



Diagrammi di architettura per i viaggi

Strategia di account e sicurezza per la piattaforma dati serverless



Strategia di account e sicurezza per la piattaforma dati serverless: Diagrammi di architettura per i viaggi

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

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

Table of Contents

Account e strategia di sicurezza i

Diagramma della strategia dell'account e della sicurezza 1

Approfondimenti 2

Storia del diagramma 3

..... iv

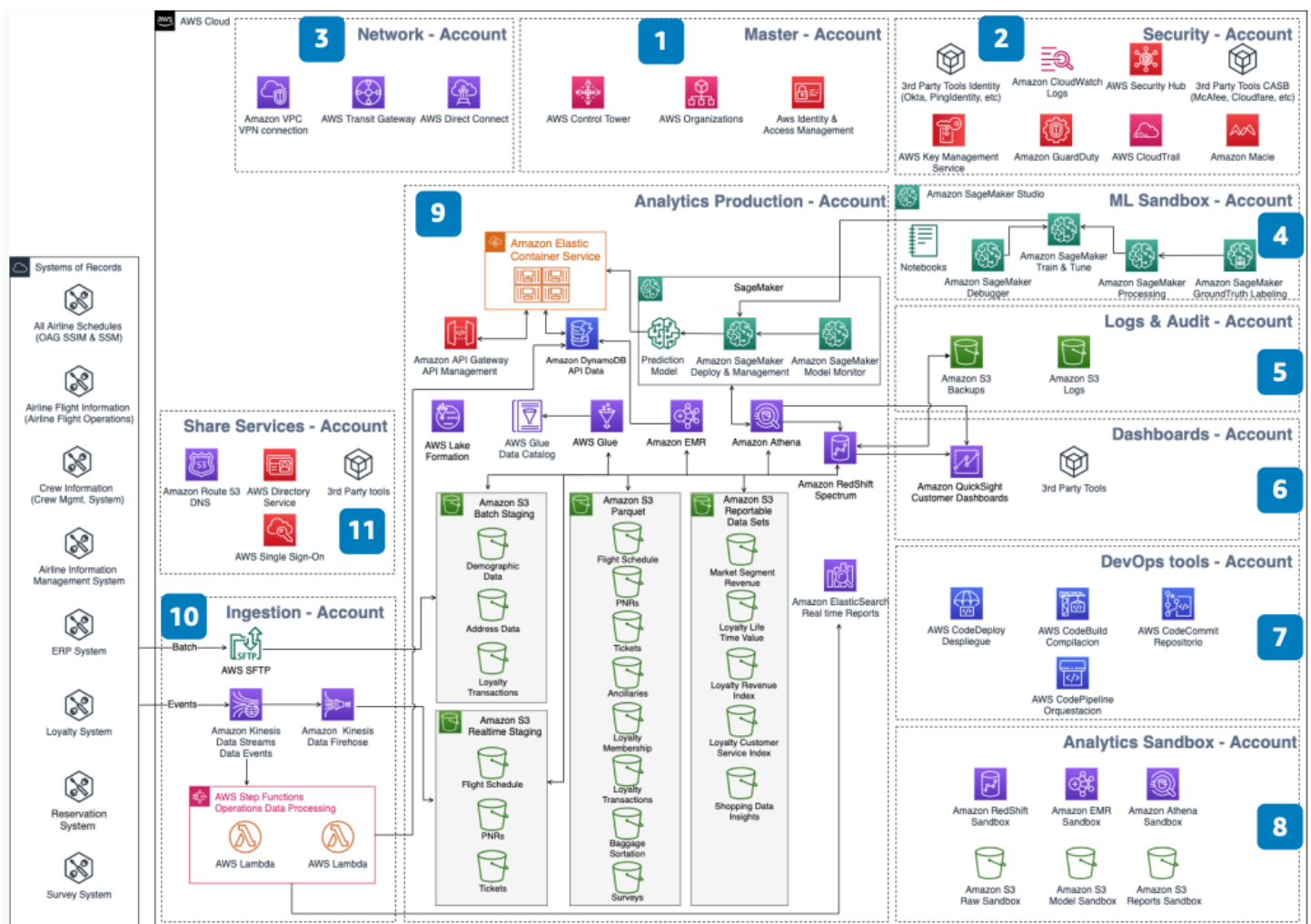
Strategia di account e sicurezza per la piattaforma dati serverless

Data di pubblicazione: 21 dicembre 2020 () [Storia del diagramma](#)

Una strategia multi-account è una best practice per l'isolamento delle risorse e della sicurezza. Un'architettura di analisi richiede una governance dei dati con elevati standard di sicurezza. È necessario concedere livelli di accesso corretti agli utenti su più account.

Questa architettura mostra come organizzare AWS gli account per una piattaforma dati serverless. Si occupa di sicurezza, governance e controllo degli accessi in tutti gli ambienti.

Diagramma della strategia dell'account e della sicurezza



I passaggi seguenti descrivono l'architettura:

1. L'account root è l'account più critico in AWS. Applica politiche di accesso restrittive per proteggere questo account.
2. L'account di sicurezza mantiene lo stato di sicurezza generale. Usalo per cercare le vulnerabilità in tutti gli account.
3. Le connessioni di rete centralizzate in locale vengono condivise con altri account. Controlla la comunicazione tra account con. [AWS Transit Gateway](#)
4. Gli utenti interagiscono con i dati e sviluppano modelli di machine learning (ML) con sicurezza e accesso ai dati corretti. Pubblica i modelli finali con l'[SageMaker IA](#).
5. I log centralizzati monitorano tutti gli account per verificare le attività. Da utilizzare [CloudWatch](#) per la registrazione unificata.
6. Utilizza tutti gli strumenti di cui i tuoi clienti hanno bisogno per presentare i dati. Questi includono strumenti o AWS servizi di terze parti come [Quick](#).
7. DevOps i flussi implementano il codice come servizio e gli artefatti negli account di acquisizione e analisi.
8. Gli utenti che necessitano di modelli di analisi per lo sviluppo e il test lavorano con sicurezza e governance dei dati corrette.
9. I servizi dati centralizzati forniscono governance e gestione delle API. Esegui query su petabyte di dati in [Amazon S3 tramite Amazon Redshift Spectrum](#). <https://docs.aws.amazon.com/redshift/latest/dg/> Trasforma i dati con Amazon EMR. <https://docs.aws.amazon.com/emr/latest/ManagementGuide/> Archivi sicuri con [Lake Formation](#).
10. Controlla l'inserimento in batch o in streaming che alimenta il data lake. Usa [Kinesis per lo streaming di dati in tempo](#) reale.
11. I servizi comuni condivisi con altri account includono le AMI dorate e la gestione DNS.

Approfondimenti

Per ulteriori informazioni, consulta le seguenti risorse:

- [AWS Icone dell'architettura](#)
- [AWS Centro di architettura](#)
- [AWS Well-Architected](#)

Storia del diagramma

Per ricevere aggiornamenti su questo diagramma di architettura di riferimento, abbonatevi al feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	Diagramma dell'architettura di riferimento pubblicato per la prima volta.	21 dicembre 2020

Requisito di abbonamento RSS

Per iscriverti agli aggiornamenti RSS, devi avere un plug-in RSS abilitato per il browser che stai utilizzando.

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.