AWS White paper

SageMaker Best practice per l'amministrazione di Studio

SageMaker Best practice per l'amministrazione di Studio: AWS White paper

Table of Contents

SageMaker Best practice per l'amministrazione di Studio

Data di pubblicazione: 25 aprile 2023 (Revisioni del documento)

Sintesi

Amazon SageMaker AI Studio offre un'unica interfaccia visiva basata sul Web in cui è possibile eseguire tutte le fasi di sviluppo dell'apprendimento automatico (ML), migliorando la produttività del team di data science. SageMaker AI Studio ti offre accesso, controllo e visibilità completi in ogni fase necessaria per creare, addestrare e valutare i modelli.

In questo white paper, discutiamo le migliori pratiche per argomenti quali modello operativo, gestione dei domini, gestione delle identità, gestione delle autorizzazioni, gestione della rete, registrazione, monitoraggio e personalizzazione. Le migliori pratiche discusse qui sono destinate all'implementazione di SageMaker AI Studio a livello aziendale, incluse le implementazioni multi-tenant. Questo documento è destinato agli amministratori della piattaforma ML, agli ingegneri ML e agli architetti ML.

Sei tu Well-Architected?

Il AWS Well-Architected Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando AWS Well-Architected Tool, disponibile gratuitamente in Console di gestione AWS, puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

In Machine Learning Lens, ci concentriamo su come progettare, implementare e progettare i carichi di lavoro di machine learning in. Cloud AWS Questo obiettivo si aggiunge alle migliori pratiche descritte nel Well-Architected Framework.

Introduzione

Quando amministri SageMaker AI Studio come piattaforma ML, hai bisogno di linee guida sulle migliori pratiche per prendere decisioni informate che ti aiutino a scalare la tua piattaforma ML man mano che i carichi di lavoro crescono. Per il provisioning, l'operatività e la scalabilità della piattaforma ML, considera quanto segue:

- Scegliete il modello operativo giusto e organizzate i vostri ambienti ML per raggiungere i vostri obiettivi aziendali.
- Scegli come configurare l'autenticazione del dominio SageMaker AI Studio per le identità degli utenti e considera le limitazioni a livello di dominio.
- Decidi come federare l'identità e l'autorizzazione dei tuoi utenti alla piattaforma ML per controlli di accesso e audit dettagliati.
- Prendi in considerazione la possibilità di impostare autorizzazioni e barriere per i vari ruoli dei tuoi personaggi ML.
- Pianifica la topologia di rete del tuo cloud privato virtuale (VPC), considerando la sensibilità del carico di lavoro ML, il numero di utenti, i tipi di istanze, le app e i processi avviati.
- Classificate e proteggete i dati archiviati e in transito con la crittografia.
- Considerate come registrare e monitorare varie interfacce di programmazione delle applicazioni (APIs) e le attività degli utenti per verificarne la conformità.
- Personalizza l'esperienza del notebook SageMaker AI Studio con le tue immagini e gli script di configurazione del ciclo di vita.

Modello operativo

Un modello operativo è un framework che riunisce persone, processi e tecnologie per aiutare un'organizzazione a fornire valore aziendale in modo scalabile, coerente ed efficiente. Il modello operativo ML fornisce un processo di sviluppo del prodotto standard per i team di tutta l'organizzazione. Esistono tre modelli per l'implementazione del modello operativo, a seconda delle dimensioni, della complessità e dei fattori di business:

- Team centralizzato di data science: in questo modello, tutte le attività di data science sono centralizzate all'interno di un singolo team o organizzazione. È simile al modello Center of Excellence (COE), in cui tutte le unità aziendali si rivolgono a questo team per progetti di data science.
- Team decentralizzati di data science: in questo modello, le attività di data science sono distribuite tra diverse funzioni o divisioni aziendali o basate su diverse linee di prodotti.
- Team federati di data science: in questo modello, le funzioni di servizi condivisi come gli archivi di codice, le pipeline di integrazione e distribuzione continua (CI/CD) e così via sono gestite dal team centralizzato e ogni unità aziendale o funzione a livello di prodotto è gestita da team decentralizzati. È simile al modello hub and spoke, in cui ogni unità aziendale ha i propri team di data science; tuttavia, questi team di business unit coordinano le proprie attività con il team centralizzato.

Prima di decidere di lanciare il tuo primo studio domain per casi d'uso in produzione, prendi in considerazione il tuo modello operativo e le AWS best practice per organizzare il tuo ambiente. Per ulteriori informazioni, consulta Organizzare AWS l'ambiente utilizzando più account.

La sezione successiva fornisce indicazioni sull'organizzazione della struttura degli account per ciascuno dei modelli operativi.

Struttura dell'account consigliata

In questa sezione, introduciamo brevemente una struttura contabile modello operativo che è possibile iniziare e modificare in base ai requisiti operativi dell'organizzazione. Indipendentemente dal modello operativo scelto, consigliamo di implementare le seguenti best practice comuni:

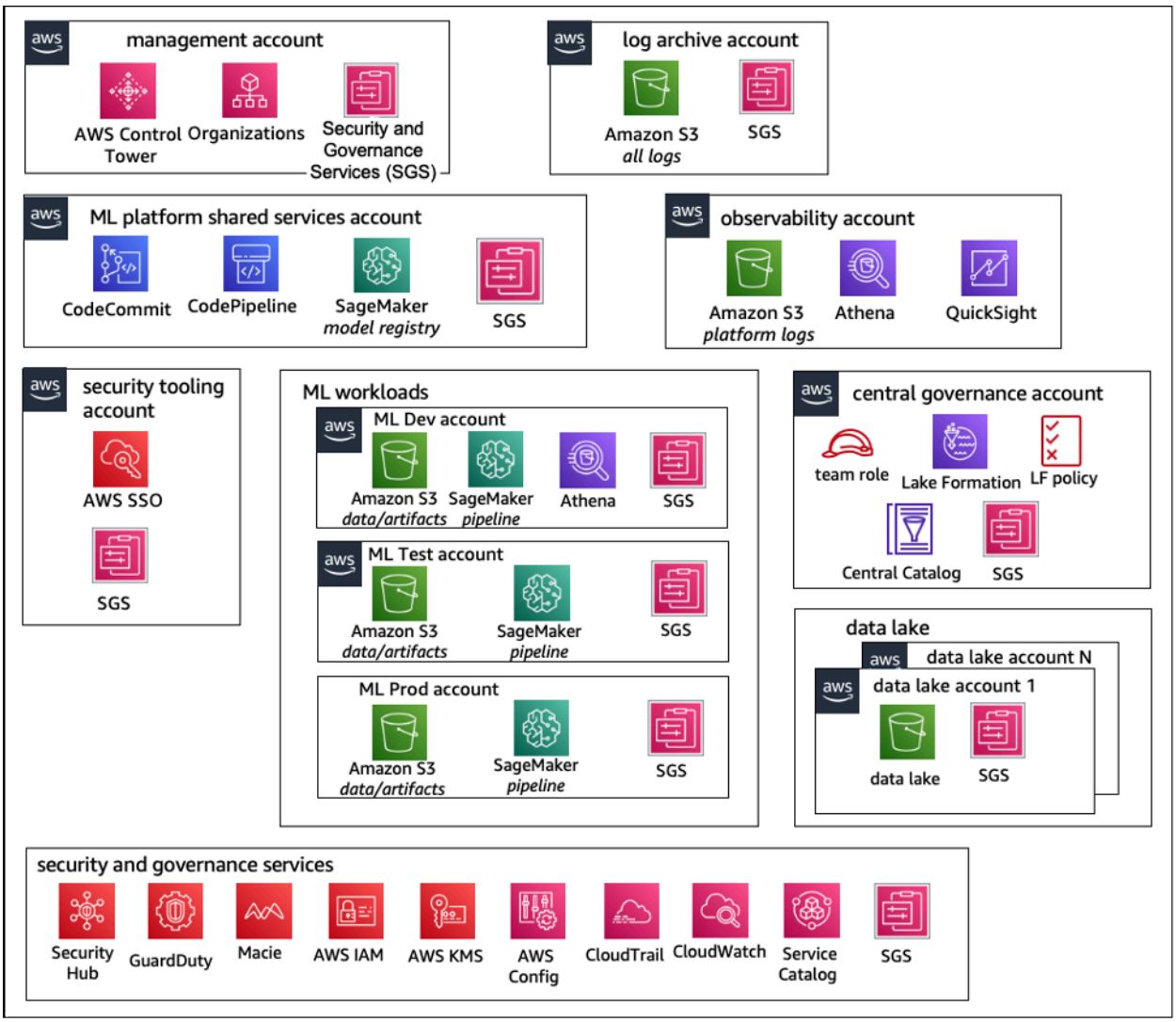
- AWS Control TowerUtilizzalo per la configurazione, la gestione e la governance dei tuoi account.
- Centralizza le tue identità con il tuo Identity Provider (IdP) e AWS IAMIdentity Center con un account Securitiy Tooling amministratore delegato e abilita l'accesso sicuro ai carichi di lavoro.

- Esegui carichi di lavoro ML con isolamento a livello di account tra carichi di lavoro di sviluppo, test e produzione.
- Trasmetti i log dei carichi di lavoro ML a un account di archiviazione dei log, quindi filtra e applica l'analisi dei log in un account di osservabilità.
- Esegui un account di governance centralizzato per il provisioning, il controllo e il controllo dell'accesso ai dati.
- Integra i servizi di sicurezza e governance (SGS) con protezioni preventive e investigative appropriate in ogni account per garantire sicurezza e conformità, in base ai requisiti dell'organizzazione e del carico di lavoro.

Struttura contabile modello centralizzata

In questo modello, il team della piattaforma ML è responsabile di fornire:

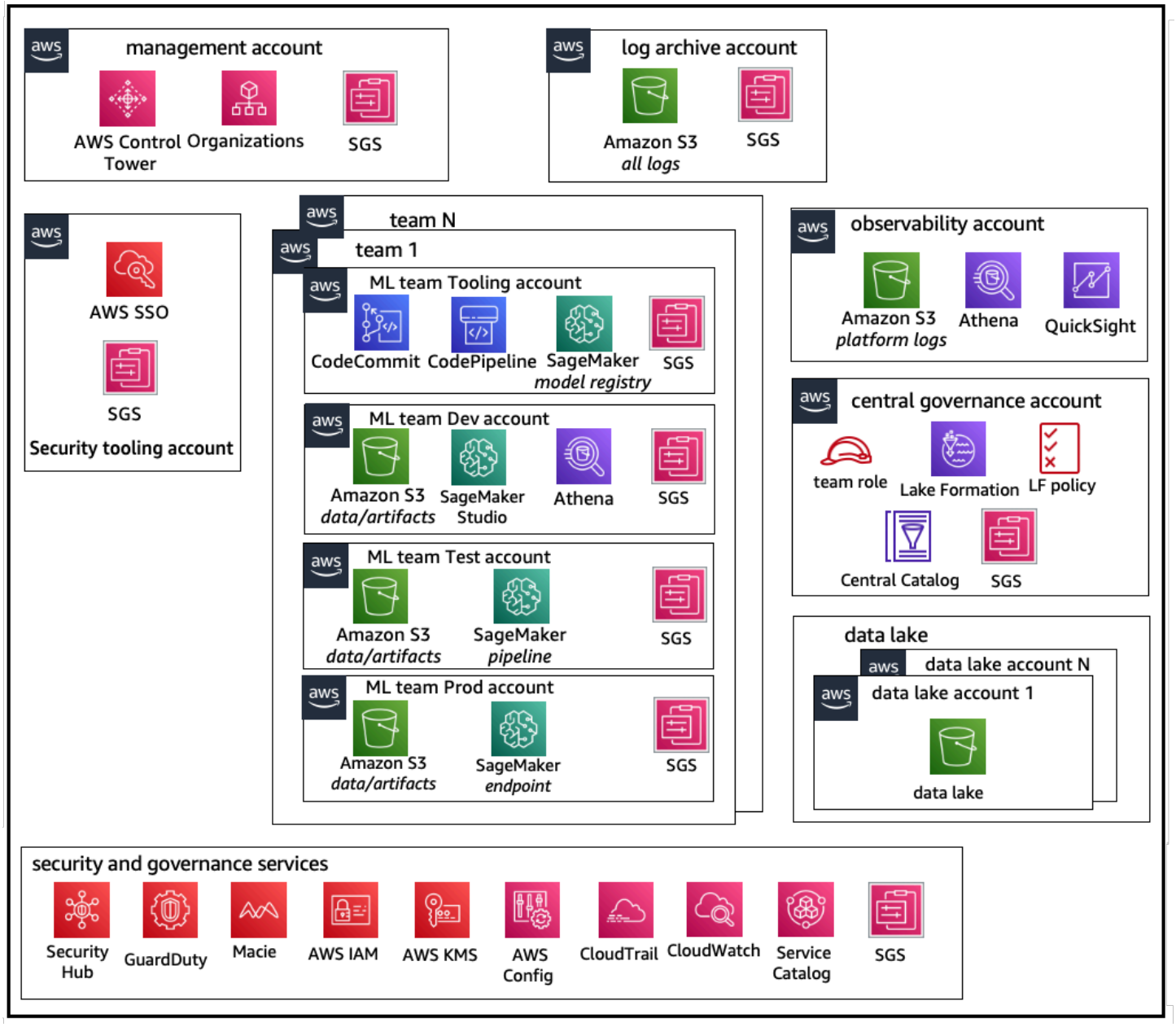
- Un account di strumenti di servizi condivisi che soddisfa i requisiti di Machine Learning Operations (MLOps) tra i team di data science.
- Account di sviluppo, test e produzione di carichi di lavoro ML condivisi tra i team di data science.
- Politiche di governance per garantire che il carico di lavoro di ogni team di data science venga eseguito in modo isolato.
- Le migliori pratiche comuni.



Struttura degli account del modello operativo centralizzato

Struttura contabile modello decentralizzata

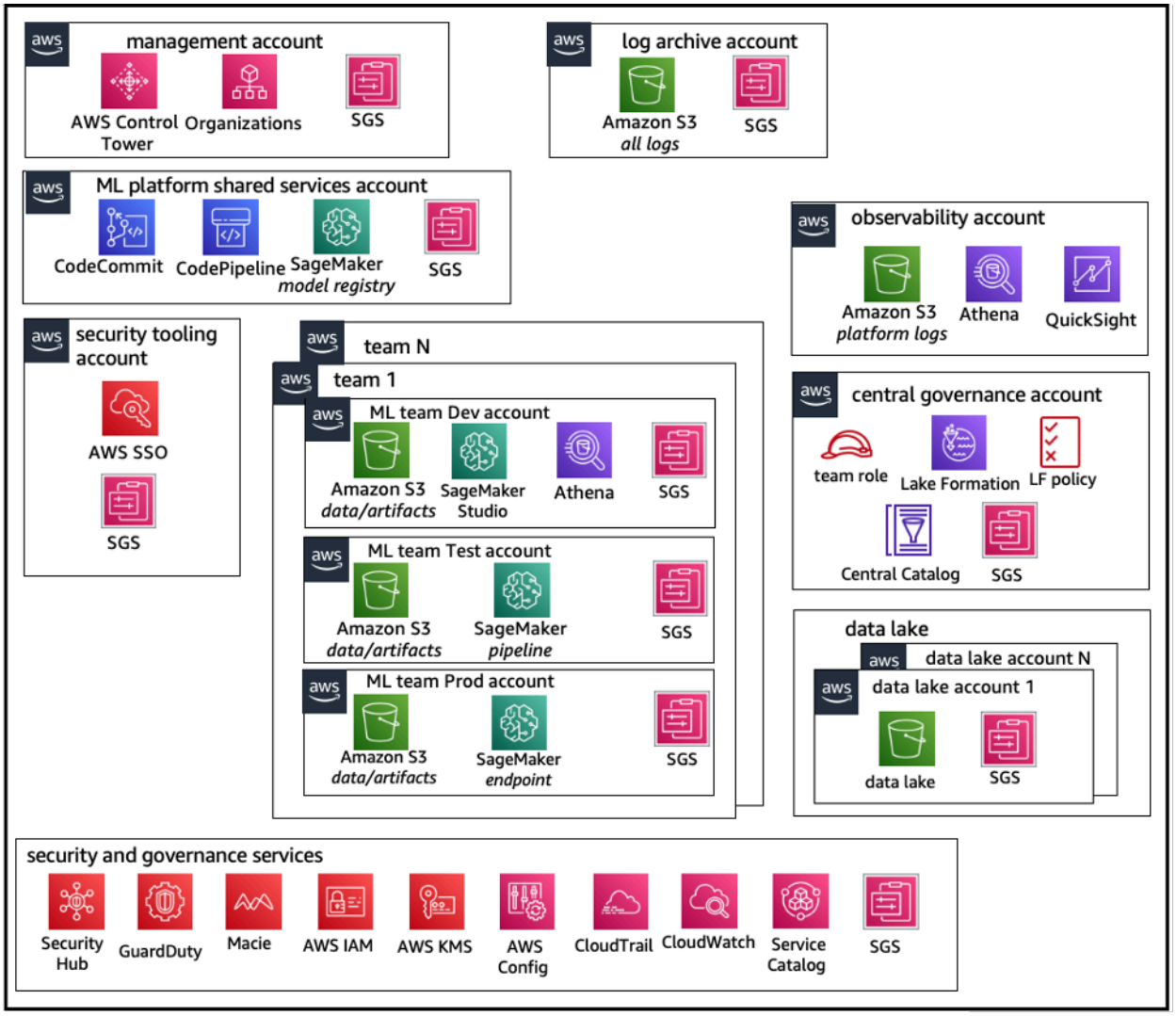
In questo modello, ogni team ML opera in modo indipendente per il provisioning, la gestione e la gestione di account e risorse ML. Tuttavia, consigliamo ai team di ML di utilizzare un approccio centralizzato basato su osservabilità e governance dei dati per semplificare la governance dei dati e la gestione degli audit.



Struttura dei conti del modello operativo decentralizzato

Struttura contabile modello federato

Questo modello è simile al modello centralizzato; tuttavia, la differenza fondamentale è che ogni science/ML team gets their own set of development/test/production carico di lavoro di dati consente un solido isolamento fisico delle risorse ML e consente inoltre a ciascun team di scalare in modo indipendente senza influire sugli altri team.



Struttura dei conti del modello operativo federato

Piattaforma ML multitenancy

La multitenancy è un'architettura software in cui una singola istanza software può servire più gruppi di utenti distinti. Un tenant è un gruppo di utenti che condividono l'accesso comune con privilegi specifici all'istanza del software. Ad esempio, se state creando diversi prodotti ML, ogni team di prodotto con requisiti di accesso simili può essere considerato un tenant o un team.

Sebbene sia possibile implementare più team all'interno di un'istanza di SageMaker AI Studio (come SageMaker AI Domain), valuta questi vantaggi rispetto a compromessi come blast radius, attribuzione dei costi e limiti a livello di account quando riunisci più team in un unico dominio di AI Studio. SageMaker Scopri di più su questi compromessi e sulle migliori pratiche nelle sezioni seguenti.

Se hai bisogno di un isolamento assoluto delle risorse, prendi in considerazione l'implementazione dei domini SageMaker AI Studio per ogni tenant in un account diverso. A seconda dei requisiti di isolamento, puoi implementare più linee di attività (LOBs) come più domini all'interno di un unico account e regione. Utilizza spazi condivisi per una collaborazione quasi in tempo reale tra i membri dello stesso LOB team/. Con più domini, continuerai a utilizzare le politiche e le autorizzazioni di Identity Access Management (IAM) per garantire l'isolamento delle risorse.

SageMaker Le risorse di intelligenza artificiale create da un dominio vengono etichettate automaticamente con il dominio Amazon Resource Name (ARN) e il profilo o lo spazio utente ARN per un facile isolamento delle risorse. Per esempi di policy, consulta la documentazione sull'isolamento delle risorse di dominio. Qui puoi vedere il riferimento dettagliato su quando utilizzare una strategia multi-account o multidominio, insieme ai confronti delle funzionalità nella documentazione, e puoi visualizzare script di esempio per riempire i tag per i domini esistenti nel repository. GitHub

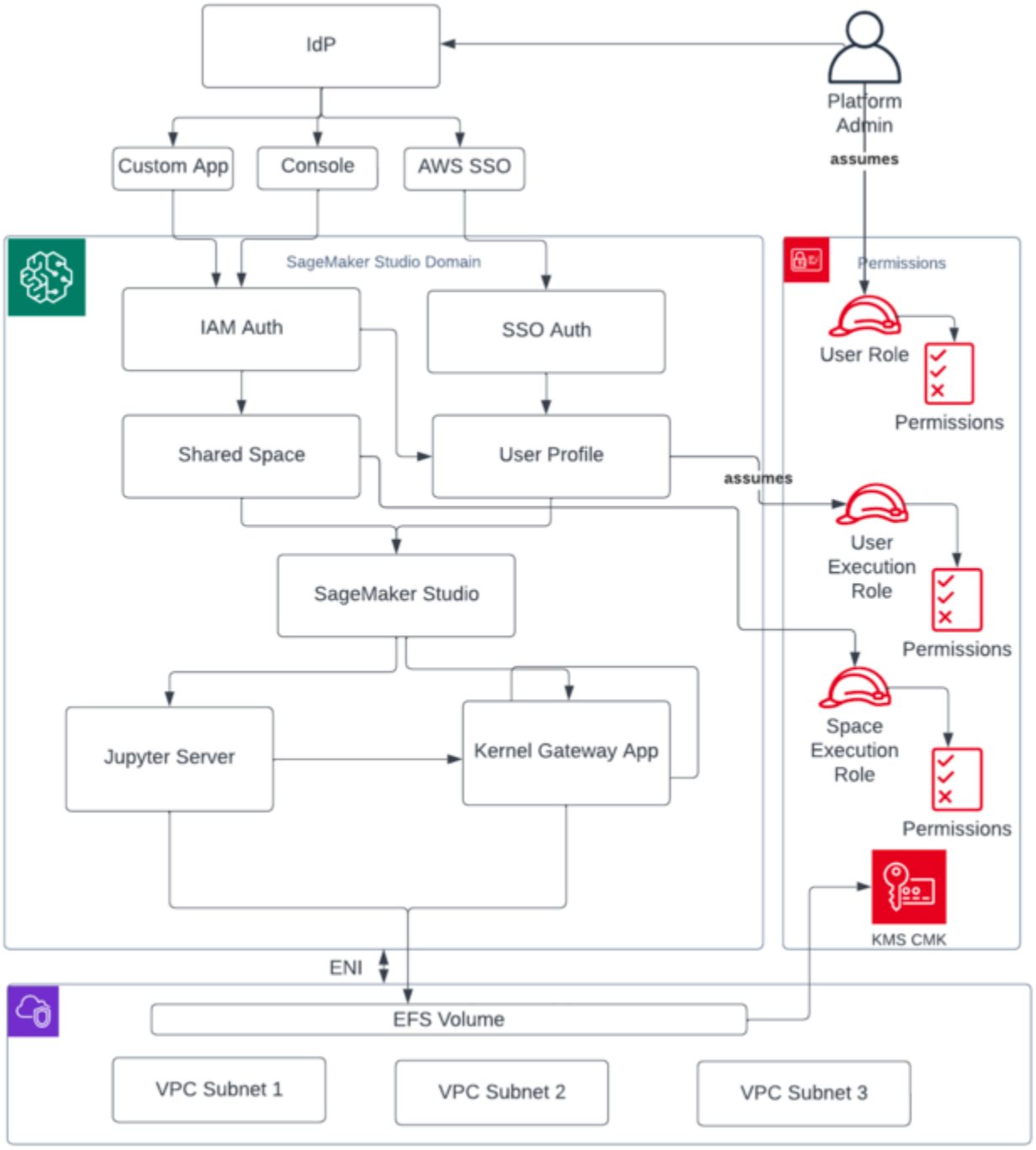
Infine, puoi implementare un'implementazione self-service delle risorse di AI Studio in più account utilizzando. SageMaker AWS Service Catalog Per ulteriori informazioni, consulta Gestire i AWS Service Catalog prodotti in più Account AWS e Regioni AWS.

Gestione dei domini

Un dominio Amazon SageMaker AI è composto da:

- Un volume Amazon Elastic File System (AmazonEFS) associato
- Un elenco di utenti autorizzati
- Una varietà di configurazioni di sicurezza, applicazioni, policy e Amazon Virtual Private Cloud (AmazonVPC)

Il diagramma seguente fornisce una visione di alto livello dei vari componenti che costituiscono un dominio: SageMaker AIStudio

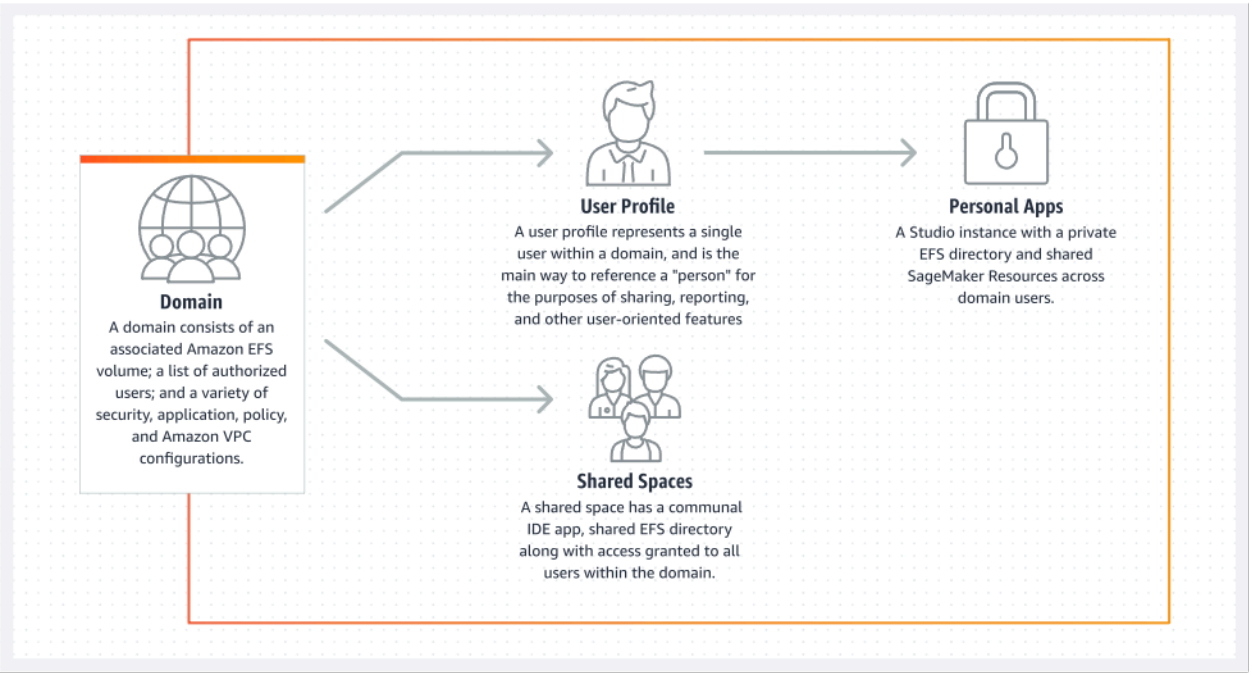


Vista di alto livello dei vari componenti che costituiscono un dominio AI Studio SageMaker

Domini multipli e spazi condivisi

Amazon SageMaker AI ora supporta la creazione di più domini SageMaker AI in un unico dominio Regione AWS per ogni account. Ogni dominio può avere le proprie impostazioni di dominio, come la modalità di autenticazione e le impostazioni di rete, come VPC le sottoreti. Un profilo utente non può essere condiviso tra domini. Se un utente umano fa parte di più team separati da domini, crea un profilo utente per l'utente in ogni dominio. Consulta la panoramica sui domini multipli per ulteriori informazioni sul riempimento dei tag per i domini esistenti.

Ogni dominio configurato in modalità di IAM autenticazione può utilizzare lo spazio condiviso per una collaborazione quasi in tempo reale tra gli utenti. Con uno spazio condiviso, gli utenti hanno accesso a una EFS directory Amazon condivisa e a un'JupyterServerapp condivisa per l'interfaccia utente e possono modificare insieme quasi in tempo reale. L'etichettatura automatica delle risorse create dagli spazi condivisi consente agli amministratori di tenere traccia dei costi a livello di progetto. L' JupyterServer interfaccia utente condivisa filtra anche risorse come esperimenti e voci del registro dei modelli in modo che vengano visualizzati solo gli elementi pertinenti all'attività di machine learning condivisa. Il diagramma seguente fornisce una panoramica delle app private e degli spazi condivisi all'interno di ciascun dominio.



Panoramica delle app private e degli spazi condivisi all'interno di un singolo dominio

Configura spazi condivisi nel tuo dominio

Gli spazi condivisi vengono in genere creati per una particolare attività o progetto di machine learning in cui i membri di un singolo dominio richiedono l'accesso quasi in tempo reale allo stesso archivio di file sottostante e. IDE L'utente può accedere, leggere, modificare e condividere i propri taccuini quasi in tempo reale, il che gli offre il percorso più rapido per iniziare a iterare con i colleghi.

Per creare uno spazio condiviso, è necessario innanzitutto designare un ruolo di esecuzione predefinito dello spazio che regolerà le autorizzazioni per qualsiasi utente che utilizza lo spazio. Al momento della stesura di questo documento, tutti gli utenti all'interno di un dominio avranno accesso a tutti gli spazi condivisi del proprio dominio. Fai riferimento a Creare uno spazio condiviso per la documentazione più recente sull'aggiunta di spazi condivisi a un dominio esistente.

Configura il tuo dominio per la IAM federazione

Prima di configurare AWS Identity and Access Management (IAM) la federazione per il tuo dominio SageMaker AI Studio, devi configurare un ruolo utente IAM federativo (ad esempio un amministratore di piattaforma) nel tuo IdP, come discusso nella sezione Gestione delle identità.

Per istruzioni dettagliate sulla configurazione di SageMaker AI Studio con l'IAMopzione, consulta Onboard to Amazon SageMaker Domain Using IAM Identity Center.

Configura il tuo dominio per la federazione Single Sign-on () SSO

Per utilizzare la federazione Single Sign-on (SSO), devi abilitarla AWS IAM Identity Center nel tuo account di AWS Organizationsgestione nella stessa regione in cui devi eseguire AI Studio. SageMaker I passaggi di configurazione del dominio sono simili ai passaggi di IAM federazione, tranne per la selezione AWS IAM Identity Center(iDC) nella sezione Autenticazione.

Per istruzioni dettagliate, consulta Onboard to Amazon SageMaker Domain Using IAM Identity Center.

SageMaker Profilo utente AI Studio

Un profilo utente rappresenta un singolo utente all'interno di un dominio ed è il modo principale per fare riferimento a una «persona» ai fini della condivisione, della creazione di report e di altre funzionalità orientate all'utente. Questa entità viene creata quando un utente entra a far parte di toSageMaker AI Studio. Se un amministratore invita una persona via e-mail o la importa da iDC,

viene creato automaticamente un profilo utente. Un profilo utente è il principale detentore delle impostazioni per un singolo utente e ha un riferimento alla home directory privata Amazon Elastic File System (AmazonEFS) dell'utente. Consigliamo di creare un profilo utente per ogni utente fisico dell'applicazione SageMaker AI Studio. Ogni utente ha la propria directory dedicata su Amazon e EFS i profili utente non possono essere condivisi tra domini dello stesso account.

Ogni profilo utente che condivide il dominio SageMaker AI Studio riceve risorse di elaborazione dedicate (come istanze SageMaker AI Amazon Elastic Compute Cloud (AmazonEC2)) per eseguire i notebook. Le istanze di calcolo assegnate al primo utente sono completamente isolate da quelle assegnate al secondo utente. Analogamente, le risorse di calcolo assegnate agli utenti in un AWS account sono completamente separate da quelle assegnate agli utenti in un altro account. Ogni utente può eseguire fino a quattro applicazioni (app) all'interno di contenitori Docker isolati o immagini sullo stesso tipo di istanza.

App Jupyter Server

Quando avvii un notebook Amazon SageMaker AI Studio per un utente accedendo al file prefirmato URL o effettuando l'accesso tramite AWS IAM iDC, l'app Jupyter Server viene avviata nell'istanza gestita dal servizio AI. SageMaker VPC Ogni utente ottiene la propria app Jupyter Server dedicata in un'app privata. Per impostazione predefinita, l'app Jupyter Server per notebook SageMaker AI Studio viene eseguita su un'*`ml.t3.medium`*istanza dedicata (riservata come tipo di istanza di sistema). Il calcolo per questa istanza non viene fatturato al cliente.

L'app Jupyter Kernel Gateway

L'app Kernel Gateway può essere creata tramite l'interfaccia API o l'interfaccia SageMaker AI Studio e viene eseguita sul tipo di istanza scelto. Questa app può essere eseguita utilizzando una delle immagini integrate di SageMaker AI Studio preconfigurate con i più diffusi pacchetti di data science e deep learning come TensorFlowApache MXNet e. PyTorch

Gli utenti possono avviare ed eseguire più kernel di notebook Jupyter, sessioni terminali e console interattive all'interno dello stesso Studio. SageMaker image/Kernel Gateway app. Users can also run up to four Kernel Gateway apps or images on the same physical instance—each isolated by its container/image

Per creare app aggiuntive, è necessario utilizzare un tipo di istanza diverso. Un profilo utente può avere una sola istanza in esecuzione, di qualsiasi tipo di istanza. Ad esempio, un utente può eseguire

sulla stessa istanza sia un semplice notebook utilizzando l'immagine di data science integrata in SageMaker AI Studio, sia un altro notebook utilizzando l' TensorFlow immagine integrata. Agli utenti viene fatturato il tempo in cui l'istanza è in esecuzione. Per evitare costi quando l'utente non esegue attivamente SageMaker AI Studio, deve chiudere l'istanza. Per ulteriori informazioni, consulta Chiudi e aggiorna le app di Studio.

Ogni volta che chiudi e riapri un'app Kernel Gateway dall'interfaccia di SageMaker AI Studio, quell'app viene avviata su una nuova istanza. Ciò significa che l'installazione del pacchetto non viene mantenuta dopo il riavvio della stessa app. Analogamente, se un utente modifica il tipo di istanza su un notebook, i pacchetti installati e le variabili di sessione andranno persi. Tuttavia, puoi utilizzare funzionalità come Bring Your Own Image e Lifecycle Script per portare i pacchetti dell'utente in SageMaker AI Studio e renderli permanenti durante i cambi di istanza e il lancio di nuove istanze.

Volume Amazon Elastic File System

Quando viene creato un dominio, viene creato un singolo volume Amazon Elastic File System (AmazonEFS) che può essere utilizzato da tutti gli utenti all'interno del dominio. Ogni profilo utente riceve una home directory privata all'interno del EFS volume Amazon per archiviare i notebook, gli GitHub archivi e i file di dati dell'utente. Ogni spazio all'interno di un dominio riceve una directory privata all'interno del EFS volume Amazon a cui è possibile accedere da più profili utente. L'accesso alle cartelle è separato per utente, tramite le autorizzazioni del filesystem. SageMaker AI Studio crea un ID utente unico globale per ogni profilo utente o spazio e lo applica come interfaccia del sistema operativo portatile () POSIX dall'accesso ai suoi dati. user/group ID for the user's home directory on EFS, which prevents other users/spaces

Backup e ripristino

Un EFS volume esistente non può essere collegato a un nuovo dominio SageMaker AI. In un'impostazione di produzione, assicurati di aver eseguito il backup EFS del volume Amazon (su un altro EFS volume o su Amazon Simple Storage Service (Amazon S3)). Se un EFS volume viene eliminato accidentalmente, l'amministratore deve smontare e ricreare il dominio AI Studio. SageMaker Di seguito è riportato il procedimento:

Esegui il backup dell'elenco dei profili utente, degli spazi e dell'EFSutente associato IDs (UIDs) tramite `ListUserProfiles` `DescribeUserProfileList Spaces`, e chiamate. `DescribeSpace` API

1. Crea un nuovo dominio SageMaker AI Studio.
2. Crea i profili e gli spazi utente.
3. Per ogni profilo utente, copia i file dal backup su EFS /Amazon S3.
4. Facoltativamente, elimina tutte le app e i profili utente nel vecchio dominio SageMaker AI Studio.

Per istruzioni dettagliate, consulta la sezione dell'appendice Backup e ripristino del dominio SageMaker AI Studio.

> **Note**
>
> Ciò può essere ottenuto anche eseguendo `LifecycleConfigurations` il backup dei dati da e verso S3 ogni volta che un utente avvia l'app.

EBSVolume Amazon

Un volume di storage Amazon Elastic Block Store (AmazonEBS) è inoltre collegato a ciascuna istanza di SageMaker AI Studio Notebook. Viene utilizzato come volume principale del contenitore o dell'immagine in esecuzione sull'istanza. Sebbene EFS lo storage Amazon sia persistente, il EBS volume Amazon collegato al container è temporaneo. I dati archiviati localmente sul EBS volume Amazon non verranno conservati se il cliente elimina l'app.

Garantire l'accesso ai file prefirmati URL

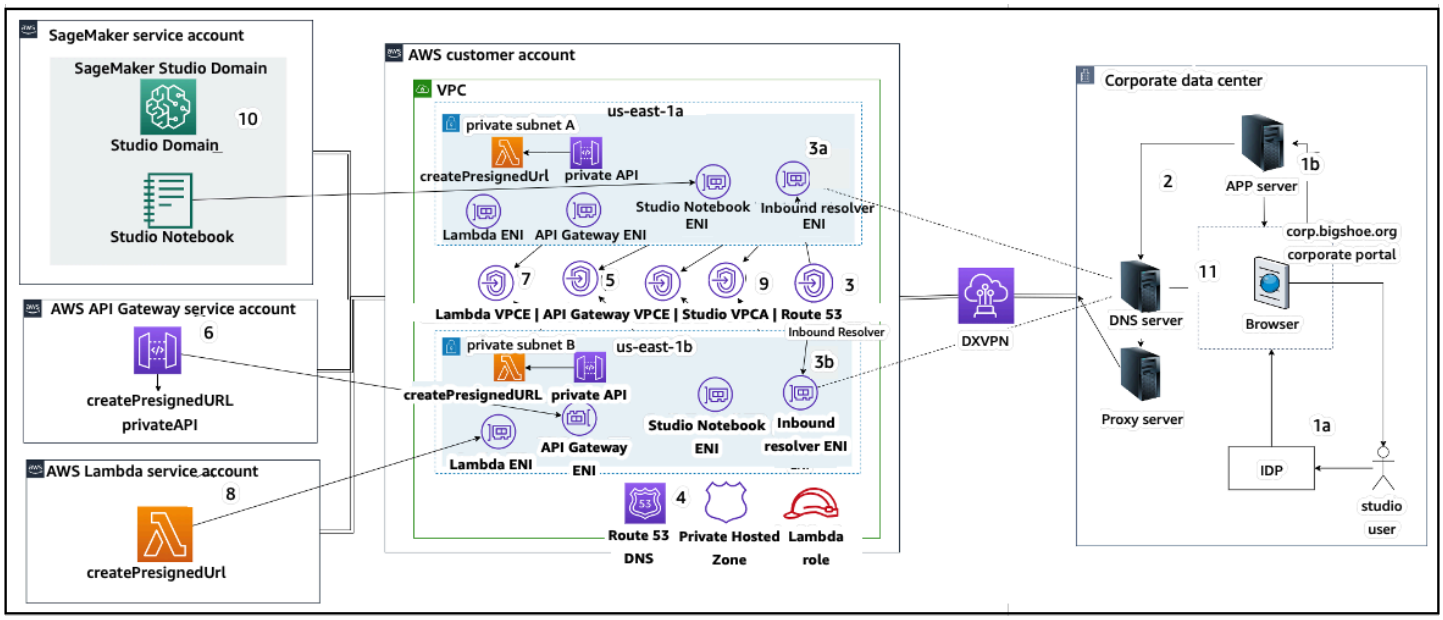
Quando un utente di SageMaker AI Studio apre il collegamento al notebook, SageMaker AI Studio convalida la IAM politica dell'utente federato per autorizzare l'accesso e genera e risolve la politica prefirmata per l'utente. URL Poiché la console SageMaker AI funziona su un dominio Internet, questo dominio generato e prefirmato URL è visibile nella sessione del browser. Ciò rappresenta un vettore di minaccia indesiderato per il furto di dati e l'accesso ai dati dei clienti quando non vengono applicati i controlli di accesso adeguati.

Studio supporta alcuni metodi per applicare i controlli di accesso contro il furto di dati prefirmati: URL

- Convalida dell'IP del client utilizzando la condizione della policy IAM `aws:sourceIp`
- VPCConvalida del client utilizzando la condizione IAM `aws:sourceVpc`
- Convalida VPC degli endpoint del client utilizzando la condizione della policy IAM `aws:sourceVpce`

Quando accedi SageMaker ai notebook AI Studio dalla console SageMaker AI, l'unica opzione disponibile consiste nell'utilizzare la convalida dell'IP del client con la condizione della policy. IAM `aws:sourceIp` Tuttavia, puoi utilizzare prodotti di routing del traffico via browser come Zscaler per garantire scalabilità e conformità per l'accesso a Internet della tua forza lavoro. Questi prodotti di routing del traffico generano il proprio IP di origine, il cui intervallo IP non è controllato dal cliente aziendale. Ciò rende impossibile per questi clienti aziendali utilizzare `aws:sourceIp` questa condizione.

Per utilizzare la convalida degli VPC endpoint del client utilizzando la condizione della IAM policy`aws:sourceVpce`, la creazione di un dispositivo prefirmato URL deve provenire dallo stesso cliente in VPC cui viene implementato SageMaker AI Studio e la risoluzione delle URL esigenze prefirmate deve avvenire tramite un endpoint SageMaker AI Studio VPC sul cliente. VPC Questa risoluzione dei dati prefirmati URL durante il periodo di accesso per gli utenti della rete aziendale può essere eseguita utilizzando regole di DNS inoltro (sia in Zscaler che aziendaliDNS) e quindi nell'endpoint del cliente VPC utilizzando un resolver in ingresso Amazon Route 53, come mostrato nella seguente architettura:



Accesso a Studio prefirmato URL con VPC endpoint tramite rete aziendale

Per step-by-step indicazioni sulla configurazione dell'architettura precedente, consulta Secure Amazon SageMaker AI Studio presigned URLs Part 1: Foundational infrastructure.

SageMaker Quote e limiti dei domini AI

- SageMaker La SSO federazione dei domini di AI Studio è supportata solo nella regione, tra gli account dei membri dell' AWS organizzazione in cui viene fornito AWS Identity Center.
- Gli spazi condivisi non sono attualmente supportati con i domini configurati con AWS Identity Center.
- VPCe la configurazione della sottorete non può essere modificata dopo la creazione del dominio. È tuttavia possibile creare un nuovo dominio con una configurazione di sottorete diversaVPC.
- L'accesso al dominio non può essere cambiato da una SSO modalità all'altra dopo la creazione del dominio. IAM È possibile creare un nuovo dominio con una modalità di autenticazione diversa.
- È previsto un limite di quattro app kernel gateway per tipo di istanza lanciate per ogni utente.
- Ogni utente può avviare solo un'istanza per ogni tipo di istanza.
- Esistono limiti alle risorse consumate all'interno di un dominio, ad esempio il numero di istanze avviate per tipo di istanza e il numero di profili utente che è possibile creare. Consulta la pagina relativa alle quote di servizio per un elenco completo dei limiti del servizio.
- I clienti possono presentare una richiesta di assistenza aziendale motivando la propria attività ad aumentare i limiti predefiniti relativi alle risorse, ad esempio il numero di domini o i profili utente, entro limiti a livello di account.
- Il limite rigido al numero di app simultanee per account è di 2.500 app. I domini e i limiti dei profili utente dipendono da questo limite rigido. Ad esempio, un account può avere un singolo dominio con 1.000 profili utente o 20 domini con 50 profili utente ciascuno.

Gestione delle identità

Questa sezione illustra come gli utenti della forza lavoro presenti in un elenco aziendale si federano Account AWS e accedono ad AI Studio. SageMaker Innanzitutto, descriveremo brevemente come vengono mappati utenti, gruppi e ruoli e come funziona la federazione degli utenti.

Utenti, gruppi e ruoli

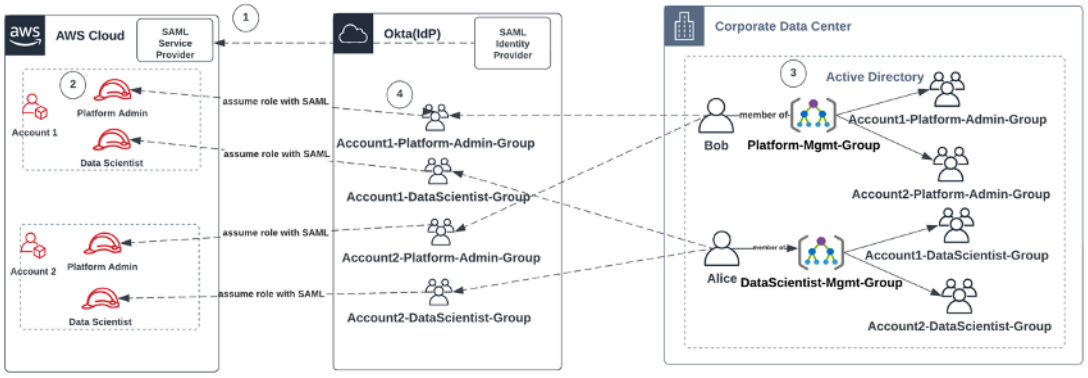
In AWS, le autorizzazioni delle risorse vengono gestite utilizzando utenti, gruppi e ruoli. I clienti possono gestire i propri utenti e gruppi tramite IAM o in una directory aziendale come Active Directory (AD), abilitata tramite un IdP esterno come Okta, che consente loro di autenticare gli utenti su varie applicazioni in esecuzione nel cloud e in locale.

Come illustrato nella sezione AWS Security Pillar Identity Management, è consigliabile gestire le identità degli utenti in un IdP centrale, poiché ciò aiuta a integrarsi facilmente con i processi HR di back-end e aiuta a gestire l'accesso agli utenti della forza lavoro.

IdPs come Okta, consentono agli utenti finali di autenticarsi a uno o più ruoli Account AWS e di accedere a ruoli specifici utilizzando SSO il linguaggio di markup di assertazione di sicurezza (). SAML Gli amministratori IdP hanno la possibilità di scaricare ruoli da Account AWS IdP e assegnarli agli utenti. Quando si accede a AWS, agli utenti finali viene presentata una AWS schermata che mostra un elenco dei AWS ruoli loro assegnati in uno o più ruoli. Account AWS Possono selezionare il ruolo da assumere per l'accesso, che definisce le loro autorizzazioni per la durata di quella sessione autenticata.

In IdP deve esistere un gruppo per ogni combinazione specifica di account e ruolo a cui desideri fornire l'accesso. Puoi pensare a questi gruppi come a gruppi con AWS ruoli specifici. A qualsiasi utente che fa parte di questi gruppi con ruoli specifici viene concessa un'unica autorizzazione: l'accesso a un ruolo specifico in uno specifico. Account AWS Tuttavia, questo singolo processo di autorizzazione non è scalabile per gestire l'accesso degli utenti assegnando ogni utente a gruppi di ruoli specifici. AWS Per semplificare l'amministrazione, si consiglia inoltre di creare una serie di gruppi per tutti i diversi set di utenti dell'organizzazione che richiedono set di autorizzazioni diversi. AWS

Per illustrare la configurazione centrale dell'IdP, si consideri un'azienda con configurazione AD, in cui utenti e gruppi sono sincronizzati con la directory IdP. Nel AWS, questi gruppi AD sono mappati su ruoli. IAM Di seguito sono riportate le fasi principali del flusso di lavoro:



Flusso di lavoro per l'onboarding di utenti, gruppi e ruoli AD IAM

1. Nel AWS, configura SAML l'integrazione per ognuno di voi Account AWS con il proprio IdP.
2. In AWS, configura i ruoli in ciascuno Account AWS e sincronizza con IdP.
3. Nel sistema AD aziendale:
   a. Crea un gruppo AD per ogni ruolo dell'account e sincronizzalo con IdP (ad esempio, `Account1-Platform-Admin-Group` (noto anche come gruppo di AWS ruoli)).
   b. Crea un gruppo di gestione a ogni livello di persona (ad esempio`Platform-Mgmt-Group`) e assegna gruppi di AWS ruoli come membri.
   c. Assegna gli utenti a quel gruppo di gestione per consentire l'accesso ai Account AWS ruoli.
4. In IdP, associa i gruppi di AWS ruoli (ad esempio`Account1-Platform-Admin-Group`) ai Account AWS ruoli (come Platform Admin in Account1).
5. Quando Data Scientist Alice accede a Idp, viene presentata un'interfaccia utente AWS della Federation App con due opzioni tra cui scegliere: «Account 1 Data Scientist» e «Account 2 Data Scientist».
6. Alice sceglie l'opzione «Account 1 Data Scientist» e viene collegata alla sua applicazione autorizzata in Account 1 (AI Console). AWS SageMaker

Per istruzioni dettagliate sulla configurazione della federazione degli SAML account, consulta How to Configure SAML 2.0 for Account Federation di Okta. AWS

Federazione degli utenti

L'autenticazione per SageMaker AI Studio può essere eseguita utilizzando IAM o IAM IDC. Se gli utenti sono gestiti tramiteIAM, possono scegliere la IAM modalità. Se l'azienda utilizza un IdP

esterno, può eseguire la federazione tramite IAM o IDC. IAM Tieni presente che la modalità di autenticazione non può essere aggiornata per un dominio SageMaker AI Studio esistente, quindi è fondamentale prendere una decisione prima di creare un dominio SageMaker AI Studio di produzione.

Se SageMaker AI Studio è configurato in IAM modalità, gli utenti di SageMaker AI Studio accedono all'app tramite un account prefirmato URL che consente di accedere automaticamente all'app SageMaker AI Studio quando vi si accede tramite un browser.

utenti IAM

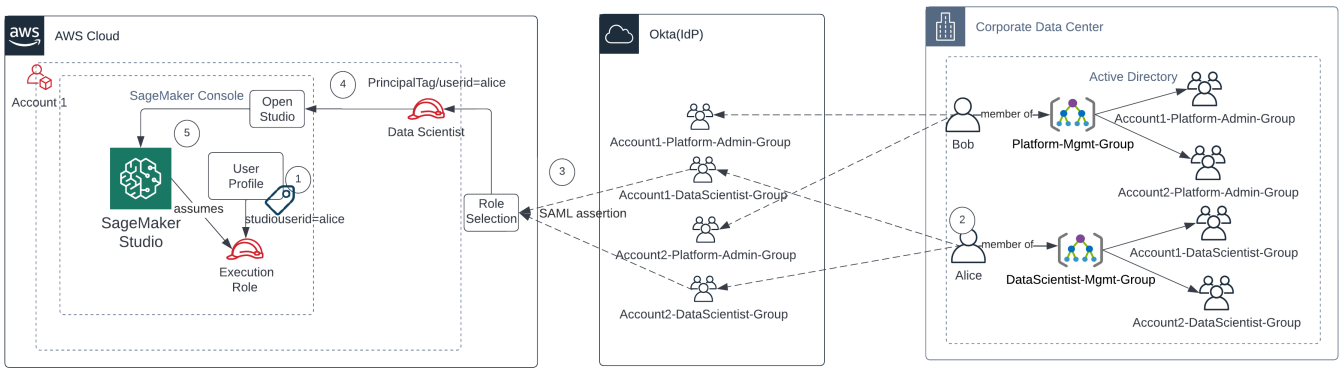
Per IAM gli utenti, l'amministratore crea profili utente di SageMaker AI Studio per ogni utente e associa il profilo utente a un IAM ruolo che consente le azioni necessarie che l'utente deve eseguire dall'interno di Studio. Per impedire a un AWS utente di accedere solo al proprio profilo utente di SageMaker AI Studio, l'amministratore deve taggare il profilo utente di SageMaker AI Studio e allegare all'utente una IAM policy che gli consenta di accedere solo se il valore del tag è uguale al nome AWS utente. La dichiarazione politica ha il seguente aspetto:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:username}"
                }
            }
        }
    ]
}
```

AWS IAMo federazione degli account

Il metodo di Account AWS federazione consente ai clienti di federarsi nella console SageMaker AI dal proprio SAML IdP, come Okta. Per impedire agli utenti di accedere solo al proprio profilo utente,

l'amministratore deve taggare il profilo utente di SageMaker AI Studio, aggiungere `PrincipalTags` l'IdP e impostarlo come tag transitivi. Il diagramma seguente mostra come l'utente federato (Data Scientist Alice) è autorizzato ad accedere al proprio SageMaker profilo utente di AI Studio.



Accesso a SageMaker AI Studio in IAM modalità federazione

1. Il profilo utente di Alice SageMaker AI Studio è contrassegnato con il relativo ID utente e associato al ruolo di esecuzione.
2. Alice si autentica su IdP (Okta).
3. IdP autentica Alice e pubblica un'SAMLasserzione con i due ruoli (Data Scientist per gli account 1 e 2) di cui Alice è membro. Alice seleziona il ruolo di Data Scientist per l'account 1.
4. Alice ha effettuato l'accesso all'Account 1 SageMaker AI Console, con il ruolo assunto di Data Scientist. Alice apre l'istanza dell'app Studio dall'elenco delle istanze dell'app Studio.
5. Il tag principale di Alice nella sessione di ruolo presunta viene convalidato rispetto al tag del profilo utente dell'istanza dell'app SageMaker AI Studio selezionata. Se il tag del profilo è valido, viene avviata l'istanza dell'app SageMaker AI Studio, assumendo il ruolo di esecuzione.

Se desideri automatizzare la creazione di ruoli e policy di SageMaker AI Execution come parte dell'onboarding degli utenti, ecco un modo per farlo:

1. Configura un gruppo AD, ad esempio `SageMaker AI-Account1-Group` a livello di account e dominio Studio.
2. Aggiungi SageMaker AI-Account1-Group all'appartenenza al gruppo dell'utente quando devi inserire un utente in AI Studio. SageMaker

Imposta un processo di automazione che ascolti l'evento di `SageMaker AI-Account1-Group` iscrizione e utilizzalo per AWS APIs creare il ruolo, le politiche, i tag e il profilo utente di SageMaker AI Studio in base all'appartenenza ai gruppi AD. Associa il ruolo al profilo utente. Per un esempio di politica, fare riferimento aImpedisci agli utenti di SageMaker AI Studio di accedere ad altri profili utente.

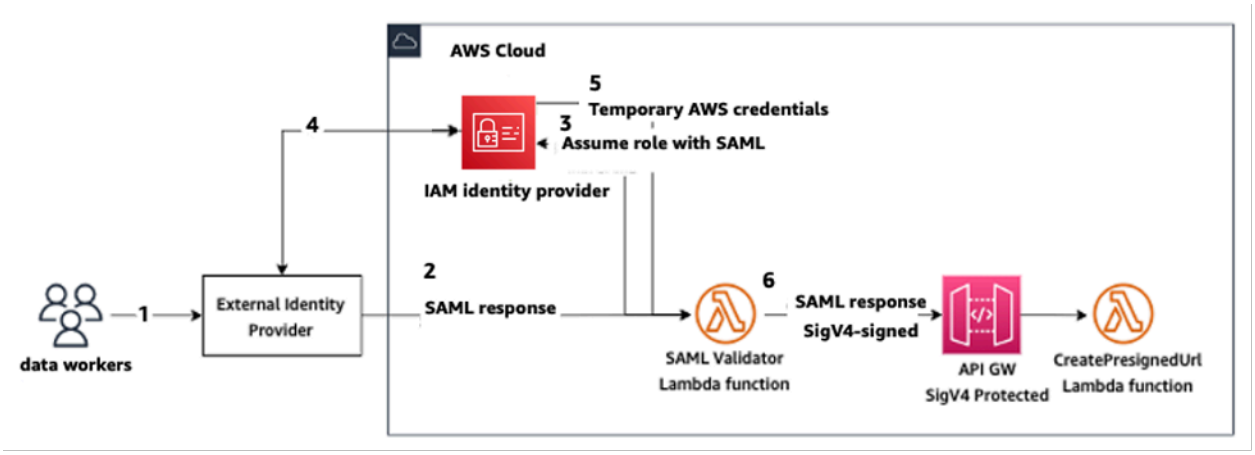
SAMLautenticazione tramite AWS Lambda

In IAM modalità, gli utenti possono anche essere autenticati in SageMaker AI Studio utilizzando SAML asserzioni. In questa architettura, il cliente dispone di un IdP esistente, in cui può creare un'SAMLapplicazione per consentire agli utenti di accedere a Studio (anziché l'applicazione AWS Identity Federation). L'IdP del cliente viene aggiunto a. IAM Una AWS Lambda funzione aiuta a convalidare l'SAMLasserzione utilizzando IAM eSTS, quindi, richiama direttamente un gateway API o una funzione Lambda per creare il dominio prefirmato. URL

Il vantaggio di questa soluzione è che la funzione Lambda può personalizzare la logica di accesso a SageMaker AI Studio. Per esempio:

- Crea automaticamente un profilo utente se non ne esiste uno.
- Allega o rimuovi ruoli o documenti di policy al ruolo di esecuzione di SageMaker AI Studio analizzando gli SAML attributi.
- Personalizza il profilo utente aggiungendo Life Cycle Configuration (LCC) e aggiungendo tag.

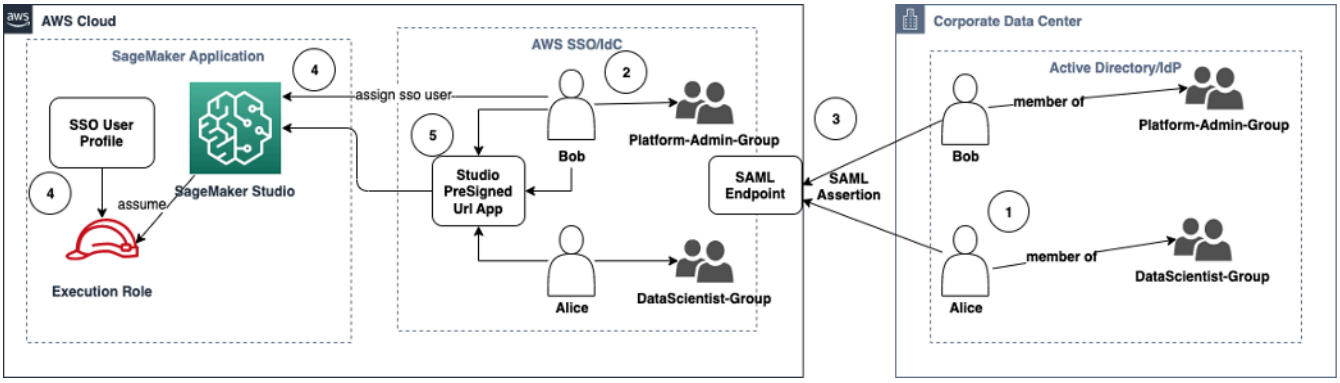
In sintesi, questa soluzione esporrà SageMaker AI Studio come un'applicazione SAML2 2.0 con logica personalizzata per l'autenticazione e l'autorizzazione. Per i dettagli di implementazione, fare riferimento alla sezione dell'appendice Accesso a SageMaker Studio tramite SAML assertion.



Accesso a SageMaker AI Studio tramite un'applicazione personalizzata SAML

AWSIAMFederazione iDC

Il metodo di federazione iDC consente ai clienti di federarsi direttamente nell'applicazione SageMaker AI Studio dal proprio SAML IdP (come Okta). Il diagramma seguente mostra come l'utente federato è autorizzato ad accedere alla propria istanza di AI Studio. SageMaker



Accesso a SageMaker AI Studio in modalità iDC IAM

1. Nell'AD aziendale, l'utente è membro di gruppi AD come il gruppo Platform Admin e il gruppo Data Scientist.
2. L'utente AD e i gruppi AD di Identity Provider (IdP) sono sincronizzati con AWS IAM Identity Center e disponibili rispettivamente come utenti e gruppi Single Sign-On per le assegnazioni.
3. L'IdP pubblica un'SAMLasserzione sull' AWS endpoint IdC. SAML
4. In SageMaker AI Studio, l'utente iDC viene assegnato all'applicazione Studio. SageMaker Questa assegnazione può essere eseguita utilizzando iDC Group e SageMaker AI Studio verrà applicata a ciascun livello di utente iDC. Quando viene creata questa assegnazione, SageMaker AI Studio crea il profilo utente iDC e assegna il ruolo di esecuzione del dominio.
5. L'utente accede all'applicazione SageMaker AI Studio utilizzando l'applicazione sicura prefirmata URL ospitata come cloud dall'iDC. SageMaker AI Studio assume il ruolo di esecuzione associato al proprio profilo utente iDC.

Guida all'autenticazione del dominio

Ecco alcune considerazioni sulla scelta della modalità di autenticazione di un dominio:

1. Se desideri che i tuoi utenti non accedano Console di gestione AWS e visualizzino direttamente l'interfaccia utente di SageMaker AI Studio, utilizza la modalità Single Sign-on con iDC. AWS IAM

2. Se desideri che i tuoi utenti non accedano Console di gestione AWS e visualizzino l'interfaccia utente di SageMaker AI Studio direttamente in IAM modalità, puoi farlo utilizzando una funzione Lambda nel backend per generare un predefinito URL per il profilo utente e reindirizzarli all'interfaccia utente di AI Studio. SageMaker
3. In modalità iDC, ogni utente viene mappato su un singolo profilo utente.
4. A tutti i profili utente viene assegnato automaticamente il ruolo di esecuzione predefinito in modalità iDC. Se desideri che ai tuoi utenti vengano assegnati ruoli di esecuzione diversi, dovrai aggiornare i profili utente utilizzando il UpdateUserProfileAPI.
5. Se desideri limitare l'accesso all'interfaccia utente di SageMaker AI Studio in IAM modalità (utilizzando il predefinito generatoURL) a un VPC endpoint, senza attraversare Internet, puoi utilizzare un resolver personalizzato. DNS Consulta il post di blog Secure Amazon SageMaker AI Studio presigned URLs Part 1: Foundational infrastructure.

Gestione delle autorizzazioni

Questa sezione illustra le migliori pratiche per la configurazione di IAM ruoli, policy e guardrail di uso comune per il provisioning e il funzionamento del dominio AI Studio. SageMaker

Ruoli e policy IAM

Come best practice, potresti innanzitutto identificare le persone e le applicazioni pertinenti, note come responsabili coinvolte nel ciclo di vita del machine learning, e quali AWS autorizzazioni devi concedere loro. Poiché l' SageMaker intelligenza artificiale è un servizio gestito, è necessario considerare anche i principali servizi, ossia i AWS servizi che possono effettuare API chiamate per conto di un utente. Il diagramma seguente illustra i diversi IAM ruoli che potresti voler creare, corrispondenti ai diversi personaggi dell'organizzazione.

SageMaker Ruoli dell'IA IAM

Questi ruoli sono descritti in dettaglio, insieme ad alcuni esempi di ruoli specifici di cui IAMpermissions avranno bisogno.

- Ruolo utente di ML Admin: è un preside che fornisce l'ambiente ai data scientist creando domini di studio e profili utente (`sagemaker:CreateDomain`,`sagemaker:CreateUserProfile`), creando AWS Key Management Service (AWS KMS) chiavi per gli utenti, creando bucket S3 per i data scientist e creando ECR repository Amazon per ospitare i contenitori. Possono anche impostare configurazioni predefinite e script del ciclo di vita per gli utenti, creare e allegare immagini personalizzate al dominio SageMaker AI Studio e fornire prodotti Service Catalog come progetti personalizzati e modelli Amazon. EMR

  Poiché questo responsabile non eseguirà lavori di formazione, ad esempio, non ha bisogno di autorizzazioni per avviare lavori di formazione o elaborazione SageMaker AI. Se utilizzano l'infrastruttura come modelli di codice, ad esempio CloudFormation o Terraform, per fornire domini e utenti, questo ruolo verrebbe assunto dal servizio di provisioning per creare le risorse per conto

dell'amministratore. Questo ruolo può avere accesso in sola lettura all'intelligenza artificiale utilizzando. SageMaker Console di gestione AWS

Questo ruolo utente richiederà inoltre determinate EC2 autorizzazioni per avviare il dominio all'interno di un ambiente privatoVPC, KMS autorizzazioni per crittografare il EFS volume e autorizzazioni per creare un ruolo collegato al servizio per Studio (). `iam:CreateServiceLinkedRole` Descriveremo queste autorizzazioni granulari più avanti nel documento.

- Ruolo utente di Data Scientist: questo principio è l'utente che accede a SageMaker AI Studio, esplora i dati, crea processi e pipeline di elaborazione e formazione e così via. L'autorizzazione principale di cui l'utente ha bisogno è l'autorizzazione per avviare SageMaker AI Studio, mentre il resto delle policy può essere gestito dal ruolo del servizio di esecuzione SageMaker AI.
- SageMaker Ruolo del servizio di esecuzione SageMaker AI: poiché l'IA è un servizio gestito, avvia lavori per conto di un utente. Questo ruolo è spesso il più ampio in termini di autorizzazioni consentite, poiché molti clienti scelgono di utilizzare un unico ruolo di esecuzione per eseguire lavori di formazione, elaborazione o hosting di modelli. Sebbene si tratti di un modo semplice per iniziare, poiché i clienti maturano nel loro percorso di crescita, spesso suddividono il ruolo di esecuzione dei notebook in ruoli separati per API azioni diverse, soprattutto quando eseguono tali lavori in ambienti distribuiti.

  Al momento della creazione, associ un ruolo al dominio SageMaker AI Studio. Tuttavia, poiché i clienti potrebbero richiedere la flessibilità di avere ruoli diversi associati ai diversi profili utente del dominio (ad esempio, in base alla loro funzione lavorativa), puoi anche associare un IAM ruolo separato a ciascun profilo utente. Ti consigliamo di mappare un singolo utente fisico a un singolo profilo utente. Se non si associa un ruolo a un profilo utente al momento della creazione, il comportamento predefinito consiste nell'associare anche il ruolo di esecuzione del SageMaker AIStudio dominio al profilo utente.

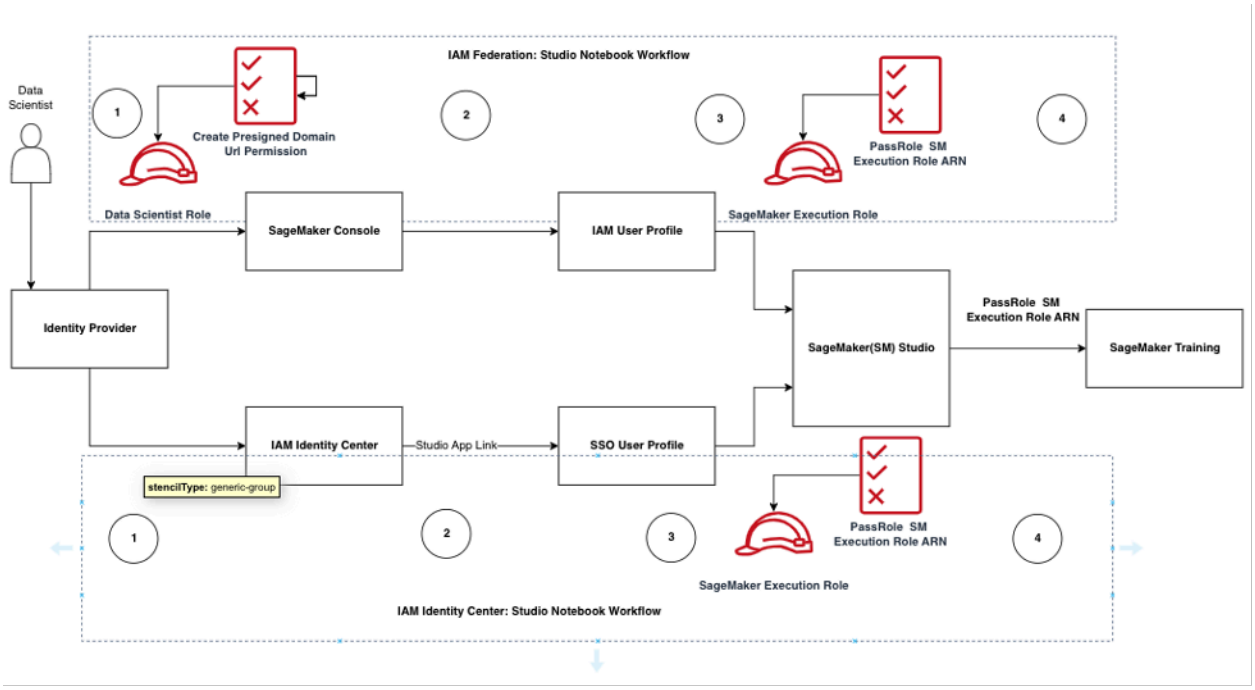
  Nei casi in cui più data scientist e ingegneri ML collaborino su un progetto e abbiano bisogno di un modello di autorizzazione condiviso per accedere alle risorse, ti consigliamo di creare un ruolo di esecuzione del servizio di SageMaker intelligenza artificiale a livello di team per condividere IAM le autorizzazioni tra i membri del team. Nei casi in cui è necessario bloccare le autorizzazioni a ogni livello di utente, è possibile creare un ruolo di esecuzione del servizio di SageMaker intelligenza artificiale individuale a livello di utente; tuttavia, è necessario prestare attenzione ai limiti del servizio.

SageMaker Flusso di lavoro di autorizzazione di AI Studio Notebook

Questa sezione illustra come funziona l'autorizzazione di SageMaker AI Studio Notebook per le varie attività che il Data Scientist deve eseguire per creare e addestrare il modello direttamente da SageMaker AI Studio Notebook. Il dominio SageMaker AI supporta due modalità di autorizzazione:

- Federazione IAM
- IAMIdentity Center

Successivamente, questo paper illustra il flusso di lavoro di autorizzazione di Data Scientist per ciascuna di queste modalità.



Flusso di lavoro di autenticazione e autorizzazione per gli utenti di Studio

IAMFederazione: flussi di lavoro di SageMaker Studio Notebook

1. Un Data Scientist si autentica nel proprio provider di identità aziendale e assume il ruolo utente di Data Scientist (il ruolo di federazione degli utenti) nella SageMaker console di intelligenza artificiale. Questo ruolo federativo è `iam:PassRole` API autorizzato al ruolo di esecuzione dell' SageMaker IA a trasferire il ruolo Amazon Resource Name (ARN) a SageMaker Studio.

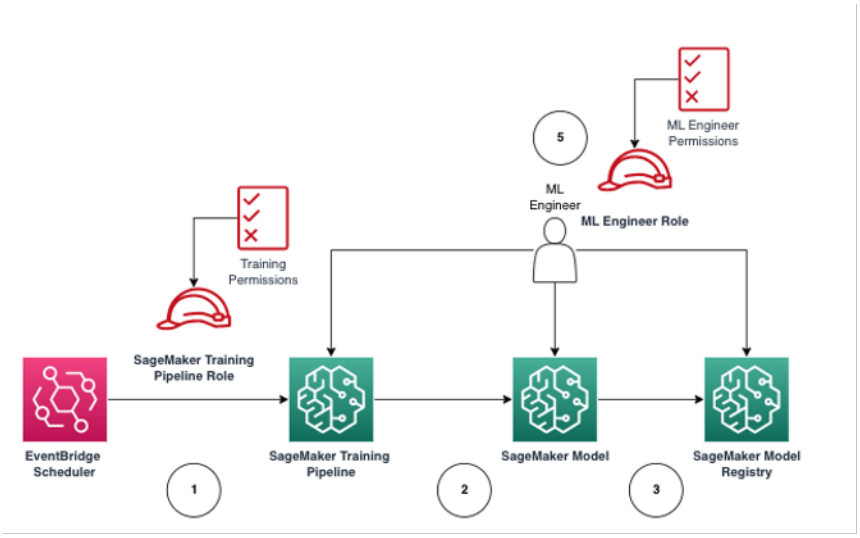
2. Il Data Scientist seleziona il link Open Studio dal proprio profilo IAM utente Studio associato al ruolo di esecuzione dell' SageMaker IA
3. Il IDE servizio SageMaker Studio viene avviato, presupponendo le autorizzazioni del ruolo di SageMaker esecuzione del profilo utente. Questo ruolo ha l'`iam:PassRole`APIautorizzazione del ruolo di esecuzione dell' SageMaker IA a trasferire il ruolo ARN al servizio di formazione sull' SageMaker intelligenza artificiale.
4. Quando Data Scientist avvia il processo di formazione nei nodi di elaborazione remota, il ruolo di esecuzione dell' SageMaker IA ARN viene passato al servizio di formazione SageMaker AI. Questo crea una nuova sessione di ruolo con questo ARN ed esegue il processo di formazione. Se è necessario definire ulteriormente l'autorizzazione per un lavoro di formazione, è possibile creare un ruolo specifico per la formazione e assegnare tale ruolo al ARN momento della chiamata al corso di formazioneAPI.

IAMIdentity Center: flusso di lavoro di SageMaker AI Studio Notebook

1. Il Data Scientist si autentica nel proprio provider di identità aziendale e fa clic su AWS IAM Identity Center. Al Data Scientist viene presentato all'utente Identity Center Portal.
2. Il Data Scientist fa clic sul collegamento dell'app SageMaker AI Studio creato dal proprio profilo utente iDC, associato al ruolo di esecuzione SageMaker AI.
3. Il IDE servizio SageMaker AI Studio viene avviato, presupponendo le autorizzazioni del ruolo di esecuzione SageMaker AI del profilo utente. Questo ruolo ha l'`iam:PassRole`APIautorizzazione del ruolo di esecuzione dell' SageMaker IA a trasferire il ruolo ARN al servizio di formazione sull' SageMaker intelligenza artificiale.
4. Quando il Data Scientist avvia il processo di formazione nei nodi di elaborazione remota, il ruolo di esecuzione dell' SageMaker IA ARN viene passato al servizio di formazione SageMaker AI. Il ruolo di esecuzione ARN crea una nuova sessione di ruolo con questo ARN ruolo ed esegue il processo di formazione. Se è necessario definire ulteriormente l'autorizzazione per i lavori di formazione, è possibile creare un ruolo specifico per la formazione e assegnare tale ruolo al ARN momento della convocazione del corso di formazione. API

Ambiente implementato: SageMaker flusso di lavoro di formazione basato sull'intelligenza artificiale

In ambienti distribuiti come i test di sistema e la produzione, i lavori vengono eseguiti tramite una pianificazione automatizzata e i trigger di eventi e l'accesso umano a tali ambienti è limitato dai SageMaker notebook AI Studio. Questa sezione illustra come i IAM ruoli interagiscono con la pipeline di formazione sull' SageMaker intelligenza artificiale nell'ambiente distribuito.



SageMaker Flusso di lavoro di formazione sull'intelligenza artificiale in un ambiente di produzione gestito

1. Amazon EventBridge scheduler attiva il processo della pipeline di formazione sull' SageMaker intelligenza artificiale.
2. Il ruolo della pipeline di formazione SageMaker AI assume il ruolo della pipeline di formazione SageMaker AI per addestrare il modello.
3. Il modello di SageMaker intelligenza artificiale addestrato è registrato nell' SageMaker AI Model Registry.
4. Un ingegnere ML assume il ruolo utente di ingegnere ML per gestire la pipeline di formazione e il modello di SageMaker intelligenza artificiale.

Autorizzazioni per i dati

La capacità degli utenti di SageMaker AI Studio di accedere a qualsiasi fonte di dati è regolata dalle autorizzazioni associate al loro ruolo di IAM esecuzione SageMaker AI. Le policy allegate possono

autorizzarli a leggere, scrivere o eliminare da determinati bucket o prefissi Amazon S3 e connettersi ai database Amazon. RDS

Accesso ai dati AWS Lake Formation

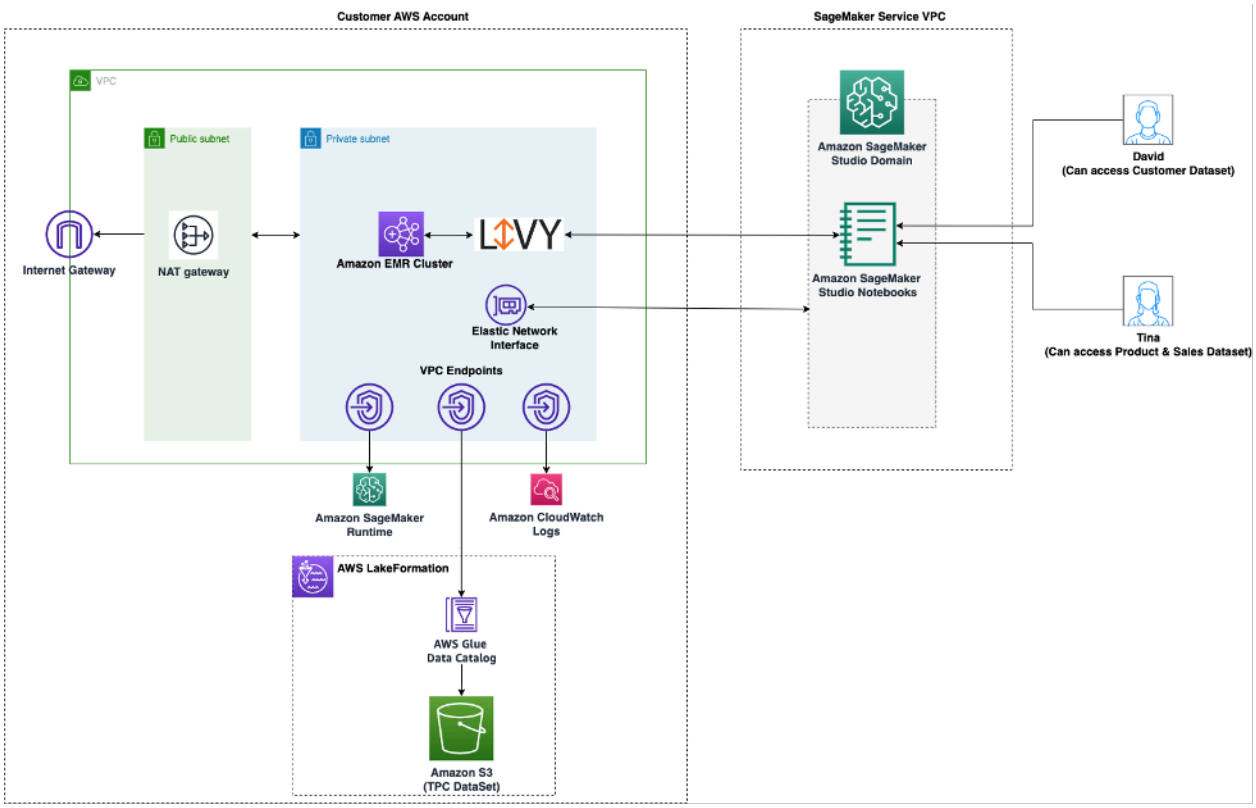
Molte aziende hanno iniziato a utilizzare data lake governati da AWS Lake Formationper consentire l'accesso granulare ai dati per i propri utenti. Come esempio di tali dati governati, gli amministratori possono mascherare le colonne sensibili per alcuni utenti, abilitando al contempo le query sulla stessa tabella sottostante.

Per utilizzare Lake Formation di SageMaker AI Studio, gli amministratori possono registrare i ruoli di IAM esecuzione dell' SageMaker IA come. `DataLakePrincipals` Per ulteriori informazioni, consulta Lake Formation Permissions Reference. Una volta autorizzati, esistono tre metodi principali per accedere e scrivere dati governati da SageMaker AI Studio:

1. Da un SageMaker AI Studio Notebook, gli utenti possono utilizzare motori di query come Amazon Athena o librerie basate su boto3 per estrarre i dati direttamente sul notebook. The AWSSDKfor Pandas (precedentemente nota come awswrangler) è una libreria popolare. Di seguito è riportato un esempio di codice per mostrare quanto possa essere semplice:

```
transaction_id = wr.lakeformation.start_transaction(read_only=True)
df = wr.lakeformation.read_sql_query(
    sql=f"SELECT * FROM {table};",
    database=database,
    transaction_id=transaction_id
)
```

2. Usa la connettività nativa di SageMaker AI Studio con Amazon EMR per leggere e scrivere dati su larga scala. Attraverso l'uso dei ruoli di EMR runtime di Apache Livy e Amazon, SageMaker AI Studio ha creato una connettività nativa che ti consente di trasferire il tuo IAM ruolo di esecuzione dell' SageMaker IA (o un altro ruolo autorizzato) a un EMR cluster Amazon per l'accesso e l'elaborazione dei dati. Per up-to-date istruzioni, consulta Connect to an Amazon EMR Cluster from Studio.



Architettura per l'accesso ai dati gestita da Lake Formation di SageMaker Studio

3. Usa la connettività nativa di SageMaker AI Studio per sessioni AWS Glue interattive per leggere e scrivere dati su larga scala. SageMaker I notebook AI Studio dispongono di kernel integrati che consentono agli utenti di eseguire comandi in modo interattivo. AWS Glue Ciò consente l'uso scalabile dei backend Python, Spark o Ray che possono leggere e scrivere senza problemi dati su larga scala da fonti di dati controllate. I kernel consentono agli utenti di assegnare la propria esecuzione o altri ruoli autorizzati SageMaker . IAM Per ulteriori informazioni, consulta Preparare i dati utilizzando sessioni AWS Glue interattive.

Guardrail comuni

Questa sezione illustra i guardrail più comunemente utilizzati per applicare la governance alle risorse ML utilizzando IAM policy, policy relative alle risorse, policy sugli VPC endpoint e policy di controllo dei servizi (). SCPs

Limita l'accesso ai notebook a istanze specifiche

Questa politica di controllo dei servizi può essere utilizzata per limitare i tipi di istanze a cui i data scientist hanno accesso durante la creazione di notebook Studio. Tieni presente che qualsiasi utente

avrà bisogno dell'istanza «di sistema» autorizzata a creare l'app Jupyter Server predefinita che ospita AI Studio. SageMaker

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "LimitInstanceTypesforNotebooks",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateApp"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringNotLike": {
                     "sagemaker:InstanceTypes": [
                         "ml.c5.large",
                         "ml.m5.large",
                         "ml.t3.medium",
                         "system"
                     ]
                 }
             }
         }
     ]
 }
```

Limita i domini di AI Studio non conformi SageMaker

Per i domini SageMaker AI Studio, è possibile utilizzare la seguente politica di controllo del servizio per imporre al traffico di accesso alle risorse dei clienti in modo che non acceda alla rete Internet pubblica, ma piuttosto a quella del cliente: VPC

```
{
     "Version": "2012-10-17",
     "Statement": [
         {   "Sid": "LockDownStudioDomain",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateDomain"
             ],
             "Resource": "*",
```

```
            "Condition": {
                        "StringNotEquals": {"sagemaker:AppNetworkAccessType":
"VpcOnly"
                },
                "Null": {
                        "sagemaker:VpcSubnets": "true",
                        "sagemaker:VpcSecurityGroupIds": "true"
                }
            }
        }
    ]
}
```

Limita il lancio di immagini AI non autorizzate SageMaker

La seguente politica impedisce a un utente di lanciare un'immagine SageMaker AI non autorizzata all'interno del proprio dominio:f

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:CreateApp"
             ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringNotLike": {
                    "sagemaker:ImageArns":
                        [
                        "arn:aws:sagemaker:*:*:image/{ImageName}"
                        ]
                }
            }
        }
    ]
}
```

Avvia i notebook solo tramite endpoint AI SageMaker VPC

Oltre agli VPC endpoint per il piano di controllo SageMaker AI, l'IA supporta gli VPC endpoint per consentire agli utenti di connettersi SageMaker ai notebook AI Studio o alle istanze di notebook SageMaker AI Studio. SageMaker Se hai già configurato un VPC endpoint per un'istanza SageMaker AI Studio/Notebook, la seguente chiave IAM condizionale consentirà le connessioni ai notebook AI Studio solo se vengono effettuate tramite l'endpoint SageMaker AI Studio o tramite l'endpoint AI. SageMaker VPC SageMaker API

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EnableSageMakerStudioAccessviaVPCEndpoint",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreatePresignedDomainUrl",
                 "sagemaker:DescribeUserProfile"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "aws:sourceVpce": [
                         "vpce-111bbccc",
                         "vpce-111bbddd"
                     ]
                 }
             }
         }
     ]
 }
```

Limita l'accesso SageMaker ai notebook AI Studio a un intervallo IP limitato

Le aziende spesso limitano l'accesso ad SageMaker AI Studio a determinati intervalli di IP aziendali consentiti. La seguente IAM politica con la chiave di `SourceIP` condizione può limitare questo limite.

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

```
            "Sid": "EnableSageMakerStudioAccess",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl",
                "sagemaker:DescribeUserProfile"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            }
        }
    ]
}
```

Impedisci agli utenti di SageMaker AI Studio di accedere ad altri profili utente

In qualità di amministratore, quando crei il profilo utente, assicurati che il profilo sia contrassegnato con il nome utente di SageMaker AI Studio con la chiave tag`studiouserid`. Il principale (utente o ruolo associato all'utente) dovrebbe avere anche un tag con la chiave `studiouserid` (questo tag può avere qualsiasi nome e non è limitato a`studiouserid`).

Successivamente, allega la seguente politica al ruolo che l'utente assumerà all'avvio di SageMaker AI Studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "sagemaker:ResourceTag/studiouserid": "${aws:PrincipalTag/
studiouserid}"
                }
            }
        }
    ]
}
```

Applica l'etichettatura

I data scientist devono utilizzare i notebook SageMaker AI Studio per esplorare i dati e creare e addestrare modelli. L'applicazione di tag ai notebook aiuta a monitorare l'utilizzo e a controllare i costi, oltre a garantire la proprietà e la verificabilità.

Per le app SageMaker AI Studio, assicurati che il profilo utente sia taggato. I tag vengono propagati automaticamente alle app dal profilo utente. Per imporre la creazione di profili utente con tag (supportati da CLI andSDK), valuta la possibilità di aggiungere questa politica al ruolo di amministratore:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceUserProfileTags",
            "Effect": "Allow",
            "Action": "sagemaker:CreateUserProfile",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Per altre risorse, come i lavori di formazione e i lavori di elaborazione, puoi rendere obbligatori i tag utilizzando la seguente politica:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceTagsForJobs",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateProcessingJob",
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Accesso root in SageMaker AI Studio

In SageMaker AI Studio, il notebook viene eseguito in un contenitore Docker che, per impostazione predefinita, non ha accesso root all'istanza host. Analogamente, a parte l'utente run-as predefinito, tutti gli altri intervalli di ID utente all'interno del contenitore vengono mappati nuovamente come utenti non privilegiati, sull'istanza host stessa. IDs Di conseguenza, la minaccia di un aumento dei privilegi è limitata al contenitore del notebook stesso.

Quando si creano immagini personalizzate, è consigliabile fornire all'utente autorizzazioni non root per controlli più rigorosi, ad esempio evitando di eseguire processi indesiderati come utente root o di installare pacchetti disponibili pubblicamente. In questi casi, puoi creare l'immagine da eseguire come utente non root all'interno del Dockerfile. Sia che tu crei l'utente come root o non root, devi assicurarti che sia impostato AppImageConfigper l'UID/GID of the user is identical to the UID/GIDapp personalizzata, che crea la configurazione per l' SageMaker IA per eseguire un'app utilizzando l'immagine personalizzata. Ad esempio, se il tuo Dockerfile è stato creato per un utente non root come il seguente:

```
ARG NB_UID="1000"
ARG NB_GID="100"
...
```

```
USER $NB_UID
```

Il `AppImageConfig` file deve menzionare lo stesso UID e GID nella sua casella: `KernelGatewayConfig`

```
{
    "KernelGatewayImageConfig": {
        "FileSystemConfig": {
            "DefaultUid": 1000,
            "DefaultGid": 100
        }
    }
}
```

I GID valoriUID/accettabili per le immagini personalizzate sono 0/0 e 1000/100 per le immagini di Studio. Per esempi di creazione di immagini personalizzate e le `AppImageConfig` impostazioni associate, consulta questo repository Github.

Per evitare che gli utenti lo manomettano, non concedete né `DeleteAppImageConfig` autorizzazioni agli utenti dei `CreateAppImageConfig` notebook AI Studio. `UpdateAppImageConfig` SageMaker

Gestione di rete

Per configurare il dominio SageMaker AI Studio, devi specificare la VPC rete, le sottoreti e i gruppi di sicurezza. Quando specificate le sottoreti VPC and, assicuratevi di effettuare l'allocazione IPs tenendo conto del volume di utilizzo e della crescita prevista, come illustrato nelle sezioni seguenti.

VPCpianificazione della rete

Le VPC sottoreti dei clienti associate al dominio SageMaker AI Studio devono essere create con l'intervallo Classless Inter-domain Routing (CIDR) appropriato, in base ai seguenti fattori:

- Numero di utenti.
- Numero di app per utente.
- Numero di tipi di istanze univoci per utente.
- Numero medio di istanze di formazione per utente.
- Percentuale di crescita prevista.

SageMaker L'intelligenza artificiale e AWS i servizi partecipanti inseriscono interfacce di rete elastiche (ENI) nella VPC sottorete del cliente per i seguenti casi d'uso:

- Amazon EFS inserisce un come ENI target di EFS montaggio per il dominio SageMaker AI (un IP per sottorete/zona di disponibilità collegata al SageMaker dominio AI).
- SageMaker AI Studio inietta un ENI per ogni istanza univoca utilizzata da un profilo utente o da uno spazio condiviso. Per esempio:
  - Se un profilo utente esegue un'app server Jupyter predefinita (un'istanza di «sistema»), un'app Data Science e un'app Base Python (entrambe in esecuzione su un'`ml.t3.medium`istanza), Studio inserisce due indirizzi IP.
  - Se un profilo utente esegue un'app server Jupyter predefinita (un'istanza di «sistema»), un'GPUapp Tensorflow (su un'`ml.g4dn.xlarge`istanza) e un'app data wrangler (su un'`ml.m5.4xlarge`istanza), Studio inietta tre indirizzi IP.
- E ENI per ogni VPC endpoint viene iniettato tra le VPC sottoreti di dominio/le zone di disponibilità (quattro IPs per gli endpoint SageMaker AI; ~sei per gli VPC endpoint dei servizi partecipanti come S3, 0, e.) IPs VPC ECR CloudWatch

- Se i processi di formazione ed elaborazione dell' SageMaker IA vengono avviati con la stessa VPC configurazione, ogni processo necessita di due indirizzi IP per istanza.

> **Note**
>
> VPCle impostazioni per SageMaker AI Studio, come le sottoreti e il VPC solo traffico, non vengono trasferite automaticamente ai lavori di formazione/elaborazione creati da AI Studio. SageMaker L'utente deve configurare VPC le impostazioni e l'isolamento della rete, se necessario, quando chiama APIs Create*Job. Per ulteriori informazioni, consulta Run Training and Inference Containers in modalità senza Internet.

Scenario: Data scientist esegue esperimenti su due diversi tipi di istanze

In questo scenario, supponiamo che un dominio SageMaker AI sia impostato in modalità VPC solo traffico. Sono configurati VPC endpoint, come SageMaker AIAPI, SageMaker AI runtime, Amazon S3 e Amazon. ECR

Un data scientist sta eseguendo esperimenti sui notebook Studio, eseguendoli su due diversi tipi di istanza (ad esempio `ml.t3.medium` e`ml.m5.large`) e avviando due app per ogni tipo di istanza.

Supponiamo che il data scientist esegua contemporaneamente un processo di formazione con la stessa VPC configurazione su un'istanza. `ml.m5.4xlarge`

In questo scenario, il servizio SageMaker AI Studio eseguirà l'iniezione ENIs come segue:

Tabella 1: ENIs iniettato nel cliente VPC per uno scenario di sperimentazione

Entità	Target	ENIiniettato	Note	Livello
EFSbersaglio di montaggio	VPCsottoreti	Tre	Tre /sottoreti AZs	Domain
Endpoint VPC	VPCsottoreti	30	Tre AZs /sottoreti da 10 ciascuna VPCE	Domain
Server Jupyter	Sottorete VPC	One	Un IP per istanza	Utente

Entità	Target	ENIiniettato	Note	Livello
KernelGateway app	Sottorete VPC	Due	Un IP per tipo di istanza	Utente
Addestramento	Sottorete VPC	Due	Due IPs per istanza di formazione Cinque IPs per istanza di formazione, se EFAutilizzata	Utente

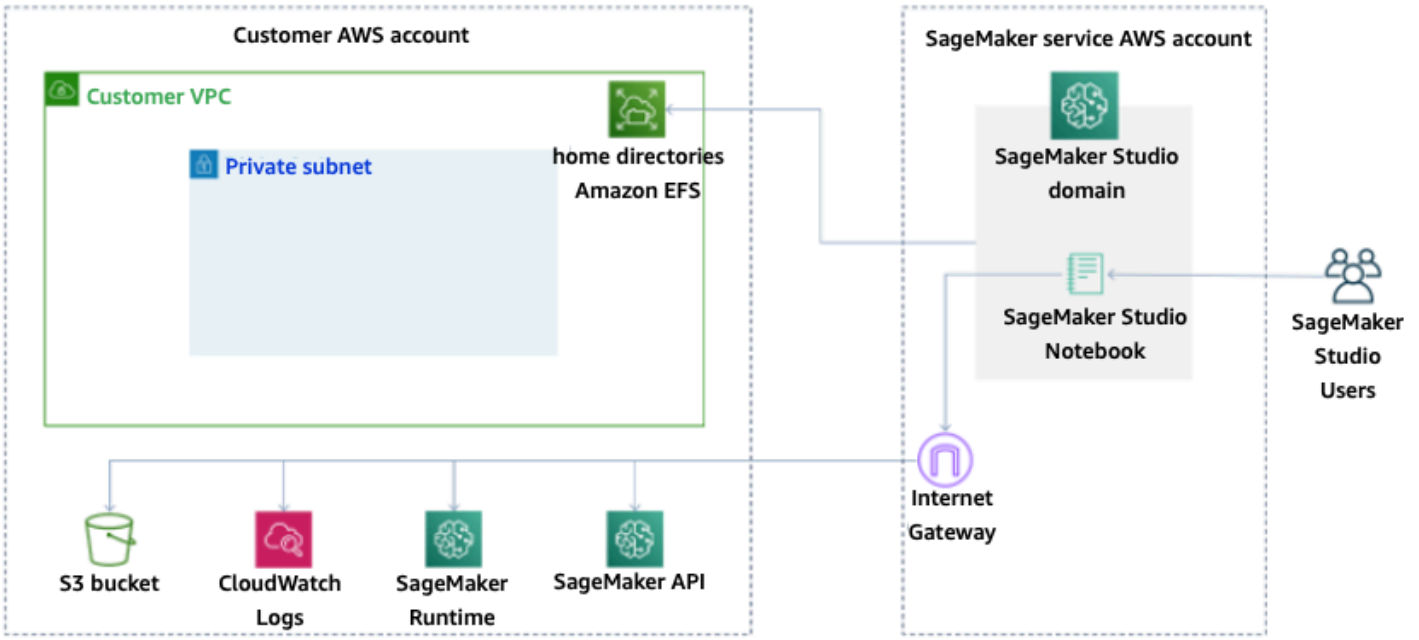
In questo scenario, il cliente ha un totale di IPs 38 utenti, di VPC cui 33 IPs sono condivisi tra gli utenti a livello di dominio e cinque IPs a livello di utente. Se hai 100 utenti con profili utente simili in questo dominio che eseguono queste attività contemporaneamente, consumerai cinque x 100 = 500 IPs a livello di utente, oltre al consumo IP a livello di dominio, che è di 11 IPs per sottorete, per un totale di 511. IPs In questo scenario, è necessario creare la VPC sottorete CIDR con /22 che allocherà 1024 indirizzi IP, con margini di crescita.

VPCopzioni di rete

Un dominio SageMaker AI Studio supporta la configurazione della VPC rete con una delle seguenti opzioni:

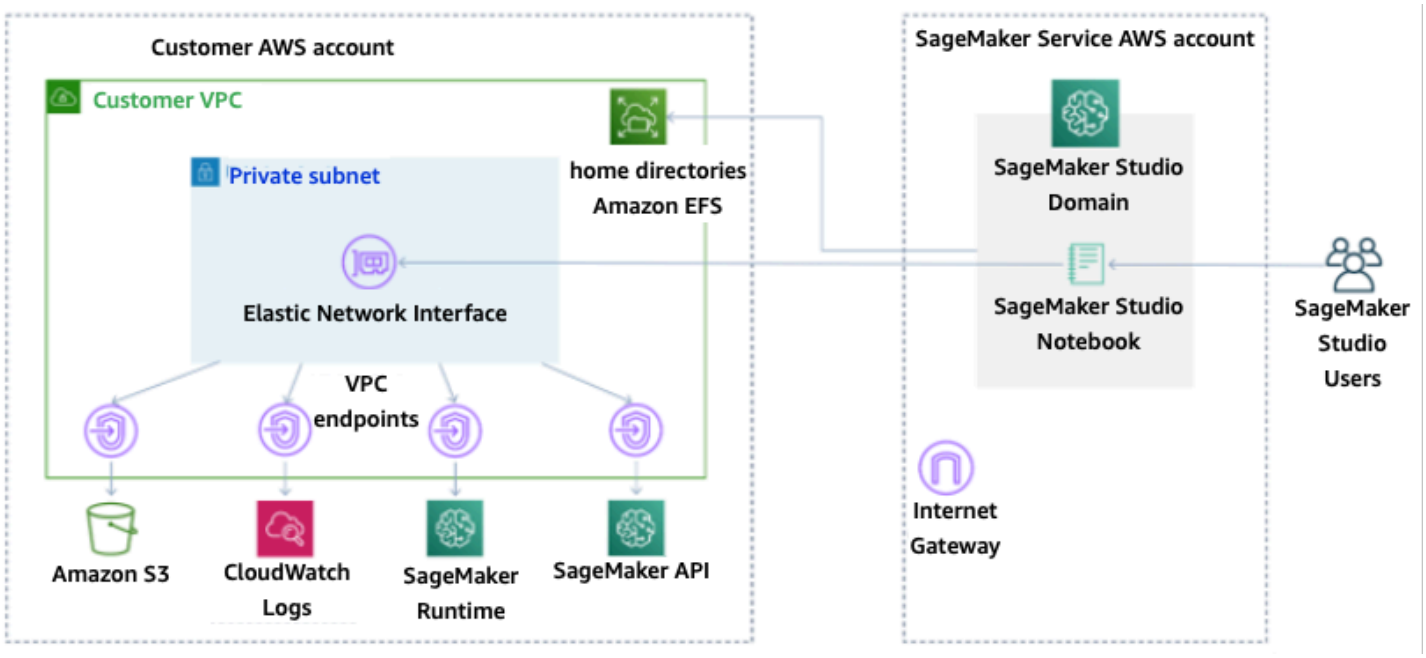
- Solo Internet pubblico
- Solo VPC

L'opzione dedicata esclusivamente alla rete Internet pubblica consente SageMaker ai API servizi di intelligenza artificiale di utilizzare la rete Internet pubblica tramite il VPC gateway Internet fornito nell'account del servizio SageMaker AI gestito dall'account, come illustrato nel diagramma seguente:



Modalità predefinita: accesso a Internet tramite account del servizio SageMaker AI

L'VPCunica opzione disabilita il routing Internet dall'account del servizio VPC Managed by the SageMaker AI e consente al cliente di configurare il traffico da indirizzare sugli VPC endpoint, come illustrato nel diagramma seguente:



VPCmodalità unica: nessun accesso a Internet tramite l'account del servizio SageMaker AI

Per un dominio configurato in modalità VPC solo, configura un gruppo di sicurezza per profilo utente per garantire l'isolamento completo delle istanze sottostanti. Ogni dominio di un AWS account può avere la propria VPC configurazione e modalità Internet. Per maggiori dettagli sulla configurazione della VPC rete, consulta Connect SageMaker AI Studio Notebooks in a VPC a External Resources.

Limitazioni

- Dopo aver creato un dominio SageMaker AI Studio, non è possibile associare nuove sottoreti al dominio.
- Il tipo di VPC rete (solo Internet pubblico o VPC solo) non può essere modificato.

Protezione dei dati

Prima di progettare un carico di lavoro ML, è necessario adottare le pratiche di base che influiscono sulla sicurezza. Ad esempio, la classificazione dei dati fornisce un modo per classificare i dati in base ai livelli di sensibilità e la crittografia protegge i dati rendendoli incomprensibili agli accessi non autorizzati. Questi metodi sono importanti perché supportano obiettivi quali la prevenzione di maltrattamenti o il rispetto degli obblighi normativi.

SageMaker AI Studio offre diverse funzionalità per proteggere i dati archiviati e in transito. Tuttavia, come descritto nel modello di responsabilitàAWS condivisa, i clienti hanno la responsabilità di mantenere il controllo sui contenuti ospitati sull'infrastruttura AWS globale. In questa sezione, descriviamo come i clienti possono utilizzare queste funzionalità per proteggere i propri dati.

Proteggi i dati inutilizzati

Per proteggere i notebook SageMaker AI Studio insieme ai dati di creazione dei modelli e agli artefatti dei modelli, l' SageMaker intelligenza artificiale crittografa i notebook, nonché l'output dei lavori di formazione e di trasformazione in batch. SageMaker L'intelligenza artificiale li crittografa per impostazione predefinita, utilizzando la AWS Managed Key per Amazon S3. Questa chiave AWS gestita per Amazon S3 non può essere condivisa per l'accesso su più account. Per l'accesso su più account, specifica la chiave gestita dal cliente durante la creazione di risorse SageMaker AI in modo che possa essere condivisa per l'accesso su più account.

Con SageMaker AI Studio, i dati possono essere archiviati nelle seguenti posizioni:

- Bucket S3: quando è abilitato un notebook condivisibile, SageMaker AI Studio condivide istantanee e metadati del notebook in un bucket S3.
- EFSvolume: SageMaker AI Studio collega un EFS volume al tuo dominio per l'archiviazione di notebook e file di dati. Questo EFS volume persiste anche dopo l'eliminazione del dominio.
- EBSvolume: EBS è collegato all'istanza su cui viene eseguito il notebook. Questo volume persiste per tutta la durata dell'istanza.

Crittografia inattiva con AWS KMS

- Puoi passare la tua AWS KMS chiave per crittografare un EBS volume collegato a notebook, training, tuning, processi di trasformazione in batch ed endpoint.

- Se non specifichi una KMS chiave, l' SageMaker intelligenza artificiale crittografa sia i volumi del sistema operativo (OS) che i volumi di dati ML con una chiave gestita dal sistema. KMS
- I dati sensibili che devono essere crittografati con una KMS chiave per motivi di conformità devono essere archiviati nel volume di archiviazione ML o in Amazon S3, entrambi i quali possono essere crittografati utilizzando una KMS chiave specificata dall'utente.

Proteggere i dati in transito

SageMaker AI Studio garantisce che gli artefatti del modello ML e altri artefatti di sistema siano crittografati in transito e a riposo. Le richieste all' SageMaker IA API e alla console vengono effettuate tramite una connessione sicura (). SSL Alcuni dati tra reti in transito (all'interno della piattaforma del servizio) sono non crittografati. Questo include:

- Comunicazioni di comando e controllo tra il piano di controllo del servizio e le istanze del processo di addestramento (non i dati del cliente).
- Comunicazioni tra nodi in processi di elaborazione e formazione distribuiti (all'interno della rete).

Tuttavia, è possibile scegliere di crittografare la comunicazione tra i nodi in un cluster di addestramento. L'abilitazione della crittografia del traffico tra container può incrementare il tempo di addestramento, soprattutto se si utilizzano algoritmi di deep learning distribuiti.

Per impostazione predefinita, Amazon SageMaker AI esegue lavori di formazione in Amazon VPC per proteggere i tuoi dati. Puoi aggiungere un altro livello di sicurezza per proteggere i contenitori e i dati di formazione configurandone uno privatoVPC. Inoltre, puoi configurare il tuo dominio SageMaker AI Studio per l'esecuzione in modalità VPC solo e configurare gli VPC endpoint per instradare il traffico su una rete privata senza far uscire il traffico su Internet.

Barriere per la protezione dei dati

Crittografa i volumi di hosting SageMaker AI inattivi

Utilizza la seguente politica per applicare la crittografia durante l'hosting di un endpoint SageMaker AI per l'inferenza online:

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

```
    {
        "Sid": "Encryption",
        "Effect": "Allow",
        "Action": [
            "sagemaker:CreateEndpointConfig"
        ],
        "Resource": "*",
        "Condition": {
            "Null": {
                "sagemaker:VolumeKmsKey": "false"
            }
        }
    }
  ]
}
```

Crittografa i bucket S3 utilizzati durante il monitoraggio del modello

Model Monitoring acquisisce i dati inviati al tuo endpoint SageMaker AI e li archivia in un bucket S3. Quando configuri Data Capture Config, devi crittografare il bucket S3. Attualmente non esiste un controllo di compensazione in merito.

Oltre a registrare gli output degli endpoint, il servizio Model Monitoring verifica l'eventuale deviazione rispetto a una linea di base prestabilita. È necessario crittografare gli output e i volumi di archiviazione intermedi utilizzati per monitorare la deriva.

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateMonitoringSchedule",
             "sagemaker:UpdateMonitoringSchedule"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false",
                 "sagemaker:OutputKmsKey": "false"
             }
```

```
        }
    }
  ]
}
```

Crittografa il volume di archiviazione di un dominio SageMaker AI Studio

Applica la crittografia al volume di archiviazione collegato al dominio Studio. Questa politica richiede che un utente fornisca un file CMK per crittografare i volumi di archiviazione collegati ai domini di studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EncryptDomainStorage",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:VolumeKmsKey": "false"
                }
            }
        }
    ]
}
```

Crittografa i dati archiviati in S3 utilizzati per condividere notebook

Questa è la politica per crittografare tutti i dati archiviati nel bucket utilizzato per condividere notebook tra utenti in un dominio AI Studio: SageMaker

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EncryptDomainSharingS3Bucket",
            "Effect": "Allow",
```

```
            "Action": [
                "sagemaker:CreateDomain",
                "sagemaker:UpdateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:DomainSharingOutputKmsKey": "false"
                }
            }
        }
    ]
}
```

Limitazioni

- Una volta creato un dominio, non è possibile aggiornare lo storage del EFS volume collegato con una chiave personalizzata. AWS KMS
- Non è possibile aggiornare i lavori di formazione/elaborazione o le configurazioni degli endpoint con le KMS chiavi una volta create.

Registrazione di log e monitoraggio

Per aiutarti a eseguire il debug di processi di compilazione, processi di elaborazione, lavori di formazione, endpoint, processi di trasformazione, istanze notebook e configurazioni del ciclo di vita delle istanze notebook, tutto ciò che un contenitore di algoritmi, un contenitore modello o una configurazione del ciclo di vita di un'istanza notebook invia a stdout o stderr viene inviato anche ad Amazon Logs. CloudWatch Puoi monitorare SageMaker AI Studio utilizzando Amazon CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per 15 mesi, così puoi accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni della tua applicazione o del tuo servizio web.

Registrazione con CloudWatch

Poiché il processo di data science è intrinsecamente sperimentale e iterativo, è essenziale registrare attività come l'utilizzo del notebook, la durata dei lavori di formazione/elaborazione, le metriche di formazione e le metriche di servizio degli endpoint come la latenza di chiamata. Per impostazione predefinita, l' SageMaker intelligenza artificiale pubblica le metriche in CloudWatch Logs e questi log possono essere crittografati con chiavi gestite dal cliente utilizzando. AWS KMS

Puoi anche utilizzare gli VPC endpoint a cui inviare i log senza utilizzare la rete Internet pubblica. CloudWatch È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

SageMaker AI crea un singolo gruppo di log per Studio, sotto`/aws/sagemaker/studio`. Ogni profilo utente e app ha il proprio flusso di log in questo gruppo di log e anche gli script di configurazione del ciclo di vita hanno il proprio flusso di log. Ad esempio, un profilo utente denominato «studio-user» con un'app Jupyter Server e uno script del ciclo di vita allegato e un'app Data Science Kernel Gateway hanno i seguenti flussi di log:

`/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default`

`/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default/LifecycleConfigOnStart`

`/aws/sagemaker/studio/<domain-id>/studio-user/KernelGateway/datascience-app`

Affinché l' SageMaker IA possa inviare i log per tuo conto, il chiamante CloudWatch del lavoro avrà bisogno delle seguenti autorizzazioni: Training/Processing/Transform APIs

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "logs:CreateLogDelivery",
                 "logs:CreateLogGroup",
                 "logs:CreateLogStream",
                 "logs:DeleteLogDelivery",
                 "logs:Describe*",
                 "logs:GetLogEvents",
                 "logs:GetLogDelivery",
                 "logs:ListLogDeliveries",
                 "logs:PutLogEvents",
                 "logs:PutResourcePolicy",
                 "logs:UpdateLogDelivery"
             ],
             "Resource": "*",
             "Effect": "Allow"
         }
     ]
 }
```

Per crittografare tali registri con una AWS KMS chiave personalizzata, dovrai prima modificare la politica delle chiavi per consentire al CloudWatch servizio di crittografare e decrittografare la chiave. Dopo aver creato una chiave di crittografia dei log, modifica la politica della AWS KMS chiave per includere quanto segue:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
    ]
}
```

Tieni presente che puoi sempre utilizzare `ArnEquals` e fornire un Amazon Resource Name (ARN) specifico per il CloudWatch log che desideri crittografare. Qui mostriamo che puoi usare questa chiave per crittografare tutti i log di un account per semplificare la procedura. Inoltre, gli endpoint di formazione, elaborazione e modello pubblicano metriche sull'utilizzo dell'istanza CPU e della memoria, sulla latenza delle chiamate di hosting e così via. Puoi configurare ulteriormente Amazon SNS per notificare agli amministratori gli eventi quando vengono superate determinate soglie. L'utente della formazione e dell'elaborazione APIs deve disporre delle seguenti autorizzazioni:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "cloudwatch:DeleteAlarms",
                 "cloudwatch:DescribeAlarms",
                 "cloudwatch:GetMetricData",
                 "cloudwatch:GetMetricStatistics",
                 "cloudwatch:ListMetrics",
                 "cloudwatch:PutMetricAlarm",
                 "cloudwatch:PutMetricData",
                 "sns:ListTopics"
             ],
             "Resource": "*",
             "Effect": "Allow",
             "Condition": {
                 "StringLike": {
                     "cloudwatch:namespace": "aws/sagemaker/*"
                 }
             }
```

```
        },
        {
            "Action": [
                "sns:Subscribe",
                "sns:CreateTopic"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*SageMaker*",
                "arn:aws:sns:*:*:*Sagemaker*",
                "arn:aws:sns:*:*:*sagemaker*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Verifica con AWS CloudTrail

Per migliorare il tuo livello di conformità, verifica tutto ciò che haiAPIs. AWS CloudTrail Per impostazione predefinita, tutte le SageMaker IA APIs sono registrate con. AWS CloudTrail Non sono necessarie IAM autorizzazioni aggiuntive per l'attivazione. CloudTrail

Tutte le azioni di SageMaker intelligenza artificiale, ad eccezione di `InvokeEndpoint` e`InvokeEndpointAsync`, vengono registrate CloudTrail e documentate nelle operazioni. Ad esempio, le chiamate alle `CreateNotebookInstance` azioni `CreateTrainingJob`e `CreateEndpoint`, e generano voci nei file di CloudTrail registro.

Ogni voce CloudTrail dell'evento contiene informazioni su chi ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente AWS IAM o root.
- 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. Per un evento di esempio, consulta la sezione Registra API chiamate SageMaker AI con CloudTrail documentazione.

Per impostazione predefinita, CloudTrail registra il nome del ruolo di esecuzione di Studio del profilo utente come identificatore per ogni evento. Funziona se ogni utente ha il proprio ruolo di esecuzione. Se più utenti condividono lo stesso ruolo di esecuzione, puoi utilizzare la `sourceIdentity`

configurazione per propagare il nome del profilo utente di Studio. CloudTrail Per abilitare la `sourceIdentity` funzionalità, consulta Monitoraggio dell'accesso alle risorse degli utenti da Amazon SageMaker AI Studio. In uno spazio condiviso, tutte le azioni si riferiscono allo spazio ARN come origine e non è possibile eseguire il controllo`sourceIdentity`.

Attribuzione dei costi

SageMaker AI Studio ha funzionalità integrate per aiutare gli amministratori a tenere traccia della spesa dei singoli domini, degli spazi condivisi e degli utenti.

Etichettatura automatica

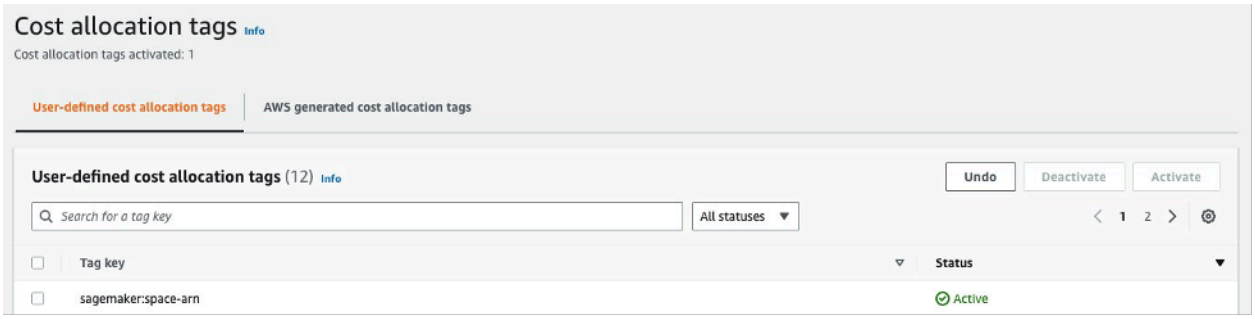
SageMaker AI Studio ora tagga automaticamente SageMaker le nuove risorse come i lavori di formazione, i lavori di elaborazione e le app del kernel con le rispettive. `sagemaker:domain-arn` A un livello più granulare, l' SageMaker IA contrassegna anche la risorsa con `sagemaker:user-profile-arn` o `sagemaker:space-arn` per designare il principale creatore della risorsa.

SageMaker EFSI volumi di dominio AI sono etichettati con una chiave denominata `ManagedByAmazonSageMakerResource` con il valore del dominio. ARN Non dispongono di tag granulari per comprendere l'utilizzo dello spazio a livello di utente. Tuttavia, gli amministratori possono collegare il EFS volume a un'EC2istanza per un monitoraggio personalizzato.

Monitoraggio dei costi

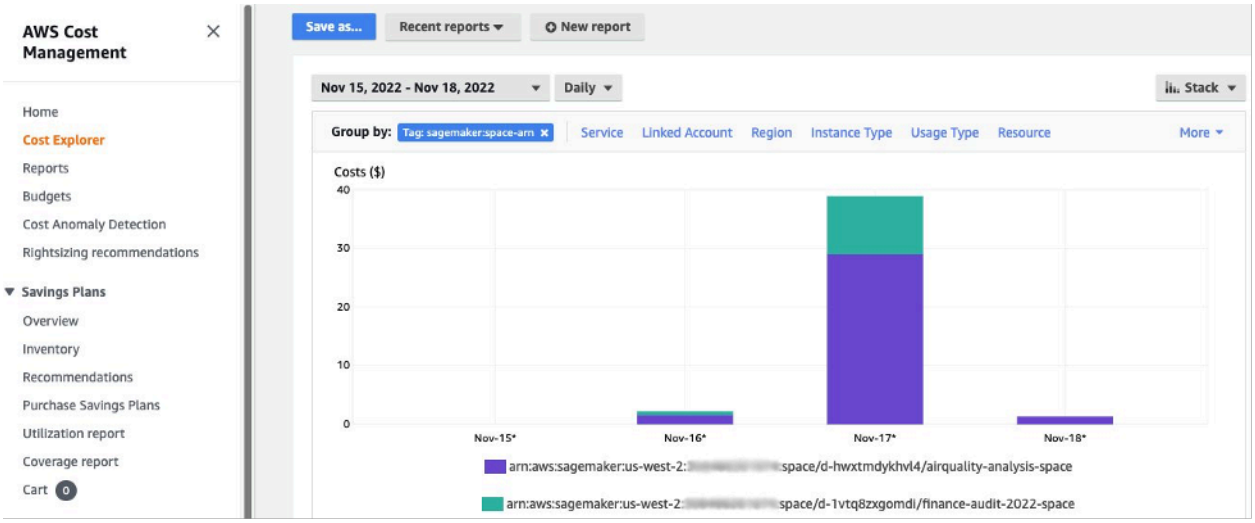
I tag automatici consentono agli amministratori di tracciare, riportare e monitorare la spesa per il machine out-of-the-box learning attraverso soluzioni come AWS Cost Explorere Budget AWS, oltre a soluzioni personalizzate basate sui dati dei report sui AWS costi e sull'utilizzo (). CURs

Per utilizzare i tag allegati per l'analisi dei costi, è necessario prima attivarli nella sezione Tag di allocazione dei costi della AWS Billing console. La visualizzazione dei tag nel pannello dei tag di allocazione dei costi può richiedere fino a 24 ore, quindi dovrai creare una risorsa di SageMaker intelligenza artificiale prima di abilitarli.



Spazio ARN abilitato come tag di allocazione dei costi su Cost Explorer

Dopo aver abilitato un tag di allocazione dei costi, AWS inizieranno a tracciare le risorse contrassegnate e, dopo 24-48 ore, i tag verranno visualizzati come filtri selezionabili in Cost Explorer.



Costi raggruppati per spazio condiviso per un dominio di esempio

Controllo dei costi

Quando il primo utente di SageMaker AI Studio viene integrato, SageMaker AI crea un EFS volume per il dominio. I costi di archiviazione sono sostenuti per questo EFS volume poiché i notebook e i file di dati vengono archiviati nella home directory dell'utente. Quando l'utente avvia i notebook Studio, vengono avviati per le istanze di calcolo che eseguono i notebook. Consulta i prezzi di Amazon SageMaker AI per una ripartizione dettagliata dei costi.

Gli amministratori possono controllare i costi di elaborazione specificando l'elenco di istanze che un utente può avviare, utilizzando le IAM politiche indicate nella sezione Common guardrails. Inoltre, consigliamo ai clienti di utilizzare l'estensione per lo spegnimento automatico di SageMaker AI Studio per risparmiare sui costi chiudendo automaticamente le app inattive. Questa estensione del server verifica periodicamente la presenza di app in esecuzione per profilo utente e chiude le app inattive in base a un timeout impostato dall'amministratore.

Per impostare questa estensione per tutti gli utenti del tuo dominio, puoi utilizzare una configurazione del ciclo di vita come descritto nella sezione Personalizzazione. Inoltre, puoi anche utilizzare il correttore delle estensioni per assicurarti che tutti gli utenti del tuo dominio abbiano l'estensione installata.

Personalizzazione

Configurazione del ciclo di vita

Le configurazioni del ciclo di vita sono script di shell avviati da eventi del ciclo di vita di AI Studio, come l'avvio di un nuovo notebook AI Studio. SageMaker SageMaker Puoi utilizzare questi script di shell per automatizzare la personalizzazione dei tuoi ambienti SageMaker AI Studio, come l'installazione di pacchetti personalizzati, l'estensione Jupyter per lo spegnimento automatico delle app per notebook inattive e la configurazione di Git. Per istruzioni dettagliate su come creare configurazioni del ciclo di vita, consulta questo blog: Personalizza Amazon SageMaker AI Studio usando le configurazioni del ciclo di vita.

Immagini personalizzate per notebook AI Studio SageMaker

I notebook Studio sono dotati di un set di immagini predefinite, costituite da Amazon AI SageMaker Python SDK e dall'ultima versione del runtime o del kernel. IPython Con questa funzionalità, puoi portare le tue immagini personalizzate sui notebook Amazon SageMaker AI. Queste immagini sono quindi disponibili per tutti gli utenti autenticati nel dominio.

Gli sviluppatori e i data scientist possono richiedere immagini personalizzate per diversi casi d'uso:

- Accesso a versioni specifiche o più recenti dei framework ML più diffusi come TensorFlow, MXNet PyTorch, o altri.
- Aggiungi codice o algoritmi personalizzati sviluppati localmente nei notebook SageMaker AI Studio per una rapida iterazione e formazione dei modelli.
- Accesso ai data lake o agli archivi dati locali tramite. APIs Gli amministratori devono includere i driver corrispondenti all'interno dell'immagine.
- Accesso a un runtime di backend (chiamato anche kernel), diverso da IPython (come R, Julia o altri). Puoi anche usare l'approccio descritto per installare un kernel personalizzato.

Per istruzioni dettagliate su come creare un'immagine personalizzata, consulta Creare un'immagine SageMaker AI personalizzata.

JupyterLab estensioni

Con SageMaker AI Studio JuypterLab 3 Notebook, puoi sfruttare la community in continua crescita di estensioni open source JupyterLab. Questa sezione ne evidenzia alcune che si adattano naturalmente al flusso di lavoro degli sviluppatori di SageMaker intelligenza artificiale, ma ti invitiamo a sfogliare le estensioni disponibili o persino a crearne di tue.

JupyterLab 3 ora semplifica notevolmente il processo di impacchettamento e installazione delle estensioni. È possibile installare le suddette estensioni tramite script bash. Ad esempio, in SageMaker AI Studio, apri il terminale di sistema dal programma di avvio di Studio ed esegui i seguenti comandi. Inoltre, puoi automatizzare l'installazione di queste estensioni utilizzando configurazioni del ciclo di vita in modo che rimangano permanenti tra i riavvii di Studio. Puoi configurarlo per tutti gli utenti del dominio o a livello di singolo utente.

Ad esempio, per installare un'estensione per un browser di file Amazon S3, esegui i seguenti comandi nel terminale di sistema e assicurati di aggiornare il browser:

```
conda init
conda activate studio
pip install jupyterlab_s3_browser
jupyter serverextension enable --py jupyterlab_s3_browser
conda deactivate
restart-jupyter-server
```

Per ulteriori informazioni sulla gestione delle estensioni, incluso come scrivere configurazioni del ciclo di vita che funzionino per entrambe le versioni 1 e 3 dei JupyterLab notebook per la compatibilità con le versioni precedenti, consulta Installazione delle estensioni e Jupyter Server. JupyterLab

Archivi Git

SageMaker AI Studio è preinstallato con un'estensione Jupyter Git che consente agli utenti di accedere a un URL repository Git personalizzato, clonarlo nella directory, inviare modifiche e EFS visualizzare la cronologia dei commit. Gli amministratori possono configurare i repository git suggeriti a livello di dominio in modo che vengano visualizzati come selezioni a discesa per gli utenti finali. Per up-to-date istruzioni, consulta Allega repository Git suggeriti a Studio.

Se un repository è privato, l'estensione chiederà all'utente di inserire le proprie credenziali nel terminale utilizzando l'installazione git standard. In alternativa, l'utente può memorizzare le credenziali ssh nella propria EFS directory individuale per una gestione più semplice.

Ambiente Conda

SageMaker I notebook AI Studio utilizzano Amazon EFS come livello di storage persistente. I data scientist possono utilizzare lo storage persistente per creare ambienti conda personalizzati e utilizzare questi ambienti per creare kernel. Questi kernel sono supportati EFS e sono persistenti tra i riavvii del kernel, dell'app o di Studio. Studio seleziona automaticamente tutti gli ambienti validi come kernel. KernelGateway

Il processo di creazione di un ambiente conda è semplice per un data scientist, ma i kernel impiegano circa un minuto per essere compilati sul selettore del kernel. Per creare un ambiente, esegui quanto segue in un terminale di sistema:

```
mkdir -p ~/.conda/envs
conda create --yes -p ~/.conda/envs/custom
conda activate ~/.conda/envs/custom
conda install -y ipykernel
conda config --add envs_dirs ~/.conda/envs
```

Per istruzioni dettagliate, consulta la sezione Persisti gli ambienti Conda nel EFS volume Studio in Quattro approcci per gestire i pacchetti Python nei notebook Amazon Studio. SageMaker

Conclusioni

In questo white paper, abbiamo esaminato diverse best practice in aree quali modello operativo, gestione dei domini, gestione delle identità, gestione delle autorizzazioni, gestione della rete, registrazione, monitoraggio e personalizzazione per consentire agli amministratori della piattaforma di configurare e gestire la piattaforma AI Studio. SageMaker

Appendice

Confronto tra più locazioni

Tabella 2 — Confronto tra più locazioni

Multidominio	Account multiplo	Controllo degli accessi basato sugli attributi (ABAC) all'inter no di un singolo dominio
L'isolamento delle risorse si ottiene utilizzando i tag. SageMaker AI Studio etichetta automaticamente tutte le risorse con il dominio ARN e il profilo/spazio utente. ARN	Ogni inquilino ha il proprio account, quindi c'è un isolamento assoluto delle risorse.	L'isolamento delle risorse si ottiene utilizzando i tag. Gli utenti devono gestire l'etichet tatura delle risorse create perABAC.
L'elenco APIs non può essere limitato dai tag. Il filtraggio delle risorse tramite interfacc ia utente viene eseguito sugli spazi condivisi, tuttavia, API le chiamate List effettuate tramite AWS CLI o Boto3 SDK elencheranno le risorse in tutta la regione.	È anche possibile APIs l'isolamento delle liste, poiché gli inquilini sono nei loro account dedicati.	L'elenco APIs non può essere limitato dai tag. Elenca API le chiamate effettuate tramite AWS CLI o Boto3 SDK elencherà le risorse in tutta la regione.
SageMaker I costi di calcolo e archiviazione di AI Studio per tenant possono essere facilmente monitorati utilizzan do Domain ARN come tag di allocazione dei costi.	SageMaker I costi di calcolo e archiviazione di AI Studio per tenant sono facili da monitorar e con un account dedicato.	SageMaker I costi di calcolo di AI Studio per tenant devono essere calcolati utilizzando tag personalizzati. SageMaker I costi di archiviaz ione di AI Studio non possono essere monitorati per dominio

Multidominio	Account multiplo	Controllo degli accessi basato sugli attributi (ABAC) all'interno di un singolo dominio
		poiché tutti i tenant condividono lo stesso volume. EFS
Le quote di servizio sono impostate a livello di account, quindi un singolo tenant potrebbe comunque utilizzare tutte le risorse.	Le quote di servizio possono essere impostate a livello di account per ogni tenant.	Le quote di servizio sono impostate a livello di account, in modo che un singolo tenant possa comunque utilizzare tutte le risorse.
La scalabilità a più tenant può essere ottenuta tramite Infrastructure as code (IaC) o Service Catalog.	La scalabilità a più tenant coinvolge Organizations e la vendita di più account.	La scalabilità richiede un ruolo specifico del tenant per ogni nuovo tenant e i profili utente devono essere etichettati manualmente con i nomi dei tenant.
La collaborazione tra gli utenti all'interno di un tenant è possibile tramite spazi condivisi.	La collaborazione tra utenti all'interno di un tenant è possibile tramite spazi condivisi.	Tutti gli inquilini avranno accesso allo stesso spazio condiviso per la collaborazione.

SageMaker Backup e ripristino del dominio AI Studio

In caso di EFS eliminazione accidentale o quando è necessario ricreare un dominio a causa di modifiche alla rete o all'autenticazione, segui queste istruzioni.

Opzione 1: eseguire il backup da un dispositivo esistente EFS EC2

SageMaker Backup del dominio Studio

1. Elenca i profili utente e gli spazi in SageMaker Studio (CLI, SDK).
2. Mappa i profili/gli spazi utente su UIDs on. EFS
   a. Per ogni utente nell'elenco di users/spaces, describe the user profile/space (CLI, SDK).

b. Mappa il profilo/spazio utente su. `HomeEfsFileSystemUid`

c. Mappa il profilo utente per verificare `UserSettings['ExecutionRole']` se gli utenti hanno ruoli di esecuzione distinti.

d. Identifica il ruolo di esecuzione Space predefinito.

3. Crea un nuovo dominio e specifica il ruolo di esecuzione Space predefinito.
4. Crea profili e spazi utente.
   - Per ogni utente nell'elenco di utenti, crea il profilo utente (CLI, SDK) utilizzando la mappatura dei ruoli di esecuzione.
5. Crea una mappatura per il nuovo EFS e. UIDs
   a. Per ogni utente nell'elenco di utenti, descrivi il profilo utente (CLI, SDK).

   b. Mappa il profilo utente su`HomeEfsFileSystemUid`.
6. Facoltativamente, elimina tutte le app, i profili utente, gli spazi, quindi elimina il dominio.

Backup EFS

Per eseguire il backupEFS, segui le seguenti istruzioni:

1. Avvia l'EC2istanza e collega i gruppi di sicurezza in entrata/uscita del vecchio dominio SageMaker Studio alla nuova EC2 istanza (consenti il NFS traffico sulla TCP porta 2049). Fare riferimento a Connect SageMaker Studio Notebooks in VPC a Risorse esterne.
2. Monta il EFS volume SageMaker Studio sulla nuova istanza. EC2 Fare riferimento a Montaggio dei EFS file system.
3. Copia i file nella memoria EBS locale: `>sudo cp -rp /efs /studio-backup:`
   a. Allega i nuovi gruppi di sicurezza del dominio all'EC2istanza.

   b. Monta il nuovo EFS volume sull'EC2istanza.

   c. Copia i file nel nuovo EFS volume.

   d. Per ogni utente nella raccolta dell'utente:
      i. Crea la directory:`mkdir new_uid`.

      ii. Copia i file dalla vecchia UID cartella alla nuova UID cartella.

      iii. Cambia la proprietà di tutti i file: `chown <new_UID>` per tutti i file.

Opzione 2: Esegui il backup dall'esistente EFS utilizzando S3 e la configurazione del ciclo di vita

1. Fai riferimento a Migrare il tuo lavoro su un'istanza di SageMaker notebook Amazon con Amazon Linux 2.
2. Crea un bucket S3 per il backup (ad esempio. `>studio-backup`
3. Elenca tutti i profili utente con ruoli di esecuzione.
4. Nel dominio SageMaker Studio corrente, imposta uno LCC script predefinito a livello di dominio.
   - InLCC, copia tutto nel `/home/sagemaker-user` prefisso del profilo utente in S3 (ad esempio,`s3://studio-backup/studio-user1`).
5. Riavvia tutte le app Jupyter Server predefinite (per eseguirleLCC).
6. Elimina tutte le app, i profili utente e i domini.
7. Crea un nuovo dominio SageMaker Studio.
8. Crea nuovi profili utente dall'elenco dei profili utente e dei ruoli di esecuzione.
9. Configura un LCC a livello di dominio:
   - InLCC, copia tutto ciò che è contenuto nel prefisso del profilo utente in S3 su `/home/sagemaker-user`
10. Crea app Jupyter Server predefinite per tutti gli utenti con la LCC configurazione (,). CLISDK

SageMaker Accesso allo studio tramite assertion SAML

Configurazione della soluzione:

1. Crea un'SAMLapplicazione nel tuo IdP esterno.
2. Configura l'IdP esterno come provider di identità in. IAM
3. Crea una funzione `SAMLValidator` Lambda a cui l'IdP può accedere (tramite una funzione URL o un gateway). API
4. Crea una funzione `GeneratePresignedUrl` Lambda e un API gateway per accedere alla funzione.
5. Crea un IAM ruolo che gli utenti possano assumere per richiamare il API Gateway. Questo ruolo deve essere passato in SAML forma di attributo nel seguente formato:
   - Nome dell'attributo: https://aws.amazon.com/SAML/ Attributes/Role
   - Valore dell'attributo:, `<IdentityProviderARN> <RoleARN>`

6. Aggiorna l'endpoint SAML Assertion Consumer Service (ACS) all'`SAMLValidator`invoke. URL

SAMLcodice di esempio di validatore:

```
import requests
import os
import boto3
from urllib.parse import urlparse, parse_qs
import base64
import requests
from aws_requests_auth.aws_auth import AWSRequestsAuth
import json


# Config for calling AssumeRoleWithSAML
idp_arn = "arn:aws:iam::0123456789:saml-provider/MyIdentityProvider"
api_gw_role_arn = 'arn:aws:iam:: 0123456789:role/APIGWAccessRole'
studio_api_url = "abcdef.execute-api.us-east-1.amazonaws.com"
studio_api_gw_path = "https://" + studio_api_url + "/Prod "

# Every customer will need to get SAML Response from the POST call
def get_saml_response(event):
    saml_response_uri = base64.b64decode(event['body']).decode('ascii')
    request_body = parse_qs(saml_response_uri)
    print(f"b64 saml response: {request_body['SAMLResponse'][0]}")
    return request_body['SAMLResponse'][0]


def lambda_handler(event, context):
    sts = boto3.client('sts')

    # get temporary credentials
    response = sts.assume_role_with_saml(
                    RoleArn=api_gw_role_arn,
                    PrincipalArn=durga_idp_arn,
                    SAMLAssertion=get_saml_response(event)
                )
    auth = AWSRequestsAuth(aws_access_key=response['Credentials']['AccessKeyId'],
                      aws_secret_access_key=response['Credentials']['SecretAccessKey'],
                      aws_host=studio_api_url,
                      aws_region='us-west-2',
                      aws_service='execute-api',
                      aws_token=response['Credentials']['SessionToken'])
```

```
    presigned_response = requests.post(
        studio_api_gw_path,
        data=saml_response_data,
        auth=auth)

    return presigned_response
```

Approfondimenti

- Configurazione di ambienti di machine learning sicuri e ben gestiti su AWS (AWS blog)
- Configurazione di Amazon SageMaker AI Studio per team e gruppi con isolamento completo delle risorse (AWS blog)
- Onboarding di Amazon SageMaker AI Studio con AWS SSO Okta Universal Directory (blog)AWS
- Come configurare SAML 2.0 per AWS Account Federation (documentazione Okta)
- Crea una piattaforma di Machine Learning aziendale sicura su AWS (guida AWS tecnica)
- Personalizza Amazon SageMaker AI Studio utilizzando le configurazioni del ciclo di vita (blog)AWS
- Trasferire l'immagine del contenitore personalizzata nei notebook Amazon SageMaker AI Studio (blog)AWS
- Crea modelli di progetto SageMaker AI personalizzati: best practice (blog)AWS
- Implementazione di modelli multi-account con Amazon SageMaker AI Pipelines (blog)AWS
- Parte 1: Come NatWest Group ha creato una MLOps piattaforma scalabile, sicura e sostenibile (blog)AWS
- Amazon SageMaker AI Studio sicuro preconfigurato URLs Parte 1: infrastruttura di base (blog)AWS

Collaboratori

Hanno collaborato alla stesura del presente documento:

- Ram Vittal, architetto di soluzioni ML, Amazon Web Services
- Sean Morgan, architetto di soluzioni ML, Amazon Web Services
- Durga Sury, architetto di soluzioni ML, Amazon Web Services

Un ringraziamento speciale ai seguenti che hanno contribuito con idee, revisioni e prospettive:

- Alessandro Cerè, Architetto di soluzioni AI/ML, Amazon Web Services
- Sumit Thakur, responsabile dei prodotti di SageMaker intelligenza artificiale, Amazon Web Services
- Han Zhang, ingegnere senior dello sviluppo software, Amazon Web Services
- Bhadrinath Pani, ingegnere di sviluppo software, Amazon Web Services, Amazon Web Services

Revisioni del documento

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed RSS.

Modifica	Descrizione	Data
Whitepaper aggiornato	Corretti i collegamenti interrotti e numerose modifiche editoriali.	25 aprile 2023
Pubblicazione iniziale	Whitepaper pubblicato.	19 ottobre 2022

Note

I clienti hanno la responsabilità di effettuare la propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWSi prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per 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.