Guida per l'utente

AWS Control Tower

AWS Control Tower: Guida per l'utente

Table of Contents

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 (OU), gli account, gli utenti e le altre risorse che desideri siano soggette alle

normative di conformità. Una landing zone può essere ridimensionata per soddisfare le esigenze di un'azienda di qualsiasi dimensione.

- Controlli: un controllo (a volte chiamato guardrail) è una regola di alto livello che fornisce una governance continua per l'intero ambiente. AWS È espresso in linguaggio normale. Esistono tre tipi di controlli: preventivo, investigativo e proattivo. Ai controlli si applicano tre categorie di linee guida: obbligatorie, fortemente raccomandate o facoltative. Per ulteriori informazioni sui controlli, vedereCome 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 unità organizzate per account e unità organizzate.

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.
- 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 offre funzionalità essenziali per la gestione di un ambiente multi-account, tra cui governance e gestione centralizzate degli account, creazione di account tramite AWS Organizations API e policy di controllo dei servizi (SCP).

- 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 apportate. 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 della AWS Control Tower eAWS strategia multi-account per la tua landing zone AWS della 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, consultaGestione degli aggiornamenti della 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: l'elemento principale che contiene tutte le altre unità organizzative presenti nella 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. Questa e altre unità organizzative registrate contengono gli account registrati con cui i tuoi utenti lavorano per eseguire i loro carichi di lavoro AWS.
- Directory IAM Identity Center: questa directory ospita gli utenti di IAM Identity Center. Definisce l'ambito delle autorizzazioni per ogni utente IAM Identity Center.
- 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 (OU): 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, consulta Linee guida per la creazione e la modifica delle risorse AWS Control Tower.
- Quando abiliti i controlli opzionali (quelli con linee guida fortemente consigliate o facoltative), AWS Control Tower crea AWS risorse che gestisce nei tuoi account. Non modificare o eliminare risorse create da AWS Control Tower. Ciò può far sì che i controlli entrino in uno stato sconosciuto.

Cosa sono gli account condivisi?

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

Cos'è l'account di gestione?

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

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

Per ulteriori informazioni, consulta Gestione dell'account.

Cos'è l'account di archiviazione dei log?

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

Per ulteriori informazioni, consulta Account di archivio 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 dalle API AWS Control Tower. I controlli obbligatori vengono sempre applicati e non possono essere modificati.

I controlli preventivi impediscono il verificarsi di azioni. Ad esempio, il controllo elettivo denominato Disallow Changes to Bucket Policy per Amazon S3 Buckets (precedentemente chiamato Disallow Policy Changes to Log Archive) impedisce qualsiasi modifica alla policy IAM all'interno dell'account condiviso dell'archivio di log. Qualsiasi tentativo di eseguire un'azione impedita viene negato e registrato. CloudTrail Anche la risorsa è connessa. AWS Config

I controlli Detective rilevano eventi specifici quando si verificano e registrano l'azioneCloudTrail. 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. AWS CloudFormation

Per chi conosce AWS: In AWS Control Tower i controlli preventivi sono implementati con Service Control Policies (SCP). I controlli investigativi sono implementati con AWS Config regole. I controlli proattivi sono implementati con AWS CloudFormation ganci.

Argomenti correlati

- Rileva e risolvi la deriva in AWS Control Tower

Come funziona AWS Control Tower con StackSets

AWS Control Tower utilizza AWS CloudFormation StackSets per configurare le risorse nei tuoi account. Ogni set di stack StackInstances corrisponde a un account e uno Regioni AWS per 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 AWS 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 AWS 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, AWS 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, AWS 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. AWS 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 eOUs, consulta la AWS Organizations terminologia e i concetti. Se non conosci AWS Control Tower, questa terminologia è un buon punto di partenza.
- AWS Organizationsè un AWS servizio che ti aiuta a gestire centralmente il tuo ambiente man mano che cresci e a scalare i carichi di lavoro. AWS AWSControl Tower si affida AWS Organizations alla creazione di account, all'applicazione di controlli preventivi a livello di unità organizzativa 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 regione di origine della AWS Control Tower è la AWS regione in cui è stata dispiegata la landing zone della AWS Control Tower. Puoi visualizzare la tua regione d'origine nelle impostazioni della landing zone.
- AWS Service Catalogconsente 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 account provenienti da progetti personalizzati.
- AWS CloudFormation StackSetssono 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 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 OrganizationsÈ possibile utilizzare un pacchetto di conformità per personalizzare l'ambiente AWS Control Tower. Per i blog tecnici che forniscono maggiori dettagli, consulta Informazioni correlate.

- Una baseline in AWS Control Tower è un gruppo di risorse e configurazioni specifiche che è possibile applicare a un obiettivo. L'obiettivo di base più comune può essere un'unità organizzativa (OU). Ad esempio, la linea di base 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 AWS 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 al AWS Control Tower di funzionare correttamente.
- Risorsa non conforme: 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. È possibile scegliere nomi personalizzati per l'account di archiviazione dei log e l'account di controllo durante la configurazione.
- Account membro: un account membro appartiene all'organizzazione AWS Control Tower. L'account membro può essere registrato o annullato in Control TowerAWS. Quando un'unità organizzativa registrata contiene una combinazione di account registrati e non registrati:
  - I controlli preventivi abilitati sull'unità organizzativa si applicano a tutti gli account al suo interno, compresi quelli non registrati. Questo è vero perché i controlli preventivi vengono applicati SCPs a livello di unità organizzativa, non a livello di account. Per ulteriori informazioni, consulta Inheritance for Service Control Policy nella documentazione. AWS Organizations
  - I controlli Detective abilitati sull'unità organizzativa non si applicano agli account non registrati.

  Un account può essere membro di una sola organizzazione alla volta e i relativi addebiti vengono fatturati sull'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 IAM utente) 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 a AWS Control Tower tramite la registrazione dell'account o il processo di registrazione 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 conSCPs. I controlli investigativi sono implementati con AWS Config regole. I controlli proattivi sono implementati con AWS CloudFormation ganci. Per ulteriori informazioni, consulta Come funzionano i controlli.
- 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.
- OU annidata: un'unità organizzativa nidificata in AWS Control Tower è un'unità organizzativa contenuta in un'altra unità organizzativa. Un'unità organizzativa nidificata può avere esattamente un'unità organizzativa principale e ogni account può essere membro di una sola 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 figliOUs.
- 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 viene gestita e controllata nell'ambiente dell'utente da AWS Control Tower, in base alle politiche di governance stabilite dall'organizzazione. Questi Regioni AWS vengono monitorati 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 governato: le regioni che mostrano lo stato Non governato non sono controllate o monitorate da AWS Control Tower. Questi Regioni AWS di solito non aderiscono alle stesse politiche di

governance applicate da AWS Control Tower. È possibile creare risorse in queste aree, ma tali risorse non sono protette dai controlli AWS Control Tower.

- Negata: una regione negata viene bloccata specificamente da AWS Control Tower. Nell'ambiente AWS Control Tower in uso, non è possibile effettuare il provisioning di risorse in questi ambienti Regioni AWS.

Prezzi

Non sono previsti costi aggiuntivi per l'utilizzo di AWS Control Tower. Paghi solo 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 ConfigPer informazioni dettagliate, consulta Prezzi diAWS 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, consultaMonitora 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 dell'uso AWS Control Tower per la prima volta, segui i passaggi descritti in questa sezione per creare un AWS account e proteggi il tuo AWS Control Tower account di gestione. Per informazioni sulle attività di configurazione aggiuntive, specifiche per AWS Control Tower, consulta Guida introduttiva a AWS Control Tower.

Iscriviti per AWS

Quando ti iscrivi ad Amazon Web Services (AWS), il tuo AWS l'account viene registrato automaticamente per tutti i servizi in AWS, incluso AWS Control Tower. Se hai un AWS hai già un account, passa all'attività successiva. Se non ne hai uno AWS account, usa la seguente procedura per crearne uno.

Nota il tuo AWS numero di conto, perché ne hai bisogno per altre attività.

Registrati per un Account AWS

Se non disponi di un 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, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, un Utente root dell'account AWSviene creato. L'utente root ha accesso a tutti Servizi AWS e le risorse presenti 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 per un Account AWS, proteggi il tuo Utente root dell'account AWS, abilita AWS IAM Identity Center 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 a AWS Management Consolecome proprietario dell'account selezionando Utente root e inserendo il Account AWS indirizzo email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso tramite utente root, consulta Accesso come utente root in Accedi ad AWS Guida per l'utente.
2. Attiva l'autenticazione a più fattori (MFA) per il tuo utente root.

   Per istruzioni, consulta Abilitare un MFA dispositivo virtuale per il Account AWS utente root (console) nella Guida per l'IAMutente.

Crea un utente con accesso amministrativo

1. Abilita IAM Identity Center.

   Per istruzioni, vedi Abilitazione AWS IAM Identity Center nella AWS IAM Identity Center Guida per l'utente.
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, vedi Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella AWS IAM Identity Center Guida per l'utente.

Accesso come utente amministratore

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

  Per informazioni sull'accesso tramite un utente di IAM Identity Center, vedi Accesso a AWS accedere al portale in Accedi ad AWS Guida per l'utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, vedere Creare un set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella AWS IAM Identity Center Guida per l'utente.

> **Sicurezza per i tuoi account**
>
> Puoi trovare ulteriori indicazioni su come impostare le migliori pratiche per proteggere la sicurezza dei tuoi AWS Control Tower conti, in 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 landing zone utilizzando la console o le API AWS Control Tower.

Se AWS al momento sei un cliente, ma non conosci AWS Control Tower, prima di procederePianifica la tua landing zone della AWS Control Tower, potresti voler esaminare la sezione chiamata.

Argomenti

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 Fase 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 utilizzati, questi servizi possono comportare dei costi, come indicato nella pagina dei prezzi. La console AWS di gestione mostra l'utilizzo di tutti i servizi a pagamento e i costi sostenuti. AWS Control Tower non crea costi aggiuntivi.

Prima di iniziare

La decisione più importante da prendere prima di iniziare il processo di configurazione è scegliere la regione di residenza. La tua regione di origine è la AWS regione in cui eseguirai la maggior parte dei

tuoi carichi di lavoro o archivierai la maggior parte dei tuoi dati. Non può essere modificato dopo aver configurato la landing zone di AWS Control Tower. Per ulteriori informazioni su come scegliere una regione d'origine, consulta Suggerimenti amministrativi per la configurazione delle landing zone .

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

La procedura di avvio rapido presuppone che accetterai i valori predefiniti per le risorse nel tuo ambiente AWS Control Tower. Molte di queste scelte possono essere modificate in seguito. Alcune scelte da effettuare una sola volta sono elencate nella sezione Aspettative per la configurazione delle landing zone denominata.

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

Passaggi di avvio rapido

1. Accedi alla console di AWS gestione con le tue credenziali utente di amministratore.
2. Accedi alla console AWS Control Tower all'indirizzo https://console.aws.amazon.com/controltower.
3. Verifica di lavorare nella regione di residenza desiderata.
4. Scegli 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 per 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 o CloudTrail. 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 Registrare 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.

Inizia a usare AWS Control Tower dalla console

Questa procedura introduttiva è destinata agli amministratori AWS di Control Tower. Segui questa procedura quando sei pronto per configurare la 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, potresti voler rivedere la sezione chiamataPianifica la tua landing zone della AWS Control Tower, prima di procedere.

Argomenti

- Aspettative per la configurazione delle landing zone
- Passaggio 1: crea gli indirizzi email del tuo account condiviso
- Fase 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 AWS del Control Tower prevede diversi passaggi. Alcuni aspetti della landing zone della 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, è possibile selezionare nomi personalizzati per gli account condivisi creati da AWS Control Tower, denominati archivio log e audit per impostazione predefinita, ma non è possibile 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 si prevede di specificare AWS account esistenti e se tali account dispongono di AWS Config risorse esistenti, è necessario eliminare le AWS Config risorse esistenti prima di poter registrare gli account in AWS Control Tower. (Questa è una selezione una tantum).
- Se ti stai configurando per la prima volta o se stai effettuando l'aggiornamento alla versione 3.0 della landing zone, puoi scegliere se consentire a AWS Control Tower di impostare un percorso a livello di organizzazione per la tua organizzazione, oppure puoi disattivare i AWS CloudTrail trail gestiti da Control Tower AWS 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 Control Tower. AWS È possibile personalizzare gli account in un secondo momento se non si dispone 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 stai fornendo account Account Factory conVPCs, non VPC CIDRs possono essere modificati 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, vediConfigurazione.

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

Gli indirizzi e-mail sono necessari per:

- Account di controllo: 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 procedura consigliata, quando si eseguono azioni in questi account, si consiglia di utilizzare un utente dell'IAMIdentity Center con le autorizzazioni appropriate.

> **Note**
>
> Se si specificano AWS account esistenti come account di controllo 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 AWS Control Tower (OUs) per allinearla alla strategia AWS multi-account. Potresti notare alcune incongruenze mentre stiamo effettuando una transizione per migliorare la chiarezza di questi nomi. L'unità organizzativa di sicurezza era precedentemente denominata Core OU. L'unità organizzativa Sandbox era precedentemente denominata Custom OU.

Fase 2: Configura e avvia la tua landing zone

Prima di lanciare la landing zone AWS della Control Tower, stabilite la regione d'origine più appropriata. Per ulteriori informazioni, consulta Suggerimenti amministrativi per la configurazione delle landing zone .

Important

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

Scopri come configurare e avviare la tua landing zone utilizzando AWS CLI inInizia 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 in 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 installato AWS Control Tower, non puoi cambiare la regione d'origine.

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

Per selezionare 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 predefinitiOUs, non devi intraprendere alcuna azione per continuare la configurazione. Per modificare i nomi diOUs, inserisci i nuovi nomi direttamente nel campo del modulo.

- Foundational OU — 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 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 nellaLinee guida per configurare un ambiente ben progettato. Se hai già 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, agli indirizzi e-mail non devono già essere associati AWS account.

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 Control TowerAWS, 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 configuri 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 tra più account tramite Identity Center. IAM È possibile modificare questa selezione in un secondo momento.

Per impostazione predefinita, AWS Control Tower configura AWS IAM l'Identity Center per la landing zone, in linea con le linee guida sulle migliori pratiche definite in Organizzazione AWS dell'ambiente utilizzando più account. La maggior parte dei clienti sceglie l'impostazione predefinita. 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 IAMGuida all'Identity Center.

Configura facoltativamente i percorsi AWS CloudTrail

Come procedura consigliata, si consiglia di configurare la registrazione. Se desideri consentire a AWS Control Tower di creare 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 KMS chiave ogni volta che aggiorni la landing zone.

Quando selezioni Configura landing zone, AWS Control Tower esegue un controllo preliminare per convalidare la tua KMS chiave. 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 KMS chiave

Prima di poter aggiornare una politica KMS chiave, è necessario creare una KMS chiave. Per ulteriori informazioni, consulta Creazione di una policy delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Per utilizzare una KMS chiave con AWS Control Tower, è necessario aggiornare la politica delle KMS chiavi predefinita aggiungendo le autorizzazioni minime richieste per AWS Config e AWS CloudTrail. Come procedura consigliata, si consiglia di includere le autorizzazioni minime richieste in qualsiasi politica. Quando aggiorni una politica KMS chiave, puoi aggiungere le autorizzazioni come gruppo in un'unica JSON istruzione o riga per riga.

La procedura descrive come aggiornare la politica delle KMS chiavi predefinita nella AWS KMS console aggiungendo istruzioni di policy che consentono AWS Config e possono CloudTrail essere utilizzate AWS KMS per la crittografia. Le dichiarazioni politiche richiedono l'inclusione delle seguenti informazioni:

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— l'ID dell'account di gestione in cui verrà configurata AWS Control Tower.
- **`YOUR-HOME-REGION`**— la regione d'origine che selezionerai durante la configurazione del AWS Control Tower.
- **`YOUR-KMS-KEY-ID`**— l'ID della KMS chiave che verrà utilizzato con la politica.

Per aggiornare la politica KMS chiave

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 KMS chiave 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 KMS politica chiave

La seguente politica di esempio mostra come potrebbe apparire la politica KMS chiave dopo aver aggiunto le dichiarazioni di policy che concedono AWS Config e CloudTrail le autorizzazioni minime richieste. La politica di esempio non include la politica KMS chiave 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:aws: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: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/*"
                }
            }
        }
    ]
}
```

Per visualizzare altre politiche di esempio, consulta le pagine seguenti:

- Concessione delle autorizzazioni di crittografia nella Guida per l'AWS CloudTrail utente.
- Autorizzazioni richieste per la KMS chiave (quando si utilizza il servizio Roless3 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

Il AWS Key Management Service (AWS KMS) consente di creare chiavi multiregionali e KMS chiavi asimmetriche; tuttavia, Control Tower AWS non supporta chiavi multiregione o chiavi asimmetriche. AWSControl Tower esegue un controllo preliminare delle chiavi esistenti. È possibile che venga visualizzato un messaggio di errore se si seleziona 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 Guida per AWS KMS gli sviluppatori.

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

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 Control Tower. AWS È possibile personalizzare gli account in un secondo momento se non si dispone 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, rivedi le autorizzazioni del servizio e, quando sei pronto, scegli Comprendo le autorizzazioni che AWS Control Tower utilizzerà per amministrare AWS le risorse e far rispettare le regole per mio conto.
2. Per finalizzare le selezioni e inizializzare il lancio, scegli Configura 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 Root, l'unità organizzativa di sicurezza e gli account condivisi. Altre AWS risorse vengono create, modificate o eliminate.

> ⚠ Conferma le SNS sottoscrizioni
>
> L'indirizzo e-mail che hai fornito per l'account di controllo riceverà le e-mail di AWS notifica — conferma dell'abbonamento da tutte le AWS regioni supportate da AWS Control Tower. Per ricevere e-mail di conformità nel tuo account di controllo, 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 AWS di 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 AWS CloudFormation console o tramite. AWS CLI

Prima di lanciare la landing zone AWS del Control Tower, esegui queste operazioni 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

Il processo di configurazione della landing zone AWS del Control Tower prevede diversi passaggi. Alcuni aspetti della landing zone della 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, è possibile selezionare nomi personalizzati per gli account condivisi creati da AWS Control Tower, denominati archivio log e audit per impostazione predefinita, ma non è possibile modificare questi nomi dopo la configurazione. (Questa è una selezione una tantum).
- Durante la configurazione conAPIs, 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 ti stai configurando per la prima volta o se stai effettuando l'aggiornamento alla versione 3.0 della landing zone, puoi scegliere se consentire a AWS Control Tower di impostare un percorso a livello di organizzazione per la tua organizzazione, oppure puoi disattivare i AWS CloudTrail trail gestiti da Control Tower AWS 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 stai fornendo account conVPCs, non VPC CIDRs possono essere modificati dopo la loro creazione.

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

Fase 1: Configura la tua landing zone

Il processo di configurazione della landing zone AWS del Control Tower prevede diversi passaggi. Alcuni aspetti della landing zone del AWS Control Tower sono configurabili, ma altre scelte non possono essere modificate dopo la configurazione. Per saperne di più su queste importanti considerazioni prima di lanciare la landing zone, consulta. Aspettative per la configurazione delle landing zone

Prima di utilizzare la landing zone AWS Control TowerAPIs, devi prima chiamare APIs altri AWS servizi per configurare la tua landing zone prima del lancio. Il processo prevede tre fasi principali:

- creazione di una nuova AWS Organizations organizzazione,
- configurazione degli indirizzi e-mail degli account condivisi,
- e creando un IAM ruolo o un utente dell'IAMIdentity Center con le autorizzazioni necessarie per chiamare la landing zoneAPIs.

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

1. Chiama AWS Organizations `CreateOrganization` API e abilita tutte le funzionalità per creare l'unità organizzativa Foundational. AWSControl Tower inizialmente la chiama Security OU. Questa unità organizzativa di sicurezza contiene i due account condivisi, che per impostazione predefinita sono denominati account di archiviazione dei registri e account di controllo.

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

   AWSControl 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, si consiglia di denominarla Sandbox OU, come indicato nellaAWS strategia multi-account per la tua landing zone AWS della Control Tower.

Fase 2. Fornisci account condivisi, se necessario:

Per configurare la landing zone, AWS Control Tower richiede due indirizzi e-mail. Se si utilizza la landing zone APIs per configurare AWS Control Tower per la prima volta, è necessario utilizzare AWS gli account di sicurezza e di archiviazione dei log esistenti. È possibile utilizzare gli indirizzi e-mail correnti di quelli esistenti 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 a AWS Control Tower.

Per iniziare a configurare una nuova landing zone, se non disponi di AWS account esistenti, puoi fornire gli account di sicurezza e di archiviazione AWS dei log utilizzando AWS Organizations APIs.

1. Chiamali AWS Organizations `CreateAccount` API per creare l'account di archiviazione dei log e l'account di controllo 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"
   ```

2. (Facoltativo) Verificare lo stato dell'`CreateAccount`operazione utilizzando il AWS Organizations `DescribeAccount`API.

Fase 3. Creare i ruoli di servizio richiesti

Crea i seguenti ruoli IAM di servizio che consentono a AWS Control Tower di eseguire le API chiamate necessarie per configurare la tua landing zone:

- AWSControlTowerAdmin
- AWSControlTowerCloudTrailRole
- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

Per ulteriori informazioni su questi ruoli e le relative politiche, vedereUtilizzo di policy basate sull'identità (policy IAM) per AWS Control Tower.

Per creare un IAM ruolo:

1. Crea un IAM ruolo con le autorizzazioni necessarie per chiamare tutte le landing zoneAPIs. In alternativa, puoi creare un utente dell'IAMIdentity Center e assegnare le autorizzazioni necessarie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "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": "*"
        }
    ]
}
```

Fase 2: Avvia la landing zone

La AWS Control Tower `CreateLandingZone` API richiede una versione di landing zone e un file manifest come parametri di input. È possibile utilizzare il file manifest per configurare le seguenti funzionalità:

- Configura facoltativamente la conservazione dei registri
- Facoltativamente, gestisci automaticamente l'accesso Account AWS
- Configura facoltativamente i percorsi AWS CloudTrail
- Configurare facoltativamente AWS KMS keys

Dopo aver compilato il file manifest, sei pronto per creare una nuova landing zone.

> **Note**
>
> AWSControl Tower non supporta il Region deny control quando si utilizza APIs per configurare e lanciare una landing zone. Dopo aver avviato con successo la tua landing zone utilizzandoAPIs, puoi utilizzare la console AWS Control Tower per configurare la regione deny control.

1. Chiama la AWS Control Tower `CreateLandingZone`API. Ciò API richiede una versione della landing zone e un file manifest come input.

```
aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
LandingZoneManifest.json"
```

Esempio di manifesto in LandingZoneManifestformato.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> Come mostrato nell'esempio, gli SecurityRoles account AccountIdfor the CentralizedLogging and devono essere diversi.

Output:

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

2. Chiama il `GetLandingZoneOperation` API per verificare lo stato dell'`CreateLandingZone`operazione. `GetLandingZoneOperation`APIRestituisce lo stato di `SUCCEEDEDFAILED`, o`IN_PROGRESS`.

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

Output:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Quando lo stato ritorna come`SUCCEEDED`, puoi chiamare il `GetLandingZone` API per rivedere la configurazione della landing zone.

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

Output:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
```

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

Identifica la tua landing zone

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

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

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

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 richiamarlo `UpdateLandingZone` API e fare riferimento a un file manifest aggiornato. Questo API restituisce un `OperationIdentifier` file, che puoi quindi utilizzare quando chiami il `GetLandingZoneOperation` API per verificare lo stato dell'operazione di aggiornamento.

Per aggiornare la landing zone

1. Chiama la AWS Control Tower `UpdateLandingZone` API e fai riferimento alla versione aggiornata della landing zone o al tuo manifest aggiornato.

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

LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

Output:

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

Facoltativamente, registrare nuovamente l'unità organizzativa per aggiornare gli account

Per le AWS Control Tower registrate OUs con meno di 300 account, è possibile utilizzare la console AWS Control Tower, accedere alla pagina OU nella dashboard e selezionare Registra nuovamente l'unità organizzativa 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 identificare se la tua landing zone è alla deriva, puoi chiamare il `GetLandingZone`API. Ciò API restituisce lo stato di deriva della zona di atterraggio pari a o. `DRIFTED` `IN_SYNC`

Per risolvere il problema della deriva all'interno della tua landing zone, puoi `ResetLandingZone` API utilizzare il comando per ripristinare la configurazione originale della landing zone. Ad esempio, AWS Control Tower abilita di default IAM Identity Center per aiutarti a gestire la tua Account AWS... ma se configuri i parametri originali della landing zone con IAM Identity Center disabilitato, la chiamata `ResetLandingZone` mantiene la configurazione disabilitata IAM dell'Identity Center.

Puoi utilizzarlo solo `ResetLandingZone` API se utilizzi l'ultima versione di landing zone disponibile. Puoi chiamare `GetLandingZone` API 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. Chiama il `GetLandingZone`API. Se API restituisce uno stato di deriva di`DRIFTED`, la tua landing zone è in deriva.
2. Chiamalo `ResetLandingZone` API 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-446XXXXXXXXX"
}
```

> **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.

Disattiva la tua landing zone

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 lalanding 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. Procedura dettagliata: smantellamento di una AWS Control Tower Landing Zone

Per disattivare una landing zone, chiama `DeleteLandingZone`API. Ciò API restituisce un`OperationIdentifier`, che è quindi possibile utilizzare quando si chiama il `GetLandingZoneOperation` API 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-446XXXXXXXXX"
}
```

Visualizza lo stato delle operazioni nelle tue landing zone

L'`ListLandingZoneOperations`API 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-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

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

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
 AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
```

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

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

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

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

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

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 richiesti.

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

Fase 2. Crea i ruoli IAM richiesti.

`AWSControlTowerAdmin`

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

AWSControlTowerCloudTrailRole

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

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
```

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

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Fase 3. Ottieni gli ID degli account e genera il file manifest delle landing zone.

I primi due comandi dell'esempio seguente memorizzano gli ID degli account 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/4B3H0ULNUOL2AXXX",
    "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 dell'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/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

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'ListLandingZoneOperationsAPI.

Avvia una landing zone usando AWS CloudFormation

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

Argomenti

- Prerequisiti per il lancio di una landing zone utilizzando AWS CloudFormation
- Crea una nuova landing zone usando AWS CloudFormation
- Gestisci una landing zone esistente usando AWS CloudFormation

Prerequisiti per il lancio di una landing zone utilizzando AWS CloudFormation

1. Da AWS CLI, utilizzare il AWS Organizations `CreateOrganization` API per creare un'organizzazione e abilitare tutte le funzionalità.

   Per istruzioni più dettagliate, consulta Fase 1: Configura la tua landing zone .
2. Dalla AWS CloudFormation console o utilizzando il AWS CLI, distribuisci un AWS 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 AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, e AWSControlTowerStackSetRoledi servizio.

     Per informazioni su come AWS Control Tower utilizza questi ruoli per eseguire API chiamate di landing zone, vedi 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 AWS CloudFormation

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

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    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 AWS CloudFormation

Puoi utilizzarla AWS CloudFormation per gestire una landing zone che hai già lanciato importando la landing zone in uno AWS 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, il AWS CLI, o il `ResetLandingZone`API.

Passaggi successivi

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 sicurezzaConvalida 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.
- Prova a visitare un elenco selezionato di YouTube video che spiegano di più su come utilizzare la funzionalità di AWS Control Tower.
- 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 della configurazione in AWS Control Tower.
- Se riscontri problemi durante l'utilizzo di AWS Control Tower, consultaRisoluzione 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 si utilizza AWS Control Tower. Se non riesci a configurare la landing zone a causa di un problema relativo alla quota di servizio, contatta AWS Support.

Per ulteriori informazioni sulle limitazioni specifiche dei controlli, consultaLimitazioni di controllo.

> La guida di riferimento ai controlli
>
> Le informazioni dettagliate sui controlli AWS Control Tower sono state spostate nella AWS Control Tower Controls 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.

- AWSControl 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. È possibile eseguire fino a cento (100) operazioni relative al controllo alla volta, in totale, indipendentemente dal fatto che vengano richiamate dalla console o da un. API Di queste 100 operazioni, fino a 20 alla volta possono essere operazioni di controllo proattive.
  - 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.
- Gli indirizzi e-mail degli account condivisi nella Security OU possono essere modificati, ma è necessario aggiornare la landing zone per visualizzare queste modifiche nella console AWS Control Tower.
- OUsNella landing zone della AWS Control Tower si applica un limite di cinque (5) SCPs per unità organizzativa.
- AWSControl Tower supporta fino a 10.000 account nell'organizzazione della tua zona di atterraggio, suddivisi tra tutti i tuoiOUs.

- 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 registrazioneOUs, consulta. Limitazioni basate sui servizi sottostanti AWS
- Le personalizzazioni per AWS Control Tower (cFCT) non sono disponibili in questi casi Regioni AWS, poiché alcune dipendenze non sono disponibili:
  - Regione Europa (Zurigo), eu-central-2
  - Regione Europa (Spagna), eu-south-2
  - Canada occidentale (Calgary)

  È possibile distribuire e gestire risorse in queste regioni con cFCT, se si distribuisce cFCT nella regione di origine del Control TowerAWS, ma non è possibile creare cFCT in queste regioni.
- AWSControl Tower Account Factory for Terraform (AFT) non è disponibile nelle versioni seguenti Regioni AWS, poiché alcune dipendenze non sono disponibili:
  - Regione Europa (Zurigo), eu-central-2
  - Regione Europa (Spagna), eu-south-2
  - Canada occidentale (Calgary)
- AWSControl Tower Account Factory for Terraform (AFT) non può essere distribuito da nuovi AFT clienti nelle seguenti regioni, poiché AWS CodeStar Connections non è disponibile per la connessione a un sistema di controllo della versione di terze parti ()VCS:
  - 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) e Medio Oriente (UAE)
- Le seguenti regioni non supportano Identity Center. IAM
  - Medio Oriente (UAE) Regione, me-central-1
  - Regione Asia Pacifico (Hyderabad), ap-south-2
  - Canada occidentale (Calgary), ca-west-1

  Per ulteriori informazioni Regioni AWS e supporto per IAM Identity Center, vedere Regioni ed endpoint nella AWS Identity and Access Management User Guide.
- Le seguenti regioni non sono AWS Service Catalogsupportate.
  - Canada occidentale (Calgary), ca-west-1

  Per ulteriori informazioni sulla funzionalità AWS Control Tower nelle regioni non supportate AWS Service Catalog, vedereAWSControl Tower disponibile in AWS Canada occidentale (Calgary).

- Quando si chiama un controllo API 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.
- Entro il limite complessivo di 100 operazioni di controllo, possono essere operazioni di controllo proattive fino a 20 operazioni alla volta.
- 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 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.

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 si aggiungono account oltre questo limite, non è possibile eseguire il processo di registrazione delle unità organizzative in AWS Control Tower. Per ulteriori informazioni sul numero di account per unità organizzativa, Limitazioni basate sui servizi sottostanti AWS consulta la documentazione 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 della AWS Control Tower possono cambiare dopo un aumento della quota. Ad esempio, l'aggiornamento di un'unità organizzativa potrebbe richiedere più tempo quando sono presenti più account. In alternativa, il completamento di

un'azione su un'unità organizzativa con cinque unità potrebbe richiedere più tempo SCPs rispetto a treSCPs.

> **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 AWS della Control Tower.

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

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

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

Video dettagliato degli aumenti delle quote in AWS Control Tower.

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

Ulteriori informazioni sulle AWS quote sono disponibili nella Guida generale.AWS

Limitazioni di controllo

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

> **La guida di riferimento ai controlli**
>
> Le informazioni dettagliate sui controlli AWS Control Tower sono state spostate nella AWS Control Tower Controls Controls Reference Guide.

Se modifichi le risorse AWS Control Tower, ad esempio unaSCP, o rimuovi una AWS Config risorsa, come un registratore o un aggregatore Config, Control Tower AWS non può più garantire che i controlli funzionino come previsto. Pertanto, la sicurezza dell'ambiente con più account potrebbe essere compromessa. Il modello di sicurezza a responsabilità AWS condivisa è applicabile a tutte le modifiche apportate dall'utente.

> **Note**
>
> AWSControl 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 alcuni Paesi in Regioni AWS cui è disponibile AWS Control Tower, perché tali Regioni non supportano le funzionalità sottostanti richieste. Di conseguenza, quando distribuisci 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 nello Standard: Control Tower AWS gestito dal servizio Security Hub. 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 sui controlli del 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, vedereConsiderazioni sull'attivazione delle regioni opt-in AWS.

> **Note**
>
> Per le informazioni più aggiornate sui controlli e sul supporto regionale, ti consigliamo di chiamare il servizio `GetControl`and `ListControls`APIoperations.

Trova i controlli e le regioni disponibili

È possibile visualizzare le regioni disponibili per ogni controllo nella console AWS Control Tower. È possibile visualizzare le regioni disponibili a livello di codice con `GetControl`e `ListControls`APIsda AWS Control Catalog.

Vedi anche la tabella di riferimento dei controlli AWS Control Tower e delle regioni supportate, Controlla la disponibilità per regione, nella AWS Control Tower Controls Controls Reference Guide.

Non supportato Regioni AWS per AWS Security Hub Service-Managed Standard: Control Tower AWS

Per informazioni sui AWS Security Hub controlli del Service-Managed Standard: AWS Control Tower che non sono supportati in alcune aree Regioni AWS, vedere «Regioni non supportate» nello standard Security Hub.

Le seguenti Regioni AWS, come regione di origine, non supportano l'implementazione di controlli proattivi. Puoi implementare controlli proattivi per gestire queste regioni se distribuisci i controlli da un'altra regione d'origine che supporta i controlli proattivi.

- Canada occidentale (Calgary)

La tabella seguente mostra i controlli proattivi che non sono supportati in alcune. Regioni AWS

Identificatore di controllo	Regioni non distribuibili
`CT.DAX.PR.2`	ca-west-1, us-west-1
`CT.REDSHIFT.PR.5`	ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ovest-1, eu-central-2, eu-central-2, eu-sud-2, il-central-1, me-central-1

La tabella seguente mostra i controlli investigativi di AWS Control Tower che non sono supportati in alcuni casi Regioni AWS.

Identificatore di controllo	Regioni non distribuibili
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, ap-southeast-4, ap-southeast-4, ca-ovest-1, il-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-4, a-ovest-1, eu-central-2, eu-central-2, eu-sud-1, eu-sud-2, il-central-1, me-central-1 al-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-4, ca-ovest-1, eu-central-2, eu-sud-2, il-central-1
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	af-sud-1, ap-northeast-3, ap-sud-2, ap-sud-est-3, ap-southeast-4, ap-sud-est-1, eu-centro-2, eu-central-2, eu-sud-1, eu-sud-1 me-central-1, me-central-1
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-sud-1, il-central-1

Identificatore di controllo	Regioni non distribuibili
AWS-GR_IAM_USER_MFA_ENABLED	ap-south-2, ap-southeast-4, il-west-1, eu-central-2, eu-central-2, eu-sud-2, il-central-1, me-central-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	ap-south-2, ap-southeast-4, il-west-1, eu-central-2, eu-central-2, eu-sud-2, il-central-1, me-central-1
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-sud-2, ap-southeast-3, ca-ovest-1, eu-sud-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-sud-1, eu-sud-2, il-central-1
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, ap-southeast-1, eu-south-2
AWS-GR_RESTRICTED_SSH	af-sud-1, eu-sud-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	ca-west-1, il-central-1, me-central-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	eu-central-2, eu-south-2, il-central-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	af-sud-1, ap-northeast-3, ap-sud-2, ap-sud-est-3, ap-southeast-4, ap-sud-est-1, eu-centro-2, eu-central-2, eu-sud-1, eu-sud-1 me-central-1, me-central-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	ca-west-1, il-central-1

Identificatore di controllo	Regioni non distribuibili
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3

Limitazioni basate sui servizi sottostanti AWS

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

Linee guida generali

Come regola generale, prevediamo che il numero di account supportati durante la registrazione di un'unità organizzativa diminuisca all'aumentare del numero di regioni governate e del numero di controlli abilitati per tale unità organizzativa. Queste linee guida generali presuppongono che siano abilitati 15 controlli opzionali. Se sull'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.

AWS 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 AWS 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 <= 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 vengono conteggiati ai fini di 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 che aderiscono

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. Per esempio:

- AWS Service Catalog non è disponibile 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 a Regioni AWS causa della mancanza di funzionalità di base.

- AFT e cFCT non sono completamente disponibili a Regioni AWS causa della mancanza di funzionalità di base.

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

- È AWS Service Catalog disponibile nella regione di residenza desiderata?
- Sono disponibili i controlli necessari? Vedi Limitazioni del controllo.
- IAM Identity Center è disponibile nella regione di residenza desiderata?

Novità: guida di riferimento ai controlli AWS Control Tower

Le informazioni sui controlli in AWS Control Tower sono state trasferite in una nuova guida, la AWS Control Tower Controls Reference Guide.

Le migliori pratiche per gli amministratori AWS di 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 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 in modo efficiente l'ambiente AWS Control Tower.

Spiegazione dell'accesso agli utenti

La console AWS Control Tower è disponibile solo per gli utenti con le autorizzazioni di amministratore dell'account di gestione. Solo questi utenti possono svolgere attività amministrative all'interno della tua landing zone. Secondo le migliori pratiche, 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 membro, 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 AWS Identity and Access Management (IAM) access advisor consente di determinare le autorizzazioni di cui dispongono gli sviluppatori analizzando l'ultimo timestamp in cui un'IAMentità, 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.
- IAMsimulatore di policy: con il simulatore di IAM policy, puoi testare e risolvere i problemi di policy IAM basate su e risorse. Per ulteriori informazioni, consulta Testing Policies with the Policy Simulator. IAM IAM
- AWS CloudTrail log: puoi esaminare i AWS CloudTrail log per vedere le azioni intraprese da un utente, un 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 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.

  È possibile visualizzare una tabella riassuntiva degli eventi 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 policy utilizzando le policy di controllo del servizio (). SCPs In confronto, un controllo investigativo ti informa di vari eventi o stati esistenti, mediante AWS Config regole definite.

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.

Per 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 sulle relative funzioni, consulta Informazioni sui controlli in AWS Control Tower.

Pianifica la tua landing zone della AWS Control Tower

Durante la procedura di configurazione, AWS Control Tower avvia una risorsa chiave associata al tuo account, chiamata landing zone, che funge da casa 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, consultaAWS strategia multi-account per la tua landing zone AWS della Control Tower.

Modi per configurare AWS Control Tower

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

- Avvia AWS Control Tower in un'organizzazione esistente: Questa sezione è dedicata ai clienti già AWS Organizations pronti per essere gestiti da AWS Control Tower.
- Lancia 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 della 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 a 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 crea una struttura parallela, a AWS Organizations livello. Non modifica gli account OUs e all'interno dell'organizzazione esistente.

Informazioni sull'estensione della 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 AWS della 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 AWS solution architect prima di provare ad abilitare AWS Control Tower nella tua organizzazione. AWSLa Control Tower non può effettuare controlli preliminari per determinare se la AWS Control Tower possa interferire con l'attuale dispiegamento 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 AWS Control Tower in un'organizzazione esistente, puoi iniziare a lavorare immediatamente, in parallelo all' AWS Organizations ambiente esistente. Gli altri tuoi OUs file creati all'interno AWS Organizations sono invariati, perché non sono registrati con AWS Control Tower. Puoi continuare a utilizzare quelli OUs e gli account esattamente come sono.

AWSControl 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 AWS di 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

AWSControl 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 Audit e Log archive vengono visualizzati nella Security OU all'interno della landing zone AWS della Control Tower.

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

Riepilogo delle funzionalità

L'attivazione AWS di 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 AWS della Control Tower in un' AWS Organizations organizzazione esistente non consente di estendere la governance AWS della Control Tower da tale organizzazione ad altre organizzazioni OUs o account che non sono 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, vedere Gestisci organizzazioni e account con AWS Control Tower.

Lancia AWS Control Tower in una nuova organizzazione

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

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

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

AWSI clienti 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 consigli, denominata strategia multi-account, per aiutarti a utilizzare al meglio le tue AWS risorse, inclusa la landing zone della 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 AWS multi-account per AWS account e. AWS Organizations Dopo aver configurato la landing zone, AWS Control Tower continua ad assisterti nel mantenimento delle politiche 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 AWS della Control Tower, è possibile estendere l'implementazione AWS della 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 AWS della 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 practice per le unità organizzative con. 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 impostato 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.

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

Definizione di un ambiente ben progettato

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

AWSControl Tower offre una landing zone che viene configurata automaticamente. Implementa i controlli per garantire la conformità alle linee guida aziendali su più account dell'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 puntare su un unico account che gestisca il carico di lavoro del settore delle carte di pagamento (PCI).
- Isolamento: un account è un'unità di protezione della sicurezza. I potenziali rischi e le minacce alla sicurezza possono essere contenuti all'interno di un account senza influire sugli altri. Pertanto, per esigenze di sicurezza potrebbe essere necessario isolare gli account l'uno dall'altro. Ad esempio, potresti avere team con profili di sicurezza diversi.
- Molti team: i team hanno responsabilità e esigenze di risorse diverse. Configurando più account, i team non possono interferire l'uno con l'altro, come potrebbero fare quando utilizzano lo stesso account.
- Isolamento dei dati: l'isolamento degli archivi dati in un account consente di limitare il numero di persone che hanno accesso ai dati e possono gestire l'archivio dati. Questo isolamento aiuta a prevenire l'esposizione non autorizzata di dati altamente privati. Ad esempio, l'isolamento dei dati aiuta a garantire 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

AWSControl 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. OUssono progettati per gestire l'applicazione delle politiche su più account.

La nostra raccomandazione è di creare almeno un ambiente di preproduzione (o staging) distinto dall'ambiente di produzione, con controlli e politiche distinti. Gli ambienti di produzione e messa in scena possono essere creati e gestiti come 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

AWSControl 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 un'altra OUs nella tua landing zone.

Si consiglia di consentire a AWS Control Tower di creare almeno un'unità organizzativa aggiuntiva, denominata Sandbox OU. Questa unità organizzativa è destinata agli ambienti di sviluppo software. AWSControl Tower può configurare l'unità organizzativa Sandbox per te durante la creazione della 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 altre OUs nella tua landing zone tramite la console AWS Control Tower nella pagina Unità organizzative.

Consigliato OUs oltre a quelli impostati automaticamente

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

> **Note**
>
> AWSControl 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**
>
> AWSControl 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**
>
> AWSControl Tower non configura l'unità organizzativa Workloads per te.

Per ulteriori informazioni, vedere Production starter organization with AWS Control Tower.

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

AWSControl Tower supporta una gerarchia di unità organizzative annidate, il che significa che è possibile creare una struttura di unità organizzative gerarchica che soddisfi i requisiti dell'organizzazione. Puoi creare un ambiente AWS Control Tower che corrisponda alle 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 esteso e piatto con indicazioni per AWS più account, vedi Esempio: carichi di lavoro in una struttura Flat OU.

- Per ulteriori informazioni su come AWS Control Tower funziona con strutture di unità organizzative annidate, vedereUnità organizzative annidate 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 dueOUs, Infrastructure_Test (per l'infrastruttura di preproduzione) e Infrastructure_Prod (per l'infrastruttura di produzione).

Nell'OUsarea 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 dueOUs, 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 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 Control TowerAWS. Si consiglia di non spostare questi bucket.
- Puoi creare i tuoi bucket di log nell'account Log Archive, ma non è consigliabile. 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.
- All'avvio, 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.
- AWSControl Tower supporta l'etichettatura solo per i controlli abilitati. Per ulteriori informazioni, consulta AWSControl Tower supporta l'etichettatura per i controlli abilitati.
- Consigliamo di abilitare l'autenticazione a più fattori (MFA) per ogni account gestito da AWS Control Tower.

Considerazioni su VPCs

- Il AWS Control Tower VPC creato da 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 aree non supportate potrebbero voler disabilitare il file creato con VPC il tuo account Account Factory. Potrebbero preferire crearne uno nuovo VPC utilizzando il portafoglio Service Catalog o crearne uno personalizzato VPC che venga eseguito solo nelle regioni richieste.
- L'impostazione predefinita VPC creata da AWS Control Tower non è uguale a VPC quella predefinita creata per tutti Account AWS. Nelle regioni in cui è supportata la AWS Control

Tower, AWS Control Tower elimina le impostazioni predefinite VPC quando crea la AWS Control TowerVPC.

- Se elimini le impostazioni predefinite VPC nella tua AWS regione d'origine, è meglio eliminarle in tutte le altre AWS regioni.

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 IAM ruolo o una policy che consenta agli amministratori di gestire solo le azioni di AWS Control Tower. L'approccio consigliato consiste nell'utilizzare la IAM policy`arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`. 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 tue politiche 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 AWS Identity and Access Management (IAM) ruoli 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 eliminate il `AWSControlTowerExecution` ruolo dai vostri account membro, nemmeno negli account non registrati. Se lo fai, non potrai registrare questi account con AWS Control Tower o registrare il genitore OUs diretto.
- Non impedirne l'utilizzo Regioni AWS tramite SCPs o AWS Security Token Service ()AWS STS. In questo modo AWS Control Tower entrerà in uno stato indefinito. Se non autorizzi l'opzione Regioni con AWS STS, la funzionalità non funzionerà in quelle aree, poiché l'autenticazione non sarebbe disponibile in quelle aree. Affidati invece alla capacità di negazione della regione di 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 Region di controllo nega il controllo applicata all'unità organizzativa, che funziona a livello di unità organizzativa per limitare l'accesso alle regioni.
- AWS Organizations `FullAWSAccess`SCPDeve essere applicata e non deve essere unita ad altre. SCPs Le modifiche apportate non SCP vengono segnalate come deviazioni; tuttavia, alcune modifiche possono influire sulla funzionalità AWS Control Tower in modi imprevedibili, se l'accesso a determinate risorse viene negato. Ad esempio, se 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 il pulsante AWS Organizations `DisableAWSServiceAccess` API per disattivare l'accesso al servizio AWS Control Tower all'organizzazione in cui hai impostato la landing zone. In tal caso, alcune funzionalità di rilevamento della deriva del 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 possa riportare in modo accurato lo stato di conformità delle unità organizzative, degli account e dei controlli dell'organizzazione. Per ulteriori informazioni, consulta API_DisableAWSServiceAccess nel 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:

  - AWSControl Tower consente azioni simultanee per implementare controlli opzionali. Per ulteriori informazioni, consulta Distribuzione simultanea per i controlli opzionali.
  - AWSControl 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, vedereCosa 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 di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.
- 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 AWS Account Management di riferimento.

> **Note**
>
> Per modificare o abilitare il piano AWS Support, devi accedere come utente root o essere un utente con le IAM autorizzazioni 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 richiederlo da AWS Control Tower. Apri la console per l'account di gestione, scegli Account e cerca l'indirizzo email.

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.

AWS Organizations guida

AWSControl Tower è strettamente associata a AWS Organizations. Ecco alcune indicazioni specifiche su come collaborano al meglio per proteggere AWS l'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 utilizzare AWS Organizations per aggiornare le politiche di controllo del servizio (SCPs) allegate a un'unità organizzativa registrata con AWS Control Tower. In questo modo, i controlli potrebbero entrare in uno stato sconosciuto, che richiederà di reimpostare la landing zone o registrare nuovamente l'unità organizzativa in AWS Control Tower. Invece, puoi crearne di nuovi SCPs e allegarli al file creato da Control Tower OUs anziché modificare SCPs quello creato da AWS Control Tower.
- Il trasferimento di account individuali, già registrati, in AWS Control Tower, dall'esterno di un'unità organizzativa registrata, causa una deriva che deve essere risolta. Per informazioni, consulta Tipi di deviazione dalla 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 tali modifiche non vengono registrate. Se devi accedere a questi account tramiteSSO, vedi Accesso all'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.
- AWSControl Tower gestisce il filtraggio delle autorizzazioni in modo diverso rispetto a come AWS Organizations lo fa. Se i tuoi account sono dotati di 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
- AWSControl Tower non supporta autorizzazioni miste nelle 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.
- AWS Organizations `FullAWSAccess`SCPDevono essere applicati e non devono essere uniti ad altri. SCPs Le modifiche apportate non SCP vengono segnalate come deviazioni; tuttavia, alcune modifiche possono influire sulla funzionalità AWS Control Tower in modi imprevedibili, se l'accesso a determinate risorse viene negato. Ad esempio, se SCP viene scollegato o modificato, un account potrebbe perdere l'accesso a un AWS Config registratore o creare una lacuna nella registrazione. CloudTrail
- Non AWS Organizations `DisableAWSServiceAccess` API utilizzarlo per disattivare l'accesso al servizio AWS Control Tower all'organizzazione in cui hai configurato la landing zone. In tal caso, alcune funzionalità di rilevamento della deriva del 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 possa riportare in modo accurato lo stato di conformità delle unità organizzative, degli account e dei controlli dell'organizzazione. Per ulteriori informazioni, consulta API_DisableAWSServiceAccess nel AWS Organizations API Reference.

IAMGuida all'Identity Center

AWSControl 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 IAM configurarlo 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**
>
> SSOè 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 Managemente abbreviato in Identity Center. IAMIAM

Per impostazione predefinita, AWS Control Tower configura AWS IAM l'Identity Center per la landing zone, in linea con le linee guida sulle migliori pratiche definite in Organizzazione AWS dell'ambiente utilizzando più account. La maggior parte dei clienti sceglie l'impostazione predefinita. 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.

Scelta di un'opzione

Dalla console, puoi scegliere di gestire autonomamente IAM Identity Center durante il processo di configurazione della landing zone, anziché consentire a 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 automaticamente AWS IAM Identity Center come IdP, Control AWS Tower crea solo i ruoli e le policy necessari per gestire Control AWS Tower, ad esempio `AWSControlTowerAdmin` e. `AWSControlTowerAdminPolicy` Per le landing zone autogestite, AWS Control Tower non crea più IAM ruoli e raggruppamenti 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 AWS della Control Tower, gli utenti, i gruppi e i set di autorizzazioni creati dalla 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 dell' AWS IAMIdentity 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 Control Tower sui controlli pre-lancio della pagina Guida introduttiva 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 Considerazioni per la modifica della fonte di identità nella Guida per l'utente di IAM Identity Center.
- Utilizzo di AWS IAM Identity Center e AWS Control TowerPer ulteriori informazioni sull'utilizzo di AWS Control Tower e IAM Identity Center, vedere.

Guida Account Factory

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 Risoluzione dei problemi della AWSControl Tower User Guide.

Si consiglia di creare utenti o IAM ruoli federati anziché utenti. IAM Gli utenti e IAM i ruoli federati forniscono credenziali temporanee. IAMgli utenti dispongono di credenziali a lungo termine che possono essere difficili da gestire. Per ulteriori informazioni, consulta IAMle identità (utenti, gruppi di utenti e ruoli) nella Guida per l'IAMutente.

Se ti sei autenticato come IAM utente o utente dell'IAMIdentity Center durante il provisioning di un nuovo account in Account Factory o quando utilizzi la funzionalità di registrazione dell'account AWS Control Tower, verifica che l'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 Guida per l'utente di AWS Control Tower.

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

Linee guida sulla sottoscrizione a Topics SNS

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

- L'`aws-controltower-AllConfigNotificationsSNS`argomento 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 Configsu ciò che pubblicano quando questo argomento è configurato.)
- I dati degli eventi del `aws-controltower-BaselineCloudTrail` percorso sono impostati per essere pubblicati anche sull'`aws-controltower-AllConfigNotificationsSNS`argomento.
- Per ricevere notifiche dettagliate sulla conformità, ti consigliamo di iscriverti all'`aws-controltower-AllConfigNotificationsSNS`argomento. 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'`aws-controltower-AggregateSecurityNotificationsSNS`argomento.
- Per ricevere notifiche sugli errori di AWS Control Tower Account Factory for Terraform (AFT), puoi iscriverti a un SNS argomento chiamato aft_failure_notifications, mostrato nel AFT repository. Per esempio:

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

- Tutti gli SNS argomenti inattivi sono crittografati con la crittografia del disco. Per ulteriori informazioni, consulta Crittografia dei dati.

Per ulteriori informazioni sugli SNS argomenti e sulla conformità, vedere Prevenzione e notifica.

Guida per KMS le chiavi

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

AWS KMS consente di creare chiavi multiregionali e KMS chiavi asimmetriche. Tuttavia, AWS Control Tower non supporta chiavi multiregionali o chiavi asimmetriche. AWSControl Tower esegue un controllo preliminare delle chiavi esistenti. È possibile che venga visualizzato un messaggio di errore se si seleziona 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 HSM cluster AWS Cloud: crea un archivio di chiavi personalizzato associato al tuo HSM cluster Cloud. Quindi puoi creare una KMS chiave, che risiede nell'archivio di chiavi HSM personalizzato Cloud che hai creato. Puoi aggiungere questa KMS chiave a AWS Control Tower.

È necessario apportare un aggiornamento specifico alla politica delle autorizzazioni di una KMS chiave per farla funzionare con AWS Control Tower. Per i dettagli, consulta la sezione chiamataAggiorna la politica KMS chiave.

Procedure consigliate per gli aggiornamenti delle landing zone

Questa sezione fornisce alcune considerazioni e le migliori pratiche da tenere a mente quando stai considerando di aggiornare la 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.
- Procedura consigliata: se disattivi il CloudTrail percorso a livello di organizzazione in AWS Control Tower, configura e gestisci i tuoi percorsi.
- Procedura consigliata: quando utilizzi l'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 KMS chiave
- Personalizza il periodo di conservazione dei log
- Controlli obbligatori avanzati
- Maggiore numero di controlli disponibili
- Integrato con AWS Security Hub
- 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 i AWS CloudTrail trail a livello di account che AWS gestisce.
- 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 si esegue l'aggiornamento alla versione 3.0 o successiva, AWS Control Tower elimina i percorsi a livello di account creati originariamente, dopo 24 ore.
- Nessun dato proveniente da questi percorsi viene perso. I registri esistenti vengono conservati anche quando i sentieri vengono rimossi.
- AWSControl Tower crea un nuovo percorso nello stesso bucket Amazon S3 per i trail, per differenziare i percorsi a livello di account dai percorsi a livello di organizzazione.
  - Il percorso del registro delle tracce degli account ha la seguente forma: `/orgId/AWSLogs/...`
  - Un percorso di log del trail organizzativo ha la seguente forma: `/orgId/AWSLogs/orgId/...`
- Le CloudTrail tracce aggiuntive che hai implementato, quelle non utilizzate da AWS Control Tower, non vengono toccate.
- 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 si disattiva un percorso a livello di organizzazione, AWS Control Tower continua a creare il percorso, ma ne imposta lo stato su Disattivato.
- Come buona prassi, 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 alla Foundational OU. Non apporta modifiche agli account del carico di lavoro o. OUs Tuttavia, come best practice, quando si utilizza l'ambiente AWS Control Tower, si consiglia di configurare un ambiente di test. All'interno dell'ambiente di test isolato, puoi testare gli aggiornamenti della landing zone di AWS Control Tower, nonché tutte le modifiche che potresti apportare alle politiche 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,

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 SCP politiche 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 SCP politiche di disattivazione dell'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 della 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 assicura 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	Descrizione
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
2.8	2-10-2022	Zona di atterraggio versione 2.8

Versione	Data di rilascio	Descrizione
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 chiavi di AWS KMS crittografia
- 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 ultime funzionalità di 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 alla versione precedente della 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, consultaImpossibile aggiornare la zona di atterraggio.

Hai la possibilità di cancellare le mappature AWS dell'Identity Center (precedentemente chiamate AWS SSO) non utilizzate quando aggiorni la landing zone. Per ulteriori informazioni, vedere Note sul campo: Cancella automaticamente le mappature degli IAM Identity Center non utilizzate durante gli aggiornamenti del 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 funzione 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 tua landing zone e poi aggiornare gli account registrati individualmente. 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 nell'unità organizzativa registrata. Sono necessari aggiornamenti completi con una nuova versione di AWS Control Tower come 2.9, 3.0 e così via.

> **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 AWS della Control Tower è tramite la pagina delle impostazioni della Landing zone, a cui puoi accedere selezionando le impostazioni della zona di atterraggio nella barra di navigazione a sinistra della dashboard 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, consultaAggiorna 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 inAggiorna l'account nella console.

> **Facoltativamente, registra nuovamente OU per aggiornare gli account**
>
> Per le AWS Control Tower registrate OUs con meno di 300 account, puoi andare alla pagina OU 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 la versione 3.1 o successiva della zona di atterraggio AWS Control Tower, 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 della landing zone nella console AWS Control Tower o tramite la AWS Control TowerAPIs.

> **Note**
>
> Se scegli di implementare una versione di landing zone che salti una versione intermedia, ad esempio se passi dalla 3.1 alla 3.3, AWS Control Tower distribuirà automaticamente la versione intermedia come parte dell'operazione di aggiornamento.
> Nelle conversazioni, 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, vai 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 registratiOUs.

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

AWSLe zone di atterraggio 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

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 AWS Control Tower, versione 3.0 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, vedereAWSControl Tower landing zone versione 3.1.

Schema della zona di atterraggio 3.1

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "centralizedLogging": {
            "$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
        },
        "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
    },
    "OrganizatinalUnit": {
        "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": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                }
            },
            "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": {
            "$ref": "#/definitions/AccessManagement"
        },
        "centralizedLogging": {
            "$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
        },
        "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": {
```

```
                "$ref": "#/definitions/S3BucketConfiguration"
            }
        },
        "additionalProperties": false
    },
    "OrganizatinalUnit": {
        "type": "object",
        "required": [
            "name"
        ],
        "properties": {
            "name": {
                "type": "string",
                "maxLength": 120,
                "minLength": 1,
                "pattern": "^[\\s\\S]*$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "OrganizationStructure": {
        "type": "object",
        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizatinalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizatinalUnit"
            }
        },
        "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 3.3

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "centralizedLogging": {
            "$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": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "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
        },
        "OrganizatinalUnit": {
            "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": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                }
            },
            "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
        }
    }
}
```

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 SCPs consentono di identificare le risorse che necessitano di modifiche o aggiornamenti della configurazione da apportare per risolvere la deriva.

Per riparare la maggior parte dei tipi di deriva, scegli Ripristina nella pagina delle impostazioni della zona di atterraggio. Inoltre, puoi risolvere alcuni tipi di deriva scegliendo di registrare nuovamente un'unità organizzativa. Per ulteriori informazioni sui tipi di deriva e su come risolverli, vedere e. Tipi di deviazione dalla 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 chiamataTipi 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 Reimposta e poi scegli Conferma, 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.

Fornisci e aggiorna gli account utilizzando l'automazione

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

- È possibile effettuare il provisioning e personalizzare gli account con AWSControl 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 delle personalizzazioni per AWS Control Tower (cFCT) .
- Automazione degli script: se si preferisce utilizzare un API approccio, è possibile aggiornare gli account utilizzando il APIframework di Service Catalog e AWS CLI aggiornare gli account in un processo batch. Dovresti chiamare il `UpdateProvisionedProduct`APIService Catalog per ogni account. Puoi scrivere uno script per aggiornare gli account, uno per uno, con questoAPI. 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 Procedura dettagliata: automatizza il provisioning degli account nelle API di AWS Control Tower tramite Service Catalog.

> Procedura guidata: video
>
> Procedura guidata: videoÈ progettato per il provisioning automatico degli account con uno script, ma i passaggi si applicano anche all'aggiornamento dell'account. Usa `UpdateProvisionedProduct` API invece di. `ProvisionProduct` API

Un ulteriore passaggio dell'automazione tramite script consiste nel verificare lo stato Succeed dell'evento del `UpdateLandingZone` ciclo di vita 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 API
- AWS Organizations API
- API AWS Control Tower
- 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 le API di AWS Control Tower, consulta il post sul blog AWS Control Tower rilascia API, controlli predefiniti per le unità organizzative.

Automatizzazione delle attività relative alle landing zone

Le API per le zone di atterraggio di AWS Control Tower ti aiutano 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

Le API di base di AWS Control Tower ti aiutano 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 Chiudi 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 AWS 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 Fornisci 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 e policy di controllo dei servizi (SCP). Per ulteriori informazioni, consulta Panoramica delle 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 principali 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 API e CLI. AWS 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 in AWS CLI: è una shell preautenticata basata su browser che puoi avviare direttamente da. AWS Management Console 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 AWS Management Console, 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 IAM le autorizzazioni per AWS CloudShell

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

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

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

Se si desidera limitare l'ambito delle azioni che un IAM utente o un utente di IAM Identity Center può eseguire AWS CloudShell, è possibile creare una politica personalizzata che utilizzi la politica `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 IAM le politiche nella Guida per l'AWS CloudShell utente.

> **Note**
>
> La tua IAM identità richiede anche una politica 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 AWS Management Console, 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 TowerAWS CloudShell

Dopo l'avvio AWS CloudShell da AWS Management Console, 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' AWS Management Console accesso nella regione di origine della tua landing zone e devi aver effettuato l'accesso come utente dell'IAMIdentity Center o IAM utente con autorizzazioni amministrative per l'account di gestione che contiene la tua landing zone.

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

   Esempio: controlla il tuo AWS Config stato

   Comandi di visualizzazione:

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - La risposta normale è qualcosa del genere `"name": "default"`
2. Se 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 AWS CLI i comandi da 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:wad4a567d8bfd9a1234ebeea56\""}
```

`ETag`È 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. AWS CloudFormation fornisce e configura tali risorse per te.

Quando si utilizza AWS 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 aree geografiche.

AWS Control Tower e AWS CloudFormation modelli

Per fornire e configurare le risorse AWS Control Tower e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON oYAML. Questi modelli descrivono le risorse che desideri inserire nei tuoi AWS CloudFormation stack. Se non conosci JSON oYAML, puoi usare AWS CloudFormation Designer per iniziare a usare i AWS CloudFormation modelli. Per ulteriori informazioni, consulta Che cos'è AWS 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. AWS CloudFormation Per ulteriori informazioni, inclusi esempi JSON e YAML modelli per questi tipi di risorse, consulta AWS Control Towerla Guida per l'AWS CloudFormation utente.

> **Note**
>
> Il limite per `EnableControl` gli `DisableControl` aggiornamenti AWS Control Tower è di 100 operazioni simultanee, di cui fino a 20 relative ai controlli proattivi.

Per visualizzare alcuni AWS Control Tower esempi relativi alla console CLI e alla console, consulta Abilitare i controlli con. AWS CloudFormation

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation APIRiferimento
- 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. È possibile rinominare le unità organizzative in qualsiasi momento utilizzando la AWS Organizations console, ma apportare modifiche alle unità organizzative AWS Organizations può 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 deselezionare 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 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 AWS CloudFormation risorse prima che vengano fornite, per assicurarsi che le nuove risorse siano conformi agli obiettivi di controllo dell'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. Per 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 (SCP). Puoi distribuire modelli e policy personalizzati a singoli account e unità organizzative (OU) all'interno della tua organizzazione.

  Il codice sorgente per cFCT è disponibile in un GitHub repository.

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-codepersonalizzazione integra AWS CloudFormation modelli con policy di controllo dei AWS servizi (SCP) ed 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 account e unità organizzative nella landing zone distribuendo risorse specificate dall'utente.

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 risorse su account e unità organizzative in modo automatico.
- Estendi l'architettura di rete: puoi implementare architetture di rete personalizzate che migliorano e proteggono la 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-samples`repository.
- 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 delle personalizzazioni per AWS Control Tower (cFCT)

Customizations for AWS Control Tower (cFCT) ti aiuta a personalizzare la tua landing zone AWS della Control Tower e a rimanere in linea con AWS le migliori pratiche. Le personalizzazioni sono implementate con AWS CloudFormation modelli e politiche di controllo del servizio (). SCPs

Questa funzionalità cFCT è integrata con gli eventi del ciclo di vita di AWS Control Tower, in modo che l'implementazione delle risorse rimanga sincronizzata 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.

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 l'implementazione di Customizations for AWS Control Tower (cFCT). Include un collegamento al AWS CloudFormationmodello che avvia, configura ed esegue i AWS servizi richiesti, in linea con le migliori pratiche per la sicurezza e la 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 ultimi aggiornamenti e modifiche a Customizations for AWS Control Tower (cFCT), fate riferimento al CHANGELOGfile.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.

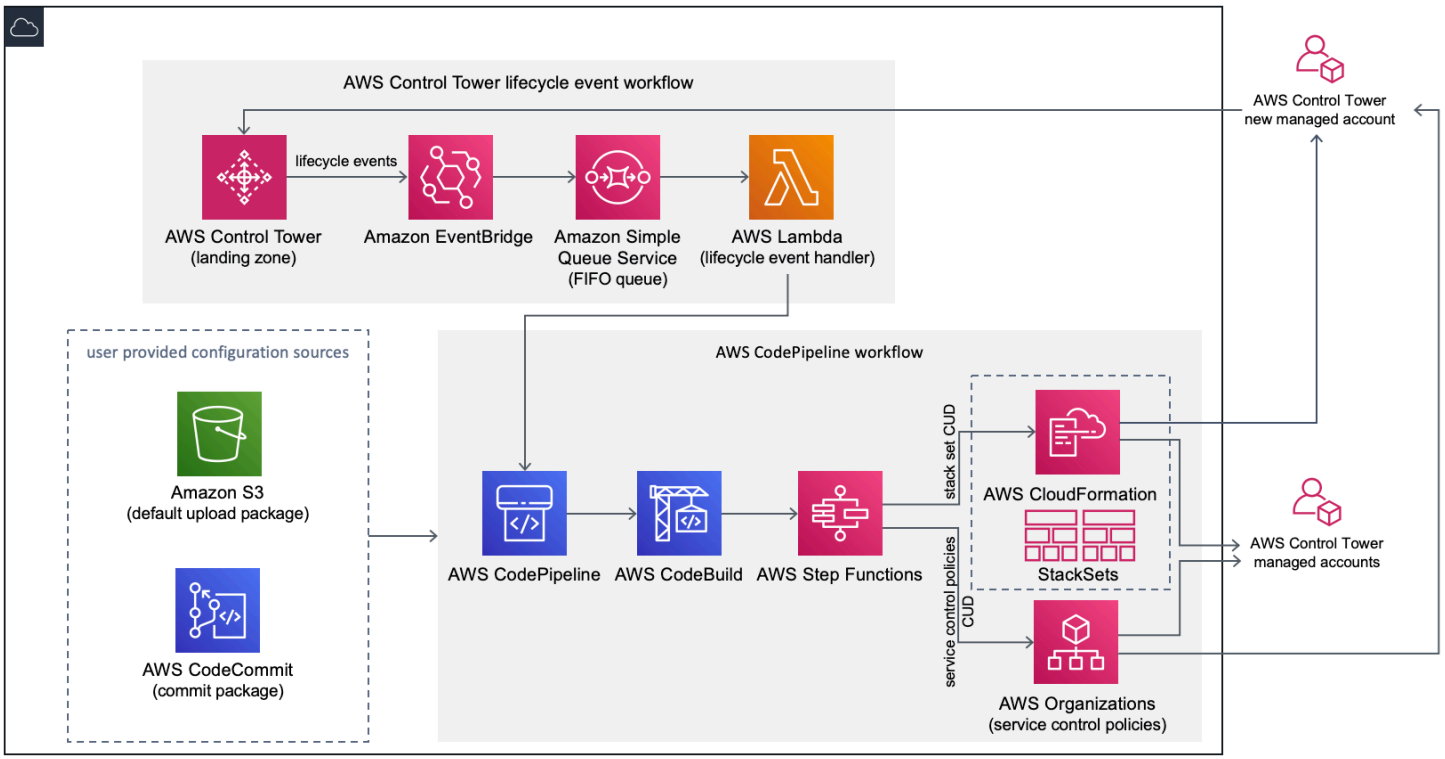

Figura 1: Personalizzazioni per l'architettura AWS Control Tower

cFct include un AWS CloudFormation modello che puoi 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 del AWS Control Tower.

> **Nota**
>
> CfCT deve essere utilizzato nella regione di origine della AWS Control Tower e nell'account di gestione AWS Control Tower, poiché è lì che viene dispiegata la zona di atterraggio AWS della Control Tower. Per informazioni sulla configurazione di una landing zone AWS della Control Tower, fare riferimento aNozioni 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 StackSetsmacchina 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 CodePipelineun flusso di lavoro
- e un flusso di lavoro AWS relativo agli eventi del ciclo di vita di Control Tower.

Il flusso di lavoro AWS CodePipeline

Il AWS CodePipeline flusso di lavoro configura AWS CodePipeline, AWS CodeBuildprogetta e AWS Step Functionscoordina la gestione dell'organizzazione AWS CloudFormation StackSets e all'SCPsinterno 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
- SCPStage: richiama la macchina a stati della policy di controllo del servizio, che chiama to create. AWS Organizations API SCPs
- AWS CloudFormation Stage: richiama lo stack set state machine per distribuire le risorse specificate nell'elenco degli account o quelle fornite OUs nel 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 AWS lavoro degli eventi del ciclo di vita di 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 evento Amazon, una coda first-in first-out (SQS) di Amazon Simple Queue Service (AmazonFIFO) 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 SQS FIFO coda di Amazon, richiama la AWS Lambda funzione e richiama la pipeline di codice per eseguire la distribuzione a valle di stack set 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 CodeCommiti 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 AWS CloudFormation modello, cFct può creare un AWS CodeCommitrepository 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 SQS Amazon e nei parametri sensibili nel AWS Systems Manager Parameter Store. 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 FIFO coda o ai `SecureString` valori del Parameter Store, è necessario aggiungere amministratori alla policy. `CustomControlTowerKMSKey` La rotazione automatica dei tasti è abilitata per impostazione predefinita.

AWS Lambda

cFct utilizza AWS Lambda funzioni per richiamare i componenti di installazione durante l'installazione 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 SNS (Amazon) durante il flusso di lavoro. Amazon SNS viene lanciato solo quando scegli di ricevere notifiche di approvazione della pipeline.

Amazon Simple Storage Service

Quando distribuisci 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 landing zone AWS della Control Tower. Il manifesto di esempio identifica le configurazioni richieste per i set di stack e le politiche di controllo del servizio (SCPs) necessarie per implementare le 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 Amazon Simple Queue Service SQS (Amazon) per acquisire gli FIFO eventi del ciclo di vita da Amazon. EventBridge Attiva una AWS Lambda funzione, che richiama la distribuzione o. 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

AWSSystems 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 installata la tua landing zone di AWS Control Tower; ovvero, devi installarla nell'account di gestione Control Tower AWS nella tua regione di origine della Control TowerAWS. 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 AWS 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. A tale scopo, seleziona l'`CodeCommit`opzione nel parametro. AWS CloudFormation

> **Comprimere o non comprimere?**
>
> Quando utilizzi il bucket S3 predefinito, assicurati che il pacchetto di configurazione sia disponibile come `.zip` file. Se stai usando 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 tue 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, l'implementazione procede all'esecuzione delle fasi rimanenti della pipeline, in base alle esigenze, per implementare la funzionalità Customizations for AWS Control Tower (cFCT).

È possibile utilizzare il parametro di approvazione manuale per impedire l'esecuzione delle personalizzazioni per la configurazione AWS Control Tower, rifiutando il primo tentativo di esecuzione nella pipeline. Questo parametro consente inoltre di convalidare manualmente le personalizzazioni per le modifiche alla configurazione del 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 AWS 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 GitHubrepository 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 implementato nel tuo account di gestione AWS Control Tower e nella tua regione di origine AWS Control Tower. Se non hai configurato una landing zone, vediNozioni 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 AWS 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 AWS CloudFormation modello in questa sezione implementa Customizations for 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 una AWS regione diversa, 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 installato la landing zone di AWS Control Tower, che è la tua regione d'origine.

3. Nella pagina Crea stack, verifica che nella casella di URLtesto sia URL visualizzato il modello corretto e scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack cFCT.
5. In Parametri, esaminate i seguenti parametri e 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”.

Configurazione della pipeline		
Parametro	Predefinito	Descrizione
Indirizzo e-mail di approvazione della pipeline	<Optional Input>	L'indirizzo e-mail per le notifiche di approvazione. Per utilizzare questo parametro, è necessario impostare il parametro Pipeline Approval **`Yes`** Stage su.
AWS CodePipelineFonte	`Amazon S3`	La fonte per aiutarti AWS CodePipeline a scegliere dove archiviare e configurare le personalizzazioni cFCT.
AWS CodeCommit Configurazione		
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 CodeCommit Repository? parametrizza `Yes` e inserisci il nome esatto di quel repository.

AWS CodeCommit Configurazione		
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` .
AWS 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.

AWS 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 l'AWS CloudFormation operazion e venga interrotta in quella regione. Il valore minimo consentito è 0 e il valore massimo consentito è 100. Per ulteriori informazioni, consulta le opzioni operative di Stack Set.

6. Scegli Next (Successivo).
7. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
8. Nella pagina Rivedi, verifica e conferma le impostazioni. Assicurati di selezionare la casella per confermare che il modello creerà AWS Identity and Access Management (IAM) risorse.
9. Seleziona Create (Crea) per implementare lo stack.

   Puoi visualizzare lo stato dello stack nella AWS 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 politiche di controllo del servizio (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. Accedere alla console AWS CloudFormation.
2. Seleziona lo CloudFormation stack Customizations for AWS Control Tower (cFCT) esistente, quindi seleziona Aggiorna.
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 Amazon S3 URL, inserisci il modello URL per il modello da GitGub cui hai precedentemente caricato su Amazon S3, quindi scegli Avanti.
   c. Verifica che il modello URL 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 per confermare che il modello potrebbe creare AWS Identity and Access Management (IAM) risorse.
9. Scegliete Visualizza set di modifiche e verificate 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, ALLle 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 consoleAWS 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, vederethe 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`

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 gli ambienti Control Tower AWS 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 implementare 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 i seguenti elementi:

- Un file manifesto
- Un set di modelli di accompagnamento
- Altri JSON file 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 modificare la posizione di origine del AWS CodeCommit repository. Per ulteriori informazioni, consulta Modificare una pipeline CodePipeline nella Guida per l'AWS CodePipeline utente.

Il file manifest è un file di testo che descrive le AWS risorse che puoi utilizzare per personalizzare la tua landing zone. CodePipeline svolge le seguenti 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 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 AWS CloudFormation modelli inclusi nel pacchetto o ospitati in remoto, utilizzando and. AWS CloudFormation `validate-template` `cfn_nag` Se il file manifesto e i AWS 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 della politica di controllo del servizio

La fase della politica di controllo del servizio richiama la macchina a stati della politica di controllo del servizio per AWS Organizations APIs richiamare la creazione delle politiche di controllo del servizio ()SCPs.

5. AWS CloudFormation fase delle risorse

   La fase AWS CloudFormation delle risorse richiama la macchina a stati dello stack set per distribuire le risorse specificate nell'elenco degli account o delle unità organizzative (OUs), fornito nel file manifest. La macchina a stati crea le AWS CloudFormation risorse nell'ordine in cui sono specificate nel file manifest. 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 personalizzata AWS di Control Tower con il file manifest, il set di modelli di accompagnamento e altri JSON file. 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 manifesto

Il `manifest.yaml` file è un file di testo che descrive AWS le tue risorse. L'esempio seguente mostra la struttura del file manifest.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

Come illustrato 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 AWS di 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 home AWS Control Tower è l'impostazione predefinita quando si creano risorse AWS Control Tower personalizzate (ad esempio AWS CloudFormation StackSets), a meno che non venga specificata una regione più specifica per la risorsa.

```
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 aAggiornamenti della versione manifesto.

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

Questo argomento descrive la sezione delle risorse del file manifesto, in cui definirete le risorse necessarie per le personalizzazioni. Questa sezione del file manifesto inizia dalla parola chiave resources e continua fino alla fine del file.

La sezione delle risorse del file manifesto specifica l' AWS CloudFormation StackSets or AWS Organizations SCPs, che cFCT distribuisce automaticamente tramite la pipeline del codice. È possibile elencareOUs, account e regioni per distribuire istanze stack.

Le istanze dello stack vengono distribuite a livello di account anziché a livello di unità organizzativa. SCPsvengono 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
    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. AWS CloudFormation StackSets La stringa fornita assegna un nome più intuitivo per un set di stack.

- Tipo: Stringa
- Campo obbligatorio: sì
- Valori validi: a-z, A-Z, 0-9 e un trattino basso (_). Qualsiasi altro carattere viene sostituito automaticamente con un carattere di sottolineatura (_).

description — La descrizione della risorsa.

- Tipo: Stringa
- Required: No

resource_file: questo file può essere specificato come posizione relativa al file manifest, un Amazon S3 URI o URL che rimanda a un AWS CloudFormation modello o a una politica di controllo del AWS Organizations servizio per la creazione di risorse o. JSON AWS CloudFormation SCPs

- Tipo: Stringa
- Campo obbligatorio: sì

1. L'esempio seguente mostra la`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 Amazon S3 URI

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. L'esempio seguente mostra il file di risorse fornito come Amazon S3 HTTPS URL

```
resources:
  - name: SecurityRoles
```

```
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Se fornisci un Amazon S3URL, verifica che la bucket policy consenta l'accesso in lettura all'account di gestione AWS Control Tower da cui stai distribuendo cFCT. Se fornisci un Amazon S3 HTTPSURL, 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 sui bucket di Amazon S3 e un ARN luogo 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 il *`AccountId`* variabile mostrata nell'esempio con l'ID AWS dell'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. AWS CloudFormation

- Tipo: MapList
- Required: No

La sezione dei parametri contiene coppie di parametri chiave/valore. 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'`stack_set`opzione per la distribuzione delle risorse tramite AWS CloudFormation StackSets o l'opzione in caso di distribuzione. `scp` SCPs

- Tipo: Stringa
- Valori validi: `stack_set` | `scp`
- Campo obbligatorio: sì

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

> **Note**
>
> Se si desidera distribuire un, la destinazione deve essere un'unità organizzativaSCP, non un account.

- Tipo: Elenco di stringhe `account name` o `account number` per indicare che questa risorsa verrà distribuita nell'elenco di account specificato o 0U `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 `0U 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. cFCT non supporta l'implementazione di istanze stack nell'account di gestione dell'organizzazione.

export_outputs — Elenco di coppie nome/valore che denotano le chiavi dei parametri. SSM Queste chiavi SSM parametriche consentono di memorizzare gli output del modello 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 SSM parametri e il valore contiene la `value` stringa del parametro.
- Valori validi: qualsiasi stringa o `$[output_`*`CfnOutput-Logical-ID`*`]` variabile in cui *`CfnOutput-Logical-ID`* corrisponde alla variabile di output del modello. Per ulteriori informazioni sulla sezione Output di un AWS CloudFormation modello, consulta Output nella Guida per l'AWS CloudFormation utente.
- Required: No

Ad esempio, il seguente frammento di codice memorizza la variabile di `VPCID` output del modello nella chiave del SSM parametro 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 AWS 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.
- Required: No

Unità organizzativa root

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

- Se si sceglie il metodo di distribuzione di`scp`, quando si aggiunge Root in`organizational_units`, AWS Control Tower applica le politiche a tutti i OUs file sotto Root. Se si sceglie il metodo di distribuzione di`stack_set`, quando si aggiunge Root under`organizational_units`, cFCT distribuisce gli stack set in tutti gli account sotto il Root registrati in Control Tower, ad eccezione dell'account di AWS 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 migliori pratiche, l'implementazione 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 AWSControlTowerExecutionruolo 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 IAM i ruoli 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 aggiungete Root come unità organizzativa in`organizational_units`, non aggiungetene 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`, AWS Control Tower distribuisce l'unità SCPs all'ultima unità organizzativa nel percorso dell'unità organizzativa annidata. Per 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, si consideri il percorso. `OUName1:OUName2:OUName3` L'ultima unità organizzativa del percorso è`OUName3`. cFct distribuisce i set SCPs to `OUName3` e stack solo su tutti gli account direttamente sotto`OUName3`.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> La funzionalità di unità organizzativa annidata è supportata solo nella versione V2 del file manifest (15/03/2021).

Crea le tue personalizzazioni

Per creare personalizzazioni personalizzate, è possibile modificare il `manifest.yaml` file aggiungendo o aggiornando le politiche di controllo del servizio (SCPs) e AWS CloudFormation le risorse. 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 le politiche di controllo del servizio

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

Fase 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 file personalizzato SCP nella `example-configuration` cartella del pacchetto zip archiviato nel bucket Amazon S3, apri il `example-manifest.yaml` file e inizia a modificarlo.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #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
    #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 Amazon URL S3 per il file di risorse e utilizzi parametri con coppie chiave/valore.

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

- Un JSON file di policy contiene SCPs il file da OUs distribuire.

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`

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
```

```
    ]
}
```

Configurare un pacchetto di configurazione per AWS CloudFormation StackSets

Questa sezione spiega come impostare un pacchetto di configurazione per AWS 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 AWS 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 l'impostazione di un pacchetto di configurazione. SCPs 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
    #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 AWS 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
    #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 si aggiorna la struttura delle cartelle, è possibile includere tutti i file AWS CloudFormation modello e i file di SCP policy di supporto 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 AWS CloudFormation

CFct fornisce un meccanismo noto come alfred helper per ottenere il valore di una chiave SSMParameter Store definita nel modello. AWS CloudFormation Utilizzando l'helper alfred, è possibile utilizzare i valori memorizzati nel SSM Parameter Store e senza aggiornare il modello. AWS CloudFormation Per ulteriori informazioni, consulta Cos'è un AWS CloudFormation modello? nella Guida AWS 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, valuta la possibilità di lavorare con valori che non cambiano da un'istanza dello stack all'altra. 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. AWS 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 che l'`VPC ID`and `subnet ID` possa essere passato 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 AWS CloudFormation .

AWS 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
```

AWS CloudFormation set di pila 2:

Lo snippet mostra i parametri specificati nel file AWS 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]
```

AWS 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 AWS 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]"
```

JSONschema per il pacchetto di personalizzazione

Lo JSON schema per il pacchetto di personalizzazione per cFct si trova nel repository del codice sorgente su. GitHub Puoi usare lo schema con molti dei tuoi strumenti di sviluppo preferiti e potresti trovarlo utile per ridurre gli errori quando crei il tuo file. `manifest.yaml`

Aggiornamenti della versione manifesto

Per informazioni sulla versione più recente di Customizations for AWS Control Tower (cFCT), consultate il CHANGELOGfile.md nel repository. GitHub

Warning

La versione 2.2.0 di Customizations for AWS Control Tower (cFCT) ha introdotto uno schema manifest (versione 2021-03-15) per allinearsi 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.AWS CloudFormation SCPs DevOps
Ti consigliamo vivamente di aggiornare lo schema del manifesto 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 dell'unità organizzativa principale e dell'unità organizzativa annidata non sono supportate nella versione 2020-01-01.

Proprietà obsolete nella versione manifest 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

Passaggi di aggiornamento obbligatori

Quando si esegue l'aggiornamento alla versione dello schema del manifesto 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 cartella SCPs in organization_policies tra le 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.

AWS 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 altamente consigliati

AWS 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 e il valore del parametro dal JSON file dei parametri esistente nel nuovo formato per la proprietà parameters. Questo vi aiuterà a gestirli nel file manifest.

> **Note**
>
> La proprietà parameter_file è supportata nella versione manifest 2021-03-15.

Rete in AWS Control Tower

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

Se la configurazione o le funzionalità predefinite 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 VPC e AWS Control Tower, consulta Creazione di un'infrastruttura di rete AWS multi-VPC scalabile e sicura.

Argomenti correlati

- Per informazioni su come funziona AWS Control Tower quando registri account con VPC esistenti, consulta. Registrazione di 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 per i VPC, consulta la documentazione di Account Factory sull'aggiornamento di un account.
- Per ulteriori informazioni sull'utilizzo di reti e VPC in AWS Control Tower, consulta la sezione sulle reti nella pagina di informazioni correlate di questa Guida per l'utente.

VPC e AWS regioni in AWS Control Tower

Come parte standard della creazione dell'account, AWS crea un VPC AWS predefinito in ogni regione, anche nelle regioni che non 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 i VPC AWS predefiniti 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 VPC

Ecco alcuni dati essenziali sui VPC AWS Control Tower:

- Il VPC creato da AWS Control Tower quando si effettua il provisioning di un account in Account Factory non è lo stesso del AWS VPC predefinito.
- 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 avere AWS VPC aggiuntivi entro il limite dell'account.
- Ogni VPC AWS Control Tower ha tre zone di disponibilità in tutte le regioni ad eccezione della regione Stati Uniti occidentali (California settentrionale) e due zone di disponibilità all'interno. `us-west-1` `us-west-1` Per impostazione predefinita, a ogni zona di disponibilità è assegnata una sottorete pubblica e due sottoreti private. Pertanto, nelle regioni ad eccezione degli Stati Uniti occidentali (California settentrionale), ogni VPC AWS Control Tower contiene nove sottoreti per impostazione predefinita, suddivise in tre zone di disponibilità. Negli Stati Uniti occidentali (California settentrionale), sei sottoreti sono suddivise in due zone di disponibilità.
- A ciascuna delle sottoreti del tuo VPC AWS Control Tower viene assegnato un intervallo univoco, di uguali dimensioni.
- Il numero di sottoreti in un VPC è configurabile. Per ulteriori informazioni su come modificare la configurazione delle sottoreti del VPC, consulta l'argomento Account Factory.
- Poiché gli indirizzi IP non si sovrappongono, le sei o nove sottoreti all'interno del tuo VPC AWS Control Tower possono comunicare tra loro senza restrizioni.

Quando si lavora con VPC, AWS Control Tower non fa distinzioni a livello di regione. Ogni sottorete viene allocata secondo l'esatto intervallo CIDR specificato. Le sottoreti VPC possono esistere in qualsiasi regione.

Note

Gestisci i costi del VPC

Se imposti la configurazione VPC di Account Factory in modo che le sottoreti pubbliche siano abilitate durante il provisioning di un nuovo account, Account Factory configura VPC per creare un gateway NAT. Ti verrà addebitato l'utilizzo da parte di Amazon VPC.

VPC e impostazioni di controllo

Se esegui il provisioning di account Account Factory con le impostazioni di accesso a Internet VPC abilitate, tale impostazione Account Factory ha la precedenza sul controllo Impedisci l'accesso a Internet per un'istanza Amazon VPC gestita da un cliente. Per evitare di abilitare l'accesso a Internet per gli account appena assegnati, è necessario modificare l'impostazione in Account Factory. Per ulteriori informazioni, consulta Procedura dettagliata: Configurazione di AWS Control Tower senza un VPC.

CIDR e peering per VPC e AWS Control Tower

Questa sezione è destinata principalmente agli amministratori di rete. L'amministratore di rete della tua azienda di solito è la persona che seleziona l'intervallo CIDR complessivo per la tua organizzazione AWS Control Tower. L'amministratore di rete alloca quindi le sottoreti a partire da tale intervallo per scopi specifici.

Quando scegli un intervallo CIDR per il tuo VPC, AWS Control Tower convalida gli intervalli di indirizzi IP in base alla specifica RFC 1918. Account Factory consente un blocco CIDR fino /16 a 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` (nessun IP al di fuori dell'intervallo `192.168`)

Se l'intervallo specificato non rientra in questi valori, AWS Control Tower fornisce un messaggio di errore.

L'intervallo CIDR predefinito è `172.31.0.0/16`.

Quando AWS Control Tower crea un VPC utilizzando l'intervallo CIDR selezionato, assegna lo stesso intervallo CIDR a ogni VPC per ogni account creato all'interno dell'unità organizzativa (OU). A causa della sovrapposizione predefinita degli indirizzi IP, questa implementazione inizialmente non consente il peering tra nessuno dei tuoi VPC AWS Control Tower nell'unità organizzativa.

Sottoreti

All'interno di ogni VPC, AWS Control Tower divide l'intervallo CIDR specificato in modo uniforme in nove sottoreti (tranne negli Stati Uniti occidentali (California settentrionale), dove è composto da sei sottoreti). Nessuna delle sottoreti all'interno di un VPC si sovrappone. Pertanto, tutti possono comunicare tra loro, all'interno del VPC.

In sintesi, per impostazione predefinita, la comunicazione tra sottoreti all'interno del VPC è illimitata. La best practice per controllare la comunicazione tra le sottoreti VPC, se necessario, è quella di configurare liste di controllo degli accessi con regole che definiscono il flusso di traffico consentito. Per il controllo del traffico tra istanze specifiche, utilizza i gruppi di sicurezza. Per ulteriori informazioni sulla configurazione di gruppi di sicurezza e firewall in AWS Control Tower, consulta Walkthrough: Configurare i gruppi di sicurezza in AWS Control Tower With Firewall Manager AWS.

Peering

AWS Control Tower non limita il peering da VPC a VPC per la comunicazione tra più VPC. Tuttavia, per impostazione predefinita, tutti i VPC AWS Control Tower hanno lo stesso intervallo CIDR

predefinito. Per supportare il peering, è possibile modificare l'intervallo CIDR nelle impostazioni di Account Factory in modo che gli indirizzi IP non si sovrappongano.

Se modifichi l'intervallo CIDR nelle impostazioni di Account Factory, a tutti i nuovi account che vengono successivamente creati da AWS Control Tower (utilizzando Account Factory) viene assegnato il nuovo intervallo CIDR. I vecchi account non vengono aggiornati. Ad esempio, è possibile creare un account, quindi modificare l'intervallo CIDR e creare un nuovo account e i VPC allocati a questi due account possono essere collegati in peering. Il peering è possibile perché i relativi intervalli di indirizzi IP non sono identici.

Ruoli e autorizzazioni correlati

AWSControl Tower utilizza IAM i ruoli 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 IAM gruppi e le relative autorizzazioni in AWS Control Tower, consulta IAMIdentity Center groups for AWS Control Tower.
- Per informazioni sulle autorizzazioni necessarie per il provisioning degli account, vedi Autorizzazioni richieste per gli account.
- Per informazioni sulle autorizzazioni della console richieste per AWS Control Tower, vedi 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, vedere Creare ruoli e assegnare autorizzazioni e Ruoli programmatici e relazioni di trust per l'account di audit Control Tower AWS.
- Per informazioni sugli altri ruoli utilizzati da AWS Control Tower per gestire gli account, vedere Utilizzo delle politiche (politiche) basate sull'identità per AWS Control Tower e delle IAM politiche gestite per Control Tower AWS.
- Per informazioni su AWS Control Tower e AWS Config ruoli, vedi AWSControl Tower ConfigRecorderRole.
- Per informazioni sui ruoli utilizzati da AWS Control Tower per l'aggregazione AWS Config informazioni per i tuoi account, vedi Come si aggrega AWS Control Tower AWS Config regole negli account non gestitiOUs.
- Per informazioni su come proteggere le risorse durante l'assegnazione di ruoli e autorizzazioni, vedi Condizioni opzionali per le relazioni di fiducia tra i ruoli, Configurazione facoltativa AWS KMS chiavi e Impedisci l'impersonificazione tra servizi.
- Per informazioni specifiche sul provisioning automatico degli account in AWS Control Tower con IAM ruoli, vedere Automated Account Provisioning with IAM Roles.
- Per visualizzare la politica che protegge il AWS Config SNSargomento, vedere The AWS Config SNSpolitica dell'argomento.

Come funziona AWS Control Tower con i ruoli per creare e gestire gli account

In generale, i ruoli fanno parte della gestione delle identità e degli accessi (IAM) in AWS. Per informazioni generali IAM e ruoli in AWS, consulta l'argomento sui IAM ruoli nel AWS IAMGuida per l'utente di .

Ruoli e creazione di account

AWSControl Tower crea l'account di un cliente chiamando `CreateAccount` API il AWS Organizations. Quando AWS Organizations crea questo account, crea un ruolo all'interno di quell'account, che AWS Control Tower nomina passando un parametro aAPI. Il nome del ruolo è `AWSControlTowerExecution`.

AWSControl Tower assume il `AWSControlTowerExecution` ruolo di tutti gli account creati da Account Factory. Utilizzando questo ruolo, AWS Control Tower definisce le baseline 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. AWSLe linee di base di Control Tower sono contenute nei ruoli che applichi a ogni account registrato.

Per ulteriori informazioni sugli account e sulle risorse, consulta. Informazioni su Account AWS in AWS Control Tower

Il AWSControlTowerExecution ruolo, spiegato

Il ruolo `AWSControlTowerExecution` deve essere presente in tutti gli account registrati. Consente a AWS Control Tower di gestire i singoli account e di riportare le 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 nella Security OU (a volte chiamati account core), AWS Control Tower crea il ruolo al momento della configurazione iniziale della 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 Control TowerAWS.
- Quando si estende la governance a un'unità organizzativa, AWS Control Tower utilizza il StackSet-AWSControlTowerExecutionRole per creare il ruolo in tutti gli account di quell'unità organizzativa.

Scopo del `AWSControlTowerExecution` ruolo:

- `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, consultaAggiungi manualmente il IAM ruolo richiesto a un ruolo esistente Account AWS e registralo.

Come funziona il `AWSControlTowerExecution` ruolo conOUs:

Il `AWSControlTowerExecution` ruolo garantisce che i controlli della 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:

- È possibile fornire report di conformità e sicurezza più facilmente, in base alle funzionalità di controllo e registrazione incorporate dai controlli Control TowerAWS.
- 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

Puoi imporre condizioni nelle tue politiche 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 evitare che un utente malintenzionato ottenga l'accesso alle tue risorse, modifica manualmente la policy di fiducia di AWS Control Tower aggiungendone almeno una `aws:SourceArn` o a `aws:SourceAccount` determinate condizioni all'informativa. Come best practice di sicurezza, consigliamo vivamente di 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'intera ARN risorsa o se stai specificando più risorse, puoi utilizzare la `aws:SourceArn` condizione con caratteri jolly (*) per le parti sconosciute di. ARN Ad esempio, `arn:aws:controltower:*:123456789012:*` funziona se non desideri specificare una regione.

L'esempio seguente dimostra l'uso della `aws:SourceArn` IAM condizione con le policy di fiducia relative al IAM ruolo. Aggiungi la condizione nella tua relazione di fiducia per il AWSControlTowerAdminruolo, perché il responsabile del servizio AWS Control Tower interagisce con esso.

Come mostrato nell'esempio, la fonte ha ARN il formato: `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Sostituisci le stringhe `${HOME_REGION}` `${CUSTOMER_AWSACCOUNT_id}` con la tua regione di origine e l'ID dell'account chiamante.

```
{
  "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, la Source ARN designata come `arn:aws:controltower:us-west-2:012345678901:*` è l'unica ARN autorizzata a eseguire l'`sts:AssumeRole`azione. 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`.

L'esempio successivo mostra le `aws:SourceArn` condizioni `aws:SourceAccount` e applicate alla politica di fiducia dei ruoli.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "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, vedereGestisci l'accesso alle risorse.

Raccomandazioni:

Si consiglia di aggiungere condizioni ai ruoli creati da AWS Control Tower, poiché tali ruoli vengono assunti direttamente da altri AWS servizi. Per ulteriori informazioni, vedere l'esempio di AWSControlTowerAdmin, mostrato in precedenza in questa sezione. Per il AWS Config ruolo del registratore, si consiglia di aggiungere la `aws:SourceArn` condizione, specificando il registratore ARN Config come fonte consentita. ARN

Per ruoli simili AWSControlTowerExecutiono per gli altri ruoli programmatici che possono essere assunti dall'account AWS Control Tower Audit in tutti gli account gestiti, si consiglia di aggiungere la `aws:PrincipalOrgID` condizione alla politica di fiducia per questi ruoli, che convalida che il principale che accede alla risorsa appartenga a un account nel modo corretto AWS organizzazione. Non aggiungete l'istruzione `aws:SourceArn` condizionale, perché non funzionerà come previsto.

> **Note**
>
> In caso di deriva, è possibile che un ruolo AWS della Control Tower venga ripristinato in determinate circostanze. Si consiglia di ricontrollare periodicamente i ruoli, se li avete personalizzati.

Come si aggrega AWS Control Tower AWS Config regole negli account non gestiti OUs

L'account di gestione AWS Control Tower crea un aggregatore a livello di organizzazione, che aiuta a rilevare elementi esterni AWS Config regole, in modo che AWS Control Tower non debba accedere agli account non gestiti. La console AWS Control Tower mostra quante sono state create esternamente AWS Config regole che 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 politica `AWSConfigRoleForOrganizations` gestita e una relazione di fiducia con. `config.amazonaws.com`

Ecco la IAM politica (JSONartefatto) allegata al ruolo:

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Ecco la relazione di `AWSControlTowerConfigAggregatorRoleForOrganizations` fiducia:

```
{
    "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 quando crea il AWS Config aggregatore:

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
```

```
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

Nuove risorse create: `AWSControlTowerConfigAggregatorRoleForOrganizations` e `aws-controltower-ConfigAggregatorForOrganizations`

Quando sei pronto, puoi registrare gli account singolarmente o registrarli come gruppo registrando un'unità organizzativa. Quando hai registrato 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 a AWS Config console in cui è possibile visualizzare i dettagli di ogni regola esterna per l'account. Utilizza le informazioni contenute nel AWS Config console e la console AWS Control Tower per determinare se sono abilitati 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 controllo e assumere il ruolo di esaminare gli 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 a AWS Solo funzioni Lambda. Per motivi di sicurezza, questi ruoli hanno relazioni di fiducia con altri ruoli, il che significa che le condizioni in base alle quali i ruoli possono essere utilizzati sono rigorosamente definite.

Lo stack AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` crea questi IAM ruoli esclusivamente programmatici e interaccount nell'account di audit:

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

Lo stack AWS Control Tower `StackSet-AWSControlTowerSecurityResources` crea questi IAM ruoli esclusivamente programmatici e interaccount 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 da AWS Solo servizio 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— AWS policy gestita

2. AssumeRole-aws-controltower- AuditAdministratorRole — politica in linea — Creato da Control TowerAWS, segue l'artefatto.

```
{
  "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 da AWS Solo servizio 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— AWS policy gestita

2. AssumeRole-aws-controltower- AuditReadOnlyRole — politica in linea — Creato da Control TowerAWS, segue l'artefatto.

```
{
  "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"
    }
  ]
}
```

Fornitura automatica 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 AWSControlTowerExecutionruolo 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 IAM seguente politica di autorizzazioni, oltre a. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso: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:SearchGroupsWithGroupName",
                "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:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA` e `sso:ProvisionSAMLProvide` sono richieste da AWS Control Tower Account Factory per interagire con AWS IAMIdentity Center.

Risorse in AWS Control Tower

- Per informazioni generali sulla proprietà delle risorse in AWS Control Tower, vedere Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower.
- Per informazioni sulle risorse create da AWS Control Tower negli account condivisi, vedere Informazioni sugli account condivisi.
- Per informazioni sulle risorse che AWS Control Tower crea quando effettua il provisioning di un account tramite Account Factory, vedere Considerazioni sulle risorse per Account Factory.
- Per visualizzare i dettagli sui tipi di AWS risorse definiti da AWS Control Tower, da utilizzare con AWSControl Tower APIs, vedere 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

Attualmente, AWS Control Tower è supportato nelle seguenti AWS regioni:

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- US West (Oregon)
- Canada (Centrale)
- Asia Pacifico (Sydney)
- Asia Pacifico (Singapore)
- Europa (Francoforte)
- Europa (Irlanda)
- Europe (London)
- Europa (Stoccolma)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Tokyo)
- Europa (Parigi)
- Sud America (San Paolo)
- Stati Uniti occidentali (California settentrionale)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Osaka-Locale)
- Europa (Milano)
- Africa (Città del Capo)
- Medio Oriente (Bahrein)
- Israele (Tel Aviv)
- Medio Oriente (UAE)
- Europa (Spagna)
- Asia Pacific (Hyderabad)

- Europa (Zurigo)
- Asia Pacifico (Melbourne)
- Canada occidentale (Calgary)

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 d'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 si attiva AWS Control Tower in una nuova regione, vedereConfigura 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 della AWS Control Tower in AWS regioni in cui non sono necessari carichi di lavoro per funzionare. La disattivazione di una regione non ti 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 imposta 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

Quando configuri le regioni AWS del 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 ti 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 della 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 AWS delle regioni 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 API framework di Service Catalog e AWS CLI aggiornare gli account in un processo batch. Per ulteriori informazioni, consulta Fornisci e aggiorna gli account utilizzando l'automazione.

Evita una governance mista durante la configurazione delle regioni

È importante aggiornare tutti gli account in un'unità organizzativa dopo aver esteso la governance AWS della Control Tower a una nuova Regione AWS e dopo aver rimosso la governance AWS della 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 disciplinano ciascun account all'interno di un'unità organizzativa. La governance mista si verifica in un'unità organizzativa se gli account non vengono aggiornati dopo che AWS Control Tower ha esteso la governance a una nuova Regione AWS o ha rimosso la governance.

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

In un'unità organizzativa con governance mista, se si effettua il provisioning di un nuovo account, tale nuovo account riceve la stessa 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 registrataOUs.

> **Note**
>
> AWSControl 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 implementare 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. È possibile che venga visualizzato un messaggio `FAILED_TO_ENABLE` di 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, l'`EnableControl`APIoperazione sull'unità organizzativa non riesce per quanto riguarda 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 dello Standard: AWS Control Tower gestito dal servizio Security Hub non possono segnalare la conformità in modo accurato nelle regioni in cui vi è una discrepanza tra la configurazione della landing zone e gli account che non vengono aggiornati.
- La governance mista non modifica il comportamento dei controlli SCP basati (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

- Scegli Aggiorna account per ogni account nell'unità organizzativa che mostra lo stato Aggiorna disponibile nella pagina Organizzazioni della console.
- Scegli Re-Register OU nella pagina Organizations, che aggiorna automaticamente tutti gli account nell'unità organizzativa, per chi OUs ha meno di 1000 account.

Considerazioni sull'attivazione delle regioni opt-in AWS

Sebbene la Regioni AWS maggior parte sia attiva per impostazione predefinita per le tue 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 o semplicemente regioni.

Il termine opt-in ha una base storica. Tutte le Regioni AWS regioni introdotte dopo il 20 marzo 2019 sono considerate regioni opt-in. Le regioni opt-in hanno requisiti di sicurezza più elevati rispetto alle regioni commerciali, per quanto riguarda la condivisione di IAM dati tramite account attivi nelle regioni opt-in. Tutti i dati gestiti tramite il IAM servizio sono considerati dati di identità, inclusi utenti, gruppi, ruoli, politiche, 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 i criteri per le 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 di attivazione come regione principale del AWS Control Tower, attivala prima seguendo i passaggi descritti 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 opzionali 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
- Medio Oriente (UAE) Regione, 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

AWSControl Tower dispone di alcuni controlli che funzionano in modo diverso nelle regioni opt-in rispetto alle regioni commerciali. Per ulteriori informazioni, consulta Limitazioni di controllo. Di seguito sono riportate alcune considerazioni da tenere a mente quando si distribuiscono i carichi di lavoro in regioni opzionali.

> **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. AWSControl 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 alla AWS Control Tower, come la console di AWS fatturazione o. AWS SDK

- Quando AWS Control Tower estende la governance a una regione opt-in, attiva (opts-in) la regione in tutti gli account dei membri. Quando rimuovi una regione dalla governance, AWS Control Tower non disattiva (disattiva) la regione negli account dei membri.
- Durante la deselezione della regione, AWS Control Tower salta la rimozione delle risorse da una regione che ha aderito se tale regione è stata disattivata manualmente per un account proveniente da una fonte esterna a Control TowerAWS, come la AWS console di fatturazione o. AWS SDK 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, comprese le Regioni che hanno aderito all'iniziativa. Tuttavia, AWS Control Tower non disattiva le Regioni opt-in. È possibile disattivare le regioni opzionali 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 configurata con una regione di attivazione 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.
- La piattaforma sottostante API ha dei limiti di capacità, che possono aumentare la latenza da pochi minuti a molte ore, a seconda del numero di regioni, account e carico del servizio. Come procedura ottimale, è consigliabile effettuare l'opt-in solo per quelle Regioni AWS in cui verranno eseguiti i carichi di lavoro e optare per 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 che hanno aderito, 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

AWSControl Tower offre due controlli Region Deny. 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 registratiOUs.
- Questo controllo non può essere configurato per singoli utentiOUs.

> **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 si rimuove il controllo, questo viene rimosso su tutte le regioni registrate OUs e tutte le regioni non governate in AWS Control Tower rimangono nello stato Non governato ed è possibile distribuire risorse in Regioni al di fuori della disponibilità della 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 il Region Deny ControlSCP, consulta Deny access to in AWS base alla richiesta Regione AWS nel riferimento AWSControl Tower Control. La AWS Control Tower SCP è simile SCPalla forma AWS Organizations, ma non identica.

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.

Esegui il provisioning e gestisci gli account in AWS Control Tower

Questo capitolo include una panoramica e le procedure per il provisioning e la gestione degli account dei membri nella landing zone AWS della Control Tower.

Include anche una panoramica e le procedure per la registrazione di un AWS account esistente in AWS Control Tower.

Per ulteriori informazioni sugli account in AWS Control Tower, vedereInformazioni su Account AWS in AWS Control Tower. Per informazioni sulla registrazione di più account in AWS Control Tower, vedere. Registra un'unità organizzativa esistente con AWS Control Tower

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

Metodi di approvvigionamento

AWSControl 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

Il modo standard per creare account membri è tramite Account Factory, un prodotto basato su console che fa parte del Service Catalog. Se la tua landing zone non è in stato di deriva, puoi utilizzare Crea account come metodo per aggiungere nuovi account dalla console e Registra account per registrare AWS account esistenti in Control TowerAWS.

Con Account Factory, puoi fornire account di base, facendo affidamento sulle impostazioni predefinite di AWS Control Tower. È inoltre possibile 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 sulla 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).

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 funzione di registrazione dell'account all'interno di AWS Control Tower, se la landing zone non è in stato di deriva. Per informazioni, consulta Registra un account esistente.
- 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 atterraggio AWS Control Tower, utilizzando il codice Lambda e i ruoli appropriati. IAM Vedi Provisioning automatico degli account con ruoli. IAM
- Terraform: dalla AWS Control Tower Account Factory per 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 Fornisci account con AWS Control Tower Account Factory for Terraform (AFT) .
- Personalizzazione di Account Factory nella console AWS Control Tower: dopo i passaggi 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 AWS CloudFormation modelli o modelli Terraform.

> **Note**
>
> AWS CloudFormation i progetti 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.

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 Per la procedura di registrazione di un dispositivo esistente Account AWS utilizzando la console AWS Control Tower, consultaRegistra un account esistente.

Dietro le quinte della creazione dell'account

1. È possibile avviare la richiesta, ad esempio, dalla pagina AWS Control Tower Account Factory, direttamente dalla AWS Service Catalog console o chiamando il Service Catalog `ProvisionProduct`API.
2. AWS Service Catalog chiama AWS Control Tower.
3. AWSControl Tower avvia un flusso di lavoro, che come primo passaggio chiama il AWS Organizations `CreateAccount`API.
4. Dopo aver AWS Organizations creato l'account, AWS Control Tower completa il processo di provisioning applicando progetti e controlli.
5. Service Catalog continua a sondare AWS Control Tower per verificare il completamento del processo di approvvigionamento.
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.

Autorizzazioni richieste per gli account

Le autorizzazioni richieste per ogni metodo di fornitura e aggiornamento degli account sono discusse rispettivamente in ciascuna sezione. 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.

> **Note**
>
> Quando si effettua il provisioning di un account, il richiedente dell'account deve sempre disporre delle autorizzazioni e delle autorizzazioni. `CreateAccount` `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.

Quando crei account dalla console AWS Control Tower con Account Factory, devi accedere a un account con un IAM utente che ha i `AWSServiceCatalogEndUserFullAccess` criteri abilitati, oltre alle autorizzazioni per utilizzare la console AWS Control Tower, e non puoi accedere come utente root.

Per informazioni generali sulle autorizzazioni richieste in AWS Control Tower, vedereUtilizzo di policy basate sull'identità (policy IAM) per AWS Control Tower. Per informazioni sui ruoli e gli account in AWS Control Tower, consulta Ruoli e account.

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 su Account AWS in AWS Control Tower

An Account AWS è il contenitore per tutte le risorse di tua proprietà. Queste risorse includono le AWS Identity and Access Management (IAM) identità accettate dall'account, che determinano chi ha accesso a quell'account. IAMIe identità possono includere utenti, gruppi, ruoli e altro. Per ulteriori informazioni sull'utilizzo di utentiIAM, 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, incluse le risorse sotto forma di modelli Account Factory e altre risorse nella landing zone. Queste risorse possono includere IAM ruoli, AWS CloudTrail percorsi, prodotti forniti da Service Catalog e utenti IAM dell'Identity Center. AWSControl Tower distribuisce anche le risorse, come richiesto dalla configurazione di controllo, per l'unità organizzativa (OU) in cui il nuovo account è destinato a diventare un account membro.

AWSControl Tower orchestra l'implementazione 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, consultaLinee guida per la creazione e la modifica delle risorse AWS Control Tower.

Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti

Prima di accettare un Account AWS account di sicurezza o di registrazione, AWS Control Tower verifica l'eventuale presenza di risorse in conflitto con i requisiti AWS della 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.

AWSControl Tower non rimuove alcuna risorsa esistente negli account di registrazione e sicurezza forniti. Tuttavia, se scegli di abilitare la funzionalità di Regione AWS negazione, il Region deny control impedisce l'accesso alle risorse nelle aree negate.

Visualizza i tuoi account

La pagina Organizzazione elenca tutti gli account OUs e dell'organizzazione, indipendentemente dall'unità organizzativa o dallo stato di iscrizione in AWS Control Tower. È possibile 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 nella pagina Organizzazione, puoi scegliere Account solo dal menu a discesa in alto a destra, quindi selezionare 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 tale account. Se l'unità organizzativa principale non è registrata, nessun controllo si applica a questo account.

- Iscrizione: l'account viene sottoposto alla governance da AWS Control Tower. Stiamo allineando l'account alla configurazione di controllo dell'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 Control TowerAWS. 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.

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, consultaConsiderazioni 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.

AWSservizio	Tipo di risorsa	Nome risorsa
AWS Organizations	Account	audit log archive
AWS Organizations	OUs	Security

AWSservizio	Tipo di risorsa	Nome risorsa
		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)

AWSservizio	Tipo di risorsa	Nome risorsa
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) 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

AWSservizio	Tipo di risorsa	Nome risorsa
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Product	AWSAccount Factory Control Tower
AWS Config	Aggregatore	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Registri	aws-controltower/CloudTrailLogs
AWS Identity and Access Management	Roles	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Policy	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWSservizio	Tipo di risorsa	Nome risorsa
AWS IAM Identity Center	Gruppi di directory	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	Set di autorizzazioni	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

Note

Non AWS 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.

AWSservizio	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)

AWSservizio	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

AWSservizio	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.

AWSservizio	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)

AWSservizio	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

AWSservizio	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 condivisi

Tre speciali Account AWS sono associati a 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, vedere 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, consultaRisorse create negli account condivisi.

Gestione dell'account

Questo Account AWS avvia AWS Control Tower. Per impostazione predefinita, l'utente root di questo account e l'IAMutente o l'utente IAM amministratore di questo account hanno pieno accesso a tutte le risorse all'interno della landing zone.

> **Note**
>
> Come procedura consigliata, consigliamo di accedere come utente IAM Identity Center con privilegi di amministratore quando si eseguono funzioni amministrative all'interno della console AWS Control Tower, anziché accedere come utente root o utente IAM amministratore per questo account.

Per ulteriori informazioni sui ruoli e le risorse disponibili nell'account di gestione, vedereRisorse create negli account condivisi.

Account di archivio dei log

L'account condiviso dell'archivio dei log viene configurato automaticamente quando crei la landing zone.

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 versione 3.3 e successive della zona di atterraggio di AWS Control Tower, gli account devono soddisfare una `aws:SourceOrgID` condizione per qualsiasi autorizzazione di scrittura nel bucket Audit. Questa condizione garantisce che nel bucket S3 sia possibile scrivere i log CloudTrail solo per conto degli account all'interno dell'organizzazione; impedisce ai CloudTrail log esterni all'organizzazione di scrivere nel bucket Control Tower AWS S3. Per ulteriori informazioni, consulta AWSControl Tower landing zone 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.

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 (AmazonSNS). 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 accountOUs, gli utenti e nella tua SCPs landing zone. Per ulteriori informazioni su drift, 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 Amazon SNS locale. 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, vedere Ruoli programmatici e relazioni di fiducia per l'account di audit AWS Control Tower.

> **Important**
>
> L'indirizzo e-mail che fornisci per l'account di controllo riceve e-mail di AWS notifica - conferma dell'abbonamento da tutti quelli Regione AWS supportati da AWS Control Tower. Per ricevere e-mail di conformità nel tuo account di controllo, devi scegliere il link Conferma iscrizione all'interno di ogni e-mail Regione AWS supportata da AWS Control Tower.

Informazioni sugli account dei membri

Gli account membro sono gli account tramite i quali gli utenti eseguono i propri AWS carichi di lavoro. Questi account membro possono essere creati in Account Factory, dagli utenti di IAM Identity Center con privilegi di amministratore nella console Service Catalog o con metodi automatizzati. Una volta

creati, questi account membro esistono in un'unità organizzativa creata nella console AWS Control Tower o registrata presso AWS Control Tower. Per ulteriori informazioni, consulta questi argomenti correlati:

- Fornitura e gestione degli account con Account Factory
- Automatizza le attività in AWS Control Tower
- AWS Terminologia e concetti relativi alle organizzazioni nella Guida per l'AWS Organizations utente.

Consultare anche Fornisci account con AWS Control Tower Account Factory for Terraform (AFT) .

> **Account e controlli**
>
> Gli account dei membri possono essere registrati a AWS Control Tower oppure possono essere 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 allocate da AWS Control Tower, vedereConsiderazioni sulle risorse per Account Factory.

Iscrivi un esistente Account AWS

È possibile estendere la governance della AWS Control Tower a un individuo, esistente Account AWS quando lo si iscrive 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.

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

Imposta prima un accesso affidabile

Prima di poter registrare un utente esistente Account AWS in AWS Control Tower, devi autorizzare AWS Control Tower a gestire o governare l'account. In particolare, AWS Control

Tower richiede l'autorizzazione per stabilire un accesso affidabile tra AWS CloudFormation e AWS Organizations per conto dell'utente, in modo da AWS 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, AWS CloudFormation puoi creare, aggiornare o eliminare pile su più account e Regioni AWS con un'unica operazione. AWSControl 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 saperne di più sull'accesso affidabile e AWS CloudFormation StackSets, vedi AWS CloudFormationStackSets e AWS Organizations.

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 AWS Control Tower all'account.

> **Account e percorsi a livello di organizzazione CloudTrail**
>
> Tutti gli account dei membri di un'unità organizzativa sono regolati dalla cronologia dell' AWS CloudTrail unità organizzativa, indipendentemente 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 hai già implementato un CloudTrail trail, potresti vedere addebiti duplicati, a meno che non elimini il trail esistente per l'account prima di registrarlo in AWS Control Tower.
> - Se si trasferisce un account in un'unità organizzativa registrata, ad esempio tramite la AWS Organizations console, e non si procede alla registrazione dell'account in Control TowerAWS, è possibile rimuovere eventuali percorsi a livello di account rimanenti relativi all'account. Se hai già installato un trail, dovrai sostenere addebiti doppi. CloudTrail 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.

Registrazione di account esistenti con VPCs

AWSControl 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 l' AWS impostazione predefinita VPC e ne crea uno nuovo VPC per quell'account.
- Quando si registra un account esistente, AWS Control Tower non ne crea uno nuovo VPC per quell'account.
- Quando si registra un account esistente, AWS Control Tower non rimuove alcun account esistente VPC o AWS predefinito VPC associato all'account.

> **Tip**
>
> Puoi modificare il comportamento predefinito per i nuovi account configurando Account Factory, in modo che non ne venga impostato uno predefinito VPC per gli account della tua organizzazione in AWS Control Tower. Per ulteriori informazioni, consulta Crea un account in AWS Control Tower senza un VPC.

Prerequisiti per l'iscrizione

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

1. Per iscrivere un account esistente Account AWS, il `AWSControlTowerExecution` ruolo deve essere presente nell'account che si sta 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 della relazione di attendibilità:

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::Management Account ID: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 Control Tower AWS.

> **Note**
>
> Quando registri un account su AWS Control Tower, il tuo account è regolato dal AWS CloudTrail percorso dell'organizzazione AWS Control Tower. Se hai già implementato un CloudTrail trail, potresti vedere addebiti duplicati, a meno che non elimini il trail esistente per l'account prima di registrarlo in AWS Control Tower.

Registra un account esistente

La funzione Enroll account è disponibile nella console AWS Control Tower, per le iscrizioni esistenti in Account AWS modo che siano gestite da AWS Control Tower. Per ulteriori informazioni, consulta Registrare un esistente. Account AWS

La funzionalità Enroll account (Registra account) è disponibile quando la landing zone non è in uno stato di deviazione. Per visualizzare questa funzionalità nella console:

- Vai alla pagina Organizzazione in AWS Control Tower.
- 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.
- Segui i passaggi per la registrazione di un singolo account, come mostrato nella sezione. Passaggi per registrare un account

> **Note**
>
> Quando registri un indirizzo email esistente Account AWS, assicurati di verificare l'indirizzo email esistente. Altrimenti, potrebbe essere creato un nuovo account.

Alcuni errori possono richiedere di aggiornare la pagina e di riprovare. 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 fino a quando la deriva della tua 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 l'account factory AWS Control Tower, come faresti con qualsiasi altro account. AWS Service Catalog Le procedure di aggiornamento sono fornite nella sezione chiamata Aggiorna e sposta gli account di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.

Passaggi per registrare un account

Dopo aver AdministratorAccessimpostato l'autorizzazione (politica) nel tuo account esistente, segui questi passaggi per registrare l'account:

Per registrare un account individuale in AWS Control Tower

- Vai alla pagina dell'organizzazione AWS di Control Tower.
- Nella pagina Organizzazione, gli account idonei alla registrazione consentono di selezionare Iscriviti 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 IAM ruolo 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.

- AWSControl 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.
- Il tuo IAM preside potrebbe non avere le autorizzazioni necessarie per fornire un account.
- AWS Security Token Service (AWS STS) è disabilitato Account AWS nella tua regione di residenza 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, consulta Registrare account che dispongono di risorse esistenti AWS Config e Interagisci con AWS Control TowerAWS CloudShell.
- Se l'account appartiene a un'altra unità organizzativa con un account di gestione, inclusa un'altra unità AWS organizzativa 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'SCPunità organizzativa della 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 l'etichettatura delle risorse. Per assistenza, contatta il rappresentante del tuo account oppure. AWS Support

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 degli account esistenti e delle relative configurazioni con AWS Control Tower, puoi seguire le best practice consigliate nella sezione seguente.

Consigliato: puoi impostare un approccio in due passaggi per la registrazione dell'account

- Innanzitutto, utilizza un pacchetto di AWS Config conformità per valutare in che modo i tuoi account potrebbero essere influenzati da alcuni AWS controlli Control Tower. Per determinare in che modo l'iscrizione a AWS Control Tower può influire sui tuoi account, consulta Estendere la governance AWS della Control Tower utilizzando i AWS Config conformance pack.
- 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 AWS della Control Tower, potresti dover rimuovere il canale di AWS Config consegna e il registratore di configurazione creati per la valutazione. Quindi sarai in grado di configurare AWS Control Tower con successo.

> **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 AWS Control Tower. È possibile 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 iscritti alla governance di AWS Control Tower devono far parte della stessa organizzazione generale. Per soddisfare questo prerequisito per la registrazione dell'account, puoi seguire questi passaggi preparatori per trasferire un account nella stessa organizzazione di Control Tower. AWS

Fasi preparatorie per inserire un account nella stessa organizzazione di AWS Control Tower

1. Eliminare 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 l'impostazione predefinitaVPC. (Questa parte è facoltativa. AWSControl Tower non modifica le impostazioni predefinite esistentiVPC.)
3. Elimina o modifica qualsiasi registratore AWS Config di configurazione o canale di distribuzione esistente tramite AWS CLI o AWS CloudShell. Per ulteriori informazioni, consulta AWS Config CLIComandi di esempio per lo stato delle risorse 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. Questo passaggio porta l'account alla piena governance AWS della 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 AWS 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'accountAnnullare 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.

AWS Config CLIComandi di esempio per lo stato delle risorse

Di seguito sono riportati alcuni AWS Config CLI comandi di esempio 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`

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`

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

Se hai già configurato la landing zone AWS della 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 sarà pronta, completa i seguenti passaggi per far sì che gli account esistenti vengano gestiti manualmente da AWS Control Tower.

Assicuratevi di leggere quanto Prerequisiti per l'iscrizione indicato in precedenza in questo capitolo.

Prima di registrare un account con AWS Control Tower, devi concedere a AWS Control Tower l'autorizzazione 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 IAM ruolo 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 IAM ruolo 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 AWS Management Console 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.

Passaggio 2: autorizza AWS Control Tower a gestire l'account.

1. Passa a IAM.
2. Vai a Ruoli.
3. Scegliere Crea ruolo.
4. Quando ti viene chiesto di selezionare il servizio a cui è destinato il ruolo, scegli Politica di fiducia personalizzata.
5. Copia l'esempio di codice mostrato qui e incollalo nel documento di policy. Sostituisci la stringa *`ID dell'account di gestione`* con l'effettivo ID dell'account di gestione del tuo account di gestione. Ecco la politica da incollare:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID: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. Scegliere 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 vai a AWS Control Tower.
2. Registra l'account.
   - Dalla pagina Organizzazione in AWS Control Tower, seleziona il tuo account, quindi scegli Registrati dal menu a discesa Azioni in alto a destra.
   - Segui i passaggi per la registrazione di un account individuale, come mostrato nella pagina. Passaggi per registrare un account
3. Verifica l'iscrizione.
   - Da AWS Control Tower, scegli Organizzazione 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 questa procedura, accedi a ogni account dell'organizzazione che desideri registrare a AWS Control Tower. Ripeti i passaggi relativi ai prerequisiti e i passaggi di registrazione per ogni account.

Registrazione automatica degli account AWS Organizations

Puoi utilizzare il metodo di registrazione descritto in un post del blog chiamato Registra AWS gli account esistenti in Control Tower per registrare i tuoi AWS Organizations account in AWS Control Tower con un processo AWS programmatico.

Il YAML modello seguente 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, consultaAWS Config CLIComandi di esempio per lo stato delle risorse.

> **Note**
>
> Se prevedi di portare AWS account esistenti in AWS Control Tower come account di audit e di archiviazione dei log e se tali account dispongono di AWS Config risorse esistenti, devi eliminare completamente AWS Config le risorse esistenti prima di poterli registrare in AWS

Control Tower a questo scopo. Per gli account che non sono destinati a diventare account di archiviazione Audit e Log, è possibile modificare le risorse Config esistenti.

Esempi di risorse AWS Config

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

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 AWS Control Tower governate dall'account di gestione.
- Il tuo account non è l'account di gestione di AWS Control Tower.
- Il tuo account non è soggetto a cambiamenti di governance.

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. Potrai inviare un unico ticket di supporto per tutti gli account che desideri registrare, come descritto in quanto segue. Fase 1: contatta l'assistenza clienti con un ticket per aggiungere l'account all'elenco degli account consentiti di AWS Control Tower

Limitazioni

- L'account può essere registrato solo utilizzando il flusso di lavoro AWS Control Tower per estendere la governance.
- 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.

> **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.

Questo processo prevede 5 fasi principali.

1. Aggiungi l'account all'elenco degli account consentiti da 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.

Fase 1: contatta l'assistenza clienti con un ticket per aggiungere l'account all'elenco degli account consentiti di AWS Control Tower

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
- 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 AWS 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 Tower CustomerCreatedConfigRecorderRoleForControl
4. Creare lo stack.

> **Note**
>
> Qualsiasi SCP che crei dovrebbe escludere un `aws-controltower-ConfigRecorderRole*` ruolo. Non modificate le autorizzazioni che limitano la capacità AWS Config delle regole di eseguire valutazioni.
> Segui queste linee guida in modo da non ricevere un messaggio `AccessDeniedException` quando hai SCP che `aws-controltower-ConfigRecorderRole*` impediscono di chiamare Config.

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.

- `LOGGING_ACCOUNT`- l'ID dell'account di registrazione
- `AUDIT_ACCOUNT`- l'ID dell'account Audit
- `IAM_ROLE_ARN`- il ruolo IAM ARN creato nella Fase 1

- `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
- S3BucketName: il nome del bucket di registrazione dell'account di registrazione AWS Control Tower

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: l'ARN dell'argomento SNS dell'account di controllo, con il seguente formato:

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

Questa modifica può essere effettuata tramite la AWS CLI utilizzando il seguente comando. Sostituite la stringa *DELIVERY_CHANNEL_NAME* con il nome del AWS Config registratore esistente.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

Fase 5c. Modifica le risorse di AWS Config autorizzazione all'aggregazione

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 AWS 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 esiste un AWS Config registratore.

1. Accedi alla AWS CloudFormation console dell'account di gestione.
2. Creane uno nuovo StackSet con il nome CustomerCreatedConfigResourcesForControlTower.
3. Copia e aggiorna il seguente modello:

```
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::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${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 LOGGING_ACCOUNT_ID e HOME_REGION*

b. ***Nel campo S3, sostituisci ORGANIZATION_ID KeyPrefix***

c. *Nel campo **SnsTopicARN**, sostituisci AUDIT_ACCOUNT*

d. *Nel **AuthorizedAccountId**campo, sostituisci AUDIT_ACCOUNT*

e. *Nel **AuthorizedAwsRegion**campo, sostituisci HOME_REGION*

4. Durante la distribuzione sulla AWS CloudFormation console, aggiungi il numero di account 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

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

Autorizzazioni per la configurazione e il provisioning degli account

Il AWS Control Tower Account Factory consente agli amministratori e agli utenti del cloud AWS IAM Identity Center di effettuare il provisioning degli account nella 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 con qualsiasi account che dispone di 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 Iscrivi un esistente Account AWS.

Per ulteriori informazioni sulle autorizzazioni, consultare Autorizzazioni richieste per gli account.

Fornire account con AWS Service Catalog Account Factory

La procedura seguente descrive come creare e fornire account come utente in IAM Identity Center tramite AWS Service Catalog. Questa procedura viene anche definita fornitura avanzata degli account o fornitura manuale degli account. Facoltativamente, potresti essere in grado di effettuare il provisioning degli account a livello di codice, con AWS CLI 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 progetti 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 dal tuo portale utenteURL.
2. Da Le tue applicazioni, scegli AWS Account.
3. Dall'elenco degli account, scegli l'ID dell'account per il tuo account di gestione. Questo ID può anche avere un'etichetta, ad esempio (Gestione).
4. Da AWSServiceCatalogEndUserAccess, scegli Console di gestione. Verrà aperta la finestra AWS Management Console per questo utente in questo account.

5. Assicurati di aver selezionato la regione corretta Regione AWS per il provisioning degli account, 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 AWSControl Tower Account Factory, quindi scegli il pulsante Avvia prodotto. Questa selezione avvia la procedura guidata per effettuare il provisioning di un nuovo account.
9. Compilare le informazioni e tenere presente quanto segue:

   - SSOUserEmailPuò essere un nuovo indirizzo e-mail o l'indirizzo e-mail associato a un utente esistente di IAM Identity Center. A prescindere dalla scelta, questo utente dispone dell'accesso a livello amministrativo all'account di cui si sta effettuando il provisioning.
   - AccountEmailDeve essere un indirizzo e-mail che non sia già associato a un Account AWS. Se hai usato un nuovo indirizzo email in SSOUserEmail, puoi usare quell'indirizzo email qui.

10. Non definire TagOptionse non abilitare le notifiche, altrimenti il provisioning dell'account potrebbe non essere eseguito. Quando hai finito, scegli Launch product.
11. Esaminare le impostazioni dell'account, quindi scegliere Launch (Avvia). Non creare un piano di risorse, altrimenti il provisioning dell'account non verrà eseguito.
12. L'account è ora in fase di provisioning. Il completamento può richiedere alcuni minuti. Puoi ricaricare la pagina per aggiornare le informazioni sullo stato visualizzate.

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

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 venduto 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 dell'indirizzo e-mail dell'utente precedente di IAM Identity Center da IAM Identity Center, vedere Disabilitazione di un utente.

Aggiorna e sposta gli account di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog

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 spostato Gli aggiornamenti dell'account sono necessari anche come parte di un aggiornamento completo delle landing zone.

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.

Controlla il comportamento quando gli account vengono spostati da un account all'altro OUs

Quando si sposta un account da un altroOUs, 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 conSCPs: I controlli SCP basati dell'unità organizzativa precedente sono rimosso. I controlli SCP basati sull'unità organizzativa di destinazione entrano in vigore su questo account.
- Per i controlli implementati con AWS CloudFormation gli 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.

Aggiorna l'account nella console

Per aggiornare un account nella console AWS Control Tower

1. Una volta effettuato l'accesso a AWS Control Tower, vai alla pagina Organizzazione.
2. Nell'elenco degli OUs account, seleziona il nome dell'account che desideri aggiornare. Gli account disponibili per l'aggiornamento mostrano lo stato Aggiornamento disponibile.
3. Successivamente vedrai la pagina dei dettagli dell'account per l'account selezionato.
4. In alto a destra, scegli Aggiorna account.

Aggiorna il prodotto fornito

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.

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 dell'IAMIdentity Center in uno `AWSAccountFactory` o più `AWSServiceCatalogAdmins` gruppi).

2. Nel riquadro di navigazione, scegli Provisioning, quindi scegli Provisioned products.
3. Per ciascuno degli account membro elencati, esegui le seguenti operazioni per aggiornare tutti gli account membro:

   a. Seleziona un account membro. Verrai indirizzato alla pagina dei dettagli del prodotto Provisioned relativa a quell'account.

   b. Nella pagina dei dettagli del prodotto Provisioned, scegli la scheda Eventi.

   c. Prendere nota dei seguenti parametri:

      - SSOUserEmail(Disponibile nei dettagli del prodotto fornito)

- AccountEmail(Disponibile nei dettagli del prodotto fornito)
- SSOUserFirstName(Disponibile in IAM Identity Center)
- SSOUSerLastName(Disponibile in IAM Identity Center)
- AccountName(Disponibile in IAM Identity Center)

d. Da Actions (Operazioni), scegliere Update (Aggiorna).

e. Scegliere il pulsante accanto alla casella Version (Versione) del prodotto da aggiornare e selezionare Next (Avanti).

f. Fornire i valori dei parametri citati in precedenza.

- Se desideri mantenere l'unità organizzativa esistente ManagedOrganizationalUnit, scegli l'unità organizzativa in cui si trovava già l'account.
- Se desideri migrare l'account verso una nuova unità organizzativa ManagedOrganizationalUnit, scegli la nuova unità organizzativa per l'account.

Un amministratore cloud centrale può trovare queste informazioni nella console AWS Control Tower, nella pagina Organizzazione.

g. Scegli Next (Successivo).

h. Rivedere le modifiche, quindi scegliere Update (Aggiorna). Questo processo può richiedere alcuni minuti per account.

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 riportata in questa sezione.

> **Note**
>
> La procedura seguente 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 persa o dimenticata?
2. Accedi all'account con la password dell'utente root.
3. Cambia l'indirizzo email come faresti per qualsiasi altro Account AWS 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 riportata 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 cambiare 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. AWSControl Tower si aggiorna automaticamente per riflettere il cambio di 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 VPC configurazione di Amazon disponibili per i tuoi utenti finali quando effettuano il provisioning di nuovi account.

Per configurare le VPC impostazioni Amazon 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 VPC configurazione 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 AmazonVPC. Per impostazione predefinita, la sottorete accessibile da Internet non è consentita.

> **Note**
>
> Se imposti la VPC configurazione di fabbrica dell'account 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 L'utilizzo ti verrà fatturato da AmazonVPC. Per ulteriori informazioni, consulta la sezione VPCPrezzi.

- 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 avere la forma di un blocco routing (CIDR) inter-domain senza classi (ad esempio, l'impostazione predefinita è). `172.31.0.0/16` Questo CIDR blocco fornisce l'intervallo complessivo di indirizzi IP di sottorete per l'VPCaccount creato da Account Factory per il tuo account. All'interno dell'utenteVPC, le sottoreti vengono assegnate automaticamente in base all'intervallo specificato e hanno dimensioni uguali. Per impostazione predefinita, le sottoreti all'interno dell'utente VPC non si sovrappongono. Tuttavia, gli intervalli di indirizzi IP di sottorete VPCs di tutti gli account assegnati potrebbero sovrapporsi.
- Scegli una regione o tutte le regioni per creare un VPC momento in cui viene fornito un account. Per impostazione predefinita, sono selezionate tutte le regioni disponibili.
- Dall'elenco, scegli il numero di zone di disponibilità per cui configurare le sottoreti in ciascuna. VPC Il numero predefinito e consigliato è 3.
- Seleziona Salva.

Puoi configurare queste opzioni di configurazione per creare nuovi account che non includano un. VPC Consulta la procedura dettagliata.

Annullare 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 blueprint. L'account viene spostato da qualsiasi

unità AWS organizzativa Control Tower e nell'area Root. L'account non fa più parte di un'unità organizzativa registrata e non è più soggetto a AWS Control TowerSCPs. È possibile chiudere l'account tramite AWS Organizations.

L'annullamento della registrazione di un account può essere effettuato anche nella console Service Catalog da un utente di IAM Identity Center del `AWSAccountFactory` gruppo, interrompendo il Provisioned Product. Per ulteriori informazioni sugli utenti o i gruppi di IAM Identity Center, consulta Gestire gli utenti e l'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

1. Apri la console Service Catalog nel tuo browser web all'indirizzohttps://console.aws.amazon.com/servicecatalog.
2. Nel riquadro di navigazione a sinistra, scegli Elenco dei prodotti Provisioned.
3. Dall'elenco degli account assegnati, scegli il nome dell'account che non desideri più che AWS Control Tower gestisca.
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

Quando annulli la registrazione di un account personalizzato, AWS Control Tower rimuove le risorse distribuite dal blueprint, nonché tutte le altre risorse che Control Tower ha creato all'AWSinterno dell'account. Dopo aver annullato la registrazione dell'account, puoi chiuderlo tramite. AWS Organizations

> **Note**
>
> Un account non registrato non viene chiuso o eliminato. Una volta annullata la registrazione dell'account, l'utente dell'IAMIdentity Center 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 dell'utente di IAM Identity Center per l'account. Per ulteriori informazioni, consulta Aggiorna e sposta gli account di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.

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.

È possibile visualizzare un elenco di AWS YouTube video che spiegano le attività più comuni in AWS Control Tower.

Chiudere 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 è la stessa cosa che annullare la registrazione di un account da AWS Control Tower: si tratta di azioni separate. È necessario annullare la registrazione dell'account prima di chiuderlo.

Chiudi un account membro AWS Control Tower tramite AWS Organizations

È possibile chiudere gli account dei membri di AWS Control Tower dall'account di gestione dell'organizzazione senza dover accedere a ciascun account membro singolarmente con le credenziali di AWS Organizations root, tramite. Tuttavia, non è possibile chiudere l'account di gestione in questo modo.

Quando si chiama il AWS Organizations CloseAccount API, o chiudi un account nella AWS Organizations console, l'account del 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.

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 documentazione relativa a AWS Organizations CloseAccount API.

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/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole

AWS servizio	Tipo di risorsa	Nome risorsa
		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

Personalizza gli account con Account Factory Customization (AFC)

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 fabbrica dell'account, 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.

I tuoi account personalizzati vengono forniti in Account Factory, tramite AWS CloudFormation modelli o con Terraform. Definirai un modello che funge 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

> **Note**
>
> AWS Control Tower contiene controlli proattivi che monitorano AWS 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.

I blueprint 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 un 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.

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.

> **Prima di iniziare**
>
> 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.

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

Preparazione per la personalizzazione

- È possibile creare un nuovo account che funga da account hub oppure utilizzarne uno esistente Account AWS. Ti consigliamo vivamente di non utilizzare l'account di gestione AWS Control Tower come account Blueprint Hub.

- Se intendi Account AWS registrarti 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.
- 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

Configurazione 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.

Fase 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 l'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 sezioni seguenti.

Accedi alla console IAM per configurare il ruolo richiesto.

Per configurare il 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.

> **Note**
>
> 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 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 AWSControlTowerBlueprintAccessruolo 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId: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.

Fase 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 AWS 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 AWS 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: nodejs16.x
     Handler: index.handler
     Timeout: 5
     Code:
       ZipFile: >
         const response = require("cfn-response");
         exports.handler = function (event, context) {
           const awsAccountId = context.invokedFunctionArn.split(":")[4]
           const connectionString= "fake connection string that's specific to account
" + awsAccountId;
           const responseData = {
             Value: connectionString,
           }
           response.send(event, context, response.SUCCESS, responseData);
           return connectionString;
         };

 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 Adminstrator Guide.

Fase 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.

> **Note**
>
> 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 AWS 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, consulta 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 AWS Management Console.
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.

Registra e personalizza gli account

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 procedure seguenti descrivono come aggiornare i blueprint personalizzati e come distribuirli.

Per aggiornare i blueprint personalizzati

1. Aggiorna il AWS 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 distribuisci 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 per le 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 uscire

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, in modo che non sia 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 AWS CloudFormation crearne uno per tuo StackSet conto. AWS CloudFormation richiede l'accesso al tuo account gestito per creare AWS CloudFormation stack in. StackSet Sebbene disponga AWS CloudFormation già dei privilegi di amministratore nell'account gestito tramite il `AWSControlTowerExecution` ruolo, questo ruolo non può essere assunto da. AWS CloudFormation

Come parte dell'abilitazione di un blueprint, AWS Control Tower crea un ruolo nell'account del membro, che AWS 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 AWS CloudFormation l'account di destinazione. Puoi fornire una policy personalizzata, che AWS Control Tower applica al ruolo che crea AWS CloudFormation per essere utilizzato. Ad esempio, se il tuo blueprint crea un parametro SSM chiamato qualcosa di importante, puoi fornire la seguente politica:

```
{
    "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'`AllowCloudFormationActionsOnStacks`istruzione è obbligatoria per tutte le politiche personalizzate AFC; AWS CloudFormation utilizza questo ruolo per creare istanze di stack, pertanto richiede l'autorizzazione per eseguire azioni sugli stack. AWS CloudFormation La `AllowSsmParameterActions` sezione è specifica del modello da abilitare.

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 AWS 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.

```
{
    "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.

Fornisci 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.

> **Note**
>
> 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.

Con AFT, si crea 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.

Prerequisiti

Prima di iniziare con AFT, è necessario creare quanto segue:

- 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)
- Uno o più `git` repository AFT nel tuo ambiente AFT completamente distribuito. Per ulteriori informazioni, consulta le fasi successive all'implementazione di AFT.

> **Tip**
>
> Facoltativamente, è possibile creare una cartella di modelli di account nel aft-account-customizationsrepository.

Per informazioni su Regioni AWS dove AFT presenta limitazioni di distribuzione, consulta Limitazioni e quote in AWS Control Tower e. Limitazioni di controllo

Fornisci un nuovo account con AFT

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 unico 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 /aft/account-request/custom-fields/. 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

È possibile aggiornare gli account forniti da AFT modificando le richieste di account inviate in precedenza ed eseguendole`git push`. Questo comando richiama il flusso di lavoro per il provisioning degli account e può elaborare le richieste di aggiornamento degli account. È possibile aggiornare l'input for`ManagedOrganizationalUnit`, che fa parte del valore richiesto per`control_tower_parameters`, e altri parametri nel file Terraform di richiesta dell'account. Per ulteriori informazioni, consulta Fornire un nuovo account con AFT.

> **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.

Implementa AWS Control Tower Account Factory per Terraform () AFT

Questa sezione è dedicata agli amministratori degli 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 AFT gestione dedicato.

> **Note**
>
> Viene distribuito un modulo Terraform. AFT Questo modulo è disponibile nel AFTrepository di e l'intero AFT repository è considerato il modulo. GitHub

Ti consigliamo di fare riferimento ai AFT moduli presenti GitHub invece di clonare il repository. AFT In questo modo è possibile controllare e utilizzare gli aggiornamenti dei moduli non appena sono disponibili.

Per i dettagli sulle ultime versioni 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'AFTambiente, è necessario disporre di quanto segue:

- Una landing zone della AWS Control Tower. Per ulteriori informazioni, consulta Pianifica la tua landing zone della AWS Control Tower.
- Una regione d'origine per la landing zone AWS della Control Tower. Per ulteriori informazioni, consulta How Regioni AWS work with AWS Control Tower.
- Una versione e una distribuzione di Terraform. Per ulteriori informazioni, consulta Terraform e AFT versioni.
- Un VCS provider per il monitoraggio e la gestione delle modifiche al codice e ad altri file. Per impostazione predefinita, AFT utilizza AWS CodeCommit. Per ulteriori informazioni, vedi Cos'è AWS CodeCommit? nella Guida AWS CodeCommit per l'utente.

  Se esegui la distribuzione AFT per la prima volta e non disponi di un CodeCommit repository esistente, devi scegliere un VCS provider esterno, ad GitHub esempio o. 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 si installaAFT.
- AFTopzioni di funzionalità. Per ulteriori informazioni, consulta 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 AFT seguendo l'Introduzione al AFT laboratorio sul sito Web di AWS Workshop Studio.

Fase 1: Avvia la landing zone AWS della 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 della 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:
>
> - IAMIdentità (utenti, gruppi di utenti e ruoli) nella Guida per l'AWS Identity and Access Management utente
> - AdministratorAccessnella AWS Managed Policy Reference Guide

Fase 2: Creare una nuova unità organizzativa per AFT (scelta consigliata)

Si consiglia di creare un'unità organizzativa separata nella propria AWS organizzazione. Qui è dove si distribuisce l'account di AFT gestione. Crea la nuova unità organizzativa con il tuo account di gestione AWS Control Tower. Per ulteriori informazioni, consulta Creare una nuova unità organizzativa.

Fase 3: Eseguire il provisioning dell'account AFT di gestione

AFTrichiede il provisioning di un AWS account dedicato alle operazioni AFT di gestione. L'account di gestione AWS Control Tower, associato alla landing zone AWS della Control Tower, vende l'account di AFT gestione. Per ulteriori informazioni, consulta Fornire account con AWS Service Catalog Account Factory.

> **Note**
>
> Se hai creato un'unità organizzativa separata perAFT, assicurati di selezionarla quando crei l'account di AFT gestione.

Il provisioning completo dell'account di AFT gestione 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**
>
> AFTsupporta la versione Terraform `1.6.0` o successiva.

Passaggio 5: chiama il modulo Account Factory for Terraform per l'implementazione AFT

Chiama il AFT modulo con il ruolo che hai creato per l'account di gestione AWS Control Tower con AdministratorAccesscredenziali. AWSControl Tower fornisce un modulo Terraform tramite l'account di gestione AWS Control Tower, che stabilisce tutta l'infrastruttura necessaria per orchestrare le richieste Control AWS Tower Account Factory.

È possibile visualizzare il AFT modulo nel repository su. AFT GitHub L'intero GitHub repository è considerato il AFT modulo. Fate riferimento al READMEfile per informazioni sugli input necessari per eseguire il AFT modulo e distribuirlo. AFT In alternativa, puoi visualizzare il AFT modulo nel registro Terraform.

Il AFT modulo include un `aft_enable_vpc` parametro che specifica se AWS Control Tower effettua il provisioning delle risorse dell'account all'interno di un cloud privato virtuale (VPC) nell'account di AFT gestione centrale. Per impostazione predefinita, il parametro è impostato su. `true` Se si imposta questo parametro su`false`, AWS Control Tower esegue la distribuzione AFT senza l'uso di VPC risorse di rete private, come NAT gateway o VPC endpoint. La disabilitazione `aft_enable_vpc` può aiutare a ridurre i costi operativi di alcuni modelli AFT di utilizzo.

> **Note**
>
> La riattivazione del `aft_enable_vpc` parametro (modifica del valore da `false` a`true`) può richiedere l'esecuzione del `terraform apply` comando due volte di seguito.

Se nel tuo ambiente disponi di pipeline stabilite per la gestione di Terraform, puoi integrare il AFT modulo nel tuo flusso di lavoro esistente. Altrimenti, esegui il AFT modulo 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 IAM nella Guida per l'AWS Identity and Access Management utente.

> **Note**
>
> Potresti attendere fino a 30 minuti per AFT completare la distribuzione tramite il modulo Terraform.

Passaggio 6: gestire il file di stato Terraform

Un file di stato Terraform viene generato durante la distribuzione. AFT Questo artefatto descrive lo stato delle risorse create da Terraform. Se prevedi di aggiornare la AFT versione, assicurati di conservare il file di stato Terraform o di configurare un backend Terraform utilizzando Amazon S3 e DynamoDB. Il AFT modulo 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 AFT dell'infrastruttura, segui questi passaggi aggiuntivi per completare il processo di configurazione e prepararti al provisioning degli account.

Fase 1: Completare CodeConnections con il VCS provider desiderato

Se scegli un VCS fornitore terzo CodeConnections, AFT lo stabilisce e lo confermi. Fai riferimento Alternative per il controllo della versione del codice sorgente in AFT a per scoprire come configurare il tuo AFT dispositivo preferitoVCS.

La fase iniziale per stabilire la AWS CodeStar connessione viene eseguita daAFT. È necessario confermare la connessione.

Passaggio 2: popola ogni repository

AFTrichiede 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 AFT account, vedereFornisci un nuovo account con AFT.
2. AFTpersonalizzazioni del provisioning degli account: questo repository gestisce le personalizzazioni che vengono applicate a tutti gli account creati e gestiti conAFT, prima di iniziare la fase di personalizzazione globale. Esempi disponibili. Per creare personalizzazioni per il provisioning degli AFT account, consulta. 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 AFT globali, consultaApplica 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 AFT dell'account, consultaApplica le personalizzazioni dell'account.

AFTsi aspetta 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

Panoramica di AWS Control Tower Account Factory for Terraform () AFT

Account Factory for Terraform (AFT) imposta una pipeline Terraform per aiutarti a fornire e personalizzare gli account in Control TowerAWS. AFTti offre il vantaggio del provisioning degli account basato su Terraform, consentendoti al contempo di governare i tuoi account con Control Tower. AWS

Dopo AFT aver creato un account, richiedi il file Terraform per ottenere l'input che attiva il flusso di lavoro per il provisioning dell'account. AFT Una volta completata la fase di fornitura dell'account, esegue AFT automaticamente una serie di passaggi prima che inizi la fase di personalizzazione dell'account. Per ulteriori informazioni, consulta la pipeline di provisioning AFT degli account.

AFTsupporta Terraform Cloud, Terraform Enterprise e Terraform Community Edition. Con AFT puoi 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 e le linee guida di conformità standard della tua organizzazione.

AFTsupporta il tracciamento delle richieste di personalizzazione dell'account. Ogni volta che invii una richiesta di personalizzazione dell'account, AFT genera un token di tracciamento univoco che passa attraverso una macchina a AWS Step Functions stati di AFT personalizzazione, 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 associati al 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 AWS Step Functions sviluppatori

AFTcombina le funzionalità di altri AWS servizi comeServizi per i componenti, per creare un framework, con pipeline che implementano Terraform Infrastructure as Code (IaC). AFT consente di:

- Invia 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

AFTcrea un account separato, denominato account di AFT gestione, per distribuire AFT le funzionalità. Prima di poter effettuare la configurazioneAFT, è necessario disporre di una landing zone esistente AWS della Control Tower. L'account di AFT gestione non è lo stesso dell'account di gestione AWS Control Tower.

AFToffre flessibilità

- Flessibilità per la tua 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

AFToffre 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 dell'impostazione predefinita per gli account AWS VPC
- Registrazione degli account assegnati al piano Enterprise AWS Support

> **Note**
>
> La AFT pipeline non è destinata all'uso nella distribuzione di risorse, come le EC2 istanze Amazon, 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 gli account con AWS Control Tower Account Factory for Terraform. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

Video dettagliato del provisioning automatico degli account in Control TowerAWS.

AFTArchitettura

Ordine delle operazioni

AFTLe operazioni vengono eseguite nell'account AFT di gestione. 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.
4. 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.

AWSControl Tower Account Factory for Terraform: flusso di lavoro per la fornitura degli account

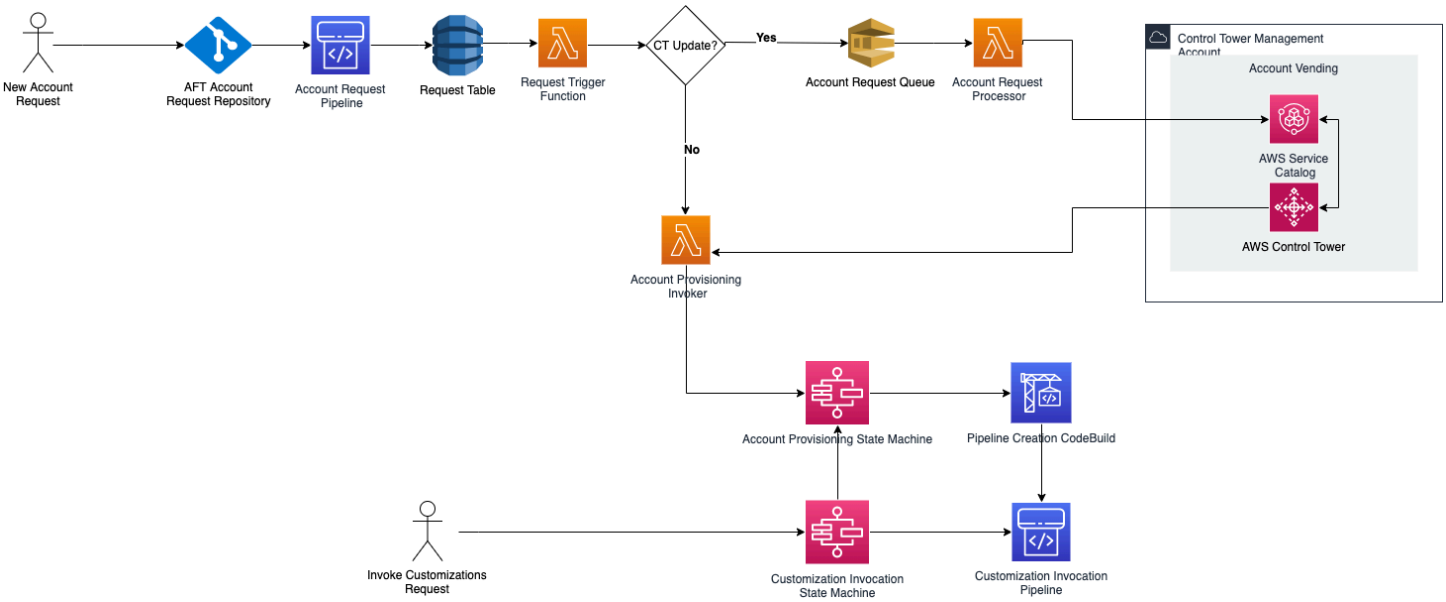

Figura 1: Account Factory AWS di Control Tower per Terraform

Costo

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

La AFT configurazione predefinita include l'allocazione degli AWS PrivateLink endpoint, per una maggiore protezione e sicurezza dei dati, e un NAT gateway necessario per il supporto. AWS CodeBuild Per i dettagli sui prezzi di questa infrastruttura, consulta i AWS PrivateLink prezzi e i VPC prezzi Amazon per il NAT Gateway. Contatta il rappresentante AWS del tuo account per informazioni più specifiche sulla gestione di questi costi. Puoi modificare queste impostazioni predefinite perAFT.

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 tutte le API richieste. Per motivi di sicurezza, è necessario evitare di registrare il valore di questo token nel sistema di controllo della versione (VCS) assegnando una variabile terraform, come mostrato nell'esempio che segue.

```
# Sensitive variable managed in 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 tua 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

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 AFTPer 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 tutti i VPC AWS predefiniti nell'account di gestione e in tutto Regioni AWS, anche se non sono state distribuite le risorse AWS Control Tower in tali account. Regioni AWS

AFT non elimina automaticamente i VPC AWS predefiniti per nessun account AWS Control Tower di cui AFT fornisce o per AWS gli account esistenti registrati in AWS Control Tower tramite AFT.

Per impostazione predefinita, i nuovi AWS account vengono creati con un VPC configurato in ciascuno Regione AWSdi essi. La tua azienda potrebbe avere procedure standard per la creazione di VPC, che richiedono di eliminare il VPC AWS predefinito ed evitare di abilitarlo, in particolare per l'account di gestione AFT.

Per abilitare questa opzione, imposta il seguente flag di funzionalità su True nella configurazione di input della distribuzione AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Per ulteriori informazioni sui VPC predefiniti, consulta VPC predefiniti e sottoreti predefinite.

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.

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	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	Policy	aws-ct-aft-*
CodeCommit	Repositories	aws-ct-aft-*
CodeBuild	Progetti di compilazione	aws-ct-aft-*

AWS service	Tipo di risorsa	Nome risorsa
Codice Pipeline	Pipeline	*-baseline-*
Amazon S3	Bucket	*-aws-ct-aft-* aws-ct-aft-*
Lambda	Funzioni	aws-ct-aft-*
Lambda	Livelli	aws-ct-aft-common-layer
DynamoDB	Tabelle	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Macchine a stato	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Argomenti	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	Bus di eventi	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Regole dell'evento	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor

AWS service	Tipo di risorsa	Nome risorsa
Servizio di gestione delle chiavi (KMS)	Chiavi gestite dal cliente	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	Archivio dei parametri	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Queues	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Gruppi di log	/aws/*/aws-ct-aft-* aws-ct-aft-*
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	AWSAFTExecutionRole AWSAFTExecution

AWS service	Tipo di risorsa	Nome risorsa
		aws-ct-aft-controltower-events-rule
AWS Systems Manager	Archivio dei parametri	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (Facoltativo)	Policy di controllo dei servizi	aws-ct-aft-protect-resources
CloudTrail (Opzionale)	Trail	aws-ct-aft-BaselineCloudTrail
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	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
Servizio di gestione delle chiavi (KMS)	Chiavi gestite dal cliente	*-aws-ct-aft-kms-gd-findings
Amazon S3	Bucket	*-aws-ct-aft-logs* aws-ct-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	AWSAFTExecutionRole AWSAFTExecution
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`

```
{
    "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.

```
{
  "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 `AWSAFTService` 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`

```
{
  "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 approvvigionamento 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`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Servizi per i componenti

Al momento della distribuzioneAFT, i componenti vengono aggiunti all' AWS ambiente da ciascuno di questi AWS servizi.

- AWSControl Tower: AFT utilizza AWS Control Tower Account Factory nell'account di gestione AWS Control Tower per effettuare il provisioning degli account.
- Amazon DynamoDB: crea tabelle AFT Amazon DynamoDB nell'account di gestione, che archiviano le richieste degli account, AFT la cronologia di controllo degli aggiornamenti degli account, i metadati degli account e gli eventi del ciclo di vita di Control Tower. AWS AFTcrea anche trigger DynamoDB Lambda per avviare processi a valle, come l'avvio del flusso di lavoro di provisioning degli account. AFT
- Amazon Simple Storage Service: AFT crea bucket Amazon Simple Storage Service (S3) nell'account di AFT gestione e nell'account di archiviazione dei log AWS Control Tower, che archiviano i log generati dai servizi richiesti dalla AWS pipeline. AFT AFTcrea anche un bucket S3

di backend Terraform, nelle AWS regioni primarie e secondarie, per archiviare gli stati Terraform generati durante i flussi di lavoro delle pipeline. AFT

- Amazon Simple Notification Service: AFT crea argomenti Amazon Simple Notification Service (SNS) nell'account di AFT gestione, che memorizza le notifiche di successo e di fallimento dopo l'elaborazione di ogni richiesta di AFT account. Puoi ricevere questi messaggi utilizzando il protocollo che preferisci.
- Amazon Simple Queuing Service: AFT crea una FIFO coda Amazon Simple Queuing Service (AmazonSQS) nell'account di gestione. AFT La coda consente di inviare più richieste di account in parallelo, ma invia una richiesta alla volta a AWS Control Tower Account Factory, per l'elaborazione sequenziale.
- AWS CodeBuild— AFT crea progetti di AWS CodeBuild compilazione nell'account di AFT gestione per inizializzare, compilare, testare e applicare i piani Terraform per il codice AFT sorgente in varie fasi di compilazione.
- AWS CodePipeline— AFT crea AWS CodePipeline pipeline nell'account di AFT gestione per l'integrazione con il provider di AWS CodeStar connessioni supportato selezionato per il codice AFT sorgente e per attivare i processi di compilazione. AWS CodeBuild
- AWSLambda: crea funzioni e livelli AFT AWS Lambda nell'account di AFT gestione per eseguire i passaggi durante i processi di richiesta dell'account, fornitura dell'AFTaccount e personalizzazione dell'account.
- AWSSystems Manager Parameter Store: AFT configura AWS Systems Manager Parameter Store nell'account di AFT gestione, per memorizzare i parametri di configurazione richiesti per i processi della AFT pipeline.
- Amazon CloudWatch: AFT crea gruppi di CloudWatch log Amazon nell'account di AFT gestione per archiviare i log generati dai AWS servizi utilizzati dalla AFT pipeline. 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 dell'account di AFT gestione in un ambiente di rete separato, per una maggiore sicurezza.
- AWSKMS— AFT utilizza il AWS Key Management Service (KMS) nell'account di AFT gestione e nell'account di archivio dei registri AWS Control Tower. AFTcrea chiavi per crittografare gli stati di Terraform, i dati archiviati nelle tabelle e gli argomenti di DynamoDB. SNS Questi log e artefatti vengono generati quando AWS risorse e servizi vengono distribuiti da. AFT KMSper impostazione predefinita, le chiavi 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 AFT gestione,

negli account AWS Control Tower e negli AFT account assegnati, secondo necessità, per eseguire le azioni richieste durante il AFT flusso di lavoro della pipeline.

- AWS Step Functions: AFT crea macchine a stati AWS Step Functions nell'account di AFT gestione. Queste macchine a stati orchestrano e automatizzano il processo e le fasi per il framework di provisioning e le AFT personalizzazioni degli account.
- 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 AFT gestione. AFTcrea regole di CloudWatch eventi Amazon negli account di AFT gestione e AWS Control Tower, che attivano più passaggi necessari durante l'esecuzione del flusso di lavoro della AFT pipeline
- 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. AFTinvia 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 daAFT. 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 fornite per il provisioning degli account AFT. 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, potreste 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 configurare 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 () AFTPer 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 tue 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 AWS come parte della fase di personalizzazione dell'account.

Panoramica

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 di personalizzazione

Prima di iniziare a personalizzare gli account, assicurati che questi prerequisiti siano soddisfatti.

- Un AFT completamente distribuito. Per informazioni su come eseguire la distribuzione, vedere. Configura e avvia il tuo AWS Control Tower Account Factory per Terraform
- `git`Archivi 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 ***`[account_customizations_name] /api_helpers/python`*** che si trova nel tuo repository.
   - ***Se le tue configurazioni personalizzate sono sotto forma di script Bash, inseriscile nella cartella [account_customizations_name] / api_helpers che si trova nel tuo repository.***
   - ***Se le tue configurazioni personalizzate sono in forma di Terraform, inseriscile nella cartella [account_customizations_name] /terraform che si trova nel tuo repository.***

   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 input`account_customizations_name`. Inserisci il nome della personalizzazione del tuo 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 è 1.6.5 o successiva, puoi scegliere come target le unità organizzative annidate (con la sintassi). `OU Name (ou-id-1234` Per ulteriori informazioni, consulta il seguente argomento su. GitHub

Dopo aver compilato i parametri dell'evento, Step Functions viene eseguito e richiama le personalizzazioni corrispondenti. AFT può richiamare un massimo di 5 personalizzazioni alla volta. Step Functions attende e si ripete fino al completamento di tutti gli account che soddisfano i criteri dell'evento.

Fase 3: Monitora l'output di AWS Step Function e guarda AWS CodePipeline in esecuzione

- L'output Step Function risultante contiene ID di account che corrispondono alla fonte dell'evento di input di Step Function.
- Accedi ad AWS CodePipeline in Developer Tools e visualizza le pipeline di personalizzazione corrispondenti per l'ID dell'account.

Risoluzione dei problemi relativi al tracciamento delle richieste di personalizzazione dell'account AFT

Flussi di lavoro di personalizzazione degli account basati su AWS Lambda registri di emissione contenenti l'account di destinazione e gli ID delle richieste di personalizzazione. AFT ti consente di tracciare e risolvere i problemi delle richieste di personalizzazione con Amazon CloudWatch Logs fornendoti le query di CloudWatch Logs Insights che puoi utilizzare per filtrare i CloudWatch log relativi alla tua richiesta di personalizzazione in base all'account di destinazione o all'ID della richiesta di personalizzazione. Per ulteriori informazioni, consulta Analyzing log data with Amazon CloudWatch Logs nella Amazon CloudWatch Logs User Guide.

Per utilizzare CloudWatch Logs Insights for AFT

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Dal riquadro di navigazione, scegli Logs, quindi seleziona Logs insights.
3. Scegli Query.
4. In Query di esempio, scegli Account Factory for Terraform, quindi seleziona una delle seguenti query:

   - Registri di personalizzazione per ID account

   > **Note**
   >
   > Assicurati di sostituire *«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 sostituire *«YOUR-CUSTOMIZATION-REQUEST-ID» con l'ID della richiesta di personalizzazione*. Puoi trovare l'ID della tua 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

AFTutilizza un sistema AWS CodeCommit di controllo della versione del codice sorgente (VCS) e ne consente altri CodeConnectionsche soddisfino i requisiti aziendali o l'architettura esistente.

Se esegui la distribuzione AFT per la prima volta e non disponi di un CodeCommit repository esistente, devi specificare un VCS provider esterno, come parte dei prerequisiti di AFT distribuzione. Per ulteriori informazioni, consulta Alternative per il controllo della versione del codice sorgente in. AFT

AFTsupporta le seguenti alternative di controllo del codice sorgente:

- GitHub
- GitHub Enterprise Server
- BitBucket

> **Note**
>
> Se lo specifichi AWS CodeCommit come tuoVCS, non sono necessari passaggi aggiuntivi. AFTcrea i `git` repository necessari nel tuo ambiente, con nomi predefiniti. Tuttavia, è possibile sostituire i nomi dei repository predefiniti per conformarsi CodeCommit, se necessario, agli standard organizzativi.

Imposta un sistema di controllo della versione del codice sorgente alternativo (personalizzato) con VCS AFT

Per configurare un sistema di controllo della versione del codice sorgente alternativo per la tua AFT distribuzione, segui questi passaggi.

Passaggio 1: Crea **`git`** repository in un sistema di controllo delle versioni di terze parti supportato (VCS).

Se non lo utilizzi AWS CodeCommit, devi creare `git` repository nell'ambiente di un provider di terze parti AFT supportato da un VCS provider di terze parti per i seguenti elementi.

- AFTrichieste di account. Codice di esempio disponibile. Per ulteriori informazioni sulle richieste di AFT account, vedereFornisci un nuovo account con AFT.
- AFTpersonalizzazioni del provisioning degli account. Codice di esempio disponibile. Per ulteriori informazioni sulle personalizzazioni AFT del provisioning degli account, consulta. Crea il tuo account AFT (provisioning customizations state machine)
- AFTpersonalizzazioni globali. Codice di esempio disponibile. Per ulteriori informazioni sulle personalizzazioni AFT globali, consultaPersonalizzazioni dell'account.
- AFTpersonalizzazioni dell'account. Codice di esempio disponibile. Per ulteriori informazioni sulle personalizzazioni AFT degli account, consultaPersonalizzazioni dell'account.

Fase 2: Specificare i parametri VCS di configurazione necessari per la distribuzione AFT

I seguenti parametri di input sono necessari per configurare il VCS provider come parte della AFT distribuzione.

- vcs_provider: se non lo utilizzi AWS CodeCommit, specifica il VCS provider come, o `"bitbucket"` `"github"``"githubenterprise"`, in base al tuo caso d'uso.
- github_enterprise_url: solo per i clienti Enterprise, specifica il. GitHub GitHub URL
- account_request_repo_name: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-request` In un ambiente di VCS provider AFT di terze parti supportato, aggiorna questo valore di input con il nome effettivo del repository. Per BitBucket Github ed GitHub Enterprise, il nome del repository deve avere il formato. `[Org]/[Repo]`
- account_customizations_repo_name: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-customizations` In un ambiente di VCS provider di terze parti AFT supportato, aggiorna questo valore di input con il nome del tuo repository. Per BitBucket Github ed GitHub Enterprise, il nome del repository deve avere il formato. `[Org]/[Repo]`
- account_provisioning_customizations_repo_name: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-account-provisioning-customizations` In un ambiente di provider di terze parti supportato, aggiorna questo valore di input con il nome del AFT tuo repository. VCS Per BitBucket Github ed GitHub Enterprise, il nome del repository deve avere il formato. `[Org]/[Repo]`
- global_customizations_repo_name: per gli utenti, questo valore è impostato su. AWS CodeCommit `aft-global-customizations` In un ambiente di VCS provider di terze parti AFT supportato, aggiorna questo valore di input con il nome del tuo repository. Per BitBucket Github ed GitHub Enterprise, il nome del repository deve avere il formato. `[Org]/[Repo]`
- account_request_repo_branch: il ramo è `main` predefinito, ma il valore può essere sovrascritto.

Per impostazione predefinita, le fonti provengono dal ramo di ogni repository. AFT `main` `git` È possibile sovrascrivere il valore del nome del ramo con un parametro di input aggiuntivo. Per ulteriori informazioni sui parametri di input, fate riferimento al README file nel AFTmodulo Terraform.

> **Per i clienti esistenti AWS CodeCommit**
>
> Se si crea un CodeCommit repository con un nuovo nome perAFT, è possibile aggiornare il nome del repository aggiornando i valori di questi parametri di input.

Passaggio 3: Completare la AWS CodeStar connessione per i provider di terze parti VCS

Quando la distribuzione viene eseguita, AFT crea i AWS CodeCommit repository richiesti oppure crea una AWS CodeStar connessione per il VCS provider di terze parti scelto. In quest'ultimo caso, è necessario accedere manualmente alla console dell'account di AFT gestione per completare la connessione in sospeso AWS CodeStar . Consulta la AWS CodeStar documentazione per ulteriori istruzioni su come completare la AWS CodeStar connessione.

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 e `git` così via.

Crittografia dei dati inattivi

AFT crea bucket Amazon S3, argomenti Amazon SNS, code Amazon SQS e database Amazon DynamoDB crittografati a riposo con chiavi del 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 richiama 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 archiviate 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 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 Amazon `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. AWSUtilizziamo 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 segnalazione:

- 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    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
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

- 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 gli ID delle richieste di personalizzazione. 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 AWS di 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

AWSControl Tower rileva automaticamente la deriva. Per rilevare la deriva, il `AWSControlTowerAdmin` ruolo richiede un accesso persistente all'account di gestione in modo che AWS Control Tower possa effettuare chiamate di sola lettura API verso. AWS Organizations Queste API chiamate vengono visualizzate come eventi. AWS CloudTrail

Drift viene visualizzato nelle notifiche di Amazon Simple Notification Service SNS (Amazon) aggregate nell'account di controllo. Le notifiche in ogni account membro inviano avvisi a un SNS argomento Amazon locale e a una funzione Lambda.

Per i controlli che fanno parte del AWS Security Hub Service-Managed Standard: AWS Control Tower, la deriva viene mostrata nelle pagine Account e Account dei dettagli dell'account nella console AWS Control Tower, nonché tramite una notifica Amazon. SNS

Gli amministratori degli account membri possono (e come best practice dovrebbero) iscriversi alle notifiche di SNS drift per account specifici. Ad esempio, l'`aws-controltower-AggregateSecurityNotifications`SNSargomento fornisce notifiche di deriva. La console AWS Control Tower indica agli amministratori degli account di gestione quando si è verificata una deriva. Per ulteriori informazioni sugli SNS argomenti 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 SNS notifica 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.

Esempi: lo scostamento e lo scostamento dell'account vengono gestiti nel modo SCP seguente

- Se modifichi lo stesso gestore SCP più volte, ricevi una notifica per la prima volta che lo modifichi.
- Se modifichi una deriva gestitaSCP, quindi correggi e poi la modifichi nuovamente, riceverai due notifiche.
- Se un account viene spostato OUs più volte tra la stessa origine e la stessa destinazione, senza prima correggere la deriva, viene inviata una sola notifica, anche se l'account è stato spostato da una destinazione all'altra più di una volta. OUs

Tipi di deviazione dell'account

- Account trasferito tra OUs
- 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

Tipi di deviazione delle politiche

- SCPaggiornato
- SCPallegato a OU
- SCPstaccato da OU
- SCPcollegato all'account

Per ulteriori informazioni, vedere Types of Governance Drift.

Risolvere la deriva

Mentre il rilevamento è automatico, la procedura per risolvere la deviazione deve essere eseguita tramite la console.

- Molti tipi di deriva possono essere risolti tramite la pagina delle impostazioni della zona di atterraggio. Puoi scegliere il pulsante Ripristina nella sezione Versioni per risolvere questi tipi di deriva.
- Se l'unità organizzativa ha meno di 1000 account, è possibile risolvere la deriva negli account forniti da Account Factory, o SCP drift, selezionando Registra nuovamente l'unità organizzativa nella pagina Organizzazione o nella pagina dei dettagli dell'unità organizzativa.
- È possibile risolvere il problema della deriva dell'account, ad esempio aggiornando un singolo Account membro spostato account. Per ulteriori informazioni, consulta Aggiorna l'account nella console.

⚠ 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 Reimposta e poi scegli Conferma, 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 sulle scansioni SCP

AWSControl Tower esegue SCPs quotidianamente una scansione del file gestito per verificare che i controlli corrispondenti siano applicati correttamente e che non abbiano subito variazioni. Per recuperarli SCPs ed eseguirne i controlli, AWS Control Tower chiama per tuo AWS Organizations conto, utilizzando un ruolo nel tuo account di gestione.

Se una scansione AWS del Control Tower rileva una deriva, riceverai una notifica. AWSControl 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 oggetto di deriva.

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 TPSlimite, velocità di limitazione o frequenza di API richiesta. Quando AWS Control Tower effettua una verifica SCPs chiamando AWS Organizations, le API chiamate effettuate da AWS Control Tower vengono conteggiate ai fini del TPS limite, poiché AWS Control Tower utilizza l'account di gestione per effettuare le chiamate.

In rare situazioni, questo limite può essere raggiunto chiamando la stessa persona APIs ripetutamente, tramite una soluzione di terze parti o uno script personalizzato scritto dall'utente. Ad esempio, se tu e AWS Control Tower chiamate nello AWS Organizations APIs stesso momento (entro 1 secondo) e TPS i limiti vengono raggiunti, le chiamate successive vengono limitate. Cioè, queste chiamate restituiscono un errore del tipo. `Rate exceeded`

Se viene superata una frequenza di API richiesta

- 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 SCP scansione giornaliera è composta da

1. Recupero dei dati attivi di recente. OUs
2. Per ogni unità organizzativa registrata, recuperando tutte le unità SCPs gestite da AWS Control Tower collegate all'unità organizzativa. SCPsI 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 gestiteSCPs.

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 del 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 controlla determinati AWS Identity and Access Management (IAM) ruoli quando accedi alla console per rilevare eventuali variazioni dei IAMruoli. 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, vedereAutorizzazioni necessarie per utilizzare la console AWS Control Tower.
- Non eliminare tutte le informazioni aggiuntiveOUs: se elimini l'unità organizzativa originariamente denominata Sandbox durante la configurazione della landing zone da parte di AWS Control Tower, la tua landing zone si troverà in uno stato di deriva, ma potrai comunque utilizzare AWS Control Tower. È necessaria almeno un'unità organizzativa aggiuntiva per AWS il funzionamento di Control Tower, ma non deve essere necessariamente l'unità organizzativa Sandbox.
- Non rimuovere gli account condivisi: se rimuovi gli account condivisi da FoundationalOUs, ad esempio rimuovendo l'account di registrazione dalla Security OU, la tua landing zone sarà in uno stato di deriva. La landing zone deve essere ripristinata prima di poter continuare a utilizzare la console AWS Control Tower.

Modifiche riparabili alle risorse

Di seguito è riportato un elenco delle modifiche consentite alle risorse AWS Control Tower, 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, vedere Managing Resources Outside of AWS Control Tower.

Modifiche consentite all'esterno della console AWS Control Tower

- Modifica il nome di un'unità organizzativa registrata.
- Modificare il nome dell'unità organizzativa di sicurezza.
- Cambia il nome degli account dei membri in Non-FoundationalOUs.

- Cambia il nome degli account condivisi di AWS Control Tower nell'unità organizzativa di sicurezza.
- Eliminare un'unità organizzativa non fondamentale.
- Eliminare un account registrato da un'unità organizzativa non fondamentale.
- Modifica l'indirizzo e-mail di un account condiviso nell'unità organizzativa di sicurezza.
- Modifica l'indirizzo e-mail di un account membro in un'unità organizzativa registrata.

> **Note**
>
> Lo spostamento di account da OUs un account all'altro è considerato una deriva e deve essere risolto.

Provisioning di nuovi account e deviazioni

Se la tua landing zone è in uno stato di deriva, la funzione di registrazione dell'account in AWS Control Tower non funzionerà. In tal caso, è necessario effettuare il provisioning di nuovi account tramite AWS Service Catalog. Per istruzioni, consulta Fornire account con AWS Service Catalog 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 deviazione dalla governance

La deriva della governance, chiamata anche deriva organizzativa OUsSCPs, si verifica quando gli account dei membri vengono modificati o aggiornati. I tipi di deriva della governance che possono essere rilevati in AWS Control Tower sono i seguenti:

- Account membro spostato
- Rimosso account membro
- Aggiornamento non pianificato a Managed SCP
- SCPAllegato all'account del membro
- SCPAllegato a Managed OU
- SCPDistaccato da Managed OU

- Foundational OU eliminata
- Deriva del controllo del Security Hub
- Accesso affidabile disabilitato

Un altro tipo di deriva è la deriva delle landing zone, che può essere trovata tramite l'account di gestione. La deriva dalla zona di atterraggio consiste nella deriva dei IAM ruoli o in qualsiasi tipo di deriva organizzativa che influisca in modo specifico sugli account Foundational e condivisi. OUs

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, consulta Non eliminare i ruoli richiesti nella sezione chiamata. Tipi di deriva da risolvere immediatamente

AWSControl Tower non cerca differenze rispetto ad altri servizi che funzionano con l'account di gestione CloudTrail CloudWatch, tra cui IAM Identity Center e così via. AWS CloudFormation AWS Config Negli account per bambini non è disponibile alcuna funzione di rilevamento delle deviazioni, in quanto tali account sono protetti da controlli preventivi obbligatori.

Tuttavia, segnala una deriva per quanto riguarda i controlli che fanno parte del AWS Security Hub Service-managed Standard: Control Tower AWS.

Account membro spostato

Questo tipo di deriva si verifica sull'account anziché sull'unità organizzativa. Questo tipo di deriva può verificarsi quando un account membro della AWS Control Tower, l'account di audit o l'account di archiviazione dei registri viene spostato da un'unità organizzativa AWS Control Tower registrata a qualsiasi altra unità organizzativa. Di seguito è riportato un esempio di SNS notifica Amazon 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:

- Vai alla pagina Organizzazione nella console AWS Control Tower, seleziona l'account e scegli 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 Registrati nuovamente per l'unità organizzativa che contiene l'account (l'opzione più veloce per più account). Per ulteriori informazioni, consulta Registra un'unità organizzativa esistente con AWS Control Tower.
- Aggiornamento del prodotto fornito in Account Factory. Per ulteriori informazioni, consulta Aggiorna e sposta gli account di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.

  > **Note**
  >
  > Se hai diversi account individuali da aggiornare, consulta anche questo metodo per effettuare aggiornamenti con uno script:Fornisci e aggiorna gli account utilizzando l'automazione.

- Quando si verifica questo tipo di deriva in un'unità organizzativa con più di 1000 account, la risoluzione della deriva può dipendere dal tipo di account spostato, come spiegato nei paragrafi successivi. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.
  - Se un account dotato di Account Factory viene spostato: in un'unità organizzativa con meno di 1000 account, puoi risolvere il problema aggiornando il prodotto di cui hai effettuato il provisioning in Account Factory, registrando nuovamente l'unità organizzativa o aggiornando la landing zone.

    In un'unità organizzativa con più di 1000 account, è necessario risolvere il problema aggiornando ogni account spostato, tramite la console AWS Control Tower o il prodotto fornito, poiché

la nuova registrazione dell'unità organizzativa non eseguirà l'aggiornamento. Per ulteriori informazioni, consulta Aggiorna e sposta gli account di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.

- Se viene spostato un account condiviso: puoi risolvere il problema derivante dallo spostamento dell'account di controllo o dell'archivio dei log aggiornando la landing zone. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.

> ⚠ Nome di campo obsoleto
>
> Il nome del campo `MasterAccountID` è stato modificato in conformità `ManagementAccountID` alle linee guida. AWS Il vecchio nome è obsoleto. A partire dal 2022, gli script che contengono il nome di campo obsoleto non funzioneranno più.

Rimosso account membro

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 SNS notifica Amazon 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 deriva in un account membro, puoi risolvere il problema 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 di fabbrica dell'account con AWS Control Tower o con AWS Service Catalog.

- Se un account condiviso viene rimosso da un'unità organizzativa Foundational, devi risolvere il problema reimpostando la landing zone. Finché questa deriva non sarà risolta, non sarà possibile utilizzare la console AWS Control Tower.
- Per ulteriori informazioni sulla risoluzione di drift per gli account eOUs, 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 `TAINTED` 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 Managed SCP

Questo tipo di deriva può verificarsi quando un controllo SCP for a viene aggiornato nella AWS Organizations console o programmaticamente utilizzando AWS CLI o uno dei. AWS SDKs Di seguito è riportato un esempio di SNS notifica Amazon 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, puoi risolverlo con:

- 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, risolvilo aggiornando la landing zone. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.

SCPAllegato a Managed OU

Questo tipo di deriva può verificarsi quando un controllo SCP per un è collegato a qualsiasi altra unità organizzativa. Questo evento è particolarmente comune quando si lavora OUs dall'esterno della console AWS Control Tower. Di seguito è riportato un esempio di SNS notifica Amazon 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 attached to 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-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_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, puoi risolverlo con:

- 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, risolvilo aggiornando la landing zone. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.

SCPDistaccato da Managed OU

Questo tipo di deriva può verificarsi quando un controllo SCP for a è stato scollegato da un'unità organizzativa gestita da AWS Control Tower. Questo evento è particolarmente comune quando si lavora dall'esterno della console AWS Control Tower. Di seguito è riportato un esempio di SNS notifica Amazon 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, puoi risolverlo con:

- 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, consultaAggiorna la tua landing zone.

Se si verifica questo tipo di deriva in un'unità organizzativa con più di 1000 account, risolvilo aggiornando la landing zone. Se la deriva influisce su un controllo obbligatorio, il processo di aggiornamento crea una nuova politica di controllo del servizio (SCP) e la collega all'unità organizzativa per risolvere la deriva. Per ulteriori informazioni su come aggiornare la landing zone, consultaAggiorna la tua landing zone.

SCPAllegato all'account del membro

Questo tipo di deriva può verificarsi quando un controllo SCP for a è collegato a un account nella console Organizations. Guardrail e i relativi SCPs possono essere attivati OUs (e quindi applicati a tutti gli account registrati di un'unità organizzativa) tramite la console AWS Control Tower. Di seguito è riportato un esempio di SNS notifica Amazon 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 attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

Risoluzione

Questo tipo di deriva si verifica sull'account anziché sull'unità organizzativa.

Quando si verifica questo tipo di deriva per gli account di un'unità organizzativa di base, come l'unità organizzativa di sicurezza, la soluzione è aggiornare la landing zone. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.

Quando si verifica questo tipo di deviazione in un'unità organizzativa non di base con un massimo di 1000 account, è possibile risolverlo nei seguenti modi:

- Scollegare la AWS Control Tower SCP dall'account di fabbrica dell'account.
- 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.

Quando si verifica questo tipo di deviazione in un'unità organizzativa con più di 1000 account, è possibile tentare di risolverlo aggiornando la configurazione di fabbrica dell'account per l'account. Potrebbe non essere possibile risolverlo correttamente. Per ulteriori informazioni, consulta Aggiorna la tua landing zone.

Foundational OU eliminata

Questo tipo di deriva si applica solo a AWS Control Tower FoundationalOUs, come Security OU. 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 la Foundational OU nella posizione originale. L'esempio seguente mostra una SNS notifica Amazon 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, AWS Control Tower viene aggiornato automaticamente.

Per ulteriori informazioni sulla risoluzione di drift per gli account eOUs, consulta. Se gestisci risorse al di fuori di AWS Control Tower

Deriva del controllo del Security Hub

Questo tipo di deriva si verifica quando un controllo che fa parte del AWS Security Hub Service-Managed Standard: AWS Control Tower segnala uno stato di deriva. Il AWS Security Hub servizio stesso non segnala uno stato di deriva per questi controlli. Invece, il servizio invia i risultati a AWS Control Tower.

La deriva di controllo del Security Hub può essere rilevata anche se AWS Control Tower non riceve un aggiornamento di stato da Security Hub da più di 24 ore. Se tali risultati non vengono ricevuti come previsto, AWS Control Tower verifica che il controllo sia alla deriva. L'esempio seguente mostra una SNS notifica Amazon 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" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

Risoluzione

Per OUs chi ha meno di 1000 account, la soluzione è registrare nuovamente l'unità organizzativa, che ripristina il controllo allo stato originale. Per qualsiasi unità organizzativa, è possibile rimuovere e riattivare il controllo tramite la console o la AWS Control TowerAPIs, 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 AWS della Control Tower. Si verifica quando si disabilita l'accesso affidabile alla AWS Control Tower AWS Organizations dopo aver configurato la AWS Control Tower landing zone.

Quando l'accesso affidabile è disabilitato, AWS Control Tower non riceve più eventi di modifica da AWS Organizations. AWSControl Tower si affida a questi eventi di modifica per rimanere sincronizzata. AWS Organizations Di conseguenza, AWS Control Tower potrebbe non rilevare modifiche organizzative negli account eOUs. Ecco perché è importante registrare nuovamente ogni unità organizzativa ogni volta che si aggiorna la landing zone.

Esempio: SNS notifica Amazon

Di seguito è riportato un esempio della SNS notifica Amazon che ricevi 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

AWSControl Tower ti avvisa quando si verifica questo tipo di deriva nella console AWS Control Tower. La soluzione è resettare la landing zone AWS della Control Tower. Per ulteriori informazioni, consulta Risolvere la 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 nuove unità organizzative e account 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 (OU) 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 (OU) 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 con AWS Organizations. Il flusso di lavoro Reset garantisce la coerenza tra i servizi per le unità organizzative fondamentali e aggiuntive. È possibile 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 delle unità organizzative 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 AWS Billing and Cost Management 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 sarà possibile eseguire alcuna azione nella console AWS Control Tower e non sarà possibile creare nuovi account AWS Service Catalog fino al completamento del ripristino.
- Non sarai in grado di 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. AWS Support

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 (SCP). Risultato: le risorse create da AWS Control Tower nell'account possono essere modificate o eliminate.
- L'account non è più associato all'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 di queste operazioni:
   - Accedi all'account condiviso che è stato rimosso, quindi vai a https://console.aws.amazon.com/organizations/home#/invites
   - 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. Verrà visualizzata 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. AWS Support

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#/invites 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. AWS Support

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 unità organizzative e 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 (OU) vuote utilizzando l'API o la console. Le unità organizzative che contengono account non possono essere eliminate.

AWS Control Tower riceve una notifica AWS Organizations quando un'unità organizzativa viene eliminata. Aggiorna l'elenco delle unità organizzative in Account Factory, in modo che l'elenco delle unità organizzative registrate rimanga coerente.

> **Note**
>
> Nel AWS Service Catalog, Account Factory viene aggiornato per rimuovere l'unità organizzativa eliminata dall'elenco delle unità organizzative disponibili 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 `TAINTED` e in uno stato di errore. Per eseguire la pulizia, passare a AWS Service Catalog, scegliere il prodotto di cui è stato eseguito il provisioning, quindi scegliere Terminate (Termina).

Gestisci organizzazioni e account con AWS Control Tower

Tutte le unità organizzative (OUs) e gli account creati in AWS Control Tower sono gestiti automaticamente da AWS Control Tower. Inoltre, se disponi di account esistenti OUs e 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. Iscrivi un esistente Account AWS

Terminologia

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

Visualizza i tuoi OUs e i tuoi account

Nella pagina AWS Control Tower Organization, puoi visualizzare tutto ciò OUs che è tuo AWS Organizations, compresi quelli registrati presso AWS Control Tower e quelli che non lo sono. OUs È possibile visualizzare in modalità annidata 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 iscrizione in AWS Control Tower. Un modo semplice per visualizzare gli 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 diOUs, 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 della AWS Control Tower. Per ulteriori informazioni sulla pagina Organizzazione, puoi vedere la guida video.

Procedura guidata: video

Questo video (4:01) descrive come utilizzare la pagina Organizzazione in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

Guida video su Come lavorare con la pagina dell'organizzazione in AWS Control Tower.

Argomenti

- Registra un'unità organizzativa esistente con AWS Control Tower
- Iscrivi un esistente Account AWS

Estendi la governance a un'organizzazione esistente

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

Ecco cosa aspettarsi quando si configura la landing zone AWS della Control Tower in un'organizzazione esistente.

- Puoi avere una landing zone per AWS Organizations organizzazione.
- AWSControl Tower utilizza l'account di gestione AWS Organizations dell'organizzazione esistente come account di gestione. Non è necessario un nuovo account di gestione.
- AWSControl 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 avviato la landing zone o registrato un'unità organizzativa, i controlli AWS della Control Tower si applicano automaticamente a tutti gli account registrati in quell'unità organizzativa.
- È possibile registrare altri AWS account esistenti in un'unità organizzativa gestita da AWS Control Tower, in modo che i controlli si applichino a tali account.
- Puoi aggiungerne altri OUs in AWS Control Tower e puoi registrare quelli esistentiOUs.

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

Ecco ulteriori dettagli su come i controlli della AWS Control Tower non si applicano alle OUs AWS organizzazioni che non dispongono di zone di atterraggio AWS della 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 e non registrati presso AWS Control Tower non sono vincolati dai controlli, a meno che non si registrino specificamente tali account in AWS Control Tower. OUs Per ulteriori informazioni sulla registrazione degli account, consulta Iscrivi un esistente Account AWS.
- Le organizzazioni esistenti aggiuntive, gli account esistenti e gli account nuovi OUs o creati dall'utente al di fuori di AWS Control Tower non sono vincolati dai controlli della AWS Control Tower, a meno che l'utente non registri separatamente l'unità organizzativa o registri l'account.

Per ulteriori informazioni su come applicare AWS Control Tower agli account OUs e agli account esistenti, vedereRegistra un'unità organizzativa esistente con AWS Control Tower.

Per una panoramica del processo di configurazione di una landing zone di 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 solution architect 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 AWS della Control Tower nelle 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 (IAMIdentity Center) è già configurato, la regione principale del AWS Control Tower deve essere la stessa dell'IAMIdentity Center.
- AWSControl Tower non elimina una configurazione esistente.
- Se IAM Identity Center è già abilitato e si utilizza IAM Identity Center Directory, AWS Control Tower aggiunge risorse come set di autorizzazioni, gruppi e così via, e procede come al solito.
- Se è configurata un'altra directory (esterna, AD, Managed AD), AWS Control Tower non modifica la configurazione esistente. Per ulteriori dettagli, consulta Considerazioni per i clienti AWS IAM Identity Center (IAM Identity Center).

Accesso ad altri AWS servizi

Dopo aver portato la tua organizzazione alla governance di AWS Control Tower, avrai ancora accesso a tutti AWS i servizi disponibili tramite AWS Organizations, tramite la AWS Organizations console eAPIs. Per ulteriori informazioni, consulta Servizi correlati AWS.

Unità organizzative annidate in AWS Control Tower

Questo capitolo elenca le aspettative e le considerazioni di cui devi essere consapevole quando lavori con unità organizzative annidate in AWS Control Tower. In molti modi, lavorare con unità organizzative annidate equivale a lavorare con una struttura di unità organizzative piatta. Le funzionalità Register e Re-register funzionano con le unità organizzative annidate, ad eccezione dei comportamenti modificati descritti in questo capitolo.

Procedura guidata: video

Questo video (4:46) descrive come gestire le distribuzioni di unità organizzative annidate in AWS Control Tower. Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

Guida video sulla gestione delle unità organizzative annidate in AWS Control Tower.

Per indicazioni sulle best practice per le unità organizzative annidate e le zone di atterraggio, consulta il post sul blog Organizing your AWS Control Tower landing zone with nested OU.

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. Tutti gli account dell'unità organizzativa annidata verranno registrati.
   - 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 delle unità organizzative annidate e dei relativi account membro, 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.

OU e ruoli annidati

AWS Control Tower distribuisce il `AWSControlTowerExecution` ruolo agli account all'interno dell'unità organizzativa di destinazione e agli account di tutte le unità organizzative annidate sotto l'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 abbia 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 le unità organizzative principali immediate, 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 delle unità organizzative e degli account annidati

Quando registri o registri nuovamente un'unità organizzativa annidata, AWS Control Tower registra tutti gli account non registrati dell'unità organizzativa di destinazione e aggiorna tutti gli account registrati. Ecco cosa aspettarsi.

AWS Control Tower 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 nelle relative unità organizzative annidate.
- 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).
- Le unità organizzative annidate devono essere registrate 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 organizzative più in alto nell'albero non siano state registrate correttamente in un determinato momento (alcune potrebbero essere state eliminate).
- È possibile registrare un'unità organizzativa che si trova sotto un'unità organizzativa superiore spostata, ma la deriva non viene riparata da tale azione.

Limitazioni dell'unità organizzativa annidata

- Le unità organizzative possono essere annidate a una profondità massima di 5 livelli sotto la radice.
- Le unità organizzative nidificate sotto l'unità organizzativa di destinazione devono essere registrate o registrate 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 sulle unità organizzative superiori vengono applicati automaticamente a questa unità organizzativa e a tutte le unità organizzative inferiori.

- Gli errori di registrazione delle unità organizzative non si propagano all'interno dell'albero gerarchico. È possibile visualizzare i dettagli sugli stati delle unità organizzative annidate nella pagina dei dettagli dell'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.

OU annidate e conformità

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

Considerazioni sulla conformità per le unità organizzative e gli account annidati

- La conformità di un'unità organizzativa non è determinata in base alla conformità delle unità organizzative annidate al suo interno.
- Lo stato di conformità di un controllo viene calcolato su tutte le unità organizzative su cui è abilitato il controllo, incluse le unità organizzative nidificate. Consulta lo stato di conformità di AWS Control Tower per le unità organizzative e gli account w.
- Un'unità organizzativa viene indicata come non conforme solo se ha account non conformi, indipendentemente dalla posizione dell'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 delle unità organizzative o degli account.

Unità organizzative annidate e deriva

In alcune situazioni, la deriva può impedire la registrazione delle unità organizzative annidate.

Aspettative relative alla deriva e alle unità organizzative annidate

- È possibile abilitare i controlli sulle unità organizzative con genitori alla deriva, ma non direttamente sulle unità organizzative che si trovano alla deriva.
- 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 nelle unità organizzative di primo livello. I controlli obbligatori vengono ignorati quando si registra un'unità organizzativa annidata.
- Un controllo obbligatorio protegge AWS Config le risorse; pertanto, per registrare le unità organizzative annidate, tale controllo deve avvenire in uno stato di non deriva. In caso di deviazione, AWS Control Tower blocca la registrazione delle unità organizzative annidate.
- 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.

Unità organizzative e controlli annidati

Quando si abilita un controllo su un'unità organizzativa registrata, i controlli preventivi e investigativi hanno comportamenti diversi. Per le unità organizzative annidate, i controlli proattivi si comportano in modo simile ai controlli investigativi.

Controlli preventivi

- I controlli preventivi vengono applicati alle unità organizzative annidate.
- I controlli preventivi obbligatori vengono applicati a tutti gli account dell'unità organizzativa e delle relative unità organizzative annidate.
- I controlli preventivi riguardano tutti gli account e le unità organizzative annidati nell'unità organizzativa di destinazione, anche se tali account e unità organizzative non sono registrati.

Controlli investigativi e proattivi

- Le unità organizzative annidate non ereditano automaticamente i controlli 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 altre unità organizzative.
- Lo stato Fallito indica che il controllo non è applicato su questa unità organizzativa, indipendentemente dallo stato in altre unità organizzative.

> **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.

Le unità organizzative annidate e la 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 le unità organizzative. Nel contesto delle unità organizzative nidificate, è il nodo in cui sono annidate tutte le altre unità organizzative.

Registra un'unità organizzativa esistente con AWS Control Tower

Un modo efficace per portare più AWS account esistenti in AWS Control Tower consiste nell'estendere la governance tramite AWS Control Tower a un'intera unità organizzativa (OU).

Per abilitare la governance della AWS Control Tower su un'unità organizzativa esistente creata con AWS Organizations e i relativi account, registra l'unità organizzativa nella landing zone AWS della Control Tower. È possibile registrare account OUs contenenti 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 membri vengono registrati nella landing zone di AWS Control Tower. Sono regolati dai controlli che si applicano alle rispettive unità organizzative.

> **Note**
>
> Se non disponi già di una landing zone della 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, consultaGuida introduttiva a AWS Control Tower.

Cosa succede ai miei account quando registro la mia unità organizzativa?

AWSControl Tower richiede l'autorizzazione per stabilire un accesso affidabile tra AWS CloudFormation e AWS Organizations per conto dell'utente, in modo da AWS CloudFormation poter distribuire automaticamente lo stack sugli account dell'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.

IAMprerequisiti utente per la registrazione di un'unità organizzativa

La tua AWS Identity and Access Management (IAM) identità (utente o ruolo) o l'IAMidentità utente di 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'IAMutente o sull'IAMidentità dell'utente Identity Center durante la registrazione di un'unità organizzativa.

Il portafoglio rilevante è quello creato da AWS Control Tower, chiamato AWSControl Tower Account Factory Portfolio. Accedete ad esso selezionando Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. Seleziona quindi la scheda denominata Gruppi, ruoli e utenti per visualizzare la tua IAM identità IAM o quella dell'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

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 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.

Risultati della registrazione di un'unità organizzativa esistente

Dopo aver registrato un'unità organizzativa esistente, il `AWSControlTowerExecution` ruolo consente a 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 tramite l'account di audit AWS Control Tower.
- `AWSControlTowerExecution`ti 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 della Control Tower selezionati si applichino automaticamente a ogni singolo account del tuo OUs account e a ogni nuovo account che crei in AWS Control Tower.

Per un'unità organizzativa registrata, è possibile fornire report di conformità e sicurezza basati sulle funzionalità di controllo e registrazione incorporate nei controlli Control TowerAWS. 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, vedere. 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 è stato creato un account in un'unità organizzativa registrata e successivamente lo si sposta in un'altra unità organizzativa non registrata, in particolare se si utilizza AWS Organizations per spostare l'account, nella pagina dei dettagli dell'unità organizzativa viene visualizzato il risultato «1 di 0» account. 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. Scegli 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 annidateOUs, 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, vedereUnità organizzative annidate in AWS Control Tower.

Cause comuni di errore durante la registrazione o la nuova registrazione

In generale, quando si registra o si registra 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 AWS della Control Tower. Se hai SCPs più di quanto consentito dalla quota, devi eliminare o combinare ilSCPs.

- Conflittente SCPs

  L'account esistente SCPs può essere applicato all'unità organizzativa o all'account, il che impedisce a AWS Control Tower di registrare l'account. Controlla la politica applicata SCPs per eventuali politiche che potrebbero impedire AWS il funzionamento di Control Tower. Assicurati di controllare quelle ereditate dai OUs livelli più alti 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 CloudFormationnella Guida per l'utente di AWS CloudFormation .

- Supera il limite dell'account

  AWSControl Tower limita ogni unità organizzativa a 1000 account durante la registrazione.

Errori dell'account

- Controlli preliminari impediti sugli account

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

- 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.

- STSdisabilitato

  AWS Security Token Service (AWS STS) può essere disabilitato nell'account. AWS STSgli endpoint devono essere attivati negli account di tutte le regioni supportate da AWS Control Tower.

- IAMConflitto tra Identity Center

  La regione principale di AWS Control Tower non è la stessa della regione AWS IAM Identity Center (IAMIdentity Center). Se IAM Identity Center è già configurato, la regione principale di AWS Control Tower deve essere la stessa dell'IAMIdentity Center.

- Argomento in conflitto SNS

  L'account ha un nome tematico Amazon Simple Notification Service (AmazonSNS) che AWS Control Tower deve utilizzare. AWSControl Tower crea risorse (come SNS argomenti) con nomi specifici. Se questi nomi sono già utilizzati, l'installazione AWS del 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.

- IAMutente non presente 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 IAM ruolo 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 a Control TowerAWS. Se CloudTrail è abilitata su un account precedente alla registrazione,

potresti riscontrare una doppia fatturazione a meno che non la 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 nel registrare nuovamente l'unità organizzativa.

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.
- Se hai più di un'unità organizzativa registrata nella tua landing zone, registra nuovamente 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. Per informazioni, consulta Aggiorna l'account nella console.

Aggiorna più account nella stessa unità organizzativa

Ripeti questi passaggi per ogni unità organizzativa dell'organizzazione AWS Control Tower, se devi aggiornare tutti i tuoi account eOUs.

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 del riquadro a sinistra, scegli Organizzazione.
3. Nella pagina Organizzazione, scegli un'unità organizzativa qualsiasi per visualizzare la pagina dei dettagli dell'unità organizzativa.
4. In Azioni in alto a destra, seleziona Registra nuovamente l'unità organizzativa.

In alternativa, puoi selezionare qualsiasi account con lo stato Aggiornamento disponibile 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 a 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 si registra nuovamente l'unità organizzativa, il **`AWSControlTowerExecution`** ruolo viene aggiunto a tutti gli account con lo stato Non registrato o Registrazione non riuscita.
- AWSControl Tower crea un accesso Single Sign-on (IAMIdentity Center) per i nuovi account registrati.
- Gli account registrati vengono registrati nuovamente in Control TowerAWS.
- 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 Iscrivi un esistente Account AWS.

> **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 -. AWSControlTowerExecutionRole Questa operazione StackSet nell'account di gestione può fallire perché il AWSControlTowerExecutionIAMruolo 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

È possibile aggiornare i 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, consultaAggiorna 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 Aggiorna il prodotto fornito 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

- Implementa ambienti con AWS 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
- Fornisci account tramite AWS Service Catalog
- Tieni traccia degli avvisi tramite Amazon Simple Notification Service
- Crea applicazioni distribuite con AWS Step Functions

Implementa ambienti con AWS CloudFormation

AWS 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 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 AWS CloudFormation stackset per applicare i controlli sugli account. Per ulteriori informazioni sulla collaborazione tra AWS Control Tower AWS 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 chiamato le AWS API per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state effettuate le chiamate e l'ora in cui sono avvenute le chiamate. È possibile effettuare l' CloudTrail integrazione 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 l'accesso. Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

Monitora risorse e servizi con CloudWatch

Amazon CloudWatch offre una soluzione di monitoraggio affidabile, scalabile e flessibile che puoi iniziare a utilizzare in pochi minuti. Non sarà più necessario configurare, gestire e ridimensionare sistemi di monitoraggio propri e relativa infrastruttura. Per ulteriori informazioni, consulta 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 relative 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 di`managed-by-control-tower`.

Per ulteriori informazioni su come AWS Config monitora e registra le risorse in AWS Control Tower e su come vengono fatturate, consulta. Monitora le modifiche alle risorse con AWS Config

AWS Control Tower utilizza Regole di AWS Config per implementare controlli investigativi. Per ulteriori informazioni, consulta Informazioni sui controlli in AWS Control Tower.

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) ti consente di creare e controllare chiavi che proteggono i tuoi 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 effettuare il provisioning o gestire i 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 vengono raggruppati in gruppi logici, denominati unità organizzative. Per ulteriori informazioni su Organizations, consulta la AWS Organizations User Guide.

AWS Control Tower utilizza le seguenti unità organizzative:

- Root: il contenitore principale per tutti gli account e tutte le altre unità organizzative presenti 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. Questa unità organizzativa e le altre unità organizzative per bambini presenti nella tua landing zone contengono i tuoi account utente. Questi sono gli account a cui gli utenti finali accedono per eseguire operazioni sulle AWS risorse.

> **Note**
>
> Puoi aggiungere unità organizzative aggiuntive nella tua landing zone tramite la console AWS Control Tower nella pagina Unità organizzative.

Considerazioni

Le unità organizzative create tramite AWS Control Tower possono avere dei controlli applicati. Le unità organizzative create al di fuori di AWS Control Tower non possono, per impostazione predefinita. Tuttavia, è possibile registrare tali unità organizzative. 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 Registrare un'unità organizzativa esistente con AWS Control Tower.

Archivia oggetti con Amazon S3

Amazon Simple Storage Service (Amazon S3) è un servizio di storage su Internet. È possibile utilizzare Amazon S3 per memorizzare e recuperare qualsiasi volume di dati, in qualunque momento e da qualunque luogo tramite il Web. Queste operazioni possono essere eseguite tramite l'interfaccia Web semplice e intuitiva della AWS Management Console. 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

AWS Control Tower è integrato con AWS Security Hub tramite lo standard Security Hub chiamato 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 denominati «blueprint personalizzati». Per ulteriori informazioni, consulta Step2. Crea il AWS Service Catalog prodotto.

AWS Control Tower può anche utilizzare le API Service Catalog per automatizzare ulteriormente il provisioning e l'aggiornamento degli account. Per i dettagli, consulta la Developer Guide. AWS Service Catalog

Passaggio 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 ha effetto 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, restituisci 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 AWS CloudFormationo 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.

Tieni traccia degli avvisi tramite Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) è un servizio Web che consente alle applicazioni, agli utenti finali e ai dispositivi di inviare e ricevere notifiche istantaneamente dal cloud. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

AWS Control Tower utilizza Amazon SNS per inviare avvisi programmatici agli indirizzi e-mail del tuo account di gestione e del tuo account di controllo. Questi avvisi ti aiutano a prevenire la deriva all'interno della tua 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 in una serie di passaggi in un flusso di lavoro visivo. Si possono creare ed eseguire stati macchina che permettono di eseguire le fasi dell'applicazione in modo affidabile e scalabile. Per ulteriori informazioni, consulta la AWS Step Functions Guida per sviluppatori.

Gestione delle identità e degli accessi in AWS Control Tower

Per eseguire qualsiasi operazione nella tua landing zone, come il provisioning degli account in Account Factory o la creazione di nuove unità organizzative (OUs) nella console AWS Control Tower, AWS Identity and Access Management (IAM) o AWS IAM Identity Center richiederti di autenticare che sei un utente approvato AWS utente. Ad esempio, se utilizzi la console AWS Control Tower, autentichi la tua identità fornendo AWS credenziali, fornite dall'amministratore.

Dopo aver autenticato la tua identità, IAM controlla il tuo accesso a AWS con un insieme definito di autorizzazioni su un insieme specifico di operazioni e risorse. Se sei un amministratore di account, puoi IAM utilizzarlo per controllare l'accesso di altri IAM utenti alle risorse associate al tuo account.

Argomenti

Autenticazione

Hai accesso a AWS come uno dei seguenti tipi di identità:

- AWS account root user — Quando si crea per la prima volta un AWS account, si inizia con un'identità che ha accesso completo a tutti AWS servizi e risorse presenti nell'account. Questa identità è denominata AWS utente root dell'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 o IAM utente di IAM Identity Center (scelta consigliata) (non è una procedura consigliata nella maggior parte dei casi d'uso). Quindi conservare al sicuro le credenziali dell'utente root e utilizzarle per eseguire solo alcune attività di gestione dell'account e del servizio. Per ulteriori informazioni, consulta Quando accedere come utente root.

- IAMutente: un IAMutente è un'identità all'interno dell'utente AWS account con autorizzazioni specifiche e personalizzate. È possibile utilizzare le credenziali IAM utente per accedere in modo sicuro AWS pagine web come AWS Console di gestione, AWS Forum di discussione o AWS Centro di supporto. AWS le migliori pratiche consigliano di creare un utente di IAM Identity Center anziché un IAM utente, poiché il rischio per la sicurezza aumenta quando si crea un IAM utente con credenziali a lungo termine.

  Se è necessario creare un IAM utente per un determinato scopo, oltre alle credenziali di accesso, è possibile generare chiavi di accesso per ogni utente. IAM È possibile utilizzare questi tasti quando si chiama AWS servizi a livello di codice, tramite uno dei tanti SDKs o utilizzando il AWS Interfaccia a riga di comando ()CLI. CLIGli strumenti SDK and utilizzano le chiavi di accesso per firmare crittograficamente la richiesta. Se non lo usi AWS strumenti, devi firmare tu stesso la richiesta. AWSControl Tower supporta Signature Version 4, un protocollo per l'autenticazione delle richieste in entrataAPI. Per ulteriori informazioni sull'autenticazione delle richieste, consulta la sezione Processo di firma della versione 4 di Signature nel AWS Riferimento generale.
- IAMruolo: un IAMruolo è un'IAMidentità che puoi creare nel tuo account con autorizzazioni specifiche. Un IAM ruolo è simile a un IAM utente in quanto è un AWS identità e dispone di politiche di autorizzazione che determinano ciò che l'identità può e non può fare in AWS. Tuttavia, anziché essere associato esclusivamente a una persona, un ruolo è pensato per essere assunto da chiunque ne abbia bisogno. 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. IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:
  - Accesso utente federato: anziché creare un IAM utente, è possibile utilizzare identità esistenti da AWS Directory Service, la tua rubrica utenti aziendale o un provider di identità web. Questi sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando l'accesso viene richiesto tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta Federated Users and Roles nella Guida per l'utente. IAM
  - AWS accesso al servizio: un ruolo di servizio è un IAM ruolo che un servizio assume per eseguire azioni sull'account dell'utente per conto dell'utente. Quando ne configuri alcuni AWS ambienti di servizio, è necessario definire un ruolo che il servizio deve assumere. Questo ruolo di servizio deve includere tutte le autorizzazioni necessarie affinché il servizio possa accedere a 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. È possibile creare, modificare

ed eliminare un ruolo di servizio dall'internoIAM. 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, vedere Creazione di un ruolo per delegare le autorizzazioni a un AWS Servizio nella Guida per l'IAMutente.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza Amazon e in fase di creazione AWS CLIoppure AWS APIrichieste. È preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza Amazon. Per assegnare un AWS assegna il ruolo a un'EC2istanza Amazon e la rendi disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza Amazon di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

- IAML'autenticazione degli utenti di IAM Identity Center al portale utenti di Identity Center è controllata dalla directory che hai collegato a IAM Identity Center. Tuttavia, l'autorizzazione al AWS gli account disponibili per gli utenti finali all'interno del portale utenti sono determinati da due fattori:
  - A chi è stato assegnato l'accesso a tali AWS conti in AWS IAMconsole Identity Center. Per ulteriori informazioni, consulta Single Sign-On Access nel AWS IAM Identity Center Guida per l'utente.
  - Quale livello di autorizzazioni è stato concesso agli utenti finali nel AWS IAMConsole Identity Center per consentire loro l'accesso appropriato a tali AWS conti. Per ulteriori informazioni, vedere Set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.

Controllo accessi

Per creare, aggiornare, eliminare o elencare risorse AWS Control Tower o altro AWS per le risorse presenti nella tua landing zone ti servono 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 sulla 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. IAMGuida all'Identity Center

Per un breve tutorial su come configurare gli utenti e le autorizzazioni del tuo IAM Identity Center in AWS Control Tower, puoi guardare questo video (6:23). Per una migliore visualizzazione, seleziona l'icona nell'angolo in basso a destra del video per ingrandirlo a schermo intero. È disponibile la didascalia.

Guida video alla configurazione di AWS IAM Identity Center in AWS Control Tower.

Informazioni sulla configurazione di AWS Control Tower con IAM Identity Center

Quando configuri inizialmente AWS Control Tower, solo l'utente root e tutti gli utenti IAM con le autorizzazioni corrette possono aggiungere utenti IAM Identity Center. Tuttavia, dopo che gli utenti finali sono stati aggiunti al AWSAccountFactorygruppo, possono creare nuovi utenti IAM Identity Center dalla procedura guidata Account Factory. Per ulteriori informazioni, consulta 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 corrispondo agli utenti in gruppi all'interno degli account. I seguenti gruppi vengono creati quando configuri la landing zone.

AWSAccountFactory

Account	Set di autorizzazioni	Descrizione
Gestione dell'account	AWSServiceCatalogEndUserAccess	Questo gruppo viene utilizzato in questo account solo per fornire nuovi account utilizzando Account Factory.

AWSServiceCatalogAdmins

Account	Set di autorizzazioni	Descrizione
Gestione dell'account	AWSServiceCatalogAdminFullAccess	Questo gruppo viene utilizzato solo in questo account per apportare modifiche amministr

Account	Set di autorizzazioni	Descrizione
		ative a Account Factory. Gli utenti di questo gruppo non possono fornire nuovi account a meno che non facciano parte anche loro del AWSAccountFactorygruppo.

AWSControlTowerAdmins

Account	Set di autorizzazioni	Descrizione
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 archivio dei log	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.
Account di audit	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.
Account membri	AWSOrganizationsFullAccess	Gli utenti hanno pieno accesso a Organizations in questo account.

AWSSecurityAuditPowerUsers

Account	Set di autorizzazioni	Descrizione
Gestione dell'account	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportan

Account	Set di autorizzazioni	Descrizione
		o lo sviluppo AWS consapevole delle applicazioni.
Account di archivio dei log	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 di audit	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo di applicazioni AWS consapevoli.
Account membri	AWSPowerUserAccess	Gli utenti possono eseguire attività di sviluppo di applicazioni e creare e configurare risorse e servizi che supportano lo sviluppo di applicazioni AWS consapevoli.

AWSSecurityAuditors

Account	Set di autorizzazioni	Descrizione
Gestione dell'account	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.
Account di archivio dei log	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS

Account	Set di autorizzazioni	Descrizione
		servizi e le risorse di questo account.
Account di audit	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.
Account membri	AWSReadOnlyAccess	Gli utenti hanno accesso in sola lettura a tutti i AWS servizi e le risorse di questo account.

AWSLogArchiveAdmins

Account	Set di autorizzazioni	Descrizione
Account di archivio dei log	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.

AWSLogArchiveViewers

Account	Set di autorizzazioni	Descrizione
Account di archivio 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	Descrizione
Account di audit	AWSAdministratorAccess	Gli utenti avranno accesso amministratore in questo account.

Panoramica sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower

Ogni AWS la risorsa è di proprietà di un Account AWS e le autorizzazioni per creare o accedere a una risorsa sono regolate dalle politiche di autorizzazione. Un amministratore di account può associare criteri di autorizzazione alle IAM identità (ovvero utenti, gruppi e ruoli). Alcuni servizi (come 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 IAMBest Practices nella Guida per l'IAMutente.

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 le autorizzazioni e delle azioni specifiche che devono essere consentite per il funzionamento di tali risorse.

Argomenti

- AWSRisorse e operazioni Control Tower
- Informazioni sulla proprietà delle risorse
- Gestisci l'accesso alle risorse
- Specificare gli elementi della politica: azioni, effetti e principi
- Specifica delle condizioni in una policy

AWSRisorse e operazioni Control Tower

In AWS Control Tower, la risorsa principale è una landing zone. AWSControl 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.

Risorse e sottorisorse in AWS sono associati ad Amazon Resource Names (ARNs) univoci, come illustrato nell'esempio seguente.

AWSControl Tower fornisce una serie di API operazioni per lavorare con le risorse AWS Control Tower. Per un elenco delle operazioni disponibili, vedi AWS Control Tower the AWS Control Tower API Reference.

Per ulteriori informazioni su AWS CloudFormation risorse in AWS Control Tower, vedi il AWS CloudFormation Guida per l'utente.

Informazioni sulla proprietà delle risorse

Il AWS l'account possiede le risorse create nell'account, indipendentemente da chi ha creato le risorse. In particolare, il proprietario della risorsa è AWS conto dell'entità principale (vale a dire, il Account AWS utente root, un utente di IAM Identity Center, un IAM utente o un IAM ruolo) che autentica la richiesta di creazione delle risorse. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi il plugin AWS credenziali utente root dell'account AWS account per configurare una landing zone, il tuo AWS account è il proprietario della risorsa.
- Se crei un IAM utente 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 l'account, a cui appartiene l'utente, possiede la risorsa landing zone.
- Se crei un IAM ruolo nel tuo AWS Se si dispone dei permessi necessari per configurare una landing zone, chiunque possa assumere il ruolo può configurare una landing zone. Il tuo AWS l'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 IAM nel contesto di AWS Control Tower. Non fornisce informazioni dettagliate sul IAM servizio. Per la IAM documentazione completa, vedi Cos'èIAM? nella Guida IAM per l'utente. Per informazioni sulla sintassi e le descrizioni delle IAM policy, vedere AWS IAMRiferimento alle politiche nella Guida per l'IAMutente.

Le politiche associate a un'IAMidentità sono denominate politiche basate sull'identità (politiche)IAM. Le policy collegate a una risorsa vengono definite policy basate sulle risorse.

> **Note**
>
> AWSControl Tower supporta solo policy (policy) IAM basate sull'identità.

Argomenti

- Informazioni sulle politiche (politiche) basate sull'identità IAM
- Crea ruoli e assegna autorizzazioni
- Policy basate su risorse

Informazioni sulle politiche (politiche) basate sull'identità IAM

È possibile allegare politiche alle identità. IAM Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo nel tuo account: per concedere a un utente le autorizzazioni per creare una risorsa AWS Control Tower, come la configurazione di una landing zone, puoi allegare una politica di autorizzazioni a un utente o gruppo a cui appartiene l'utente.
- Associare una politica di autorizzazioni a un ruolo (concedere autorizzazioni per più account): puoi allegare una politica di autorizzazioni basata sull'identità a un ruolo per concedere autorizzazioni su più account. IAM Ad esempio, un amministratore per uno AWS account (Account A) può creare un

ruolo che concede autorizzazioni multiaccount a un altro account AWS account (Account B) oppure l'amministratore può creare un ruolo che concede le autorizzazioni a un altro AWS servizio.

1. L'amministratore dell'Account A crea un IAM ruolo 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 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 ti danno accesso alle risorse, in AWS Control Tower e in altri AWS servizi, incluso l'accesso programmatico alle risorse.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate in Creare un set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.
- Utenti gestiti IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate in Creazione di un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente.
- IAMutenti:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella sezione Creazione di un ruolo per un IAM utente nella Guida per l'IAMutente.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate in Aggiungere autorizzazioni a un utente (console) nella Guida per l'IAMutente.

Per ulteriori informazioni sull'utilizzo per IAM delegare le autorizzazioni, consulta Gestione degli accessi nella Guida per l'IAMutente.

> **Note**
>
> Quando configuri una landing zone di AWS Control Tower, avrai bisogno di un utente o di un ruolo con la policy AdministratorAccessgestita. (arn:aws:iam: :aws:policy/) AdministratorAccess

Creare un ruolo per un Servizio AWS (IAMconsole)

1. Accedi a AWS Management Console e apri la IAM console all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione della IAM console, scegli Ruoli, quindi scegli Crea ruolo.
3. Per il tipo di entità attendibile, scegli 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 in modo da includere la policy di attendibilità richiesta dal servizio.
5. Scegli Next (Successivo).
6. Per i criteri di autorizzazione, le opzioni dipendono dal caso d'uso selezionato:
   - Se il servizio definisce le autorizzazioni per il ruolo, non è possibile selezionare le politiche di autorizzazione.
   - Seleziona da un set limitato di politiche di autorizzazione.
   - Seleziona tra tutte le politiche di autorizzazione.
   - Seleziona nessuna politica di autorizzazione, crea le politiche dopo la creazione del ruolo e quindi associa le politiche al ruolo.
7. (Facoltativo) Impostare un limite delle autorizzazioni. Questa è una caratteristica avanzata disponibile per i ruoli di servizio, ma non per i ruoli collegati ai servizi.
   a. Apri la sezione Imposta i limiti delle autorizzazioni, quindi scegli Usa un limite di autorizzazioni per controllare il numero massimo di autorizzazioni per il ruolo.

      IAMinclude un elenco di AWS politiche 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 Role name, le opzioni dipendono dal servizio:
   - Se il servizio definisce il nome del ruolo, non è possibile modificare il nome del ruolo.

- Se il servizio definisce un prefisso per il nome del ruolo, è possibile inserire un suffisso opzionale.
- Se il servizio non definisce il nome del ruolo, puoi assegnare un nome al ruolo.

> **Important**
>
> Quando assegnate un nome a un ruolo, tenete presente quanto segue:
>
> - I nomi dei ruoli devono essere univoci all'interno del Account AWS e non possono essere resi unici per caso.
>
> Ad esempio, non creare ruoli denominati entrambi **`PRODROLE`** e**`prodrole`**. Quando un nome di ruolo viene utilizzato in una policy o come parte di unaARN, il nome del ruolo fa distinzione tra maiuscole e minuscole, tuttavia quando un nome di ruolo viene visualizzato dai 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 la sua creazione perché altre entità potrebbero 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, nelle sezioni Passo 1: Seleziona entità attendibili o Passaggio 2: Aggiungi autorizzazioni, scegli Modifica.
12. (Facoltativo) Per facilitare l'identificazione, l'organizzazione o la ricerca del ruolo, aggiungi tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo dei tag inIAM, consulta Etichettare IAM le risorse nella Guida per l'IAMutente.
13. Verificare il ruolo e quindi scegliere Create role (Crea ruolo).

Per utilizzare l'editor delle JSON politiche per creare una politica

1. Accedi al AWS Management Console e apri la IAM console 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 Policy editor, scegli l'JSONopzione.

5. Inserisci o incolla un documento JSON di policy. Per i dettagli sul linguaggio delle IAM politiche, consulta il riferimento alle IAM JSON politiche.
6. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la convalida delle policy, quindi scegli Next (Successivo).

   > **Note**
   >
   > Puoi passare tra le opzioni Visual e JSONEditor in qualsiasi momento. Tuttavia, se apporti modifiche o scegli Avanti nell'editor visuale, IAM potresti ristrutturare la tua politica per ottimizzarla per l'editor visuale. Per ulteriori informazioni, consulta la sezione Ristrutturazione delle politiche nella Guida per l'IAMutente.

7. (Facoltativo) Quando si crea o si modifica una politica nel AWS Management Console, è possibile generare un modello di YAML policy JSON o da utilizzare in AWS CloudFormation modelli.

   A tale scopo, nell'editor delle politiche scegli Azioni, quindi scegli Genera CloudFormation modello. Per ulteriori informazioni su AWS CloudFormation, vedi AWS Identity and Access Management riferimento al tipo di risorsa in AWS CloudFormation Guida 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 inIAM, consulta Taggare IAM le risorse nella Guida per l'IAMutente.
11. Seleziona Crea policy per salvare la nuova policy.

Per utilizzare l'editor visivo per creare una policy.

1. Accedi al AWS Management Console e apri la IAM console 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 Create Policy (Crea policy).
4. Nella sezione Policy editor, individua la sezione Seleziona un servizio, quindi scegli un Servizio AWS. Puoi utilizzare la casella di ricerca in alto per limitare i risultati nell'elenco dei 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 IAMnega per impostazione predefinita, come procedura consigliata per la sicurezza consigliamo di concedere le autorizzazioni solo alle azioni e alle risorse di cui un utente ha bisogno. Crea un'JSONistruzione per negare le autorizzazioni solo se desideri sostituire un'autorizzazione concessa separatamente da un'altra dichiarazione o politica. Si consiglia di limitare al minimo il numero di autorizzazioni di rifiuto perché possono aumentare la difficoltà di risoluzione dei problemi relative alle autorizzazioni.
6. Per Risorse, se il servizio e le azioni selezionati nei passaggi precedenti non supportano la scelta di risorse specifiche, tutte le risorse sono consentite e non è possibile modificare questa sezione.

   Se si selezionano una o più operazioni che supportano le autorizzazioni a livello di risorsa, l'editor visivo elenca tali risorse. È possibile selezionare Risorse per specificare le risorse per la policy.

   È possibile specificare le risorse nei seguenti modi:

   - Scegli Aggiungi ARNs per specificare le risorse in base ai loro nomi di risorse Amazon (ARN). Puoi utilizzare l'ARNeditor visivo o l'elenco ARNs manualmente. Per ulteriori informazioni sulla

ARN sintassi, consulta Amazon Resource Names (ARNs) nella Guida per l'IAMutente. Per informazioni sull'utilizzo ARNs nell'`Resource`elemento di una policy, consulta IAMJSONPolicy elements: Resource in the IAMUser 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 JSON politica. Ad esempio, puoi specificare che un utente può eseguire le operazioni sulle risorse solo quando la richiesta dell'utente viene effettuata entro un determinato intervallo di tempo. Puoi anche utilizzare condizioni di uso comune per limitare se un utente deve essere autenticato utilizzando un dispositivo di autenticazione a più fattori (MFA). In alternativa, è possibile richiedere che la richiesta provenga da un determinato intervallo di indirizzi IP. Per un elenco di tutte le chiavi di contesto che è possibile utilizzare in una condizione di policy, consulta Azioni, risorse e chiavi di condizione per AWS 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 Condizione, vedere Elementi IAM JSON della politica: Condizione nella Guida per l'IAMutente.

8. Per aggiungere più blocchi di autorizzazioni, seleziona Aggiungi ulteriori autorizzazioni. Per ogni blocco, ripetere le fasi da 2 a 5.

> **Note**
>
> È possibile passare tra le opzioni Visual e JSONEditor in qualsiasi momento. Tuttavia, se apporti modifiche o scegli Avanti nell'editor visuale, IAM potresti ristrutturare la tua politica per ottimizzarla per l'editor visuale. Per ulteriori informazioni, consulta la sezione Ristrutturazione delle politiche nella Guida per l'IAMutente.

9. (Facoltativo) Quando si crea o si modifica una politica nel AWS Management Console, è possibile generare un modello di YAML policy JSON o da utilizzare in AWS CloudFormation modelli.

   A tale scopo, nell'editor delle politiche scegli Azioni, quindi scegli Genera CloudFormation modello. Per ulteriori informazioni su AWS CloudFormation, vedi AWS Identity and Access Management riferimento al tipo di risorsa in AWS CloudFormation Guida 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 inIAM, consulta Taggare IAM le risorse nella Guida per l'IAMutente.
13. Seleziona Crea policy per salvare la nuova policy.

Per concedere l'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con AWS al di fuori del AWS Management Console. 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
Identità della forza lavoro	Utilizza credenziali temporane e per firmare le richieste	Segui le istruzioni per l'interfa ccia che desideri utilizzare.

Quale utente necessita dell'accesso programmatico?	Per	Come
(Utenti gestiti in IAM Identity Center)	programmatiche a AWS CLI, AWS SDKs, oppure AWS APIs.	• Per il AWS CLI, vedere Configurazione di AWS CLI da usare AWS IAM Identity Center nella AWS Command Line Interface Guida per l'utente. • In AWS SDKs, strumenti e AWS APIs, vedi Autenticazione in IAM Identity Center nella AWS SDKse Guida di riferimento agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche a AWS CLI, AWS SDKs, oppure AWS APIs.	Seguendo le istruzioni riportate in Utilizzo delle credenziali temporanee con AWS risorse nella Guida per l'IAMutente.

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, oppure AWS APIs.	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per il AWS CLI, vedere Autenticazione tramite credenziali IAM utente nella AWS Command Line Interface Guida per l'utente. • In AWS SDKse strumenti, vedi Autenticazione tramite credenziali a lungo termine nel AWS SDKse Guida di riferimento agli strumenti. • In AWS APIs, vedi Gestione delle chiavi di accesso per IAM gli utenti nella Guida per l'IAMutente.

Proteggiti dagli aggressori

Per ulteriori informazioni su come proteggere dagli aggressori quando concedi autorizzazioni ad altri AWS responsabili del servizio, consulta Condizioni opzionali per le relazioni di fiducia relative al ruolo. Aggiungendo determinate condizioni alle policy, 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 maggiori privilegi a eseguire un'azione, ad esempio con l'impersonificazione tra diversi servizi. Per informazioni generali sulle condizioni delle polizze, consulta anche. Specifica delle condizioni in una policy

Per ulteriori informazioni sull'utilizzo di policy basate sull'identità con AWS Control Tower, vedere. 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. IAM

Policy basate su 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. AWSControl Tower non supporta politiche basate sulle risorse.

Specificare gli elementi della politica: 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 landing zone, devi essere un IAM utente con le autorizzazioni amministrative definite in una IAM policy.

I seguenti elementi sono quelli più basilari che è possibile identificare in una policy:

- Risorsa: in una policy, utilizzi un Amazon Resource Name (ARN) per identificare la risorsa a cui si applica la policy. Per ulteriori informazioni, consulta AWSRisorse e operazioni 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, vedere Azioni definite da AWS Control Tower.
- Effetto: l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe 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 (IAMpolitiche), l'utente a cui è associata la politica 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). AWSControl Tower non supporta politiche basate sulle risorse.

Per ulteriori informazioni sulla sintassi e sulle descrizioni IAM delle policy, consulta AWS IAMRiferimento alle politiche nella Guida per l'IAMutente.

Specifica delle condizioni in una policy

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della IAM policy per specificare le condizioni in cui una politica deve avere effetto. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni sulla specificazione delle condizioni in un linguaggio di policy, consulta Condition nella Guida per l'IAMutente.

Per esprimere le condizioni, è possibile utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per AWS Control Tower. Tuttavia, ci sono AWS-chiavi di condizione ampie che è possibile utilizzare a seconda delle esigenze. Per un elenco completo di AWS-wide keys, vedi Available Keys for Conditions nella Guida per l'IAMutente.

Impedisci l'impersonificazione tra servizi

In AWS, l'impersonificazione trasversale può portare alla confusione del vicesceriffo. 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 politiche per limitare le autorizzazioni che AWS Control Tower concede a un altro servizio per l'accesso alle tue risorse.

- `aws:SourceArn`Utilizzatela se desiderate 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 quello ARN per un bucket Amazon S3, devi utilizzare entrambe le condizioni per limitare le autorizzazioni.
- Se utilizzi entrambe le condizioni e se il `aws:SourceArn` valore contiene l'ID dell'account, il `aws:SourceAccount` valore e l'account nel `aws:SourceArn` valore devono mostrare lo stesso ID account se utilizzati nella stessa dichiarazione politica

Per maggiori informazioni ed esempi, consulta https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Utilizzo di policy basate sull'identità (policy IAM) per AWS Control Tower

Questo argomento fornisce esempi di 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 sulla gestione delle autorizzazioni di accesso alle risorse AWS Control Tower.

Autorizzazioni necessarie per utilizzare la console AWS Control Tower

AWS Control Tower crea automaticamente tre ruoli quando 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

- AWS ControlTowerAdmin ruolo
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Ti consigliamo di limitare l'accesso alle tue politiche di fiducia dei ruoli per questi ruoli. Per ulteriori informazioni, consulta Condizioni opzionali per le relazioni di fiducia tra i ruoli.

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:

```
{
  "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:

```
{
    "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 ControlTowerServiceRolePolicySi 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 (OU) governati da AWS Control Tower.

Gli aggiornamenti a questa policy gestita sono riepilogati nella tabella,. Policy gestite per AWS Control Tower

Per ulteriori informazioni, consulta AWSControlTowerServiceRolePolicyla AWS Managed Policy Reference Guide.

Nome della policy gestita: AWS ControlTowerServiceRolePolicy

L'artefatto JSON per AWS ControlTowerServiceRolePolicy è il seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
```

```
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
```

```
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Politica di fiducia dei ruoli:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

La politica in linea è`AWSControlTowerAdminPolicy`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation assume questo ruolo per distribuire set di stack negli account creati da AWS Control Tower. Policy inline:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Policy di trust

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control CloudTrail Tower è una best practice e fornisce questo ruolo a CloudTrail. CloudTrailassume questo ruolo per creare e pubblicare i CloudTrail log. Policy inline:

```
{
    "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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess requisiti di ruolo

AWS Control Tower richiede la creazione del `AWSControlTowerBlueprintAccess` ruolo nell'account Blueprint Hub designato, all'interno della stessa organizzazione.

Role name (Nome ruolo)

Il nome del ruolo deve essere`AWSControlTowerBlueprintAccess`.

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 `AWSControlTowerAdmin` 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Autorizzazioni relative ai ruoli

È necessario allegare la politica gestita AWSServiceCatalogAdminFullAccessal 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 `AWSServiceRoleForAWSControlTower` ruolo 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:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

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 risultati per le risorse gestite dai controlli del Security Hub che fanno parte dello standard gestito dal Security Hub Service-managed: 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 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 del 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`

L'artefatto JSON per `AWSControlTowerAccountServiceRolePolicy` è il seguente:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com"
```

```
    }
   }
  },
  // More managed rule permissions
  {
   "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
  },
  // Add permission to publish the security notifications to SNS
  {
   "Sid": "AllowControlTowerToPublishSecurityNotifications",
   "Effect": "Allow",
   "Action": "sns:publish",
   "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
   "Condition": {
    "StringEquals": {
     "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
   }
  },
  // For drift verification
  {
   "Sid": "AllowActionsForSecurityHubIntegration",
   "Effect": "Allow",
   "Action": [
    "securityhub:DescribeStandardsControls",
    "securityhub:GetEnabledStandards"
   ],
   "Resource": "arn:aws:securityhub:*:*:hub/default"
  }
 ]
}
```

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
AWSControlTowerAccountServiceRolePolicy— 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, in base a tali regole, di gestire il rilevamento delle deviazioni per i controlli correlati a Security Hub. Questa modifica è necessaria per consentire ai clienti di visualizzare le risorse alla deriva nella console, quando tali risorse sono correlate ai controlli del Security Hub che fanno parte del Security Hub Service-managed Standard: AWS Control Tower.	22 maggio 2023
AWS ControlTowerServiceRolePolicy: aggiornamento a una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di effettuare chiamate verso e alle `GetRegionOptStatus` API implementate dal servizio	6 aprile 2023

Modifica	Descrizione	Data
	AWS Account Management, 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). `EnableRegion ListRegions` 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.	

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy: aggiornamento a una policy esistente	AWS Control Tower ha aggiunto nuove autorizzazioni che consentono ad AWS Control Tower di assumere il `AWSControlTowerBlueprintAccess` 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 `AWSControlTowerBlueprintAccess` 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 effettuare il provisioning di account personalizzati tramite AWS Control Tower Account Factory.	28 ottobre 2022

Modifica	Descrizione	Data
AWS ControlTowerServiceRolePolicy: aggiornamento a 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 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 a 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. AWS CloudTrail `PutEventSelector` La modifica alla politica consente al AWS ControlTowerAdminruolo di chiamare l' AWS CloudTrail `PutEventSelector` 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 a 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 aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza AWS Control Tower. I seguenti argomenti mostrano come configurare AWS Control Tower per soddisfare gli 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 tutto il Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management

(IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'uso dei CloudTrail percorsi per registrare 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 FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard () 140-3. FIPS

Ti consigliamo vivamente 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 consoleAPI, AWS CLI, 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel 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 modello di responsabilitàAWS condivisa e il post di GDPR blog sul AWS Security Blog. AWSControl 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

AWSControl Tower utilizza bucket Amazon S3 e database Amazon DynamoDB crittografati a riposo utilizzando Amazon S3 Managed Keys (-S3) a supporto della landing zone. SSE Questa crittografia è configurata di default quando configuri la landing zone. Facoltativamente, puoi configurare la landing zone per crittografare le risorse con chiavi di KMS crittografia. 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

AWSControl Tower utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito a supporto della landing zone. Inoltre, l'accesso a AWS Control Tower richiede l'utilizzo della console, a cui è possibile accedere solo tramite un HTTPS endpoint. 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 IAM delle autorizzazioni giuste o, nel caso degli utenti di IAM Identity Center, che siano nei gruppi corretti.

- Per ulteriori informazioni sui ruoli e le politiche per le IAM entità, consulta la Guida per IAMl'utente.
- Per ulteriori informazioni sui gruppi IAM Identity Center creati quando configuri la landing zone, consultaGruppi IAM Identity Center per AWS Control Tower.

Convalida della conformità per AWS Control Tower

AWSControl Tower è un servizio ben progettato che può aiutare l'organizzazione a soddisfare le 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 PCIRAMP, Fed 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 utilizzi AWS Control Tower è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi. HIPAA
- AWS Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- 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— 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 nella 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, vedereCome 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

AWSControl Tower è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzate API le chiamate AWS pubblicate per accedere ai AWS servizi e alle risorse all'interno della vostra landing zone attraverso la rete. Richiediamo Transport Layer Security (TLS) 1.2 e consigliamo Transport Layer Security (TLS) 1.3 o versione successiva. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi configurare gruppi di sicurezza per fornire una protezione aggiuntiva 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 nei log, in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. AWS fornisce diversi strumenti per monitorare le risorse e le attività nella landing zone.

Ad esempio, lo stato dei comandi viene monitorato costantemente. Puoi vedere il loro stato a colpo d'occhio nella console AWS Control Tower o in modo programmatico tramite le API AWS Control Tower. Inoltre, lo stato e lo stato degli account che hai fornito in Account Factory vengono monitorati costantemente.

Visualizza le azioni registrate dalla pagina Attività

Nella console AWS Control Tower, la pagina Attività fornisce una panoramica delle azioni dell'account di gestione AWS Control Tower. Per accedere alla pagina delle attività di AWS Control Tower, seleziona Activities dalla barra di navigazione a sinistra.

Le attività mostrate nella pagina Attività sono le stesse riportate nel registro degli AWS CloudTrail eventi per AWS Control Tower, ma sono mostrate in formato tabellare. Per ulteriori informazioni su un'attività specifica, selezionare l'attività dalla tabella e quindi scegliere View details (Visualizza dettagli).

Puoi visualizzare le azioni e gli eventi degli account dei membri nei file di archivio dei log.

Le seguenti sezioni descrivono il monitoraggio e la registrazione in AWS Control Tower con maggiori dettagli:

Argomenti

Informazioni sulla registrazione in AWS Control Tower

AWS Control Tower registra automaticamente azioni ed eventi, attraverso la sua integrazione con AWS CloudTrail e AWS Config, e li registra. 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'CloudTrail utente.

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 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: AWSBucketPermissionsCheck
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
              - config.amazonaws.com
          Action: s3:GetBucketAcl
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
        - Sid: AWSConfigBucketExistenceCheck
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
              - config.amazonaws.com
          Action: s3:ListBucket
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
        - Sid: AWSBucketDeliveryForConfig
          Effect: Allow
          Principal:
            Service:
              - config.amazonaws.com
          Action: s3:PutObject
          Resource:
            - Fn::Join:
                - ""
                -
                  - !Sub "arn:${AWS::Partition}:s3:::"
                  - !Ref "S3AuditBucket"
                  - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
          Condition:
            StringEquals:
              aws:SourceOrgID: !Ref OrganizationId
        - Sid: AWSBucketDeliveryForOrganizationTrail
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
          Action: s3:PutObject
          Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
```

```
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

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. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon 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 log da istanze Amazon EC2 e altre CloudTrail fonti. 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 CloudTrailacquisisce 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. CloudWatchLe 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 percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli 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:

API pubbliche

- Per un elenco completo delle API pubbliche di AWS Control Tower e dettagli su ciascuna di esse, consulta The AWS Control Tower API Reference. Le chiamate a queste API pubbliche vengono registrate da. AWS CloudTrail

Altre API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.
- Se la richiesta è stata rifiutata perché accesso negato o elaborata correttamente.

Per ulteriori informazioni, vedete l'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, AWS Config genera cinque CI, uno per ogni regione. Altre risorse globali, come le zone ospitate da Route 53, vengono registrate una sola volta in tutte le regioni. Ad esempio, se crei una nuova zona ospitata su Route 53 in un account registrato, AWS Config genera un CI, indipendentemente dal numero di regioni selezionate per quell'account. Per un elenco che ti aiuti a distinguere questi tipi di risorse, consultaLa 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 in una chiamata API Descrive 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 poter visualizzare gli IC in AWS Config una dashboard. Per ulteriori informazioni, consulta il post del blog intitolato AWS Config support Amazon CloudWatch metrics.

A livello di programmazione, per visualizzare AWS Config i dati, puoi utilizzare la AWS CLI o utilizzare altri strumenti. AWS

Interroga 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 Amazon QuickSight

Puoi visualizzare e interrogare le risorse registrate da AWS Config tutta l'organizzazione. Per ulteriori informazioni, consulta Visualizzazione AWS Config dei dati con Amazon Athena e Amazon QuickSight.

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 CI. Se esegui questi processi in un account non di produzione, valuta la possibilità di annullare la registrazione dell'account. Potrebbe essere necessario disattivare manualmente il AWS Config registratore per quell'account.

> **Note**
>
> Dopo aver annullato la registrazione dell'account, AWS Control Tower non può applicare controlli investigativi o registrare gli eventi dell'account, come AWS Config le attività, per le risorse in quell'account.

Per ulteriori informazioni, consulta Annullare la gestione di un account registrato. Per informazioni su come disattivare il AWS Config registratore, vedere Gestione del registratore di configurazione.

La stessa risorsa viene registrata più volte

Verifica se la risorsa è una risorsa globale. Per le zone di atterraggio di AWS Control Tower precedenti alla versione 3.0, AWS Config è AWS Config 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 unità organizzative (OU), account e controlli.

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.

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 UpdateManagedAccountper cercare gli eventi del ciclo di vita e 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 log registra se AWS Control Tower ha completato con successo ogni azione per abilitare il controllo su un'unità organizzativa creata da AWS Control Tower.
- `DisableGuardrail`: Il registro registra se AWS Control Tower ha completato con successo ogni azione per disabilitare un controllo su un'unità organizzativa creata da AWS Control Tower.
- `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.

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 management account.
    "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": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
```

```
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "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'`guardrailId`and `guardrailBehavior` del controllo e l'`organizationalUnitName`e `organizationalUnitId` dell'unità organizzativa su cui è abilitato il controllo.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
   "account": "XXXXXXXXXXXX",
   "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
Format: yyyy-MM-dd'T'hh:mm:ssZ
   "region": "us-east-1",                                             // AWS Control Tower
home region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",
       "eventSource": "controltower.amazonaws.com",
       "eventName": "EnableGuardrail",
       "awsRegion": "us-east-1",
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "0000000-0000-0000-1111-123456789012",
       "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`and `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": "0000000-0000-0000-1111-123456789012",
        "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 l'`organizationalUnitName`e `organizationalUnitId` per ciascuna delle unità organizzative e l'`accountName`e `accountId` per ogni account che vengono creati quando AWS Control Tower configura la landing zone.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
```

```
            "accountId": "XXXXXXXXXXXX",                          // Management-account
ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "SetupLandingZone",
        "awsRegion": "us-east-1",                                 // AWS Control Tower
home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                         // This value is
generated by CloudTrail.
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "setupLandingZoneStatus": {
                "state": "SUCCEEDED",                              // Status of entire
lifecycle operation.
                "message": "AWS Control Tower successfully set up a new landing zone.",

                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",           // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                  },
                ],
               "accounts": [                                       // All created
accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
```

```
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
  }
}
```

UpdateLandingZone

Questo evento del ciclo di vita registra se AWS Control Tower ha aggiornato 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 l'`organizationalUnitName`e `organizationalUnitId` per ciascuna delle unità organizzative e l'`accountName`e `accountId` per ogni account, creati in precedenza, quando AWS Control Tower aveva originariamente impostato la landing zone.

```
{
    "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": "XXXXXXXXXX"
                 }
             ],
             "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": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",
```

```
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

Questo evento del ciclo di vita registra se AWS Control Tower ha disabilitato con successo le sue funzionalità di governance su un'unità organizzativa. Questo evento corrisponde all'evento AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail . Il registro degli eventi del ciclo di vita include la `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": "0000000-0000-0000-1111-123456789012",
```

```
        "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",                    // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"           // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

Questo evento del ciclo di vita registra se AWS Control Tower ha eseguito 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"
}
```


Utilizzo delle notifiche AWS utente con AWS Control Tower

Puoi utilizzare le notificheAWS 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 tramite più canali, tra cui e-mail, notifiche di AWS Chatbotchat o notifiche push dell'appAWS Console Mobile. 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 ricevute 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'area campanella/notifiche sulla 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 Security Hub. Un frammento di codice in JSON per configurare l'abbonamento alle notifiche può essere simile al seguente:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filtraggio degli eventi

- Puoi filtrare gli eventi per servizio e nome utilizzando i filtri disponibili nella console AWS User Notifications.
- Puoi filtrare gli eventi in base a proprietà specifiche se crei il tuo EventBridge filtro dal codice JSON.

Evento di esempio AWS Control Tower

Ecco un esempio generalizzato di evento per AWS Control Tower.

- È un EventBridge evento.
- Puoi iscriverti a EventBridge eventi (come questo) utilizzando le notifiche AWS utente.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 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
        }
    }
}
```

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

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: automatizza il provisioning degli account nelle API di AWS Control Tower tramite Service Catalog

AWS Control Tower è integrato con diversi altri AWS servizi, ad esempio AWS Service Catalog. Puoi utilizzare le API per creare ed effettuare il provisioning degli account dei membri in AWS Control Tower.

Il video mostra come effettuare il provisioning degli account in modo automatico e in batch, richiamando le AWS Service Catalog API. Per il provisioning, chiamerai l'`ProvisionProduct`API dall'interfaccia a riga di AWS comando (CLI) e specificherai un file JSON che contiene i parametri per ogni account che desideri configurare. Il video illustra l'installazione e l'utilizzo dell'ambiente di sviluppo AWS Cloud9 per eseguire questo lavoro. I comandi CLI sarebbero gli stessi se si utilizza AWS Cloudshell anziché Cloud9. AWS

> **Note**
>
> Puoi anche adattare questo approccio per automatizzare gli aggiornamenti degli account, chiamando l'`UpdateProvisionedProduct`API di per ogni account. AWS Service Catalog È possibile scrivere uno script per aggiornare gli account, uno per uno.

Trattandosi di un metodo di automazione completamente diverso, se conosci Terraform, puoi effettuare il provisioning degli account con AWS Control Tower Account Factory for Terraform (AFT).

Esempio di ruolo di amministrazione dell'automazione

Ecco un modello di esempio che puoi utilizzare per configurare il tuo ruolo di amministrazione dell'automazione nell'account di gestione. È necessario configurare questo ruolo nel proprio account di gestione in modo che possa eseguire l'automazione con l'accesso di amministratore negli account di destinazione.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
```

```
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Esempio di ruolo di esecuzione dell'automazione

Di seguito è riportato un modello di esempio che è possibile utilizzare per configurare il ruolo di esecuzione dell'automazione. Dovresti configurare questo ruolo negli account di destinazione.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
```

```
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Dopo aver configurato questi ruoli, chiami le AWS Service Catalog API per eseguire le attività automatiche. I comandi CLI sono riportati nel video.

Esempio di input di provisioning per l'API Service Catalog

Ecco un esempio dell'input che puoi fornire all'API Service Catalog se utilizzi l'`ProvisionProduct`API per effettuare il provisioning degli account AWS Control Tower:

```
{
  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.

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 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 alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Cerca **VPC** o seleziona VPC dalle opzioni del Service Catalog. Viene quindi visualizzato il VPC Dashboard (Pannello di controllo VPC).
3. Dal menu a sinistra, scegliere Your VPCs (I tuoi VPC). Viene quindi visualizzato un elenco di tutti i tuoi VPC.
4. Identifica 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 AWS VPC 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.

Crea un account in AWS Control Tower senza un VPC

Se i carichi di lavoro degli utenti finali non richiedono VPC, puoi utilizzare questo metodo per configurare account utente finale per i quali non vengono creati automaticamente dei VPC.

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 VPC

1. Apri un browser Web e accedi alla console AWS Control Tower all'indirizzo https://console.aws.amazon.com/controltower.
2. Scegli Account Factory dal menu a sinistra.
3. Viene quindi visualizzata la pagina Account Factory con la sezione Configurazione di rete.
4. Annota le impostazioni correnti qualora desiderassi ripristinarle in un secondo momento.
5. Scegli il pulsante Edit (Modifica) nella sezione Network Configuration (Configurazione di rete).

6. Nella pagina Edit account factory network configuration (Modifica configurazione rete Factory Account), vai alla sezione VPC Configuration options for new accounts (Opzioni di configurazione VPC per i nuovi account).

   Puoi seguire l'opzione 1 o l'opzione 2, o entrambe, per assicurarti che AWS Control Tower non crei un VPC durante il provisioning di un account.

   a. Opzione 1: rimozione delle sottoreti

      - Disattiva l'interruttore 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. Selezionare 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 VPC.

- 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.

Procedura dettagliata: smantellamento di una AWS Control Tower Landing Zone

AWS Control Tower ti 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 lalanding zone esistente dopo averla disattivata.

Panoramica del processo di smantellamento

Quando richiedi lo smantellamento della tua landing zone, AWS Control Tower esegue le seguenti azioni.

- Disattiva ogni controllo investigativo abilitato nella landing zone. AWS Control Tower elimina le AWS CloudFormation risorse che supportano il controllo.
- Disattiva ogni controllo preventivo rimuovendo le policy di controllo dei servizi (SCP) da. AWS Organizations Se una policy è vuota (cosa che dovrebbe succedere dopo aver rimosso tutti gli SCP gestiti da AWS Control Tower), AWS Control Tower rimuove ed elimina completamente la policy.
- Elimina tutti i blueprint distribuiti come. AWS 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 alle OU create dal cliente.
- Elimina i record interni che identificano la regione di origine.

> **Note**
>
> Dopo la disattivazione, è possibile rimuovere il blueprint VPC Account Factory (`BP_ACCOUNT_FACTORY_VPC`) per ripulire le route e i gateway NAT, se il VPC non era vuoto.

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 due unità organizzative (OU), denominate Security e Sandbox. Quando si disattiva la landing zone, la gerarchia dell'organizzazione viene mantenuta, come segue:

- Le unità organizzative (OU) create dalla console AWS Control Tower non vengono rimosse.
- Le unità organizzative Security e Sandbox non vengono rimosse.
- L'organizzazione non viene eliminata da AWS Organizations.

- Nessun account AWS Organizations (condiviso, assegnato o di gestione) viene spostato o rimosso.

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 account AWS e set di autorizzazioni IAM Identity Center non vengono rimosse.
- Le directory di IAM Identity Center non vengono modificate.

Roles

Durante la configurazione, AWS Control Tower crea determinati ruoli per te se usi la console o ti chiede di creare questi ruoli se configuri la landing zone tramite le API. Quando disattivate la vostra landing zone, i seguenti ruoli non vengono rimossi:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Bucket Amazon S3

Durante la configurazione, AWS Control Tower crea bucket nell'account di registrazione per la registrazione e per l'accesso alla registrazione. Quando si disattiva la landing zone, le seguenti risorse non vengono rimosse:

- I bucket S3 della registrazione e di accesso alla registrazione nell'account di registrazione non vengono rimossi.
- I contenuti dei bucket di accesso alla registrazione e alla registrazione non vengono rimossi.

Account condivisi

Due account condivisi (Audit e Log Archive) vengono creati nell'unità organizzativa di sicurezza durante la configurazione di AWS Control Tower. Quando si disattiva la landing zone:

- Gli account condivisi creati durante la configurazione di AWS Control Tower non vengono chiusi.
- Il ruolo `OrganizationAccountAccessRole` IAM viene ricreato per allinearlo alla configurazione standard AWS Organizations .
- Il ruolo `AWSControlTowerExecution` viene rimosso.

Account di cui è stato eseguito il provisioning

I clienti AWS Control Tower possono utilizzare account factory per creare nuovi account AWS. 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 allinearlo 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-MANAGEMENT` Questo gruppo di log non viene rimosso. Al contrario, il blueprint viene eliminato e le risorse vengono mantenute.

- Questo gruppo di log deve essere eliminato manualmente prima di impostare un'altra landing zone.

> **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 condivisi e dai 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 inGestisci le risorse di AWS Control Tower.

Gestisci le risorse di 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 Procedura dettagliata: smantellamento di una AWS Control Tower Landing Zone 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' AWS Management Console accesso 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

Eliminazione di SCP

AWS Control Tower utilizza policy di controllo dei servizi (SCP) per i propri controlli. Questa procedura spiega come eliminare gli SCP specificamente correlati ad AWS Control Tower.

Per eliminare gli SCP AWS Organizations

1. Apri la console Organizations all'indirizzo https://console.aws.amazon.com/organizations/.
2. Aprire la scheda Policies (Policy) e trovare le policy di controllo dei servizi (SCP) che hanno il prefisso aws-guardrails- ed eseguire la procedura seguente per ogni SCP:
   a. Scollegare l'SCP dall'unità organizzativa associata.
   b. Eliminare l'SCP.

Elimina StackSets e impila

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 AWS CloudFormation StackSets

1. Apri la AWS CloudFormation console all'indirizzo 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, annota gli ID degli AWS account 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 gli ID degli AWS account che hai registrato nel passaggio 3.b, separati 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 AWS CloudFormation

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Dalla dashboard Stacks, cerca tutti gli stack con il prefisso. AWSControlTower
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-controltower.
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. Passare all'URL del portale all'indirizzo *`directory-id`*.awsapps.com/start
2. In AWS Account, trova l'account di gestione.
3. Da AWSServiceCatalogAdminFullAccess, scegli Console di gestione per accedere a AWS Management Console 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 AWSServiceCatalogEndUserAccess 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.

Come disattivare una landing zone

Per disattivare la landing zone di AWS Control Tower, 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
```

Attività di pulizia manuale necessarie dopo la disattivazione

- 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 CloudFormation stack AWS 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.

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 riattivare una landing zone, ma non è necessario eliminarla.
- Potresti voler rimuovere il VPC creato da AWS Control Tower.
- La configurazione fallisce se gli indirizzi e-mail specificati per gli account di registrazione o di controllo sono associati a un account esistente AWS . Puoi chiudere gli AWS account o utilizzare indirizzi e-mail diversi per configurare nuovamente una landing zone. In alternativa, puoi riutilizzare questi account condivisi esistenti, con la funzione che ti consente di creare i tuoi account di registrazione e controllo. Per ulteriori informazioni, consulta Considerazioni sull'utilizzo degli account di sicurezza o di registrazione esistenti.

- L'installazione non riesce se nell'account di registrazione sono già presenti bucket Amazon S3 con i seguenti nomi riservati:
  - `aws-controltower-logs-{accountId}-{region}` (utilizzato per il bucket di registrazione).
  - `aws-controltower-s3-access-logs-{accountId}-{region}` (utilizzato per il bucket di accesso alla registrazione).

  È necessario rinominare o rimuovere questi bucket oppure utilizzare un account diverso per l'account di registrazione.
- L'installazione fallisce se l'account di gestione ha il gruppo di log esistente,`aws-controltower/CloudTrailLogs`, in Logs. CloudWatch È necessario rinominare o rimuovere il gruppo di log.

Prima di eseguire la configurazione in un nuovo Regione AWS

Se intendi configurare una nuova landing zone in una nuova AWS regione, segui questi passaggi aggiuntivi.

- Immettete il seguente comando tramite la CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Elimina la 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 unità organizzative di primo livello denominate Security o Sandbox. È necessario rinominare o rimuovere queste unità organizzative per impostare nuovamente una landing zone.

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.

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.
- AWS 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 AWS 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 visualizzare un elenco di Regioni AWS quelli supportati da AWS Control Tower, consultaCome funzionano AWS le regioni con AWS Control Tower.

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 Fornire account con AWS Service Catalog 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 AWS 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 Registrare 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 imposti 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.

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 rimuovile 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, 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. Potrebbe sembrare che il messaggio non spieghi il problema in modo adeguato, 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 Registrare 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-dpqqfywxxxx
```

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:

- Potresti aver 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 il tuo utente IAM Identity Center a uno di questi gruppi di autorizzazioni: AWSAccountFactory(per l'accesso da parte dell'utente finale) o AWSServiceCatalogAdmins(per l'accesso da amministratore).
- Se sei autenticato come utente IAM, devi aggiungerlo al AWS Service Catalog portafoglio in modo che disponga delle autorizzazioni corrette.
- Questo problema si verifica anche se disponi delle autorizzazioni corrette, ma viene rilevata una deriva da AWS Control Tower ed è necessaria una riparazione della deriva. Per riparare la maggior parte dei tipi di deriva, scegli Ripristina nella pagina delle impostazioni della zona di atterraggio.

È stato ricevuto un errore di autorizzazioni insufficienti

È possibile che il tuo account non disponga delle autorizzazioni necessarie per eseguire determinate operazioni in alcuni casi. AWS Organizations Se riscontri il seguente tipo di errore, controlla tutte le aree di autorizzazione, ad esempio le autorizzazioni IAM o IAM Identity Center, per assicurarti che l'autorizzazione non venga negata da quelle aree:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Se ritieni che il tuo lavoro richieda l'azione che stai tentando e non riesci a individuare alcuna restrizione pertinente, contatta l'amministratore di sistema o 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 creati in nessuna regione finché i singoli account all'interno delle unità organizzative governate da AWS Control Tower non vengono aggiornati. I controlli investigativi esistenti sugli account esistenti sono ancora in vigore.

Se provi ad attivare un controllo investigativo prima di aggiornare i tuoi account, potresti visualizzare un messaggio di errore simile al seguente:

`AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, 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, consultaQuando aggiornare AWS Control Tower OUs e gli account.

Per aggiornare più account individuali a livello di codice, puoi utilizzare le API e la AWS Service Catalog AWS CLI per automatizzare gli aggiornamenti. Per ulteriori informazioni su come affrontare il processo di aggiornamento, vedere questo Procedura guidata: video. Puoi sostituire l'API con l'UpdateProvisionedProductAPI mostrata nel ProvisionProductvideo.

Se hai ulteriori difficoltà ad abilitare i controlli investigativi sui tuoi account, contatta il AWS servizio clienti.

Frequenza superata (errore restituito 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 i tuoi SCP fossero andati alla deriva.

Passaggi da seguire

Se riscontri una limitazione o un `rate exceeded` errore dell'API, prova questi passaggi:

- Esegui i tuoi carichi di lavoro in un momento diverso. (Fai riferimento alla pianificazione della scansione dell'invarianza SCP di AWS Control Tower per regione per scoprire quando AWS Control Tower esegue le sue scansioni di audit.)
- Se chiami le API direttamente tramite HTTP: utilizza l' AWS SDK, che riprova automaticamente le azioni non riuscite
- Richiedi un aumento del limite tramite Service Quotas and Support AWS

Un esempio di istruzioni per la risoluzione dei problemi relativi alla limitazione delle API in Elastic Beanstalk è disponibile qui: `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Mancato trasferimento di un account Account Factory direttamente da una landing zone AWS Control Tower a un'altra landing zone AWS Control Tower

> **Warning**
>
> Questa pratica non soddisfa i prerequisiti per la registrazione di account idonei, poiché gli account idonei devono far parte della stessa AWS Organization generale e ogni organizzazione può avere una sola landing zone. Se hai provato a eseguire questa azione e ti accorgi di ricevere più messaggi di errore, ecco alcune informazioni che potrebbero esserti utili.

Per spostare un account di cui hai effettuato il provisioning tramite Account Factory in un'altra landing zone gestita da AWS Control Tower, con un altro account di gestione, devi rimuovere tutti i ruoli IAM e gli stack associati a quell'account dall'unità organizzativa originale. Rimuovi queste risorse da ogni regione in cui è distribuito l'account.

> **Note**
>
> Il modo migliore per rimuovere le risorse consiste nel deprovisioning dell'account nell'unità organizzativa originale prima di provare a spostarlo.

Se non si rimuovono le risorse, l'iscrizione alla nuova unità organizzativa fallirà, in modo alquanto spettacolare. È possibile che vengano visualizzati uno o più messaggi di errore e continuerai a ricevere messaggi di errore simili fino a quando i ruoli e gli stack rimanenti non verranno rimossi da ogni regione in cui è stato distribuito l'account.

Ogni volta che si riceve un messaggio di errore, è necessario rimuovere l'account dalla nuova unità organizzativa, eliminare la vecchia risorsa oggetto del messaggio di errore e quindi tentare di riportare l'account nella nuova unità organizzativa. Questo processo 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, l'obiettivo di base può essere un account condiviso o la landing zone nel suo insieme. 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 per un obiettivo, la linea di base viene rappresentata come una AWS CloudFormation risorsa, chiamata risorsa. `EnabledBaseline`

AWS Control Tower include quattro tipi essenziali di linee di base:

- Un tipo può essere applicato a un'unità organizzativa registrata presso AWS Control Tower o a un'unità organizzativa che intendi registrare applicando la linea di base.
- Tre tipi di base possono essere applicati a una landing zone o a un account condiviso, durante la configurazione iniziale o durante un aggiornamento della landing zone.

Tipo di base applicabile a livello di unità organizzative, per la registrazione e l'aggiornamento delle unità organizzative

- Nome: `AWSControlTowerBaseline`

  Descrizione: configura le risorse e i controlli obbligatori per gli account dei membri all'interno dell'unità organizzativa di destinazione, necessari per la governance 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'`EnableBaseline`API 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, vedi Come funzionano gli SCP con deny nella documentazione. AWS Organizations

Raccomandazione: ti consigliamo di confermare le regioni in cui l'unità organizzativa di destinazione potrebbe eseguire carichi di lavoro e di confrontare i risultati con la landing zone Region deny control prima di chiamare l'`EnableBaseline`API per l'unità organizzativa, altrimenti potresti perdere l'accesso alle risorse in determinate regioni.

> **Note**
>
> Le linee di base della zona di atterraggio si comportano in modo diverso rispetto alle linee di base a livello di unità organizzativa.

AWS Control Tower abilita automaticamente le linee di base che si applicano a livello di landing zone, come parte del processo di configurazione e aggiornamento della 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.

Tipi di base che possono essere applicati alla tua landing zone o agli account condivisi

- Nome: `AuditBaseline`

  Descrizione: configura le risorse per monitorare la sicurezza e la conformità degli account nell'organizzazione. Non è possibile modificare questa linea di base, viene distribuita da AWS Control Tower.
- Nome: `LogArchiveBaseline`

Descrizione: configura un archivio centrale per i registri delle attività delle API e delle configurazioni delle risorse degli account dell'organizzazione. Non è possibile modificare questa linea di base, viene distribuita da AWS Control Tower.

- 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.

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'`ResetEnabledBaseline`API, 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'`ResetEnabledBaseline`API 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 API per le linee di base

Quando modifichi lo stato di governance di un'unità organizzativa, la console AWS Control Tower esegue automaticamente più operazioni per te, rispetto alla modifica della governance tramite le API per le linee di base.

Differenze

- Registrazione e fornitura di prodotti

  Quando registri un'unità organizzativa tramite la console, AWS Control Tower crea prodotti Service Catalog per gli account dei membri dell'unità organizzativa, come parte della registrazione di ciascun account. Quando si registra un'unità organizzativa tramite l'`EnableBaseline`API e`AWSControlTowerBaseline`, AWS Control Tower non crea prodotti forniti per gli account dei membri nell'unità organizzativa.
- Annullare la registrazione di un'unità organizzativa

  Ogni volta che annulli la registrazione di un'unità organizzativa, devi prima rimuovere tutti gli account membro e le OU annidate. Quindi, AWS Control Tower rimuove tutti i controlli applicati all'unità organizzativa.
  - Se si seleziona Elimina l'unità organizzativa dalla console, AWS Control Tower procede all'annullamento della registrazione e quindi all'eliminazione dell'unità organizzativa dall'organizzazione.
  - Tuttavia, se annulli la registrazione dell'unità organizzativa chiamando l'`DisableBaseline`API 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 impostazioni predefinite per il controllo delle versioni

Se la tua landing zone AWS Control Tower è già configurata e scegli di abilitare una landing zone di base, AWS Control Tower abilita la versione più recente della linea di base compatibile con la versione della tua landing zone. Se scegli di abilitare una baseline per un'unità organizzativa che non

è già registrata presso AWS Control Tower, AWS Control Tower fornisce automaticamente l'ultima versione compatibile della linea di base per quell'unità organizzativa.

Compatibilità delle versioni di base delle unità organizzative e delle landing zone

Le linee di base di AWS Control Tower ti consentono di impostare uno standard di governance a livello di unità organizzativa, anziché a livello di landing zone, se la tua azienda lo richiede. La linea di base chiamata `AWSControlTowerBaseline` è disponibile per aiutarti a registrare le unità organizzative con AWS Control Tower.

> **Note**
>
> Una baseline è un gruppo di controlli e risorse che collaborano per stabilire un ambiente di governance stabile all'interno della landing zone.

Quando abiliti una baseline su un'unità organizzativa, richiamando l'`EnableBaseline`API in AWS Control Tower, devi specificare una versione di base compatibile con la versione corrente della landing zone di AWS Control Tower. Dopo aver specificato una linea di base, tutti gli account dei membri di un'unità organizzativa seguono la linea di base fornita per l'unità organizzativa. In altre parole, ai nuovi account viene fornita la linea di base aggiornata e gli account dei membri esistenti vengono regolati in base alla nuova linea di base.

Se non si seleziona una linea di base per le unità organizzative e gli account esistenti, la versione della landing zone determina l'intero assetto di governance, per impostazione predefinita. Tuttavia, a ciascuna unità organizzativa registrata nella zona di atterraggio viene assegnata una versione di base, che è la versione di base più recente compatibile con la versione corrente della landing zone. Pertanto, a ciascuna unità organizzativa e a ogni account membro registrato è associata una linea di base, anche se non viene mai assegnata una linea di base specifica.

Per quanto riguarda la 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	Controlli inclusi	Modifica rispetto alla linea di base precedente	
1	Da 2,0 a 2,7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, risorse IAM	Tutti i controlli obbligatori	Nessuno	
2.0	da 2.8 a 2.9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, risorse IAM	Tutti i controlli obbligatori	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	Controlli 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	Tutti i controlli obbligatori	Nuovo AWS Config progetto. Passa alla registrazione delle risorse globali solo nella regione d'origine. CloudTrail 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	Tutti i controlli obbligatori	Nuovo modello SLR	

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 sulle tue unità organizzative, 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 per le linee di base

- Se l'unità organizzativa richiede un aggiornamento di base, non è possibile fornire nuovi account o registrare account esistenti in tale unità organizzativa.
- Dopo un aggiornamento della landing zone, se prevedi di aggiornare anche una baseline dell'unità organizzativa, devi registrare nuovamente l'unità organizzativa o aggiornare la versione di base dell'unità organizzativa a livello di codice.
- Ti consigliamo di eseguire l'aggiornamento alla versione di base più compatibile per la versione di landing zone che stai utilizzando, in modo da ottenere tutti i vantaggi della landing zone e della baseline combinati. Ad esempio, se esegui l'aggiornamento alla versione 3.3 della landing zone, puoi continuare a utilizzare la baseline 3.0, ma non otterrai tutti i vantaggi della versione 3.3 della landing zone a meno che non esegui anche l'aggiornamento alla baseline 4.0.

- Gli aggiornamenti di base non possono essere ripristinati.
- L'abilitazione di base si rivolge a un'unità organizzativa alla volta. Pertanto, le unità organizzative nidificate non vengono aggiornate automaticamente quando viene aggiornata l'unità organizzativa principale. Si consiglia di aggiornare l'unità organizzativa principale prima di aggiornare le unità organizzative nidificate.
- Quando si chiama l'`UpdateEnabledBaseline`API o si registra nuovamente un'unità organizzativa dalla console, l'unità organizzativa conserva tutti i controlli abilitati prima dell'aggiornamento di base.
- Quando 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: registrare un'unità organizzativa AWS Control Tower solo con API

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 registrare nuovamente le OU per fornire loro le ultime modifiche. Segui questi passaggi per registrare nuovamente un'unità organizzativa a livello di codice, reimpostando la risorsa associata. `EnabledBaseline`

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>
```

Esempi di utilizzo di base API

Questa sezione contiene esempi di parametri di input e output per la linea di base AWS APIs Control Tower.

`DisableBaseline`

Per ulteriori informazioni su questa API operazione, vedere DisableBaseline.

`DisableBaseline`ingresso:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`uscita:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`CLIesempio:

```
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 questa API operazione, vedere EnableBaseline.

`EnableBaseline`ingresso:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`EnableBaseline`output, restituendo una nuova risorsa:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

`EnableBaseline`CLIesempio:

Questo esempio mostra l'abilitazione di una linea di base per un AWS Organizations organizzazione a cui è stata attivata la landing zone AWS IAMAccesso all'Identity Center, gestito da AWS Control Tower. Per recuperare l'identificatore dell'`EnabledBaseline`Identity Center, puoi utilizzare il `ListEnabledBaselines` API filtro di base dell'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 ARN valore 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-
lk87jh65 \
    --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 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-
lk87jh65 \
    --region us-west-2
```

GetBaseline

Per ulteriori informazioni su questa API operazione, vedere. GetBaseline

`GetBaseline`ingresso:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`uscita:

```
{
    "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.",
}
```

`GetBaseline`CLIesempio:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

Per ulteriori informazioni su questa API operazione, vedere GetBaselineOperation.

`GetBaselineOperation`ingresso:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation`uscita:

```
{
    "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"
    }
}
```

`GetBaselineOperation`CLIesempio:

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

`GetEnabledBaseline`

Per ulteriori informazioni su questa API operazione, vedere GetEnabledBaseline.

`GetEnabledBaseline`ingresso:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

`GetEnabledBaseline`uscita:

```
{
    "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-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
```

```
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

`GetEnabledBaseline`CLIesempio:

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`ListBaselines`

Per ulteriori informazioni su questa API operazione, vedere ListBaselines.

`ListBaselines`input (utilizzando ingressi opzionali):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`uscita:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-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-west-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-west-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."
        }
    ]
}
```

`ListBaselines`CLIesempio:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Per ulteriori informazioni su questa API operazione, vedere ListEnabledBaselines.

`ListEnabledBaselines`input (senza filtri):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`input (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
}
```

`ListEnabledBaselines`sinput (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
}
```

`ListEnabledBaselines`sinput (`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
}
```

`ListEnabledBaselines`suscita:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
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"
}
```

CLIesempio con un tipo di filtro (`baselineIdentifiers`filtro):

```
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
```

CLIesempio di utilizzo di più filtri (`baselineIdentifiers`e `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 questa API operazione, vedere ResetEnabledBaseline.

`ResetEnabledbaseline`ingresso:

```
{
```

```
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline`uscita:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`CLIesempio:

```
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 questa API operazione, vedere UpdateEnabledBaseline.

`UpdateEnabledBaseline`ingresso:

```
{
    "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/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`UpdateEnabledBaseline`uscita:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaselineCLIesempio:

```
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 migliori pratiche per le funzionalità di AWS Control Tower e alcuni miglioramenti aggiuntivi.

Tutorial e laboratori

- AWSControl Tower lab: questi laboratori offrono una panoramica di alto livello delle attività comuni relative a AWS Control Tower.
- Nella dashboard AWS di Control Tower, scegli Ottieni indicazioni personalizzate se hai in mente un caso d'uso ma non sai da dove iniziare.
- Prova a visitare un elenco selezionato di YouTube video che spiegano di più su come utilizzare la funzionalità AWS Control Tower.

Rete

Imposta modelli ripetibili e gestibili per le reti in. AWS Scopri di più sulla progettazione, l'automazione e le appliance comunemente utilizzate dai clienti.

- AWS VPCArchitettura 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 lanciare AWS servizi e altre risorse.
- Self-service VPCs in AWS Control Tower utilizzando AWS Service Catalog: questo post del blog descrive un modo per configurare Account Factory in modo da poter fornire account personalizzatiVPCs.
- Implementazione di Serverless Transit Network Orchestrator () in STNO Control Tower AWS: questo post sul blog dimostra come automatizzare l'accesso alla connettività di rete tra gli account. Questo blog è destinato agli amministratori AWS di 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 degli avvisi con gli eventi del ciclo di vita di AWS Control Tower: questo post sul blog descrive come automatizzare l'abilitazione e la configurazione del Security Hub in un ambiente multi-account Control AWS 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 Access Analyzer. IAM
- AWSSystems Manager Parameter Store fornisce uno storage sicuro e gerarchico per la gestione dei dati di configurazione e la gestione dei segreti. È possibile utilizzarlo per condividere le informazioni di configurazione in un luogo sicuro, per l'utilizzo da parte di AWS Systems Manager e di AWS CloudFormation. Ad esempio, è possibile memorizzare un elenco di regioni in cui si desidera distribuire i pacchetti di conformità.

Identità

- Collega l'identità utente di Azure AD AWS agli account e alle applicazioni per il Single Sign-On: questo post di blog descrive come usare Azure AD con IAM Identity Center e Control Tower. AWS
- Gestisci l'accesso AWS centralizzato 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 registri su più account e regioni. AWS AWS

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.
- Implementazione continua di Cloud Custodian su Control Tower AWS

Lavorare 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.
- Porta un account sotto AWS Control Tower: questo post sul blog descrive come implementare AWS Control Tower nelle AWS organizzazioni esistenti.
- Estendi la governance della AWS Control Tower utilizzando i pacchetti di conformità AWS Config: questo post sul blog descrive come implementare pacchetti di AWS Config conformità per aiutare a portare gli account e le organizzazioni esistenti alla governance da parte di Control Tower. AWS
- Come rilevare e mitigare la violazione di Guardrail con AWS Control Tower: questo post sul blog descrive come aggiungere controlli e come iscriversi alle SNS notifiche in modo da poter ricevere notifiche via e-mail in caso di violazioni della conformità ai controlli.

Automazione e integrazione

Automatizza la creazione degli account e integra gli eventi del ciclo di vita con Control TowerAWS.

- Eventi del ciclo di vita: questo post sul blog descrive come utilizzare gli eventi del ciclo di vita con Control Tower. AWS
- 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 VPC flusso di Amazon: questo post di blog descrive come automatizzare e centralizzare Amazon VPC Flow Logs in un ambiente con più account.
- Automatizza l'VPCetichettatura con gli eventi del ciclo di vita di AWS Control Tower: questo post sul blog descrive come automatizzare l'etichettatura delle risorse perVPCs, tramite gli eventi del ciclo di vita in Control Tower. AWS
- 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

Utilizza 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 correlati AWS

AWSControl Tower funge da livello di orchestrazione per. AWS Organizations Pertanto, tramite la console AWS OrganizationsAPIs, hai accesso a oltre 20 altri AWS servizi 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, vedi AWSi servizi che puoi usare con AWS Organizations.
- Per abilitare le funzionalità multi-account per questi AWS servizi correlati, è necessario abilitare l'accesso affidabile. Per ulteriori informazioni, vedere Using AWS Organizations with other AWS services.

  > **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 tramite 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 dei gruppi di sicurezza con AWS Firewall Manager.

Marketplace AWS soluzioni

Scopri le soluzioni di Marketplace AWS.

- AWSControl 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.

AWSNote di rilascio di Control Tower

Le sezioni seguenti mostrano i dettagli sulle versioni di AWS Control Tower che richiedono un aggiornamento per una landing zone di AWS Control Tower, nonché le versioni che 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. Poiché può verificarsi un ritardo tra il momento in cui la funzionalità o la versione viene documentata e quella in cui viene annunciata ufficialmente, la data indicata per una funzionalità o una versione qui potrebbe differire leggermente dalla data riportata nel. Cronologia dei documenti

Funzionalità rilasciate nel 2024

Funzionalità rilasciate nel 2023

Funzionalità rilasciate nel 2022

Funzionalità rilasciate nel 2021

Funzionalità rilasciate nel 2020

Funzionalità rilasciate nel 2019

Gennaio 2024 - Presente

Da gennaio 2024, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- AWSControl Tower supporta fino a 1000 account per unità organizzativa
- AWSControl Tower aggiunge la selezione della versione della landing zone
- Controllo descrittivo API disponibile, accesso esteso alle regioni e ai controlli
- AWSControl Tower supporta AFT e cFCT nelle regioni opt-in
- AWSControl Tower aggiunge `ListLandingZoneOperations` API
- AWSControl Tower supporta fino a 100 operazioni di controllo simultanee
- AWSControl Tower disponibile in AWS Canada occidentale (Calgary)
- AWSControl Tower supporta l'aggiustamento delle quote in modalità self-service
- AWSControl Tower rilascia la Controls Reference Guide
- AWSControl Tower aggiorna e rinomina due controlli proattivi

- I controlli obsoleti non sono più disponibili
- AWSControl Tower supporta l'etichettatura `EnabledControl` delle risorse in AWS CloudFormation
- AWSControl Tower supporta APIs la registrazione e la configurazione delle unità organizzative con linee di base

AWSControl 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.)

AWSControl 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 entra subito nella governance di AWS Control Tower, senza modificare la struttura dell'unità organizzativa. I processi di registrazione e ri-registrazione delle unità organizzative sono inoltre più efficienti e richiedono molto meno tempo per implementare le risorse di base di AWS Control Tower negli account.

Alcune limitazioni relative agli account sono ancora valide a causa delle limitazioni relative al numero di AWS CloudFormation set di pile disponibili. In particolare, il numero massimo di account che è possibile registrare in un'unità organizzativa può variare a seconda del numero di regioni soggette a governance. Per ulteriori informazioni, visita Limitazioni basate sui dati sottostanti AWS servizi nella AWSControl Tower User Guide. Per un elenco completo di Regioni AWS dove è disponibile AWS Control Tower, vedi Regione AWS tavolo.

AWSControl 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 la versione 3.1 o successiva della landing zone AWS Control Tower, puoi aggiornare o riparare la landing zone esistente nella versione attuale oppure puoi passare 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.

Controllo descrittivo API disponibile, accesso esteso alle regioni e ai controlli

6 agosto 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ha aggiunto due nuove API operazioni che consentono di trovare ulteriori informazioni sui controlli disponibili, a livello di codice. Questa funzionalità semplifica l'implementazione dei controlli con l'automazione.

- `GetControl`APIRestituisce i dettagli su un controllo abilitato, incluso l'identificatore di destinazione, un riepilogo delle informazioni di controllo, un elenco di regioni di destinazione e lo stato di deriva.
- `ListControls`APIrestituisce un elenco impaginato di tutti i controlli disponibili nella libreria di controlli AWS Control Tower.

Questi APIs vengono raggiunti tramite AWS Spazio dei nomi 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 poterli visualizzare AWS controlli in base ad alcuni casi d'uso comuni, ad esempio: sicurezza, costi, durabilità e operazioni. Per ulteriori informazioni, consulta il Control Catalog API Reference.

Disponibilità estesa della regione

A partire da questa versione, è possibile estendere la governance AWS di Control Tower a Regioni AWS dove alcuni dei 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 AWScontrollo Control Tower APIs e il catalogo di controllo APIs possono aiutarti a ottenere informazioni su AWS

Regioni in cui sei protetto da controlli abilitati e regioni in cui è possibile implementare controlli aggiuntivi. Le informazioni sulla regione e sul controllo sono disponibili anche nella console AWS Control Tower.

AWSControl 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 AWS Control Tower Account Factory for Terraform (AFT) e Customizations for Control AWS Tower (cFCT) sono disponibili in cinque ulteriori cinque Regioni AWS: Asia Pacifico (Hyderabad, Giacarta e Osaka), Israele (Tel Aviv) e Medio Oriente (). UAE

Account Factory for Terraform (AFT) imposta una pipeline Terraform per aiutarti a fornire e personalizzare gli account in Control TowerAWS. Customizations for AWS Control Tower (cFCT) ti aiuta a personalizzare la tua landing zone e gli AWS account della Control Tower con AWS CloudFormation modelli e politiche di controllo del servizio ()SCPs.

Per saperne di più, 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 Github e sulla pagina AFT Github di cFct. AFTe cfCT sono supportati in tutti AWS Regioni, con alcune eccezioni. Per informazioni specifiche, consulta Limitazioni regionali.

AWSControl Tower aggiunge **`ListLandingZoneOperations`** API

26 giugno 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ne ha aggiunto uno API che consente di recuperare un elenco delle operazioni recentemente applicate alla landing zone e delle operazioni attualmente in corso. APIPossono restituire la cronologia delle operazioni relative alle 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 su `ListLandingZoneOperations`API, vedere `ListLandingZoneOperations`il AWSControl Tower API Reference.

AWSControl 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.)

AWSControl Tower ora supporta più operazioni di controllo con una maggiore concorrenza. Puoi inviare fino a 100 AWS operazioni di controllo Control Tower, tra più unità organizzative (OUs), contemporaneamente, dalla console o conAPIs. 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 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 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.

AWSControl Tower disponibile in 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 installato AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione, puoi farlo con la landing zone AWS APIs Control Tower. Oppure dalla console, vai alla pagina Impostazioni nella dashboard di AWS Control Tower, seleziona le tue regioni e aggiorna la landing zone.

La regione Canada occidentale (Calgary) non supporta AWS Service Catalog. Per questo motivo, alcune funzionalità di AWS Control Tower sono diverse. La modifica di funzionalità più importante è che Account Factory non è disponibile. Se scegli Canada West (Calgary) come regione di residenza, le procedure per l'aggiornamento degli account, 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 quindi di registrarlo in un'unità organizzativa

registrata. Per ulteriori informazioni, vedere Registrazione di un account esistente e Procedura per la registrazione di 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 West (Calgary), a causa della mancanza di altre dipendenze sottostanti per Control Tower. AWS Se estendi la governance alla regione Canada occidentale (Calgary), puoi continuare a gestire AFC i blueprint in tutte le regioni supportate da AWS Control Tower, purché Service Catalog sia disponibile nella tua regione di origine.

Controlli

Controlli e controlli proattivi per AWS Security Hub 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 AWS Config non sono disponibili. Per informazioni dettagliate, consultare Limitazioni di controllo.

Provider di identità

IAMIdentity 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 West (Calgary).

L'indisponibilità di Service Catalog nella regione Canada occidentale (Calgary) non ha alcun effetto sulle altre regioni supportate da AWS Control Tower. Queste differenze si applicano solo se la tua regione di residenza è Canada occidentale (Calgary).

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta AWS Tabella delle regioni.

AWSControl 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.)

AWSControl 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.

AWSControl Tower rilascia la Controls Reference Guide

21 aprile 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl 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 AWSControl Tower User Guide. La Controls Reference Guide copre i controlli in un formato esteso. Per ulteriori informazioni, consulta la AWSControl Tower Controls Controls Reference Guide.

AWSControl Tower aggiorna e rinomina due controlli proattivi

26 marzo 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl 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 da usare TLSv1 .2

Abbiamo aggiornato i nomi dei controlli e gli artefatti di questi due controlli per allinearli alla recente versione di Amazon OpenSearch Service, che ora supporta 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 TLS versione 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 AWS Support.

I controlli obsoleti non sono più disponibili

12 marzo 2024

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl 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

AWSControl Tower supporta l'etichettatura **`EnabledControl`** delle risorse in AWS 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, è possibile aggiungere tag a `EnabledControl` risorse configurabili mediante AWS CloudFormation modelli. In precedenza, era possibile aggiungere tag APIs solo tramite la console AWS Control Tower.

AWSControl Tower `GetEnabledControl` e `EnableControl` le `ListTagsforResource` API operazioni vengono aggiornate con questa versione, poiché si basano sulla funzionalità delle `EnabledControl` risorse.

Per ulteriori informazioni, consulta Tagging `EnabledControl` resources in AWS Control Tower e `EnabledControl`in AWS CloudFormation Guida per l'utente.

AWSControl 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 si abilita una baseline 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 consente controlli opzionali e controlli obbligatori. Durante la chiamataAPIs, potrebbe essere necessario completare un passaggio aggiuntivo per abilitare i controlli opzionali.

Una linea di base AWS di Control Tower incorpora le migliori pratiche per la governance di AWS Control Tower di un'unità organizzativa e degli account dei membri. Ad esempio, quando si abilita una linea di base su un'unità organizzativa, gli account membri all'interno dell'unità organizzativa ricevono un gruppo definito di risorse, tra cui AWS CloudTrail, AWS Config, IAM Identity Center e obbligatorio AWS IAMruoli.

Linee di base specifiche sono compatibili con versioni specifiche AWS delle landing zone di Control Tower. AWSControl Tower può applicare l'ultima 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 elementi 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. Sono APIs inoltre in grado di gestire OUs quelle che sono già gestite dalla AWS Control Tower, in modo da poterti registrare nuovamente OUs dopo gli aggiornamenti delle landing zone. APIsIncludono il supporto per un AWS 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 saperne di piùAPIs, consulta le Baseline nella AWS Control Tower User Guide e nel API Reference. Le nuove APIs sono disponibili in Regioni AWS dove AWS Control Tower è disponibile, ad eccezione delle regioni GovCloud (Stati Uniti). Per un elenco di Regioni AWS dove è disponibile AWS Control Tower, vedi Regione AWS tavolo.

gennaio - dicembre 2023

Nel 2023, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 3)
- AWSControl Tower landing zone versione 3.3
- Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 2)
- AWSControl Tower annuncia i controlli per favorire la sovranità digitale
- AWSControl Tower supporta la landing zone APIs
- AWSControl Tower supporta l'etichettatura per i controlli abilitati
- AWSControl Tower disponibile nella regione Asia Pacifico (Melbourne)
- Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 1)
- Nuovo controllo disponibile API
- AWSControl Tower aggiunge controlli aggiuntivi
- Nuovo tipo di deriva segnalato: accesso affidabile disabilitato
- Quattro aggiuntivi Regioni AWS
- AWSControl Tower disponibile nella regione di Tel Aviv

- AWSControl Tower lancia 28 nuovi controlli proattivi
- AWSControl Tower depreca due controlli
- AWSControl Tower landing zone versione 3.2
- AWSControl Tower gestisce gli account in base all'ID
- Controlli di rilevamento aggiuntivi del Security Hub disponibili nella libreria dei controlli AWS Control Tower
- AWSControl Tower pubblica tabelle di metadati di controllo
- Supporto Terraform per la personalizzazione di Account Factory
- AWS IAMAutogestione dell'Identity Center disponibile per la landing zone
- AWSControl Tower affronta la governance mista per OUs
- Sono disponibili controlli proattivi aggiuntivi
- Controlli EC2 proattivi Amazon aggiornati
- Sette aggiuntive Regioni AWS disponibile
- Tracciamento delle richieste di personalizzazione dell'account Account Factory for Terraform (AFT)
- AWSControl Tower landing zone versione 3.1
- Controlli proattivi generalmente disponibili

Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 3)

14 dicembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower non supporta più Terraform Open Source come tipo di prodotto (blueprint) durante la creazione di nuovi Account AWS. Per ulteriori informazioni e per istruzioni sull'aggiornamento dei blueprint del tuo account, consulta la sezione Transizione al AWS Service Catalog Tipo di prodotto esterno.

Se non aggiorni i blueprint del tuo account per utilizzare il tipo di prodotto esterno, puoi solo aggiornare o chiudere gli account che hai fornito utilizzando i blueprint Terraform Open Source.

AWSControl Tower landing zone versione 3.3

14 dicembre 2023

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.3. Per informazioni, vedereAggiorna 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 implementa negli account, in modo che sia necessario soddisfare una `aws:SourceOrgID` condizione per qualsiasi autorizzazione di scrittura. Con questa versione, AWS i servizi hanno accesso alle risorse dell'utente solo quando la richiesta proviene dall'organizzazione o dall'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 i log per conto degli account all'interno dell'organizzazione nel bucket S3; impedisce ai CloudTrail log esterni all'organizzazione di scrivere nel bucket Control Tower AWS S3.

Abbiamo apportato questa modifica per correggere 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 IAM documentazione e il post del IAM blog intitolato "Use scalable controls for AWS servizi che accedono alle tue risorse».

Aggiornamenti alla politica nella AWS Config SNSargomento

Abbiamo aggiunto la nuova chiave di `aws:SourceOrgID` condizione alla politica per il AWS Config SNSARGOMENTO. Per visualizzare la politica aggiornata, vedere The AWS Config SNSpolitica dell'argomento.

Aggiornamenti alla landing zone Region Deny control

- Rimosso. `discovery-marketplace:` Questa azione è coperta dall'`aws-marketplace:*`esenzione.
- Aggiunto `quicksight:DescribeAccountSubscription`

Aggiornato AWS CloudFormation modello

Abbiamo aggiornato il AWS CloudFormation il modello per lo stack denominato `BASELINE-CLOUDTRAIL-MASTER` in modo che non mostri la deriva quando AWS KMS la crittografia non viene utilizzata.

Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 2)

7 dicembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

HashiCorp ha aggiornato la licenza 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, denominato External.

Per evitare interruzioni dei carichi di lavoro esistenti e AWS risorse nei tuoi account, segui i passaggi di transizione AWS di Control Tower in Transition to the AWS Service Catalog Tipo di prodotto esterno entro il 14 dicembre 2023.

AWSControl 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.)

AWSControl Tower ne annuncia 65 nuovi AWS-controlli gestiti, per aiutarvi a soddisfare i 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 le modifiche delle risorse relative alla residenza dei dati, alla restrizione granulare dell'accesso, alla crittografia e alle funzionalità 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 Require an AWS AppSync APIcache per abilitare la crittografia in transito o Richiedi un AWS Network Firewall da implementare su più zone di disponibilità. Puoi anche personalizzare la regione AWS Control Tower Deny Control per applicare le restrizioni regionali più adatte alle tue esigenze aziendali specifiche.

Questa versione offre funzionalità di negazione della regione AWS Control Tower ben avanzate. 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 del nuovo sistema Region Deny Enhancement, questa versione ne include uno nuovo API`UpdateEnabledControl`, che consente di ripristinare i controlli abilitati alle impostazioni predefinite. Ciò 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 sul nuovoAPI, consulta il AWS Control Tower API Reference

Nuovi controlli proattivi

- CT.APIGATEWAY.PR.6: richiedi un REST dominio Amazon API Gateway per utilizzare una policy di sicurezza che specifichi una versione minima del TLS protocollo di .2 TLSv1
- CT.APPSYNC.PR.2: Richiede un AWS AppSync GraphQL API da configurare con visibilità privata
- CT.APPSYNC.PR.3: Richiedi che un AWS AppSync GraphQL non API è autenticato con chiavi API
- CT.APPSYNC.PR.4: Richiede un AWS AppSync APICache GraphQL per abilitare la crittografia in transito.
- CT.APPSYNC.PR.5: Richiede un AWS AppSync APICache GraphQL per abilitare la crittografia a riposo.
- CT.AUTOSCALING.PR.9: Richiede un EBS volume Amazon configurato tramite una configurazione di avvio di Amazon EC2 Auto Scaling per crittografare i dati inattivi
- CT.AUTOSCALING.PR.10: richiede solo un gruppo Amazon EC2 Auto Scaling per l'uso AWS Tipi di istanze Nitro quando si sovrascrive un modello di avvio
- CT.AUTOSCALING.PR.11: Richiede solo AWS Tipi di istanze Nitro che supportano la crittografia del traffico di rete tra istanze da aggiungere a un gruppo Amazon Auto EC2 Scaling, quando si sovrascrive 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 AWS Database Migration Service (DMS) Endpoint per crittografare le connessioni per gli endpoint di origine e di destinazione
- CT.EC2.PR.15: richiedi un'EC2istanza Amazon per utilizzare un AWS Tipo di istanza Nitro quando si crea dal tipo di `AWS::EC2::LaunchTemplate` risorsa
- CT.EC2.PR.16: richiedi un'EC2istanza Amazon per utilizzare un AWS Tipo di istanza Nitro se creata utilizzando il tipo di `AWS::EC2::Instance` risorsa
- CT.EC2.PR.17: richiede un host EC2 dedicato Amazon per utilizzare un tipo di istanza AWS Nitro
- CT.EC2.PR.18: Richiedi a una EC2 flotta Amazon di sostituire solo i modelli di lancio con AWS Tipi di istanze Nitro

- CT.EC2.PR.19: Richiedi a un'EC2istanza Amazon 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 a una EC2 flotta Amazon di sostituire solo i modelli di lancio con AWS Tipi di istanze Nitro che supportano la crittografia in transito tra 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: Richiedi un broker Amazon MQ ActiveMQ per utilizzare la modalità di distribuzione attiva/standby 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 MSK Kafka () per applicare la crittografia in transito tra i nodi del broker del cluster
- CT.MSK.PR.2: Richiedi che un cluster Amazon Managed Streaming for Apache MSK Kafka () sia configurato con disabilitato PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Richiedi un AWS Firewall di rete: firewall da implementare 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 RDS cluster Amazon non sia configurato per essere accessibile pubblicamente tramite la proprietà PubliclyAccessible "
- CT.RDS.PR.30: Richiedi che un'istanza di RDS database Amazon abbia la crittografia a riposo configurata per utilizzare una KMS chiave 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.1 Richiedi che un AWS AppSync GraphQL API è configurato con visibilità privata

- CT.EC2.PV.1 Richiedi la creazione di EBS uno snapshot Amazon da un volume crittografato EC2
- CT.EC2.PV.2 Richiedi che un EBS volume Amazon collegato sia configurato per crittografare i dati inattivi
- CT.EC2.PV.3 Richiedi che uno EBS snapshot Amazon non possa essere ripristinato pubblicamente
- CT.EC2.PV.4 Richiedi che Amazon EBS Direct APIs non venga chiamato
- CT.EC2.PV.5 Impedisci l'uso dell'importazione e dell'esportazione di Amazon EC2 VM
- CT.EC2.PV.6 Impedisci l'uso di Amazon e azioni obsolete EC2 RequestSpotFleet RequestSpotInstances API
- CT.KMS.PV.1 Richiedi un AWS KMS politica chiave per avere una dichiarazione che limiti la creazione di AWS KMS sovvenzioni a AWS services
- CT.KMS.PV.2 Richiedi che un AWS KMS la chiave asimmetrica con materiale RSA chiave utilizzato per la crittografia non ha una lunghezza di 2048 bit
- CT.KMS.PV.3 Richiedete che un AWS KMS la chiave è configurata con il controllo di sicurezza del blocco della politica di bypass abilitato
- CT.KMS.PV.4 Richiedi che un AWS KMS la chiave gestita dal cliente (CMK) è configurata con materiale chiave proveniente da AWS Cloud HSM
- CT.KMS.PV.5 Richiedi che un AWS KMS la chiave gestita dal cliente (CMK) è configurata con materiale chiave importato
- CT.KMS.PV.6 Richiedi che un AWS KMS la chiave gestita dal cliente (CMK) è configurata con materiale chiave proveniente da un archivio di chiavi esterno () XKS
- CT.LAMBDA.PV.1 Richiede un AWS Lambda funzione URL da usare AWS IAMautenticazione basata
- CT.LAMBDA.PV.2 Richiede un AWS Lambda funzione URL da configurare per l'accesso solo ai responsabili interni Account AWS
- CT. MULTISERVICE.PV.1: nega l'accesso a AWS in base alla richiesta Regione AWS per un'unità organizzativa

I nuovi controlli investigativi che migliorano la vostra posizione di governance della sovranità digitale fanno parte del AWS Security Hub AWSControl Tower Standard con gestione dei servizi.

Nuovi controlli investigativi

- SH.ACM.2: RSA i certificati gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit
- SH.AppSync.5: AWS AppSync GraphQL non APIs deve essere autenticato con chiavi API
- SH.CloudTrail.6: Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico:
- SH.DMS.9: DMS gli endpoint devono utilizzare SSL
- SH.DocumentDB.3: le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche
- SH.DynamoDB.3: i cluster DynamoDB Accelerator DAX () devono essere crittografati quando sono inattivi
- SH.EC2.23: I EC2 Transit Gateway non dovrebbero accettare automaticamente le richieste di allegati VPC
- SH.EKS.1: gli endpoint EKS del cluster non devono essere accessibili al pubblico
- SH.ElastiCache.3: i gruppi di ElastiCache replica devono avere il failover automatico abilitato
- SH.ElastiCache.4: i gruppi di ElastiCache replica avrebbero dovuto essere abilitati encryption-at-rest
- SH.ElastiCache.5: i gruppi di ElastiCache replica avrebbero dovuto essere abilitati encryption-in-transit
- SH.ElastiCache.6: i gruppi di ElastiCache replica delle versioni precedenti di Redis dovrebbero avere Redis abilitato AUTH
- SH.EventBridge.3: i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata
- SH.KMS.4: AWS KMS la rotazione dei tasti deve essere abilitata
- SH.Lambda.3: Le funzioni Lambda devono trovarsi in un VPC
- SH.MQ.5: i broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby
- SH.MQ.6: I broker RabbitMQ devono utilizzare la modalità di distribuzione cluster
- SH.MSK.1: MSK i cluster devono essere crittografati durante il transito tra i nodi broker
- SH.RDS.12: IAM l'autenticazione deve essere configurata per i cluster RDS
- SH.RDS.15: i cluster RDS DB devono essere configurati per più zone di disponibilità
- SH.S3.17: I bucket S3 devono essere crittografati quando sono inattivi con AWS KMS keys

Per ulteriori informazioni sui controlli aggiunti al AWS Security Hub Service-Managed Standard AWS Control Tower vedi i controlli che si applicano a Service-Managed Standard: Control Tower AWS nel AWS Security Hub documentazione.

Per un elenco di Regioni AWS che non supportano determinati controlli che fanno parte del AWS Security Hub Service Managed Standard AWS Control Tower, vedere Regioni non supportate.

Nuovo controllo configurabile per Region Deny a livello di unità organizzativa

CT. MULTISERVICE.PV.1: Questo controllo accetta parametri per specificare le regioni, i IAM principali e le azioni esentati consentiti, a livello di unità organizzativa, anziché per l'intera landing zone della Control TowerAWS. È un controllo preventivo, implementato dalla policy di controllo del servizio (). SCP

Per ulteriori informazioni, consulta Region Deny Control applicato all'unità organizzativa.

La **`UpdateEnabledControl`** API

Questa versione AWS di Control Tower aggiunge il seguente API supporto per i controlli:

- La versione aggiornata `EnableControl` API può configurare controlli configurabili.
- L'aggiornamento `GetEnabledControl` API mostra i parametri configurati su un controllo abilitato.
- Il nuovo `UpdateEnabledControl` API può modificare i parametri su un controllo abilitato.

Per ulteriori informazioni, consulta il AWS Control Tower APIReference.

AWSControl Tower supporta la landing zone APIs

26 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta la configurazione delle landing zone e l'utilizzo del lancioAPIs. Puoi creare, aggiornare, ottenere, elencare, ripristinare ed eliminare le zone di atterraggio utilizzandoAPIs.

Quanto segue ti APIs consente di configurare e gestire la tua landing zone in modo programmatico utilizzando AWS CloudFormation o il AWS CLI.

AWSControl Tower supporta quanto segue APIs per le zone di atterraggio:

- `CreateLandingZone`—Questa API chiamata crea una landing zone utilizzando una versione di landing zone e un file manifest.
- `GetLandingZoneOperation`—Questa API chiamata restituisce lo stato di un'operazione di landing zone specificata.
- `GetLandingZone`—Questa API chiamata restituisce dettagli sulla landing zone specificata, tra cui la versione, il file manifest e lo status.
- `UpdateLandingZone`—Questa API chiamata aggiorna la versione della landing zone o il file manifest.
- `ListLandingZone`—Questa API chiamata restituisce un landing zone identifier (ARN) per una configurazione di landing zone nell'account di gestione.
- `ResetLandingZone`—Questa API chiamata ripristina la landing zone ai parametri specificati nell'ultimo aggiornamento, che può riparare la deriva. Se la landing zone non è stata aggiornata, questa chiamata reimposta la landing zone ai parametri specificati al momento della creazione.
- `DeleteLandingZone`—Questa API chiamata disattiva la landing zone.

Per iniziare con la landing zoneAPIs, consulta ilInizia a usare AWS Control Tower utilizzando APIs.

AWSControl Tower supporta l'etichettatura per i controlli abilitati

10 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta il tagging delle risorse per i controlli abilitati, dalla console AWS Control Tower o tramite. APIs È possibile aggiungere, rimuovere o elencare i tag per i controlli abilitati.

Con la versione seguenteAPIs, puoi configurare i tag per i controlli che abiliti in AWS Control Tower. I tag ti aiutano a gestire, identificare, organizzare, cercare e filtrare le risorse. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri.

AWSControl Tower supporta quanto segue APIs per la codifica di controllo:

- `TagResource`—Questa API chiamata aggiunge tag ai controlli abilitati in AWS Control Tower.
- `UntagResource`—Questa API chiamata rimuove i tag dai controlli abilitati in AWS Control Tower.
- `ListTagsForResource`—Questa API chiamata restituisce i tag per i controlli abilitati in AWS Control Tower.

AWSI controlli Control Tower APIs sono disponibili in Regioni AWS dove è disponibile AWS Control Tower. Per un elenco completo di Regioni AWS in cui è disponibile AWS Control Tower, vedi AWS Tabella delle regioni. Per un elenco completo di AWS Control TowerAPIs, consulta il APIReference.

AWSControl Tower disponibile nella regione Asia Pacifico (Melbourne)

3 novembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower è disponibile nella regione Asia Pacifico (Melbourne).

Se utilizzi già AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione nei tuoi account, vai alla pagina Impostazioni nella dashboard della AWS Control Tower, seleziona la Regione e quindi aggiorna la tua landing zone. Dopo l'aggiornamento della landing zone, devi aggiornare tutti gli account governati da AWS Control Tower, per riportare i tuoi OUs account e riordinarli nella nuova Regione. Per ulteriori informazioni, consulta Informazioni sugli aggiornamenti.

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta Regione AWS Tabella.

Transizione al nuovo AWS Service Catalog Tipo di prodotto esterno (fase 1)

31 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

HashiCorp ha aggiornato la licenza Terraform. Di conseguenza, AWS Service Catalog supporto aggiornato per i prodotti Terraform Open Source e ha fornito prodotti a un nuovo tipo di prodotto, denominato External.

AWSControl Tower non supporta le personalizzazioni di Account Factory che si basano su AWS Service Catalog Tipo di prodotto esterno. Per evitare interruzioni dei carichi di lavoro esistenti e AWS risorse nei tuoi account, segui i passaggi di transizione della AWS Control Tower nell'ordine suggerito, entro il 14 dicembre 2023:

1. Aggiorna il tuo Terraform Reference Engine esistente per AWS Service Catalog per includere il supporto per i tipi di prodotto External e Terraform Open Source. Per istruzioni sull'aggiornamento di Terraform Reference Engine, consulta il AWS Service Catalog GitHub Deposito.

2. Andare su AWS Service Catalog e duplica qualsiasi progetto Terraform Open Source esistente per utilizzare il nuovo tipo di prodotto esterno. Non terminate i progetti Terraform Open Source esistenti.
3. Continua a utilizzare i tuoi progetti Terraform Open Source esistenti per creare o aggiornare gli account in AWS Control Tower.

Nuovo controllo disponibile API

14 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta un componente aggiuntivo API che puoi utilizzare per implementare e gestire i controlli AWS della Control Tower, su larga scala. Per ulteriori informazioni sul AWS controllo Control TowerAPIs, vedere il APIReference.

AWSControl Tower ha aggiunto un nuovo controlloAPI.

- `GetEnabledControl`—La API chiamata fornisce dettagli su un controllo abilitato.

Abbiamo anche aggiornato questoAPI:

`ListEnabledControls`—Questa API chiamata elenca i controlli abilitati da AWS Control Tower sull'unità organizzativa specificata e gli account in essa contenuti. Ora restituisce informazioni aggiuntive in un `EnabledControlSummary` oggetto.

Con questeAPIs, è possibile eseguire diverse operazioni comuni a livello di codice. Per esempio:

- Ottieni un elenco di tutti i controlli che hai abilitato dalla libreria dei controlli AWS Control Tower.
- Per ogni controllo abilitato, puoi ottenere informazioni sulle regioni in cui il controllo è supportato, sull'identificatore del controllo (ARN), sullo stato di deriva del controllo e sul riepilogo dello stato del controllo.

AWSI controlli Control Tower APIs sono disponibili in Regioni AWS dove è disponibile AWS Control Tower. Per un elenco completo di Regioni AWS in cui è disponibile AWS Control Tower, vedi AWS Tabella delle regioni. Per un elenco completo di AWS Control TowerAPIs, consulta il APIReference.

AWSControl Tower aggiunge controlli aggiuntivi

5 ottobre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower annuncia nuovi controlli proattivi e investigativi.

I controlli proattivi in AWS Control Tower sono implementati mediante AWS CloudFormation Hooks, che prima identificavano e bloccavano le risorse non conformi AWS CloudFormation li fornisce. I controlli proattivi completano le funzionalità di controllo preventivo e di rilevamento esistenti in AWS Control Tower.

Nuovi controlli proattivi

- [CT.ATHENA.PR.1] Richiedi un gruppo di lavoro Amazon Athena per crittografare i risultati delle query Athena a riposo
- [CT.ATHENA.PR.2] Richiedi a un gruppo di lavoro Amazon Athena di crittografare i risultati delle query Athena inattivi con un AWS Key Management Service chiave () KMS
- [CT.CLOUDTRAIL.PR.4] Richiede un AWS CloudTrail Lake Event Data Store per abilitare la crittografia a riposo con un AWS KMS Chiave
- [CT.DAX.PR.2] Richiedi un DAX cluster Amazon per distribuire i nodi in almeno tre zone di disponibilità
- [CT.EC2.PR.14] Richiedi un EBS volume Amazon configurato tramite un modello di EC2 avvio Amazon per crittografare i dati inattivi
- [CT.EKS.PR.2] Richiedi che un EKS cluster Amazon sia configurato con crittografia segreta utilizzando AWS Chiavi del servizio di gestione delle chiavi (KMS)
- [CT.ELASTICLOADBALANCING.PR.14] Richiede un Network Load Balancer per attivare il bilanciamento del carico tra zone
- [CT.ELASTICLOADBALANCING.PR.15] Richiede che un gruppo target Elastic Load Balancing v2 non disabiliti esplicitamente il bilanciamento del carico tra zone
- [CT.EMR.PR.1] Richiede che una configurazione di sicurezza Amazon EMR (EMR) sia configurata per crittografare i dati inattivi in Amazon S3
- [CT.EMR.PR.2] Richiedi che una configurazione di sicurezza Amazon EMR (EMR) sia configurata per crittografare i dati inattivi in Amazon S3 con un AWS KMS Chiave

- [CT.EMR.PR.3] Richiede che una configurazione di sicurezza Amazon EMR (EMR) sia configurata con la crittografia del disco locale del EBS volume utilizzando un AWS KMS Chiave
- [CT.EMR.PR.4] Richiedi che una configurazione di sicurezza Amazon EMR (EMR) sia configurata per crittografare i dati in transito
- [CT.GLUE.PR.1] Richiede un AWS Glue job per avere una configurazione di sicurezza associata
- [CT.GLUE.PR.2] Richiede un AWS Glue la configurazione di sicurezza per crittografare i dati nei target Amazon S3 utilizzando AWS KMSchiavi
- [CT.KMS.PR.2] Richiedi che un AWS KMS la chiave asimmetrica con materiale RSA chiave utilizzato per la crittografia ha una lunghezza della chiave superiore a 2048 bit
- [CT.KMS.PR.3] Richiede un AWS KMS politica chiave per avere una dichiarazione che limiti la creazione di AWS KMS sovvenzioni a AWS services
- [CT.LAMBDA.PR.4] Richiede un AWS Lambda autorizzazione al livello per concedere l'accesso a un AWS organizzazione o specifica AWS account
- [CT.LAMBDA.PR.5] Richiedi un AWS Lambda funzione URL da usare AWS IAMautenticazione basata
- [CT.LAMBDA.PR.6] Richiede un AWS Lambda URLCORSpolitica delle funzioni per limitare l'accesso a origini specifiche
- [CT.NEPTUNE.PR.4] Richiede un cluster Amazon Neptune DB per abilitare l'esportazione dei log di CloudWatch Amazon per i log di controllo
- [CT.NEPTUNE.PR.5] Richiedi un cluster Amazon Neptune DB per impostare un periodo di conservazione dei backup maggiore o uguale a sette giorni
- [CT.REDSHIFT.PR.9] Richiede che un gruppo di parametri del cluster Amazon Redshift sia configurato per utilizzare Secure Sockets Layer (SSL) per la crittografia dei dati in transito

Questi nuovi controlli proattivi sono disponibili in commercio Regioni AWS dove è disponibile AWS Control Tower. Per maggiori dettagli su questi controlli, consulta Controlli proattivi. Per maggiori dettagli su dove sono disponibili i controlli, consulta Limitazioni dei controlli.

Nuovi controlli investigativi

Sono stati aggiunti nuovi controlli al Security Hub Service-Managed Standard: AWS Control Tower. Questi controlli ti aiutano a migliorare la tua posizione di governance. Fanno parte del Security Hub Service-Managed Standard: AWS Control Tower, dopo averli abilitati su una specifica unità organizzativa.

- [SH.Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi
- [SH.Neptune.1] I cluster Neptune DB devono essere crittografati a riposo
- [SH.Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch
- [SH.Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche
- [SH.Neptune.4] I cluster Neptune DB devono avere la protezione da eliminazione abilitata
- [SH.Neptune.5] I cluster Neptune DB dovrebbero avere i backup automatici abilitati
- [SH.Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate a riposo
- [SH.Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database abilitata IAM
- [SH.Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee
- [SH.RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi

Il nuovo AWS Security Hub i controlli investigativi sono disponibili nella maggior parte Regioni AWS dove è disponibile AWS Control Tower. Per maggiori dettagli su questi controlli, consulta Controlli che si applicano a Service-Managed Standard: AWS Control Tower. Per ulteriori dettagli su dove sono disponibili i controlli, consulta. Limitazioni di controllo

Nuovo tipo di deriva segnalato: accesso affidabile disabilitato

21 settembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

Dopo aver configurato la landing zone AWS della Control Tower, puoi disabilitare l'accesso affidabile alla AWS Control Tower in AWS Organizations. Tuttavia, così facendo si provoca una deriva.

Con il tipo di deriva affidabile con accesso disabilitato, AWS Control Tower ti avvisa quando si verifica questo tipo di deriva, così puoi riparare la zona di atterraggio della AWS Control Tower. Per ulteriori informazioni, consulta Types of governance drift.

Quattro aggiuntivi Regioni AWS

13 settembre 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower è ora disponibile in Asia Pacifico (Hyderabad), Europa (Spagna e Zurigo) e Medio Oriente (UAE).

Se utilizzi già AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione nei tuoi account, vai alla pagina Impostazioni nella dashboard della AWS Control Tower, seleziona la Regione e quindi aggiorna la tua landing zone. Dopo l'aggiornamento della landing zone, devi aggiornare tutti gli account governati da AWS Control Tower, per riportare i tuoi OUs account e riordinarli nella nuova Regione. Per ulteriori informazioni, consulta Informazioni sugli aggiornamenti.

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta Regione AWS Tabella.

AWSControl Tower disponibile nella regione di Tel Aviv

28 agosto 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower annuncia la disponibilità nella regione di Israele (Tel Aviv).

Se utilizzi già AWS Control Tower e desideri estenderne le funzionalità di governance a questa regione nei tuoi account, vai alla pagina Impostazioni nella dashboard della AWS Control Tower, seleziona la Regione e quindi aggiorna la tua landing zone. Dopo l'aggiornamento della landing zone, devi aggiornare tutti gli account governati da AWS Control Tower, per riportare i tuoi OUs account e riordinarli nella nuova Regione. Per ulteriori informazioni, consulta Informazioni sugli aggiornamenti.

Per un elenco completo delle regioni in cui è disponibile AWS Control Tower, consulta Regione AWS Tabella.

AWSControl Tower lancia 28 nuovi controlli proattivi

24 luglio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower sta aggiungendo 28 nuovi controlli proattivi, per aiutarvi a gestire i AWS ambiente.

I controlli proattivi migliorano le capacità di governance di AWS Control Tower su più account AWS ambienti, bloccando le risorse non conformi prima che vengano fornite. Questi controlli aiutano a gestire AWS servizi come Amazon CloudWatch, Amazon Neptune, Amazon, ElastiCache AWS Step Functions e Amazon DocumentDB. I nuovi controlli ti aiutano a raggiungere obiettivi di controllo come stabilire la registrazione e il monitoraggio, crittografare i dati inattivi o migliorare la resilienza.

Ecco un elenco completo dei nuovi controlli:

- [CT. APPSYNC.PR.1] Richiede un AWS AppSync GraphQL API per abilitare la registrazione
- [CT. CLOUDWATCH.PR.1] Richiedi che un CloudWatch allarme Amazon abbia un'azione configurata per lo stato di allarme
- [CT. CLOUDWATCH.PR.2] Richiedere la conservazione di un gruppo di CloudWatch log Amazon per almeno un anno
- [CT. CLOUDWATCH.PR.3] Richiedi che un gruppo di CloudWatch log Amazon sia crittografato quando è inattivo con un AWS KMSchiave
- [CT. CLOUDWATCH.PR.4] Richiedi l'attivazione di un'azione di CloudWatch allarme Amazon
- [CT. DOCUMENTDB.PR.1] Richiede la crittografia di un cluster Amazon DocumentDB a riposo
- [CT. DOCUMENTDB.PR.2] Richiede un cluster Amazon DocumentDB per abilitare i backup automatici
- [CT. DYNAMODB.PR.2] Richiedi che una tabella Amazon DynamoDB venga crittografata quando è inattiva utilizzando AWS KMS keys
- [CT. EC2.PR.13] Richiedi che un'EC2istanza Amazon abbia abilitato il monitoraggio dettagliato
- [CT. EKS.PR.1] Richiede la configurazione di un EKS cluster Amazon con accesso pubblico disabilitato all'endpoint del server Kubernetes del cluster API
- [CT. ELASTICACHE.PR.1] Richiedi un cluster Amazon ElastiCache for Redis per attivare i backup automatici
- [CT. ELASTICACHE.PR.2] Richiedi l'attivazione degli aggiornamenti automatici delle versioni secondarie di un cluster Amazon ElastiCache for Redis
- [CT. ELASTICACHE.PR.3] Richiede l'attivazione del failover automatico da parte di un gruppo di replica Amazon ElastiCache for Redis
- [CT. ELASTICACHE.PR.4] Richiedere a un gruppo di ElastiCache replica Amazon di attivare la crittografia a riposo
- [CT. ELASTICACHE.PR.5] Richiedere a un gruppo di replica Amazon ElastiCache for Redis di attivare la crittografia in transito
- [CT. ELASTICACHE.PR.6] Richiedi un cluster di ElastiCache cache Amazon per utilizzare un gruppo di sottoreti personalizzato
- [CT. ELASTICACHE.PR.7] Richiedi l'autenticazione Redis di un gruppo di ElastiCache replica Amazon con versioni Redis precedenti AUTH

- [CT. ELASTICBEANSTALK.PR.3] Richiede un AWS Ambiente Elastic Beanstalk per avere una configurazione di registrazione
- [CT. LAMBDA.PR.3] Richiede un AWS Lambda la funzione deve trovarsi in un Amazon Virtual Private Cloud () gestito dal cliente VPC
- [CT. NEPTUNE.PR.1] È necessario disporre di un cluster Amazon Neptune DB AWS Identity and Access Management (IAM) autenticazione del database
- [CT. NEPTUNE.PR.2] Richiede un cluster Amazon Neptune DB per abilitare la protezione da eliminazione
- [CT. NEPTUNE.PR.3] Richiede un cluster Amazon Neptune DB per abilitare la crittografia dello storage
- [CT. REDSHIFT.PR.8] Richiedi la crittografia di un cluster Amazon Redshift
- [CT.S3.PR.9] Richiede che un bucket Amazon S3 abbia S3 Object Lock attivato
- [CT.S3.PR.10] Richiede un bucket Amazon S3 per configurare la crittografia lato server utilizzando AWS KMS keys
- [CT.S3.PR.11] Richiede un bucket Amazon S3 per abilitare il controllo delle versioni
- [CT. STEPFUNCTIONS.PR.1] Richiede un AWS Step Functions state machine per attivare la registrazione
- [CT. STEPFUNCTIONS.PR.2] Richiede un AWS Step Functions macchina statale da avere AWS X-Ray tracciamento attivato

I controlli proattivi in AWS Control Tower sono implementati mediante AWS CloudFormation Hooks, che prima identificavano e bloccavano le risorse non conformi AWS CloudFormation li fornisce. I controlli proattivi completano le funzionalità di controllo preventivo e di rilevamento esistenti in AWS Control Tower.

Questi nuovi controlli proattivi sono disponibili in tutti Regioni AWS dove è disponibile AWS Control Tower. Per maggiori dettagli su questi controlli, consulta Controlli proattivi.

AWSControl Tower depreca due controlli

18 luglio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower effettua revisioni periodiche dei propri controlli di sicurezza per garantire che siano aggiornati e che siano ancora considerati le migliori pratiche. I due controlli seguenti sono

obsoleti a partire dal 18 luglio 2023 e verranno rimossi dalla libreria dei controlli a partire dal 18 agosto 2023. Non puoi più abilitare questi controlli su nessuna unità organizzativa. Puoi scegliere di disattivare questi controlli prima della data di rimozione.

- [SH.S3.4] I bucket S3 devono avere la crittografia lato server abilitata
- [CT.S3.PR.7] Richiede un bucket Amazon S3 per configurare la crittografia lato server

Motivo della deprecazione

A partire da gennaio 2023, Amazon S3 ha configurato la crittografia predefinita su tutti i bucket non crittografati nuovi ed esistenti per applicare la crittografia lato server con chiavi gestite S3 SSE (-S3) come livello base di crittografia per i nuovi oggetti caricati in questi bucket. Non sono state apportate modifiche alla configurazione di crittografia predefinita per un bucket esistente che aveva già la crittografia -S3 o lato server con SSE AWS Servizio di gestione delle chiavi (AWS KMS) tasti (SSE-KMS) configurati.

AWSControl Tower landing zone versione 3.2

16 giugno 2023

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.2. Per informazioni, vedereAggiorna la tua landing zone).

AWSLa versione 3.2 della landing zone di Control Tower include i controlli che fanno parte del AWS Security Hub Service-Managed Standard: AWS Control Tower verso la 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 al servizio (SLR), chiamato. AWSServiceRoleForAWSControlTower Questo ruolo assiste AWS Control Tower creando una regola EventBridge gestita, denominata AWSControlTowerManagedRulein ogni account membro. Questa regola gestita raccoglie AWS Security Hub La ricerca degli eventi, con AWS Control Tower, può determinare la deriva del controllo.

Questa regola è la prima regola gestita creata da AWS Control Tower. La regola non viene distribuita da uno stack; 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 aveva il AWSControlTowerExecutionruolo 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 account multiplo AWS ambiente. 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 e verificare la derivaSNS. Per ulteriori informazioni, consulta AWSServiceRoleForAWSControlTower.

L'aggiornamento landing zone 3.2 include anche una nuova StackSet risorsa nell'account di gestioneBP_BASELINE_SERVICE_LINKED_ROLE, che inizialmente implementa il ruolo collegato ai servizi.

Quando segnala una deriva di controllo del Security Hub (nella landing zone 3.2 e successive), AWS Control Tower riceve un aggiornamento giornaliero dello stato da Security Hub. Sebbene i controlli siano attivi in ogni regione governata, AWS Control Tower invia AWS Security Hub Ricerca di eventi solo nella regione di origine del 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

- AWS Billing and Cost Management (`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.

AWSControl Tower gestisce gli account in base all'ID

14 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora crea e gestisce gli account che crei in Account Factory tracciando il AWS l'ID dell'account, anziché l'indirizzo e-mail dell'account.

Quando si effettua il provisioning di un account, il richiedente dell'account deve sempre disporre delle autorizzazioni `CreateAccount` e delle `DescribeCreateAccountStatus` autorizzazioni. 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.

Controlli di rilevamento aggiuntivi del Security Hub disponibili nella libreria dei controlli AWS Control Tower

12 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ne ha aggiunti dieci nuovi AWS Security Hub controlli investigativi alla libreria dei controlli AWS Control Tower. Questi nuovi controlli riguardano servizi come API Gateway, AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon e SageMaker AWS WAF. Questi nuovi controlli ti aiutano a migliorare la tua posizione di governance soddisfacendo gli obiettivi di controllo, come stabilire la registrazione e il monitoraggio, limitare l'accesso alla rete e crittografare i dati inattivi.

Questi controlli fanno parte del Security Hub Service-Managed Standard: AWS Control Tower, dopo averli abilitati su una specifica unità organizzativa.

- [Sh.account.1] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS

- [SH. APIGateway.8] Le rotte API gateway devono specificare un tipo di autorizzazione
- [SH. APIGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages
- [SH. CodeBuild.3] I log CodeBuild S3 devono essere crittografati
- [SH. EC2.25] i modelli di EC2 avvio non devono assegnare interfacce pubbliche IPs alle interfacce di rete
- [SH. ELB.1] Application Load Balancer deve essere configurato per HTTP reindirizzare tutte le richieste a HTTPS
- [sh.redshift.10] I cluster Redshift devono essere crittografati a riposo
- [SH. SageMaker.2] le istanze dei SageMaker notebook devono essere avviate in modo personalizzato VPC
- [SH. SageMaker.3] Gli utenti non devono avere accesso root alle istanze dei SageMaker notebook
- [SH. WAF.10] Un WAFV2 Web ACL dovrebbe avere almeno una regola o un gruppo di regole

Il nuovo AWS Security Hub i controlli investigativi sono disponibili in tutti Regioni AWS dove è disponibile AWS Control Tower. Per maggiori dettagli su questi controlli, consulta Controlli che si applicano a Service-Managed Standard: AWS Control Tower.

AWSControl Tower pubblica tabelle di metadati di controllo

7 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora fornisce tabelle complete di metadati di controllo come parte della documentazione pubblicata. Quando si lavora con il controlloAPIs, è possibile cercare ogni controllo APIcontrolIdentifier, che è unico ARN associato a ciascuno Regione AWS. Le tabelle includono i framework e gli obiettivi di controllo coperti da ciascun controllo. In precedenza, queste informazioni erano disponibili solo nella console.

Le tabelle includono anche i metadati per i controlli Security Hub che fanno parte del AWS Security Hub Standard gestito dai servizi: AWS Control Tower. Per tutti i dettagli, consulta Tabelle dei metadati di controllo.

Per un elenco abbreviato di identificatori di controllo e alcuni esempi di utilizzo, vedi Identificatori di risorse e controlli. APIs

Supporto Terraform per la personalizzazione di Account Factory

6 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower offre supporto per una singola regione per Terraform tramite Account Factory Customization (). AFC A partire da questa versione, puoi utilizzare AWS Control Tower e Service Catalog insieme, per definire i progetti AFC degli account, in Terraform open source. Puoi personalizzare il tuo nuovo ed esistente Account AWS, prima di effettuare il provisioning delle risorse in AWS Control Tower. Per impostazione predefinita, questa funzionalità ti consente di distribuire e aggiornare gli account, con Terraform, nella tua regione di origine di AWS Control Tower.

Un modello di account descrive le risorse e le configurazioni specifiche richieste quando un Account AWS viene fornito. È possibile utilizzare il blueprint come modello per crearne di più Account AWS su larga scala.

Per iniziare, usa il motore di riferimento Terraform su GitHub. Il Reference Engine configura il codice e l'infrastruttura necessari affinché il motore open source Terraform funzioni con Service Catalog. Questa procedura di configurazione unica richiede alcuni minuti. Successivamente, puoi definire i requisiti del tuo account personalizzato in Terraform e quindi distribuire i tuoi account con il flusso di lavoro di fabbrica degli account AWS Control Tower ben definito. I clienti che preferiscono lavorare con Terraform possono utilizzare la personalizzazione dell'account AWS Control Tower su larga scala e ottenere l'accesso immediato a ciascun account dopo il provisioning. AFC

Per informazioni su come creare queste personalizzazioni, consulta Creazione di prodotti e Introduzione all'open source Terraform nella documentazione del Service Catalog. Questa funzionalità è disponibile in tutti Regioni AWS dove è disponibile AWS Control Tower.

AWS IAMAutogestione dell'Identity Center disponibile per la landing zone

6 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta una scelta opzionale di identity provider per una landing zone della AWS Control Tower, che puoi configurare durante la configurazione o l'aggiornamento. Per impostazione predefinita, è abilitato l'utilizzo della landing zone AWS IAMIdentity Center, in linea con le linee guida sulle migliori pratiche definite in Organizing Your AWS Ambiente che utilizza più account. Ora hai tre alternative:

- È possibile accettare l'impostazione predefinita e consentire a AWS Control Tower di configurare e gestire AWS IAMIdentity Center per te.
- Puoi scegliere di gestirla autonomamente AWS IAMIdentity Center, per riflettere i tuoi requisiti aziendali specifici.
- Facoltativamente, puoi utilizzare e gestire autonomamente un provider di identità di terze parti, collegandolo tramite IAM Identity Center, se necessario. È consigliabile utilizzare l'opzione del provider di identità se l'ambiente normativo richiede l'utilizzo di un provider specifico o se si opera in Regioni AWS dove AWS IAMIdentity Center non è disponibile.

Per ulteriori informazioni, consulta IAMGuida all'Identity Center.

La selezione di provider di identità a livello di account non è supportata. Questa funzione si applica solo alla landing zone nel suo insieme. AWSL'opzione del provider di identità Control Tower è disponibile in tutti Regioni AWS dove è disponibile AWS Control Tower.

AWSControl Tower affronta la governance mista per OUs

1 giugno 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

Con questa versione, AWS Control Tower impedisce l'implementazione dei controlli su un'unità organizzativa (OU), se tale unità organizzativa si trova in uno stato di governance mista. La governance mista si verifica in un'unità organizzativa se gli account non vengono aggiornati dopo che AWS Control Tower ha esteso la governance a una nuova Regione AWS o rimuove la governance. Questa versione consente di garantire la conformità uniforme degli account dei membri di tale unità organizzativa. Per ulteriori informazioni, consulta Evita una governance mista durante la configurazione delle regioni.

Sono disponibili controlli proattivi aggiuntivi

19 maggio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower sta aggiungendo 28 nuovi controlli proattivi per aiutarvi a gestire l'ambiente multi-account e a raggiungere obiettivi di controllo specifici, come la crittografia dei dati inattivi o la limitazione dell'accesso alla rete. I controlli proattivi sono implementati con AWS CloudFormation

ganci che controllano le risorse prima che vengano fornite. I nuovi controlli possono aiutare a governare AWS servizi come Amazon OpenSearch Service, Amazon EC2 Auto Scaling, Amazon, Amazon API Gateway e SageMaker Amazon Relational Database Service (). RDS

I controlli proattivi sono supportati in tutte le applicazioni commerciali Regioni AWS dove è disponibile AWS Control Tower.

OpenSearch Servizio Amazon

- [CT. OPENSEARCH.PR.1] Richiede un dominio Elasticsearch per crittografare i dati inattivi
- [CT. OPENSEARCH.PR.2] Richiedi la creazione di un dominio Elasticsearch in un Amazon specificato dall'utente VPC
- [CT. OPENSEARCH.PR.3] Richiede un dominio Elasticsearch per crittografare i dati inviati tra i nodi
- [CT. OPENSEARCH.PR.4] Richiedi un dominio Elasticsearch per inviare i log degli errori ad Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.5] Richiedi un dominio Elasticsearch per inviare i log di controllo ad Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.6] Richiede che un dominio Elasticsearch disponga del riconoscimento delle zone e di almeno tre nodi dati
- [CT. OPENSEARCH.PR.7] Richiedi che un dominio Elasticsearch abbia almeno tre nodi master dedicati
- [CT. OPENSEARCH.PR.8] Richiede un dominio Elasticsearch Service da utilizzare .2 TLSv1
- [CT. OPENSEARCH.PR.9] Richiedi un dominio Amazon OpenSearch Service per crittografare i dati inattivi
- [CT. OPENSEARCH.PR.10] Richiedi la creazione di un dominio Amazon OpenSearch Service in un Amazon specificato dall'utente VPC
- [CT. OPENSEARCH.PR.11] Richiedi un dominio Amazon OpenSearch Service per crittografare i dati inviati tra i nodi
- [CT. OPENSEARCH.PR.12] Richiedi un dominio Amazon OpenSearch Service per inviare i log degli errori ad Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.13] Richiedi un dominio Amazon OpenSearch Service per inviare i log di controllo ad Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.14] Richiedi che un dominio Amazon OpenSearch Service disponga del riconoscimento delle zone e di almeno tre nodi dati

- [CT. OPENSEARCH.PR.15] Richiedi un dominio Amazon OpenSearch Service per utilizzare un controllo granulare degli accessi
- [CT. OPENSEARCH.PR.16] Richiedi un dominio Amazon OpenSearch Service da usare .2 TLSv1

Amazon EC2 Auto Scaling

- [CT. AUTOSCALING.PR.1] Richiedi che un gruppo Amazon EC2 Auto Scaling disponga di più zone di disponibilità
- [CT. AUTOSCALING.PR.2] Richiede una configurazione di avvio del gruppo Amazon EC2 Auto Scaling per configurare le istanze Amazon per EC2 IMDSv2
- [CT. AUTOSCALING.PR.3] Richiedi una configurazione di avvio di Amazon EC2 Auto Scaling per avere un limite di risposta ai metadati a hop singolo
- [CT. AUTOSCALING.PR.4] Richiedi un gruppo Amazon EC2 Auto Scaling associato a Amazon Elastic Load Balancing () per attivare i controlli di integrità ELB ELB
- [CT. AUTOSCALING.PR.5] Richiede che una configurazione di avvio di un gruppo Amazon EC2 Auto Scaling non contenga istanze Amazon EC2 con indirizzi IP pubblici
- [CT. AUTOSCALING.PR.6] Richiede a qualsiasi gruppo Amazon EC2 Auto Scaling di utilizzare più tipi di istanze
- [CT. AUTOSCALING.PR.8] Richiede un gruppo Amazon EC2 Auto Scaling per configurare i modelli di lancio EC2

Amazon SageMaker

- [CT. SAGEMAKER.PR.1] Richiede un'istanza Amazon SageMaker Notebook per impedire l'accesso diretto a Internet
- [CT. SAGEMAKER.PR.2] Richiede la distribuzione delle istanze di SageMaker notebook Amazon all'interno di un Amazon personalizzato VPC
- [CT. SAGEMAKER.PR.3] Richiede che alle istanze di SageMaker notebook Amazon non sia consentito l'accesso root

Amazon API Gateway

- [CT. APIGATEWAY.PR.5] Richiedi Amazon API Gateway V2 Websocket e HTTP route per specificare un tipo di autorizzazione

Amazon Relational Database Service RDS ()

- [CT. RDS.PR.25] Richiede un cluster di RDS database Amazon per configurare la registrazione

Per ulteriori informazioni, consulta Proactive controls.

Controlli EC2 proattivi Amazon aggiornati

2 maggio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ha aggiornato due controlli proattivi: CT.EC2.PR.3 e CT.EC2.PR.4.

Per l'aggiornamento CT.EC2.PR.3 controllo, qualsiasi AWS CloudFormation una distribuzione che fa riferimento a un elenco di prefissi per una risorsa del gruppo di sicurezza non può essere distribuita, a meno che non sia per la porta 80 o 443.

Per la versione aggiornata CT.EC2.PR.4 controllo, qualsiasi AWS CloudFormation una distribuzione che fa riferimento a un elenco di prefissi per una risorsa del gruppo di sicurezza è bloccata se la porta è 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888.

Sette aggiuntive Regioni AWS disponibile

19 aprile 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower è ora disponibile in sette versioni aggiuntive Regioni AWS: California settentrionale (San Francisco), Asia Pacifico (Hong Kong, Giacarta e Osaka), Europa (Milano), Medio Oriente (Bahrein) e Africa (Città del Capo). Queste regioni aggiuntive per AWS Control Tower, chiamate regioni opt-in, non sono attive per impostazione predefinita, ad eccezione della regione Stati Uniti occidentali (California settentrionale), che è attiva per impostazione predefinita.

Alcuni controlli in AWS Control Tower non funzionano in alcuni di questi controlli aggiuntivi Regioni AWS dove AWS Control Tower è disponibile, perché tali regioni non supportano le funzionalità sottostanti richieste. Per informazioni dettagliate, consultare Limitazioni di controllo.

Tra queste nuove regioni, cFCT non è disponibile in Asia Pacifico (Giacarta e Osaka). Disponibilità in altre Regioni AWS è invariata.

Per ulteriori informazioni su come AWS Control Tower gestisce i limiti delle regioni e dei controlli, vedereConsiderazioni sull'attivazione delle regioni opt-in AWS.

Gli VPCe endpoint richiesti da non AFT sono disponibili nella regione del Medio Oriente (Bahrein). I clienti che effettuano l'implementazione AFT in questa regione devono eseguire la distribuzione con parametri. `aft_vpc_endpoints=false` Per ulteriori informazioni, consulta il parametro nel README file.

AWSControl Tower VPCs ha due zone di disponibilità nella regione Stati Uniti occidentali (California settentrionale)`us-west-1`, a causa di una limitazione in AmazonEC2. Negli Stati Uniti occidentali (California settentrionale), sei sottoreti sono suddivise in due zone di disponibilità. Per ulteriori informazioni, consulta Panoramica di AWS Control Tower e VPC.

AWSControl Tower ha aggiunto nuove autorizzazioni `AWSControlTowerServiceRolePolicy` che consentono a AWS Control Tower di effettuare chiamate verso `EnableRegionListRegions`, e `GetRegionOptStatus` APIs implementate da AWS Servizio di gestione degli account, per renderle aggiuntive Regioni AWS disponibile per i tuoi account condivisi nella landing zone (account di gestione, account di archiviazione dei log, account di audit) e per i tuoi account membro dell'OU. Per ulteriori informazioni, consulta Policy gestite per AWS Control Tower.

Tracciamento delle richieste di personalizzazione dell'account Account Factory for Terraform (AFT)

16 febbraio 2023

AFTsupporta il tracciamento delle richieste di personalizzazione dell'account. Ogni volta che invii una richiesta di personalizzazione dell'account, AFT genera un token di tracciamento univoco che passa attraverso una personalizzazione AFT AWS Step Functions state machine, che registra il token come parte della sua esecuzione. Puoi 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 associati al token, in modo da poter tracciare la richiesta di personalizzazione dell'account durante l'intero flusso di lavoro. AFT Per ulteriori informazioni suAFT, vedere Panoramica di AWS Control Tower Account Factory for Terraform. 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? nel AWS Step Functions Guida per gli sviluppatori

AWSControl Tower landing zone versione 3.1

9 febbraio 2023

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.1. Per informazioni, vedereAggiorna la tua landing zone)

AWSLa versione 3.1 della landing zone 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 AWS Support Piani e AWS Artifact.
- La disattivazione della registrazione degli accessi al server per il bucket di registrazione degli accessi AWS Control Tower fa sì che Security Hub crei una ricerca per il bucket di registrazione degli accessi dell'account Log Archive, a causa di un AWS Security Hub regola, [S3.9] La registrazione degli accessi al server bucket S3 deve essere abilitata. In linea con Security Hub, ti consigliamo di eliminare questo particolare risultato, come indicato nella descrizione di questa regola da parte del Security Hub. Per ulteriori informazioni, consulta 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 maggiori dettagliSCP, consulta Negare l'accesso a AWS in base alla richiesta Regione AWSe controlli che migliorano la protezione della residenza dei dati.

  Servizi globali aggiunti:

  - AWS Account Management (`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:*`)
- IAMIdentity Center (`sso:*`)
- AWS Support App (`supportapp:*`)
- AWS Support Piani (`supportplans:*`)
- AWS Sostenibilità (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- Marketplace AWS Informazioni sui fornitori () `vendor-insights:ListEntitledSecurityProfiles`

Controlli proattivi generalmente disponibili

24 gennaio 2023

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

I controlli proattivi opzionali, precedentemente annunciati in anteprima, sono ora disponibili a tutti. Questi controlli vengono definiti proattivi perché controllano le risorse, prima che le risorse vengano distribuite, per determinare se le nuove risorse sono conformi ai controlli attivati nell'ambiente. Per ulteriori informazioni, consulta I controlli completi aiutano a AWS fornitura e gestione delle risorse.

gennaio - dicembre 2022

Nel 2022, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- Operazioni simultanee sull'account

- Personalizzazione Account Factory () AFC
- I controlli completi aiutano a AWS fornitura e gestione delle risorse
- Lo stato di conformità è visualizzabile per tutti AWS Config rules
- APIper i controlli e un nuovo AWS CloudFormation risorsa
- cFct supporta l'eliminazione dei set di stack
- Conservazione personalizzata dei log
- È disponibile la riparazione della deriva dei ruoli
- AWSControl Tower landing zone versione 3.0
- La pagina Organizzazione combina visualizzazioni e account OUs
- Registrazione e aggiornamento semplificati per gli account dei singoli membri
- AFTsupporta la personalizzazione automatizzata per gli account AWS Control Tower condivisi
- Operazioni simultanee per tutti i controlli opzionali
- Account di sicurezza e registrazione esistenti
- AWSControl Tower landing zone versione 2.9
- AWSControl Tower landing zone versione 2.8

Operazioni simultanee sull'account

16 dicembre 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl 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 di fabbrica consente di personalizzare gli account nuovi ed esistenti direttamente dalla console AWS Control Tower. Queste nuove funzionalità di

personalizzazione offrono la flessibilità necessaria per definire i progetti degli account, che sono AWS 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 da 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 dell'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. È possibile applicare progetti per creare nuovi account, per iscriverne altri AWS account in AWS Control Tower e per aggiornare 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. È inoltre possibile selezionare soluzioni gestite dai partner dal AWS Libreria introduttiva. Per ulteriori informazioni, consulta Personalizza gli account con Account Factory Customization (AFC).

I controlli completi aiutano a AWS fornitura e gestione delle risorse

28 novembre 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta una gestione completa dei controlli, inclusi nuovi controlli proattivi opzionali, implementati tramite AWS CloudFormation ganci. Questi controlli vengono definiti proattivi perché controllano le risorse, prima che le risorse vengano distribuite, per determinare se le nuove risorse saranno conformi ai controlli attivati nell'ambiente.

Oltre 130 nuovi controlli proattivi vi aiutano a raggiungere obiettivi di policy specifici per il vostro ambiente AWS Control Tower, a soddisfare i requisiti dei framework di conformità standard del settore e a governare le interazioni di Control Tower in più di AWS venti altri AWS servizi.

La libreria di controlli AWS Control Tower classifica questi controlli in base ai relativi AWS servizi e risorse. Per ulteriori dettagli, consulta Controlli proattivi.

Con questa versione, AWS Control Tower è integrato anche con AWS Security Hub, tramite il nuovo Security Hub Service-Managed Standard: AWS Control Tower, che supporta AWS Standard Foundational Security Best Practices ()FSBP. Puoi visualizzare oltre 160 controlli Security Hub insieme ai controlli AWS Control Tower nella console e puoi ottenere un punteggio di sicurezza Security Hub per il tuo ambiente AWS Control Tower. Per ulteriori informazioni, consulta Controlli del Security Hub.

Lo stato di conformità è visualizzabile per tutti AWS Config rules

18 novembre 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora mostra lo stato di conformità di tutti AWS Config regole distribuite nelle unità organizzative registrate presso AWS Control Tower. È possibile visualizzare lo stato di conformità di tutti AWS Config regole che influiscono sugli account in AWS Control Tower, registrati o annullati, senza dover uscire dalla console Control TowerAWS. I clienti possono scegliere di configurare le regole di Config, chiamate controlli investigativi, in AWS Control Tower o di configurarle direttamente tramite AWS Config servizio. Le regole implementate da AWS Config vengono mostrate, insieme alle regole implementate da AWS Control Tower.

In precedenza, AWS Config regole implementate tramite AWS Config il servizio non era visibile nella console AWS Control Tower. I clienti dovevano accedere al AWS Config servizio per identificare i casi non conformi AWS Config regole. Ora puoi identificare qualsiasi non conforme AWS Config regola all'interno della console AWS Control Tower. Per visualizzare lo stato di conformità di tutte le regole di Config, vai 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 AWS Control Tower e Config distribuite all'esterno di Control TowerAWS.

APIper i controlli e un nuovo AWS CloudFormation risorsa

1 settembre 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora supporta la gestione programmatica dei controlli, noti anche come guardrail, tramite una serie di chiamate. API Una nuova AWS CloudFormation la risorsa supporta la API funzionalità 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. APIsIncludono il supporto per AWS CloudFormation, in modo da poterlo gestire AWS risorse come infrastructure-as-code (IaC). AWSControl Tower offre controlli preventivi e investigativi opzionali che esprimono le intenzioni politiche riguardanti un'intera unità organizzativa (OU) e ogni AWS account all'interno dell'unità organizzativa. Queste regole rimangono in vigore anche quando si creano nuovi account o si apportano modifiche agli account esistenti.

APIsincluso in questa versione

- EnableControl— Questa API chiamata attiva un controllo. Avvia un'operazione asincrona che crea AWS risorse sull'unità organizzativa specificata e sugli account in essa contenuti.
- DisableControl— Questa API chiamata disattiva un controllo. Avvia un'operazione asincrona che elimina AWS risorse sull'unità organizzativa specificata e sugli account in essa contenuti.
- GetControlOperation— Restituisce lo stato di un particolare EnableControlo di DisableControlun'operazione.
- ListEnabledControls— Elenca i controlli abilitati da AWS Control Tower sull'unità organizzativa specificata e gli account in essa contenuti.

Per visualizzare un elenco di nomi di controllo per i controlli opzionali, consulta Identificatori di risorse APIs e controlli nella AWSControl Tower User Guide.

cFct supporta l'eliminazione dei set di stack

26 agosto 2022

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

Customizations for AWS Control Tower (cFCT) ora supporta l'eliminazione degli stack set, impostando un parametro nel file. `manifest.yaml` Per ulteriori informazioni, consulta Eliminazione di un set di stack.

> **Important**
>
> Quando inizialmente impostate il valore di `enable_stack_set_deletion` to`true`, la volta successiva che richiamate cfCT, ALLle risorse che iniziano con il prefisso`CustomControlTower-`, che hanno il tag chiave associato e che non sono dichiarate nel file manifest`Key:AWS_Solutions, Value: CustomControlTowerStackSet`, vengono eliminate.

Conservazione personalizzata dei log

15 agosto 2022

(Aggiornamento richiesto per la landing zone AWS del Control Tower. Per informazioni, vedereAggiorna la tua landing zone)

AWSControl Tower ora offre la possibilità di personalizzare la politica di conservazione per i bucket Amazon S3 che archiviano i log della 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 il processo di configurazione della 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.)

AWSControl 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.

AWSControl Tower landing zone versione 3.0

29 luglio 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 3.0. Per informazioni, vedereAggiorna la tua landing zone)

AWSLa versione 3.0 della landing zone Control Tower include i seguenti aggiornamenti:

- La possibilità di scegliere il livello di organizzazione AWS CloudTrail sentieri, o per rinunciare ai CloudTrail sentieri gestiti da AWS Control Tower.

- Due nuovi controlli investigativi per determinare se AWS CloudTrail sta registrando l'attività nei tuoi account.
- L'opzione di aggregazione AWS Config informazioni sulle risorse globali solo nella tua regione d'origine.
- Un aggiornamento della Region Deny Control.
- Un aggiornamento della politica gestita, AWSControlTowerServiceRolePolicy.
- Non creiamo più il IAM ruolo `aws-controltower-CloudWatchLogsRole` e il gruppo di CloudWatch log `aws-controltower/CloudTrailLogs` in ogni account registrato. In precedenza, li creavamo in ogni account come traccia degli account. 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 Control Tower AWS

Con la versione 3.0 di landing zone, AWS Control Tower ora supporta il livello di organizzazione AWS CloudTrail sentieri.

Quando aggiorni la landing zone AWS di Control Tower alla versione 3.0, hai la possibilità di selezionare il livello dell'organizzazione AWS CloudTrail sentieri come preferenza di registrazione o per 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. AWSControl 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 percorso a livello di organizzazione, potresti incorrere in addebiti duplicati per i percorsi 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 gestisce. 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 è possibile 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 le informazioni di registrazione a quella posizione. Se scegli di disattivare i percorsi gestiti da AWS Control Tower, i log esistenti rimangono nel secchio, 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 i CloudTrail percorsi a livello di organizzazione è diverso dal percorso predefinito per un percorso a livello di organizzazione creato manualmente, che avrebbe la forma seguente:

- `/AWSLogs/org id/…`

Per ulteriori informazioni sulla denominazione dei percorsi, vedi Ricerca dei file di registro CloudTrail . CloudTrail

> **Tip**
>
> Se hai intenzione di creare e gestire percorsi a livello di account, ti consigliamo di creare i nuovi percorsi prima di completare l'aggiornamento alla versione 3.0 della landing zone di AWS Control Tower, per iniziare subito 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, a livello di account AWS CloudTrail i trail non sono supportati da AWS Control Tower. Puoi creare e gestire i tuoi percorsi a livello di account in qualsiasi momento oppure puoi optare per percorsi a livello di organizzazione gestiti da Control Tower. AWS

Registra AWS Config risorse solo nella regione d'origine

Nella versione 3.0 della landing zone, AWS Control Tower ha aggiornato la configurazione di base per AWS Config in modo che registri le risorse globali solo nella regione d'origine. Dopo l'aggiornamento alla versione 3.0, la registrazione delle risorse per le risorse globali è abilitata solo nella tua regione di origine.

Questa configurazione è considerata una procedura consigliata. È consigliata da AWS Security Hub e AWS Config e 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, è stato creato un elemento di configurazione per ogni elemento in ogni regione governata.

Due nuovi controlli investigativi per AWS CloudTrail disboscamento

Come parte del passaggio al livello di organizzazione AWS CloudTrail trail, AWS Control Tower sta introducendo due nuovi controlli investigativi che controllano 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 di sicurezza dispongono di AWS CloudTrail o CloudTrail Lake è abilitato

Controllo fortemente consigliato: rileva se un account ha AWS CloudTrail o CloudTrail Lake 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 AWS della 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 della AWS Control Tower esistente alla Landing Zone 3.

La pagina Organizzazione combina visualizzazioni e account OUs

18 luglio 2022

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

La nuova pagina Organizzazione in AWS Control Tower mostra una visualizzazione gerarchica di tutte le unità organizzative (OUs) e gli account. Combina le informazioni delle pagine OUse Account, che esistevano in precedenza.

Nella nuova pagina, puoi vedere le relazioni tra i genitori OUs e i relativi nidificati 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.

Registrazione e aggiornamento semplificati per gli account dei singoli membri

31 maggio 2022

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora ti offre una migliore capacità di aggiornare e registrare gli account dei membri individualmente. Ogni account mostra quando è disponibile per un aggiornamento, così puoi assicurarti più facilmente che i tuoi account membro includano la configurazione più recente. Puoi aggiornare la landing zone, porre rimedio alla deriva dell'account o registrare un account in un'unità organizzativa registrata in pochi passaggi semplificati.

Quando aggiorni un account, non è necessario includere l'intera unità organizzativa (OU) di un account in ogni azione di aggiornamento. Di conseguenza, il tempo necessario per aggiornare un singolo account si riduce notevolmente.

Puoi registrare gli account in AWS Control Tower OUs con l'aiuto della console AWS Control Tower. Gli account esistenti registrati a AWS Control Tower devono comunque soddisfare i prerequisiti dell'account e devi aggiungere il `AWSControlTowerExecution` ruolo. Quindi, puoi scegliere qualsiasi unità organizzativa registrata e registrare l'account selezionando il pulsante Registra.

Abbiamo separato la funzionalità Registra account dal flusso di lavoro Crea account in account factory, per distinguere meglio questi processi simili e aiutarti a evitare errori di configurazione quando inserisci le informazioni sull'account.

AFTsupporta la personalizzazione automatizzata per gli account AWS Control Tower condivisi

27 maggio 2022

(Non è richiesto alcun aggiornamento per la landing zone AWS di 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 controllo e l'account di archiviazione dei log, insieme agli account registrati. Potete centralizzare la

personalizzazione dell'account e la gestione degli aggiornamenti, proteggendo al contempo la sicurezza delle configurazioni degli account, poiché siete voi a definire il ruolo che svolge il lavoro.

Il AWSAFTExecutionruolo esistente ora implementa personalizzazioni in tutti gli account. È possibile impostare IAM autorizzazioni con limiti che limitano l'accesso al AWSAFTExecutionruolo in base ai requisiti aziendali e di sicurezza. Puoi anche delegare a livello di codice le autorizzazioni di personalizzazione approvate in quel ruolo, per utenti fidati. Come procedura consigliata, si consiglia di limitare le autorizzazioni a quelle necessarie per implementare le personalizzazioni richieste.

AFTora crea il nuovo AWSAFTServiceruolo per distribuire AFT le risorse in tutti gli account gestiti, inclusi gli account condivisi e l'account di gestione. Le risorse in precedenza venivano utilizzate dal ruolo. AWSAFTExecution

Il provisioning degli account condivisi e di gestione di AWS Control Tower non viene fornito tramite Account Factory, quindi non dispongono di prodotti forniti corrispondenti in 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

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl 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 quando AWS Control Tower è in fase di configurazione della landing zone o sta estendendo la 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 diversiOUs, 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 riscontrare questi miglioramenti della concorrenza di controllo in tutte le versioni rilasciate di AWS Control Tower.

Quando si applicano controlli preventivi a nestedOUs, 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 le Service Control Policies (SCPs), che fanno parte di AWS Organizations. I controlli Detective sono 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 su come ogni account è conforme alle politiche abilitate. Per un elenco completo dei controlli disponibili, consulta la libreria di controlli The AWS Control Tower.

Account di sicurezza e registrazione esistenti

16 maggio 2022

(Disponibile durante la configurazione iniziale.)

AWSControl Tower ora offre la possibilità di specificare un esistente AWS account come account di sicurezza o di registrazione 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 API attività e delle configurazioni delle risorse di tutti gli account nella landing zone.

Integrando gli account di sicurezza e registrazione esistenti, è più facile estendere la governance AWS della Control Tower alle organizzazioni esistenti o passare a 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. AWSControl 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 aggiungerne di esistenti AWS account in AWS Control Tower come account di controllo e archiviazione dei log e se tali account esistono AWS Config risorse, è necessario eliminare quelle esistenti AWS Config risorse prima di poter registrare gli account in AWS Control Tower.

AWSControl Tower landing zone versione 2.9

22 aprile 2022

(Aggiornamento richiesto per la landing zone AWS di Control Tower alla versione 2.9. Per informazioni, vedereAggiorna la tua landing zone)

AWSLa versione 2.9 della landing zone di 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.

AWSControl Tower landing zone versione 2.8

10 febbraio 2022

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.8. Per informazioni, vedereAggiorna la tua landing zone)

AWSLa versione 2.8 della zona di atterraggio Control Tower aggiunge funzionalità in linea con i recenti aggiornamenti di AWS Best practice di sicurezza di base.

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 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 modo che corrispondano AWS Config migliori pratiche. I clienti che non effettuano l'upgrade continueranno a utilizzare il ruolo esistente.
- Questa versione semplifica il processo di KMS configurazione AWS Control Tower per la crittografia. AWS Config dati e migliora la relativa messaggistica di stato in. CloudTrail
- La versione include un aggiornamento del Region Deny Control, per consentire l'utilizzo della `route53-application-recovery` funzionalità. `us-west-2`
- Aggiornamento: il 15 febbraio 2022, abbiamo rimosso la coda delle lettere morte per AWS Funzioni Lambda.

Ulteriori dettagli:

- Se disattivate la vostra landing zone, AWS Control Tower non rimuove il AWS Config ruolo legato al servizio.
- Se si elimina il provisioning di un account Account Factory, AWS Control Tower non rimuove il AWS Config ruolo collegato al 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 gestiti da AWS Control Tower, come indicato inGestione degli aggiornamenti della 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
- AWSControl Tower introduce il provisioning e la personalizzazione degli account Terraform
- Nuovo evento sul ciclo di vita disponibile
- AWSControl Tower consente il nested OUs
- Detective controlla la concorrenza
- Sono disponibili due nuove regioni
- Deselezione della regione
- AWSControl Tower funziona con AWS Sistemi di gestione delle chiavi
- Controlli rinominati, funzionalità invariata
- AWSControl Tower esegue scansioni SCPs giornaliere per verificare eventuali deviazioni
- Nomi e account personalizzati OUs
- AWSControl Tower landing zone versione 2.7
- Tre nuove AWS Regioni disponibili
- Governa solo le regioni selezionate
- AWSControl Tower ora estende la governance all'esistenza OUs nel tuo AWS organizations
- AWSControl Tower fornisce aggiornamenti collettivi degli account

Funzionalità di negazione della regione

30 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone di AWS Control Tower.)

AWSControl Tower ora offre funzionalità Region Deny, che aiutano a limitare l'accesso a AWS servizi e operazioni per gli account registrati nell'ambiente AWS Control Tower. La funzione Region Deny integra le funzioni di selezione della regione e di deselezione della regione esistenti in Control TowerAWS. Insieme, queste funzionalità consentono di 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 a AWS servizi in regioni al di fuori della regione di Francoforte. Puoi selezionare Regioni con restrizioni durante il processo di configurazione del AWS Control Tower o nella pagina delle impostazioni della zona di atterraggio. La funzione Region Deny è disponibile quando aggiorni la versione della landing zone AWS di Control Tower. Select AWS i 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 AWS di Control Tower)

AWSControl Tower ora offre controlli appositamente progettati per garantire che tutti i dati dei clienti vengano caricati su AWS i servizi si trovano solo nel AWS Regioni specificate. È possibile selezionare AWS Regione o regioni in cui i dati dei clienti vengono archiviati ed elaborati. Per un elenco completo di AWS Regioni in cui è disponibile AWS Control Tower, vedi AWS Tabella delle 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 È possibile visualizzare lo stato di conformità dei controlli nella console AWS Control Tower. Per un elenco completo dei controlli disponibili, consulta la libreria di controlli The AWS Control Tower.

AWSControl Tower introduce il provisioning e la personalizzazione degli account Terraform

29 novembre 2021

(Aggiornamento opzionale per la landing zone AWS di Control Tower)

Ora puoi utilizzare Terraform per fornire e aggiornare account personalizzati tramite AWS Control Tower, con AWSControl Tower Account Factory for Terraform (). AFT

AFTfornisce un'unica pipeline Terraform infrastructure as code (IaC), che fornisce gli account gestiti da Control TowerAWS. 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 AFT automatica degli account 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, fornite da AFT AWS per personalizzazioni comuni.

Inizia a usare AWS Control Tower Account Factory for Terraform seguendo i passaggi forniti nella AWSControl Tower User Guide e scaricando AFT per la tua istanza Terraform. Implementa AWS Control Tower Account Factory per Terraform () AFT AFTsupporta 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 AWS di Control Tower)

L'`PrecheckOrganizationalUnit`evento registra se alcune risorse impediscono l'esito positivo dell'attività Extend governance, incluse le risorse in OUs nested. Per ulteriori informazioni, consulta `PrecheckOrganizationalUnit`.

AWSControl Tower consente il nested OUs

16 novembre 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora ti consente di includere i nidificati OUs come parte della tua landing zone.

AWSControl 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. È possibile registrare contenuti OUs annidatiOUs, creare e registrare OUs sotto la voce principale e

abilitare i controlli su qualsiasi unità organizzativa registrataOUs, indipendentemente dalla profondità. Per supportare questa funzionalità, la console mostra il numero di account gestiti eOUs.

Con nestedOUs, puoi allineare la tua AWS Control Tower OUs al AWS grazie a una strategia multi-account, puoi ridurre il tempo necessario per abilitare i controlli su più accountOUs, applicando i controlli a livello dell'unità organizzativa principale.

Considerazioni chiave

1. È possibile registrare un'unità organizzativa esistente a più livelli OUs con AWS Control Tower un'unità organizzativa alla volta, iniziando dall'unità organizzativa di livello superiore e poi procedendo verso il basso. Per ulteriori informazioni, consulta Espandi da una struttura OU piatta a una struttura di unità organizzative annidata.
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. Controlli investigativi (AWS Le regole di Config) vengono NOT ereditate automaticamente.
5. La conformità ai controlli investigativi viene segnalata da ciascuna unità organizzativa.
6. SCPla deriva su un'unità organizzativa si ripercuote su tutti gli OUs account e su di essa.
7. Non è possibile crearne di nuovi annidati OUs nell'unità organizzativa di sicurezza (Core OU).

Detective controlla la concorrenza

5 novembre 2021

(Aggiornamento opzionale per la landing zone AWS di Control Tower)

AWSI controlli investigativi Control Tower ora supportano operazioni simultanee per i controlli investigativi, migliorando la facilità d'uso e le prestazioni. È possibile 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 MFA per l'utente root è abilitato 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 dispositivi OUs contemporaneamente 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 deselezione della regione, disponibili nella versione più recente.

Sono disponibili due nuove regioni

29 luglio 2021

(Aggiornamento richiesto per la landing zone AWS del Control Tower)

AWSControl Tower è ora disponibile in due versioni aggiuntive AWS Regioni: 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 AWS Control Tower in una o più regioni supportate, vai alla pagina Impostazioni della Landing Zone nella dashboard AWS Control Tower, quindi seleziona le Regioni. Dopo aver aggiornato la landing zone, devi aggiornare tutti gli account gestiti da AWS Control Tower.

Deselezione della regione

29 luglio 2021

(Aggiornamento opzionale per la landing zone AWS di Control Tower)

AWSLa deselezione della regione Control Tower migliora la capacità di gestire l'impronta geografica delle risorse della AWS Control Tower. Puoi deselezionare le Regioni che non vuoi più governare da AWS Control Tower. Questa funzionalità offre la possibilità di risolvere i problemi di conformità e normativi, bilanciando al contempo i costi associati all'espansione in altre regioni.

La deselezione della regione è disponibile quando aggiorni la versione della landing zone AWS di 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, Control Tower implementa le sue funzionalità di governance, che includono registrazione, monitoraggio e AWS 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 implementare AWS risorse o carichi di lavoro in tali regioni.

AWSControl Tower funziona con AWS Sistemi di gestione delle chiavi

28 luglio 2021

(Aggiornamento opzionale per la landing zone AWS di Control Tower)

AWSControl Tower offre la possibilità di utilizzare un AWS Servizio di gestione delle chiavi (AWS KMS) chiave. Una chiave viene fornita e gestita dall'utente per proteggere i servizi distribuiti da AWS Control Tower, tra cui AWS CloudTrail, AWS Config e i dati Amazon S3 associati. AWS KMSla crittografia è un livello di crittografia avanzato rispetto alla crittografia SSE -S3 utilizzata di default da AWS Control Tower.

L'integrazione di AWS KMSil supporto in AWS Control Tower è in linea con AWS Buone pratiche di sicurezza di base, che consigliano un ulteriore livello di sicurezza per i file di registro sensibili. Dovresti usare AWS KMS—chiavi gestite (SSE-KMS) per la crittografia a riposo. AWS KMSil supporto per la crittografia è disponibile quando si configura una nuova landing zone o quando si aggiorna la landing zone esistente AWS della Control Tower.

Per configurare questa funzionalità, puoi selezionare KMSKey Configuration durante la configurazione iniziale della landing zone. Puoi scegliere una KMS chiave esistente oppure puoi selezionare un pulsante che ti indirizza al AWS KMSconsole per crearne una nuova. Hai anche la flessibilità di passare dalla crittografia predefinita a SSE - KMS o a una KMS chiave diversaSSE.

Per una landing zone esistente di AWS Control Tower, puoi eseguire un aggiornamento per iniziare a utilizzare AWS KMSchiavi.

Controlli rinominati, funzionalità invariata

26 luglio 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower sta rivedendo alcuni nomi e descrizioni dei controlli per riflettere 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.

AWSControl Tower esegue scansioni SCPs giornaliere per verificare eventuali deviazioni

11 maggio 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora esegue scansioni automatiche giornaliere dei gestori SCPs per verificare che i controlli corrispondenti siano applicati correttamente e che non abbiano subito deviazioni. Se una scansione rileva una deviazione, riceverai una notifica. AWSControl 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 oggetto di deriva.

Nomi e account personalizzati OUs

16 aprile 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora ti 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 ai AWS linee guida sulle migliori pratiche per più account. Tuttavia, se l'azienda ha politiche di denominazione specifiche o se dispone già di un'unità organizzativa o di un account esistente con lo stesso nome consigliato, la nuova funzionalità di denominazione dell'unità organizzativa e degli account 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 con la situazione generale AWS linee guida sulle migliori pratiche per la denominazione.

I nuovi clienti vedranno questi nuovi nomi di unità organizzative. I clienti esistenti continueranno a vederne i nomi originaliOUs. 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 dal AWS Console di gestione, vai alla console AWS Control Tower e seleziona Configura landing zone in alto a destra. Per ulteriori informazioni, puoi leggere come pianificare la tua landing zone AWS della Control Tower.

AWSControl Tower landing zone versione 2.7

8 aprile 2021

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.7. Per informazioni, vedereAggiorna la tua landing zone)

Con la versione 2.7 di AWS Control Tower, AWS Control Tower introduce quattro nuovi controlli preventivi obbligatori di archiviazione dei log 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 a AWS Control Tower.

I quattro controlli modificati possono essere utilizzati insieme ai nuovi controlli obbligatori per fornire la governance a un insieme più ampio di AWS Archivi di registro. 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 vengono distribuiti da Control Tower. AWS

Nuovi controlli obbligatori:

- Impedisci modifiche alla configurazione di crittografia per i bucket S3 creati da AWS Control Tower nell'archivio dei registri
- Impedisci modifiche alla configurazione di registrazione per i bucket S3 creati da AWS Control Tower in Log Archive
- Impedisci modifiche alla policy sui bucket per i bucket S3 creati da AWS Control Tower in Log Archive
- Impedisci 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]

AWSLa versione 2.7 di Control Tower include modifiche al blueprint della zona di atterraggio AWS Control Tower che possono causare incompatibilità con le versioni precedenti dopo l'aggiornamento alla 2.7.

- In particolare, la versione 2.7 AWS di Control Tower abilita `BlockPublicAccess` automaticamente i bucket S3 distribuiti da Control TowerAWS. 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.

- AWSLa versione 2.7 di Control Tower include un requisito perHTTPS. Tutte le richieste inviate ai bucket S3 distribuiti da AWS Control Tower devono utilizzare secure socket layer (). SSL Solo HTTPS le richieste possono essere inoltrate. Se utilizzi HTTP (withoutSSL) 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 invece diHTTP.

Tre nuove AWS Regioni disponibili

8 aprile 2021

(Aggiornamento richiesto per la landing zone AWS del Control Tower)

AWSControl Tower è disponibile in tre versioni aggiuntive AWS Regioni: 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 AWS di Control Tower)

AWSLa selezione della regione Control Tower offre una migliore capacità di gestire l'impronta geografica delle risorse della AWS Control Tower. Per ampliare il numero di regioni in cui offri ospitalità AWS risorse o carichi di lavoro, per motivi di conformità, normative, di costo o di altro tipo, ora puoi selezionare le regioni aggiuntive da gestire.

La selezione della regione è disponibile quando configuri una nuova landing zone o aggiorni la versione della landing zone AWS Control Tower. Quando si utilizza Account Factory per creare un

nuovo account o registrare un account membro preesistente, o quando si utilizza Extend Governance per registrare gli account in un'unità organizzativa preesistente, Control Tower AWS implementa le sue funzionalità di governance di registrazione, monitoraggio e controlli centralizzati nelle Regioni prescelte negli account. Per ulteriori informazioni sulla selezione delle regioni, vedere. Configura le tue regioni AWS Control Tower

AWSControl Tower ora estende la governance all'esistenza OUs nel tuo AWS organizations

28 gennaio 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

Estendi la governance alle unità organizzative esistenti (OUs) (quelle non presenti nella AWS Control Tower) dall'interno della console AWS Control Tower. Con questa funzionalità, puoi portare gli account di primo livello OUs e quelli 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 si registra 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, vedere. 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 a usare AWS Control Tower per YouTube AWS Organizations.

AWSControl Tower fornisce aggiornamenti collettivi degli account

28 gennaio 2021

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

Con la funzionalità di aggiornamento in blocco, ora puoi aggiornare tutti gli account di un account registrato AWS Organizations unità organizzativa (OU) contenente fino a 300 account, con un solo clic, dalla dashboard 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 consente inoltre di mantenere aggiornati gli account quando si aggiorna la landing zone di AWS Control Tower per espanderla in nuove regioni o quando si desidera registrare nuovamente un'unità organizzativa per assicurarsi che a tutti gli account in quella 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, vedereAggiorna 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:

- AWSLa console Control Tower ora si collega a una console esterna AWS Regole di configurazione
- AWSControl Tower ora disponibile in altre regioni
- Aggiornamento Guardrail
- AWSLa console Control Tower mostra maggiori dettagli sugli OUs account
- Usa AWS Control Tower per configurare un nuovo account multiplo AWS ambienti in AWS Organizations
- Personalizzazioni per la soluzione AWS Control Tower
- Disponibilità generale della versione 2.3 di AWS Control Tower
- Provisioning degli account in un'unica fase in AWS Control Tower
- AWSStrumento di smantellamento Control Tower
- AWSNotifiche degli eventi relativi al ciclo di vita del Control Tower

AWSLa console Control Tower ora si collega a una console esterna AWS Regole di configurazione

29 dicembre 2020

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.6. Per informazioni, vedereAggiorna la tua landing zone)

AWSControl Tower ora include un aggregatore a livello di organizzazione, che aiuta a rilevare elementi esterni AWS Regole di Config. Ciò fornisce la visibilità nella console AWS Control Tower per vedere l'esistenza di elementi creati esternamente AWS Regole di Config oltre a quelle AWS Regole di configurazione create da AWS Control Tower. L'aggregatore consente a AWS Control Tower di rilevare regole esterne e fornire un collegamento a AWS Config console senza la necessità che AWS Control Tower acceda 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 si aggrega AWS Control Tower AWS Config regole negli account non gestitiOUs.

AWSControl Tower ora disponibile in altre regioni

18 novembre 2020

(Aggiornamento richiesto per la landing zone di AWS Control Tower alla versione 2.5. Per informazioni, vedereAggiorna la tua landing zone)

AWSControl Tower è ora disponibile in 5 versioni aggiuntive AWS Regioni:

- Regione Asia Pacifico (Singapore)
- Regione Europa (Francoforte)
- Regione Europa (Londra)
- Regione Europa (Stoccolma)
- Regione Canada (Centrale)

L'aggiunta di queste 5 AWS Regions è l'unica modifica introdotta per la versione 2.5 di AWS Control Tower.

AWSControl Tower è disponibile anche nella regione Stati Uniti orientali (Virginia settentrionale), nella regione degli Stati Uniti orientali (Ohio), nella regione degli 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 a AWS Control Tower per governare nei 10 supportati AWS Regioni. Per informazioni, consultare Configura le tue regioni AWS Control Tower.

Aggiornamento Guardrail

8 ottobre 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di 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, vedere Impedire modifiche a AWS IAMRuoli impostati da AWS Control Tower e AWS CloudFormationnella AWS Control Tower Controls Reference Guide.

AWSLa console Control Tower mostra maggiori dettagli sugli OUs account

22 luglio 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di 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 sul tuo AWS conti 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 tra tutte le tabelle.

Usa AWS Control Tower per configurare un nuovo account multiplo AWS ambienti in AWS Organizations

22 aprile 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di 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:

- Esistenti AWS Organizations i clienti 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.

AWSControl 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 proprio account multiplo nuovo o esistente AWS ambiente e governo 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 fornirne di nuovi AWS contabilizza rapidamente, senza indebite preoccupazioni sulla conformità.

Per informazioni sulla configurazione di una landing zone, vederePianifica la tua landing zone della AWS Control Tower. Puoi anche visitare la pagina web del prodotto AWS Control Tower o guardare questo video su come iniziare a usare AWS Control Tower per YouTube AWS Organizations.

Oltre a questa modifica, la funzionalità Quick Account Provisioning in AWS Control Tower è stata rinominata Account Enroll. Ora consente la registrazione di file esistenti AWS account e creazione di nuovi account. Per ulteriori informazioni, consulta Registra un account esistente.

Personalizzazioni per la soluzione AWS Control Tower

17 marzo 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora include una nuova implementazione di riferimento che semplifica l'applicazione di modelli e policy personalizzati alla landing zone AWS della Control Tower.

Con le personalizzazioni per AWS Control Tower, puoi usare AWS CloudFormation modelli per distribuire nuove risorse agli account esistenti e nuovi all'interno dell'organizzazione. È inoltre possibile applicare politiche 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 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 l'implementazione delle risorse rimanga sincronizzata con la landing zone.

La documentazione di implementazione per questa architettura di soluzione AWS Control Tower è disponibile tramite AWS Pagina web delle soluzioni.

Disponibilità generale della versione 2.3 di AWS Control Tower

5 marzo 2020

(Aggiornamento richiesto per la landing zone AWS del Control Tower. Per informazioni, vedereAggiorna la tua landing zone.)

AWSControl Tower è ora disponibile nella regione Asia-Pacifico (Sydney) AWS Regione, oltre alle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon) ed Europa (Irlanda). L'aggiunta della regione Asia Pacifico (Sydney) è l'unica modifica introdotta per la versione 2.3 di AWS Control Tower.

Se non hai mai utilizzato AWS Control Tower in precedenza, puoi avviarlo oggi stesso in una qualsiasi delle regioni supportate. Se 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 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 AWS della Control Tower in regioni in cui non hai bisogno di carichi di lavoro per funzionare.

Per informazioni sul comportamento previsto dei controlli investigativi a seguito di una distribuzione in una nuova regione, consulta Configura le regioni del AWS Control Tower.

Provisioning degli account in un'unica fase in AWS Control Tower

2 marzo 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl 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 direttamente dalla console AWS Control Tower.

Per utilizzare il modulo semplificato, accedi ad Account Factory nella console AWS Control Tower, quindi scegli Quick account provisioning. AWSControl Tower assegna lo stesso indirizzo e-mail all'account fornito e all'utente Single Sign-on (IAMIdentity 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 degli 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 registrarsi AWS conti. Per ulteriori informazioni, consulta Registra un account esistente.

AWSStrumento di smantellamento Control Tower

28 febbraio 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower ora supporta uno strumento di smantellamento automatico per aiutarvi a ripulire le risorse allocate da Control TowerAWS. Se non intendi più utilizzare AWS Control Tower per la tua azienda o se hai bisogno di una ridistribuzione importante delle tue risorse organizzative, potresti voler ripulire le risorse create durante la configurazione iniziale della landing zone.

Per smantellare la tua landing zone utilizzando un processo per lo più automatizzato, contatta AWS Support per ricevere assistenza sui passaggi aggiuntivi necessari. Per ulteriori informazioni sulla disattivazione, vedere. Procedura dettagliata: smantellamento di una AWS Control Tower Landing Zone

AWSNotifiche degli eventi relativi al ciclo di vita del Control Tower

22 gennaio 2020

(Non è richiesto alcun aggiornamento per la landing zone AWS di Control Tower)

AWSControl Tower annuncia la disponibilità delle notifiche degli 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.

AWSControl 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.

AWSControl Tower utilizza più AWS servizi per creare e gestire un sistema multi-account basato sulle migliori pratiche AWS ambiente. Il completamento di un'azione AWS Control Tower può richiedere diversi minuti. È possibile tenere traccia degli eventi del ciclo di vita nei CloudTrail log per verificare se l'azione Control AWS Tower originaria è stata completata correttamente. È possibile creare una EventBridge regola per avvisare l'utente quando CloudTrail registra un evento del ciclo di vita o per attivare automaticamente la fase successiva del flusso di lavoro di automazione.

gennaio - dicembre 2019

Dal 1° gennaio al 31 dicembre 2019, AWS Control Tower ha rilasciato i seguenti aggiornamenti:

- Disponibilità generale della versione 2.2 di AWS Control Tower
- Nuovi controlli opzionali in AWS Control Tower
- Nuovi controlli investigativi in AWS Control Tower
- AWSControl Tower accetta indirizzi e-mail per account condivisi con domini diversi dall'account di gestione
- Disponibilità generale della versione 2.1 di AWS Control Tower

Disponibilità generale della versione 2.2 di AWS Control Tower

13 novembre 2019

(Aggiornamento richiesto per la landing zone AWS del Control Tower. Per informazioni, vedereAggiorna la tua landing zone.)

AWSLa versione 2.2 di Control Tower offre tre nuovi controlli preventivi che impediscono la deriva degli account:

- Impedisci modifiche ai gruppi di log di Amazon CloudWatch Logs configurati da AWS Control Tower
- Impedisci l'eliminazione di AWS Config Autorizzazioni di aggregazione create da AWS Control Tower
- Impedisci l'eliminazione dell'archivio di registro

Il controllo è una regola di alto livello che fornisce una governance continua per l'intera azienda AWS ambiente. Quando crei la landing zone della 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 AWS di Control Tower)

AWSControl 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'insieme 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 AWS di Control Tower)

AWSControl Tower ora include i seguenti otto nuovi controlli investigativi:

- Rileva se il controllo delle versioni per i bucket Amazon S3 è abilitato
- Rileva se MFA è abilitato per gli utenti di IAM AWS Console
- Rileva se MFA è abilitata per IAM gli utenti
- Scopri se Amazon EBS Optimization è abilitato per Amazon EC2 Instances
- Rileva se EBS i volumi Amazon sono collegati alle EC2 istanze Amazon
- Scopri se l'accesso pubblico alle istanze di RDS database Amazon è abilitato
- Scopri se l'accesso pubblico agli snapshot RDS del database Amazon è abilitato
- Rileva se la crittografia dello storage è abilitata per le istanze di RDS database Amazon

Il controllo è una regola di alto livello che fornisce una governance continua per tutto AWS ambiente. 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.

AWSControl 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 AWS di Control Tower)

In AWS Control Tower, ora puoi inviare indirizzi e-mail per account condivisi (archivio di registro e membro di controllo) e account figlio (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 fornisci nuovi account per bambini.

Disponibilità generale della versione 2.1 di AWS Control Tower

24 giugno 2019

(Aggiornamento richiesto per la landing zone AWS del Control Tower. Per informazioni, consulta Aggiorna la tua zona di atterraggio.)

AWSControl Tower è ora disponibile a livello generale e supportato per l'uso in produzione. AWSControl Tower è destinato alle organizzazioni con più account e team che cercano il modo più semplice per configurare il loro nuovo account multiplo AWS ambiente e governo su larga scala. Con AWS Control Tower, puoi contribuire a garantire che gli account della tua organizzazione siano conformi alle politiche stabilite. Gli utenti finali dei team distribuiti possono effettuare il provisioning di nuovi AWS conti in modo rapido.

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, gestione delle identità degli utenti e dell'accesso federato con AWS IAM Identity Center, abilitando il provisioning degli account tramite Service Catalog e creando un archivio di log centralizzato utilizzando AWS CloudTrail e AWS Config.

Per una governance continua, è possibile 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. Il pannello AWS di controllo Control Tower offre una visibilità centralizzata su un AWS ambiente che include 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 anticipati per l'utilizzo di AWS Control Tower. Paghi solo per quelli AWS servizi abilitati per configurare una landing zone e implementare controlli selezionati.

Cronologia dei documenti

- Ultimo aggiornamento della documentazione: 30 agosto 2024

La tabella seguente descrive le modifiche importanti alla AWSControl Tower User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi iscriverti al RSS feed.

Modifica	Descrizione	Data
AWSControl Tower supporta fino a 1000 account per unità organizzativa	Un aumento del limite di account per unità organizzativa.	30 agosto 2024
AWSControl 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 ListControls API operazioni disponibili	Due nuove operazioni del Control Catalog consentono di trovare ulteriori informazioni sui controlli.	6 agosto 2024
AWSControl Tower supporta AFT e cFCT nelle regioni opt-in	AFTe cFCT sono disponibili in aggiunta Regioni AWS.	18 luglio 2024
AWSControl Tower aggiunge `ListLandingZoneOperations` API	Una novità API che ti consente di recuperare le operazioni recenti per la tua landing zone.	26 giugno 2024
AWSControl Tower supporta fino a 100 operazioni di controllo simultanee	Un aumento della quota delle operazioni di controllo simultanee a 100.	20 maggio 2024

AWSControl Tower disponibile in AWS Regione di Calgary West (Canada)	AWSControl Tower è disponibile nella regione Canada occidentale (Calgary).	3 maggio 2024
AWSControl Tower supporta l'aggiustamento delle quote in modalità self-service	AWSControl Tower è integrato con AWS Service Quotas nella console.	25 aprile 2024
La documentazione relativa ai controlli è stata spostata in una nuova guida	AWSControl Tower ha pubblicato la Controls Reference Guide.	21 aprile 2024
Etichettare `EnabledControl` le risorse in AWS CloudFormation	AWSControl Tower supporta l'aggiunta di tag alle `EnabledControl` risorse, tramite AWS CloudFormation modelli.	22 febbraio 2024
Linea di base disponibile APIs	AWSControl Tower ha rilasciato una nuova versione APIs per la registrazione OUs programmatica.	14 febbraio 2024
AWSControl Tower landing zone versione 3.3	AWSDisponibile la versione 3.3 della landing zone Control Tower.	14 dicembre 2023
AWSControl Tower annuncia i controlli per favorire la sovranità digitale	AWSControl Tower ha rilasciato una serie di controlli per aiutare i clienti con requisiti di sovranità digitale.	27 novembre 2023
AWSControl Tower supporta la landing zone APIs	AWSControl Tower supporta la configurazione e il lancio di zone di atterraggio utilizzando new. APIs	26 novembre 2023

AWSControl Tower supporta i controlli abilitati all'etich ettatura	AWSControl Tower supporta l'etichettatura dei controlli abilitati, in console e con nuoviAPIs.	10 novembre 2023
AWSControl Tower disponibi le in Asia Pacifico (Melbourne) Regione AWS	Disponibile nella regione Asia Pacifico (Melbourne).	3 novembre 2023
Nuovo controllo API disponibi le	AWSControl Tower ha rilasciat o un nuovo controlloAPI.	14 ottobre 2023
AWSControl Tower lancia nuovi controlli	AWSControl Tower ha rilasciat o nuovi controlli proattivi e investigativi.	5 ottobre 2023
AWSI report di Control Tower derivano dalla disabilitazione dell'accesso affidabile	AWSControl Tower avvisa i clienti quando si verifica una deriva, se i clienti disattiva no l'accesso affidabile a AWS Control Tower in AWS Organizations.	21 settembre 2023
AWSControl Tower disponibi le in quattro versioni aggiuntiv e Regioni AWS	Disponibile in Asia Pacifico (Hyderabad), Europa (Spagna e Zurigo) e Medio Oriente (UAE).	13 settembre 2023
AWSControl Tower disponibile nella regione di Tel Aviv	AWSControl Tower è disponibi le nella regione di Tel Aviv, il-central-1.	28 agosto 2023
AWSControl Tower lancia 28 nuovi controlli proattivi	AWSControl Tower ha rilasciat o 28 nuovi controlli proattivi.	24 luglio 2023

AWSControl Tower depreca 2 controlli	AWSControl Tower rimuoverà due controlli dalla libreria dei controlli, a partire dal 18 agosto 2023.	18 luglio 2023
AWSDisponibile la landing zone 3.2 della Control Tower	AWSÈ disponibile la versione 3.2 della landing zone Control Tower.	16 giugno 2023
AWSControl Tower gestisce gli account in base all'ID	AWSControl Tower traccia il AWS ID dell'account, anziché l'indirizzo e-mail dell'account.	14 giugno 2023
Sono disponibili controlli di rilevamento aggiuntivi del Security Hub	AWSControl Tower aggiunge dieci nuovi controlli alla libreria dei controlli, per il Security Hub Service-Managed Standard: AWS Control Tower.	12 giugno 2023
AWSControl Tower pubblica tabelle di metadati di controllo	AWSControl Tower ora fornisce tabelle di metadati di controllo come parte della documentazione pubblicata.	7 giugno 2023
Supporto Terraform per la personalizzazione di Account Factory	Supporto in un'unica regione per i progetti open source Terraform in. AFC	6 giugno 2023
AWS IAMautogestione disponibile per la landing zone	AWSControl Tower ora supporta i clienti nella scelta del proprio provider di identità per una landing zone.	6 giugno 2023

Nuovo ruolo aggiunto	AWSControl Tower ha aggiunto un nuovo ruolo collegato al servizio e una policy associata. AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy	1 giugno 2023
Aggiornamento misto della governance	Aggiornamento per consigliare i clienti in merito alla governance mista.	1 giugno 2023
Sono disponibili controlli proattivi aggiuntivi	I nuovi controlli proattivi ti aiutano a gestire l'ambiente multi-account e a raggiungere obiettivi di controllo specifici.	19 maggio 2023
Sono disponibili sette regioni aggiuntive	AWSControl Tower è ora disponibile in sette versioni aggiuntive 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
Passaggio a una politica gestita	Abbiamo modificato il codice AWSControlTowerServiceRolePolicyin modo che AWS Control Tower possa chiamare i `EnableRegion` `ListRegions` ,, `GetRegionOptStatus` APIs che sono implementati dal AWS Servizio di gestione dell'account.	6 aprile 2023

Il tracciamento delle richieste di personalizzazione dell'account è generalmente disponibile	AWSControl Tower ora supporta la possibilità di tracciare le richieste di personalizzazione dell'account utilizzando il flusso di lavoro Account Factory for Terraform (AFT).	16 febbraio 2023
IAMaggiornamento delle migliori pratiche	Guida aggiornata per allinears i alle raccomandazioni sulle IAM migliori pratiche. Per ulteriori informazioni, consulta le migliori pratiche di sicurezza in IAM.	15 febbraio 2023
AWSDisponibile la landing zone 3.1 della Control Tower	AWSÈ disponibile la landing zone 3.1 della Control Tower.	9 febbraio 2023
Controlli proattivi generalmente disponibili	I controlli proattivi vengono avviati dallo stato di anteprima alla disponibilità generale.	24 gennaio 2023
Operazioni simultanee sull'account	AWSControl Tower ora supporta fino a cinque (5) azioni simultanee in account factory. Puoi creare, aggiornare o registrare fino a cinque account alla volta.	16 dicembre 2022
I controlli proattivi aiutano nell'approvvigionamento delle risorse	AWSControl Tower ora supporta controlli proattivi , implementati tramite AWS CloudFormation ganci.	28 novembre 2022

Personalizzazione dell'account in fabbrica disponibile	AWSControl Tower ora supporta il provisioning degli account con modelli di account personalizzabili, chiamati blueprint, direttamente dalla console AWS Control Tower.	28 novembre 2022
Lo stato di conformità è visualizzabile per tutti AWS Config regole	AWSControl Tower ora mostra lo stato di conformità di tutti AWS Config regole distribui te nelle unità organizzative registrate presso AWS Control Tower.	18 novembre 2022
Passaggio a una politica gestita	L'abbiamo modificato AWSControlTowerSer viceRolePolicyin modo che AWS Control Tower possa assumere il `AWSContro lTowerBlueprintAcc ess` ruolo necessario per le personalizzazioni di Account Factory.	28 ottobre 2022
APIsper i controlli, AWS CloudFormation risorsa	AWSControl Tower ora supporta l'attivazione e la disattivazione dei controlli tramite una serie di API chiamate e una nuova AWS CloudFormation risorsa.	1 settembre 2022
cFct supporta l'eliminazione dei 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 archivian o i CloudTrail log del AWS Control Tower, in increment i di giorni o anni, fino a un massimo di 15 anni.	15 agosto 2022
È disponibile la riparazione di Role Drift	AWSControl Tower supporta la riparazione in caso di deriva dei ruoli, senza una riparazio ne completa della landing zone.	11 agosto 2022
Disponibile la versione 3.0	AWSLa versione 3.0 della landing zone di Control Tower cambia rispetto alla versione basata sull'account AWS CloudTrail indirizza verso percorsi basati sull'orga nizzazione e aggiorna la policy gestita per abilitare percorsi a livello di organizzazione. Ti consente di aggregare AWS Config informazioni solo nella tua regione d'origine. La versione 3.0 include anche un aggiornamento alla Region Deny Control e due nuovi controlli investigativi.	29 luglio 2022
La pagina Organizzazione combina visualizzazioni OUs e account	La nuova pagina Organizza zione in AWS Control Tower mostra una visualizzazione gerarchica di tutte le unità organizzative (OUs) e gli account.	18 luglio 2022

Passa a una politica gestita	Abbiamo modificato il sistema AWSControlTowerServiceRolePolicyin modo che i clienti possano avere un livello organizzativo AWS CloudTrail percorsi da aggregare AWS CloudTrail registri.	20 giugno 2022
Registrazione e aggiornamento semplificati degli account dei membri	AWSControl Tower ora ti dà 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
AFTsupporta la personalizzazione degli account condivisi	AWSControl Tower Account Factory for Terraform ora supporta la personalizzazione dell'account di gestione AWS Control Tower, dell'archivio dei log e degli account di controllo.	27 maggio 2022
Operazioni simultanee per tutti i controlli opzionali	AWSControl Tower ora consente di applicare e rimuovere contemporaneamente protezioni preventive opzionali e controlli investigativi.	18 maggio 2022

Account di sicurezza e registrazione esistenti	AWSControl Tower ora supporta la possibilità di utilizzare gli account di sicurezza e di registrazione esistenti, anziché crearne di nuovi durante la configura zione della landing zone.	16 maggio 2022
Disponibile la versione 2.9	AWSLa versione 2.9 della landing zone di Control Tower aggiorna il server di inoltro di notifiche Lambda per utilizzare il runtime Python versione 3.9.	22 aprile 2022
Supporto aggiornato per AWS migliori pratiche, disponibile la versione 2.8	AWSLa versione 2.8 della landing zone di Control Tower fornisce un supporto aggiuntiv o per garantire che i carichi di lavoro e AWS gli account sono in linea con AWS migliori pratiche.	10 febbraio 2022
Region nega il controllo	AWSControl Tower ora include un controllo che consente di limitare l'accesso a AWS Regioni, per risolvere i problemi di conformità e regolamentazione.	30 novembre 2021
Controlli sulla residenza dei dati	AWSControl Tower ora supporta controlli che aiutano a gestire la residenza dei dati con un controllo granulare.	30 novembre 2021

AWSFabbrica di account Control Tower per Terraform	AWSControl Tower ora supporta Terraform per il provisioning e l'aggiornamento automatici 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	AWSControl Tower ora consente alla landing zone di contenere strutture di unità organizzative annidate.	16 novembre 2021
Detective controlla la concorrenza	AWSI controlli di rilevamento Control Tower ora supportano operazioni di attivazione e disabilitazione simultanee.	5 novembre 2021
Sono disponibili due nuove regioni	AWSControl Tower è ora disponibile in due nuove versioni AWS Regioni, regione Europa (Parigi) e regione Sud America (San Paolo).	29 luglio 2021
Deselezione della regione	È possibile deselezionare AWS Regioni che non desideri più governare tramite AWS Control Tower.	29 luglio 2021
KMSchiavi disponibili	Facoltativamente, puoi creare o scegliere KMS le chiavi da gestire per crittografare dati e risorse.	28 luglio 2021

Passa a una politica gestita	Abbiamo modificato il sistema AWSControlTowerSer viceRolePolicyin modo che i clienti possano utilizzare le proprie chiavi di KMS crittogra fia per AWS CloudTrail registri.	28 luglio 2021
Nomi di controllo modificati, funzionalità invariata	Alcuni nomi e descrizio ni 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	AWSControl Tower esegue scansioni automatiche giornaliere di Managed SCPs to Check for Drift.	11 maggio 2021
Nomi e account personalizzati OUs	AWSControl Tower ti consente di fornire nomi personali zzati durante il processo di configurazione delle landing zone, per gli account essenzial i OUs e per gli account, senza creare deriva.	16 aprile 2021
La disattivazione di una landing zone è self-service	AWSControl Tower ora consente di disattivare una landing zone senza contattare AWS Support. 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.	9 aprile 2021

Tre regioni aggiuntive	AWSControl Tower è ora disponibile in tre versioni aggiuntive AWS Regioni: 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 della AWS Control Tower, separatam ente dalla governance delle risorse esterne alla AWS Control Tower. Le linee guida su quattro controlli esistenti sono passate da obbligato rie a facoltative. La versione 2.7 della landing zone AWS Control Tower include un requisito perHTTPS, che non può essere annullato dopo l'aggiornamento.	8 aprile 2021

Selezione della regione	AWSLa selezione della regione Control Tower offre una migliore capacità di gestire l'impronta geografic a delle risorse della AWS Control Tower. Per ampliare il numero di regioni in cui offri ospitalità AWS risorse o carichi di lavoro, per motivi di conformità, normative, di costo o di altro tipo, ora puoi selezionare le regioni aggiuntiv e da gestire.	19 febbraio 2021
Registra un'unità organizzativa e gestisci tutti i suoi account con AWS Control Tower contemporaneamente	AWSControl Tower aggiunge la possibilità di registrare un'unità organizzativa, un modo per portare più account alla governance contempor aneamente.	28 gennaio 2021

Gli aggiornamenti multipli dell'account sono registrati OUs	Ora puoi aggiornare tutti gli account di qualsiasi account registrato AWS Organizations unità organizzativa (OU) contenente fino a 300 account, con un solo clic, dalla dashboard 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 elementi esterni AWS Config regole, quindi AWS Control Tower non ha bisogno di accedere agli account non gestiti.	29 dicembre 2020

AWSControl Tower è disponibile in altre versioni AWS Regioni.	AWSControl Tower è ora disponibile per l'implementazione 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 a AWS Control Tower per governare nei 10 supportati AWS Regioni.	18 novembre 2020
Aggiornamento del controllo	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 delle informazioni correlate è ora disponibile per AWS Control Tower	La pagina delle informazioni correlate semplifica la ricerca di attività comuni che possono essere utili dopo aver configurato la landing zone AWS della Control Tower.	18 settembre 2020
AWSLa console Control Tower mostra maggiori dettagli sugli OUs account.	All'interno della console AWS Control Tower, puoi visualizzare maggiori dettagli sul tuo AWS conti 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 tra tutte le tabelle.	22 luglio 2020
AWSControl Tower consente alle organizzazioni esistenti di creare 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 account esistenti AWS account e creazione di nuovi account.	16 aprile 2020

AWSControl Tower è ora disponibile in Asia Pacifico	AWSControl Tower è ora disponibile per l'installazione nell'Asia Pacifico (Sydney) AWS Regione. 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 lo smantellamento di una landing zone della 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 Control Tower AWS	Gli eventi del ciclo di vita forniscono dettagli aggiuntivi per determinati eventi AWS Control Tower, per semplificare l'automazione del flusso di lavoro.	12 dicembre 2019

Le pagine Impostazioni e Attività sono disponibili per AWS Control Tower	Le pagine Impostazioni e Attività semplificano l'aggiornamento della landing zone e la visualizzazione degli eventi registrati.	30 novembre 2019
Sono disponibili controlli preventivi aggiuntivi per AWS Control Tower	I controlli preventivi in AWS Control Tower mantengono l'organizzazione e le risorse allineate all'ambiente.	6 settembre 2019
Sono disponibili controlli investigativi aggiuntivi per AWS Control Tower	I controlli investigativi in AWS Control Tower forniscono informazioni sullo stato dell'organizzazione e delle risorse.	27 agosto 2019
AWSControl Tower è ora disponibile a livello generale	AWSControl Tower è un servizio che offre il modo più semplice per configurare e gestire il tuo account multiplo AWS ambiente 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.