Struttura OU in zone di AWS atterraggio regolamentate: un esempio dell'industria farmaceutica

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Struttura OU in zone di AWS atterraggio regolamentate: un esempio dell'industria farmaceutica

Table of Contents

Struttura OU in zone di AWS atterraggio regolamentate: un esempio dell'industria farmaceutica

Katja Mueller, Petar Forai e Keval Sheth, Amazon Web Services ()AWS

Marzo 2023 (cronologia dei documenti)

AWS offre diverse configurazioni di Landing Zone Accelerator che supportano settori specifici, incluso il settore sanitario. Landing Zone Accelerator for Healthcare viene utilizzato in combinazione con AWS Control Tower per semplificare la gestione e la governance di un ambiente multi-account allineato alle AWS migliori pratiche e a più framework di conformità globali. Un aspetto importante dell'orchestrazione della governance consiste nel Account AWS raggruppare le unità organizzative (OUs), in modo da poterle amministrare come un'unica unità.

Questa guida illustra le best practice e le considerazioni per riprogettare le strutture di unità organizzative esistenti man mano che la maturità del cloud aziendale cresce. Presenta un esempio pratico basato sull' AWS Control Tower implementazione per una grande azienda farmaceutica e illustra le lezioni apprese da tale implementazione. AWS la progettazione delle landing zone non è uno sforzo irripetibile. Si può e si deve consentire che si evolva. Questa evoluzione può essere raggiunta con successo ed efficienza applicando le AWS migliori pratiche e i suggerimenti evidenziati in questa guida.

Panoramica

Abbiamo collaborato con un'azienda farmaceutica multinazionale per eseguire attività proof-of-concept (PoC) AWS per esplorare come migrare le proprie applicazioni dall'ambiente locale al. Cloud AWS Quando hanno iniziato a scalare e accelerare il flusso di lavoro di migrazione per includere i carichi di lavoro di produzione, è diventato chiaro che avevano bisogno di una AWS landing zone regolamentata e conforme per raggiungere il loro obiettivo. Prima progettavamo AWS Control Towere implementavamo una nuova AWS landing zone.

Un aspetto importante di una nuova AWS landing zone e della sua organizzazione è la struttura delle sue unità organizzative (OUs). Un'unità organizzativa è un raggruppamento logico di Account AWS elementi creato utilizzando AWS Organizations. È possibile utilizzarlo OUs per organizzarsi Account AWS in una gerarchia e applicare i controlli di gestione e governance in modo coerente e più semplice.

È possibile collegare controlli basati su policy a un'unità organizzativa e a. Account AWS I bambini OUs all'interno di un'unità organizzativa ereditano automaticamente tali controlli. Pertanto, OUs svolgono un ruolo fondamentale nella gestione della sicurezza e della governance in AWS Organizations.

Una policy è un documento JSON che include una o più istruzioni che definiscono i controlli da applicare a un gruppo di Account AWS. AWS Organizations attualmente supporta quattro tipi di policy, note anche come policy di controllo dei servizi (SCPs). Un SCP definisce le azioni Servizi AWS e che sono disponibili per l'uso in diversi Account AWS. Ad esempio, puoi utilizzare un SCP per richiedere che il lancio di istanze Amazon Elastic Compute Cloud EC2 (Amazon) utilizzi un tipo di istanza specifico.

Tipi di policy

I tipi di policy SCP includono quanto segue:

- Gli elenchi consentiti e gli elenchi negati sono strategie complementari che è possibile utilizzare SCPs per filtrare le autorizzazioni disponibili per gli account.
- Le politiche relative ai tag ti aiutano a mantenere i tag coerenti, incluso il trattamento preferenziale tra maiuscole e minuscole delle chiavi dei tag e dei valori dei tag tra gli account.
- Le policy di backup configurano i backup per i tipi di risorse supportati, ad esempio la finestra temporale degli archivi di backup e gli archivi di destinazione per i backup trasversali. Regioni AWS

- Le politiche di esclusione dei servizi di intelligenza artificiale consentono o disabilitano il miglioramento continuo dei servizi di intelligenza AWS artificiale (AI) a livello globale.

Comportamento relativo all'ereditarietà delle politiche: quando si allega una politica a un'unità organizzativa specifica, gli account che fanno capo direttamente a tale unità organizzativa o a qualsiasi unità organizzativa secondaria ereditano la politica. Quando si allega una politica a un account specifico, la politica ha effetto solo su quell'account. È possibile sovrascrivere le politiche ereditate introducendo politiche di eccezione. L'ereditarietà consente esplicitamente a tutte le autorizzazioni di passare dall'unità organizzativa principale (OU) a tutte le unità organizzative e a quelle secondarie, Account AWS a meno che l'utente non neghi esplicitamente un'autorizzazione. Per negare un'autorizzazione, è necessario creare una politica aggiuntiva e allegarla all'unità organizzativa o. Account AWSPer ulteriori informazioni sull'ereditarietà e le eccezioni delle politiche, consulta la documentazione.AWS Organizations

AWS Control Tower fornisce inoltre una propria serie di controlli investigativi e preventivi (chiamati anche guardrail) utilizzando la struttura dell'unità organizzativa. AWS Control Tower i controlli preventivi impediscono le azioni utilizzando l'in SCPs . AWS Organizations I controlli Detective segnalano la deriva della configurazione rispetto al controllo utilizzando. AWS ConfigPer ulteriori informazioni su questi controlli, consulta la AWS Control Tower documentazione.

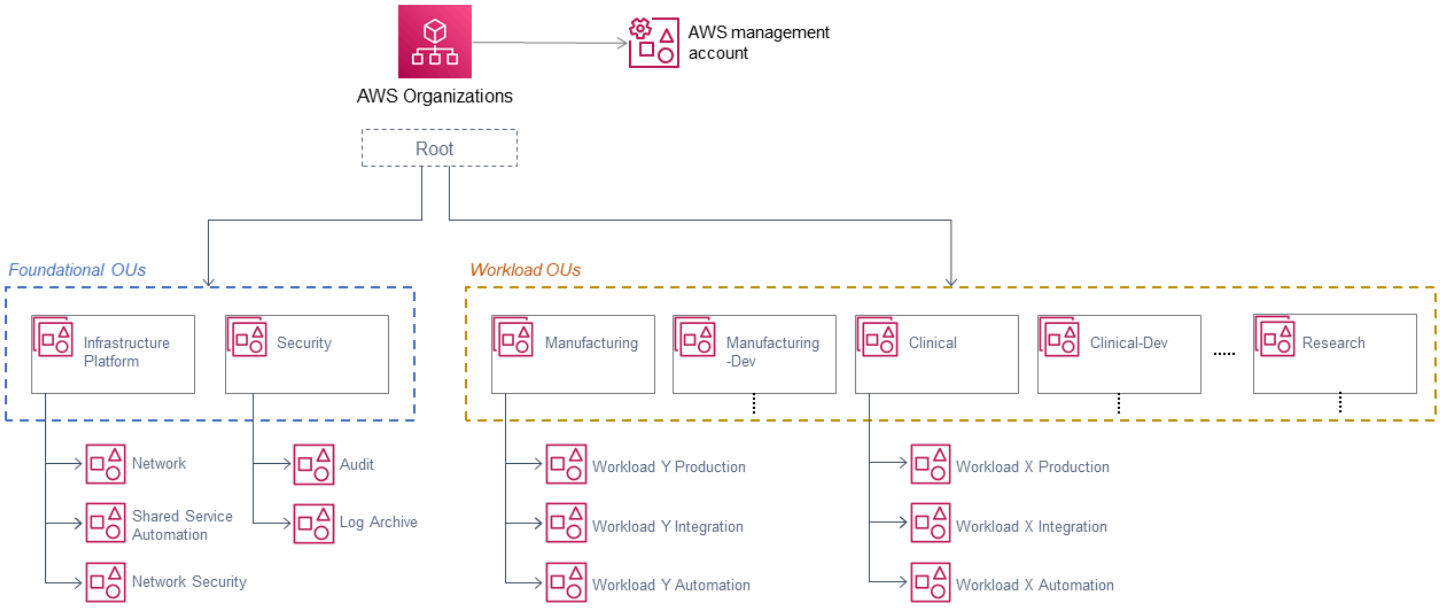
Puoi anche AWS Security Hub CSPMautomatizzare i controlli delle migliori pratiche di sicurezza, aggregare gli avvisi di sicurezza in un unico posto e formato e comprendere il livello di sicurezza generale di tutti i tuoi sistemi. Account AWS

Progettazione dell'unità organizzativa: fase 1

Per quanto riguarda l'azienda farmaceutica multinazionale oggetto del nostro esempio, la progettazione iniziale delle organizzazioni e delle unità organizzative è stata AWS Organizations seguita AWS scrupolosamente dalle raccomandazioni per la costituzione. AWS Control Tower Per un esempio, vedi Landing Zone Accelerator on AWS for Healthcare. AWS Control Tower inizialmente ho fornito una struttura di unità organizzative semplice con unità organizzative di base comuni, come descritto nel post di blog Best Practices for Organizational Units AWS Organizations, tra cui l'unità organizzativa di sicurezza, l'unità organizzativa dell'infrastruttura della piattaforma e le unità organizzative specifiche dell'azienda.

Progettazione dell’architettura

Il diagramma seguente mostra l'architettura dell'unità organizzativa iniziale.



Unità organizzativa di sicurezza

L'unità organizzativa di sicurezza raggruppa ampiamente le funzionalità Account AWS correlate alla sicurezza e utilizza due account (Audit e Log Archive) per archiviare i dati operativi di sicurezza per la registrazione centralizzata e il controllo dell'accesso all'ambiente. AWS servizi di sicurezza di base come Amazon GuardDuty e AWS Security Hub CSPM risiedono nell'account Audit.

Piattaforma di infrastruttura OU

L'Infrastructure Platform OU Account AWS si raggruppa per fornire le fondamenta dell'infrastruttura. All'interno di questa unità organizzativa sono inizialmente distribuiti i componenti della rete centrale (gateway, firewall, hub di rete centrale e servizi simili). Account AWS

Unità organizzative aggiuntive

Altre unità organizzative specifiche dell'azienda (come le unità organizzative cliniche) ampliano le unità organizzative fondamentali all'interno di una gerarchia di basso livello. I carichi di lavoro sono implementati con una struttura multi-account e con ambienti separati all'interno di tali unità organizzative.

Questa progettazione iniziale è stata ispirata da diverse considerazioni:

- Le unità organizzative annidate non erano disponibili in quel momento AWS Control Tower e richiedevano un'ampia personalizzazione.
- I carichi di lavoro iniziali destinati al cloud si concentravano su aspetti particolari dell'azienda, come le sperimentazioni cliniche o l'analisi delle apparecchiature di produzione (visualizzazioni funzionali).
- L'azienda distingue tra cinque ambienti di carico di lavoro (sviluppo, convalida, integrazione, formazione e produzione). L'azienda aveva bisogno di un terreno di gioco per lo sviluppo di applicazioni senza la rigida governance tramite AWS controlli richiesti dai carichi di lavoro di produzione. Le Manufacturing-Dev OU di sviluppo, come l'unità organizzativa, sono state assegnate a questo scopo.
- L'automazione del carico di lavoro faceva parte dell'ecosistema di ciascuna applicazione e non richiedeva alcuna separazione.
- I processi di qualificazione dell'infrastruttura (IQ) e di conformità GxP non richiedevano una distinzione AWS di controlli a livello di unità organizzativa.

Progettazione dell'unità operativa: fase 2

Nel nostro esempio, l'azienda farmaceutica ha accelerato il passaggio a una nuova fase di maturità del cloud implementando carichi di lavoro di produzione qualificati nelle unità organizzative esistenti. Ciò ha dato inizio a una revisione del progetto iniziale e la struttura di fase 1 è stata messa alla prova con la migrazione di più carichi di lavoro verso la landing zone regolamentata. AWS

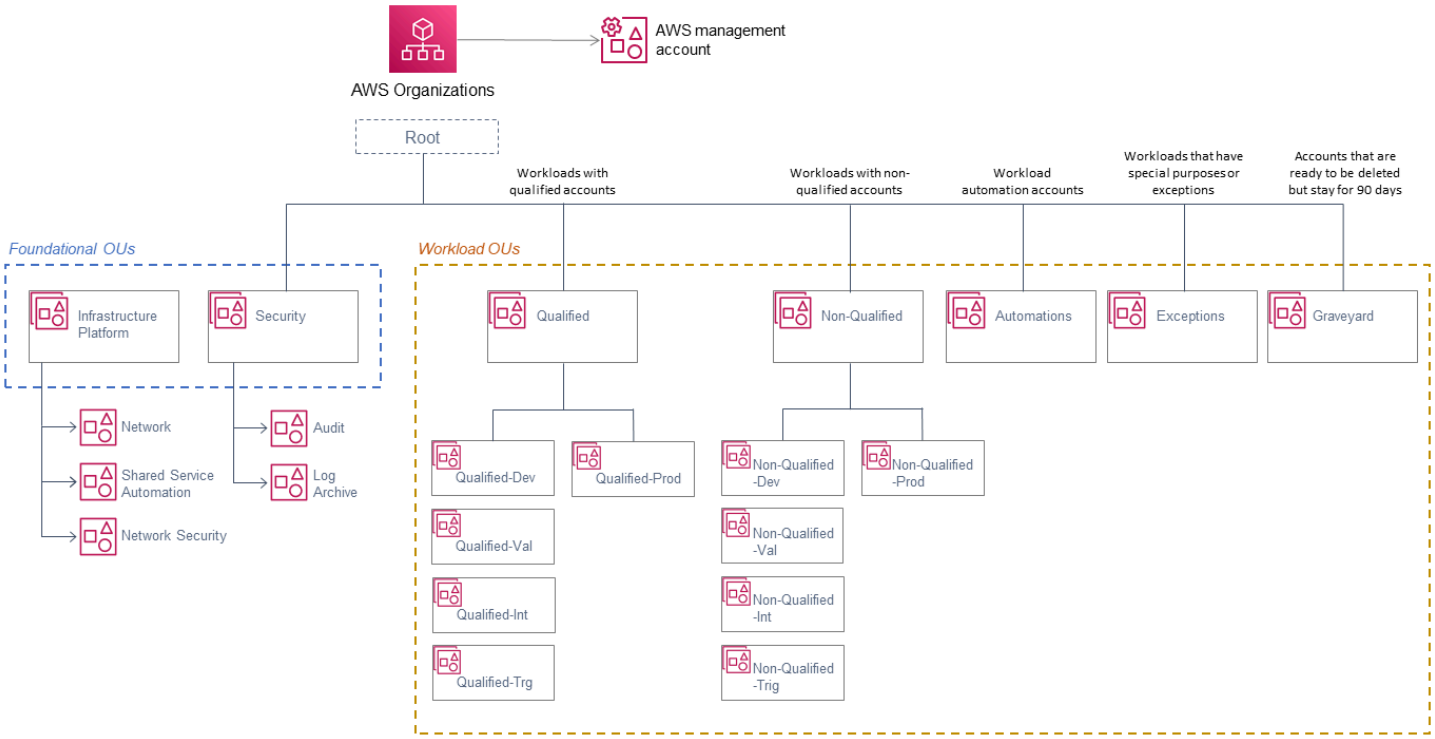
I seguenti nuovi requisiti e approfondimenti sono diventati importanti:

- L'azienda ha implementato modelli di carico di lavoro basati su modelli di condivisione dei dati, in modo che le applicazioni acquisissero una natura polivalente che non poteva più essere assegnata a unità organizzative separate, come quelle cliniche o di produzione.
- La qualificazione (in particolare, la qualificazione continua) è diventata un aspetto fondamentale di molti carichi di lavoro. Questi carichi di lavoro dovevano essere integrati nei processi operativi in modo che potessero seguire più facilmente le migliori pratiche di sicurezza. I carichi di lavoro qualificati richiedevano AWS controlli più rigorosi, che sono stati impostati a livello di unità organizzativa nella fase 1.
- La funzionalità Nested OU è diventata disponibile in. AWS Control Tower
- L'aggiornamento delle competenze e l'esperienza hanno portato a una migliore comprensione di quali politiche specifiche fossero rilevanti per i carichi di lavoro.
- La società ha definito e concordato un modello operativo basato sull'allineamento delle responsabilità.
- I modelli di segmentazione e strutturazione del carico di lavoro sono maturati e sono stati adottati per le migrazioni dei carichi di lavoro.

Di conseguenza, un nuovo design è stato implementato nella fase 2 e Account AWS migrato verso quella nuova struttura. Questa nuova struttura include le unità organizzative descritte nelle sezioni seguenti.

Progettazione dell’architettura

Il diagramma seguente mostra l'architettura dell'unità organizzativa per la fase 2.



Unità organizzativa di sicurezza

L'unità organizzativa di sicurezza contiene funzionalità ampiamente Account AWS correlate alla sicurezza e utilizza due account (Audit e Log Archive) per archiviare i dati operativi di sicurezza per la registrazione centralizzata e il controllo dell'accesso all'ambiente. AWS servizi di sicurezza di base come Amazon GuardDuty e AWS Security Hub CSPM risiedono nell'account di controllo. Questa unità organizzativa rimane invariata rispetto al design originale.

Infrastructure Platform OU

L'unità organizzativa Infrastructure Platform contiene account di infrastruttura di base come il networking e l'automazione condivisa nella AWS landing zone. Questa unità organizzativa rimane invariata rispetto al design originale.

OU qualificata

L'unità organizzativa qualificata contiene carichi di lavoro che richiedono un'infrastruttura qualificata, ad esempio rigorose procedure di gestione delle modifiche, qualificazione e convalida.

Non-qualified OU

L' Non-Qualified unità organizzativa contiene carichi di lavoro che non hanno requisiti GxP o che non sono critici per l'azienda.

Automazioni (OU)

L'unità organizzativa Automations contiene risorse condivise per l'automazione dei carichi di lavoro, come pipeline di integrazione continua e distribuzione continua (CI/CD) per la gestione dell'infrastruttura. A seconda dei requisiti, l'automazione può essere suddivisa tra ambienti o ospitata in un unico ambiente. Account AWS

Eccezioni OU

L'unità organizzativa Exceptions contiene carichi di lavoro che richiedono un trattamento speciale che altrimenti verrebbe impedito dalle politiche. Ad esempio, i bucket Amazon Simple Storage Service (Amazon S3) ampiamente accessibili e leggibili farebbero parte dell'unità organizzativa Exceptions.

Graveyard OU

L'unità organizzativa Graveyard contiene quattro carichi Account AWS di lavoro che verranno eliminati. Le policy di questi account devono essere rimosse per un accesso amministrativo semplice ed efficace fino alla scadenza o all'eliminazione dell'account.

Migrazione e verifica delle unità organizzative

Per l'azienda farmaceutica multinazionale oggetto del nostro esempio, i team di progettazione della piattaforma cloud e di gestione delle modifiche hanno concordato un piano e una pianificazione della migrazione. Account AWS sono stati esaminati e classificati in base all'impatto e alla criticità aziendali nell'ambito della pianificazione.

La nuova struttura di unità organizzative è stata implementata parallelamente alla struttura delle unità organizzative esistente per consentire l'implementazione di nuove politiche e la migrazione incrementale. Ne abbiamo creati di nuovi vuoti OUs con figli OUs e assegnato AWS Organizations politiche e AWS Control Tower controlli a tali bambini. OUs

Le AWS Organizations politiche sono state migrate manualmente applicando le politiche desiderate alla nuova struttura. Abbiamo utilizzato il controllo manuale a campione per verificare AWS Organizations le politiche e i meccanismi automatici per verificare AWS Control Tower i controlli. Account AWS sono stati spostati nella nuova versione OUs solo dopo che questi controlli hanno avuto esito positivo.

La migrazione degli account è stata semiautomatica e ha seguito un approccio scaglionato o in batch. La migrazione iniziale era considerata meno critica, utilizzando un batch di cinque Account AWS per ciclo di migrazione. Account AWS I batch di migrazione non superavano i 10 account. Al momento della migrazione degli account, i revisori e i tester hanno utilizzato la AWS Control Tower console per verificare che tali account fossero stati spostati nell'unità organizzativa corretta e monitorato AWS CloudTrail i log per individuare eventuali errori. I revisori hanno inoltre verificato che le AWS Control Tower console AWS Service Catalog e le console non presentassero anomalie o che presentassero account contaminati o sconosciuti.

Le modifiche al posizionamento degli account da parte delle unità organizzative non hanno influito sulla connettività o sull'accessibilità delle risorse. Non è stata segnalata alcuna interruzione in un'applicazione di produzione.

Lezioni apprese e migliori pratiche

- La progettazione della struttura delle unità organizzative non è un'operazione irripetibile. Man mano che un'azienda aumenta l'adozione del cloud e migra carichi di lavoro aggiuntivi nella AWS landing zone, anche il design delle unità organizzative (e implicitamente il suo concetto di policy) si evolverà naturalmente.
- Non confondetele con cartelle; consideratele un obiettivo OUs per le policy. Le OUs e la relativa gerarchia forniscono l'elemento strutturante per le politiche Account AWS e devono essere sempre trattate come contenitori per le politiche. Si consiglia di inserire tutto ciò Account AWS che richiede lo stesso set di politiche nella stessa unità organizzativa. Questa linea guida si estende anche a nidificato OUs (OUs all'interno OUs).

  AWS gli ambienti che richiedono funzionalità condivise centralmente e capacità di condivisione dei dati tra carichi di lavoro (spesso presenti nelle piattaforme di dati aziendali) sono più facili da inserire in una struttura di unità organizzative non basata sulla classificazione delle funzioni delle linee di business (LOB). Ad esempio, un ambiente di produzione per un'applicazione di produzione non è diverso da un ambiente di produzione per un'applicazione di analisi di sperimentazione clinica in termini di politiche in. AWS Organizations
- Rispetta e usa l'ereditarietà. Quando si associa una politica a un'unità organizzativa specifica, le persone Account AWS che fanno capo direttamente a tale unità organizzativa o a un'unità organizzativa secondaria ereditano la politica. Quando si allega una politica a una specifica Account AWS, la politica influisce solo su quella Account AWS.

  Lo sforzo di migrazione da una struttura di unità organizzativa a un'altra dipende dalla misura in cui le politiche esistenti sono state configurate a livello di unità organizzativa o Account AWS a livello di unità organizzativa. Un altro fattore importante è la quantità di ereditarietà delle politiche utilizzata nella gerarchia delle unità organizzative esistente o se l'ereditarietà è stata interrotta. La complessità della migrazione aumenta con l'implementazione di percorsi di ereditarietà irregolari o devianti. Ad esempio, se si applicano le politiche a Account AWS livello individuale o si fanno frequenti eccezioni alle politiche (che interrompono l'ereditarietà), la migrazione di tali politiche in una nuova struttura richiederà uno sforzo molto maggiore. In questi casi di elevata complessità, si consiglia di dedicare del tempo alla revisione e alla riprogettazione dell'ereditarietà delle politiche durante la pianificazione della migrazione.
- Prenditi cura sia delle AWS Organizations politiche che dei controlli. AWS Control Tower La struttura dell'unità organizzativa è condivisa tra AWS Control Tower e AWS Organizations. AWS

Control Tower fornisce una propria serie di controlli investigativi e preventivi. Questi controlli si applicano a livello Account AWS di unità organizzativa. AWS Organizations orchestra le politiche a livello di unità organizzativa. In una migrazione di unità organizzative, si consiglia di migrare innanzitutto AWS Organizations le politiche, poiché queste hanno un peso maggiore ai fini della conformità. Si consiglia di applicare AWS Control Tower i controlli alla nuova struttura dell'unità organizzativa nella seconda fase di migrazione.

- L'aggiornamento richiede tempo Account AWS. È necessario registrare nuovamente le Account AWS singole unità esistenti nella nuova struttura dell'unità organizzativa utilizzando. AWS Control Tower Questa operazione richiede tempo. Se disponi di un numero elevato di account, ti consigliamo di semplificare questa operazione mediante l'automazione per controllare e automatizzare il posizionamento delle unità organizzative di. Account AWS Ecco due scenari di esempio:
  - Modifica manuale per una migrazione di piccole dimensioni: il responsabile della migrazione riassegna ciascuna unità Account AWS organizzativa dalla vecchia unità organizzativa alla nuova unità organizzativa in. Console di gestione AWS Quando la riassegnazione è completa per tutti Account AWS, il lead di migrazione si apre per ciascuno Account AWS separatamente AWS Control Tower o per tutti. OUs La nuova registrazione AWS Control Tower richiede Account AWS 10-15 minuti per ogni account, Account AWS a seconda del numero di utenti Regioni AWS utilizzati nell'account. AWS Control Tower consente l'esecuzione in parallelo di un massimo di cinque operazioni simultanee di questo tipo.
  - Automazione delle modifiche personalizzata: l'automazione semplifica e fa risparmiare fatica. Ad esempio, è possibile automatizzare la gestione di un Account AWS ciclo di vita dalla creazione alla migrazione e alla conclusione. È possibile utilizzare AWS Control Tower Account Factory per modificare l'assegnazione dell'unità organizzativa per un Account AWS ed eseguire il processo di nuova registrazione. Questa automazione supporta la migrazione su larga scala di centinaia di. Account AWS

Risorse

- AWS Organizations Guida per l'utente (AWS documentazione)
- AWS Organizations terminologia e concetti (AWS documentazione)
- Politiche di controllo dei servizi (SCPs) (AWS documentazione)
- AWS Organizations Riferimento all'API (AWS documentazione)
- AWS Control Tower Guida per l'utente (AWS documentazione)
- Presentazione di Landing Zone Accelerator for Healthcare (post AWS sul blog)
- Gestione dell'ambiente multi-account utilizzando AWS Organizations e AWS Control Tower (AWS post sul blog)
- Migliori pratiche per le unità organizzative con AWS Organizations (post AWS sul blog)
- AWS Architettura di riferimento per la sicurezza (AWS SRA) (guidaAWS prescrittiva)
- Stabilisci la tua Cloud Foundation su AWS (white paper)AWS
- Organizzazione AWS dell'ambiente utilizzando più account (white paper)AWS

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	28 marzo 2023

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.