizi globali, come IAM e AWS Organizations, sono esenti dalla Region Deny Control. Per ulteriori informazioni, consulta [Negare l'accesso a in AWS base alla richiesta](#). Regione AWS

- Nome di controllo completo: nega l'accesso in AWS base alla regione richiesta AWS

- Descrizione del controllo: non consente l'accesso alle operazioni non elencate nei servizi globali e regionali al di fuori delle regioni specificate.
- Si tratta di un controllo elettivo con guida preventiva.

Per visualizzare il modello per Region deny control SCP, consulta [Deny access to in AWS base a quanto richiesto Regione AWS nel](#) riferimento AWS Control Tower Control. L'AWS Control Tower SCP è simile a [SCP for AWS Organizations](#), ma non è identico.

È possibile determinare gli endpoint dei servizi regionali nella pagina Servizi [regionali](#).

Considerazioni relative alla regione a livello di unità organizzativa negano il controllo

La considerazione principale sulla Region deny control a livello di unità organizzativa consiste nel determinare come interagirà con la landing zone Region deny control, se entrambe sono attivate. Per ulteriori informazioni, vedere [Region Deny Control](#) applicato all'unità organizzativa.

È inoltre possibile consultare [Configure the Region Deny](#) Control.

Informazioni su Account AWS 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'API `ProvisionProduct` di 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'API `CreateAccount` di AWS Organizations.

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: Audit) o di registrazione (nome predefinito: archivio log), AWS Control Tower verifica l'account per individuare eventuali 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 AWS Security Token Service (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](#)

Informazioni sugli account condivisi

Tre speciali Account AWS sono associati ad AWS Control Tower: l'account di gestione, l'account di audit e l'account di archiviazione dei log. Questi account vengono generalmente definiti account condivisi o talvolta account principali.

- Puoi selezionare nomi personalizzati per gli account di controllo e di archiviazione dei log 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 sicurezza o di registrazione esistente Account AWS come AWS Control Tower durante il processo di configurazione iniziale della landing zone. Questa opzione elimina la necessità per AWS Control Tower di creare nuovi account condivisi. (Questa è una selezione una tantum).

Per ulteriori informazioni sugli account condivisi e sulle risorse associate, consulta [Risorse create negli account condivisi](#).

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 condivisi](#).

Account di archiviazione dei log

L'account condiviso dell'archivio dei log viene configurato automaticamente quando crei la landing zone, se non utilizzi specificamente un altro AWS account.

Questo account contiene un bucket Amazon S3 centrale per l'archiviazione di una copia di tutti i file AWS CloudTrail e di AWS Config registro per tutti gli altri account nella tua landing zone. Come best practice, consigliamo di limitare l'accesso agli account di archiviazione dei log ai team responsabili della conformità e delle indagini e ai relativi strumenti di sicurezza o controllo. Questo account può essere utilizzato per controlli di sicurezza automatici o per ospitare funzioni personalizzate Regole di AWS Config, come le funzioni Lambda, per eseguire azioni correttive.

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 [Landing zone di AWS Control Tower versione 3.3](#).

Per ulteriori informazioni sui ruoli e le risorse disponibili nell'account di archiviazione dei log, consulta [Registra e archivia le risorse dell'account](#)

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 di audit

Questo account condiviso viene configurato automaticamente quando crei la landing zone, se non utilizzi specificamente un altro account.

L'account di audit dovrebbe essere riservato ai team di sicurezza e conformità con ruoli trasversali di auditor (sola lettura) e amministratore (accesso completo) a 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 di controllo riceve anche notifiche tramite il servizio Amazon Simple Notification Service (Amazon SNS). È possibile 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 OUs, gli utenti e nella tua SCPs landing zone. Per ulteriori informazioni sulla deriva, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Le notifiche di controllo che vengono 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 relative all'account di controllo 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 di controllo, vedere. [Controlla le risorse dell'account](#)

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 di audit riceve e-mail di AWS notifica - conferma della sottoscrizione da tutti quelli Regione AWS supportati da AWS Control Tower. Per ricevere e-mail di conformità nel tuo account di audit, devi scegliere il link di conferma dell'iscrizione all'interno di ogni e-mail di ciascuna e-mail Regione AWS supportata da AWS Control Tower.

Risorse create negli account condivisi

Questa sezione mostra le risorse che AWS Control Tower crea negli account condivisi, 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	audit
		log archive
AWS Organizations	OUs	Security
		Sandbox
AWS Organizations	Policy di controllo dei servizi	aws-guardrails-*
AWS CloudFormation	Stack	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER
		AWSControlTowerBP-BASELINE-CONFIG-MASTER(nella versione 2.6 e successive)
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Non distribuito nella versione 3.0 e successive)
		AWSControlTowerBP-BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)

Servizio AWS	Tipo di risorsa	Nome risorsa
		AWSControlTowerBP-BASELINE-CLOUDWATCH
		AWSControlTowerBP-BASELINE-CONFIG
		AWSControlTowerBP-BASELINE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-ROLES
		AWSControlTowerBP-SECURITY-TOPICS
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED
		AWSControlTowerLoggingResources
		AWSControlTowerSecurityResources
		AWSControlTowerExecutionRole
AWS Service Catalog	Prodotto	Account Factory di AWS Control Tower

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS Config	Aggregatore	aws-controltower-ConfigAggregatorForOrganizations
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
AWS IAM Identity Center	Gruppi di directory	AWSAccountFabbrica
		AWSAuditAccountAdmins
		AWSControlTowerAdmins
		AWSLogArchiveAdmins
		AWSLogArchiveViewers
		AWSSecurityAuditors
		AWSSecurityAuditPowerUsers
		AWSServiceCatalogAdmins
AWS IAM Identity Center	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.

Registra e archivia le risorse dell'account

Quando configuri la landing zone, le seguenti AWS risorse vengono create all'interno del tuo account di archivio dei log.

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED-
		StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-
		StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

Servizio AWS	Tipo di risorsa	Nome risorsa
		StackSet-AWSControlTowerBP-BASELINE-ROLES-
		StackSet-AWSControlTowerLoggingResources-
AWS Config	Regole di AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
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
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-*

Controlla le risorse dell'account

Quando configuri la landing zone, all'interno del tuo account di controllo vengono create le seguenti AWS risorse.

Servizio AWS	Tipo di risorsa	Nome risorsa
AWS CloudFormation	Stack	StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC- READ-PROHIBITED-
		StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC-WRI TE-PROHIBITED-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-LINKED-ROLE-(In 3.2 and later)

Servizio AWS	Tipo di risorsa	Nome risorsa
		StackSet-AWSControlTowerBP-SECURITY-TOPICS-
		StackSet-AWSControlTowerBP-BASELINE-ROLES-
		StackSet-AWSControlTowerSecurityResources-*
AWS Config	Aggregatore	aws-controltower-GuardrailsComplianceAggregator
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
		aws-controltower-AuditAdministratorRole
		aws-controltower-AuditReadOnlyRole
		AWSControlTowerExecution
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Argomenti	aws-controltower-AggregateSecurityNotifications
		aws-controltower-AllConfigNotifications
		aws-controltower-SecurityNotifications
AWS Lambda	Funzioni	aws-controltower-NotificationForwarder

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](#)
- [Fornitura e gestione degli account con Account Factory](#)
- [Automatizza le attività in AWS Control Tower](#)
- [Sposta e registra gli account con la registrazione automatica](#)
- [Esegui 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 annidati in base all'ereditarietà. OUs

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 in AWS Control Tower by Service Catalog APIs](#)
- [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 denominata provisioning avanzato degli account o provisioning 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 APIs, con 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 \(AFC\)](#)

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. Si apre 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:
 - L'SSOUser-mail può 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 l'account non verrà fornito.
 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 in AWS Control Tower by Service Catalog APIs

AWS Control Tower è integrato con diversi altri AWS servizi, ad esempio AWS Service Catalog. Puoi utilizzarlo APIs per creare e fornire i tuoi account membro in AWS Control Tower o per registrare account membro esistenti.

 Note

Se hai disattivato IAM Identity Center nelle impostazioni della landing zone, i valori forniti durante il provisioning dell'account con la console AWS Service Catalog APIs o non vengono utilizzati.

Il video mostra come effettuare il provisioning degli account in modo automatico e in batch, chiamando il. AWS Service Catalog APIs Per il provisioning, chiamerai l'[ProvisionProductAPI](#) 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, li chiami AWS Service Catalog APIs 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. È possibile 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 disattivato IAM Identity Center nelle impostazioni della landing zone, i valori forniti durante il provisioning dell'account con la console AWS Service Catalog APIs o non vengono utilizzati.

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:
 - SSOUserE-mail (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 Next (Successivo).
- 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. AWS IAM Identity Center 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 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 registrato.
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 venga visualizzato lo stato dell'account Non registrato.

Esegui il provisioning e gestisci gli account in AWS Control Tower

Questo capitolo include:

- una panoramica e procedure per il provisioning e la gestione di nuovi account membro 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 su Account AWS 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) con abilitato. AWSControl TowerBaseline Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare ResetEnabledBaseline e attivare EnabledBaselines e ResetEnabledControl APIs EnabledControls attivare l'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControl TowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

Note

È possibile eseguire contemporaneamente fino a cinque (5) operazioni relative all'account, tra cui il provisioning, l'aggiornamento e la registrazione.

Autorizzazioni necessarie 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 tutti gli 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, oltre 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 dell'account deve sempre disporre delle autorizzazioni `CreateAccount` e delle autorizzazioni `DescribeCreateAccountStatus`. Questo set di autorizzazioni fa parte del ruolo di amministratore e viene fornito automaticamente quando un richiedente assume il ruolo di amministratore. Se deleghi l'autorizzazione a fornire 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](#).

Esegui il provisioning degli 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, mentre 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 fornire nuovi account, nonché l'account `Enroll` per registrare AWS account esistenti in AWS Control Tower, se la tua landing zone non è in uno stato di deriva.

Con Account Factory, puoi fornire account di base, basandoti sulle impostazioni predefinite di AWS Control Tower. Puoi anche fornire account personalizzati che soddisfino 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 \(AFC\)](#).

Registrazione automatica

Puoi anche creare file Account AWS esterni ad AWS Control Tower e spostarli in un'unità organizzativa registrata con AWS Control Tower, senza creare derive di ereditarietà, se attivi la funzionalità di registrazione automatica dell'account nelle impostazioni della tua landing zone. Per ulteriori informazioni, consulta [Sposta e registra gli account con la registrazione automatica](#).

Metodi basati su console:

- Tramite la console Account Factory di cui fa parte AWS Service Catalog, per account di base o personalizzati. Leggi [Fornitura e gestione degli account con Account Factory](#) i dettagli e le 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 funzionalità dell'account Enroll all'interno di AWS Control Tower, se la landing zone non è in stato di deriva. Per informazioni, 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 automatizzati:

- Codice Lambda: dall'account di gestione della zona di destinazione AWS Control Tower, utilizzando il codice Lambda e i ruoli IAM appropriati. Vedi [Provisioning automatizzato 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. Per informazioni, consulta [Esegui 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. APIs 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 richiederà alcuna configurazione aggiuntiva o manutenzione della pipeline. Il provisioning degli account viene effettuato tramite un AWS Service Catalog prodotto chiamato blueprint. Un blueprint 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 tutti OUs gli account dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di registrazione in AWS Control Tower. Puoi visualizzare e registrare gli account dei membri in AWS Control Tower, individualmente o per gruppi di unità organizzative, se ogni 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, è possibile 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 dell'unità organizzativa.

Nella pagina Organizzazione e nella pagina dei dettagli dell'account, puoi vedere lo stato dell'account, che è uno di questi:

- **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 non si applicano a questo account. Se l'unità organizzativa principale non è registrata, nessun controllo si applica a questo account.
- **Registrazione:** l'account viene sottoposto alla 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.
- **Registrato:** l'account è governato dai controlli configurati per l'unità organizzativa principale. È completamente gestito da AWS Control Tower.
- **Registrazione non riuscita:** l'account non può essere registrato in AWS Control Tower. Per ulteriori informazioni, consulta [Cause comuni di mancata iscrizione](#).
- **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 di registrare nuovamente l'unità organizzativa e aggiornare tali account contemporaneamente.

Informazioni sulla registrazione di account esistenti

Puoi estendere la governance di AWS Control Tower a un individuo esistente Account AWS quando lo registri in un'unità organizzativa (OU) già governata da AWS Control Tower. Esistono account idonei non registrati OUs che fanno parte della stessa AWS Organizations organizzazione dell'unità organizzativa AWS Control Tower.

Esistono diversi metodi per registrare gli account in AWS Control Tower. Le informazioni contenute in questa pagina si applicano a tutti i metodi di registrazione.

 Note

Non puoi registrare un AWS account esistente come account di controllo o di archiviazione dei log tranne durante la configurazione iniziale della landing zone.

Cosa succede durante la registrazione dell'account

Durante il processo di registrazione, AWS Control Tower esegue le seguenti 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. AWS IAM Identity Center AWS Organizations
- Inserisce l'account nell'unità organizzativa specificata. Assicurati di applicare tutto ciò SCPs che viene applicato nell'unità organizzativa corrente, in modo che il tuo livello di sicurezza rimanga coerente.
- Applica i controlli obbligatori all'account mediante quelli SCPs che si applicano all'unità organizzativa selezionata nel suo complesso.
- 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 landing zone, se hai selezionato l' AWS CloudTrail integrazione opzionale nelle impostazioni della landing zone:

- Tutti gli account dei membri di un'unità organizzativa sono regolati dal AWS CloudTrail percorso dell'unità organizzativa, a prescindere dal fatto che siano registrati o meno.
- Quando registri un account in AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso della nuova organizzazione. Se disponi già di una distribuzione di un CloudTrail trail, potresti riscontrare addebiti duplicati, a meno che non elimini il trail 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 oppure, APIs potresti voler rimuovere eventuali percorsi a livello di account rimanenti relativi all'account. Se disponi già di un'implementazione di un CloudTrail trail, dovrai sostenere addebiti doppi. CloudTrail

Se aggiorni la landing zone e scegli di disattivare i trail a livello di organizzazione, o se la tua landing zone è precedente alla versione 3.0, i CloudTrail percorsi a livello di organizzazione non si applicano ai tuoi account.

Registra gli account esistenti con VPCs

AWS Control Tower si comporta VPCs in modo diverso quando si effettua il provisioning di un nuovo account in Account Factory rispetto a quando si registra un account esistente.

- Quando crei 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 account con risorse AWS Config

L'account da registrare non deve disporre di risorse esistenti AWS Config . Vedi [Registrare 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 distribuzione.

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"

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 hai selezionato la funzionalità opzionale di registrazione automatica nella pagina delle impostazioni della landing zone o se utilizzi una versione della landing zone precedente alla 3.1.

Questi prerequisiti sono necessari prima di poter registrare un account esistente Account AWS in AWS Control Tower:

 Note

Il prerequisito per aggiungere il **AWSControlTowerExecution** ruolo non è necessario se hai attivato la funzionalità di registrazione automatica di AWS Control Tower nella pagina delle impostazioni della landing zone o se stai registrando l'account come parte di un processo di registrazione dell'account. Tuttavia, in tutti i casi, l'account da registrare potrebbe non disporre di risorse esistenti. AWS Config Vedi [Registrazione account che dispongono di risorse esistenti AWS Config](#)

1. Per iscrivere un account esistente Account AWS, il `AWSControlTowerExecution` ruolo deve essere presente nell'account che stai registrando. Puoi consultare [Registra un account](#) per dettagli e istruzioni.
2. Oltre al `AWSControlTowerExecution` ruolo, l'esistente che Account AWS desideri iscrivere deve disporre delle seguenti autorizzazioni e relazioni di fiducia. In caso contrario, la registrazione avrà esito negativo.

Autorizzazione del ruolo: `AdministratorAccess` (politica AWS gestita)

Ruolo, relazione di fiducia:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. È consigliabile 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 [gli account Enroll che dispongono di AWS Config risorse esistenti](#) per istruzioni su come modificare le risorse esistenti.

4. L'account che desideri registrare deve appartenere alla stessa AWS Organizations organizzazione dell'account di gestione 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 presso 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 trail, potresti riscontrare addebiti duplicati, a meno che non elimini il trail 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 tuo conto, in modo da CloudFormation poter distribuire automaticamente lo stack agli account dell'organizzazione selezionata. Con questo accesso affidabile, il **AWSControlTowerExecution** ruolo svolge le attività necessarie per gestire ogni 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 pile su più account e Regioni AWS con un'unica operazione. AWS Control Tower si affida a questa funzionalità di fiducia in modo da poter applicare ruoli e autorizzazioni agli account esistenti prima di trasferirli in un'unità organizzativa registrata e quindi sottoporli alla governance.

[Per ulteriori informazioni su Trusted Access and AWS CloudFormationStackSets, consulta AWS CloudFormationStackSets 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 abiliti facoltativamente questa funzionalità, puoi utilizzare la console AWS Organizations APIs and per spostare gli account in AWS Control Tower, senza creare differenze di [ereditarietà](#). 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 OUs all'interno di AWS Control Tower, senza creare differenze di ereditarietà, se i due OUs 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 landing zone nella console AWS Control Tower oppure chiamando AWS Control Tower **CreateLandingZone** oppure **UpdateLandingZone** APIs, con il valore del parametro impostato su Inheritance Drift. **RemediationType**

Per applicare la registrazione automatica: dopo aver selezionato questa opzione nella pagina Impostazioni, puoi spostare un account tramite la AWS Organizations console, l' AWS Organizations MoveAccountAPI o la console AWS Control Tower.

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.

Note

Se l'origine e la destinazione OUs in AWS Control Tower hanno configurazioni diverse, l'account potrebbe mostrare delle variazioni [Account membro trasferito](#).

Prerequisiti: configurazione per la registrazione automatica

- Devi eseguire AWS Control Tower landing zone versione 3.1 o successiva.
- Attiva la funzionalità di registrazione automatica di AWS Control Tower tramite la pagina delle impostazioni della landing zone nella console o tramite la landing zone di AWS Control Tower APIs, impostando il valore del parametro su. RemediationTypes Inheritance Drift Dopo l'attivazione, AWS Control Tower reagisce agli move account eventi e corregge immediatamente la deriva ereditaria per gli 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 al riguardo APIs, consulta [CreateAccounte MoveAccount](#) nell'AWS Organizations API Reference.

Considerazioni

- Cronologia della registrazione: un account trasferito in un'unità organizzativa registrata presso 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 trasferiti.
- Processo di annullamento della registrazione: puoi utilizzare lo stesso processo per annullare la registrazione degli account da AWS Control Tower spostandoli in un'unità organizzativa esterna ad AWS Control Tower. Questo processo rimuove tutti i ruoli e le risorse distribuiti da AWS Control Tower e tutti i controlli abilitati in AWS Control Tower.

Registra un account esistente dalla console AWS Control Tower

Esistono due modi comuni per iscrivere un individuo Account AWS in AWS Control Tower.

1. Dopo aver selezionato la funzionalità di registrazione automatica nella pagina Impostazioni, puoi creare un'unità Account AWS esterna di 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 delle landing zone.
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. Vai alla pagina 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.

Quindi, segui i passaggi per la registrazione di un singolo account, come mostrato nella sezione.

[Passaggi per registrare un account manualmente](#)

Considerazioni sulla registrazione dalla console

- La funzionalità dell'account Enroll disponibile nella console AWS Control Tower è destinata alla registrazione degli account esistenti Account AWS in modo che siano governati da AWS Control Tower. Per ulteriori informazioni, consulta [Registrare](#) un esistente. Account AWS
- [La funzionalità dell'account Enroll basata sulla console è disponibile quando la landing zone non è in stato di deriva.](#) 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 fornire nuovi account tramite Account Factory o un altro metodo, fino a quando la deriva della landing zone non sarà risolta.
- Quando registri account dalla console AWS Control Tower, devi accedere a un account con un utente con la AWSServiceCatalogEndUserFullAccess policy abilitata, oltre alle autorizzazioni di accesso di amministratore per utilizzare la console AWS Control Tower, e non puoi accedere come utente root.
- Gli account che registri possono essere aggiornati tramite AWS Control Tower Account Factory, come faresti con qualsiasi altro account. Le procedure di aggiornamento sono fornite nella sezione chiamata [Aggiorna e sposta gli account con AWS Control Tower](#).

Note

Quando ne registri uno esistente Account AWS, assicurati di verificare l'indirizzo e-mail esistente. Altrimenti, potrebbe essere creato un nuovo account.

Passaggi per registrare un account manualmente

Dopo aver AdministratorAccess impostato 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 il pulsante Registra account quando vengono visualizzati nella pagina dei dettagli dell'account.
- Quando scegli Registra account, vedrai una pagina di registrazione dell'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 esistente Account AWS e registralo](#)
- Quindi, selezionare un'unità organizzativa registrata dall'elenco a discesa. Se l'account si trova già in un'unità organizzativa registrata, questo elenco mostrerà l'unità organizzativa.
- Scegli Enroll account (Registra account).
- Verrà visualizzato 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 iscrizione

- 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.
- AWS Security Token Service (AWS STS) è disabilitato Account AWS nella tua regione d'origine o in qualsiasi regione supportata da AWS Control Tower.
- È possibile che tu abbia effettuato l'accesso a un account che deve essere aggiunto al portafoglio Account Factory in AWS Service Catalog. L'account 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 cercando di registrare potrebbe avere AWS Config impostazioni residue. In particolare, l'account può disporre di un registratore di configurazione o di un canale di distribuzione. Questi devono essere eliminati o modificati tramite il AWS CLI prima di poter registrare un account. Per ulteriori informazioni, consultare [Registrazione account che dispongono di risorse esistenti AWS Config](#) e [Interagisci con AWS Control Tower AWS CloudShell](#).
- Se l'account appartiene a un'altra unità organizzativa con un account di gestione, inclusa un'altra unità organizzativa AWS Control Tower, è necessario 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 dall'unità organizzativa originale. In caso contrario, la registrazione avrà esito negativo.
- L'approvvigionamento e la registrazione dell'account falliscono se le unità organizzative di destinazione SCPs non consentono di creare tutte le risorse necessarie per quell'account. Ad esempio, un SCP nell'unità organizzativa di destinazione può bloccare la creazione di risorse senza determinati tag. In questo caso, il provisioning o la registrazione dell'account falliscono, perché AWS Control Tower non supporta il tagging delle risorse. Per assistenza, contatta il rappresentante del tuo account oppure. 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 è possibile confermare che un'unità esistente Account AWS soddisfi i prerequisiti di registrazione, è possibile configurare un'unità organizzativa di registrazione e registrare l'account in tale unità organizzativa. Una volta completata la registrazione, è possibile spostare l'account nell'unità organizzativa desiderata. Se l'iscrizione non va a buon fine, significa che nessun altro account è OUs interessato dall'errore.

Se hai dubbi sulla compatibilità dei tuoi 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 di 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 usando pacchetti di AWS Config conformità](#).

- 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 effettuato 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 con successo AWS Control Tower.

Note

Il pacchetto di conformità funziona anche in situazioni in cui gli account sono OUs registrati da AWS Control Tower, ma i carichi di lavoro vengono eseguiti all'interno di AWS regioni che non dispongono del supporto di AWS Control Tower. Puoi utilizzare il Conformance Pack 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 registrati nella 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. È necessario fornire un metodo di pagamento separato se si utilizza questo approccio.
2. Invita l'account a entrare a far parte dell'organizzazione AWS Control Tower. Per ulteriori informazioni, consulta [Invitare un AWS account a far parte della propria organizzazione](#) nella Guida per l'AWS Organizations utente.
3. Accetta l'invito. L'account viene visualizzato nella cartella principale dell'organizzazione. Questo passaggio sposta l'account nella stessa organizzazione di AWS Control Tower SCPs e stabilisce una fatturazione consolidata.

 Tip

Puoi inviare l'invito per la nuova organizzazione prima che l'account esca dalla vecchia organizzazione. L'invito rimarrà 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 facoltativa. 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 account con risorse AWS Config](#) e [Registrare account che dispongono di risorse esistenti AWS Config](#).

Dopo aver completato questi passaggi preparatori, puoi registrare l'account in AWS Control Tower. Per ulteriori informazioni, consulta [Passaggi per registrare un account manualmente](#). Questo passaggio porta l'account alla completa governance di AWS Control Tower.

Passaggi opzionali per rimuovere il provisioning di un account, in modo che possa essere registrato e mantenerne lo stack

1. Per mantenere lo CloudFormation stack applicato, eliminate l'istanza dello stack dai set di stack e scegliete Retain stacks per l'istanza.
2. Termina 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. (Esegui questa operazione, 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 [Annullare la registrazione di un account](#).
5. Se hai un'unità organizzativa sospesa con controlli definiti, puoi spostare l'account lì invece di eseguire la Fase 1.

Aggiungi manualmente il ruolo IAM richiesto a un ruolo esistente Account AWS e registralo

Se hai già configurato la 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 landing zone, segui i passaggi descritti nella Guida per l'utente di AWS Control Tower alla [Getting Started, Step 2](#). Una volta che la landing zone è pronta, completa i seguenti passaggi per far sì che gli account esistenti vengano governati manualmente da AWS Control Tower.

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 quell'account. A tale scopo, aggiungerai un ruolo con accesso completo all'account, come illustrato nei passaggi seguenti. Questi passaggi devono essere eseguiti per ogni account che registri.

Per ogni account:

Passaggio 1: accedi con accesso da amministratore all'account di gestione dell'organizzazione che attualmente contiene l'account che desideri registrare.

Ad esempio, se hai creato questo account AWS Organizations e utilizzi un ruolo IAM multiaccount 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 l'ID dell'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 a questo account da più account. Il nome di questo ruolo è stato definito al momento della creazione dell'account. Se non hai specificato un nome di ruolo quando hai creato l'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 secondario.
8. Quando hai finito, resta nell'account per bambini per la parte successiva della procedura.

9. Prendi nota dell'ID dell'account di gestione, perché dovrai inserirlo nel passaggio successivo.

Fase 2: autorizzare AWS Control Tower a gestire l'account.

1. Vai a IAM.
2. Vai a Ruoli.
3. Scegli 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 di 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 Successivo: Tag.
8. È possibile che venga visualizzata una schermata opzionale intitolata Aggiungi tag. Per ora salta questa schermata scegliendo Avanti:Revisione
9. Nella schermata di revisione, nel campo Nome del ruolo, inserisci.
AWSControlTowerExecution
10. Inserisci una breve descrizione nella casella Descrizione, ad esempio Consente l'accesso completo all'account per l'iscrizione.

11. Scegli Crea ruolo.

Fase 3: Registrare l'account spostandolo in un'unità organizzativa registrata e verificare 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 accedi ad 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 la registrazione di un singolo account, come mostrato nella pagina. [Passaggi per registrare un account manualmente](#)
3. Verifica l'iscrizione.
 - Da AWS Control Tower, scegli Organization nella barra di navigazione a sinistra.
 - Cerca l'account che hai registrato di recente. Il suo stato iniziale mostrerà lo stato di Iscrizione.
 - Quando lo stato cambia in Registrato, lo spostamento ha avuto esito positivo.

Per continuare questo processo, accedi a ogni account dell'organizzazione che desideri registrare in AWS Control Tower. Ripeti i passaggi preliminari 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
```

Registrare account che dispongono di risorse esistenti AWS Config

Questo argomento fornisce un step-by-step approccio su come registrare account che dispongono di risorse esistenti. AWS Config Per esempi su come controllare le risorse esistenti, consulta [Registra account con risorse AWS Config](#).

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 cosa SCPs tu 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 avviso `AccessDeniedException` quando ti viene SCPs `aws-controltower-ConfigRecorderRole*` impedito di chiamare Config.

Fase 3: Identifica le 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 le AWS regioni prive di 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.

Fase 5: Modifica le risorse esistenti in ogni AWS regione

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 S3aws-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 S3aws-controltower-config-logs-AUDIT_ACCOUNT-<REGION_STRING>-<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 principale 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. Modifica le risorse del canale AWS Config di distribuzione

Può esistere un solo canale di AWS Config consegna per regione. Se ne esiste un altro, modifica le impostazioni come mostrato.

- Nome: DON'T CHANGE
- ConfigSnapshotDeliveryProperties: TwentyFour _Ore
- S3: BucketName CONFIG_BUCKET
- S3: KeyPrefix 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. Modifica le risorse di AWS Config 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 IncludeGlobalResourcesTypesparametro abbia il valoreGLOBAL_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 BucketName campo S3, sostituisci il *CONFIG_BUCKET*
 - b. Nel KeyPrefix campo S3, 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-register OU.

Fornitura e gestione degli account con Account Factory

Note

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

Questo capitolo include una panoramica e le procedure per il provisioning di nuovi account membro in una landing zone di AWS Control Tower con Account Factory.

Autorizzazioni per la configurazione e il provisioning degli account

L'AWS Control Tower Account Factory consente agli amministratori e agli utenti del cloud AWS IAM Identity Center di effettuare il provisioning degli account nella tua landing zone. Per impostazione predefinita, gli utenti di IAM Identity Center che forniscono gli account devono far parte del AWSAccountFactory gruppo o del gruppo di gestione.

Note

Fai attenzione quando lavori dall'account di gestione, come faresti quando utilizzi qualsiasi account con autorizzazioni all'interno dell'organizzazione.

L'account di gestione AWS Control Tower ha una relazione di fiducia con il `AWSControlTowerExecution` ruolo, che consente la configurazione dell'account dall'account di gestione, incluse alcune configurazioni automatiche dell'account. Per ulteriori informazioni sul `AWSControlTowerExecution` ruolo, consulta [Ruoli e account](#).

Note

Per registrare 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 di account esistenti](#).

Per ulteriori informazioni sulle autorizzazioni, consultare [Autorizzazioni necessarie per il provisioning degli account](#).

Considerazioni sulla gestione degli account in Account Factory

Puoi aggiornare, annullare la registrazione e chiudere gli account che crei e fornisci 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 fornito associato a un account fornito da Account Factory, se si specifica un nuovo indirizzo e-mail utente per AWS IAM Identity Center il quale 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 e-mail utente di 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 i problemi, ad esempio. [Account membro trasferito](#) Gli aggiornamenti dell'account sono necessari anche come parte di un aggiornamento completo delle landing zone.

Aggiorna l'account nella console

Per aggiornare un account nella console AWS Control Tower

1. Una volta effettuato l'accesso ad AWS Control Tower, accedi alla pagina Organizzazione.
2. Nell'elenco degli account OUs e, 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 possono essere diversi dai controlli della precedente unità organizzativa. Assicurati che i controlli della nuova unità organizzativa soddisfino i requisiti delle policy per l'account.

Gli account AWS Control Tower vengono modificati in modo diverso, a seconda che tu abbia scelto o meno la registrazione automatica degli account. Per ulteriori informazioni sulla registrazione automatica, vedere. [Configurare facoltativamente la registrazione automatica per gli account](#)

Controlla il comportamento quando gli account vengono spostati da un account all'altro OUs, 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 dall'unità organizzativa. I controlli e le linee di base dell'unità organizzativa precedente 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 trasferiti da un account all'altro OUs, senza registrazione automatica

Quando si sposta un account da un account all'altro OUs, i controlli per l'unità organizzativa di destinazione vengono applicati al conto. Tuttavia, i controlli applicati all'account della precedente unità organizzativa non lo sono rimosso. L'esatto comportamento dei controlli è specifico dell'implementazione di controlli attivi sull'unità organizzativa precedente 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 SCPs: I controlli basati su SCP dell'unità organizzativa precedente sono rimosso. I controlli basati su SCP per l'unità organizzativa di destinazione entrano in vigore su questo account.
- Per i controlli implementati con gli 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 rimosso e i controlli nell'unità organizzativa di destinazione vengono applicati a conto.

Modifica l'indirizzo e-mail di un account registrato

Per modificare l'indirizzo e-mail di un account membro registrato in AWS Control Tower, segui la procedura in questa sezione.

Note

La seguente procedura non consente di modificare l'indirizzo e-mail di un account di gestione, di un account di archiviazione dei log o di un account di controllo. Per ulteriori informazioni a riguardo, vedi [Come posso modificare l'indirizzo e-mail associato al mio AWS account?](#) o contatta l' AWS assistenza.

Per modificare l'indirizzo e-mail di un account creato da AWS Control Tower

1. Recupera la password dell'utente root per l'account. Puoi seguire i passaggi indicati nell'articolo [Come posso recuperare una AWS password smarrita o dimenticata?](#)
2. Accedi all'account con la password dell'utente root.
3. Cambia l'indirizzo email come faresti per qualsiasi altro Account AWS e attendi che la modifica si rifletta AWS Organizations. È possibile che si verifichi un ritardo durante il completamento dell'aggiornamento della modifica dell'indirizzo e-mail.
4. Aggiorna il prodotto fornito in Service Catalog utilizzando l'indirizzo e-mail che in precedenza apparteneva all'account. Il processo di aggiornamento del prodotto fornito include l'associazione del nuovo indirizzo e-mail al prodotto fornito. In questo modo la modifica dell'indirizzo e-mail ha effetto in AWS Control Tower. Utilizza il nuovo indirizzo e-mail per gli aggiornamenti dei prodotti forniti successivamente.

Per modificare la password o l'indirizzo e-mail di un account membro con cui hai creato AWS Organizations, consulta [Accedere a un account membro come utente root](#) nella Guida per l'AWS Organizations utente.

In alternativa, puoi aggiornare l'indirizzo e-mail di un Account Factory o di un altro account membro dalla AWS Organizations console senza accedere come utente root. Per ulteriori informazioni, vedere [Aggiornamento dell'indirizzo e-mail dell'utente root per un account membro AWS Organizations](#) nella Guida per l'AWS Organizations utente.

Cambia il nome di un account registrato

Segui la procedura 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 e accedere come utente root dell'account.

Per modificare il nome di un account creato da AWS Control Tower, utilizzando la AWS Organizations console o APIs

- 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 root 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 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 in base alla modifica del nome. Questo aggiornamento non si rifletterà nel prodotto fornito in AWS Service Catalog.

Configurare 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 di unità organizzative (OUs) e il loro stato nell'elenco delle unità consentite. Per impostazione predefinita, tutte OUs sono incluse nell'elenco delle unità consentite, il che significa che è possibile assegnare il provisioning agli account in base a tali account. È possibile disabilitarne alcuni OUs per il provisioning dell'account tramite AWS Service Catalog.

Puoi visualizzare le opzioni di configurazione di Amazon VPC disponibili per gli utenti finali quando effettuano il provisioning di nuovi account.

Per configurare le impostazioni di Amazon VPC in Account Factory

1. In qualità di amministratore 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 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 stabilire per tutti i nuovi account Account Factory che gli utenti finali possono creare e inserisci le 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.
- Inserisci l'intervallo di indirizzi IP per creare il tuo account. VPCs 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 creato da Account Factory 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 di sottorete VPCs di tutti gli account forniti 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.
- Scegli Save (Salva).

Puoi impostare queste opzioni di configurazione per creare nuovi account che non includono un VPC. Consulta la [procedura dettagliata](#).

Annulare 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 l'account venga gestito da AWS Control Tower in una landing zone, 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 eventuali controlli e blueprint. L'account viene spostato da

qualsiasi unità organizzativa AWS Control Tower e viene spostato nell'area Root. L'account non fa più parte di un'unità organizzativa registrata e non è più soggetto ad AWS Control Tower SCPs. 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 + accanto all'unità organizzativa.
4. Seleziona l'account, quindi scegli Annulla gestione.

Note

Attendi che venga visualizzato lo stato dell'account Non registrato.

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

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 la registrazione dell'account in questo modo. Tuttavia, è possibile registrare nuovamente l'account restituendolo all'unità organizzativa.

Quando annulli la registrazione di un account personalizzato, AWS Control Tower rimuove le risorse distribuite dalla landing zone e tutte le altre risorse che AWS Control Tower ha creato all'interno dell'account. AWS Control Tower rimuove anche il `AWSControlTowerExecution` ruolo, anche se è stato aggiunto manualmente. La rimozione di questo ruolo è conforme al principio del privilegio minimo, poiché un ruolo di esecuzione del servizio non dovrebbe 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 che hai selezionato al momento della creazione dell'account in Account Factory ha ancora 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 modificando l'indirizzo e-mail 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](#).

Puoi visualizzare un elenco di AWS [YouTube video](#) che spiegano le attività più comuni 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 AWS account nella Guida di riferimento alla gestione degli account](#).

 Note

Chiudere un account non Account AWS equivale a 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.

Chiudere un account membro 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 singolarmente con credenziali root, tramite AWS Organizations. Tuttavia, non puoi chiudere il tuo account di gestione in questo modo.

Quando chiami l' API [CloseAccountAPI](#) o chiudi un account nella AWS Organizations console, l'account membro viene isolato per 90 giorni, come qualsiasi altro Account AWS. L'account mostra lo stato Sospeso in AWS Control Tower e AWS Organizations. Se tenti di utilizzare l'account durante quei 90 giorni, AWS Control Tower visualizza un messaggio di errore.

Note

Se un'unità organizzativa ha account sospesi, EnabledControl le operazioni relative ai controlli regionali sull'obiettivo falliranno.

Prima della scadenza dei 90 giorni, puoi ripristinare l'account membro, come puoi fare con qualsiasi altro Account AWS. Dopo quel periodo di 90 giorni, i record dell'account vengono rimossi.

Come best practice, consigliamo 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 Registrato. Di conseguenza, se si tenta di registrare nuovamente l'unità organizzativa dell'account durante quei 90 giorni, AWS Control Tower genera un messaggio di errore. L'account sospeso blocca essenzialmente le azioni di nuova registrazione con un errore di controllo preliminare. Se si rimuove l'account dall'unità organizzativa, è possibile registrare nuovamente l'unità organizzativa, ma AWS potrebbe verificarsi un errore relativo a un metodo di pagamento mancante per l'account. Per aggirare questo vincolo, crea un'altra unità organizzativa e sposta l'account in tale unità prima di provare a effettuare una nuova registrazione. Si consiglia di denominare questa unità organizzativa sospesa.

Note

Se non annulli la registrazione dell'account prima di chiuderlo, devi eliminare il prodotto fornito dall'account entro il AWS Service Catalog termine dei 90 giorni.

[Per ulteriori informazioni, consulta la AWS Organizations documentazione sull'API. CloseAccount](#)

Considerazioni sulle risorse per Account Factory

Quando a un account viene fornito 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-*
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
		StackSet-AWSControlTowerBP-BASELINE-CONFIG-*
		StackSet-AWSControlTowerBP-BASELINE-ROLES-*
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Regole dell'evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registri	aws-controltower/CloudTrail Logs
		/aws/lambda/aws-controltower-NotificationForwarder

AWS servizio	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
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 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) con AWSControl TowerBaseline abilitato. Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare ResetEnabledBaseline e attivare EnabledBaselines e ResetEnabledControl APIs EnabledControls attivare l'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControl TowerBaseline [Tipi di base applicabili a livello di unità organizzativa](#)

AWS Control Tower ti consente di personalizzare nuove ed esistenti Account AWS quando effettui il provisioning delle relative risorse dalla console AWS Control Tower. Dopo aver configurato 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.

Fornisci nuovi account con progetti

I tuoi account personalizzati vengono forniti in AWS Control Tower Account Factory, tramite CloudFormation modelli o con Terraform. Definirai un modello che funga da modello di account personalizzato. Il blueprint descrive le risorse e le configurazioni specifiche necessarie per il provisioning di un account. Sono disponibili anche blueprint predefiniti, 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 progetti 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 progetti dell'account sono archiviati in un account Account AWS, che per i nostri scopi viene denominato account hub. I blueprint vengono archiviati sotto forma di prodotto Service Catalog. Chiamiamo questo prodotto un modello, per distinguerlo da qualsiasi altro prodotto Service Catalog.

Per ulteriori informazioni su come creare prodotti Service Catalog, vedere [Creating products](#) nella AWS Service Catalog Administrator Guide.

Note

AWS Control Tower contiene controlli proattivi che monitorano CloudFormation le risorse in AWS Control Tower. Facoltativamente, puoi attivare questi controlli nella tua landing zone. Quando applichi controlli proattivi, questi controllano che le risorse che stai per distribuire ai tuoi account siano conformi alle politiche e alle procedure dell'organizzazione. [Per ulteriori informazioni sui controlli proattivi, consulta Controlli proattivi.](#)

Per ulteriori informazioni sull'utilizzo di AFC, consulta [Automatizzare la personalizzazione dell'account utilizzando Account Factory Customization in AWS Control Tower.](#)

Prerequisiti

Prima di iniziare a creare account personalizzati con AWS Control Tower Account Factory, è necessario disporre di un ambiente di landing zone AWS Control Tower e disporre di un'unità organizzativa (OU) registrata presso AWS Control Tower, in cui verranno collocati i nuovi account creati.

Preparazione per la personalizzazione

- Designare un account hub: è possibile creare un nuovo account che funga da account hub o utilizzarne uno esistente. Account AWS Ti consigliamo vivamente di non utilizzare l'account di gestione AWS Control Tower come account Blueprint Hub.
- Aggiungi il ruolo necessario: se prevedi di 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 i blueprint dei partner con requisiti di abbonamento al marketplace, devi configurarli dal tuo account di gestione 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 a partire 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](#)
- [Rimuovere un blueprint da un account](#)
- [Progetti per i partner](#)
- [Considerazioni sulle personalizzazioni di Account Factory \(AFC\)](#)
- [In caso di errore del blueprint](#)
- [Personalizzazione del documento di policy per i blueprint AFC in base a CloudFormation](#)
- [Autorizzazioni aggiuntive necessarie per creare un prodotto Service Catalog basato su Terraform](#)
- [Transizione al tipo di prodotto AWS Service Catalog esterno](#)

Configura per la personalizzazione

Le sezioni successive illustrano i passaggi per configurare Account Factory per il processo di personalizzazione. Si consiglia 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), dove sono archiviati i prodotti Service Catalog, chiamati anche blueprint.
- Fase 2. Crea il prodotto. AWS Service Catalog Crea il AWS Service Catalog prodotto (chiamato anche «prodotto modello») che ti servirà per creare la base dell'account personalizzato.
- Fase 3. Rivedi il tuo progetto personalizzato. Ispeziona il AWS Service Catalog prodotto (blueprint) che hai creato.
- Fase 4. Chiama il tuo progetto per creare un account personalizzato. Inserisci le informazioni sul prodotto blueprint 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 dell'hub. Il ruolo deve essere denominato `AWSControlTowerBlueprintAccess`.

AWS Control Tower assume questo ruolo per creare una risorsa Portfolio per tuo conto in AWS Service Catalog, quindi aggiungere il tuo blueprint come prodotto Service Catalog a questo portafoglio e quindi condividere questo portafoglio e il tuo blueprint con il tuo account membro durante il provisioning dell'account.

Sarai tu a creare il `AWSControlTowerBlueprintAccess` ruolo, come spiegato nelle seguenti sezioni. Puoi impostare 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. Federa o accedi come principale nell'account di gestione AWS Control Tower.
2. Dal principale federato nell'account di gestione, assumi o passa al `AWSControlTowerExecution` ruolo nell'account AWS Control Tower registrato che scegli per fungere da account Blueprint Hub.
3. Dal `AWSControlTowerExecution` ruolo nell'account AWS Control Tower registrato, crea il `AWSControlTowerBlueprintAccess` ruolo con autorizzazioni e relazioni di fiducia adeguate.

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 all'uso da parte di 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 `AWSControlTowerBlueprintAccess` ruolo.

Per configurare il `AWSControl TowerBlueprintAccess` ruolo in un account membro non registrato

1. Federati o accedi come principale all'account che desideri designare come account hub, utilizzando il metodo che preferisci.
2. Una volta effettuato l'accesso come responsabile dell'account, crea il `AWSControlTowerBlueprintAccess` ruolo con le autorizzazioni e le relazioni di fiducia appropriate.

Il `AWSControlTowerBlueprintAccess` ruolo deve essere impostato in modo da garantire la fiducia a due responsabili:

- Il principale (utente) che esegue AWS Control Tower nell'account di gestione AWS Control Tower.
- Il ruolo indicato `AWSControlTowerAdmin` nell'account di gestione AWS Control Tower.

Ecco un esempio di policy di fiducia, simile a quella che dovrai includere per il tuo ruolo. Questa politica dimostra la migliore pratica di concedere l'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"
      }
    ]
  }
}
```

Policy sulle autorizzazioni richieste

AWS Control Tower richiede che la policy `AWSServiceCatalogAdminFullAccess` gestita 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 AWS Service Catalog del prodotto. AWS Service Catalog Puoi allegare questa policy quando crei il ruolo nella console IAM.

Potrebbero essere necessarie autorizzazioni aggiuntive

- Se memorizzi i tuoi blueprint in Amazon S3, AWS Control Tower richiede anche `AmazonS3ReadOnlyAccess` la politica di autorizzazione per `AWSControlTowerBlueprintAccess` il ruolo.
- Il tipo di prodotto AWS Service Catalog Terraform richiede l'aggiunta di alcune autorizzazioni aggiuntive alla politica IAM personalizzata AFC, se non utilizzi la politica di amministrazione predefinita. Li richiede oltre alle autorizzazioni necessarie per creare le risorse definite nel modello terraform.

Passaggio 2. Crea il prodotto AWS Service Catalog

Per creare un AWS Service Catalog prodotto, segui la procedura descritta in [Creazione di prodotti](#) nella Guida per l'AWS Service Catalog amministratore. Aggiungerai il blueprint del tuo account come modello quando creerai il AWS Service Catalog prodotto.

Important

A seguito HashiCorp dell'aggiornamento delle licenze Terraform, il supporto per i prodotti Terraform Open Source AWS Service Catalog è stato modificato e i prodotti sono stati forniti a un nuovo tipo di prodotto, chiamato External. [Per ulteriori informazioni sull'impatto di questa modifica su AFC, incluso come aggiornare i blueprint degli account esistenti al tipo di prodotto esterno, consulta la sezione Transizione al tipo di prodotto esterno.](#)

Riepilogo dei passaggi per creare un blueprint

- Crea o scarica un CloudFormation modello o un file di configurazione Terraform tar.gz che diventerà il progetto del tuo account. Alcuni esempi di modelli sono forniti più avanti in questa sezione.
- Accedi al sito in Account AWS cui archivi i tuoi blueprint Account Factory (a volte chiamato account hub).
- Vai alla AWS Service Catalog console. Scegli Elenco prodotti, quindi scegli Carica nuovo prodotto.
- Nel riquadro Dettagli del prodotto, inserisci i dettagli del tuo prodotto blueprint, ad esempio un nome e una 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 blueprint.
- 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 configurare una connessione al loro database di 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. Chiama il tuo blueprint per creare un account personalizzato

Quando segui il flusso di lavoro Create account nella console AWS Control Tower, vedrai una sezione opzionale in cui puoi inserire informazioni sul blueprint che desideri 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) A questo punto del processo è possibile aggiungere o modificare una politica di fornitura del blueprint. La policy di provisioning del blueprint è scritta in JSON e associata a un ruolo IAM, in modo da poter fornire le risorse specificate nel modello del blueprint. AWS Control Tower crea questo ruolo nell'account del membro in modo che Service Catalog possa distribuire risorse utilizzando set di CloudFormation stack. 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 tuo blueprint contiene parametri, puoi inserire i relativi valori in campi aggiuntivi nel flusso di lavoro di AWS Control Tower. I valori aggiuntivi possono includere: un nome di GitHub repository, una GitHub filiale, 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 a partire da un blueprint](#).

Crea un account personalizzato a partire da un blueprint

Dopo aver creato blueprint personalizzati, puoi iniziare a creare account personalizzati in AWS Control Tower account factory.

Segui questi passaggi per distribuire un blueprint personalizzato quando crei un nuovo account: AWS

1. Vai a AWS Control Tower in 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 e-mail.
4. Configura i dettagli di IAM Identity Center con indirizzo e-mail e nome utente.
5. Seleziona un'unità organizzativa registrata a cui aggiungere il tuo account.
6. Espandi la sezione Account factory customization.
7. Inserisci l'ID account dell'account blueprint hub che contiene i tuoi prodotti Service Catalog e scegli Convalida. Per ulteriori informazioni su un account Blueprint Hub, vedere. [Personalizza gli account con Account Factory Customization \(AFC\)](#)
8. Seleziona il menu a discesa che contiene tutti i blueprint dell'elenco di prodotti del Service Catalog (tutti i blueprint personalizzati e quelli dei partner). Scegli un blueprint e la versione corrispondente da distribuire.
9. Se il blueprint contiene parametri, questi campi vengono visualizzati e possono essere compilati. I valori predefiniti sono precompilati.
10. Infine, seleziona dove implementare il tuo blueprint, tra Home Region o Tutte le regioni governate. Potrebbe essere necessario distribuire risorse globali come Route 53 o IAM in una sola 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 progetti 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 progetto, 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. Verrà visualizzato un elenco degli account disponibili. Identifica l'account che desideri registrare con un blueprint personalizzato. La colonna Stato per quell'account dovrebbe indicare l'account con lo stato 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 dell'accesso con le informazioni sull'IAM Identity Center dell'account.
5. Seleziona l'unità organizzativa registrata a cui il tuo account diventerà membro.
6. Completa la sezione Personalizzazione di fabbrica dell'account seguendo gli stessi passaggi indicati nella procedura 7-12 della procedura [Crea account](#). Per ulteriori informazioni, vedere [Provision Account Factory accounts with AWS Service Catalog](#).

Puoi visualizzare lo stato dell'avanzamento 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 AWS Control Tower esistente, segui il flusso di lavoro Update 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 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. Vai 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 distribuisce 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 AVAILABLE stato. Se il prodotto fornito 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, consulta [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, le risorse presenti nell'account del membro possono essere rimosse. 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, ovvero la rimozione e la sostituzione del blueprint originale, soprattutto se si eseguono carichi di lavoro di produzione.

Rimuovere un blueprint da un account

Per rimuovere un blueprint da un account, segui il flusso di lavoro Update account per rimuovere il blueprint e riportare l'account alle configurazioni predefinite di AWS Control Tower.

Quando accedi al 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. Vedrai un messaggio di avviso prima che l'azione abbia inizio.

Note

AWS Control Tower aggiunge un blueprint a un account solo se selezioni un blueprint durante il processo di creazione dell'account o di aggiornamento dell'account.

Progetti per i partner

AWS Control Tower Account Factory Customization (AFC) fornisce l'accesso a blueprint di personalizzazione predefiniti creati e gestiti dai partner. AWS Questi progetti per i partner ti aiutano a personalizzare i tuoi account per casi d'uso specifici. I progetti di ogni 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 progetti dei partner di AWS Control Tower, accedi alla libreria Getting Started di Service Catalog 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 dell'hub e nella stessa regione della home region della landing zone 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: la distribuzione solo nella regione di origine o la 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. Puoi rimuovere un blueprint e quindi aggiungere un nuovo blueprint in operazioni separate.
- AWS Control Tower modifica il comportamento, a seconda che si stiano 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 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 fornito da Account Factory nell'account di gestione 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, nuovo account o 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 aggiungi il blueprint al momento della registrazione.

Errore durante la creazione del ruolo e soluzioni **AWSControlTowerBlueprintAccess** alternative

Quando crei il **AWSControlTowerBlueprintAccess** ruolo da un account AWS Control Tower, devi accedere come principale utilizzando il **AWSControlTowerExecution** ruolo. 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:

- (La scelta più 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 consentirne l'operazione.
- (Assolutamente sconsigliato) Usa il tuo account di gestione AWS Control Tower come account hub, quindi non è soggetto all'SCP.

Personalizzazione del documento di policy per i blueprint AFC in base a CloudFormation

Quando abiliti un blueprint tramite account factory, AWS Control Tower ordina di CloudFormation crearne uno per tuo StackSet conto. 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 può essere assunto da. CloudFormation

Come parte dell'abilitazione di un blueprint, AWS Control Tower crea un ruolo nell'account del membro, che CloudFormation può assumere il compito di completare le attività di StackSet gestione. Il modo più semplice per abilitare un blueprint personalizzato tramite account factory consiste nell'utilizzare una policy allow-all, poiché tali policy sono compatibili con qualsiasi modello di blueprint.

Tuttavia, le migliori pratiche suggeriscono di limitare le autorizzazioni per CloudFormation l'account di destinazione. Puoi fornire una policy personalizzata, che AWS Control Tower applica al ruolo che crea CloudFormation per essere utilizzato. Ad esempio, se il tuo blueprint crea un parametro SSM chiamato qualcosa di importante, puoi fornire la seguente politica:

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"
```

```

    }
  ]
}
```

L'AllowCloudFormationActionsOnStacksistruzione 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 del modello che viene abilitato.

Risolvi i problemi di autorizzazione

Quando si abilita un blueprint con una politica limitata, è possibile che le autorizzazioni per abilitare il blueprint siano insufficienti. Per risolvere questi problemi, rivedi il documento relativo alla policy 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 direttamente utilizzando quel ruolo.

Autorizzazioni aggiuntive necessarie per creare un prodotto Service Catalog basato su Terraform

Quando crei 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 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, vedere [Step 5: Creazione di ruoli di lancio](#) nella Service Catalog Administrator Guide.

Transizione al tipo di prodotto AWS Service Catalog esterno

AWS Service Catalog ha modificato il supporto per i prodotti Terraform Open Source e ha fornito i prodotti a un nuovo tipo di prodotto, denominato External. Per ulteriori informazioni su questa transizione, consulta [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti al tipo di prodotto esterno nella guida per l'amministratore](#).AWS Service Catalog

Questa modifica influisce sugli account esistenti che hai creato o registrato con la personalizzazione di fabbrica dell'account AWS Control Tower. Per trasferire questi account al tipo di prodotto esterno, devi apportare modifiche sia AWS Service Catalog in AWS Control Tower che in AWS.

Per passare al tipo di prodotto esterno

1. Aggiorna il tuo Terraform Reference Engine esistente AWS Service Catalog per includere il supporto per i tipi di prodotto External e Terraform Open Source. [Per istruzioni sull'aggiornamento del motore di riferimento Terraform, consulta il Repository.AWS Service Catalog GitHub](#)
2. In AWS Service Catalog, duplica tutti i prodotti Terraform Open Source esistenti (progetti), con i duplicati utilizzando il nuovo tipo di prodotto esterno. Non terminate i progetti Terraform Open Source esistenti.
3. In AWS Control Tower, aggiorna ogni account utilizzando un blueprint Terraform Open Source 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 ulteriori dettagli, consulta [Aggiungere un blueprint a un account AWS Control Tower](#).
4. Dopo che tutti gli account che utilizzano i blueprint Terraform Open Source sono stati aggiornati a blueprint esterni, ripristina AWS Service Catalog e chiudi tutti i prodotti che utilizzano Terraform Open Source come tipo di prodotto.
5. D'ora in avanti, tutti gli account creati o registrati utilizzando la personalizzazione di fabbrica dell'account AWS Control Tower devono fare riferimento ai blueprint utilizzando il tipo di prodotto CloudFormation External.

Per i blueprint creati utilizzando il tipo di prodotto External, AWS Control Tower supporta solo personalizzazioni degli account che utilizzano modelli Terraform e il motore di riferimento Terraform. Per ulteriori informazioni, consulta [Configurazione](#) per la personalizzazione.

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 [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti 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.

Esegui 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 di 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 si effettua il provisioning di un account tramite AFT o Account Factory, si verifica lo stesso flusso di lavoro di backend.

Prerequisiti

Note

La fornitura di account AFT deve essere indirizzata a un'unità organizzativa (OU) AWSControl TowerBaseline abilitata in AWS Control Tower. Per i dettagli di AWSControlTowerBaseline, consulta: [Tipi di base applicabili a livello di unità organizzativa](#).

Quando inizierai 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 di Terraform](#).
- Uno o più git repository per l'ambiente AFT completamente distribuito. Per ulteriori informazioni, consulta le [fasi successive all'implementazione di AFT](#).
- Un ambiente AFT completamente distribuito. Per ulteriori informazioni, consulta [Panoramica di AWS Control Tower Account Factory for Terraform \(AFT\)](#) e [Deploy AWS Control Tower Account Factory for Terraform \(AFT\)](#). [Consulta 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 [aft-account-customizationsrepository](#).

Per gli account registrati tramite Registrazione automatica:

- La creazione di nuovi account tramite AFT continua a funzionare normalmente.
- L'importazione di account esistenti richiede passaggi aggiuntivi:
 - Registra OU per creare i prodotti predisposti necessari prima dell'importazione.
 - Register OU emetterà UpdateManagedAccount eventi CreateManagedAccount e abiliterà le personalizzazioni AFT.

Per informazioni su Regioni AWS dove AFT presenta limitazioni di distribuzione, vedere [Limitazioni e quote in AWS Control Tower](#) e [Limitazioni di controllo](#)

La [documentazione di 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 account basato su Terraform, consentendoti al contempo di governare 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 fornitura dell'account, AFT esegue automaticamente una serie di passaggi prima che inizi la fase di personalizzazione dell'account. Per ulteriori informazioni, consulta [AFT Account Provisioning Pipeline](#).

AFT supporta Terraform Cloud, Terraform Enterprise e Terraform Community Edition. Con AFT è possibile avviare la creazione di account utilizzando un file di input e un semplice `git push` comando e personalizzare account nuovi o esistenti. La creazione di account include tutti i vantaggi di

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 dell'account. Ogni volta che si invia 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 vedere 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 and Step Functions, vedere 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 per i componenti](#), per creare un framework, con pipeline che implementano Terraform Infrastructure as Code (IaC). AFT ti consente di:

- Inviare richieste di fornitura e aggiornamento dell'account in un modello GitOps
- Archivia i metadati dell'account e la cronologia delle verifiche
- 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 landing zone 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 piattaforma: AFT supporta qualsiasi distribuzione Terraform per la distribuzione iniziale e il funzionamento continuo: Community Edition, Cloud ed Enterprise.
- Flessibilità per il sistema di controllo delle versioni: AFT supporta AWS CodeCommit e utilizza fonti di controllo delle versioni alternative. 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 AWS predefinito per gli account
- Registrazione degli account assegnati al piano Enterprise AWS Support

Note

La pipeline AFT non è pensata per l'uso nella distribuzione di risorse, come le istanze Amazon EC2, necessarie ai tuoi account per eseguire le tue applicazioni. È destinato esclusivamente al provisioning e alla personalizzazione automatizzati 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 sul 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 di 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 un first-in-first-out ordine. Per ulteriori informazioni, consulta [Inviare più richieste di account](#).
2. Ogni account viene fornito. Questa fase viene eseguita nell'account di gestione AWS Control Tower.
3. Le personalizzazioni globali vengono eseguite nelle pipeline create per ogni account venduto.

- Se le personalizzazioni sono specificate nelle richieste iniziali di provisioning dell'account, le personalizzazioni vengono eseguite solo su account mirati. Se disponi di un account già fornito, devi avviare ulteriori personalizzazioni manualmente nella pipeline dell'account.

AWS Control Tower Account Factory for Terraform: flusso di lavoro per il provisioning degli account

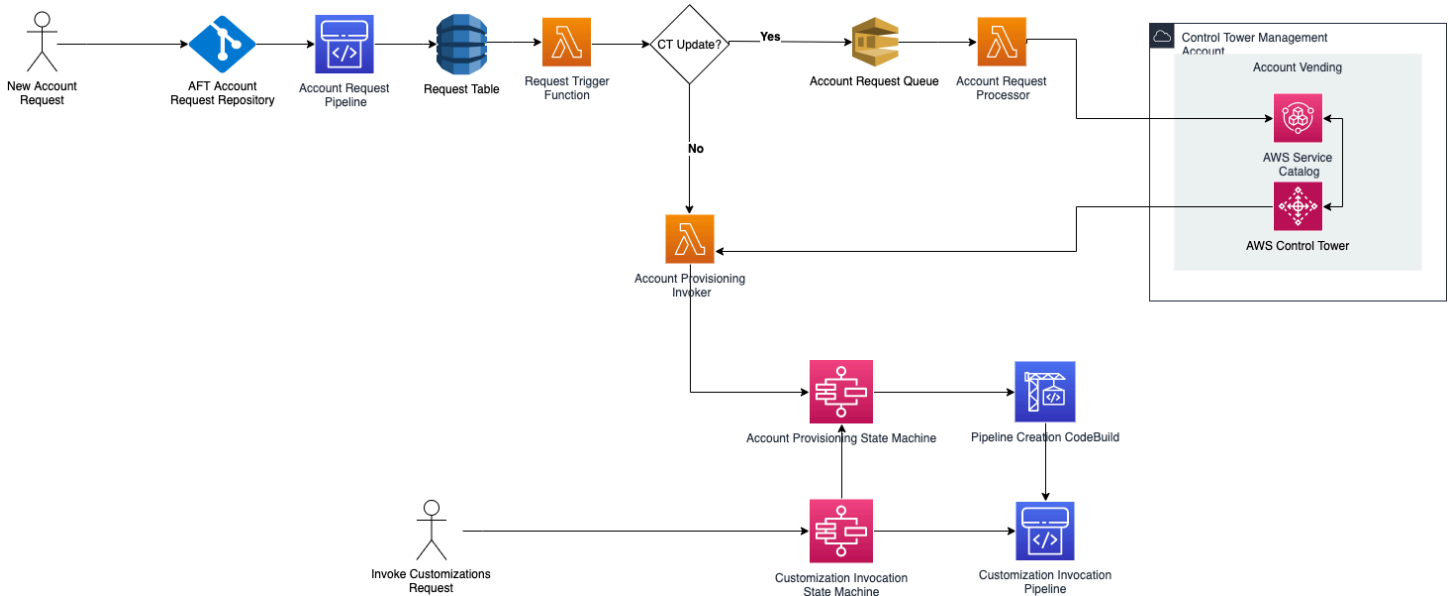


Figura 1: AWS Control Tower Account Factory per Terraform

Costo

Non sono previsti costi aggiuntivi per AFT. Paghi solo per le risorse distribuite da AFT, i AWS servizi abilitati da AFT e le risorse distribuite 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

Completa i passaggi descritti in [Guida introduttiva a 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 viene effettuato 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 1.6.0 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

La riattivazione del `aft_enable_vpc` parametro (commutazione del valore da `false` a `true`) può 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 sottoreti private IDs 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 Terraform Cloud 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.

- È possibile applicare 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, `alias/aft`, per crittografare i log e gli argomenti SNS. CloudWatch 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` and `aft-failure-notifications`) vengono crittografate utilizzando CMK. Se la variabile è impostata su `false`, che è il valore predefinito, i messaggi SNS vengono crittografati con la chiave gestita da AWS: `alias/aws/sns` 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.identityeapp.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 `AdministratorAccess` credenziali. 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 AWS Security Token Service (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](#).

Fasi successive all'implementazione

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 CodeConnections con il provider VCS desiderato

Se scegliete un provider VCS di terze parti, AFT lo stabilisce e voi 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 [Fornisci 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 il tuo account AFT \(provisioning customizations state machine\)](#)
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.](#)

Fornisci un nuovo account con AFT

Questa sezione presuppone che abbiate già configurato AFT e il vostro account di gestione AFT e che stiate fornendo account aggiuntivi.

Per fornire un nuovo account con AFT, crea un file Terraform di richiesta di account. Questo file contiene l'input per i parametri nel `aft-account-requestrepository`. Dopo aver creato un file Terraform per la richiesta di account, inizia a elaborare la richiesta dell'account eseguendo `git push`. Questo comando richiama l'`ct-aft-account-request` operazione nel AWS CodePipeline, che viene creata nell'account di gestione AFT al termine del provisioning dell'account. Per ulteriori informazioni, vedete [AFT Account Provisioning Pipeline](#).

Parametri del file Terraform di richiesta dell'account

È necessario includere i seguenti parametri nel file Terraform di richiesta dell'account. È possibile visualizzare [un esempio di file Terraform di 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 `aft-account-requestrepository` includono `e. OUName OUName (OU-ID)`

- `account_tags` acquisisce chiavi e valori definiti dall'utente, che possono essere etichettati in Account AWS base a criteri aziendali. Per ulteriori informazioni, consulta [Taggare AWS Organizations le risorse 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 fornito in `/-fields/`. `aft/account-request/custom` Puoi fare riferimento a questi metadati durante le personalizzazioni dell'account per implementare i controlli appropriati. Ad esempio, un account soggetto alla conformità normativa potrebbe implementarne altri. Regole di AWS Config I metadati con cui raccogli `custom_fields` possono richiedere un'ulteriore elaborazione durante il provisioning e l'aggiornamento dell'account. Se un campo personalizzato viene rimosso dalla richiesta dell'account, il campo personalizzato viene rimosso dall'archivio dei parametri SSM per l'account fornito.
- (Facoltativo) `account_customizations_name` acquisisce la cartella del modello di account nel repository. `aft-account-customizations` Per ulteriori informazioni, consulta [Personalizzazioni dell'account](#).

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 inviate più richieste di account alla pipeline AFT, AFT mette in coda ed elabora le richieste di account secondo un ordine di primo ingresso e primo di uscita.

Note

È possibile creare un file Terraform di richiesta di account per ogni account di cui si desidera che AFT fornisca o raggruppi più richieste di account in un singolo file Terraform di richiesta di account.

Aggiorna un account esistente

Compatibilità con registrazione automatica

Se la tua organizzazione utilizza la registrazione automatica per la registrazione automatica degli account, tieni presente che AFT ha delle limitazioni all'importazione di questi account. Gli account registrati tramite Auto Enroll non dispongono dei prodotti forniti dal Service Catalog richiesti dal flusso di lavoro di importazione di AFT.

Soluzione alternativa: utilizzate la funzione Register OU per creare prodotti predisposti 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 eseguendoli. `git push` Questo comando richiama il flusso di lavoro per il 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, consulta [Fornire un nuovo account con AFT](#).

Ad esempio, per aggiornare il nome o l'indirizzo e-mail di un account AFT, è possibile definire le specifiche come `custom_fields` nel file Account Request. In questo modo, create parametri SSM, che potete 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"
}
```

È possibile 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 Account Request:

```
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 Account Request:

```
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 `aft-account-requestrepository` includono e. `OUName` `OUName` (`OU-ID`)

Aggiorna un account che AFT non fornisce

Puoi aggiornare gli account AWS Control Tower creati al di fuori di AFT specificando l'account nel `aft-account-requestrepository`.

Note

Assicurati che tutti i dettagli dell'account siano corretti e coerenti con l'organizzazione AWS Control Tower e il rispettivo prodotto AWS Service Catalog fornito.

Prerequisiti per l'aggiornamento di un sistema esistente con AFT Account AWS

- Account AWS Devono essere registrati in AWS Control Tower.
- Account AWS Devono far parte dell'organizzazione AWS Control Tower.

Versioni Terraform e AFT

Account Factory for Terraform (AFT) supporta la versione Terraform 1.6.0 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 = "1.6.0"
```

Distribuzioni Terraform

AFT supporta tre distribuzioni Terraform:

- Terraform Community Edition
- Terraform Cloud
- 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 Terraform Cloud o Terraform Enterprise, il [token API](#) che specifichi `terraform_token` deve essere un token API User o Team. Un token Organization non è supportato per tutti i requisiti. APIs 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 Terraform Cloud:
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"
```

Terraform Cloud

Quando selezionate Terraform Cloud come distribuzione, AFT crea spazi di lavoro per i seguenti componenti nella vostra organizzazione Terraform Cloud, che avvia un flusso di lavoro basato sulle API.

- 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

Terraform Cloud gestisce la configurazione dello stato Terraform risultante.

Quando selezioni Terraform Cloud come distribuzione, fornisci i seguenti parametri di input:

- `terraform_distribution = "tfc"`
- `terraform_token`— Questo parametro contiene il valore del token Terraform Cloud. 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 Terraform Cloud.

Note

Non sono supportate più implementazioni AFT in una singola organizzazione Terraform Cloud.

[Per informazioni su come configurare Terraform Cloud, consulta la documentazione di 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 un flusso di lavoro basato sull'API 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. [Fornisci 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 relativi ai dati](#)
- [AWS Piano Enterprise Support](#)
- [Eliminare il AWS VPC predefinito](#)

AWS CloudTrail eventi relativi ai 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.

Eliminare il AWS VPC predefinito

Quando abiliti questa opzione, AFT elimina tutte le AWS impostazioni predefinite VPCs nell'account di gestione AFT e in tutto Regioni AWS, anche se non sono state distribuite le risorse AWS Control Tower in tali account. Regioni AWS

AFT non elimina VPCs automaticamente le AWS impostazioni predefinite 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 VPCs, 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
}

```

Consulta [VPC predefinito e sottoreti predefinite](#) per saperne di più sulle impostazioni predefinite. VPCs

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-*
CodeBuild	Progetti di compilazione	aft-*
		ct-aft-*
		python-layer-builder-aft-common-*
Codice Pipeline	Pipelines	<i>YourAccountId</i> -customizations-pipeline

AWS service	Tipo di risorsa	Nome risorsa
Simple Storage Service (Amazon S3)	Bucket	aft-*
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-cu stomizations aft-account-provisioning-fr amework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc
Amazon SNS	Argomenti	aft-notifications aft-failure-notifications
Amazon EventBridge	Autobus per eventi	aft-events-from-ct-manageme nt

AWS service	Tipo di risorsa	Nome risorsa
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 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-CustomizationsCloud Trail
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

AWS service	Tipo di risorsa	Nome risorsa
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 politiche 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 nella gestione AFT e negli account di gestione AWS Control Tower per supportare le operazioni della pipeline AFT. Questi ruoli vengono creati sulla base del modello di accesso con privilegi minimi, che limita le autorizzazioni ai set di azioni e risorse minimamente richiesti per ogni ruolo e policy. A questi ruoli e politiche viene assegnata una `key:value` coppia di AWS tag, per quanto riguarda `managed_by:AFT` l'identificazione.

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 AWSAFTAdmin ruolo, 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 negli account forniti da AWS Control Tower e AFT, eseguendo quindi azioni relative al provisioning e alle personalizzazioni degli account.

Ecco la policy in linea (artefatto JSON) allegata 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 artefatto 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 AWSAFTExecution ruolo, spiegato

Quando si distribuisce AFT, il AWSAFTExecution ruolo viene creato negli account di gestione AFT e AWS Control Tower. Successivamente, la pipeline AFT crea il AWSAFTExecution ruolo in ogni account fornito da 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 personalizzazione del provisioning e del provisioning del framework AFT, per gli account con provisioning AFT e per gli account condivisi.

I ruoli distinti aiutano a limitare l'ambito

Come procedura ottimale, mantieni le autorizzazioni di personalizzazione separate dalle autorizzazioni consentite durante la distribuzione iniziale delle risorse. Ricorda che il AWSAFTEService ruolo è destinato al provisioning degli account e il AWSAFTExecution ruolo è destinato alla personalizzazione dell'account. 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 sull'utente.

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 viene 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 AWSAFTService ruolo, 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 utilizzate solo in base al ruolo. AWSAFTExecution

Il AWSAFTService ruolo è destinato all'utilizzo da parte dell'infrastruttura di servizio per distribuire risorse durante la fase di provisioning e deve essere utilizzato AWSAFTExecution solo per implementare 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 viene 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 per i componenti

Quando si distribuisce 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 AWS Control Tower per effettuare il provisioning degli account.
- [Amazon DynamoDB](#): AFT crea tabelle Amazon DynamoDB nell'account di gestione AFT, che memorizzano le richieste degli 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 i bucket Amazon Simple Storage Service (S3) nell'account di gestione AFT e nell'account di archivio dei log AWS Control Tower, che archiviano i log generati dai AWS servizi richiesti dalla pipeline AFT. AFT crea anche un bucket S3 di backend Terraform, primario e secondario, per archiviare gli stati Terraform generati durante i flussi di lavoro della Regioni AWS pipeline AFT.
- [Amazon Simple Notification Service](#): AFT crea argomenti Amazon Simple Notification Service (SNS) nell'account di gestione AFT, che memorizza le notifiche di successo e di fallimento 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 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 build 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 integrarle con il provider di CodeStar connessioni AWS selezionato e supportato per il codice sorgente AFT e per avviare lavori di costruzione in AWS CodeBuild.

- [AWS Lambda](#) — AFT crea funzioni e livelli AWS Lambda nell'account di gestione AFT per eseguire i passaggi durante la richiesta dell'account, il provisioning dell'account AFT e i processi di personalizzazione dell'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 archiviazione dei log di AWS Control Tower. AFT crea chiavi per crittografare gli stati 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. Per impostazione predefinita, le chiavi KMS create da AFT hanno la rotazione annuale abilitata.
- [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 con provisioning AFT, secondo necessità, 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 degli account AFT e le personalizzazioni.
- [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 di 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 AWS Control Tower, per registrare gli eventi relativi ai dati per i bucket Amazon S3 AWS e le funzioni Lambda. AFT invia questi log a un bucket S3 centrale nell'account di archiviazione 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 Basic Support abilitato.

Pipeline di fornitura degli account AFT

Una volta completata la fase di fornitura degli account della pipeline, il framework AFT continua. Esegue automaticamente una serie di passaggi per garantire che gli account appena assegnati 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 dell'account.
2. Recupera informazioni sull'account fornito, 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 AWSAFTExecutionIAM nell'account appena assegnato. AFT assume questo ruolo per eseguire la fase di personalizzazione dell'account, poiché questo ruolo garantisce l'accesso al portafoglio Account Factory.
5. Applica i tag dell'account che hai fornito come parte dei parametri di input della richiesta di account.
6. Applica le opzioni di funzionalità AFT scelte al momento della distribuzione di AFT.
7. Applica le personalizzazioni di provisioning degli account AFT fornite. La sezione successiva fornisce ulteriori informazioni su come configurare queste personalizzazioni con una macchina a stati AWS Step Functions, in un git repository. Questa fase viene talvolta definita fase del framework di provisioning degli account. Fa parte del processo di provisioning di base, ma in precedenza avete impostato un framework che fornisce integrazioni personalizzate come parte del flusso di lavoro di provisioning degli account, prima che vengano aggiunte ulteriori personalizzazioni agli account nella fase successiva.
8. Per ogni account fornito, viene creato 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 degli account per ogni account assegnato (e scelto come target).
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 effettuare 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 vostra 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 fornito, prima che inizi la fase successiva 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 aiutanti globali nella fase di personalizzazione dell'account.

Il framework di provisioning degli account AFT richiama una macchina a stati AWS Step Functions, definita dall'utente, per implementare le personalizzazioni. Consulta la [documentazione di AWS Step Functions](#) per ulteriori informazioni sulle possibili integrazioni di macchine a stati.

Ecco alcune integrazioni comuni.

- Le funzioni di AWS Lambda nella lingua che preferisci
- Attività AWS ECS o AWS Fargate, utilizzando contenitori Docker
- Attività di AWS Step Functions con worker personalizzati, ospitati in AWS o in locale
- Integrazioni Amazon SNS o SQS

Se non è definita alcuna macchina a stati AWS Step Functions, la fase passa con un no-op. Per creare una macchina a stati per il provisioning delle personalizzazioni dell'account AFT, segui le istruzioni riportate in [Crea il tuo account AFT \(provisioning customizations state machine\)](#) 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 pre-API della personalizzazione dell'account AFT. Invece, la pipeline AFT consente 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 avviare la fase di provisioning dell'account AFT, come descritto nelle sezioni seguenti.

Prerequisiti per la creazione di una macchina a stati

- Un AFT completamente distribuito. [Implementa AWS Control Tower Account Factory per Terraform \(AFT\)](#) Per ulteriori informazioni sulla distribuzione di AFT, vedere.
- Configura un git repository nel tuo ambiente per le personalizzazioni del provisioning degli account AFT. Per ulteriori informazioni, consulta [Fasi successive all'implementazione](#).

Crea il tuo account AFT (provisioning customizations state machine)

Fase 1: Modificare la definizione della macchina a stati

Modificare la definizione di macchina a `customizations.asl.json` stati di esempio. [L'esempio è disponibile nel git repository configurato per archiviare le personalizzazioni del provisioning degli account AFT, nelle fasi successive alla distribuzione](#). Consulta la [AWS Step Functions Developer Guide](#) per ulteriori informazioni sulle definizioni delle macchine a stati.

Fase 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 dell'attività della macchina a stati, includerai il `lambda.tf` file nella stessa directory. Assicurati di includere i ruoli e le autorizzazioni IAM richiesti per le configurazioni personalizzate.

Quando fornite l'input appropriato, la pipeline AFT richiama automaticamente la vostra macchina a stati e implementa le vostre personalizzazioni come parte della fase del framework di provisioning degli account AFT.

Per riavviare il framework di provisioning degli account AFT e le personalizzazioni

AFT esegue il framework di provisioning degli account e le fasi di personalizzazione per ogni account venduto attraverso 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 di richieste di account.

2. Fornisci 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 di 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. [Richiama nuovamente le 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 per la 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](#)
- gitArchivi precompilati per personalizzazioni globali e personalizzazioni degli account nell'ambiente in uso. Per ulteriori informazioni, consulta la Fase 3: Compila ogni repository. [Fasi successive all'implementazione](#)

Applica personalizzazioni globali

Per applicare personalizzazioni globali, devi inserire una struttura di cartelle specifica nel repository prescelto.

- Se le tue configurazioni personalizzate sono sotto forma di programmi o script Python, inseriscili nella cartella `api_helpers/python` nel tuo repository.
- 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 `/api_helpers` che si trova nel tuo repository. **`[account_customizations_name]`**
- Se le tue configurazioni personalizzate sono in 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.

Richiama nuovamente le personalizzazioni

AFT offre 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. Una event-source-based

nuova richiamata consente di applicare personalizzazioni a singoli account, a tutti gli account, agli account in base alla rispettiva unità organizzativa o agli account selezionati in base ai tag.

Segui questi tre passaggi per richiamare nuovamente le personalizzazioni per gli account forniti da AFT.

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 per gli account forniti da AFT.

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 nuovamente richiamata la personalizzazione per tutti gli account forniti da AFT.

Note

Se la tua versione di AWS Control Tower Account Factory for Terraform (AFT) è la 1.6.5 o successiva, puoi scegliere come target nested (OUs con la sintassi). OU Name (ou-id-1234 Per ulteriori informazioni, consulta il seguente argomento su. [GitHub](#)

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 account IDs 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 registri di emissione contenenti l'account di AWS Lambda destinazione e la richiesta di personalizzazione. IDs 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 sul framework di provisioning degli account AFT, 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.

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 [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 Gestito in modo automatico

Note

Se lo 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 lo si utilizza AWS CodeCommit, è necessario creare git repository nell'ambiente di provider VCS di terze parti supportato da AFT per i seguenti elementi.

- Richieste di account AFT. [Codice di esempio disponibile](#). Per ulteriori informazioni sulle richieste di account AFT, vedere [Fornisci 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 il tuo account AFT \(provisioning customizations state machine\)](#)
- 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", 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 supportato da AFT, aggiorna questo valore di input con il nome effettivo del repository. Per Github BitBucket, GitHub Enterprise

e GitLab Self-managed GitLab, il nome del repository deve avere lo stesso 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 supportato da AFT, aggiorna questo valore di input con il nome del repository. Per Github BitBucket, GitHub Enterprise e GitLab Self-managed GitLab, il nome del repository deve avere lo stesso 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 supportato da AFT, aggiorna questo valore di input con il nome del repository. Per Github BitBucket, GitHub Enterprise e GitLab Self-managed GitLab, il nome del repository deve avere lo stesso 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 supportato da AFT, aggiorna questo valore di input con il nome del repository. Per Github BitBucket, GitHub Enterprise e GitLab Self-managed GitLab, il nome del repository deve avere lo stesso 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 i clienti esistenti AWS CodeCommit

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.

Spostare AFT AWS CodeCommit da un altro provider VCS

Questa sezione fornisce una panoramica di 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. Aggiungi 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`
- `aft-account-customizations`
- `aft-global-customizations`
- `aft-account-provisioning-customizations`

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 `terraform plan` per visualizzare in anteprima le modifiche, quindi `terraform apply`.

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 la cartella in sospeso AWS CodeConnections per il nuovo provider VCS, come descritto in [Aggiornare una connessione in sospeso](#), o nella AWS console, []. `https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`

3. [Riferimento: fasi successive all'implementazione](#)

Note

Le pipeline degli account mantengono 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 verso un altro provider Git](#).

Protezione dei dati

Il [modello di responsabilitàAWS condivisa](#) si applica alla protezione dei dati in AFT. Ai fini della protezione dei dati, consigliamo le seguenti migliori pratiche 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 `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 Key Management Service. AWS Per impostazione predefinita, le chiavi KMS create da AFT hanno la rotazione annuale abilitata. Se scegli le distribuzioni Terraform Cloud 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 per i componenti](#) che, per impostazione predefinita, sono crittografati a riposo. Per i dettagli, consulta la AWS documentazione per ogni 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 per i componenti](#) che utilizzano la crittografia in transito, per impostazione predefinita. Per i dettagli, consulta la AWS documentazione per ogni AWS servizio componente di AFT e scopri le pratiche di protezione dei dati seguite da ciascun servizio.

Per le distribuzioni Terraform Cloud o Terraform Enterprise, AFT chiama un'API endpoint HTTPS per l'accesso alla tua organizzazione Terraform. Se scegli un provider VCS di terze parti supportato da AWS CodeStar connessioni, AFT chiama un'API di endpoint HTTPS per l'accesso all'organizzazione del tuo 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 Terraform Cloud 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: Terraform Cloud o Terraform Enterprise

Quando scegli Terraform Cloud o Terraform Enterprise, trovi una cartella per ogni account nei bucket **aft-backend-012345678901-primary-region** e **aft-backend-012345678901-secondary-region** S3. 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 ridistribuisci 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    = "xxxxxxxxxxxxx"
```

```
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 durante l'utilizzo di Account Factory for Terraform (AFT).

Argomenti

- [Problemi generali](#)
- [Problemi relativi alla fornitura/registrazione dell'account](#)
- [Problemi relativi all'invocazione delle personalizzazioni](#)
- [Problemi relativi al flusso di lavoro di personalizzazione degli account](#)

Problemi generali

- Quote di risorse superate AWS

[Se i tuoi gruppi di log indicano che hai superato le quote di AWS risorse, contatta l'assistenza AWS](#). Account Factory utilizza Servizi AWS quote di risorse che includono AWS CodeBuild, AWS Organizations, e 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 Organizations User Guide.
- [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, vedere [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 la distribuzione di Account Factory solo se possibile.

- Autorizzazioni di ruolo Account Factory insufficienti

Account Factory crea ruoli e policy IAM per gestire le implementazioni e le personalizzazioni degli account forniti. Se modifichi questi ruoli o politiche, la pipeline Account Factory potrebbe non essere in grado di eseguire determinate azioni. Per ulteriori informazioni, consulta [Ruoli obbligatori](#).

- Gli archivi degli account non sono stati compilati correttamente

Assicurati di seguire i [passaggi successivi alla distribuzione](#) prima di effettuare il provisioning degli account.

- Non viene rilevata la 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 elemento Amazon DynamoDB, non un account diretto. Dopo che un elemento è stato modificato, 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 alla fornitura/registrazione dell'account

- La richiesta di account (indirizzo e-mail/nome) esiste già

Il problema in genere causa un guasto del prodotto Service Catalog durante il provisioning o durante il provisioning. `ConditionalCheckFailedException`

Puoi trovare ulteriori informazioni sul problema effettuando una delle seguenti operazioni:

- Controlla i tuoi gruppi di log Terraform o CloudWatch Logs.
- Esamina gli errori che vengono emessi 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 [terraform-aws-control-tower-account-factory](#) su GitHub

- Quote di risorse Exceeded AWS Organizations

Assicurati che la richiesta del tuo account non superi le quote di AWS Organizations risorse. Per ulteriori informazioni, vedere [Quotas for AWS Organizations](#).

Problemi relativi all'invocazione delle personalizzazioni

- Account Target non registrato su 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 è destinata la richiesta di personalizzazione esiste nella **aft-request-metadata** tabella DynamoDB, ma non nell'archivio delle richieste di account

Formattate la richiesta di chiamata di personalizzazione per escludere l'account incriminato effettuando una delle seguenti operazioni:

- Nella `aft-request-metadata` tabella DynamoDB, elimina la voce che fa riferimento all'account che non si trova più nell'archivio delle richieste dell'account.
 - Non usare «tutti» come obiettivo.
 - Non si rivolge all'unità organizzativa a cui appartiene l'account.
 - Non mirare direttamente all'account.
 - Token errato utilizzato per Terraform Cloud
- Assicurati di aver impostato il token corretto. Terraform Cloud supporta solo token basati sul team, non token basati sull'organizzazione.
- Impossibile creare l'account 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 di 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 DynamoDB.

[Per informazioni sulla versione 1.8.0 di AFT, consultate la release 1.8.0 su GitHub](#)

Per informazioni su come controllare e aggiornare la versione di AFT in uso, consultate 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 la richiesta di personalizzazione. IDs Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi](#) alla tracciabilità delle richieste di personalizzazione dell'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 (OUs), 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 eventuali deviazioni, 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 del 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 trasferito da un altro OUs (vedi [Deriva dell'ereditarietà sulle linee di base abilitate](#) [Variazione 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 SCPs e AWS Config le regole implementati con devono sempre essere rimossi manualmente quando un account cambia. OUs

Esempi di deviazione delle politiche

- 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 dei propri account e OUs tramite la console oppure APIs identificare quando le configurazioni dell'account e dell'unità organizzativa 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 dell'unità organizzativa e dello spostamento dell'account nella console, vai alla pagina Organizzazione, quindi seleziona gli OUs account che desideri controllare.

Per visualizzare lo stato di drift OUs e gli account a livello di programmazione, 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, usa il flag. `ListEnabledBaselines includeChildren` Puoi filtrare in base a questi stati e visualizzare solo gli account OUs 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. APIs (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, puoi scegliere Registra nuovamente l'unità organizzativa nella console. Se la deriva è causata da un singolo account, puoi scegliere Aggiorna account nella console. Per risolvere la deriva della linea di base con APIs, 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 dispone di meno di 1000 account, è possibile risolvere il problema relativo agli account forniti da Account Factory, o alla deriva da SCP, selezionando Registra nuovamente l'unità organizzativa nella pagina Organizzazione o nella pagina dei dettagli dell'unità organizzativa.
- Potresti riuscire a 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 deriva di base OUs e gli account possono essere risolti chiamando [l'ResetEnabledBaselineAPI](#) o scegliendo Re-register OU o Update account nella console AWS Control Tower.
- Per risolvere il problema della deriva ereditaria che si verifica quando gli account vengono trasferiti da un account all'altro OUs, puoi 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 la deriva in una versione con landing zone, sono possibili due comportamenti.

- Se utilizzi la versione più recente della landing zone, quando scegli Reset e poi scegli Confirm, le risorse della tua drifted landing zone vengono ripristinate alla configurazione AWS Control Tower salvata. La versione landing zone rimane la stessa.
- Se non utilizzi la versione più recente, devi scegliere Aggiorna. La landing zone viene aggiornata alla versione più recente della landing zone. La deriva viene risolta come parte di questo processo.

Considerazioni sulla deriva e sulla scansione delle politiche

AWS Control Tower analizza quotidianamente le policy gestite SCPs e dichiarative per verificare che i controlli corrispondenti siano applicati correttamente e che non abbiano subito variazioni. RCPs 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 ciascuno di essi APIs può essere chiamato. 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 le tue SCPs policy e quelle dichiarative tramite chiamate 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. RCPs

In rare situazioni, questo limite può essere raggiunto chiamando lo stesso APIs ripetutamente, tramite una soluzione di terze parti o uno script personalizzato scritto da te. Ad esempio, se tu e AWS Control Tower effettuate la stessa chiamata nello stesso momento (entro 1 secondo) e vengono raggiunti i limiti TPS, le chiamate successive vengono limitate. AWS Organizations APIs 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 dei dati attivi di recente. OUs
2. Per ogni unità organizzativa registrata, recupera tutto ciò che SCPs è gestito da AWS Control Tower e collegato all'unità organizzativa. SCPs I Managed hanno identificatori che iniziano con. `aws-guardrails`

3. Per ogni controllo preventivo abilitato sull'unità organizzativa, verifica che la dichiarazione sulla politica del controllo sia presente nell'unità organizzativa gestita dall'unità organizzativa. SCPs

Un'unità organizzativa può averne una o più gestite SCPs.

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 aggiuntive OUs: 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 gli account condivisi da Foundational OUs con la AWS Organizations console o APIs, 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.
- Cambia il nome degli account dei membri in Non-Foundational OUs.
- Cambia il nome degli account condivisi di AWS Control Tower nell'unità organizzativa di sicurezza.
- Elimina 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 da OUs un account all'altro 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 [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 OUs SCPs, si verifica quando 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 con più di LZ4 0 anni 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 in modo specifico sugli account Foundational e condivisi. OUs

- [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 (RCPs), le politiche dichiarative e i controlli che fanno parte dello standard AWS Security Hub CSPM gestito dai servizi: AWS Control Tower.

- [Deriva di controllo CSPM del Security Hub](#)
- [Controlla la deriva delle politiche](#)

Derivazione 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 la differenza di ereditarietà per le baseline abilitate (configurazioni delle risorse) su tali account. OUs [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 e sugli account. OUs

- [Variazione dell'ereditarietà sui controlli abilitati](#)

Deriva che non viene 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. AWSControl TowerBaseline

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 for the OU** 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: [Esegui il provisioning 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 Re-register OU 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 tua 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 di drift per gli account e OUs, consulta. [Se gestisci risorse al di fuori 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 programmaticamente utilizzando o uno degli AWS CLI AWS. SDKs 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 lo 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 ad AWS Control Tower Foundational OUs, come l'unità organizzativa Security. Può verificarsi se un'unità organizzativa Foundational viene eliminata al di fuori della console AWS Control Tower. Foundational OUs non può essere spostato 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 OUs solo per Foundational, la risoluzione è quella di aggiornare la landing zone. Quando OUs vengono eliminati altri tipi di file, AWS Control Tower viene aggiornato automaticamente.

Per ulteriori informazioni sulla risoluzione di drift per gli account e OUs, consulta. [Se gestisci risorse al di fuori di AWS Control Tower](#)

Deriva di controllo CSPM del Security Hub

Questo tipo di deriva si verifica quando un controllo che fa parte del 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 deviazione 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 OUs chi ha meno di 1000 account, la soluzione consigliata è chiamare l'ResetEnabledControlAPI per il controllo della deriva. Nella console, è possibile selezionare Re-register for the OU, che ripristina il controllo allo stato originale. In alternativa, per qualsiasi unità organizzativa, puoi rimuovere e riattivare il controllo tramite la console o AWS Control Tower APIs, che ripristina anche il controllo.

Per ulteriori informazioni sulla risoluzione di drift per gli account e, consulta. OUs [Se gestisci risorse al di fuori 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 (RCPs) 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 basati su SCP.

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`

Se hai meno OUs di 1000 account, un'altra soluzione della console o dell'API consiste nel registrare nuovamente l'unità organizzativa, che ripristina il controllo allo stato originale.

Per ogni singola unità organizzativa, puoi rimuovere e riattivare il controllo tramite la console o AWS Control Tower APIs, che ripristina anche il controllo.

Per ulteriori informazioni sulla risoluzione di drift per gli account e, consulta. OUs [Se gestisci risorse al di fuori 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 OUs. 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 a livello di AWS Control Tower OUs e degli account.

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 risoluzione della console è registrare nuovamente l'unità organizzativa o aggiornare l'account.

Visualizza e risolvi la deriva a livello di codice

Per visualizzare lo stato della deriva a livello di codice, puoi chiamare l'[ListEnabledBaselines](#) API per visualizzare gli stati delle linee di base abilitate sul tuo. OUs Per visualizzare gli stati dei singoli account in modo programmatico con l'API, usa il flag. `ListEnabledBaselines includeChildren`

Puoi risolvere questo tipo di deriva a livello di codice, chiamando l'API. [ResetEnabledBaseline](#)

Variazione dell'ereditarietà sui controlli abilitati

Questo tipo di deriva può verificarsi a livello di AWS Control Tower OUs e degli account.

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 pagina Organizations, nella pagina Enabled controls e nella pagina dei dettagli dell'account. La soluzione della console è registrare nuovamente l'unità organizzativa o aggiornare l'account.

Visualizza e risolvi la deriva a livello di codice

Per visualizzare a livello di codice lo stato di deriva ereditato per i controlli abilitati, puoi chiamare l'[ListEnabledControls](#) API per visualizzare gli stati dei controlli abilitati sul tuo. OUs Per visualizzare gli stati dei singoli account in modo programmatico con l'API, usa il flag. `ListEnabledControls includeChildren`

Puoi risolvere questo tipo di deriva ereditaria a livello di codice, chiamando l'API.

[ResetEnabledControl](#)

EventBridge creazione

Note

EventBridge è abilitato solo per i clienti con versioni LZ4 superiori a 0.

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 al di fuori 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 o all'esterno di AWS Control Tower. Il modo più comune per modificare le risorse al di fuori di AWS Control Tower è la AWS Organizations console. Questo argomento descrive come riconciliare le modifiche alle risorse AWS Control Tower quando le apporti al di fuori di AWS Control Tower.

La ridenominazione, l'eliminazione e lo spostamento di risorse all'esterno della console AWS Control Tower causano la mancata sincronizzazione della console. Molte modifiche possono essere riconciliate automaticamente. Alcune modifiche richiedono il ripristino della landing zone per aggiornare le informazioni visualizzate nella console AWS Control Tower.

In generale, le modifiche apportate all'esterno della console AWS Control Tower alle risorse AWS Control Tower creano uno stato di deriva risolvibile nella tua landing zone. Per ulteriori informazioni su queste modifiche, vedi [Modifiche riparabili alle risorse](#).

Attività che richiedono il ripristino della landing zone

- Eliminazione dell'unità organizzativa di sicurezza (un caso speciale, da non fare alla leggera).
- Rimozione di un account condiviso dall'unità organizzativa di sicurezza (non consigliata).
- Aggiornamento, collegamento o scollegamento di un SCP associato all'unità organizzativa di sicurezza.

Modifiche 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, consulta la sezione [Aggiornamento dei prodotti forniti nella documentazione](#). AWS Service Catalog

Riferimento a risorse esterne a AWS Control Tower

Quando crei nuovi account OUs e al di fuori di AWS Control Tower, questi non sono governati da AWS Control Tower, anche se possono essere visualizzati.

Creazione di una UO

Le unità organizzative (OUs) create al di fuori di AWS Control Tower vengono chiamate non registrate. Vengono visualizzati nella pagina Organizzazione, ma non sono regolati dai controlli di 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 Enroll account.

Modifica esterna dei nomi delle risorse AWS Control Tower

Puoi modificare i nomi delle unità organizzative (OUs) e degli account al di fuori 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 al di fuori di AWS Control Tower, la console AWS Control Tower riflette automaticamente la modifica del nome. Tuttavia, se effettui il provisioning dei tuoi account utilizzando AWS Service Catalog, devi anche reimpostare la landing zone per assicurarti che AWS Control Tower rimanga coerente AWS Organizations. Il flusso di lavoro Reset garantisce la coerenza tra i servizi Foundational e Additional OUs. Puoi risolvere questo tipo di deriva dalla pagina delle impostazioni della zona di atterraggio. Vedi la sezione chiamata «Risolvere la deriva» in [Rileva e risolvi la deriva in AWS Control Tower](#)

AWS Control Tower visualizza i nomi di OUs nella pagina Organizzazione nella dashboard di AWS Control Tower. Puoi vedere quando l'operazione di ripristino della landing zone 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 dei costi e fatturazione AWS console. Quando rinomini 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 [Managing an AWS account](#) nella AWS Billing User Guide.

Eliminazione dell'unità organizzativa di sicurezza

Questo tipo di deviazione è un caso speciale. Se elimini la Security OU, vedrai una pagina con un messaggio di errore che ti chiede di reimpostare la landing zone. Devi reimpostare la landing zone prima di poter intraprendere qualsiasi altra azione in AWS Control Tower.

- Non potrai 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 atterraggio, dove troverai il pulsante Reset.

In questa situazione, il processo di ripristino della landing zone 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 deviati. Lo stesso processo risolve il problema di questi account.

Se ritieni necessario eliminare l'unità organizzativa di sicurezza, ecco cosa devi sapere:

Prima di poter eliminare l'unità organizzativa di sicurezza, è necessario assicurarsi 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'operazione 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 gli account condivisi dall'organizzazione o spostarli dall'unità organizzativa di sicurezza. Se hai rimosso accidentalmente un account condiviso, puoi seguire i passaggi di riparazione descritti in questa sezione per ripristinare l'account.

- Dalla console AWS Control Tower: per avviare il processo di riparazione, segui i passaggi di riparazione semimanuali. 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 AWS Organizations console.
- 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 di un ruolo con la policy `AWSControlTowerServiceRolePolicy` gestita o equivalente e l'autorizzazione per eseguire tutte le azioni AWS Control Tower (`controltower: *`).
- Se le procedure di riparazione non ripristinano l'account, contatta. 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 policy di controllo dei servizi (SCPs). Risultato: le risorse create da AWS Control Tower nell'account possono essere modificate o eliminate.
- L'account non fa più parte dell'account AWS Organizations di gestione. Risultato: l'amministratore dell'account di AWS Organizations gestione non ha più visibilità sulla spesa dell'account.
- Non è più garantito il monitoraggio dell'account 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 presente 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 di 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 Detected, scegli Re-Invita per rimediare alla rimozione dell'account condiviso invitando nuovamente l'account condiviso a far parte dell'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#/inviti>
 - Se hai accesso al messaggio e-mail inviato quando hai nuovamente invitato l'account, accedi all'account rimosso, quindi fai clic sul link contenuto 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 a 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 Reset per ripristinare la landing zone.

5. Attendi il completamento del processo di ripristino.

Se la riparazione ha esito positivo, l'account condiviso appare in uno stato e in conformità normali.

Se le procedure di riparazione non ripristinano 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 rientrare nell'organizzazione. Per informazioni sui requisiti, i prerequisiti e la procedura per invitare un account a AWS Organizations, vedi [Invitare un AWS account alla 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#/inviti per accettare> l'invito.
4. Accedi nuovamente all'account di gestione.
5. Accedi alla console AWS Control Tower come utente o ruolo con la policy `AWSControlTowerServiceRolePolicy` gestita o equivalente e le autorizzazioni per eseguire tutte le azioni AWS Control Tower (`controltower: *`).
6. Vedrai la pagina Landing zone drift con un'opzione per reimpostare la landing zone. Scegli Reset per ripristinare la landing zone.
7. Attendi il completamento del processo di ripristino.

Se la riparazione ha esito positivo, l'account condiviso appare in uno stato e in conformità normali.

Se le procedure di riparazione non ripristinano 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 della console. Pertanto, gli indirizzi e-mail condivisi e gli altri account vengono aggiornati e visualizzati in modo coerente in AWS Control Tower dopo averli modificati.

Note

In AWS Service Catalog, Account Factory visualizza i parametri specificati nella console al momento della creazione di un prodotto fornito. 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 al di fuori della console AWS Control Tower.

Eliminazione di risorse AWS Control Tower all'esterno di AWS Control Tower

Puoi eliminare OUs account in AWS Control Tower e non è necessario 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, è possibile rimuovere le unità organizzative vuote (OUs) utilizzando l'API o la console. OUs che contengono account non possono essere eliminati.

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 registrate OUs rimanga coerente.

 Note

Nel AWS Service Catalog, Account Factory viene aggiornato per rimuovere l'unità organizzativa eliminata dall'elenco delle unità disponibili OUs in cui è possibile effettuare 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

Nel 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 TAIANTED 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 (OUs) e gli account che crei in AWS Control Tower sono governati automaticamente da AWS Control Tower. Inoltre, se disponi di account esistenti OUs o creati al di fuori 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. È inoltre possibile registrare gli account singolarmente. Per ulteriori informazioni sulla registrazione di singoli account, vedere. [Informazioni sulla registrazione di account esistenti](#)

Terminologia

- Quando si porta un'organizzazione esistente in AWS Control Tower, si tratta di registrare l'organizzazione o estendere la governance all'organizzazione.
- Quando si inserisce un AWS account in AWS Control Tower, si parla di registrazione dell'account.

Visualizza i tuoi OUs e i tuoi account

Nella pagina AWS Control Tower Organization, puoi visualizzare tutti i OUs componenti della tua azienda AWS Organizations, compresi OUs quelli registrati presso AWS Control Tower e quelli non registrati. Puoi visualizzare nested OUs come parte della gerarchia. Un modo semplice per visualizzare le unità organizzative nella pagina Organizzazione consiste nel selezionare solo le unità organizzative 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 registrazione in AWS Control Tower. Un modo semplice per visualizzare i tuoi account nella pagina Organizzazione consiste nel selezionare Solo account dal menu a discesa in alto a destra. È possibile visualizzare, aggiornare e registrare gli account singolarmente all'interno di OUs, se gli account soddisfano i prerequisiti per l'iscrizione.

Se non si seleziona alcun filtro, nella pagina Organizzazione vengono visualizzati gli account in base a una gerarchia. OUs È una posizione centrale per monitorare e intraprendere azioni su tutte le risorse AWS Control Tower. Per ulteriori informazioni sulla pagina Organizzazione, puoi visualizzare la guida video.

 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.

Procedura guidata: video

Questo video (4:01) descrive come utilizzare la pagina Organization 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.

[Guida video sulla pagina Working with the Organization in AWS Control Tower.](#)

Argomenti

- [Registra un'unità organizzativa esistente con AWS Control Tower](#)
- [Informazioni sulla registrazione di account esistenti](#)

Estendi la governance a un'organizzazione esistente

Puoi aggiungere la governance di AWS Control Tower a un'organizzazione esistente configurando una landing zone (LZ) come indicato nella Guida per l'utente di AWS Control Tower in [Getting Started, Step 2](#).

Ecco cosa aspettarti quando configuri la landing zone di AWS Control Tower in un'organizzazione esistente.

- Puoi avere una landing zone 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 audit e un account di registrazione.

- I limiti di servizio dell'organizzazione devono consentire la creazione di questi due account aggiuntivi.
- Dopo aver lanciato la landing zone o registrato un'unità organizzativa, i controlli di AWS Control Tower si applicano automaticamente a tutti gli account registrati in quell'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 aggiungerne altri OUs in AWS Control Tower e registrare quelli esistenti OUs.

Per verificare altri prerequisiti per la registrazione e l'iscrizione, consulta [Getting Started with AWS Control Tower](#).

Ecco ulteriori dettagli su come i controlli di AWS Control Tower non si applicano alle OUs organizzazioni AWS che non dispongono di zone di destinazione 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 in OUs che non sono registrati presso AWS Control Tower non sono vincolati dai controlli, a meno che non vengano specificamente registrati in AWS Control Tower. Per ulteriori informazioni sulla registrazione degli account, consulta [Informazioni sulla registrazione di account esistenti](#).
- Le organizzazioni esistenti aggiuntive, gli account esistenti e qualsiasi account nuovo OUs o creato al di fuori di AWS Control Tower non sono vincolati dai controlli di AWS Control Tower, a meno che non registri separatamente l'unità organizzativa o registri l'account.

Per ulteriori informazioni su come applicare AWS Control Tower agli account esistenti OUs , consulta [Registra un'unità organizzativa esistente con AWS Control Tower](#).

Per una panoramica del processo di configurazione di una landing zone AWS Control Tower nella tua organizzazione esistente, guarda il video nella sezione successiva.

Note

Durante la configurazione, AWS Control Tower esegue controlli preliminari per evitare problemi comuni. Tuttavia, se attualmente utilizzi la soluzione AWS Landing Zone per AWS Organizations, contatta il tuo AWS architetto della soluzione prima di provare ad abilitare AWS Control Tower nella tua organizzazione per determinare se AWS Control Tower possa

interferire con l'attuale implementazione della landing zone. Inoltre, vedi [Se l'account non soddisfa i prerequisiti](#) per informazioni sullo spostamento degli account da una landing zone all'altra.

Video: Attivazione di una zona di atterraggio esistente AWS Organizations

Questo video (7:48) descrive come configurare e abilitare una landing zone 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 AWS IAM Identity Center (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 utilizzi IAM Identity Center Directory, AWS Control Tower aggiunge risorse come set di autorizzazioni, gruppi e così via, e procede come al solito.
- Se è configurata un'altra directory (esterna, AD, Managed AD), AWS Control Tower non modifica la configurazione esistente. Per ulteriori dettagli, consultare [Considerazioni per i clienti AWS IAM Identity Center \(IAM Identity Center\)](#).

Accesso ad altri AWS servizi

Dopo aver introdotto la tua organizzazione nella governance di AWS Control Tower, potrai comunque accedere a tutti AWS i servizi disponibili tramite AWS Organizations, tramite la AWS Organizations console e APIs. Per ulteriori informazioni, consulta [Servizi AWS correlati](#).

Annidato OUs in AWS Control Tower

Questo capitolo elenca le aspettative e le considerazioni di cui dovresti essere consapevole quando lavori con nested OUs in AWS Control Tower. In molti modi, lavorare con nested OUs equivale a lavorare con una struttura di unità organizzative piatta. Le funzionalità Register e Re-register funzionano con nested OUs, 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.

[Guida video sulla gestione di Nested OUs in AWS Control Tower.](#)

Per indicazioni sulle migliori pratiche per nested OUs e la landing zone, consulta il post sul blog [Organizing your AWS Control Tower landing zone with OUs nested.](#)

Espandi da una struttura OU piatta a una struttura di unità organizzative annidata

Se hai creato la landing zone di AWS Control Tower con una struttura di unità organizzative piatta, puoi espanderla in una struttura di unità organizzative annidata.

Questo processo prevede quattro fasi principali:

1. Crea la struttura di unità organizzative annidate desiderata in AWS Control Tower.
2. Vai alla AWS Organizations console e usa la 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 in quanto AWS Control Tower non dispone della funzionalità Move.

3. Vai all'unità organizzativa annidata in AWS Control Tower e registrala o registrala nuovamente. Verranno registrati tutti gli account dell'unità organizzativa annidata.
 - Se hai creato l'unità organizzativa in AWS Control Tower, registra nuovamente 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 AWS Control Tower.

Controlli preliminari della registrazione delle unità organizzative annidate

Per supportare la corretta registrazione dei tuoi account nested OUs e dei relativi account membri, AWS Control Tower esegue una serie di controlli preliminari. Questi stessi controlli preliminari vengono eseguiti quando si registra qualsiasi unità organizzativa di primo livello o unità organizzativa annidata. Per ulteriori informazioni, vedere [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 alcuni 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.

Nested e ruoli OUs

AWS Control Tower distribuisce il `AWSControlTowerExecution` ruolo sugli account all'interno dell'unità organizzativa di destinazione e su tutti gli account OUs annidati all'interno dell'unità organizzativa di destinazione, anche quando l'intenzione è quella di registrare solo l'unità organizzativa di destinazione. Questo ruolo fornisce a qualsiasi utente dell'account di gestione le autorizzazioni di amministratore su qualsiasi account che ricopra il ruolo. `AWSControlTowerExecution` Il ruolo può essere utilizzato per eseguire azioni che normalmente non sarebbero consentite dai controlli di 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 il genitore diretto OUs, a meno che non ripristini il ruolo sull'account. Per eliminare il `AWSControlTowerExecution` ruolo da un account, devi aver effettuato l'accesso al `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 dei ruoli](#).

Cosa succede durante la registrazione e la nuova registrazione degli account nested OUs and

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 svolge le seguenti attività

- Aggiunge il `AWSControlTowerExecution` ruolo a tutti gli account non registrati in questa unità organizzativa e a tutti gli account non registrati nella relativa unità organizzativa. OUs
- Registra gli account dei membri che non sono registrati.
- Registra nuovamente gli account dei membri registrati.
- Crea un accesso a IAM Identity Center per gli account dei membri appena registrati.
- Aggiorna gli account dei membri registrati esistenti in base alle modifiche apportate alle landing zone.
- Aggiorna i controlli configurati per questa unità organizzativa e i relativi account membri.

Considerazioni sulla registrazione di unità organizzative annidate

- Non è possibile registrare un'unità organizzativa nell'unità organizzativa principale (Security OU).
- Nested OUs deve essere registrato separatamente.
- Non è possibile registrare un'unità organizzativa a meno che non sia registrata l'unità organizzativa principale.
- Non è possibile registrare un'unità organizzativa a meno che tutte le unità OUs 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 sotto un'unità organizzativa superiore spostata, ma la deriva non viene riparata da tale azione.

Limitazioni dell'unità organizzativa annidata

- OUs può essere annidato a una profondità massima di 5 livelli sotto la radice.

- Nidato OUs sotto l'unità organizzativa di destinazione deve essere registrato o registrato nuovamente separatamente.
- Se l'unità organizzativa di destinazione si trova al livello 2 o inferiore nella gerarchia, ovvero se non è un'unità organizzativa di livello superiore, i controlli preventivi abilitati su quella superiore OUs vengono applicati automaticamente a questa unità organizzativa e a tutte le OUs unità al di sotto di essa.
- Gli errori di registrazione delle unità organizzative non si propagano all'interno dell'albero gerarchico. È possibile visualizzare i dettagli sugli stati di nested nella pagina dei dettagli dell' OUs unità organizzativa principale.
- Gli errori di registrazione delle unità organizzative non si propagano lungo l'albero gerarchico.
- AWS Control Tower non modifica le impostazioni del VPC per account nuovi o esistenti.

Nested e conformità OUs

Dalla console AWS Control Tower, puoi visualizzare OUs gli account non conformi nella pagina Organizzazione, in modo da comprendere la conformità su larga scala.

Considerazioni sulla conformità per nested e account OUs

- La conformità di un'unità organizzativa non è determinata in base alla conformità dell'unità OUs annidata al suo interno.
- Lo stato di conformità di un controllo viene calcolato OUs su tutti gli elementi su cui il controllo è abilitato, incluso il controllo annidato. OUs Scopri [lo stato di conformità di AWS Control Tower OUs e gli account](#).
- Un'unità organizzativa viene indicata come non conforme solo se ha account non conformi, indipendentemente da dove si trova l'unità organizzativa nella gerarchia delle unità organizzative.
- 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 dei dettagli dell'account, è possibile visualizzare un elenco di risorse non conformi che potrebbero causare lo stato di non conformità dei propri account. OUs

Annidato e alla deriva OUs

In determinate situazioni, la deriva può impedire la registrazione di Nested. OUs

Aspettative relative alla deriva e alla nidificazione OUs

- È possibile attivare i controlli OUs con i genitori alla deriva, ma non su drifted direttamente. OUs
- È consentito abilitare i controlli investigativi su un'unità organizzativa alla deriva, purché non si tratti di un'unità organizzativa alla deriva di primo livello.
- I controlli obbligatori sono abilitati solo al livello superiore. OUs I controlli obbligatori vengono ignorati quando si registra un'unità organizzativa annidata.
- Un controllo obbligatorio protegge AWS Config le risorse; pertanto, tale controllo deve avvenire in uno stato di non deriva per consentire la registrazione di sistemi annidati. OUs In caso di deviazione, AWS Control Tower blocca la registrazione di nested. OUs
- Se l'unità organizzativa di primo livello è alla deriva, il controllo che protegge le AWS Config risorse potrebbe andare alla deriva. 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.

Nested OUs e controlli

Quando si abilita un controllo su un'unità organizzativa registrata, i controlli preventivi e investigativi hanno comportamenti diversi. I controlli annidati e OUs proattivi si comportano in modo simile ai controlli investigativi.

Controlli preventivi

- I controlli preventivi vengono applicati su OUs nested.
- I controlli preventivi obbligatori vengono applicati a tutti gli account dell'unità organizzativa e dei relativi account annidati. OUs
- I controlli preventivi riguardano tutti gli account e sono OUs annidati nell'unità organizzativa di destinazione, anche se tali account non OUs sono registrati.

Controlli investigativi e proattivi

- I Nested OUs non ereditano automaticamente i controlli investigativi o proattivi; questi devono essere abilitati separatamente.
- I controlli investigativi e proattivi vengono utilizzati solo sugli account registrati nelle regioni operative della tua zona di atterraggio.

Stati di controllo ed ereditarietà abilitati

È possibile visualizzare i controlli ereditati per ogni unità organizzativa nella pagina dei dettagli dell'unità organizzativa.

Tip

È possibile utilizzare l'ereditarietà dei controlli per mantenere la quota SCP di un'unità organizzativa. Ad esempio, è possibile abilitare un controllo nell'unità organizzativa di livello superiore di una gerarchia di unità organizzative, anziché abilitare direttamente un'unità organizzativa annidata.

Stato 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 è applicato su questa unità organizzativa, indipendentemente dallo stato in cui è impostato su un'altra. OUs
- Lo stato Fallito indica che il controllo non è applicato su questa unità organizzativa, indipendentemente dallo stato dell'unità organizzativa su un'altra. OUs

Note

Lo stato Ereditato indica che il controllo è stato applicato a un'unità organizzativa superiore nell'albero ed è applicato a questa unità organizzativa, ma non è stato aggiunto direttamente a questa unità organizzativa.

Se la tua landing zone non è la versione attuale

Ogni riga della tabella Controlli abilitati rappresenta un controllo abilitato su una singola unità organizzativa.

Nidato OUs e radice

La radice non è un'unità organizzativa e non può essere registrata o ri-registrata. Inoltre, non è possibile creare account direttamente nella directory principale. La radice non può essere non conforme o avere uno stato del ciclo di vita, ad esempio registrata o in deriva.

Tuttavia, la radice è il contenitore di primo livello per tutti gli account e. OUs Nel contesto di nidificato OUs, è il nodo in cui OUs sono annidati tutti gli altri.

Registra un'unità organizzativa esistente con AWS Control Tower

Un modo efficace per portare 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 landing zone di AWS Control Tower. Puoi registrare account OUs 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, i relativi account membro vengono registrati nella landing zone di AWS Control Tower. Sono regolati dai controlli che si applicano alle rispettive unità organizzative.

A partire dalla versione 4.0 di Landing Zone, è possibile 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 la registrazione in AWS Config. `ConfigBaseline` Per ulteriori informazioni, consulta [Tipi di linee di base](#) e [La guida di riferimento ai controlli di AWS Control Tower](#).

Note

Se non disponi già di una landing zone AWS Control Tower, inizia configurando una landing zone, in una nuova organizzazione creata da AWS Control Tower o in un' AWS Organizations organizzazione esistente. Per maggiori dettagli su come configurare una landing zone, 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 lo stack sugli 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 sull'unità organizzativa e su tutti i relativi account al momento della registrazione dell'unità organizzativa.

Registrazione parziale degli account dopo la registrazione di un'unità organizzativa

È possibile registrare correttamente un'unità organizzativa, 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 come parte del processo Register OU non riesce, lo stato dell'account nella pagina degli account mostra Iscrizione non riuscita. È inoltre possibile visualizzare le informazioni sull'account nella pagina dell'unità organizzativa, ad esempio 4 su 5, nel campo account.

Ad esempio, se vedi 4 su 5, significa che l'unità organizzativa ha 5 account in totale e 4 di essi sono stati registrati con successo, ma un account non è riuscito a registrarsi durante la procedura di registrazione dell'unità organizzativa. Puoi scegliere Re-Register OU per attivare la registrazione degli account, dopo esserti assicurato che soddisfino i prerequisiti di registrazione.

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 disponi già Admin delle autorizzazioni. In caso contrario, la creazione dei prodotti forniti avrà esito negativo durante la registrazione. L'errore si verifica perché AWS Control Tower si basa sulle credenziali dell'utente IAM o sull'identità utente IAM Identity Center durante 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 selezionando 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 AWS Control Tower, nella pagina Organizzazione, puoi visualizzare tutti gli account OUs e gli account della tua organizzazione in una gerarchia, compresi OUs quelli registrati con AWS Control Tower e quelli non registrati.

In generale, i non registrati OUs sono stati creati in AWS Organizations e non sono governati da nessun'altra landing zone. È possibile registrare account esistenti OUs 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 quell'unità organizzativa.
4. Nella pagina dei dettagli dell'unità organizzativa, in alto a destra, puoi selezionare Register OU dal menu a discesa Azioni.

Il processo di registrazione richiede almeno 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 APIs

Per registrare un'unità organizzativa esistente presso AWS Control Tower APIs, puoi chiamare l'EnableBaselineAPI con il `AWSControlTowerBaseline` comando `baselineIdentifier` sul campo. Per ulteriori informazioni, consulta [Registrare un'unità organizzativa AWS Control Tower APIs solo con](#).

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 singoli account. I guardrail vengono applicati e le informazioni sulle attività degli account vengono riportate agli account di controllo e registrazione.

Tra gli altri risultati si annoverano i seguenti:

- `AWSControlTowerExecution` consente il controllo da parte dell'account di controllo AWS Control Tower.
- `AWSControlTowerExecution` aiuta a configurare la registrazione della tua organizzazione, in modo che tutti i log di ogni account vengano inviati all'account di registrazione.
- `AWSControlTowerExecution` assicura che i controlli AWS Control Tower selezionati si applichino automaticamente a ogni singolo account nel tuo OUs account e a ogni nuovo account che crei in AWS Control Tower.

Per un'unità organizzativa registrata, puoi fornire report di conformità e sicurezza basati sulle 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 su drift, consulta [Rileva e risolvi la deriva in AWS Control Tower](#)

Note

Una situazione insolita può verificarsi quando AWS Control Tower visualizza i display OUs e i relativi account. Se hai creato un account in un'unità organizzativa registrata e successivamente trasferisci quell'account registrato in un'altra unità organizzativa non registrata, in particolare se utilizzi l'account AWS Organizations per spostare l'account, puoi vedere il risultato «1 di 0» account nella pagina dei dettagli dell'unità organizzativa. Inoltre, è possibile che l'utente abbia creato un altro account non registrato in quell'unità organizzativa non registrata. Se è presente un account non registrato, la console potrebbe indicare «1 di 1» per l'unità organizzativa. Sembrerà che l'account singolo (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 Organizzazione.
2. Seleziona Crea unità organizzativa dal menu a discesa Crea risorse in alto a destra.

3. Specificare un nome nel campo Nome unità organizzativa.
4. Nel menu a discesa Parent OU, puoi vedere la gerarchia dei registrati. OUs Seleziona un'unità organizzativa principale per la nuova unità organizzativa che stai creando.
5. Scegliere Aggiungi.

Tip

Per aggiungere un'unità organizzativa nidificata in meno passaggi, seleziona il nome dell'unità organizzativa principale mostrato nella tabella della pagina Organizzazione, visualizza la pagina dell'unità organizzativa principale, quindi scegli Aggiungi un'unità organizzativa dal menu a discesa Azioni in alto a destra. La nuova unità organizzativa viene creata automaticamente come unità organizzativa nidificata nell'unità organizzativa selezionata.

Note

Se la tua landing zone non è aggiornata, vedrai un elenco semplice anziché una gerarchia nel menu a discesa. Anche se la tua landing zone include unità organizzative annidate OUs, non vedrai le unità organizzative L5 nel menu a discesa, perché non puoi creare una nuova unità organizzativa al di sotto di un'unità organizzativa L5. Per ulteriori informazioni su nested OUs in AWS Control Tower, consulta [Annidato OUs in AWS Control Tower](#).

Rimuovere un'unità organizzativa

AWS Control Tower supporta azioni separate da 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

- L'unità organizzativa deve essere priva di account affinché le operazioni di eliminazione e annullamento della registrazione abbiano esito positivo.
- 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 annullandone 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 vengano rimossi dall'unità organizzativa.
5. Torna alla pagina Organizzazione e seleziona il pulsante di opzione accanto all'unità organizzativa.
6. Seleziona Annulla registrazione dell'unità organizzativa dal menu a discesa Azioni in alto a destra.
7. Fermati qui se non desideri eliminare completamente l'unità organizzativa, ma solo cancellarla da AWS Control Tower. Per eliminare completamente l'unità organizzativa, procedi 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'unità organizzativa nel suo complesso è stata registrata correttamente. In questi casi, è necessario risolvere l'errore di controllo 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 membro fallisce, AWS Control Tower restituisce messaggi di errore per gli account membri interessati. È possibile visualizzare i messaggi di errore nella pagina dei dettagli dell'unità organizzativa, in cui una tabella aggrega i precontrolli e i messaggi di errore dell'account. Se un'operazione di registrazione dell'unità organizzativa non riesce, la tabella mostra tutti i messaggi di errore per tutti gli account dell'unità organizzativa. Se necessario, è inoltre possibile 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 landing zone attuale o aggiornala alla versione più recente.

Errori OU

- Supera il numero massimo di SCPs

È possibile che tu abbia superato il limite delle politiche di controllo del servizio (SCPs) per unità organizzativa o che sia stata raggiunta un'altra quota. Il limite di 5 SCPs unità organizzative si applica a tutte le unità OUs presenti nella landing zone di AWS Control Tower. Se disponi SCPs di più di quanto consentito dalla quota, devi eliminare o combinare SCPs.

- Conflittuante SCPs

La versione esistente SCPs può essere applicata all'unità organizzativa o all'account, il che impedisce ad AWS Control Tower di registrare l'account. Verifica la policy applicata SCPs per eventuali policy che potrebbero impedire il funzionamento di AWS Control Tower. Assicurati di controllare quelle ereditate dai OUs vertici della gerarchia. SCPs

- Supera la quota impostata dallo stack

La quota dello stack set potrebbe essere stata superata. Se hai più istanze di quelle consentite dalla 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 dell'account

- Controlli preliminari impediti sugli account

Un SCP esistente sull'unità organizzativa impedisce ad AWS Control Tower di effettuare controlli preliminari sugli account dei membri dell'unità organizzativa. Per risolvere questo errore di controllo preliminare, aggiorna o rimuovi SCP dall'unità organizzativa.

- Errore relativo all'indirizzo e-mail

L'indirizzo e-mail 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 Config o canale di distribuzione 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 gestito le risorse, prima di poter registrare un account.

- STS disabilitato

AWS Security Token Service (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 tra IAM Identity Center

La regione principale di AWS Control Tower non è la stessa della regione AWS IAM Identity Center (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 tematico Amazon Simple Notification Service (Amazon SNS) che AWS Control Tower deve utilizzare. AWS Control Tower crea risorse (come argomenti SNS) con nomi specifici. Se questi nomi sono già utilizzati, la configurazione di AWS Control Tower fallisce. 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 incluso nel portfolio

Aggiungi l'utente AWS Identity and Access Management (IAM) al portafoglio 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 esistente Account AWS e registralo](#)

Ti ricordiamo che AWS CloudTrail si attiva automaticamente su tutti i tuoi AWS account quando li registri in AWS Control Tower. Se CloudTrail è abilitato su un account precedente alla registrazione, potrebbe verificarsi una doppia fatturazione a meno che non lo CloudTrail disattivi prima di iniziare la procedura 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:

- Registrare nuovamente 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 AWS Control Tower OUs e gli account

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 Registra nuovamente o Ripristina.
- Se hai più di un'unità organizzativa registrata nella tua landing zone, registra nuovamente o ripristina tutte le tue OUs 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 AWSControl TowerBaseline 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 i tuoi account e OUs.

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 AWSControl TowerBaseline è abilitata sull'unità organizzativa, seleziona Registra nuovamente l'unità organizzativa in Azioni. Se non AWSControl TowerBaseline 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 Stato indica se l'account è attualmente registrato presso AWS Control Tower (registrato), se l'account non è mai stato registrato (non registrato) o se l'iscrizione non è riuscita in precedenza (registrazione non riuscita).
- Quando registri nuovamente l'unità organizzativa, il **AWSControlTowerExecution** ruolo viene aggiunto a tutti gli account con lo stato Non registrato o Registrazione non riuscita.
- AWS Control Tower crea un accesso Single Sign-On (IAM Identity Center) per i nuovi account registrati.
- Gli account registrati vengono registrati nuovamente in AWS Control Tower.
- Gli eventuali controlli preventivi applicati all'unità organizzativa sono corretti, in quanto SCPs 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 di 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 riporta il StackSet - AWSControl TowerExecutionRole. 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 AWSControl TowerBaseline abilitato. Se un'unità organizzativa non dispone dell' AWSControlTowerBaseline opzione abilitata, è possibile attivare la registrazione automatica dell'account o utilizzare ResetEnabledBaseline e attivare

EnabledBaselines e ResetEnabledControl APIs EnabledControls attivare l'unità organizzativa per registrare gli account. Per i dettagli di, vedere: AWSControl TowerBaseline [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.

Servizi integrati

AWS Control Tower è un servizio che si basa su altri AWS servizi, per aiutarti a configurare un ambiente ben architettato. Questo capitolo fornisce una breve panoramica di questi servizi, incluse informazioni di configurazione sui servizi sottostanti e su come funzionano in AWS Control Tower.

[Per ulteriori informazioni su come misurare un ambiente ben architettato, consulta lo strumento Well-Architected AWS](#) . Consulta anche la [Management and Governance](#) Cloud Environment Guide.

Argomenti

- [AWS Opzioni di backup disponibili](#)
- [Distribuisci 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 elaborazione serverless con Lambda](#)
- [Gestisci gli account tramite AWS Organizations](#)
- [Archivia oggetti con Amazon S3](#)
- [Monitora il tuo ambiente con Security Hub CSPM](#)
- [Fornisci 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 landing zone di AWS Control Tower. Puoi incorporare un flusso di lavoro di backup e ripristino dei dati direttamente nella tua landing zone. Il piano di backup include regole predefinite, come i giorni di conservazione, la frequenza di backup e la finestra temporale durante la quale viene eseguito il backup. Per ulteriori informazioni, consulta [AWS Backup e AWS Control Tower](#).

Distribuisci ambienti con CloudFormation

CloudFormation consente di creare e fornire implementazioni di AWS infrastrutture in modo prevedibile e ripetuto. Ti aiuta a sfruttare AWS i prodotti per creare applicazioni altamente affidabili, altamente scalabili ed economiche 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 (una pila). Per ulteriori informazioni, consulta la Guida per l'utente di [AWS CloudFormation](#).

AWS Control Tower utilizza CloudFormation stackset per applicare i controlli sugli account. Per ulteriori informazioni sulla collaborazione tra AWS Control Tower CloudFormation e AWS, consulta [Crea AWS Control Tower risorse con AWS CloudFormation](#).

Monitora gli eventi con CloudTrail

AWS Control Tower si configura AWS CloudTrail per abilitare la registrazione e il controllo 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 richiesto AWS APIs i servizi di supporto CloudTrail, l'indirizzo IP di origine da cui sono state effettuate le chiamate e l'ora in cui sono avvenute le chiamate. È possibile integrarsi CloudTrail nelle applicazioni utilizzando l'API, automatizzare la creazione di percorsi per l'organizzazione, controllare lo stato dei percorsi e controllare il modo in cui gli amministratori attivano e CloudTrail disattivano la registrazione. 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 [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 visualizzazione dettagliata delle risorse associate all' AWS account, incluso il modo in cui 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 etichettate automaticamente con `aws-control-tower` e hanno un valore `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 controlli investigativi. Per ulteriori informazioni, consulta Informazioni [sui controlli in AWS Control Tower](#).

Integrazione di AWS Config nella Control Tower Landing Zone 4.0

Aggregatore di configurazione collegato ai servizi (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 AWS Config aggregator diventa l'amministratore delegato di AWS Config
- AWS Control Tower configura automaticamente le impostazioni di amministrazione delegate
- 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 di organizzazioni 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 dei dati migliorata

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 all'interno dell'organizzazione
- Supporta controlli perimetrali avanzati 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 configurato automaticamente come amministratore delegato
- Non è richiesta alcuna azione aggiuntiva da parte dei clienti per questa configurazione
- Per i clienti esistenti, il precedente account di integrazione di Security Roles (account Audit) verrà configurato come account aggregatore centrale AWS Config durante l'aggiornamento di Landing Zone 4.0

Ambito di aggregazione dei dati

- Service-Linked Config Aggregator può aggregare i dati di configurazione da:
 - Account gestiti Control Tower
 - Account non gestiti da Control Tower

- Qualsiasi account con un registratore Config attivo nell'organizzazione

Controlli di accesso

- L'accesso ai dati aggregati è gestito tramite policy IAM
- L'account aggregatore centrale AWS Config ha accesso centralizzato a tutti i dati aggregati.
- Gli account dei membri mantengono i propri registratori AWS Config individuali

Best practice

Selezione degli account di Config Central Aggregator

- Scegli un account dedicato al monitoraggio della sicurezza e della conformità
- Assicurati che siano in atto controlli di accesso adeguati
- Prendi in considerazione l'utilizzo di un account di controllo o di sicurezza esistente

Gestione dei dati

- Esamina regolarmente i dati di configurazione aggregati
- Implementa politiche di conservazione appropriate
- Monitora lo stato del registratore AWS Config su tutti gli account

Impatto sulla migrazione

Durante l'aggiornamento a Landing Zone 4.0:

Prima della migrazione

- Documenta le regole e gli aggregatori AWS Config esistenti
- Rivedi gli attuali modelli di accesso ai dati di AWS Config
- Pianifica gli eventuali aggiornamenti necessari delle policy IAM

Durante la migrazione

- Gli aggregatori AWS Config legacy verranno rimossi automaticamente

- Verrà distribuito Service-Linked Config Aggregator
- Verrà configurato l'amministratore delegato

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 controllare l'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 landing zone, puoi creare AWS IAM Identity Center 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. I tuoi 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 a 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 [AWS IAM Identity Center](#).

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 in merito AWS KMS, consulta la [AWS KMS Developer Guide](#).

Per informazioni su come configurare le AWS KMS chiavi con AWS Control Tower, consulta [Configurazione facoltativa AWS KMS delle chiavi](#).

Esegui funzioni di elaborazione serverless con Lambda

Con AWS Lambda, puoi eseguire codice senza fornire o gestire server. È possibile eseguire codice per molti tipi di applicazioni o servizi di backend, senza bisogno di sovraccarichi amministrativi aggiuntivi. Quando carichi il codice, Lambda può eseguire e scalare il codice con un'elevata disponibilità. Puoi configurare il codice in modo che venga attivato automaticamente da altri AWS servizi oppure puoi chiamarlo direttamente da qualsiasi app web o mobile.

Ad esempio, è possibile assumere determinati ruoli nell'account di audit AWS Control Tower a livello di codice, 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 da creare e gestire centralmente. Con Organizations, puoi creare account membro 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 sono raggruppati in gruppi logici, chiamati unità organizzative (OU). Per ulteriori informazioni su Organizations, consulta la [AWS Organizations User Guide](#).

AWS Control Tower utilizza quanto segue OUs:

- Root: il contenitore principale per tutti gli account e tutti gli altri OUs nella landing zone.
- Sicurezza: questa unità organizzativa contiene l'account di archiviazione dei log, l'account di controllo e le risorse di cui sono proprietari.
- Sandbox: questa unità organizzativa viene creata quando configuri la landing zone. In esso e negli altri bambini OUs presenti nella tua landing zone sono presenti i tuoi account utente. Questi sono gli account a cui gli utenti finali accedono per eseguire operazioni sulle AWS risorse.

 Note

Puoi aggiungerne altri OUs nella tua landing zone tramite la console AWS Control Tower nella pagina Unità organizzative.

Considerazioni

OUs i sistemi creati tramite AWS Control Tower possono avere dei controlli applicati. OUs per impostazione predefinita, non possono essere creati al di fuori di AWS Control Tower. Tuttavia, è possibile registrarli OUs. Dopo aver registrato un'unità organizzativa, è possibile applicare controlli all'unità organizzativa e ai relativi account. Per informazioni sulla registrazione di un'unità organizzativa, consulta [Registrazione 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 landing zone, viene creato un bucket Amazon S3 nel tuo account di archiviazione dei log per contenere tutti i log di tutti gli account nella tua landing zone.

Monitora il tuo ambiente con Security Hub CSPM

AWS Control Tower è integrato con AWS Security Hub CSPM tramite lo standard CSPM Security Hub denominato Service-Managed Standard: AWS Control Tower. Per ulteriori informazioni, vedere [Security Hub standard](#).

Fornisci 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 distribuiti utilizzando risorse AWS.

Puoi controllare gli utenti che hanno accesso a prodotti specifici, il che ti consente di far rispettare 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, vedere [Service Catalog Administrator Guide](#).

In AWS Control Tower, gli amministratori cloud centrali e gli utenti finali possono effettuare il provisioning di account personalizzati nella landing zone utilizzando AWS Service Catalog prodotti, chiamati blueprint personalizzati. [Per ulteriori informazioni, consulta Step2. Crea il AWS Service Catalog prodotto](#).

Puoi interagire con gli account AWS Control Tower tramite la AWS Service Catalog console e APIs. Per ulteriori informazioni, consulta [Interagisci con gli account AWS Control Tower da AWS Service Catalog](#)

AWS Control Tower può anche utilizzare il Service Catalog APIs per automatizzare ulteriormente il provisioning e l'aggiornamento degli account. Per i dettagli, consulta [la AWS Service Catalog Developer Guide](#).

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 audit. Questi avvisi ti aiutano a prevenire la deriva all'interno della tua landing zone. 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 le notifiche di conformità di controllo di AWS Control Tower (nel tuo account di audit) è abbonarsi `AggregateConfigurationNotifications`. È un servizio che ti aiuta a controllare 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` conduce al tuo account di controllo.

Crea applicazioni distribuite con AWS Step Functions

AWS Step Functions semplifica il coordinamento dei componenti delle applicazioni distribuite come 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 landing zone, come il provisioning degli account in Account Factory o la creazione di nuove unità organizzative (OUs) nella console AWS Control Tower, puoi farlo AWS Identity and Access Management (IAM) o AWS IAM Identity Center 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 credenziali fornite dall'amministratore.

Dopo aver autenticato la tua identità, IAM controlla il tuo accesso AWS con un set definito di autorizzazioni su un insieme 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](#)
- [Utilizzo di AWS IAM Identity Center e AWS Control Tower](#)
- [Panoramica della 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

Hai accesso a AWS uno qualsiasi dei seguenti tipi di identità:

- AWS account utente root: la prima volta che si crea un AWS account, si inizia con un'identità che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è chiamata 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. Rispetta invece la [best practice di utilizzare l'utente root solo per creare il primo utente IAM Identity Center \(consigliato\) o utente IAM \(non è una best practice nella maggior parte dei casi d'uso\)](#). 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. È possibile 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 Support Center. AWS le migliori pratiche consigliano di creare un utente IAM Identity Center anziché un utente IAM, poiché esiste 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. È possibile utilizzare questi tasti quando si chiamano AWS i servizi a livello di codice, tramite uno dei numerosi tasti SDKs 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 il [processo di firma della versione 4 di Signature nella Guida](#) generale. 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 ciò che l'identità può e non può fare. 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: invece di creare un utente IAM, puoi utilizzare le identità esistenti della tua directory utenti aziendale o di un provider di identità web. Directory Service 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 sull'account dell'utente per conto dell'utente. Quando configuri alcuni ambienti AWS di servizio, devi 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 Guida per l'utente IAM.

- 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 effettuano richieste AWS CLI o API. AWS È preferibile alla memorizzazione delle chiavi di accesso all'interno dell'istanza Amazon EC2. Per assegnare un AWS ruolo a un'istanza Amazon EC2 e renderlo disponibile per tutte le sue applicazioni, crei 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 IAM Identity Center è controllata dalla directory collegata a IAM Identity Center. Tuttavia, l'autorizzazione agli AWS account disponibili per gli utenti finali dall'interno del portale utenti 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](#) per l'AWS IAM Identity Center 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 i [set di autorizzazioni nella Guida](#) per l'AWS IAM Identity Center utente.

Controllo accessi

Per creare, aggiornare, eliminare o elencare risorse AWS Control Tower o altre AWS risorse nella tua landing zone sono necessarie le autorizzazioni per eseguire l'operazione e le 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 della gestione delle autorizzazioni di accesso alle risorse AWS Control Tower](#)
- [Utilizzo di policy basate sull'identità \(policy IAM\) per AWS Control Tower](#)

Utilizzo di 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 aver aggiunto gli utenti finali al gruppo AWSAccountFactory, possono creare nuovi utenti IAM Identity Center dalla procedura guidata Account Factory. Per ulteriori informazioni, consulta [Fornitura e gestione degli 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 AWS IAM Identity Center 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'AWS IAM Identity Center 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 [Best practice](#) nella Guida per l'utente di IAM Identity Center.

I seguenti gruppi vengono creati quando configuri la landing zone.

AWSAccountFabbrica

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 effettuare il provisioning di nuovi account a meno che non appartengano anche al gruppo AWSAccountFactory.

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 dei 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 registri	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 dei membri	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.

AWSSecurityRevisori

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 dei 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 della gestione delle autorizzazioni di accesso alle risorse AWS Control Tower

Ogni AWS risorsa è di proprietà di un Account AWS utente e le autorizzazioni per creare o accedere a una risorsa sono regolate dalle 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'associazione di politiche 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 sei responsabile della concessione delle autorizzazioni a un utente o a un ruolo, devi conoscere e tenere traccia degli utenti e dei ruoli che richiedono autorizzazioni, delle risorse per le quali ogni utente e ruolo richiede 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](#)
- [Specificate gli elementi della 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 landing zone. 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 landing zone esistente. I controlli possono essere definiti sottorisorse.

Le risorse e le sottorisorse AWS sono associate a Amazon Resource Names (ARNs) univoci, come illustrato nell'esempio seguente.

AWS Control Tower fornisce una serie di operazioni API per lavorare con le risorse AWS Control Tower. Per un elenco delle operazioni disponibili, consulta AWS Control Tower [the AWS Control Tower API Reference](#).

Per ulteriori informazioni sulle CloudFormation risorse in AWS Control Tower, consulta [la Guida AWS CloudFormation per l'utente](#).

Informazioni sulla proprietà delle risorse

L'AWS account possiede le 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 utente root del tuo AWS account per configurare una landing zone, il tuo AWS account è il proprietario della risorsa.
- Se crei un utente IAM nel tuo AWS account e concedi le autorizzazioni per configurare una landing zone a quell'utente, l'utente può configurare una landing zone purché il suo account soddisfi i prerequisiti. Tuttavia, il tuo AWS account, a cui appartiene l'utente, possiede la risorsa landing zone.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per configurare una landing zone, chiunque possa assumere il ruolo può configurare una landing zone. Il tuo AWS account, a cui appartiene il ruolo, possiede la risorsa landing zone.

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 politiche associate a un'identità IAM sono denominate politiche basate sull'identità (politiche 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](#)
- [Policy basate sulle risorse](#)

Informazioni sulle politiche basate sull'identità (politiche IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Associa una policy 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, come la configurazione di una landing zone, puoi allegare una policy di autorizzazione 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 su più 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 attribuisce una politica 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 politica identifica l'Account B come il 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 dell'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: AWS IAM Identity Center

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 AWS IAM Identity Center .

- 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)

Creare un ruolo per una (console IAM) Servizio AWS

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 policy di fiducia richiesta dal servizio.
5. Scegli Next (Successivo).
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 collegare 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 Next (Successivo).
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 account e non possono essere resi unici 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'utilizzo dei tag in IAM, consulta [Tags 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 da utilizzare nei modelli. CloudFormation

Per fare ciò, nell'editor delle politiche scegli Azioni, quindi scegli Genera modello. CloudFormation Per ulteriori informazioni CloudFormation, consulta il [riferimento al tipo di AWS Identity and Access Management risorsa](#) 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'utilizzo dei tag in IAM, consulta [Tags for AWS Identity and Access Management resources](#) in the 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 Policy editor, 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. Potete usare 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 istruzione 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:

- Scegli Aggiungi ARNs per specificare le risorse in base ai rispettivi Amazon Resource Names (ARN). È possibile utilizzare l'editor o l'elenco ARNs ARN visivo manualmente. Per ulteriori informazioni sulla sintassi ARN, consulta [Amazon Resource Names \(ARNs\)](#) nella IAM User

Guide. Per informazioni sull'utilizzo ARNs 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. È inoltre possibile utilizzare condizioni di uso comune per limitare l'autenticazione di un utente 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 gli elenchi di tutte le chiavi di contesto che è possibile utilizzare in una condizione di policy, vedere [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. Scegli la chiave di condizione, il qualificatore e l'operatore della condizione, quindi inserisci un valore. Per aggiungere più di un valore, seleziona Aggiungi. Puoi considerare i valori come collegati da un operatore logico OR. 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 ulteriori informazioni CloudFormation, consulta il [riferimento al tipo di AWS Identity and Access Management risorsa](#) 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'utilizzo dei tag in IAM, consulta [Tags for AWS Identity and Access Management resources](#) in the IAM User Guide.
13. Seleziona Crea policy per salvare la nuova policy.

Per concedere l'accesso programmatico

Gli utenti necessitano di un accesso programmatico se desiderano interagire con l' AWS esterno di 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	Segui le istruzioni per l'interfaccia che desideri utilizzare.

Quale utente necessita dell'accesso programmatico?	Per	Come
	firmare le richieste programmatiche a,, o. AWS CLI AWS SDKs AWS APIs	• Per la AWS CLI, consulta Login for AWS local development nella Guida per l'AWS Command Line Interface utente. • Per AWS SDKs, consulta Login for AWS local development nella AWS SDKs and Tools Reference Guide.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee e per firmare richieste programmatiche a AWS CLI, AWS SDKs, o. AWS APIs	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, vedere Configurazione dell'uso AWS IAM Identity Center nella AWS CLI Guida per l'utente.AWS Command Line Interface • Per AWS SDKs gli strumenti e AWS APIs, consulta l'autenticazione di IAM Identity Center nella Guida di riferimento AWS SDKs and Tools.
IAM	Utilizza credenziali temporanee e per firmare le richieste programmatiche a AWS CLI, AWS SDKs, o. AWS APIs	Seguendo le istruzioni riportate in Utilizzo delle credenziali temporanee con le AWS risorse nella Guida per l'utente IAM .

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche a AWS CLI,, AWS SDKs o. AWS APIs	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per AWS SDKs gli strumenti , consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli strumenti e agli AWS SDKs strumenti. • Per AWS APIs, consulta la sezione Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Proteggiti dagli aggressori

Per ulteriori informazioni su come contribuire alla protezione dagli aggressori quando concedi autorizzazioni ad altri responsabili del AWS servizio, consulta [Condizioni opzionali](#) per le relazioni di fiducia tra ruoli. Aggiungendo determinate condizioni alle policy, puoi contribuire a prevenire un tipo specifico di attacco, noto come attacco secondario confuso, che si verifica se un'entità costringe un'entità con più privilegi a eseguire un'azione, ad esempio con l'impersonificazione tra servizi diversi. 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.

Policy basate sulle risorse

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.

Specificate gli elementi della policy: azioni, effetti e principi

Puoi configurare e gestire la tua landing zone tramite la console AWS Control Tower o [la landing zone APIs](#). Per configurare la tua landing zone, devi essere un utente IAM con autorizzazioni amministrative come definito in una policy IAM.

I seguenti elementi sono quelli 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.
- **Principio:** nelle politiche basate sull'identità (politiche IAM), l'utente a cui è associata 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 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 puoi utilizzare a seconda delle esigenze. 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 del vice. Quando un servizio chiama un altro servizio, si verifica un'impersonificazione tra servizi se un servizio manipola un altro servizio affinché utilizzi le proprie autorizzazioni per agire sulle risorse del 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 autorizzazione legittima possano accedere alle risorse del tuo account.

Ti consigliamo di utilizzare le `aws:SourceAccount` condizioni `aws:SourceArn` e nelle tue policy, per limitare le autorizzazioni che AWS Control Tower concede a un altro servizio per l'accesso alle tue risorse.

- `aws:SourceArn` Utilizzalo se desideri associare una sola risorsa all'accesso tra servizi.
- Utilizza `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 quando vengono 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 policy basate sull'identità che dimostrano come un amministratore di account può associare policy di autorizzazione 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 consultare prima 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 della 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 configuri una landing zone. 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 a set minimi di azioni e risorse.

Tre ruoli obbligatori per l'accesso alle landing zone

- [AWS ControlTowerAdmin ruolo](#)
- [AWS ControlTowerStackSetRole](#)

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 politica.

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 le chiama `controlcatalog` APIs per recuperare determinati metadati di controllo, quindi le autorizzazioni AWS Control Tower non sono sufficienti.

Per ulteriori informazioni su come aggiornare le autorizzazioni, consulta [Creare](#) ruoli e assegnare autorizzazioni.

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 [Control Catalog APIs](#).

AWS ControlTowerAdmin ruolo

Questo ruolo fornisce ad AWS Control Tower l'accesso all'infrastruttura fondamentale per il mantenimento della landing zone. Il `AWS ControlTowerAdmin` ruolo richiede una policy gestita allegata e una policy di trust dei ruoli per il ruolo IAM. Una policy di fiducia nei ruoli è una politica basata sulle risorse, che specifica quali dirigenti possono assumere il ruolo.

Ecco un esempio di frammento di questa policy sulla 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 politiche IAM.

1. Una politica 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` Si tratta di 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, AWS Organizations nonché account e unità organizzative OUs () governati da AWS Control Tower.

Gli aggiornamenti a questa policy gestita sono riepilogati nella tabella, . [Policy gestite per AWS Control Tower](#)

Per ulteriori informazioni, vedere [AWS ControlTowerServiceRolePolicy](#) la AWS Managed Policy Reference Guide.

Politica sulla 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 selezioni IAM Identity Center come provider di identità durante la configurazione (o l'aggiornamento) della landing zone in AWS Control Tower, questa policy viene allegata al `AWS ControlTowerAdmin` ruolo.

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 CloudTrail Tower è una best practice e fornisce questo ruolo a CloudTrail. CloudTrail assume questo ruolo per creare e pubblicare i CloudTrail 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 CloudWatch Amazon Logs per conto di AWS Control Tower. Questa policy gestita sostituisce la policy in linea

utilizzata in precedenza per questo ruolo, consentendo AWS di aggiornare la policy senza l'intervento del cliente.

Per ulteriori informazioni, consulta [AWS ControlTowerCloudTrailRolePolicy](#) la AWS Managed Policy Reference Guide.

Gli aggiornamenti a questa politica gestita sono riepilogati nella tabella, [Policy gestite per AWS Control Tower](#).

Note

Prima dell'introduzione della politica gestita, questo ruolo utilizzava una politica in linea con autorizzazioni equivalenti. La politica in linea è stata sostituita dalla politica 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 Blueprint Hub designato, all'interno della stessa organizzazione.

Role name (Nome ruolo)

Il nome del ruolo deve essere AWS ControlTowerBlueprintAccess.

Politica di fiducia nei ruoli

Il ruolo deve essere impostato in modo da considerare attendibili i 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 basata sui 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 politica 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 landing zone, come la notifica di risorse alla deriva.

Il ruolo `AWSServiceRoleForAWSControlTower` richiede una policy gestita allegata e una policy di trust dei ruoli per il ruolo IAM.

Policy gestita per questo ruolo: `AWSControlTowerAccountServiceRolePolicy`

Politica di fiducia nei 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 configurazione automatica degli account e 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 standard gestito dal servizio Security Hub CSPM: AWS Control Tower e impedisce modifiche che limitano la capacità di gestire gli account dei clienti. Fa parte di un processo di rilevamento delle AWS Security Hub CSPM deviazioni in background che non viene avviato direttamente da un cliente.

La policy concede le autorizzazioni per creare EventBridge regole Amazon, in particolare per i controlli CSPM di Security Hub, in ogni account membro e queste regole devono specificare un valore esatto. EventPattern Inoltre, una regola può funzionare solo su regole gestite dal responsabile del nostro servizio.

Responsabile del servizio: `controltower.amazonaws.com`

Per ulteriori informazioni, consulta [AWS ControlTowerAccountServiceRolePolicy](#) la AWS Managed Policy Reference Guide.

Gli aggiornamenti a questa politica gestita sono riepilogati nella tabella, [Policy gestite per AWS Control Tower](#).

Policy gestite per AWS Control Tower

AWS affronta 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 ControlTowerAccountServiceRolePolicy : aggiornamento a 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.	23 marzo 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 1 StringEquals a 1 ForAllValues:StringEquals per un migliore controllo della corrispondenza dei modelli di evento mantenendo le stesse autorizzazioni funzionali.	30 dicembre 2025
AWS ControlTowerAccountServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto una nuova policy che estende le seguenti autorizzazioni: • AWS Config autorizzazioni per creare, etichettare, eliminare, gestire e leggere	10 novembre 2025

Modifica	Descrizione	Data
	un aggregatore di configurazione collegato al servizio • AWS Config autorizza zioni per descrivere tutti gli aggregatori di configurazione • AWS Organizations autorizzazione a elencare gli amministratori delegati per AWS Config • AWS Organizations permesso di descrivere l'organizzazione • CloudFormation autorizza zioni per gestire gli hook collegati ai servizi	

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy — Politica gestita aggiornata	AWS Control Tower ha aggiornato il pattern di risorse Amazon CloudWatch Logs AWS ControlTowerServiceRolePolicy per supportare l'AWS CloudTrail integrazione opzionale di Landing Zone 4.0. Il modello è cambiato da <code>aws-controltower/CloudTrailLogs:*</code> a <code>aws-controltower/CloudTrailLogs:*</code> , aggiungendo successivamente un carattere jolly <code>CloudTrailLogs</code> per consentire la gestione di gruppi di log con qualsiasi suffisso. 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 è abilitata, i gruppi di log di Amazon CloudWatch Logs vengono ricreati con suffissi unici per evitare conflitti di denominazione. L'aggiornamento è retrocompatibile con le distribuzioni esistenti.	31 ottobre 2025

Modifica	Descrizione	Data
AWS ControlTowerCloudTrailRolePolicy — Nuova politica gestita	AWS Control Tower ha introdotto la policy AWS ControlTowerCloudTrailRolePolicy gestita, che consente di CloudTrail creare flussi di log e pubblicare eventi di log in gruppi di log CloudWatch Amazon Logs gestiti da Control Tower. Questa policy gestita sostituisce la policy in linea precedentemente utilizzata da AWS ControlTowerCloudTrailRole, permettendo di aggiornare la policy senza l'intervento del AWS cliente. La policy si applica ai gruppi di log con nomi che corrispondono allo schema. <code>aws-controltower/CloudTrailLogs*</code>	31 ottobre 2025

Modifica	Descrizione	Data
AWS ControlTowerIdentityCenterManagementPolicy — Una nuova politica	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 durante la registrazione automatica degli account. Questa modifica è necessaria affinché i clienti possano configurare IAM Identity Center in AWS Control Tower e che AWS Control Tower possa porre rimedio alla deriva della registrazione automatica.	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 dello 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	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di abilitare e disabilitare le regole collegate ai servizi AWS Config . Questa modifica è necessaria per consentire ai clienti di gestire i controlli implementati dalle regole di Config.	5 giugno 2025
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate al AWS CloudFormation servizio APIs ActivateType e SetTypeConfiguration così viaAWS::ControlTower types . DeactivateType Questa modifica consente ai clienti di fornire controlli proattivi senza la distribuzione di tipi di CloudFormation Hook privati.	10 dicembre 2024

Modifica	Descrizione	Data
AWS ControlTowerAccountServiceRolePolicy — Una nuova politica	AWS Control Tower ha aggiunto un nuovo ruolo collegato ai servizi che consente ad AWS Control Tower di creare e gestire regole relative agli eventi e, sulla base di tali regole, di gestire il rilevamento delle deviazioni per i controlli correlati a Security Hub CSPM. Questa modifica è necessari a per consentire ai clienti di visualizzare le risorse alla deriva nella console, quando tali risorse sono correlate ai controlli CSPM di Security Hub che fanno parte del Security Hub CSPM Service-managed Standard: AWS Control Tower.	22 maggio 2023

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate al servizio di Account Management EnableRegion ListRegions , e GetRegionOptStatus APIs implementate dal servizio di gestione degli AWS account, per rendere Regioni AWS disponibile l'opt-in per gli account dei clienti nella landing zone (account di gestione, account di archivio dei log, account di audit, account membri dell'OU). Questa modifica è necessaria in modo che i clienti possano avere la possibilità di espandere la governance della regione tramite AWS Control Tower alle regioni opt-in.	6 aprile 2023

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	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 Service Catalog. AWS Control Tower si assume il <code>AWSControlTowerBlueprintAccess</code> ruolo di svolgere tre attività: creare un Service Catalog Portfolio, aggiungere il prodotto blueprint richiesto e condividere il portafoglio con un account membro richiesto al momento del provisioning dell'account. Questa modifica è necessaria per consentire ai clienti di fornire account personalizzati tramite AWS Control Tower Account Factory.	28 ottobre 2022

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di configurare AWS CloudTrail percorsi a livello di organizzazione, a partire dalla versione 3.0 della landing zone. La CloudTrail funzionalità basata sull'organizzazione richiede che i clienti abbiano abilitato l'accesso affidabile e per il CloudTrail servizio e l'utente o il ruolo IAM deve avere l'autorizzazione per creare un percorso a livello di organizzazione nell'account di gestione.	20 giugno 2022

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy : aggiornamento di una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ai clienti di utilizzare la crittografia a chiave KMS. La funzionalità KMS consente ai clienti di fornire la propria chiave KMS per crittografare i propri log. CloudTrail. I clienti possono anche modificare la chiave KMS durante l'aggiornamento o la riparazione della landing zone. Quando si aggiorna la chiave KMS, sono AWS CloudFormation necessarie le autorizzazioni per chiamare l'API. <code>AWS CloudTrail PutEventSelector</code>. La modifica alla politica consente al <code>AWS ControlTowerAdmin</code> ruolo di chiamare l' <code>AWS CloudTrail PutEventSelector</code> API.	28 luglio 2021
AWS Control Tower ha iniziato a tracciare le modifiche	AWS Control Tower ha iniziato a tracciare le modifiche per le sue policy 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 conformitàAWS](#). 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 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 maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal

modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, 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 AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando 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 (SSE-S3) a 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 i 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 AWS per creare applicazioni conformi allo standard HIPAA.
- [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 [Come funzionano AWS le regioni 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 le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare [AWS Security Token Service](#) (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: configurazione di 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 e inserirli nei log, in modo da poter eseguire più facilmente il debug di un errore multipunto, se ne 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 [AWS](#) Control Tower APIs. 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 delle notifiche AWS 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.

Percorsi a livello di organizzazione

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 nell'account di controllo

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 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.

Questa policy non influisce sulla funzionalità dei carichi di lavoro esistenti. La politica è illustrata nell'esempio che segue.

```
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: AWSS3ConfigBucketExistenceCheck
  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: 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

Per ulteriori informazioni su questa chiave condizionale, consulta la documentazione IAM e il post sul blog IAM intitolato "Use scalable controls for AWS services access your resources».

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 EC2 istanze Amazon e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- Amazon CloudWatch Events offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. CloudWatch Events consente 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 registro da EC2 istanze Amazon e altre fonti. CloudTrail CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).
- 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 Le funzionalità di Logs 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 un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Control Tower. CloudTrail acquisisce le azioni per AWS Control Tower come eventi. Se crei un trail, 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, è possibile determinare la richiesta effettuata ad AWS Control Tower, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

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 evento 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 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 di landing zone, AWS Control Tower creava una traccia degli account dei membri. Quando esegui l'aggiornamento alla versione 3.0, il CloudTrail percorso viene aggiornato per diventare un percorso organizzativo. Per le migliori pratiche per spostarsi tra i percorsi, consulta [Creazione di un percorso organizzativo](#) nella Guida CloudTrail per l'utente.

Consigliato: crea un percorso

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per AWS Control Tower, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un 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:

Pubblico APIs

- Per un elenco completo degli AWS Control Tower pubblici APIs e dettagli su ciascuno di essi, consulta [The AWS Control Tower API Reference](#). Le chiamate verso questi utenti pubblici APIs vengono registrate da AWS CloudTrail.

Altro APIs

- 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 perché accesso negato o elaborata correttamente.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Esempio: voci dei file di log di AWS Control Tower

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail 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 all'account di archiviazione dei log.

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 AWS Config di distribuzione in tutti gli account registrati. Attraverso questo canale di distribuzione, registra tutte le modifiche registrate AWS Config nell'account di archiviazione dei log, dove vengono archiviate in una cartella in un bucket Amazon Simple Storage Service.

Gestisci AWS Config i 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, ne AWS Config genera cinque CIs, uno per ogni regione. Altre risorse globali, come le zone ospitate su 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 i dati del AWS Config registratore sugli account registrati

AWS Config è integrato in CloudWatch modo da poterli visualizzare AWS Config CIs in 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 i dati del AWS Config 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](#).

Visualizza i 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.

AWS Config Costi elevati

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 Cls. 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 AWS Config cui opera:

- `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 landing zone, 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 fornito ai servizi Amazon e EventBridge Amazon CloudWatch Events. Nota: per ricevere gli eventi del ciclo di vita EventBridge, devi disporre di un AWS CloudTrail percorso attivo con la registrazione abilitata. Per ulteriori informazioni sugli eventi di AWS servizio forniti tramite AWS CloudTrail, consulta [AWS service events delivery via 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 AWS Control Tower, puoi creare una regola Amazon EventBridge o una regola Amazon CloudWatch Events in grado di attivare i passaggi successivi del tuo 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 proprie 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 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 tracciare le azioni di AWS Control Tower e attivare flussi di lavoro automatizzati](#).

Comportamento previsto e ciclo di vita degli eventi 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 tenta di creare nuovamente 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 automatizzati, programma la funzione `Lambda UpdateManagedAccount` per cercare sia gli eventi del ciclo di vita che gli eventi del ciclo di vita. `CreateManagedAccount`

Nomi dell'evento del ciclo di vita

Ogni evento del ciclo di vita è denominato in modo che corrisponda all'azione AWS Control Tower di origine, 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 CloudWatch eventi di Amazon.

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 `"xxxxxxxxxxxx"`. `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 ogni azione per creare e fornire un nuovo account utilizzando account factory.
- [`UpdateManagedAccount`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione di aggiornamento di un prodotto fornito associato a un account creato in precedenza utilizzando account factory.
- [`EnableGuardrail`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione per abilitare il controllo su un'unità organizzativa.
- [`DisableGuardrail`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione per disabilitare un controllo su un'unità organizzativa.
- [`SetupLandingZone`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione per configurare una landing zone.
- [`UpdateLandingZone`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione di aggiornamento della landing zone esistente.
- [`RegisterOrganizationalUnit`](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione per abilitare le sue funzionalità di governance su un'unità organizzativa.

- [DeregisterOrganizationalUnit](#): Il registro registra se AWS Control Tower ha completato con successo ogni azione 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 log registra se AWS Control Tower ha completato con successo ogni azione per abilitare una nuova baseline su un account membro di destinazione in 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 ogni azione di ripristino di una baseline abilitata esistente su un account membro di destinazione in 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 ogni azione di aggiornamento di una baseline abilitata esistente su un account membro di destinazione in 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 ogni azione per disabilitare una baseline abilitata esistente su un account membro di destinazione in un'unità organizzativa. L'operazione di disabilitazione può essere avviata utilizzando l'DisableBaselineAPI o la console.

Le seguenti sezioni forniscono un elenco di 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 correttamente un nuovo account utilizzando 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": "0000000-0000-0000-1111-123456789012",
        "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
    "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-l3zc8b3h"
        }
      }
    }
  }
}
```

```

    },
    "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 l'guardrailIdand guardrailBehavior del controllo e l'organizationalUnitNamee organizationalUnitId dell'unità organizzativa su cui è abilitato il controllo.

```

{
  "version": "0",
  "id": "999cccaa-aaaa-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 l'`guardrailId` e `guardrailBehavior` del controllo e l'`organizationalUnitName` e `organizationalUnitId` dell'unità 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 configurato correttamente una landing zone. Questo evento corrisponde all'evento AWS Control Tower SetupLandingZone CloudTrail. Il registro degli eventi del ciclo di vita include `rootOrganizationalId`, che è l'ID dell'organizzazione che AWS Control Tower crea dall'account di gestione. La voce di registro include anche il `organizationalUnitName` `accountName` e `organizationalUnitId` `accountId` per ogni account che vengono creati quando AWS Control Tower configura la landing zone. OUs

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",           // Request ID.
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.controltower",
  "account": "XXXXXXXXXXXX",                             // Management account
  "time": "2018-08-30T21:42:18Z",                         // Event time from
  "region": "us-east-1",                                  // Management account
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX",                         // Management-account
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z",                   // Timestamp when call
    "eventSource": "controltower.amazonaws.com",           was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
    "eventName": "SetupLandingZone",
    "awsRegion": "us-east-1",                             // AWS Control Tower
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "CloudTrail_event_ID",                     // This value is
    "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": "XXXXXXXXXXXXX"
        },
        {
            "accountName": "Log archive",
            "accountId": "XXXXXXXXXXXXX"
        }
    ],
    "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 con successo la landing zone esistente. Questo evento corrisponde all'evento AWS Control Tower UpdateLandingZone CloudTrail . Il registro degli eventi del ciclo di vita include `rootOrganizationalId`, che è l'ID dell'organizzazione (aggiornata) governata da AWS Control Tower. La voce di registro include anche `organizationalUnitName` `accountName` e `organizationalUnitId` `accountId` per ogni

account creato in precedenza, quando AWS Control Tower aveva originariamente configurato la landing zone. OUs

```
{
  "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 organizationalUnitName organizationalUnitId dell'unità 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"
      }
    }
  }
}

```

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 organizationalUnitName fine organizationalUnitId dell'unità organizzativa su cui AWS Control Tower ha disabilitato le funzionalità di governance.

```
{
  "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 deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
        "organizationalUnit" :
          {
            "organizationalUnitName": "Test",
            OU name.
            "organizationalUnitId": "ou-adpf-302pk332"
            OU ID.
            // Foundational
            // Foundational
          },
        "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 correttamente i precontrolli su un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower PrecheckOrganizationalUnit CloudTrail. Il log degli eventi del ciclo di vita contiene un campo per i Id failedPrechecks valori e per ogni risorsa su cui AWS Control Tower ha eseguito i controlli preliminari durante il processo di registrazione dell'unità organizzativa. Name

Il registro degli eventi contiene anche informazioni sugli account annidati su cui sono stati eseguiti i precontrolli, inclusi i accountName campi e. accountId failedPrechecks

Se il failedPrechecks valore è vuoto, significa che tutti i precontrolli 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 registra 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 all'AWS Control Tower RegisterOrganizationalUnit o EnableBaseline CloudTrail agli eventi.

Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, quella `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": "2025-02-10T17:14:57Z",
  "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/XXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",

```



```

        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXX",
        "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/XXXXXXXXXXXX"
                    }
                }
            }
        ],
        "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 in un'unità organizzativa. Questo evento corrisponde all'AWS Control Tower RegisterOrganizationalUnit o ResetEnabledBaseline CloudTrail agli eventi. Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, quella 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 con successo la baseline abilitata esistente su un account membro di destinazione in un'unità organizzativa. Questo evento corrisponde all'AWS Control Tower RegisterOrganizationalUnit o UpdateEnabledBaseline CloudTrail agli eventi. Il registro degli eventi del ciclo di vita include la baseline abilitata e la relativa versione, quella `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/XXXXXXXXXXXX"
                    }
                }
            }
        ],
        "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 in 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, quella `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/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": []
    },
    "requestedTimestamp": "2025-03-14T00:49:13Z",

```

```
        "completedTimestamp": "2025-03-14T00:50:58+0000"
      },
      "eventCategory": "Management"
    }
  }
```

Utilizzo delle notifiche AWS 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:
    "eventSource": "controltower.amazonaws.com",
    "eventName": "<event name>", // one of the 9 event names 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. Attiva i backup per AWS Control Tower nella AWS Backup console. Per ulteriori informazioni, consulta [Lavorare con i servizi supportati](#) nella AWS Backup Developer Guide.
3. Attivala AWS Backup sulla persona che OUs 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. Le copie di più account 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.

Abilita 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.

Pertanto [Prerequisiti](#), devi 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 AWS Control Tower APIs chiamando l'[UpdateLandingZone](#)API, se disponi già di una landing zone AWS Control Tower, oppure l'[CreateLandingZone](#)API se stai configurando AWS Control Tower per la prima volta. (Suggerimento: dopo di che, chiama l'[EnableBaseline](#)API 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 su OUs

Dopo aver abilitato AWS Backup nelle impostazioni della landing zone, devi eseguire il passaggio aggiuntivo per abilitare il backup sullo specifico di OUs 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 selezionati e OUs, 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 contrassegnata 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 `Registra nuovamente l'unità organizzativa` 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 OUs

Se AWS Backup è abilitata, devi disabilitare completamente la AWS Backup linea di base OUs prima di disattivarla AWS Backup per entrare nella tua landing zone.

Per disabilitare la linea di AWS Backup base su un'unità organizzativa, puoi chiamare l'`DisableBaselineAPI`. I nested OUs ereditano questo stato, in modo che la baseline di base di AWS Backup sia disabilitata anche per loro.

Comando di esempio:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

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: disattivate AWS Backup la vostra landing zone

Dopo aver soddisfatto il prerequisito disattivando i backup sul tuo OUs, 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
- Annulla la registrazione dell'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 **Registra nuovamente l'unità organizzativa** 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 altri. OUs
- 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 controlli basati su SCP 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
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?	Backup Audit Manager (BAM) <code>aws_controltower_copy_report</code> <code>aws_controltower_backup_report</code> <code>aws_controltower_restore_report</code>

Descrizione	Risorse per l'account Backup Administrator: questo è l'account amministratore delegato per AWS Backup Bucket Amazon S3 per l'archiviazione dei log BAM— <code>aws-controltower-backup-reports-<i>{accountId}</i> - *</code> Bucket di registrazione degli accessi Amazon S3— <code>aws-controltower-backup-reports-log-<i>{accountId}</i> - *</code>
Quali regioni sono incluse?	Regione di origine
Quali controlli sono correlati a queste risorse?	• <code>CT.BACKUP.PV.2</code> • <code>CT.S3.PV.1</code> • <code>CT.S3.PV.1</code>

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?	• 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) • <code>aws-controltower-hourly-backup-plan</code>

Descrizione	Risorse per gli account Audit e Log Archive
	- 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?	- CT.BACKUP.PV.3 - CT.IAM.PV.1 - CT.BACKUP.PV.3 - CT.BACKUP.PV.1

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

Descrizione	Risorse per gli account dei membri in altri OUs
Quali risorse vengono create?	• 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) • <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> • Un ruolo IAM— <code>aws-controltower-BackupRole</code>
Quali regioni sono incluse?	Tutte le regioni governate
Quali controlli sono correlati a queste risorse?	• <code>CT.BACKUP.PV.3</code> • <code>CT.IAM.PV.1</code> • <code>CT.BACKUP.PV.3</code> • <code>CT.BACKUP.PV.1</code>

Controlli per il 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 del servizio (SCPs) da. AWS Organizations Se una policy è vuota (cosa che dovrebbe succedere dopo aver rimosso tutte le policy SCPs gestite 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. `OrganizationsFullAccessRole`
 - 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. `OrganizationsFullAccessRole`
- Elimina i record relativi agli account condivisi.
- Elimina i record relativi a quelli creati dal cliente. OUs

- 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. Vai alla pagina delle impostazioni della zona di atterraggio nella console AWS Control Tower.
2. Scegli Disattiva la tua landing zone all'interno della sezione Disattiva la tua landing zone .
3. 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.

4. 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.
5. 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 sulle 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](#).

6. 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
```

Smonta la tua landing zone con APIs

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 AWS IAM Identity Center (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 (OUs). 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 (OUs) create dalla console AWS Control Tower non vengono rimosse.
- Security e Sandbox non OUs vengono rimossi.
- L'organizzazione non viene eliminata da AWS Organizations.
- Nessun account AWS Organizations (condiviso, assegnato o di gestione) viene spostato o rimosso.

AWS IAM Identity Center (SSO)

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, oppure ti chiede di creare questi ruoli se configuri la tua landing zone tramite APIs. Quando disattivate 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 AWS IAM Identity Center 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 configurarlo 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 regola gestita rimanente, chiamata `AWSControlTowerManagedRule`, dagli account condivisi e membri per tutte le regioni governate.

Note

Non è possibile configurare una nuova landing zone in un'organizzazione con un livello superiore OUs denominato Security o Sandbox. È necessario rinominarli o rimuoverli OUs per configurare nuovamente una landing zone.

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: configurazione di 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 multi-account. AWS Per ridurre l'onere della gestione di una landing zone, AWS ha creato il servizio gestito chiamato AWS Control Tower.

Non sono previste funzionalità aggiuntive per ALZ; è disponibile solo per il supporto a lungo termine. Pertanto, ti consigliamo di passare al servizio AWS Control Tower da ALZ. Il blog collegato a questo capitolo illustra diverse considerazioni su questo passaggio e spiega come pianificare una migrazione di successo da ALZ a 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 a AWS Control Tower. In sostanza, abiliterai la governance di AWS Control Tower nella tua organizzazione esistente che utilizza ALZ, sulla base di 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 spiega 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 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.

Eliminare il VPC AWS Control Tower

Al di fuori di AWS Control Tower, ogni AWS cliente dispone di un VPC predefinito, che puoi 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 VPC AWS Control Tower 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 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, scegli Your VPCs. Vedrai quindi un elenco di tutti i tuoi VPCs.
4. Identifica il VPC AWS Control Tower in base alla sua gamma CIDR.
5. Seleziona il VPC, scegli Actions (Operazioni) e quindi Delete VPC (Elimina VPC).

Un VPC AWS (predefinito) esiste già in ogni regione per l'account di gestione AWS Control Tower. Per seguire le best practice di sicurezza, se scegli di eliminare il VPC 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 ogni 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 AWS Control Tower da un account esistente `aws-controltower-VPC`, puoi rimuovere l'istanza dello stack dal AWS CloudFormation StackSet `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1` VPC, dopo esserti assicurato che non vi siano risorse o dipendenze tra le risorse esistenti nel VPC.

Crea un account in AWS Control Tower senza un VPC

Se i carichi di lavoro degli utenti finali non lo richiedono VPCs, puoi utilizzare questo metodo per configurare account utente finale che non sono stati creati automaticamente per loro. VPCs

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 finché non si modificano nuovamente le impostazioni.

Per configurare Account Factory per la creazione di account senza VPCs

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 Internet-accessible subnet (Sottorete accessibile a Internet) .
- Imposta il valore Maximum number of private subnets (Numero massimo di sottoreti private) a 0.

- b. Opzione 2 — Rimozione delle regioni AWS

- Deseleziona tutte le caselle di controllo nella colonna Regions for VPC creation (Regioni per la creazione di VPC).

7. Scegli Save (Salva).

Possibili errori

Tieni presente questi possibili errori che potrebbero verificarsi quando elimini il tuo VPC AWS Control Tower o riconfiguri Account Factory per creare account senza VPCs

- L'account di gestione esistente potrebbe avere dipendenze o risorse nel VPC AWS Control Tower, il che può causare un errore di eliminazione.
- 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: configurazione di 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 policy di sicurezza e applicare le regole di sicurezza per le tue organizzazioni AWS Control Tower e come correggere le risorse non conformi

applicando automaticamente le policy. Puoi visualizzare i gruppi di sicurezza attivi per ogni account e risorsa (come un'istanza Amazon EC2) nella tua organizzazione.

Puoi creare policy di firewall personalizzate oppure sottoscrivere le regole di fornitori attendibili.

Configurazione di 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.

[Guida video alla configurazione del firewall in AWS Control Tower.](#)

Per ulteriori informazioni, consulta la [documentazione su come configurare 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 l'[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](#)
- [Nessun errore trovato nei percorsi di avvio](#)
- [È stato ricevuto un errore di autorizzazioni insufficienti](#)
- [I controlli investigativi non hanno effetto sugli account](#)
- [Frequenza superata \(errore restituito dall' AWS Organizations API\)](#)
- [Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower](#)
- [AWS Support](#)

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 [Come funzionano AWS le regioni 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.
- Contesto/impatto: le regole di configurazione distribuite non corrispondono alla AWS 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.
- Contesto/impatto: se l'account non viene riportato all'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 la documentazione AWS Config

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

-

Gestione del Canale di Distribuzione

Nessun errore trovato nei percorsi di avvio

Quando si tenta di creare un nuovo account, è possibile che venga visualizzato un messaggio di errore simile a questo:

```
No launch paths found for resource: prod-dpqqfywxxx
```

Questo messaggio di errore viene generato da AWS Service Catalog, che è il servizio integrato che aiuta a fornire account in AWS Control Tower.

Cause comuni:

- È possibile che tu abbia effettuato l'accesso come 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 l'utente IAM Identity Center a uno di questi gruppi di autorizzazioni: AWSAccountFactory (per l'accesso 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 l'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 che crei in nessuna regione fino a quando i singoli account all'interno OUs governati 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 AWS Control Tower OUs e gli account](#).

Per aggiornare più account individuali a livello di codice, puoi utilizzare il modulo AWS Service Catalog e la APIs AWS CLI per automatizzare gli aggiornamenti. Per ulteriori informazioni su come affrontare il processo di aggiornamento, vedere questo [Procedura guidata: video](#). Puoi sostituire l'UpdateProvisionedProductAPI con l'API mostrata nel video ProvisionProduct.

Se hai ulteriori difficoltà ad abilitare i controlli investigativi sui tuoi account, contatta il [AWS servizio clienti](#).

Frequenza superata (errore restituito dall' AWS Organizations API)

Possibile causa

Il tuo carico di lavoro era in esecuzione mentre AWS Control Tower eseguiva una scansione giornaliera per verificare se SCPs avevi perso qualcosa.

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 li chiami APIs 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 provarlo 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 removing-and-deleting deve essere ripetuto per ogni risorsa rimanente, per ogni regione in cui l'account è stato distribuito, 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 Support

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, alcune linee di base potrebbero essere abilitate automaticamente sull'account condiviso. Alcune linee di base possono essere abilitate e aggiornate in base alle impostazioni e alle configurazioni della landing zone. AWS Control Tower crea e distribuisce le risorse verso l'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 sull'account condiviso, durante la configurazione della 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 regione negata al controllo a livello dell'UE non ha modo di autorizzare le regioni che la regione negato il controllo della landing zone non consente.

Per ulteriori informazioni, consulta [How SCPs work with 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. AWSControl TowerBaseline

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: AWSControl TowerBaseline e ConfigBaseline non può essere abilitato sulla stessa unità organizzativa. Solo una di esse è consentita su un'unità organizzativa.

- Nome: BackupBaseline

Descrizione: questa linea di base imposta le risorse e i 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 possono essere applicati all'account condiviso durante la configurazione della landing zone

AWS Control Tower abilita determinate linee di base sull'account condiviso, 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: `CentralSecurityRolesBaseline` e `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 **Registra nuovamente** o **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 linee di APIs 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 quattro APIs linee di base.

Differenze

- Registrazione e fornitura dei 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 dei membri e annidarli. OUs 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 registrarti OUs 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 `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 selezioni una linea di base per i tuoi account esistenti OUs e quelli esistenti, la versione della landing zone determina l'intera posizione 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 linea di base a livello di unità organizzativa `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_BASELINE_CLOUDT RAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, risorse IAM	Nessuno		
2.0	da 2,8 a 2,9	BP_BASELINE_CLOUDT RAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, risorse IAM	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		
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_IAM_ROLE, BP_BASELINE_IAM_SERVICE_ROLE, BP_BASELINE_IAM_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 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.

- Puoi continuare a utilizzare account factory e altre funzionalità senza aggiornare immediatamente la baseline dell'unità organizzativa, tranne nel caso di un aggiornamento della landing zone dalla 2.x alla 3.x.
- 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

Se aggiorni la landing zone di AWS Control Tower da qualsiasi versione 2.X a qualsiasi versione 3.X, devi aggiornare anche la versione di base sul tuo OUs, a causa del passaggio dai trail a livello di account a quelli a livello di organizzazione. AWS CloudTrail Nella console, l'unità organizzativa mostrerà lo stato di Aggiornamento richiesto.

Considerazioni relative alle 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, i nidificati non OUs vengono aggiornati automaticamente quando viene aggiornata l'unità organizzativa principale. Si consiglia di aggiornare l'unità organizzativa principale prima di aggiornare quella OUs nidificata.
- Quando chiami l'UpdateEnabledBaselineAPI o registri 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: registra un'unità organizzativa AWS Control Tower APIs solo con

Questa guida dettagliata di esempi è un documento complementare. Per spiegazioni, avvertenze e ulteriori informazioni, vedere. [Tipi di linee di base](#)

Prerequisiti

È necessario 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 si desidera registrare nuovamente ai fini dell'aggiornamento.

Registrare un'unità organizzativa

1. Controlla se IdentityCenterBaseline è abilitato per la landing zone. In tal caso, ottieni l'identificatore 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 linea di AWSControlTowerBaseline base sull'unità organizzativa di destinazione.

Se la linea di base di Identity Center 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 Identity Center Baseline non è abilitata, ometti il *parameters* flag, come segue:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Registrare nuovamente un'unità organizzativa

Dopo aver aggiornato le impostazioni della landing zone o aver aggiornato la versione della landing zone, devi registrarti nuovamente OUs per fornire loro le ultime modifiche. Segui questi passaggi per registrare nuovamente un'unità organizzativa a livello di codice, reimpostando la risorsa associata e tutte le risorse associateEnabledBaseline. EnabledControl

Important

Se l'unità organizzativa ha i controlli opzionali abilitati, è inoltre necessario chiamare l'[ResetEnabledControl](#) API per ogni controllo opzionale abilitato dopo aver ripristinato la linea di base. Questo passaggio garantisce che i controlli opzionali rimangano coerenti con l'ultima configurazione della landing zone. Se salti questo passaggio, i controlli opzionali sull'unità organizzativa potrebbero non riflettere le ultime modifiche alla landing zone. Se non hai alcun controllo opzionale abilitato, questo passaggio non è necessario.

1. Ottieni l'ARN dell'unità organizzativa di destinazione per registrarti nuovamente.


```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --  
query 'OrganizationalUnit.[Arn]'
```

2. Ottiene l'ARN della EnabledBaseline risorsa per l'unità organizzativa di destinazione.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?  
targetIdentifier==`<OUARN>`].[arn]'
```

3. Reimposta la linea di base 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 landing zone.

Elenca i controlli abilitati sull'unità organizzativa di destinazione:

```
aws controltower list-enabled-controls --target-identifier <OU ARN>
```

Per ogni controllo opzionale abilitato restituito, ripristinalo chiamando:

```
aws controltower reset-enabled-control --enabled-control-  
identifier <EnabledControlArn>
```

Per ulteriori informazioni, consulta l'[ResetEnabledControl](#) articolo AWS Control Tower API Reference.

Esempi di utilizzo delle API di base

Questa sezione contiene esempi di parametri di input e output per la baseline APIs di AWS Control Tower.

DisableBaseline

Per ulteriori informazioni su questo funzionamento dell'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": "BackupManagerBaseline",
      "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 tutti quelli OUs che hanno una linea di base specifica:

```

aws controltower list-enabled-baselines \
  --filter '{
    "baselineIdentifiers": ["BASELINE_ARN"]
  }'

```

Visualizza tutti OUs gli account che hanno 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 richiamare direttamente alcuna scrittura APIs, ad esempio ResetEnabledBaseline o EnableBaseline UpdateEnabledBaselineDisableBaseline, 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 (baselineIdentifierse targetIdentifiers filtri):

```
aws controltower list-enabled-baselines \  
  --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-  
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=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 coprono 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 indicazioni personalizzate 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 i video che spiegano di più su come utilizzare la funzionalità di AWS Control Tower.

Rete

Configura modelli ripetibili e gestibili per le reti in AWS. Scopri di più sulla progettazione, l'automazione e le appliance 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 VPCs in AWS Control Tower con AWS Service Catalog](#): questo post di blog descrive un modo per configurare Account Factory in modo da poter fornire account personalizzati VPCs.
- [Implementazione di Serverless Transit Network Orchestrator \(STNO\) in AWS Control Tower](#): questo post sul 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 AWS ambiente.

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 di blog descrive come automatizzare l'abilitazione e la configurazione CSPM di Security Hub in un ambiente multi-account AWS Control Tower su account esistenti e nuovi.
- [Abilitazione AWS Identity and Access Management](#): questo post sul 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 sicuro e gerarchico 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'uso da parte di AWS Systems Manager e AWS CloudFormation. Ad esempio, puoi memorizzare un elenco di regioni in cui desideri distribuire 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 Okta con AWS IAM Identity Center](#): questo post sul blog descrive come utilizzare Okta con IAM Identity Center e AWS Control Tower.

Registrazione di log

- AWS Soluzione di [registrazione centralizzata: questo post sulla soluzione](#) descrive la soluzione di registrazione centralizzata che consente alle organizzazioni di raccogliere, analizzare e visualizzare i log su più account e regioni. AWS AWS
- Per informazioni sulla visualizzazione AWS Config delle risorse, consulta il [Config Resource Compliance](#) Dashboard.

Implementazione delle risorse e gestione dei carichi di lavoro

Implementa e gestisci risorse e carichi di lavoro.

- [Integrazione con Getting Started Library](#): questo post del blog descrive i portafogli Getting Started che puoi utilizzare.
- [Distribuzione continua di Cloud Custodian su AWS Control Tower](#)

Collaborazione con organizzazioni e account esistenti

Lavora 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 sul blog descrive come implementare AWS Control Tower nelle tue AWS organizzazioni esistenti.
- [Estendi la governance di AWS Control Tower utilizzando i pacchetti di conformità AWS Config](#): questo post sul blog descrive come distribuire pacchetti di AWS Config conformità per aiutare a portare gli account e le organizzazioni esistenti alla governance da parte di AWS Control Tower.
- [Come rilevare e mitigare le violazioni di Guardrail con AWS Control Tower](#): questo post sul blog descrive come aggiungere controlli e come abbonarsi alle notifiche SNS in modo da poter ricevere notifiche via e-mail in caso di violazioni della conformità di controllo.

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 sul blog descrive come utilizzare gli eventi del ciclo di vita con AWS Control Tower.
- [Automatizza la creazione di account](#): questo post sul blog descrive come configurare la creazione automatica di account in AWS Control Tower.
- [Automazione dei log di flusso di Amazon VPC](#): questo post di blog descrive come automatizzare e centralizzare i log di flusso di Amazon VPC in un ambiente con più account.
- [Automatizza l'etichettatura dei VPC con gli eventi del ciclo di vita di AWS Control Tower](#): questo post sul blog descrive come automatizzare l'etichettatura delle risorse VPCs per, tramite gli eventi del ciclo di vita in AWS Control Tower.
- [Gestione automatizzata degli account](#): questo post sul blog descrive come automatizzare le attività di gestione degli account dopo la configurazione dell'ambiente AWS Control Tower.

Migrazione dei carichi di lavoro

Usa altri AWS servizi con AWS Control Tower per assistere nella migrazione dei carichi di lavoro.

- [CloudEndure migrazione](#): questo post sul 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 AWS Organizations APIs, 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 funzionalità multi-account per questi servizi AWS correlati, devi abilitare l'accesso affidabile. Per ulteriori informazioni, consulta [Using AWS Organizations con altri servizi AWS](#).

Note

Ricorda che AWS IAM Identity Center e AWS Config, AWS CloudTrail sono configurati per te in AWS Control Tower e completamente integrati. Non è necessario modificare le impostazioni di accesso attendibile o di amministrazione delegata per questi servizi.

- Alcuni AWS servizi disponibili AWS Organizations possono utilizzare l'amministrazione delegata, tra cui AWS Systems Manager e AWS Firewall Manager. Per ulteriori informazioni, vedere [Configurazione di un amministratore delegato](#) e [Abilitazione di un account amministratore delegato per Firewall Manager](#). Guarda anche questo video, [Configurazione di 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 infrastrutturali e operativi, tra cui la gestione delle identità, la sicurezza per un ambiente con più account, il networking centralizzato, l'intelligenza operativa e la 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:

- [AWS Control Tower disponibile nel cloud sovrano europeo](#)

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:

- [Landing zone di AWS Control Tower versione 4.0](#)
- [AWS Control Tower aggiunge 279 AWS Config controlli aggiuntivi a Control Catalog](#)
- [AWS Control Tower 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 IPv6 gli indirizzi](#)
- [AWS Control Tower riduce la deriva](#)

[Account Factory per Terraform versione 1.15.0 disponibile](#)

- [Controlli aggiornati con i tipi di istanze Nitro](#)
- [AWS Control Tower disponibile nella regione Asia Pacifico \(Taipei\)](#)
- [AWS Control Tower supporta PrivateLink](#)
- [Support per framework di settore aggiuntivi, metadati aggiornati](#)
- [Controlli collegati ai servizi AWS Config](#)
- [La visualizzazione della console dei controlli abilitati offre visibilità centralizzata](#)
- [the section called “Account Factory for Terraform \(AFT\) supporta nuove configurazioni al momento dell'implementazione”](#)
- [AWS Control Tower introduce la reportistica a livello di account come riferimento APIs](#)
- [the section called “AWS Control Tower disponibile nelle regioni di AWS Asia Pacifico \(Tailandia\) e Messico \(Centrale\)”](#)
- [AWS Config Controlli aggiuntivi disponibili](#)
- [Annulla registrazione ed eliminazione delle azioni per OUs](#)
- [the section called “Control Catalog supporta gli indirizzi IPv6”](#)

Landing zone 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'esperienza flessibile Controls-Only, che consente ai clienti di personalizzare il modo in cui implementano e gestiscono il loro ambiente AWS multi-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 funzionalità principali

- Integrazioni di servizi opzionali: landing zone 4.0 consente di scegliere quali integrazioni di servizi abilitare nel proprio ambiente. La disabilitazione 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 di servizi:
 - AWS Config
 - AWS CloudTrail
 - Ruoli di sicurezza
 - AWS Backup

Importante: se desideri disabilitare l'integrazione con AWS Config, devi disabilitare anche le integrazioni di Security Roles, IAM Identity Center e AWS Backup.

- Risorse dedicate anziché utilizzare risorse condivise: la landing zone 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 dei servizi:
 - 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 rimuove 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 dell'hub devono trovarsi nella stessa unità organizzativa
- Esperienza dedicata ai controlli: ora puoi creare una configurazione minima della landing zone che include:
 - 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 con AWS Config:
 - Un nuovo Config ha parlato come linea di base specifica per i controlli investigativi
 - Aggregatore di configurazione collegato al servizio (SLCA) nell'account Config hub
 - Sostituzione dei tradizionali aggregatori di organizzazioni e account
- Manifesto opzionale:
 - Il campo manifest è ora facoltativo e consente di:
 - Crea zone di atterraggio senza alcuna integrazione di servizi
 - Maggiore flessibilità nella configurazione iniziale
 - Opzioni di implementazione personalizzate

AWS Control Tower aggiunge 279 AWS Config controlli aggiuntivi a Control Catalog

14 novembre 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora include 279 AWS Config controlli aggiuntivi come parte del Control Catalog. Puoi visualizzare i controlli nella console AWS Control Tower e tramite APIs.

Alcuni controlli hanno relazioni con altri controlli. Queste relazioni sono espresse anche nella console AWS Control Tower e in APIs. I tipi di relazione includono complementari, mutuamente esclusivi e alternativi.

AWS Control Tower disponibile nella regione Asia Pacifico (Nuova Zelanda)

28 ottobre 2025

(Non è richiesto alcun aggiornamento per la landing zone 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Per i clienti che utilizzano AWS Control Tower landing zone versione 3.1 o successiva, AWS Control Tower ora consente la registrazione automatica degli account. OUs Se opti per la registrazione automatica degli account, AWS Control Tower applica le risorse e i controlli di base abilitati da un'unità organizzativa a un account, quando lo sposti in una nuova unità organizzativa. I controlli e le linee di base dell'unità organizzativa precedente 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 landing zone nella console AWS Control Tower oppure chiamando AWS Control Tower **CreateLandingZone** oppure **UpdateLandingZone** APIs, con il valore del parametro impostato su Inheritance Drift. **RemediationType**

Per applicare la registrazione automatica: dopo aver selezionato questa opzione nella pagina Impostazioni, puoi spostare un account tramite la AWS Organizations console, l' AWS Organizations MoveAccountAPI o la console AWS Control Tower.

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, vedere. [Configurare facoltativamente la registrazione automatica per gli account](#)

Questa versione include anche un aggiornamento di una policy gestita e una nuova policy gestita. Abbiamo aggiornato [AWS ControlTowerServiceRolePolicy](#) e aggiunto il nuovo [AWS ControlTowerIdentityCenterManagementPolicy](#).

Abbiamo aggiornato l'AWS Control Tower CreateLandingZone e UpdateLandingZone APIs ne abbiamo aggiunto uno nuovoRemediationType, chiamatoInheritance Drift.

AWS Control Tower aggiorna la versione Python

3 settembre 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

La versione 3.9 di Python è obsoleta. AWS Control Tower ha aggiornato le versioni di Python negli 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha aggiornato la funzionalità di Service Control Policy (SCP) drift. Con questa versione, due tipi di deviazioni di governance vengono gestite direttamente da AWS Control Tower e non causano più variazioni nell'ambiente.

Sono stati rimossi due tipi di deviazioni di governance

- SCP collegato all'unità organizzativa gestita: questo tipo di deriva si verificava quando un SCP per un controllo veniva collegato a qualsiasi altra unità organizzativa. Questo evento era particolarmente comune quando si eseguiva l'aggiornamento OUs 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 IPv6 gli indirizzi

18 agosto 2025

(Non è richiesto alcun aggiornamento per la landing zone 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. Il supporto per gli endpoint esistenti IPv4 rimane disponibile 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](#)

Account Factory per Terraform versione 1.15.0 disponibile

28 luglio 2025

(Non è richiesto alcun aggiornamento per la landing zone 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 i tipi di istanze Nitro

24 luglio 2025

(Non è richiesto alcun aggiornamento per la landing zone 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 istanze di alcuni nuovi tipi di istanze Nitro e rimuove alcuni tipi di istanze obsoleti della serie u.

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 istanze 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 disponibile nella regione Asia Pacifico (Taipei)

23 luglio 2025

(Non è richiesto alcun aggiornamento per la landing zone 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta [AWS PrivateLink](#). Puoi richiamare AWS Control Tower e Control Catalog APIs dall'interno del tuo Amazon Virtual Private Cloud (VPC) senza attraversare la rete Internet pubblica. AWS PrivateLink fornisce connettività privata tra cloud privati virtuali (VPCs), 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.

Support per framework di settore aggiuntivi, metadati aggiornati

12 giugno 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Con questa versione, AWS Control Tower si espande per includere il supporto per 10 framework di settore. [Per un elenco di framework, consulta Frameworks supportati.](#)

Ad esempio, puoi iniziare accedendo alla pagina Control Catalog nella console AWS Control Tower e cercando un framework, come PCI-DSS-v4.0, per visualizzare tutti i controlli relativi a quel framework. 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 si valutano 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 nella 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 alla più ampia gamma di framework di settore disponibili. [Per ulteriori informazioni su questa gerarchia, vedere Panoramica dell'ontologia.](#)

- Queste modifiche ai metadati si riflettono nella console AWS Control Tower e l'esperienza della console è coerente tra la torre di controllo AWS e le AWS Config console.
- Per visualizzare le informazioni di controllo nella console AWS Control Tower, devi aggiungere `controlcatalog` autorizzazioni aggiuntive alle tue policy IAM. Per ulteriori informazioni, consulta [Autorizzazioni necessarie per utilizzare la console AWS Control Tower.](#)
- Ogni controllo ha ora un nuovo campo chiamato `GovernedResources`, che mostra i tipi di risorse governati dal controllo. In alcuni casi, questo campo mostra il prefisso di servizio per le risorse e in altri casi può essere vuoto. Per ulteriori informazioni, consultare [GetControl](#) e [ListControls](#).

Con questa versione, abbiamo rinominato Controls Library in Control Catalog, per coerenza con altri termini.

Controlli collegati ai servizi AWS Config

12 giugno 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower annuncia il supporto per i controlli investigativi di AWS Control Tower da implementare come regole collegate ai servizi AWS Config .

Con questa versione, AWS Control Tower ora distribuisce regole Config collegate ai servizi direttamente negli account registrati, sostituendo il metodo di distribuzione precedente con set di stack. AWS CloudFormation Questa modifica migliora significativamente la velocità di implementazione. Inoltre, queste regole di Config collegate ai servizi aiutano a garantire una governance coerente delle risorse, poiché impediscono variazioni involontarie della configurazione che potrebbero essere causate da modifiche manuali ai set di stack o alle regole di Config. CloudFormation

In futuro, tutti i controlli AWS Control Tower implementati dalle AWS Config regole verranno implementati con questo meccanismo, che richiama direttamente il AWS Config APIs.

Important

Prima di adottare regole di Config collegate ai servizi, esamina le personalizzazioni esistenti, come le correzioni, che hai apportato alle regole di Config al di fuori di AWS Control Tower, poiché queste personalizzazioni verranno rimosse durante la transizione. AWS Config APIs Non supportano l'aggiunta di configurazioni di riparazione per le regole collegate ai servizi. AWS Config Per informazioni, consulta [PutRemediationConfigurations](#).

Dettagli e azioni richieste

- Quando aggiorni o ripristini la landing zone, AWS Control Tower aggiorna i controlli obbligatori che regolano l'unità organizzativa di sicurezza. Per completare l'aggiornamento, devi inoltre reimpostare tutti i controlli di rilevamento implementati con le AWS Config regole o registrare nuovamente l'unità organizzativa.
- L'intero ambito di questo aggiornamento si applica a te se la versione della landing zone di AWS Control Tower è 3.2 o successiva. Quando si applica questo aggiornamento, le AWS Config regole esistenti vengono modificate per diventare regole Config gestite dal servizio, insieme al nuovo metodo di distribuzione.
- Se la tua landing zone è la versione 3.1 o precedente, tutte le nuove regole di Config verranno implementate con il nuovo metodo, non più con gli Stack Sets. Le regole Config esistenti NON vengono aggiornate per diventare regole di Config gestite dal servizio. Rimarranno del tipo standard.

- È possibile identificare le regole di configurazione collegate ai servizi in base alla relativa risorsa ARN, che ha la forma:

```
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 Config investigative e collegate ai servizi di 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, prevenire variazioni di 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 al servizio (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 visibilità centralizzata

21 maggio 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha aggiunto una nuova pagina nella console che mostra tutti i controlli abilitati in un'unica visualizzazione centralizzata. In precedenza, i controlli erano visualizzabili solo con l'account o l'unità organizzativa su cui erano abilitati. La visualizzazione consolidata semplifica l'identificazione delle lacune nella governance del controllo, su larga scala.

Nella pagina Controlli abilitati, puoi filtrare i controlli in base al comportamento: Preventivo, Detective o Proattivo. È inoltre possibile filtrare in base all'implementazione del controllo, ad esempio SCP. Per ogni controllo, puoi vedere quanti OUs hanno questo controllo abilitato.

Per visualizzare la pagina Controlli abilitati, vai alla sezione Controlli nella console AWS Control Tower.

Account Factory for Terraform (AFT) supporta nuove configurazioni al momento dell'implementazione

13 maggio 2025

(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 tre configurazioni opzionali aggiuntive al momento della distribuzione. È possibile distribuire AFT in un cloud privato virtuale (VPC) personalizzato, specificare il nome del progetto Terraform per la 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 come riferimento APIs

12 maggio 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Ora puoi visualizzare lo stato di drift e di registrazione degli account in modo programmatico per i tuoi account gestiti, chiamando la linea di base APIs. Grazie a questa funzionalità, è possibile identificare quando le configurazioni di base dell'account e dell'unità organizzativa sono diverse o non sono sincronizzate. Per visualizzare lo stato della deriva a livello di codice, puoi chiamare l'API per le linee di base 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 OUs 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. La linea di base di AWS Control Tower APIs include CloudFormation il supporto, che ti consente di creare automazioni per gestire i tuoi OUs account con Infrastructure as Code (IaC).

Per ulteriori informazioni APIs, consulta [Baseline](#) nella AWS Control Tower User Guide. Le funzionalità di reporting di base APIs e appena lanciate per la deviazione e lo stato di registrazione

dell'account sono disponibili ovunque sia disponibile AWS Control Regions AWS Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower disponibile nelle regioni di AWS Asia Pacifico (Tailandia) e Messico (Centrale)

9 maggio 2025

(Non è richiesto alcun aggiornamento per la landing zone 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](#).

AWS Config Controlli aggiuntivi disponibili

11 aprile 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta 223 AWS Config regole gestite aggiuntive per vari casi d'uso, come sicurezza, costi, durabilità e operazioni. Con questo lancio, ora puoi usare AWS Control Tower per cercare e scoprire le AWS Config regole necessarie per governare il tuo ambiente multi-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 ulteriori dettagli, consulta [AWS Config Controlli integrati disponibili in AWS Control Tower](#).

Con questo lancio, abbiamo aggiornato la `ListControls` e `GetControl` APIs per supportare tre nuovi campi: `CreateTimeSeverity` e `Implementation`, che puoi utilizzare per cercare 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 implementare una regola, consulta l'elenco delle regole supportate Regioni AWS per quella regola, per vedere dove può essere abilitata.

Annula registrazione ed eliminazione delle azioni per OUs

8 aprile 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta azioni separate da console per annullare la registrazione di un'unità organizzativa ed eliminare un'unità organizzativa. È necessario annullare la registrazione dell'unità organizzativa prima di eliminarla. Puoi rimuovere un'unità organizzativa da AWS Control Tower annullandone la registrazione.

Per ulteriori informazioni, consulta [Rimuovere un'unità organizzativa](#).

Control Catalog supporta gli indirizzi IPv6

2 aprile 2025

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

L'API AWS Control Tower Control Catalog ora supporta gli indirizzi Internet Protocol versione 6 (IPv6) tramite i nostri nuovi endpoint dual-stack. Il supporto esistente per gli endpoint Control Catalog IPv4 rimane disponibile 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:

- [AWS Control Tower cFCT supporta GitHub e RCPs](#)
- [AWS Control Tower aggiunge controlli preventivi con policy dichiarative](#)
- [AWS Control Tower aggiunge opzioni di piano di backup prescrittivo](#)
- [AWS Control Tower integra i AWS Config controlli](#)

- [AWS Control Tower migliora la gestione degli hook e aggiunge regioni di controllo proattivo](#)
- [AWS Control Tower lancia politiche di controllo delle risorse gestite](#)
- [AWS Control Tower segnala variazioni nelle policy di controllo](#)
- [Nuova API `ResetEnabledControl`](#)
- [API di controllo degli aggiornamenti del catalogo `GetControl`](#)
- [AWS Control Tower AFT supporta GitLab](#)
- [AWS Control Tower disponibile nella regione AWS Asia Pacifico \(Malesia\)](#)
- [AWS Control Tower supporta fino a 1000 account per unità organizzativa](#)
- [AWS Control Tower aggiunge la selezione della versione della landing zone](#)
- [API di controllo descrittivo disponibile, accesso esteso a regioni e controlli](#)
- [AWS Control Tower supporta AFT e cFCT nelle regioni opt-in](#)
- [AWS Control Tower aggiunge l'`ListLandingZoneOperationsAPI`](#)
- [AWS Control Tower supporta fino a 100 operazioni di controllo simultanee](#)
- [AWS Control Tower disponibile nel AWS Canada occidentale \(Calgary\)](#)
- [AWS Control Tower supporta l'aggiustamento delle quote in modalità self-service](#)
- [AWS Control Tower rilascia la Controls Reference Guide](#)
- [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 APIs la registrazione e la configurazione delle unità organizzative con linee di base](#)

AWS Control Tower cFCT supporta GitHub e RCPs

9 dicembre 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 le personalizzazioni di AWS Control Tower (CFCT). Per ulteriori informazioni, consulta [Configura GitHub come origine di configurazione](#).

AWS Control Tower ora supporta le policy di controllo delle risorse (RCPs) per le personalizzazioni di AWS Control Tower (CFCT). Per ulteriori informazioni, consulta [Guida alla personalizzazione cFCT](#).

AWS Control Tower aggiunge controlli preventivi con policy dichiarative

1 dicembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta i controlli preventivi implementati da AWS Organizations policy dichiarative di. Le politiche dichiarative vengono applicate direttamente a livello di servizio. Questo approccio garantisce che la configurazione specificata venga applicata, anche quando vengono introdotte nuove funzionalità o vengono introdotte dal servizio. APIs [Per ulteriori informazioni, consulta Controlli implementati con politiche dichiarative.](#)

AWS Control Tower aggiunge opzioni di piano di backup prescrittivo

25 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 landing zone. Il piano di backup include regole predefinite, come i giorni di conservazione, la frequenza di 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 dei membri gestiti. Quando applichi un piano di backup alla landing zone, AWS Control Tower garantisce che il piano sia coerente per tutti gli account membri e in linea con le raccomandazioni sulle best practice di AWS Backup.

Per ulteriori informazioni, consulta [AWS Backup e AWS Control Tower](#).

AWS Control Tower integra i AWS Config controlli

21 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha integrato AWS Config controlli selezionati, 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 proattivo

20 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Con questa versione, puoi utilizzare l'intera capacità degli CloudFormation hook, senza restrizioni da parte 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 controllo CT.CLOUDFORMATION.PR.1, in modo che solo AWS Control Tower potesse modificarli. Con questa versione, puoi distribuire e modificare CloudFormation gli hook senza le restrizioni precedentemente richieste dal servizio AWS Control Tower.

Se attualmente distribuisce controlli proattivi, puoi passare a questa funzionalità hook migliorata. Per ripristinare tutti i controlli proattivi su un'unità organizzativa, reimposta ogni singolo controllo proattivo attivo su quell'unità organizzativa. È possibile 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 proattivo sull'unità organizzativa alla nuova funzionalità. Ripeti questo processo per ogni unità organizzativa che implementa controlli proattivi.

Dopo aver ripristinato un controllo proattivo, rimuovi il controllo CT.CLOUDFORMATION.PR.1 dalla tua AWS Control Tower, a meno che tu non abbia abilitato tale OUs controllo per un altro scopo. Se non disattivi il controllo CT.CLOUDFORMATION.PR.1, non sarai in grado di creare e modificare gli altri hook. CloudFormation

[Per ulteriori informazioni, consulta Aggiornare gli hook di controllo proattivi.](#)

AWS Control Tower lancia politiche di controllo delle risorse gestite

15 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower offre un nuovo tipo di controllo preventivo, implementato con policy di controllo delle risorse (RCPs). Questi controlli ti aiutano a stabilire un perimetro di dati nel tuo ambiente AWS Control Tower, per proteggere le tue risorse da accessi involontari.

Ad esempio, puoi abilitare i controlli basati su RCP per Amazon S3, AWS Security Token Service, Amazon AWS Key Management Service, SQS e servizi. Gestione dei segreti AWS. Un controllo basato su RCP può imporre un requisito come «Richiedi che le risorse Amazon S3 dell'organizzazione siano accessibili solo dai responsabili IAM che appartengono all'organizzazione o tramite un AWS servizio», indipendentemente dalle autorizzazioni concesse sulle singole policy dei bucket.

Puoi configurare i nuovi controlli basati su RCP e alcuni controlli preventivi esistenti basati su SCP per specificare le esenzioni IAM per i principali e le risorse. AWS. Se non desideri che un principale o una risorsa siano governati dal controllo, puoi configurare un'esenzione.

Combinando 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 preventivi basati su RCP sono disponibili in alcune Regioni AWS laddove è disponibile AWS Control Tower. Per un elenco completo delle aree e delle Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower segnala variazioni nelle policy di controllo

15 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora segnala le variazioni nelle policy di controllo, per i controlli implementati con le policy di controllo delle risorse (RCPs) e i controlli che fanno parte dello standard gestito dal servizio CSPM Security Hub: AWS Control Tower. Questo tipo di deriva può essere risolto tramite la nuova API. `ResetEnabledControl` Per ulteriori informazioni, consulta [Types of governance drift](#).

Nuova API `ResetEnabledControl`

14 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower annuncia una nuova API per aiutarti a gestire la deriva del controllo in modo programmatico. Puoi riparare la deriva del controllo e ripristinare un controllo alla configurazione prevista. L'`ResetEnabledControl` API funziona con i controlli opzionali di AWS Control Tower, inclusi i controlli Strongly recommended ed Elective.

Eccezioni di controllo

- I controlli implementati con le policy di controllo del servizio (SCPs) non possono essere ripristinati con questa API. Per ulteriori informazioni, consulta [ResetEnabledControl](#).
- I controlli obbligatori non possono essere ripristinati, poiché proteggono le risorse di AWS Control Tower.
- Il Region Deny Control per la landing zone deve essere ripristinato tramite la console.

La deriva di controllo si verifica quando un controllo AWS Control Tower viene modificato all'esterno di AWS Control Tower, ad esempio dalla AWS Organizations console. Risolvere la deriva aiuta a garantire la conformità ai requisiti di governance.

API di controllo degli aggiornamenti del catalogo **GetControl**

8 novembre 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 alcuni controlli che possono essere configurati.

L'GetControlAPI fa parte del `controlcatalog` namespace di AWS Control Tower.

Per ulteriori informazioni, consulta l'[GetControlAPI nel riferimento alle API](#) di Control Catalog.

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 viene modificato da AWS Config regola a AWS Security Hub CSPM. Il pannello di aiuto della console corrispondente viene modificato per riflettere questa modifica.
- Il valore dei `Implementation` parametri di tutti i controlli Hook esistenti viene modificato 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta GitLab TM™ e GitLab Self-managed come opzioni per un sistema di controllo della versione (VCS) di terze parti e fonte di configurazione per Account Factory for Terraform (AFT).

AWS Control Tower disponibile nella regione AWS Asia Pacifico (Malesia)

21 ottobre 2024

(Non è richiesto alcun aggiornamento per la landing zone 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

(Non è richiesto alcun aggiornamento per la landing zone 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 persone 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 sono ancora valide a causa delle limitazioni sul numero di set di CloudFormation stack disponibili. In particolare, il numero massimo di account che puoi registrare in un'unità organizzativa può variare a seconda del numero di regioni che hai sotto la governance. Per ulteriori informazioni, consulta [Limitazioni basate sui AWS servizi sottostanti](#) nella [AWS Control Tower User Guide](#). Per un elenco completo delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower aggiunge la selezione della versione della landing zone

15 agosto 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Se utilizzi AWS Control Tower landing zone versione 3.1 e successive, puoi aggiornare o riparare la landing zone esistente nella versione corrente oppure puoi eseguire l'upgrade a una versione a tua scelta. In precedenza, qualsiasi aggiornamento o riparazione della landing zone richiedeva l'aggiornamento alla versione più recente della landing zone.

Con la selezione della versione della landing zone, hai più flessibilità nella pianificazione degli aggiornamenti di versione mentre valuti le potenziali modifiche al tuo ambiente. Non è necessario scegliere tra riparare il drift per mantenere la conformità, aggiornare le configurazioni delle landing zone o passare alla versione più recente della landing zone. Se utilizzi la versione 3.1 o successiva della landing zone, puoi scegliere di mantenere la versione attuale o passare a una versione più recente quando aggiorni o ripristini le configurazioni della landing zone.

API di controllo descrittivo disponibile, accesso esteso a regioni e controlli

6 agosto 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha aggiunto due nuove operazioni API che ti aiutano a trovare ulteriori informazioni sui controlli disponibili, in modo programmatico. 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 delle regioni di destinazione e lo stato di deriva.
- L'[ListControls](#) API restituisce un elenco impaginato di tutti i controlli disponibili nella libreria di controlli AWS Control Tower.

Questi APIs vengono raggiunti tramite lo spazio dei nomi [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 ampliato 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, durabilità e operazioni. Per ulteriori informazioni, consulta [il riferimento all'API Control Catalog](#).

Disponibilità estesa della regione

A partire da questa versione, puoi estendere la governance di AWS Control Tower in aree in Regioni AWS cui alcuni dei tuoi controlli (già) abilitati non sono 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, quando non offriva coerenza tra tutti i controlli abilitati e le regioni governate. Con questa versione, hai una maggiore flessibilità e una maggiore responsabilità nel garantire che la configurazione sia corretta per tutti i controlli abilitati e tutte le regioni governate. Il [controllo AWS Control Tower APIs](#) e il [catalogo di controllo APIs](#) possono aiutarti a ottenere informazioni sulle AWS regioni in cui sei protetto dai controlli abilitati e sulle regioni in cui possono essere implementati controlli aggiuntivi. Le informazioni sulla regione e sul controllo sono disponibili anche nella console AWS Control Tower.

AWS Control Tower supporta AFT e cFCT nelle regioni opt-in

18 luglio 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 cinque aree aggiuntive Regioni AWS: Asia Pacifico (Hyderabad, Giacarta e Osaka), Israele (Tel Aviv) e Medio Oriente (Emirati Arabi Uniti).

Account Factory for Terraform (AFT) configura una pipeline Terraform per aiutarti a fornire e personalizzare gli account in AWS Control Tower. Le personalizzazioni per AWS Control Tower (cFCT) ti aiutano a personalizzare la landing zone e gli account di AWS Control Tower con CloudFormation modelli e policy di controllo dei servizi (SCPs).

Per ulteriori informazioni, visita le pagine Account Factory for Terraform e Customizations for AWS Control Tower; nella AWS Control Tower User Guide. Potresti anche voler consultare le note di rilascio sulla pagina AFT Github e sulla pagina cFCT Github. AFT e cFct sono supportati in tutte AWS le regioni, con alcune eccezioni. [Per informazioni specifiche, consulta Limitazioni regionali.](#)

AWS Control Tower aggiunge l'**ListLandingZoneOperationsAPI**

26 giugno 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha aggiunto un'API che consente di recuperare un elenco delle operazioni applicate di recente alla landing zone e delle operazioni attualmente in corso. L'API può restituire la cronologia delle operazioni di landing zone e i relativi identificatori per un massimo di 90 giorni. Per esempi di utilizzo, consulta [Visualizzare lo stato delle operazioni sulla landing zone.](#)

Per ulteriori informazioni sull'`ListLandingZoneOperations`API, consulta [ListLandingZoneOperations](#)l'articolo AWS Control Tower API Reference.

AWS Control Tower supporta fino a 100 operazioni di controllo simultanee

20 maggio 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 (OUs), contemporaneamente, dalla console o con APIs. 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 delle 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 [ListControlOperations](#)API.

La libreria AWS Control Tower contiene più di 500 controlli, che si riferiscono a diversi obiettivi di controllo, framework e servizi. Per un obiettivo di controllo specifico, come Encrypt data at rest, puoi abilitare più controlli con un'unica 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 mitiga le complessità operative.

AWS Control Tower disponibile nel AWS Canada occidentale (Calgary)

3 maggio 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

A partire da oggi, puoi attivare AWS Control Tower nella regione Canada occidentale (Calgary). Se hai già distribuito AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione, puoi farlo con la [landing zone APIs](#) di AWS Control Tower. Oppure dalla console, vai alla pagina Impostazioni nella dashboard di AWS Control Tower, seleziona le regioni e aggiorna la landing zone.

La regione Canada Ovest (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 occidentale (Calgary) come regione di residenza, le procedure per l'aggiornamento degli account, la configurazione delle automazioni degli account e qualsiasi altro processo che coinvolga Service Catalog sono diverse rispetto alle altre regioni.

Fornitura di account

Per creare e fornire un nuovo account nella regione Canada occidentale (Calgary), ti consigliamo di creare un account al di fuori di AWS Control Tower e di registrarlo in un'unità organizzativa registrata. Per ulteriori informazioni, consulta [Registrare un account esistente](#) e [Procedure per](#) registrare un account.

Il Service Catalog APIs non è disponibile nella regione Canada occidentale (Calgary). Lo script di esempio mostrato in [Automate Account Provisioning in AWS Control Tower by Service Catalog](#) non APIs 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 occidentale (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 d'origine.

Controlli

I controlli e i controlli proattivi per il 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 necessario solo per attivare i controlli proattivi basati su ganci. Alcuni controlli investigativi basati su non sono disponibili. AWS Config Per informazioni dettagliate, vedi [Limitazioni di controllo](#).

Fornitore di identità

IAM Identity Center non è disponibile in Canada occidentale (Calgary). La migliore pratica consigliata è quella di configurare la landing zone in una regione in cui è disponibile IAM Identity Center. In alternativa, hai la possibilità di gestire automaticamente la configurazione di accesso all'account se utilizzi un provider di identità esterno in Canada occidentale (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'aggiustamento delle quote in modalità self-service

25 aprile 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta gli aggiustamenti delle quote in modalità self-service tramite la console Service Quotas. Per ulteriori informazioni, consulta [Richiesta di un aumento della quota](#).

AWS Control Tower rilascia la Controls Reference Guide

21 aprile 2024

(Non è richiesto alcun aggiornamento per la landing zone 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 AWS Control Tower User Guide. La Controls Reference Guide copre i controlli in un formato esteso. Per ulteriori informazioni, consulta la [AWS Control Tower Controls Reference Guide](#).

AWS Control Tower aggiorna e rinomina due controlli proattivi

26 marzo 2024

(Non è richiesto alcun aggiornamento per la landing zone 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. 2 TLSv1](#)
- [\[CT.OPENSEARCH.PR.16 \] Richiedi un dominio Amazon OpenSearch Service per l'uso TLSv1. 2](#)

Abbiamo aggiornato i nomi dei controlli e gli artefatti per questi due controlli per allinearli alla recente versione di Amazon OpenSearch Service, che [ora supporta Transport Layer Security \(TLS\) versione 1.3](#) tra le sue opzioni di sicurezza di trasporto per la sicurezza degli endpoint di dominio.

Per aggiungere il supporto alla versione TLSv1 1.3 per questi controlli, abbiamo aggiornato l'elemento 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

(Non è richiesto alcun aggiornamento per la landing zone 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

(Non è richiesto alcun aggiornamento per la landing zone 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 a **EnabledControl**

risorse configurabili tramite modelli. CloudFormation In precedenza, era possibile aggiungere tag APIs solo tramite la console AWS Control Tower.

Le operazioni di AWS Control Tower `GetEnabledControl` e delle `ListTagsForResource` API vengono aggiornate con questa versione, poiché si basano sulla funzionalità `EnabledControl` delle risorse. `EnableControl`

Per ulteriori informazioni, consulta [Tagging EnabledControl resources in AWS Control Tower](#) e [EnabledControl](#) nella CloudFormation User Guide.

AWS Control Tower supporta APIs la registrazione e la configurazione delle unità organizzative con linee di base

14 febbraio 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Questi APIs supportano la registrazione programmatica delle unità organizzative 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 delle unità organizzative tramite la console AWS Control Tower abilita controlli opzionali e controlli obbligatori. Durante la chiamata APIs, potrebbe essere necessario completare un passaggio aggiuntivo per abilitare i controlli opzionali.

Una baseline di AWS Control Tower incorpora le best practice per la governance di AWS Control Tower di un'unità organizzativa e degli account dei membri. Ad esempio, quando si abilita una linea di base 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 .

Linee di base specifiche sono compatibili con versioni specifiche delle landing zone di AWS Control Tower. AWS Control Tower può applicare la più recente linea di base compatibile alla tua landing zone, quando modifichi le impostazioni della landing zone. Per ulteriori informazioni, consulta [Compatibilità delle versioni di base delle unità organizzative e delle landing zone](#).

Questa versione include quattro versioni essenziali [Tipi di linee di base](#)

- `AWSControlTowerBaseline`

- AuditBaseline
- LogArchiveBaseline
- IdentityCenterBaseline

Con le nuove linee di base definite, è possibile registrare APIs OUs e automatizzare il flusso di lavoro di provisioning delle unità organizzative. APIs Inoltre, possono gestire quelli OUs che sono già sotto la governance di AWS Control Tower, in modo da poterti registrare nuovamente OUs dopo gli aggiornamenti delle landing zone. APIs Includono il supporto per una CloudFormation EnabledBaseline risorsa, che consente di gestire l'infrastruttura come codice (IaC). OUs

Linea di base APIs

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Agisci sulla base di una linea di base per un'unità organizzativa.
- GetEnabledBaseline, ListEnabledBaselines: Scopri le configurazioni per le tue linee di base abilitate.
- GetBaselineOperation: Visualizza lo stato di una particolare operazione di base.
- ResetEnabledBaseline: corregge la deriva delle risorse su un'unità organizzativa con una linea di base abilitata (inclusa la deriva di controllo annidata OUs e obbligatoria). Inoltre, corregge la tendenza alla negazione del controllo da parte della regione landing-zone-level
- GetBaseline, ListBaselines: Scopri i contenuti delle linee di base di AWS Control Tower.

Per ulteriori informazioni APIs, consulta [Baseline](#) nella AWS Control Tower User Guide e nell'[API Reference](#). I nuovi APIs sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco delle aree 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 a un nuovo tipo di prodotto AWS Service Catalog esterno \(fase 3\)](#)
- [Landing zone di AWS Control Tower versione 3.3](#)
- [Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno \(fase 2\)](#)
- [AWS Control Tower annuncia i controlli per favorire la sovranità digitale](#)

- [Zona di atterraggio AWS Control Tower APIs](#)
- [Etichettatura di controllo di AWS Control Tower APIs](#)
- [AWS Control Tower disponibile in AWS Asia Pacifico \(Melbourne\)](#)
- [Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno \(fase 1\)](#)
- [AWS Control Tower aggiunge una nuova API di controllo](#)
- [AWS Control Tower aggiunge nuovi controlli](#)
- [AWS Control Tower rileva la deriva di accessi affidabili](#)
- [AWS Control Tower disponibile in quattro versioni aggiuntive Regioni AWS](#)
- [AWS Control Tower disponibile in AWS Israele \(Tel Aviv\)](#)
- [AWS Control Tower aggiunge 28 nuovi controlli proattivi](#)
- [AWS Control Tower rende obsoleti due controlli](#)
- [Landing zone di AWS Control Tower versione 3.2](#)
- [AWS Control Tower aggiunge la email-to-ID mappatura per IAM Identity Center](#)
- [AWS Control Tower aggiunge ulteriori AWS Security Hub CSPM controlli](#)
- [AWS Control Tower pubblica i metadati per i controlli AWS Security Hub CSPM](#)
- [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 di Amazon EC2](#)
- [AWS Control Tower disponibile in sette versioni aggiuntive Regioni AWS](#)
- [AWS Control Tower Account Factory Customization \(AFC\) e tracciamento delle richieste sono generalmente disponibili](#)
- [Landing zone di AWS Control Tower versione 3.1](#)
- [Controlli proattivi AWS Control Tower generalmente disponibili](#)

Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 3)

14 dicembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower non supporta più Terraform Open Source come tipo di prodotto (blueprint) durante la creazione di nuovi Account AWS. Per ulteriori informazioni e istruzioni sull'aggiornamento dei blueprint del tuo account, consulta [Transition to the AWS Service Catalog External product type](#).

Se non aggiorni i blueprint del tuo account per utilizzare il tipo di prodotto esterno, puoi solo aggiornare o chiudere gli account a cui hai fornito il provisioning utilizzando i blueprint Terraform Open Source.

Landing zone di AWS Control Tower versione 3.3

14 dicembre 2023

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.3. Per informazioni, consulta [Aggiorna la tua landing zone](#)).

Aggiornamenti alla policy sui bucket S3 nell'account AWS Control Tower Audit

Abbiamo modificato la policy dei bucket di Amazon S3 Audit che AWS Control Tower distribuisce negli account, in modo da soddisfare 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).

Puoi utilizzare la chiave di `aws:SourceOrgID` condizione e impostare il valore dell'ID dell'organizzazione nell'elemento condition della tua policy sui bucket S3. 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.

Abbiamo apportato questa modifica per porre rimedio a una potenziale vulnerabilità di sicurezza, senza influire sulla funzionalità dei carichi di lavoro esistenti. Per visualizzare la politica aggiornata, consulta [Policy sui bucket di Amazon S3 nell'account di controllo](#).

Per ulteriori informazioni sulla nuova chiave di condizione, consulta la documentazione IAM e il post sul blog IAM intitolato "Use scalable controls for AWS services access your resources».

Aggiornamenti alla policy nell'argomento AWS Config SNS

[Abbiamo aggiunto la nuova chiave di `aws:SourceOrgID` condizione alla politica per l'argomento AWS Config SNS. Per visualizzare la politica aggiornata, consulta La politica sull'argomento SNS. AWS Config](#)

Aggiornamenti alla landing zone 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-CLOUDTRAIL-MASTER` in modo che non mostri variazioni quando non viene utilizzata AWS KMS la crittografia.

Transizione a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 2)

7 dicembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

HashiCorp ha 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 in [Transition to the AWS Service Catalog External di tipo di prodotto](#) entro il 14 dicembre 2023.

AWS Control Tower annuncia i controlli per favorire la sovranità digitale

27 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 cambiamenti nelle risorse per quanto riguarda la residenza dei dati, la restrizione granulare dell'accesso, la crittografia e le capacità di resilienza. Questi controlli sono progettati per semplificare la gestione dei requisiti su larga scala. Per ulteriori informazioni sui controlli della sovranità digitale, consulta [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 abilitare la crittografia in transito o Richiedi l'implementazione di un AWS Network Firewall su più zone di disponibilità. Puoi anche personalizzare la regione AWS Control Tower Deny Control per applicare restrizioni regionali che meglio si adattano alle tue esigenze aziendali specifiche.

Questa versione offre funzionalità di negazione ben avanzate di AWS Control Tower Region. Puoi applicare un nuovo Region deny control parametrizzato a livello di unità organizzativa, per una maggiore granularità della governance, mantenendo al contempo una governance aggiuntiva della regione a livello di landing zone. Questo Region Deny Control personalizzabile consente di applicare le restrizioni regionali più adatte alle esigenze aziendali specifiche. Per ulteriori informazioni sul nuovo Region deny control configurabile, vedere [Region deny control applicato](#) all'unità organizzativa.

Come nuovo strumento per il nuovo miglioramento Region deny, questa versione include una nuova `APIUpdateEnabledControl`, che consente di ripristinare i controlli abilitati alle impostazioni predefinite. Questa API è particolarmente utile nei casi d'uso in cui è necessario risolvere rapidamente la deriva o garantire a livello di codice che un controllo non si trovi 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 un dominio REST di Amazon API Gateway per utilizzare una policy di sicurezza che specifichi una versione minima del protocollo TLS di .2 TLSv1
- CT.APPSYNC.PR.2: Richiede la configurazione di un'API AWS AppSync GraphQL con visibilità privata
- CT.APPSYNC.PR.3: Richiede che un'API AWS AppSync GraphQL non sia autenticata con 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: Richiede 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 AWS utilizzare solo i tipi di istanze Nitro quando sovrascrivi un modello di lancio

- CT.AUTOSCALING.PR.11: richiede che solo i tipi di istanze AWS Nitro che supportano la crittografia del traffico di rete tra le istanze vengano aggiunti a un gruppo Amazon EC2 Auto Scaling, quando sovrascrivi un modello di avvio
- CT.DAX.PR.3: Richiede 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 a un'istanza Amazon EC2 di utilizzare un tipo di istanza AWS Nitro durante la creazione dal tipo di risorsa AWS : : EC2 : : LaunchTemplate
- CT.EC2.PR.16: Richiedi a un'istanza Amazon EC2 di utilizzare un tipo di istanza AWS Nitro quando viene creata utilizzando il tipo di risorsa AWS : : EC2 : : Instance
- CT.EC2.PR.17: Richiede un host dedicato Amazon EC2 per utilizzare un tipo di istanza AWS Nitro
- CT.EC2.PR.18: Richiedi una flotta Amazon EC2 per sostituire solo i modelli di lancio con AWS tipi di istanze Nitro
- CT.EC2.PR.19: Richiedi a un'istanza Amazon EC2 di utilizzare un tipo di istanza nitro che supporti la crittografia in transito tra istanze quando viene creata utilizzando il tipo di risorsa AWS : : EC2 : : Instance
- CT.EC2.PR.20: Richiedi una flotta Amazon EC2 per sovrascrivere solo i modelli di lancio 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 Redis successive per attivare l'autenticazione RBAC
- CT.MQ.PR.1: Richiede un broker Amazon MQ ActiveMQ per active/standby utilizzare la modalità di distribuzione per un'elevata disponibilità
- CT.MQ.PR.2: Richiedi un broker Amazon MQ Rabbit MQ per utilizzare la modalità cluster Multi-AZ per un'elevata 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 broker del cluster
- CT.MSK.PR.2: richiede che un cluster Amazon Managed Streaming for Apache Kafka (MSK) sia configurato come disattivato PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Richiede l'implementazione di un firewall AWS Network Firewall su più zone di disponibilità
- CT.RDS.PR.26: Richiede un proxy Amazon RDS DB 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: Richiedi che un cluster Amazon RDS non sia configurato per essere accessibile al pubblico 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 disponga di una configurazione Block Public Access (BPA) con tutte le opzioni impostate su true

Nuovi controlli preventivi

- CT.APPSYNC.PV.1Richiedi che un'API AWS AppSync GraphQL sia configurata con visibilità privata
- CT.EC2.PV.1Richiedi la creazione di uno snapshot 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 possa essere ripristinato pubblicamente
- CT.EC2.PV.4Richiedi che Amazon EBS direct non APIs venga chiamato
- CT.EC2.PV.5Impedisce l'uso dell'importazione e dell'esportazione di macchine virtuali Amazon EC2
- CT.EC2.PV.6Impedisce l'uso di azioni Amazon EC2 e API obsolete RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1È necessario che una policy AWS KMS chiave contenga una dichiarazione che limiti la concessione di sovvenzioni ai servizi AWS KMS AWS
- CT.KMS.PV.2Richiede che una chiave AWS KMS asimmetrica con materiale chiave RSA utilizzato per la crittografia non abbia una lunghezza di 2048 bit
- CT.KMS.PV.3Richiede che una AWS KMS chiave sia configurata con il controllo di sicurezza del blocco della politica di bypass 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.6Richiede che una chiave AWS KMS gestita dal cliente (CMK) sia configurata con materiale chiave proveniente da un archivio di chiavi esterno (XKS)
- CT.LAMBDA.PV.1Richiedi un URL di AWS Lambda funzione per utilizzare l'autenticazione basata su IAM AWS
- CT.LAMBDA.PV.2Richiedi che l'URL di una AWS Lambda funzione sia configurato per l'accesso solo ai responsabili interni al tuo Account AWS

Zona di atterraggio AWS Control Tower APIs

26 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora offre offerte APIs che ti aiutano a gestire la tua landing zone in modo programmatico. Questi APIs consentono di creare, aggiornare e reimpostare la landing zone, nonché di recuperare informazioni sulla configurazione e sulle operazioni della landing zone. Per ulteriori informazioni, consulta [Esempi di API per le zone di atterraggio](#).

Le landing zone APIs sono disponibili in tutte le aree in Regioni AWS cui è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

Etichettatura di controllo di AWS Control Tower APIs

10 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora offre offerte APIs che ti aiutano a etichettare i controlli abilitati in modo programmatico. Queste APIs consentono di aggiungere, rimuovere ed elencare i tag per i controlli abilitati. Per ulteriori informazioni, consulta [Tagging delle risorse di AWS Control Tower](#).

I tag di controllo APIs sono disponibili in tutte le aree in Regioni AWS cui è disponibile AWS Control Tower, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower disponibile in AWS Asia Pacifico (Melbourne)

3 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 a un nuovo tipo di prodotto AWS Service Catalog esterno (fase 1)

31 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

HashiCorp ha 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 in [Transition to the AWS Service Catalog External di tipo di prodotto](#) entro il 14 dicembre 2023.

AWS Control Tower aggiunge una nuova API di controllo

27 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 si trovi in uno stato di deriva. Per ulteriori informazioni sulla nuova API, consulta [l'AWS Control Tower API Reference](#).

L'`UpdateEnabledControl` API 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 delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower aggiunge nuovi controlli

20 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 di controllo](#).

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower rileva la deriva di accessi affidabili

13 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora rileva e segnala eventuali deviazioni per ottenere impostazioni di accesso affidabili. Le impostazioni di accesso affidabili 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 [Types of governance drift](#).

Il rilevamento affidabile della deriva degli accessi è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower disponibile in quattro versioni aggiuntive Regioni AWS

29 settembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower è disponibile in quattro versioni aggiuntive Regioni AWS: Asia Pacifico (Hyderabad), Asia Pacifico (Giacarta), Europa (Spagna) ed Europa (Zurigo). Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta la [Regione AWS tabella](#).

AWS Control Tower disponibile in AWS Israele (Tel Aviv)

1 agosto 2023

(Non è richiesto alcun aggiornamento per la landing zone 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

(Non è richiesto alcun aggiornamento per la landing zone 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 di controllo](#).

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower rende obsoleti due controlli

27 luglio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha reso obsoleti due controlli: e. CT.CLOUDFORMATION.PR.2 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

Landing zone di AWS Control Tower versione 3.2

16 giugno 2023

(Aggiornamento richiesto 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 del 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 Tower. `AWSServiceRoleForAWSControlTower` Questo ruolo assiste AWS Control Tower creando una `EventBridge Managed Rule`, denominata `AWSControlTowerManagedRule` in ogni account membro. Questa regola gestita raccoglie gli eventi di AWS Security Hub CSPM Finding, che con AWS Control Tower possono 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; viene distribuita direttamente da `EventBridge APIs`. È possibile visualizzare la regola nella `EventBridge console` o tramite `EventBridge APIs`. Se il `managed-by` campo è compilato, mostrerà il principale del servizio AWS Control Tower.

In precedenza, AWS Control Tower si occupava di eseguire operazioni negli account dei membri. Questo nuovo ruolo e questa nuova regola si allineano meglio con il principio delle migliori pratiche di concedere il minimo privilegio quando si eseguono operazioni in un ambiente con più AWS account. Il nuovo ruolo fornisce autorizzazioni ridotte che consentono in particolare: 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 landing zone 3.2 include anche una nuova `StackSet` risorsa nell'account di gestione `BP_BASELINE_SERVICE_LINKED_ROLE`, che inizialmente implementa il ruolo collegato ai servizi.

Quando segnala una deviazione del controllo di Security Hub CSPM (nella landing zone 3.2 e successive), AWS Control Tower riceve un aggiornamento di stato giornaliero dal 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](#).

Aggiorna il controllo Region Deny

Questa versione della landing zone include anche un aggiornamento del Region Deny control.

Servizi globali e aggiunti APIs

- Gestione dei 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 per la console di gestione (`consoleapp:*`)
- AWS Livello gratuito (`freetier:*`)
- Fatturazione AWS (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS Notifiche utente (`notifications:*`)
- AWS Contatti per le notifiche utente (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Impostazioni fiscali (`tax:*`)

Servizi globali e APIs rimossi

- Rimossa `s3:GetAccountPublic` perché non è un'azione valida.
- Rimossa `s3:PutAccountPublic` perché non è un'azione valida.

AWS Control Tower aggiunge la email-to-ID mappatura per IAM Identity Center

13 luglio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta la email-to-ID mappatura per IAM Identity Center. Questa funzionalità consente di mappare gli indirizzi e-mail agli utenti di IAM Identity Center IDs, il che semplifica la gestione dell'accesso degli utenti al tuo ambiente AWS Control Tower. Per ulteriori informazioni sulla email-to-ID mappatura, consulta [Integrazione con IAM Identity Center](#).

Email-to-ID la mappatura è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower aggiunge ulteriori AWS Security Hub CSPM controlli

29 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ha aggiunto ulteriori 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 di controllo](#).

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower pubblica i metadati per i controlli AWS Security Hub CSPM

22 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora pubblica i metadati per AWS Security Hub CSPM i controlli. Questi metadati includono informazioni sul controllo, come l'ID del controllo, il titolo e la descrizione del controllo. Per ulteriori informazioni sui metadati, consulta Metadati di [controllo](#).

I metadati di controllo sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta 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, vedere [Account Factory Customization](#) for Terraform.

AFC for Terraform è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree 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

(Non è richiesto alcun aggiornamento per la landing zone 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](#).

Il centro di identità IAM autogestito è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree 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

(Non è richiesto alcun aggiornamento per la landing zone 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 [Mixed governance](#).

La nota di governance mista è disponibile Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower aggiunge nuovi controlli proattivi

25 maggio 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 di controllo](#).

I nuovi controlli sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower aggiorna i controlli di Amazon EC2

18 maggio 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

AWS Control Tower disponibile in sette versioni aggiuntive Regioni AWS

11 maggio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower è disponibile in sette paesi aggiuntivi Regioni AWS: Asia Pacifico (Osaka), Canada (Centrale), Europa (Milano), Europa (Stoccolma), Medio Oriente (Bahrein), 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 [Regione AWS tabella](#).

AWS Control Tower Account Factory Customization (AFC) e tracciamento delle richieste sono generalmente disponibili

27 aprile 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower Account Factory Customization (AFC) e il tracciamento delle richieste sono ora disponibili a livello generale. AFC ti consente di personalizzare i tuoi account AWS Control Tower e il tracciamento delle richieste ti consente di monitorare lo stato delle tue richieste AWS Control Tower. [Per ulteriori informazioni su AFC e il tracciamento delle richieste, vedere Account Factory Customization e Request tracing](#).

AFC e il tracciamento delle richieste sono disponibili Regioni AWS ovunque sia disponibile AWS Control Tower. Per un elenco delle aree Regioni AWS in cui è disponibile AWS Control Tower, consulta la [Regione AWS Tabella](#).

Landing zone di AWS Control Tower versione 3.1

9 febbraio 2023

(Aggiornamento richiesto per la landing zone 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. In base a una AWS Security Hub CSPM regola, [\[S3.9\] La registrazione degli accessi al server con bucket S3](#) deve essere abilitata. In linea con Security Hub CSPM, si consiglia di eliminare questo particolare risultato, come indicato nella descrizione CSPM di Security Hub di questa regola. [Per ulteriori informazioni, vedere le informazioni sui risultati soppressi.](#)
- La registrazione degli accessi per il (normale) bucket di registrazione nell'account Log Archive è rimasta 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 utilizzando la registrazione degli accessi al server nella documentazione di Amazon S3](#).
- Abbiamo aggiornato il controllo Region Deny. Questo aggiornamento consente azioni da parte di più servizi globali. Per i dettagli su questo SCP, consulta [Negare l'accesso a in AWS base alla richiesta 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 Lightsail () lightsail:Get*
- Esploratore di risorse AWS (resource-explorer-2:*)
- Amazon S3 (s3:CreateMultiRegionAccessPoint,,s3:GetBucketPolicyStatus)
s3:PutMultiRegionAccessPointPolicy
- AWS Savings Plans (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

Controlli proattivi AWS Control Tower generalmente disponibili

13 aprile 2023

(Non è richiesto alcun aggiornamento per la landing zone 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 delle aree 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 sull'account](#)
- [Personalizzazione Account Factory \(AFC\)](#)
- [I controlli completi facilitano l'approvvigionamento e AWS la gestione delle risorse](#)
- [Lo stato di conformità è visualizzabile per tutte le AWS Config regole](#)
- [API per i controlli e una nuova risorsa CloudFormation](#)
- [cFct supporta l'eliminazione di set di stack](#)
- [Conservazione personalizzata dei log](#)
- [È disponibile la riparazione della deriva dei ruoli](#)
- [Landing zone di AWS Control Tower versione 3.0](#)
- [La pagina Organizzazione combina visualizzazioni e account OUs](#)
- [Creazione e registrazione semplificate dell'account](#)
- [AFT supporta la personalizzazione automatizzata per gli account AWS Control Tower condivisi](#)
- [Operazioni simultanee per tutti i controlli opzionali](#)
- [Account di sicurezza e registrazione esistenti](#)
- [Landing zone di AWS Control Tower versione 2.9](#)
- [Landing zone di AWS Control Tower versione 2.8](#)

Operazioni simultanee sull'account

16 dicembre 2022

(Non è richiesto alcun aggiornamento per la landing zone 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 i tuoi account finiscono di crescere 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 Account Factory (AFC)

28 novembre 2022

(Non è richiesto alcun aggiornamento per la landing zone 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 necessaria per definire i blueprint degli account, che sono CloudFormation modelli contenuti in un prodotto Service Catalog specializzato. I blueprints 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 progetti per creare nuovi account, registrare altri account in AWS Control Tower e aggiornare AWS gli account AWS Control Tower esistenti.

Quando esegui il provisioning, registri o aggiorni un account in Account Factory, selezionerai il blueprint da implementare. Le risorse specificate nel blueprint vengono fornite nel tuo account. Al termine della 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. Puoi anche 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 facilitano l'approvvigionamento e AWS la gestione delle risorse

28 novembre 2022

(Non è richiesto alcun aggiornamento per la landing zone 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 vengono definiti proattivi perché controllano le risorse, prima che vengano distribuite, per determinare se le nuove risorse siano conformi ai controlli attivati nell'ambiente.

Oltre 130 nuovi controlli proattivi ti aiutano a raggiungere obiettivi di policy specifici per il tuo ambiente AWS Control Tower, a soddisfare i requisiti dei framework di conformità standard del settore e a governare le interazioni AWS Control Tower su più di venti altri servizi. AWS

La libreria di controlli AWS Control Tower classifica questi controlli in base ai AWS servizi e alle risorse associati. Per maggiori dettagli, consulta [Proactive](#) controls.

Con questa versione, AWS Control Tower è inoltre integrato con AWS Security Hub CSPM, tramite il nuovo Security Hub CSPM Service-Managed Standard: AWS Control Tower, che supporta lo standard AWS Foundational Security Best Practices (FSBP). Puoi visualizzare oltre 160 controlli Security Hub CSPM 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 del Security Hub](#).

Lo stato di conformità è visualizzabile per tutte le AWS Config regole

18 novembre 2022

(Non è richiesto alcun aggiornamento per la landing zone 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 influiscono sui tuoi account in AWS Control Tower, registrati o annullati, senza dover uscire dalla console AWS Control Tower. I clienti possono scegliere di configurare le regole di Config, chiamate controlli investigativi, in AWS Control Tower o di configurarle direttamente tramite il AWS Config servizio. AWS Config Vengono mostrate 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 conformi AWS Config . 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 Config, 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 dalle regole di AWS Control Tower e Config distribuite all'esterno di AWS Control Tower.

API per i controlli e una nuova risorsa CloudFormation

1 settembre 2022

(Non è richiesto alcun aggiornamento per la landing zone 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](#).

Questi APIs consentono di abilitare, disabilitare e visualizzare lo stato dell'applicazione dei controlli nella libreria AWS Control Tower. APIs 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 delle policy relative a un'intera unità organizzativa (OU) e a ogni AWS account all'interno dell'unità organizzativa. Queste regole rimangono in vigore quando crei nuovi account o apporti modifiche agli account esistenti.

APIs incluso 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 nell'unità organizzativa specificata e gli account in essa contenuti.
- **GetControlOperation**— Restituisce lo stato di un particolare o di un'operazione.
EnableControlDisableControl
- **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 [Resource identifiers for APIs and controls](#), nella AWS Control Tower User Guide.

cFct supporta l'eliminazione di set di stack

26 agosto 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

Le personalizzazioni per AWS Control Tower (cFCT) ora supportano l'eliminazione di stack set, impostando un parametro nel file `manifest.yaml`. Per ulteriori informazioni, consulta [Eliminazione di un set di stack](#).

Important

Quando imposti inizialmente il valore di `enable_stack_set_deletion` to `true`, la prossima volta che richiami cFCT, TUTTE le risorse che iniziano con il

prefisso `CustomControlTower-`, a cui è associato il tag `key` e che non sono dichiarate nel file `manifestKey:AWS_Solutions, Value: CustomControlTowerStackSet`, vengono eliminate.

Conservazione personalizzata dei log

15 agosto 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower. Per informazioni, vedi [Aggiorna la tua landing zone](#))

AWS Control Tower ora offre 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 aggiorni o ripari la landing zone e per i nuovi clienti tramite la configurazione di AWS Control Tower

È disponibile la riparazione della deriva dei ruoli

11 agosto 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora supporta la riparazione per la deriva dei ruoli. Puoi ripristinare un ruolo richiesto senza una riparazione completa della landing zone. Se è necessaria una riparazione del drift di questo tipo, la pagina di errore della console fornisce i passaggi per ripristinare il ruolo, in modo che la landing zone sia nuovamente disponibile.

Landing zone di 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 rinunciare ai 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 d'origine.
- Un aggiornamento alla Region Deny Control.
- 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 il relativo account trail. Con gli itinerari organizzativi, ne creiamo solo uno nell'account di gestione.

Le seguenti sezioni forniscono maggiori dettagli su ogni nuova funzionalità.

CloudTrail Percorsi a livello di organizzazione in AWS Control Tower

Con la versione 3.0 di landing zone, AWS Control Tower ora supporta percorsi a livello di organizzazione AWS CloudTrail .

Quando aggiorni la landing zone di AWS Control Tower alla versione 3.0, hai la possibilità di selezionare AWS CloudTrail percorsi a livello di organizzazione come preferenza di registrazione o di disattivare i CloudTrail percorsi gestiti da AWS Control Tower. Quando esegui l'aggiornamento alla versione 3.0, AWS Control Tower elimina gli itinerari a livello di account esistenti per gli account registrati dopo un periodo di attesa di 24 ore. AWS Control Tower non elimina gli itinerari a livello di account per gli account non registrati. Nel caso improbabile che l'aggiornamento della landing zone non vada a buon fine, ma l'errore si verifichi dopo che AWS Control Tower ha già creato il trail a livello di organizzazione, potresti incorrere in addebiti duplicati per i trail a livello di organizzazione e account, fino a quando l'operazione di aggiornamento non sarà completata correttamente.

A partire dalla landing zone 3.0, AWS Control Tower non supporta più percorsi a livello di account che AWS gestiscono. Al contrario, AWS Control Tower crea un percorso a livello di organizzazione, attivo o inattivo, in base alla selezione effettuata.

 Note

Dopo l'aggiornamento alla versione 3.0 o successiva, non hai la possibilità di continuare con gli CloudTrail itinerari 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 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 registri delle tracce degli account vengono archiviati con un percorso di questo formato: `/org id/AWSLogs/...`
- I log degli itinerari organizzativi vengono archiviati con un percorso in questo formato: `/org id/AWSLogs/org id/...`

Il percorso creato da AWS Control Tower per gli CloudTrail itinerari a livello di organizzazione è diverso dal percorso predefinito per un itinerario 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 files*.](#)
[CloudTrail](#)

 Tip

Se hai intenzione di creare e gestire percorsi a livello di account, ti consigliamo di creare i nuovi trail prima di completare l'aggiornamento alla versione 3.0 di AWS Control Tower landing zone, per iniziare subito a registrare.

In qualsiasi momento, puoi scegliere di creare nuovi percorsi a livello di account o di 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 delle landing zone alla versione 3.0 o successiva. Puoi attivare e disattivare i percorsi a livello di organizzazione ogni volta che aggiorni la tua landing zone.

Se i tuoi log sono gestiti da un servizio di terze parti, assicurati di fornire il nuovo nome del percorso al servizio.

Note

Per le zone di atterraggio nella versione 3.0 o successiva, i AWS CloudTrail trail a livello di account non sono supportati da AWS Control Tower. Puoi creare e gestire percorsi a livello di account in qualsiasi momento oppure puoi optare per 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 landing zone, 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 per le risorse globali è abilitata solo nella tua regione d'origine.

Questa configurazione è considerata una procedura consigliata. È consigliata da AWS Security Hub CSPM 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 ogni Regione governata.

Due nuovi controlli investigativi per la AWS CloudTrail registrazione

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 CloudTrail è abilitato. Il primo controllo è dotato di Indicazioni obbligatorie ed è abilitato sulla Security OU durante la configurazione o gli aggiornamenti delle landing zone della versione 3.0 e successive. Il secondo controllo include le linee guida fortemente consigliate e, facoltativamente, viene applicato a qualsiasi unità OUs diversa dalla Security OU, sulla quale è già applicata la protezione di controllo obbligatoria.

Controllo obbligatorio: [rileva se gli account condivisi nell'unità organizzativa Security hanno AWS CloudTrail o CloudTrail Lake è abilitato](#)

Controllo fortemente consigliato: [rileva se un account ha AWS CloudTrail o CloudTrail Lake è abilitato](#)

Per ulteriori informazioni sui nuovi controlli, consulta [la libreria di controlli AWS Control Tower](#).

Un aggiornamento alla Region Deny Control

Abbiamo aggiornato l'NotActionelenco nella sezione Region Deny Control per includere le azioni di 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 landing zone esistente di AWS Control Tower 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.

[Guida video sull'aggiornamento di una zona di atterraggio AWS Control Tower esistente alla Landing Zone 3.](#)

La pagina Organizzazione combina visualizzazioni e account OUs

18 luglio 2022

(Nessun aggiornamento richiesto per la landing zone di AWS Control Tower)

La nuova pagina Organization in AWS Control Tower mostra una visualizzazione gerarchica (ad albero) di tutte le unità organizzative (OUs) e gli account. Combina le informazioni delle pagine OUs e Accounts, che esistevano in precedenza.

Nella nuova pagina, puoi vedere le relazioni tra i genitori OUs e i relativi annidati OUs e gli account, puoi agire 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 OUs solo gli account, scegliere di visualizzare solo gli account registrati e registrati OUs oppure è possibile visualizzare gruppi di risorse correlate. È più facile garantire che l'intera organizzazione sia aggiornata correttamente.

Creazione e registrazione semplificate dell'account

30 giugno 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower).

AWS Control Tower ora offre 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 Service Catalog. Per ulteriori informazioni, consulta [Registra un account esistente dalla console AWS Control Tower](#).

AFT supporta la personalizzazione automatizzata per gli account AWS Control Tower condivisi

27 maggio 2022

(Nessun aggiornamento richiesto per la landing zone di AWS Control Tower)

Account Factory for Terraform (AFT) ora può personalizzare e aggiornare in modo programmatico tutti gli account gestiti da AWS Control Tower, inclusi l'account di gestione, l'account di audit e l'account di archiviazione 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 sei tu a definire il ruolo che svolge il lavoro.

Il AWSAFTExecutionruolo esistente ora implementa personalizzazioni in tutti gli account. Puoi configurare le autorizzazioni IAM con limiti che limitano l'accesso al AWSAFTExecutionruolo in base ai tuoi 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 AWSAFTServiceRuolo per distribuire le risorse AFT in tutti gli account gestiti, inclusi gli account condivisi e l'account di gestione. Le risorse in precedenza venivano impiegate dal ruolo. AWSAFTExecution

Il provisioning degli account condivisi e di gestione di AWS Control Tower non viene fornito tramite Account Factory, quindi non sono inclusi i prodotti forniti 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 landing zone 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 orari limitati sono quelli in cui AWS Control Tower è in fase di configurazione della landing zone o durante l'estensione della governance a una nuova organizzazione.

Funzionalità supportate per i controlli preventivi:

- Applica e rimuovi controlli preventivi diversi sulla stessa unità organizzativa.
- Applica e rimuovi controlli preventivi diversi su diversi OUs, contemporaneamente.
- Applica e rimuovi lo stesso controllo preventivo su più OUs dispositivi contemporaneamente.
- È possibile applicare e rimuovere qualsiasi controllo preventivo e investigativo contemporaneamente.

Puoi sperimentare questi miglioramenti della concorrenza di controllo in tutte le versioni rilasciate di AWS Control Tower.

Quando si applicano controlli preventivi a nested OUs, i controlli preventivi influiscono su tutti gli account e sono OUs annidati nell'unità organizzativa di destinazione, anche se tali account non OUs

sono registrati presso AWS Control Tower. I controlli preventivi vengono implementati utilizzando Service Control Policies (SCPs), che fanno parte di AWS Organizations. I controlli investigativi vengono implementati utilizzando AWS Config regole. I guardrail rimangono in vigore quando crei nuovi account o apporti modifiche agli account esistenti e AWS Control Tower fornisce un rapporto riepilogativo di come ogni account è conforme alle policy 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 ora offre 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 landing zone. Questa opzione elimina la necessità per AWS Control Tower di creare nuovi account condivisi. L'account di sicurezza, denominato di default account Audit, è un account con restrizioni che consente ai team di sicurezza e conformità di accedere a tutti gli account nella landing zone. L'account di registrazione, chiamato per impostazione predefinita account Log Archive, funziona come un repository. Memorizza i registri delle attività delle API e delle configurazioni delle risorse da tutti gli account nella landing zone.

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 landing zone alternativa. L'opzione per utilizzare gli account esistenti viene visualizzata durante la configurazione iniziale della landing zone. Include controlli durante il processo di configurazione, che garantiscono una corretta implementazione. AWS Control Tower implementa i ruoli e i controlli necessari sugli account esistenti. Non rimuove o unisce risorse o dati esistenti in questi account.

Limitazione: se prevedi di portare AWS account esistenti in AWS Control Tower come account di audit e archiviazione dei log e se tali account dispongono di AWS Config risorse esistenti, devi eliminare le AWS Config risorse esistenti prima di poterli registrare in AWS Control Tower.

Landing zone 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 inoltro di notifiche Lambda per utilizzare il runtime Python versione 3.9. Questo aggiornamento risolve il problema della deprecazione della versione 3.6 di Python, prevista per luglio 2022. Per le informazioni più recenti, consulta [la pagina di deprecazione di Python](#).

Landing zone 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 alle [AWS Foundational Security Best Practices](#).

In questa versione:

- La registrazione degli accessi è configurata per il bucket di log di accesso nell'account Log Archive, per tenere traccia dell'accesso al bucket di 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 periodo 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 configurare e gestire le regole di Config in base alle migliori pratiche 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. CloudTrail
- La versione include un aggiornamento alla Region Deny Control, per consentire l'utilizzo della funzionalità. `route53-application-recovery us-west-2`
- Aggiornamento: il 15 febbraio 2022, abbiamo rimosso la coda delle lettere morte per le funzioni AWS Lambda.

Ulteriori dettagli:

- Se disattivi una landing zone, AWS Control Tower non rimuove il ruolo collegato al AWS Config servizio.
- Se esegui il deprovisioning di un account Account Factory, AWS Control Tower non rimuove il ruolo collegato al AWS Config servizio.

Per aggiornare la tua landing zone alla versione 2.8, vai alla pagina delle impostazioni della zona di atterraggio, seleziona la versione 2.8, quindi scegli **Aggiorna**. Dopo aver aggiornato la landing zone, devi aggiornare tutti gli account governati 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 della regione](#)
- [Funzionalità di residenza dei dati](#)
- [AWS Control Tower introduce il provisioning e la personalizzazione degli account Terraform](#)
- [Nuovo evento sul ciclo di vita disponibile](#)
- [AWS Control Tower abilita il nested OUs](#)
- [Detective controlla la concorrenza](#)
- [Sono disponibili due nuove regioni](#)
- [Deselezione della regione](#)
- [AWS Control Tower funziona con i sistemi di gestione delle AWS chiavi](#)
- [Controlli rinominati, funzionalità invariata](#)
- [AWS Control Tower esegue scansioni SCPs giornaliere per verificare eventuali deviazioni](#)
- [Nomi e account personalizzati OUs](#)
- [Landing zone di AWS Control Tower versione 2.7](#)
- [Tre nuove AWS regioni disponibili](#)
- [Governa solo le regioni selezionate](#)
- [AWS Control Tower ora estende la governance OUs alle AWS organizzazioni esistenti](#)
- [AWS Control Tower fornisce aggiornamenti in blocco degli account](#)

Funzionalità di negazione della regione

30 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone 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 deselegione della regione esistenti in AWS Control Tower. Insieme, queste funzionalità ti aiutano a risolvere i problemi di conformità e regolamentazione, bilanciando al contempo i costi associati all'espansione in altre regioni.

Ad esempio, AWS i clienti in Germania possono negare l'accesso ai servizi in regioni AWS 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 atterraggio. La funzionalità Region Deny è disponibile quando aggiorni la versione della landing zone di AWS Control Tower. Alcuni AWS servizi sono esenti dalle funzionalità Region Deny. Per ulteriori informazioni, consulta [Configurare il Region Deny](#) Control.

Funzionalità di residenza dei dati

30 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora offre controlli appositamente progettati 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 Impedire connessioni Amazon Virtual Private Network (VPN) o Non consentire 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 landing zone 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 fornisce gli 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 Terraform Cloud, Terraform Enterprise e Terraform Open Source.

Nuovo evento sul ciclo di vita disponibile

18 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

L'evento `PrecheckOrganizationalUnit` registra se alcune risorse impediscono il successo dell'attività di governance Extend, incluse le risorse in OUs nested. Per ulteriori informazioni, consulta [PrecheckOrganizationalUnit](#).

AWS Control Tower abilita il nested OUs

16 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora ti consente di includere nested OUs come parte della tua landing zone.

AWS Control Tower fornisce supporto per unità organizzative annidate (OUs), che consentono di organizzare gli account in più livelli gerarchici e di applicare i controlli preventivi gerarchicamente. Puoi registrare contenuti OUs annidati OUs, creare e registrare OUs sotto parent e abilitare i controlli su qualsiasi unità organizzativa registrata OUs, indipendentemente dalla profondità. Per supportare questa funzionalità, la console mostra il numero di account gestiti e OUs.

Con nested OUs, puoi allineare la tua AWS Control Tower OUs alla strategia AWS multi-account e ridurre il tempo necessario per abilitare i controlli su più account OUs, applicando i controlli a livello di unità organizzativa principale.

Considerazioni chiave

1. Puoi registrare un'unità organizzativa esistente a più livelli OUs con AWS Control Tower un'unità organizzativa alla volta, iniziando dall'unità organizzativa di primo livello e poi procedendo verso il basso. Per ulteriori informazioni, consulta [Espandi da una struttura OU piatta a una struttura di unità organizzative annidate](#).
2. Gli account direttamente collegati a un'unità organizzativa registrata vengono registrati automaticamente. Gli account più in basso nell'albero possono essere registrati registrando l'unità organizzativa principale diretta.
3. I controlli preventivi (SCPs) vengono ereditati automaticamente nella gerarchia; SCPs applicati all'elemento principale vengono ereditati da tutti gli utenti annidati. OUs
4. I controlli Detective (regole di AWS Config) 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 OUs account e su di essa.
7. Non è possibile crearne di nuovi OUs annidati nella Security OU (Core OU).

Detective controlla la concorrenza

5 novembre 2021

(Aggiornamento opzionale per la landing zone 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 abilitata e rileva se è consentito l'accesso pubblico in scrittura ai bucket Amazon S3).
- Abilita diversi controlli investigativi su diversi OUs sistemi contemporaneamente.

- La messaggistica di errore di Guardrail è stata migliorata per fornire ulteriori indicazioni per le operazioni di controllo simultaneo supportate.

Non supportato in questa versione:

- L'attivazione dello stesso controllo investigativo su più controlli OUs simultanei non è supportata.
- La concorrenza del controllo preventivo non è supportata.

Puoi sperimentare 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 landing zone per sfruttare altre funzionalità, come la selezione e la deselezionazione della regione, disponibili nella versione più recente.

Sono disponibili due nuove regioni

29 luglio 2021

(Aggiornamento richiesto per la landing zone 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 multi-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 Landing Zone nella dashboard di AWS Control Tower, quindi seleziona le regioni. Dopo aver aggiornato la landing zone, devi [aggiornare tutti gli account governati da AWS Control Tower](#).

Deselezione della regione

29 luglio 2021

(Aggiornamento opzionale per la landing zone 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 siano gestite

da AWS Control Tower. Questa funzionalità offre la possibilità di affrontare i problemi di conformità e regolamentazione, bilanciando al contempo i costi associati all'espansione in altre regioni.

La deselezionazione della regione è disponibile quando aggiorni la versione della landing zone di AWS Control Tower.

Quando utilizzi 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 prescelte 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 i sistemi di gestione delle AWS chiavi

28 luglio 2021

(Aggiornamento opzionale per la landing zone 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 da te 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 avanzato di crittografia rispetto alla crittografia SSE-S3 che AWS Control Tower utilizza 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 log sensibili. È necessario utilizzare chiavi AWS gestite da KMS (SSE-KMS) per la crittografia a riposo. AWS Il supporto per la crittografia KMS è disponibile quando configuri una nuova landing zone o quando aggiorni la landing zone AWS Control Tower esistente.

Per configurare questa funzionalità, puoi selezionare KMS Key Configuration durante la configurazione iniziale della landing zone. Puoi scegliere una chiave KMS esistente oppure puoi selezionare un pulsante che ti indirizza alla console AWS KMS per crearne una nuova. Hai anche la flessibilità di passare dalla crittografia predefinita a SSE-KMS o a una chiave SSE-KMS diversa.

Per una landing zone AWS Control Tower esistente, puoi eseguire un aggiornamento per iniziare a utilizzare le chiavi AWS KMS.

Controlli rinominati, funzionalità invariata

26 luglio 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower sta rivedendo alcuni nomi e descrizioni dei controlli per rispecchiare meglio le intenzioni politiche del controllo. I nomi e le descrizioni rivisti 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 «Non consentire» a «Rileva» perché il controllo investigativo di per sé non blocca un'azione specifica, rileva solo le violazioni delle norme 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 scansioni SCPs giornaliere per verificare eventuali deviazioni

11 maggio 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora esegue scansioni automatiche giornaliere dei SCPs dati gestiti per verificare che i controlli corrispondenti siano applicati correttamente e che non abbiano subito variazioni. Se una scansione rileva una deviazione, 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.

Nomi e account personalizzati OUs

16 aprile 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora consente di personalizzare la denominazione delle landing zone. Puoi mantenere i nomi consigliati da AWS Control Tower per le unità organizzative (OUs) e gli account principali oppure puoi modificare questi nomi durante il processo di configurazione iniziale della landing zone.

I nomi predefiniti forniti da AWS Control Tower per OUs 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 delle unità organizzative e degli account ti offre la flessibilità necessaria per affrontare tali vincoli.

Oltre a modificare il flusso di lavoro durante la configurazione, l'unità organizzativa precedentemente nota come unità organizzativa principale è ora denominata Security OU e l'unità organizzativa precedentemente nota come unità organizzativa personalizzata è ora denominata Sandbox OU. Abbiamo apportato questa modifica per migliorare il nostro allineamento alle linee guida generali sulle migliori pratiche per la denominazione. AWS

I nuovi clienti vedranno questi nuovi nomi di unità organizzative. I clienti esistenti continueranno a vederne i nomi originali OUs. È possibile che si verifichino alcune incongruenze nella denominazione delle unità organizzative durante l'aggiornamento della 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 la zona di atterraggio in alto a destra. Per ulteriori informazioni, puoi leggere come pianificare la tua landing zone di AWS Control Tower.

Landing zone di AWS Control Tower versione 2.7

8 aprile 2021

(Aggiornamento richiesto per la landing zone 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 di Log Archive che implementano policy esclusivamente sulle risorse AWS Control Tower. Abbiamo modificato le linee guida su quattro controlli di Log Archive esistenti da obbligatori a facoltativi, poiché stabiliscono policy per le risorse esterne a AWS Control Tower. Questa modifica ed espansione del controllo offre la possibilità di separare la governance di Log Archive 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 garantire 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 che non sono distribuiti da AWS Control Tower.

Nuovi controlli obbligatori:

- Impedisce modifiche alla configurazione di crittografia per i bucket S3 creati da AWS Control Tower in Log Archive
- Impedisce modifiche alla configurazione di registrazione per i bucket S3 creati da AWS Control Tower in Log Archive
- Impedisce modifiche alla policy sui bucket per i bucket S3 creati da AWS Control Tower in Log Archive
- Impedisce modifiche alla configurazione del ciclo di vita per i bucket S3 creati da AWS Control Tower in Log Archive

La guida è stata modificata da obbligatoria a facoltativa:

- Non consentire modifiche alla configurazione di crittografia per tutti i bucket Amazon S3 [in precedenza: Abilita la crittografia a riposo per l'archiviazione dei log]
- Non consentire modifiche alla configurazione di registrazione per tutti i bucket Amazon S3 [in precedenza: Abilita la registrazione degli accessi per l'archiviazione dei log]
- Non consentire modifiche alla policy sui bucket per tutti i bucket Amazon S3 [in precedenza: non consentire modifiche alle policy all'archivio dei log]
- Non consentire modifiche alla configurazione del ciclo di vita per tutti i bucket Amazon S3 [in precedenza: impostare una politica di conservazione per l'archiviazione dei log]

La versione 2.7 di AWS Control Tower include modifiche al blueprint delle landing zone 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 abilita `BlockPublicAccess` automaticamente i bucket S3 distribuiti da AWS Control Tower. Puoi disattivare questa impostazione predefinita se il tuo carico di lavoro richiede l'accesso a più account. Per ulteriori informazioni su cosa succede con `BlockPublicAccess` enabled, 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 ripristinata dopo l'aggiornamento 2.7 alla landing zone.

Ti consigliamo di modificare le tue richieste per utilizzare TLS anziché HTTP.

Tre nuove AWS regioni disponibili

8 aprile 2021

(Aggiornamento richiesto per la landing zone 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 delle landing zone alla versione 2.7 per espandere la governance in queste regioni.

La tua landing zone non viene espansa automaticamente in queste regioni quando esegui l'aggiornamento alla versione 2.7, devi visualizzarle e selezionarle nella tabella Regioni per includerle.

Governa solo le regioni selezionate

19 febbraio 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

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.

La selezione della regione è disponibile quando configuri una nuova landing zone o aggiorni la versione della landing zone di AWS Control Tower. Quando usi Account Factory per creare un nuovo account o registrare un account membro preesistente, o 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 controllo centralizzati nelle regioni prescelte negli account. Per ulteriori informazioni sulla selezione delle regioni, consulta. [Configura le tue regioni AWS Control Tower](#)

AWS Control Tower ora estende la governance OUs alle AWS organizzazioni esistenti

28 gennaio 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

Estendi la governance alle unità organizzative esistenti (OUs) (quelle non presenti in AWS Control Tower) dall'interno della console AWS Control Tower. Con questa funzionalità, puoi portare account di alto livello OUs e inclusi sotto la 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 una 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 guardare questo video su come [iniziare YouTube a usare AWS Control Tower for AWS Organizations](#).

AWS Control Tower fornisce aggiornamenti in blocco degli account

28 gennaio 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

Con la funzionalità di aggiornamento in blocco, ora puoi aggiornare tutti gli account in un'unità AWS Organizations organizzativa (OU) registrata contenente fino a 300 account, con un solo clic, dalla dashboard di AWS Control Tower. Ciò è particolarmente utile nei casi in cui si aggiorna la landing zone di AWS Control Tower e si devono aggiornare anche gli account registrati per allinearli alla versione corrente della landing zone.

Questa funzionalità ti aiuta anche a mantenere aggiornati i tuoi account quando aggiorni la landing zone 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 dell'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 landing zone, vedere [Aggiorna la tua landing zone](#).

Per informazioni sulla registrazione o la 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 regole AWS Config esterne](#)
- [AWS Control Tower ora disponibile in regioni aggiuntive](#)
- [Aggiornamento Guardrail](#)
- [La console AWS Control Tower mostra maggiori dettagli sugli OUs account](#)
- [Usa AWS Control Tower per configurare nuovi AWS ambienti multi-account in AWS Organizations](#)
- [Personalizzazioni per la soluzione AWS Control Tower](#)
- [Disponibilità generale di AWS Control Tower versione 2.3](#)
- [Provisioning degli account in un'unica fase in AWS Control Tower](#)
- [Strumento di smantellamento di AWS Control Tower](#)
- [Notifiche degli eventi relativi al ciclo di vita di AWS Control Tower](#)

La console AWS Control Tower ora si collega a regole AWS Config esterne

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 Config esterne. AWS Ciò fornisce la visibilità nella console AWS Control Tower per verificare l'esistenza di regole di Config create esternamente oltre a quelle di AWS Config 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 agli 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 sono necessari controlli

aggiuntivi per il tuo account. Per informazioni, consulta [Come AWS Control Tower aggrega AWS Config le regole negli account non gestiti OUs](#).

AWS Control Tower 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 nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti occidentali (Oregon), nella regione Europa (Irlanda) e nella regione Asia Pacifico (Sydney). 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. Per informazioni, consulta [Configura le tue regioni AWS Control Tower](#).

Aggiornamento Guardrail

8 ottobre 2020

(Non è richiesto alcun aggiornamento per la landing zone 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 maggiori dettagli sugli OUs account

22 luglio 2020

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

Puoi visualizzare le organizzazioni e gli account che non sono registrati in AWS Control Tower, oltre alle organizzazioni e agli account registrati.

All'interno della console AWS Control Tower, puoi visualizzare maggiori dettagli sui tuoi AWS account e unità organizzative (OUs). 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.

Usa AWS Control Tower per configurare nuovi AWS ambienti multi-account in AWS Organizations

22 aprile 2020

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Organizations i clienti possono ora utilizzare AWS Control Tower per gestire le unità organizzative (OUs) e gli account appena creati sfruttando queste nuove funzionalità:

- AWS Organizations I clienti esistenti possono ora configurare una nuova landing zone per nuove unità organizzative (OUs) nel loro account di gestione esistente. Puoi crearne di nuovi OUs in AWS Control Tower e creare nuovi account in quelli OUs con governance AWS Control Tower.
- AWS Organizations i clienti possono registrare gli account esistenti utilizzando la procedura di registrazione dell'account o tramite script.

AWS Control Tower fornisce un servizio di orchestrazione che utilizza altri AWS servizi. È progettato per le organizzazioni con più account e team che cercano il modo più semplice per configurare il loro 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 policy stabilite. I costruttori ne traggono vantaggio perché possono fornire nuovi AWS account rapidamente, senza indebite preoccupazioni sulla conformità.

Per informazioni sulla configurazione di una landing zone, vedere [Pianifica la tua landing zone di AWS Control Tower](#). Puoi anche visitare la [pagina web del prodotto](#) AWS Control Tower o guardare questo video su come [iniziare YouTube a usare AWS Control Tower for AWS Organizations](#).

Oltre a questa modifica, la funzionalità di provisioning dell'account Quick 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

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora include una nuova implementazione di riferimento che semplifica l'applicazione di modelli e policy personalizzati alla landing zone di AWS Control Tower.

Con le personalizzazioni per AWS Control Tower, puoi utilizzare CloudFormation modelli per distribuire nuove risorse su account esistenti e nuovi all'interno della tua organizzazione. Puoi anche applicare policy di controllo del servizio personalizzate (SCPs) a tali account in aggiunta a quelle SCPs già fornite 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 landing zone.

La documentazione di distribuzione per questa architettura di soluzione AWS Control Tower è disponibile nella [pagina Web AWS Solutions](#).

Disponibilità generale di AWS Control Tower versione 2.3

5 marzo 2020

(Aggiornamento richiesto per la landing zone 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 usato AWS Control Tower in precedenza, puoi lanciarlo oggi stesso in una qualsiasi delle regioni supportate. Se utilizzi già AWS Control Tower e desideri estenderne le funzionalità di governance alla regione Asia Pacifico (Sydney) nei tuoi account, vai alla pagina Impostazioni nella dashboard di AWS Control Tower. Da lì, aggiorna la tua landing zone all'ultima versione. Quindi, aggiorna i tuoi account singolarmente.

Note

L'aggiornamento della landing zone 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 landing zone 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 [Configure your AWS Control Tower Regions](#).

Provisioning degli account in un'unica fase in AWS Control Tower

2 marzo 2020

(Non è richiesto alcun aggiornamento per la landing zone 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 dall'interno della console AWS Control Tower.

Per utilizzare il modulo semplificato, accedi a Account Factory nella console AWS Control Tower e scegli Quick account provisioning. AWS Control Tower assegna lo stesso indirizzo e-mail all'account fornito e all'utente Single Sign-on (IAM Identity Center) creato per l'account. Se desideri che questi due indirizzi e-mail siano diversi, devi effettuare il provisioning del tuo account tramite Service Catalog.

Aggiorna gli account che crei tramite il provisioning rapido dell'account utilizzando Service Catalog e l'account factory AWS Control Tower, proprio come gli aggiornamenti di qualsiasi altro account.

 Note

Nell'aprile 2020, la funzionalità Quick Account Provisioning 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 gli AWS account. Per ulteriori informazioni, consulta [Registra un account esistente dalla console AWS Control Tower](#).

Strumento di smantellamento di AWS Control Tower

28 febbraio 2020

(Non è richiesto alcun aggiornamento per la landing zone 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 redistribuzione importante delle risorse organizzative, potresti voler ripulire le risorse create durante la configurazione iniziale della landing zone.

Per smantellare la landing zone utilizzando un processo per lo più automatizzato, contattateci Supporto AWS per ricevere assistenza sui passaggi aggiuntivi necessari. Per ulteriori informazioni sulla disattivazione, vedere. [Smantellamento di una landing zone di AWS Control Tower](#)

Notifiche degli eventi relativi al ciclo di vita di AWS Control Tower

22 gennaio 2020

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower annuncia la disponibilità di notifiche sugli eventi del ciclo di vita. Un [evento del ciclo](#) di vita segna il completamento di un'azione AWS Control Tower che può modificare lo stato di risorse come unità organizzative (OUs), account e controlli creati e gestiti da AWS Control Tower. Gli eventi del ciclo di vita vengono registrati come AWS CloudTrail eventi e consegnati ad Amazon EventBridge come eventi.

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 landing zone; creazione o eliminazione di un'unità organizzativa; abilitazione o disabilitazione di un controllo su un'unità organizzativa e utilizzo di account factory per creare un nuovo account o spostare un account in un'altra unità organizzativa.

AWS Control Tower utilizza più AWS servizi per creare e gestire un ambiente multi-account AWS basato sulle best practice. 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 AWS Control Tower di origine è stata completata correttamente. Puoi creare una EventBridge regola per avvisarti quando CloudTrail registra 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 di AWS Control Tower versione 2.2](#)
- [Nuovi controlli opzionali in AWS Control Tower](#)
- [Nuovi controlli investigativi in AWS Control Tower](#)
- [AWS Control Tower accetta indirizzi e-mail per account condivisi con domini diversi dall'account di gestione](#)
- [Disponibilità generale di AWS Control Tower versione 2.1](#)

Disponibilità generale di AWS Control Tower versione 2.2

13 novembre 2019

(Aggiornamento richiesto per la landing zone di AWS Control Tower. Per informazioni, consulta [Aggiorna la tua landing zone.](#))

La versione 2.2 di AWS Control Tower offre tre nuovi controlli preventivi che impediscono la dispersione degli account:

- [Impedisci modifiche ai gruppi di log di Amazon CloudWatch Logs configurati da AWS Control Tower](#)
- [Impedire l'eliminazione delle autorizzazioni di AWS Config aggregazione create da AWS Control Tower](#)
- [Impedisci l'eliminazione dell'archivio di log](#)

Un controllo è una regola di alto livello che fornisce una governance continua per l'intero AWS ambiente. Quando crei la landing zone di AWS Control Tower, la landing zone e tutte le unità

organizzative (OUs), 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 (accidentali o intenzionali) in questo stato di conformità. Il rilevamento delle deviazioni consente di identificare le risorse che necessitano di modifiche o aggiornamenti della configurazione per risolvere la deriva. Per ulteriori informazioni, consulta [Rileva e risolvi la deriva in AWS Control Tower](#).

Nuovi controlli opzionali in AWS Control Tower

05 settembre 2019

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

AWS Control Tower ora include i seguenti quattro nuovi controlli opzionali:

- [Non consentire azioni di eliminazione su bucket Amazon S3 senza MFA](#)
- [Impedisci modifiche alla configurazione di replica per i bucket Amazon S3](#)
- [Impedisci 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

(Non è richiesto alcun aggiornamento per la landing zone 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 abilitata per gli utenti IAM della console AWS](#)
- [Scopri se l'MFA è abilitata 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 a istanze Amazon EC2](#)

- [Rileva se l'accesso pubblico alle istanze di database Amazon RDS è abilitato](#)
- [Rileva se l'accesso pubblico agli snapshot del database Amazon RDS è abilitato](#)
- [Rileva se la crittografia dello storage è abilitata per le istanze di database Amazon RDS](#)

Il 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, ad esempio le violazioni delle politiche, 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 dall'account di gestione

1 agosto 2019

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower)

In AWS Control Tower, ora puoi inviare indirizzi e-mail per account condivisi (archivio log e membro dell'audit) e account secondari (forniti tramite account factory) i cui domini sono diversi dall'indirizzo e-mail dell'account di gestione. Questa funzionalità è disponibile solo quando crei una nuova landing zone e quando esegui il provisioning di nuovi account per bambini.

Disponibilità generale di AWS Control Tower versione 2.1

24 giugno 2019

(Aggiornamento richiesto per la landing zone 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 team che cercano il modo più semplice per configurare il loro nuovo AWS ambiente multi-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 fornire rapidamente nuovi AWS account.

Utilizzando AWS Control Tower, puoi [configurare una landing zone](#) che utilizza le migliori pratiche come la configurazione di una [struttura multi-account](#) utilizzando AWS Organizations, la gestione delle identità degli utenti e dell'accesso federato con AWS IAM Identity Center, 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 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 politiche e monitorano continuamente le risorse distribuite per rilevare eventuali non conformità. La dashboard di AWS Control Tower offre una visibilità centralizzata in un AWS ambiente, tra cui il provisioning degli account, i controlli abilitati e lo stato di conformità degli account.

Puoi configurare un nuovo ambiente multi-account con un solo clic nella console AWS Control Tower. Non sono previsti costi aggiuntivi o impegni iniziali per l'utilizzo di AWS Control Tower. Paghi solo per i AWS servizi che hai abilitato per configurare una landing zone 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
Aggiornamento alla policy 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 di servizi opzionali e un ambiente di controllo dedicato	17 novembre 2025
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 <code>aws-controltower/CloudTrailLogs:*</code> a <code>aws-controltower/CloudTrailLogs*:*</code> a per consentire la gestione	5 novembre 2025

di gruppi di log con suffissi univoci. Questo aggiornamento compatibile con le versioni precedenti 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.

[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 dell'account e trasferimento da un account all'altro. OUs

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 IPv6 endpoint.	18 agosto 2025
Account Factory per Terraform versione 1.15.0	È disponibile la versione 1.15.0 di AFT.	28 luglio 2025
Controlli aggiornati con i tipi di istanze Nitro	Sono stati aggiornati otto controlli proattivi per aggiungere e nuovi tipi di istanze.	24 luglio 2025
AWS Control Tower disponibile in Asia Pacifico (Taipei)	AWS Control Tower aggiunge il supporto per l'Asia Pacifico (Taipei).	23 luglio 2025
AWS Control Tower supporta AWS PrivateLink	AWS Control Tower aggiunge il supporto per AWS PrivateLink.	30 giugno 2025
Controlli collegati ai servizi AWS Config	AWS Control Tower distribuisce controlli collegati ai servizi AWS Config .	12 giugno 2025
Metadati migliorati. Controlli aggiuntivi, nuovi framework	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
Visualizzazione dei controlli abilitati	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
<u>AWS Control Tower disponibili nelle regioni di AWS Asia Pacifico (Tailandia) e Messico (Centrale)</u>	Sono disponibili le seguenti regioni: Asia Pacifico (Tailandia) e Messico (Centrale).	9 maggio 2025
<u>AWS Control Tower aggiunge 233 AWS Config controlli</u>	Aggiunti nuovi controlli Config, tabelle di metadati rinnovate, tabelle Region, pagina identificatore globale.	11 aprile 2025
<u>AWS Control Tower aggiorna un ruolo collegato al servizio</u>	Aggiornamenti a. AWSControlTowerAccountServiceRolePolicy	10 dicembre 2024
<u>AWS Control Tower cFCT supporta GitHub</u>	Una nuova opzione per una fonte di configurazione di terze parti.	9 dicembre 2024
<u>Controlli preventivi di AWS Control Tower con policy dichiarative</u>	Un nuovo tipo di policy implementa un nuovo tipo di controllo preventivo.	1 dicembre 2024
<u>AWS Control Tower si integra con Backup AWS</u>	Puoi configurare piani per il backup delle risorse AWS Control Tower.	25 novembre 2024
<u>AWS Control Tower integra i AWS Config controlli</u>	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 RCPs.	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
AWS Control Tower supporta fino a 100 operazioni di controllo simultanee	Un aumento della quota delle operazioni di controllo simultanee a 100.	20 maggio 2024
AWS Control Tower disponibile nella AWS regione di Calgary West (Canada)	AWS Control Tower è disponibile nella regione Canada occidentale (Calgary).	3 maggio 2024
AWS Control Tower supporta l'aggiustamento delle quote in modalità self-service	AWS Control Tower è integrato con AWS Service Quotas nella console.	25 aprile 2024
La documentazione relativa ai controlli è stata spostata in una nuova guida	AWS Control Tower ha pubblicato la Controls Reference Guide.	21 aprile 2024
Etichettare EnabledControl le risorse in CloudFormation	AWS Control Tower supporta l'aggiunta di tag alle EnabledControl risorse tramite CloudFormation modelli.	22 febbraio 2024
Linea di base disponibile APIs	AWS Control Tower ha rilasciato una nuova versione APIs per la registrazione OUs programmatica.	14 febbraio 2024
Landing zone di AWS Control Tower versione 3.3	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 la landing zone APIs</u>	AWS Control Tower supporta la configurazione e il lancio di zone di atterraggio utilizzando nuove APIs	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 APIs funzionalità.	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 il Security Hub CSPM Service-Managed Standard: 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>	Supporto per una singola regione 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
<u>Nuovo ruolo aggiunto</u>	AWS Control Tower ha aggiunto un nuovo ruolo collegato al servizio, AWSServiceRoleForAWSControlTower e policy associata, . AWSControlTowerAccountServiceRolePolicy	1 giugno 2023
<u>Aggiornamento misto sulla governance</u>	Aggiornamento per consigliare i clienti in merito alla governance mista.	1 giugno 2023
<u>Sono disponibili controlli proattivi aggiuntivi</u>	I nuovi controlli proattivi ti aiutano a gestire l'ambiente multi-account e a raggiungere obiettivi di controllo specifici.	19 maggio 2023
<u>Sono disponibili sette regioni aggiuntive</u>	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 le impostazioni AWSControlTowerServiceRolePolicy in modo che AWS Control Tower possa chiamare le EnableRegionListRegions e GetRegionOptStatus APIs 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

<u>Operazioni simultanee sull'account</u>	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
<u>I controlli proattivi aiutano nell'approvvigionamento delle risorse</u>	AWS Control Tower ora supporta controlli proattivi , implementati tramite CloudFormation hook.	28 novembre 2022
<u>È disponibile la personalizzazione dell'account di fabbrica</u>	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
<u>Lo stato di conformità è visualizzabile per tutte le regole AWS Config</u>	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
<u>Passa a una policy gestita</u>	Abbiamo modificato il codice <code>AWSControlTowerServiceRolePolicy</code> in modo che AWS Control Tower possa assumere il <code>AWSControlTowerBlueprintAccess</code> ruolo necessario per le personalizzazioni di Account Factory.	28 ottobre 2022

[APIs per controlli, 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 aggregare informazioni AWS Config 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 visualizzazioni OUs e account](#)

La nuova pagina Organization in AWS Control Tower mostra una visualizzazione gerarchica di tutte le unità organizzative (OUs) e gli account.

18 luglio 2022

[Passa a una policy gestita](#)

Abbiamo modificato l'impostazione AWSControlTowerServiceRolePolicy in modo che i clienti possano disporre di AWS CloudTrail percorsi a livello di organizzazione per aggregare i log. AWS CloudTrail

20 giugno 2022

[Registrazione e aggiornamento più semplici per gli account dei membri](#)

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

[AFT supporta la personalizzazione per gli account condivisi](#)

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

[Operazioni simultanee per tutti i controlli opzionali](#)

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
Nuovo evento del ciclo di vita disponibile	L'PrecheckOrganizationalUnit evento registra se alcune risorse impediscono l'esito positivo dell'attività Extend governance, incluse le risorse in nidificato. OUs	18 novembre 2021

Annidato (disponibile) OUs	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 <code>AWSControlTowerServiceRolePolicy</code> in 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 dei dati gestiti SCPs](#)

AWS Control Tower esegue scansioni automatiche giornaliere di Managed SCPs to Check for Drift.

11 maggio 2021

[Nomi e account personalizzati OUs](#)

AWS Control Tower ti consente di fornire nomi personalizzati durante il processo di configurazione delle landing zone, per account essenziali OUs e senza creare disagi.

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

[Gli aggiornamenti multipli degli account sono registrati OUs](#)

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 degli account non gestiti e degli account OUs](#)

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 obbligatorio AWS-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 sugli OUs account.](#)

All'interno della console AWS Control Tower, puoi visualizzare maggiori dettagli sui tuoi AWS account e unità organizzative (OUs). 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 delle impostazioni e delle 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.