Guida per l'utente

AWS Deadline Cloud

Version latest

AWS Deadline Cloud: Guida per l'utente

Table of Contents

Cos'è AWS Deadline Cloud?

Deadline Cloud è uno strumento Servizio AWS che puoi utilizzare per creare e gestire progetti e lavori di rendering su istanze Amazon Elastic Compute Cloud (Amazon EC2) direttamente da pipeline e workstation per la creazione di contenuti digitali.

Deadline Cloud fornisce interfacce di console, applicazioni locali, strumenti da riga di comando e un'API. Con Deadline Cloud, puoi creare, gestire e monitorare fattorie, flotte, lavori, gruppi di utenti e sistemi di archiviazione. Puoi anche specificare i requisiti hardware, creare ambienti per carichi di lavoro specifici e integrare gli strumenti per la creazione di contenuti richiesti dalla tua produzione nella tua pipeline Deadline Cloud.

Deadline Cloud fornisce un'interfaccia unificata per gestire tutti i tuoi progetti di rendering in un unico posto. Puoi gestire gli utenti, assegnare loro progetti e concedere autorizzazioni per i ruoli lavorativi.

Argomenti

Caratteristiche di Deadline Cloud

Ecco alcuni dei modi principali in cui Deadline Cloud può aiutarti a eseguire e gestire carichi di lavoro di elaborazione visiva:

- Crea rapidamente fattorie, code e flotte. Monitora il loro stato e ottieni informazioni dettagliate sul funzionamento della tua azienda agricola e sui posti di lavoro.
- Gestisci centralmente utenti e gruppi di Deadline Cloud e assegna le autorizzazioni.
- Gestisci la sicurezza degli accessi per gli utenti del progetto e i provider di identità esterni con. AWS IAM Identity Center
- Gestisci in modo sicuro l'accesso alle risorse del progetto con politiche e ruoli AWS Identity and Access Management (IAM).

- Usa i tag per organizzare e trovare rapidamente le risorse del progetto.
- Gestisci l'utilizzo delle risorse del progetto e i costi stimati per il tuo progetto.
- Fornisci un'ampia gamma di opzioni di gestione dell'elaborazione per supportare il rendering nel cloud o di persona.

Concetti e terminologia per Deadline Cloud

Per aiutarti a iniziare a usare AWS Deadline Cloud, questo argomento spiega alcuni dei suoi concetti e della terminologia chiave.

Responsabile del budget

: Il gestore del budget fa parte del monitor Deadline Cloud. Usa il gestore del budget per creare e gestire i budget. Puoi anche usarlo per limitare le attività in modo da rispettare il budget.

Libreria client Deadline Cloud

: La Client Library include un'interfaccia a riga di comando e una libreria per la gestione di Deadline Cloud. La funzionalità include l'invio di pacchetti di lavoro basati sulla specifica Open Job Description a Deadline Cloud, il download degli output degli allegati dei lavori e il monitoraggio della fattoria utilizzando l'interfaccia a riga di comando.

Applicazione per la creazione di contenuti digitali (DCC)

: Le applicazioni per la creazione di contenuti digitali (DCC) sono prodotti di terze parti in cui è possibile creare contenuti digitali. Esempi di DCC sonoMaya, e. Nuke Houdini Deadline Cloud fornisce plugin integrati per gli inviatori di lavori per DCC specifici.

Farm

: Una fattoria è il luogo in cui si trovano le risorse del progetto. È costituita da code e flotte.

Parco istanze

: Una flotta è un gruppo di nodi di lavoro che eseguono il rendering. I nodi di lavoro elaborano i lavori. Una flotta può essere associata a più code e una coda può essere associata a più flotte.

Processo

: Un lavoro è una richiesta di rendering. Gli utenti inviano offerte di lavoro. I lavori contengono proprietà specifiche del lavoro che sono descritte come passaggi e attività.

Allegati Job

Un allegato di lavoro è una funzionalità di Deadline Cloud che puoi utilizzare per gestire input e output per i lavori. I file di lavoro vengono caricati come allegati del lavoro durante il processo di rendering. Questi file possono essere texture, modelli 3D, impianti di illuminazione e altri elementi simili.

Proprietà processo

Le proprietà del lavoro sono impostazioni che definisci quando invii un lavoro di rendering. Alcuni esempi includono l'intervallo di fotogrammi, il percorso di output, gli allegati dei lavori, la fotocamera renderizzabile e altro ancora. Le proprietà variano in base al DCC da cui viene inviato il rendering.

Modello del processo

Un modello di lavoro definisce l'ambiente di runtime e tutti i processi eseguiti come parte di un job di Deadline Cloud.

Queue

Una coda è il luogo in cui si trovano i lavori inviati e ne è programmata la visualizzazione. Una coda deve essere associata a una flotta per creare un rendering riuscito. Una coda può essere associata a più flotte.

Associazione queue-fleet

Quando una coda è associata a una flotta, esiste un'associazione queue-fleet. Utilizzate un'associazione per programmare i lavoratori di una flotta ai lavori presenti in quella coda. È possibile avviare e interrompere le associazioni per controllare la pianificazione del lavoro.

Fase

Un passaggio è un processo particolare da eseguire nel processo.

Inviatore di Deadline Cloud

Un mittente di Deadline Cloud è un plug-in per la creazione di contenuti digitali (DCC). Gli artisti lo usano per inviare lavori da un'interfaccia DCC di terze parti con cui hanno familiarità.

Tag

Un tag è un'etichetta che puoi assegnare a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale definiti dall'utente.

Con i tag, puoi classificare le tue AWS risorse in diversi modi. Ad esempio, puoi definire un set di tag per le istanze Amazon EC2 del tuo account che ti aiutino a monitorare il proprietario e il livello di stack di ogni istanza.

Puoi anche classificare le tue AWS risorse per scopo, proprietario o ambiente. Questo approccio è utile quando si dispone di molte risorse dello stesso tipo. Puoi identificare rapidamente una risorsa specifica in base ai tag che le hai assegnato.

Attività

Un'attività è un singolo componente di una fase di rendering.

Licenze basate sull'utilizzo (UBL)

Le licenze basate sull'utilizzo (UBL) sono un modello di licenza su richiesta disponibile per determinati prodotti di terze parti. Questo modello è pagato in base al consumo e ti viene addebitato il numero di ore e minuti utilizzati.

Esploratore di utilizzo

Usage explorer è una funzionalità di Deadline Cloud Monitor. Fornisce una stima approssimativa dei costi e dell'utilizzo.

Worker

I lavoratori appartengono alle flotte ed eseguono le attività assegnate da Deadline Cloud per completare fasi e lavori. I lavoratori archiviano i log delle operazioni delle attività in Amazon CloudWatch Logs. I lavoratori possono anche utilizzare la funzionalità job attachments per sincronizzare input e output con un bucket Amazon Simple Storage Service (Amazon S3).

Guida introduttiva a Deadline Cloud

Usa Deadline Cloud per creare rapidamente una render farm con impostazioni e risorse predefinite, come la configurazione dell'istanza Amazon EC2 e i bucket Amazon Simple Storage Service (Amazon S3).

Puoi anche definire le impostazioni e le risorse quando crei una render farm. Questo metodo richiede più tempo rispetto all'utilizzo delle impostazioni e delle risorse predefinite, ma offre un maggiore controllo.

Dopo aver acquisito familiarità con i concetti e la terminologia di Deadline Cloud, consulta la Guida introduttiva per step-by-step istruzioni su come creare la tua farm, aggiungere utenti e collegamenti a informazioni utili.

Accesso a Deadline Cloud

Puoi accedere a Deadline Cloud in uno dei seguenti modi:

- Console Deadline Cloud: accedi alla console in un browser per creare una farm e le relative risorse e gestire l'accesso degli utenti. Per ulteriori informazioni, consulta Guida introduttiva.
- Deadline Cloud monitor: gestisci i tuoi lavori di rendering, incluso l'aggiornamento delle priorità e dello stato dei lavori. Monitora la tua fattoria e visualizza i registri e lo stato del lavoro. Per gli utenti con autorizzazioni di proprietario, il monitor Deadline Cloud fornisce anche l'accesso per esplorare l'utilizzo e creare budget. Il monitor Deadline Cloud è disponibile sia come browser web che come applicazione desktop.
- AWS SDK e AWS CLI: utilizza AWS Command Line Interface (AWS CLI) per richiamare le operazioni dell'API Deadline Cloud dalla riga di comando sul sistema locale. Per ulteriori informazioni, consulta Configurare una workstation per sviluppatori.

Servizi correlati

Deadline Cloud funziona con quanto segue: Servizi AWS

- Amazon CloudWatch: con CloudWatch, puoi monitorare i tuoi progetti e AWS le risorse associate. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon EC2: Servizio AWS fornisce server virtuali che eseguono le applicazioni nel cloud. Puoi configurare i tuoi progetti per utilizzare le istanze Amazon EC2 per i tuoi carichi di lavoro. Per ulteriori informazioni, consulta Istanze Amazon EC2.
- Amazon EC2 Auto Scaling: con Auto Scaling, puoi aumentare o diminuire automaticamente il numero di istanze al variare della domanda delle istanze. L'Auto Scaling aiuta a garantire l'esecuzione del numero desiderato di istanze, anche in caso di errore di un'istanza. Se abiliti Auto Scaling con Deadline Cloud, le istanze avviate da Auto Scaling vengono registrate automaticamente con il carico di lavoro. Allo stesso modo, le istanze terminate da Auto Scaling vengono automaticamente cancellate dal carico di lavoro. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon EC2 Auto Scaling.
- AWS PrivateLink— AWS PrivateLink fornisce connettività privata tra cloud privati virtuali (VPC) e reti locali Servizi AWS, senza esporre il traffico alla rete Internet pubblica. AWS PrivateLink semplifica la connessione dei servizi tra diversi account e VPC. Per ulteriori informazioni, consulta AWS PrivateLink.

- Amazon S3 — Amazon S3 è un servizio di storage di oggetti. Deadline Cloud utilizza i bucket Amazon S3 per archiviare gli allegati dei lavori.
- IAM Identity Center: IAM Identity Center è un Servizio AWS luogo in cui puoi fornire agli utenti l'accesso Single Sign-On a tutti gli account e le applicazioni loro assegnati da un'unica posizione. Puoi anche gestire centralmente l'accesso a più account e le autorizzazioni utente per tutti i tuoi account in. AWS Organizations Per ulteriori informazioni, consulta FAQ AWS IAM Identity Center.

Come funziona Deadline Cloud

Con Deadline Cloud, puoi creare e gestire progetti e lavori di rendering direttamente dalle pipeline e dalle workstation per la creazione di contenuti digitali (DCC).

Puoi inviare lavori a Deadline Cloud utilizzando gli inviatori di lavori AWS SDK, AWS Command Line Interface (AWS CLI) o Deadline Cloud. Deadline Cloud supporta l'Open Job Description (OpenJD) per la specificazione dei modelli di lavoro. Per ulteriori informazioni, consulta Open Job Description sul GitHub sito web.

Deadline Cloud fornisce chi invia offerte di lavoro. Un job submitter è un plug-in DCC per l'invio di lavori di rendering da un'interfaccia DCC di terze parti, come o. Maya Nuke Con un mittente, gli artisti possono inviare lavori di rendering da un'interfaccia di terze parti a Deadline Cloud, dove le risorse del progetto vengono gestite e i lavori monitorati, il tutto in un'unica posizione.

Con una Deadline Cloud farm, puoi creare code e flotte, gestire gli utenti e gestire l'utilizzo e i costi delle risorse del progetto. Una fattoria è composta da code e flotte. Una coda è il luogo in cui si trovano i lavori inviati e ne è programmata la visualizzazione. Una flotta è un gruppo di nodi di lavoro che eseguono attività per completare i lavori. Una coda deve essere associata a una flotta in modo che i lavori possano essere visualizzati. Una singola flotta può supportare più code e una coda può essere supportata da più flotte.

I lavori sono costituiti da passaggi e ogni passaggio è costituito da attività specifiche. Con il monitor Deadline Cloud, puoi accedere a stati, registri e altre metriche di risoluzione dei problemi per lavori, passaggi e attività.

Autorizzazioni in Deadline Cloud

Deadline Cloud supporta quanto segue:

- Gestione dell'accesso alle sue operazioni API tramite AWS Identity and Access Management (IAM)

- Gestione dell'accesso degli utenti della forza lavoro mediante un'integrazione con AWS IAM Identity Center

Prima che chiunque possa lavorare su un progetto, deve avere accesso a quel progetto e alla fattoria associata. Deadline Cloud è integrato con IAM Identity Center per gestire l'autenticazione e l'autorizzazione della forza lavoro. Gli utenti possono essere aggiunti direttamente a IAM Identity Center oppure possono essere collegati al tuo provider di identità (IdP) esistente come Okta o. Active Directory Gli amministratori IT possono concedere le autorizzazioni di accesso a utenti e gruppi a diversi livelli. Ogni livello successivo include le autorizzazioni per i livelli precedenti. L'elenco seguente descrive i quattro livelli di accesso dal livello più basso a quello più alto:

- Visualizzatore: autorizzazione a visualizzare le risorse nelle fattorie, nelle code, nelle flotte e nei posti di lavoro a cui hanno accesso. Un visualizzatore non può inviare o apportare modifiche ai lavori.
- Collaboratore: identico a un visualizzatore, ma con il permesso di inviare lavori a una coda o a una fattoria.
- Responsabile: identico al collaboratore, ma con il permesso di modificare i lavori in coda a cui ha accesso e concede le autorizzazioni per le risorse a cui ha accesso.
- Proprietario: è uguale al responsabile, ma può visualizzare e creare budget e vederne l'utilizzo.

> **Note**
>
> Queste autorizzazioni non forniscono agli utenti l'accesso AWS Management Console o l'autorizzazione a modificare l'infrastruttura Deadline Cloud.

Gli utenti devono avere accesso a una farm prima di poter accedere alle code e alle flotte associate. L'accesso utente viene assegnato separatamente alle code e alle flotte all'interno di una farm.

È possibile aggiungere utenti come individui o come parte di un gruppo. L'aggiunta di gruppi a una fattoria, a una flotta o a una coda può semplificare la gestione delle autorizzazioni di accesso per grandi gruppi di persone. Ad esempio, se hai un team che sta lavorando a un progetto specifico, puoi aggiungere ogni membro del team a un gruppo. Quindi, puoi concedere le autorizzazioni di accesso all'intero gruppo per la fattoria, la flotta o la coda corrispondente.

Supporto software con Deadline Cloud

Deadline Cloud funziona con qualsiasi applicazione software che può essere eseguita da un'interfaccia a riga di comando e controllata utilizzando i valori dei parametri. Deadline Cloud supporta le OpenJD specifiche per descrivere il lavoro come un lavoro con istruzioni di script software parametrizzate (ad esempio in un intervallo di frame) in attività. Raccogli le istruzioni di OpenJD lavoro in pacchetti di lavoro con gli strumenti e le funzionalità di Deadline Cloud per creare, eseguire e concedere in licenza le fasi da un'applicazione software di terze parti.

Per il rendering dei lavori è necessaria una licenza. Deadline Cloud offre licenze basate sull'utilizzo (UBL) per una selezione di licenze di applicazioni software con fatturazione oraria in incrementi di minuti in base all'utilizzo. Con Deadline Cloud, puoi anche utilizzare le tue licenze software, se lo desideri. Se un lavoro non può accedere a una licenza, non viene visualizzato e produce un errore che viene visualizzato nel registro delle attività nel monitor di Deadline Cloud.

Iniziare con Deadline Cloud

Per creare una farm in AWS Deadline Cloud, puoi utilizzare la console Deadline Cloud o il AWS Command Line Interface ().AWS CLI Usa la console per un'esperienza guidata di creazione della fattoria, comprese code e flotte. Utilizzala AWS CLI per lavorare direttamente con il servizio o per sviluppare strumenti personalizzati compatibili con Deadline Cloud.

Per creare una farm e utilizzare il monitor Deadline Cloud, configura il tuo account per Deadline Cloud. Devi configurare l'infrastruttura di monitoraggio di Deadline Cloud solo una volta per account. Dalla tua fattoria, puoi gestire il tuo progetto, incluso l'accesso degli utenti alla tua fattoria e alle sue risorse.

Per creare una fattoria senza configurare l'infrastruttura di monitoraggio di Deadline Cloud, configura una workstation per sviluppatori per Deadline Cloud.

Per creare una farm con risorse minime per accettare lavori, seleziona Quickstart nella home page della console. Configura il monitor Deadline Cloudti guida attraverso questi passaggi. Queste fattorie iniziano con una coda e una flotta che vengono associate automaticamente. Questo approccio è un modo conveniente per creare fattorie in stile sandbox in cui sperimentare.

Argomenti

- Configurare l'account Account AWS
- Configura il monitor Deadline Cloud
- Configurazione di una workstation per sviluppatori per Deadline Cloud
- Configura i mittenti di Deadline Cloud
- Usa la fattoria

Configurare l'account Account AWS

Configura il tuo Account AWS per utilizzare AWS Deadline Cloud.

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

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.

2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

La prima volta che si crea un account Account AWS, si inizia con un'unica identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità si chiama utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account.

> **Important**
>
> Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Configura il monitor Deadline Cloud

Per iniziare, dovrai creare la tua infrastruttura di monitoraggio Deadline Cloud e definire la tua fattoria. Puoi anche eseguire passaggi aggiuntivi e opzionali, tra cui aggiungere gruppi e utenti, scegliere un ruolo di servizio e aggiungere tag alle tue risorse.

Passaggio 1: configura il monitor

Il monitor Deadline Cloud viene utilizzato AWS IAM Identity Center per autorizzare gli utenti. L'istanza IAM Identity Center che utilizzi per Deadline Cloud deve trovarsi nella Regione AWS stessa del monitor. Se la tua console utilizza una regione diversa quando crei il monitor, riceverai un promemoria per passare alla regione IAM Identity Center.

L'infrastruttura del monitor è composta dai seguenti componenti:

- Nome visualizzato del monitor: il nome visualizzato del monitor consente di identificare il monitor, ad esempio AnyCompany monitor. Il nome del monitor determina anche l'URL del monitor.

> **Important**
>
> Non è possibile modificare il nome visualizzato sul monitor dopo aver terminato la configurazione.

- URL del monitor: puoi accedere al monitor utilizzando l'URL del monitor. L'URL si basa sul nome visualizzato sul Monitor, ad esempio https://anycompanymonitor.awsapps.com.

> **Important**
>
> Non puoi modificare l'URL del monitor dopo aver terminato la configurazione.

- Regione AWS: Regione AWSè la posizione fisica per un insieme di data AWS center. Quando configuri il monitor, per impostazione predefinita la Regione è la posizione più vicina a te. Ti consigliamo di cambiare la regione in modo che sia più vicina ai tuoi utenti. Ciò riduce il ritardo e migliora la velocità di trasferimento dei dati. AWS IAM Identity Center deve essere abilitato Regione AWS come Deadline Cloud.

> **Important**
>
> Non puoi cambiare la tua regione dopo aver completato la configurazione di Deadline Cloud.

Completa le attività in questa sezione per configurare l'infrastruttura del monitor.

Per configurare l'infrastruttura del monitor

1. Accedi a per avviare la configurazione AWS Management Consoledi Welcome to Deadline Cloud, quindi scegli Avanti.
2. Inserisci il nome visualizzato sul Monitor, ad esempio**`AnyCompany Monitor`**.
3. (Facoltativo) Per modificare il nome del monitor, scegliete Modifica URL.
4. (Facoltativo) Per modificarlo Regione AWSin modo che sia più vicino ai tuoi utenti, scegli Cambia regione.

a. Seleziona la regione più vicina ai tuoi utenti.
b. Scegli Applica regione.

- (Facoltativo) Per aggiungere gruppi e utenti, seleziona (Facoltativo) Aggiungi gruppi e utenti.
- (Facoltativo) Per personalizzare ulteriormente la configurazione del monitor, seleziona Impostazioni aggiuntive.

5. Se sei pronto Fase 2: Definizione dei dettagli dell'azienda, scegli Avanti.

(Facoltativo) Aggiungi gruppi e utenti

Prima di completare la configurazione del monitor di Deadline Cloud, puoi aggiungere gli utenti del monitor e aggiungerli a un gruppo.

Una volta completata la configurazione, puoi creare nuovi utenti e gruppi e gestire gli utenti, ad esempio assegnando loro gruppi, autorizzazioni e applicazioni o eliminando utenti dal monitor.

Impostazioni aggiuntive

La configurazione di Deadline Cloud include impostazioni aggiuntive. Con queste impostazioni, puoi visualizzare tutte le modifiche apportate dalla configurazione di Deadline Cloud al tuo Account AWS, configurare il ruolo dell'utente di monitoraggio e modificare il tipo di chiave di crittografia.

AWS IAM Identity Center

AWS IAM Identity Center è un servizio Single Sign-On basato sul cloud per la gestione di utenti e gruppi. IAM Identity Center può anche essere integrato con il tuo provider Single Sign-On (SSO) aziendale in modo che gli utenti possano accedere con il proprio account aziendale.

Deadline Cloud abilita IAM Identity Center per impostazione predefinita ed è necessario per configurare e utilizzare Deadline Cloud. L'istanza IAM Identity Center che utilizzi per Deadline Cloud deve trovarsi nella Regione AWS stessa del monitor. Per ulteriori informazioni, consulta What is AWS IAM Identity Center.

Configurare il ruolo di accesso al servizio

Un AWS servizio può assumere un ruolo di servizio per eseguire azioni per conto dell'utente. Deadline Cloud richiede un ruolo di utente di monitoraggio per consentire agli utenti di accedere alle risorse del monitor.

Puoi allegare policy gestite AWS Identity and Access Management (IAM) al ruolo utente di monitoraggio. Le policy consentono agli utenti di eseguire determinate azioni, come la creazione di lavori in una specifica applicazione Deadline Cloud. Poiché le applicazioni dipendono da condizioni specifiche della policy gestita, se non si utilizzano le politiche gestite, l'applicazione potrebbe non funzionare come previsto.

È possibile modificare il ruolo dell'utente di monitoraggio dopo aver completato la configurazione, in qualsiasi momento. Per ulteriori informazioni sui ruoli utente, consulta IAM Roles.

Le seguenti schede contengono istruzioni per due diversi casi d'uso. Per creare e utilizzare un nuovo ruolo di servizio, scegli la scheda Nuovo ruolo di servizio. Per utilizzare un ruolo di servizio esistente, scegli la scheda Ruolo di servizio esistente.

New service role

Per creare e utilizzare un nuovo ruolo di servizio

1. Seleziona Crea e utilizza un nuovo ruolo di servizio.
2. (Facoltativo) Inserisci il nome del ruolo utente del servizio.
3. Scegli Visualizza i dettagli delle autorizzazioni per ulteriori informazioni sul ruolo.

Existing service role

Per utilizzare un ruolo di servizio esistente

1. Seleziona Usa un ruolo di servizio esistente.
2. Apri l'elenco a discesa per scegliere un ruolo di servizio esistente.
3. (Facoltativo) Scegli Visualizza nella console IAM per ulteriori informazioni sul ruolo.

Fase 2: Definizione dei dettagli dell'azienda

Tornando alla console Deadline Cloud, completa i seguenti passaggi per definire i dettagli della fattoria.

1. Nei dettagli della fattoria, aggiungi un nome per la fattoria.
2. Per Descrizione, inserisci la descrizione dell'azienda. Una descrizione chiara può aiutarti a identificare rapidamente lo scopo della tua azienda.

3. (Facoltativo) Per impostazione predefinita, i tuoi dati sono crittografati con una chiave che AWS possiede e gestisce per la tua sicurezza. Puoi scegliere Personalizza le impostazioni di crittografia (avanzate) per utilizzare una chiave esistente o per crearne una nuova da gestire.

   Se scegli di personalizzare le impostazioni di crittografia utilizzando la casella di controllo, inserisci un AWS KMS ARN o creane uno AWS KMS nuovo scegliendo Crea nuova chiave KMS.
4. (Facoltativo) Scegli Aggiungi nuovo tag per aggiungere uno o più tag alla tua fattoria.
5. Selezionare una delle seguenti opzioni:

   - Seleziona Salta alla revisione e Crea per rivedere e creare la tua fattoria.
   - Seleziona Avanti per procedere con ulteriori passaggi opzionali.

(Facoltativo) Fase 3: Definizione dei dettagli della coda

La coda è responsabile del monitoraggio dei progressi e della pianificazione del lavoro per i lavori.

1. A partire dai dettagli della coda, fornisci un nome per la coda.
2. In Descrizione, inserisci la descrizione della coda. Una descrizione chiara può aiutarti a identificare rapidamente lo scopo della coda.
3. Per gli allegati Job, puoi creare un nuovo bucket Amazon S3 o scegliere un bucket Amazon S3 esistente. Se non disponi di un bucket Amazon S3 esistente, dovrai crearne uno.

   a. Per creare un nuovo bucket Amazon S3, seleziona Crea nuovo bucket di lavoro. Puoi definire il nome del job bucket nel campo del prefisso Root. Ti consigliamo di chiamare il bucket. **`deadlinecloud-job-attachments-[MONITORNAME]`**

      Puoi usare solo lettere minuscole e trattini. Niente spazi o caratteri speciali.

   b. Per cercare e selezionare un bucket Amazon S3 esistente, seleziona Scegli dal bucket Amazon S3 esistente. Quindi, cerca un bucket esistente scegliendo Browse S3. Quando viene visualizzato l'elenco dei bucket Amazon S3 disponibili, seleziona il bucket Amazon S3 che desideri utilizzare per la coda.
4. Se utilizzi flotte gestite dal cliente, seleziona Abilita l'associazione con flotte gestite dal cliente.

   - Per le flotte gestite dal cliente, aggiungi un utente configurato per la coda, quindi imposta le credenziali POSIX e/o Windows. In alternativa, puoi ignorare la funzionalità run-as selezionando la casella di controllo.

5. La coda richiede l'autorizzazione per accedere ad Amazon S3 per tuo conto. Ti consigliamo di creare un nuovo ruolo di servizio per ogni coda.

   a. Per un nuovo ruolo, completa i passaggi seguenti.

      i. Seleziona Crea e utilizza un nuovo ruolo di servizio.

      ii. Inserisci un nome di ruolo per il tuo ruolo in coda o usa il nome del ruolo fornito.

      iii. (Facoltativo) Aggiungi una descrizione del ruolo in coda.

      iv. Puoi visualizzare le autorizzazioni IAM per il ruolo di coda scegliendo Visualizza i dettagli delle autorizzazioni.

   b. In alternativa, puoi scegliere un ruolo di servizio esistente.

6. (Facoltativo) Aggiungi variabili di ambiente per l'ambiente di coda utilizzando coppie di nomi e valori.

7. (Facoltativo) Aggiungi tag per la coda utilizzando coppie di chiavi e valori.

Dopo aver inserito tutti i dettagli della coda, seleziona Avanti.

(Facoltativo) Fase 4: Definizione dei dettagli della flotta

Una flotta assegna i lavoratori per eseguire le attività di rendering. Se hai bisogno di una flotta per le tue attività di rendering, seleziona la casella Crea flotta.

1. Dettagli della flotta

   a. Fornisci sia un nome che una descrizione opzionale per la tua flotta.

   b. Seleziona il modo in cui le tue risorse di calcolo devono essere scalate. L'opzione Service-managed consente a Deadline Cloud di scalare automaticamente le risorse di elaborazione. L'opzione Customer-managed ti lascia il controllo della tua scalabilità di elaborazione.

2. Nella sezione dell'opzione Istanza, scegli Spot o On-demand. Le istanze On-demand di Amazon EC2 offrono una disponibilità più rapida e le istanze Spot di Amazon EC2 sono migliori per ridurre i costi.

3. Per la scalabilità automatica del numero di istanze del tuo parco istanze, scegli sia un numero minimo di istanze che un numero massimo di istanze.

   Ti consigliamo vivamente di impostare sempre il numero minimo di istanze per **0** evitare costi aggiuntivi.

4. La tua flotta richiede l'autorizzazione a scrivere a CloudWatch tuo nome. Ti consigliamo di creare un nuovo ruolo di servizio per ogni flotta.

   a. Per un nuovo ruolo, completa i passaggi seguenti.

      i. Seleziona Crea e utilizza un nuovo ruolo di servizio.

      ii. Inserisci un nome di ruolo per il ruolo del tuo parco veicoli o utilizza il nome del ruolo fornito.

      iii. (Facoltativo) Aggiungi una descrizione del ruolo della flotta.

      iv. Puoi visualizzare le autorizzazioni IAM per il ruolo della flotta scegliendo Visualizza i dettagli delle autorizzazioni.

   b. In alternativa, puoi utilizzare un ruolo di servizio esistente.

5. (Facoltativo) Aggiungi tag per la flotta utilizzando coppie di chiavi e valori.

Dopo aver inserito tutti i dettagli della flotta, seleziona Avanti.

(Facoltativo) Fase 5: Configurazione dei requisiti dei lavoratori

Definisci i requisiti per le tue istanze di lavoro.

1. Esamina le impostazioni del sistema operativo (OS) e dell'architettura della CPU per maggiori informazioni.
2. Aggiorna il numero minimo e massimo di vCPU per i tuoi requisiti hardware.
3. Aggiorna il numero minimo e massimo di memoria (GiB) per i tuoi requisiti hardware.
4. È possibile filtrare i tipi di istanze consentendo o escludendo i tipi di istanze di lavoro. In entrambe le opzioni di filtro, puoi filtrare fino a 10 tipi di istanze Amazon EC2.
5. In Requisiti aggiuntivi (facoltativi), puoi definire il volume EBS principale per dimensione (GiB), IOPS e velocità effettiva (MiB/s).
6. Dopo aver impostato tutti i requisiti dei lavoratori, scegli Avanti per definire il livello di accesso dei tuoi gruppi.

(Facoltativo) Fase 6: Definizione dei livelli di accesso

Se hai gruppi collegati al monitor, puoi definirne il livello di accesso. L'autorizzazione all'uso delle funzionalità di Deadline Cloud è gestita in base ai livelli di accesso. Puoi assegnare diversi livelli di accesso a gruppi di utenti.

1. Utilizza il menu del livello di accesso della farm Deadline Cloud per selezionare il livello di autorizzazione per il gruppo.
2. Scegli Avanti per continuare e rivedere tutti i dettagli della fattoria inseriti.

Passaggio 7: rivedi e crea

Controlla tutte le informazioni inserite per creare la tua fattoria. Quando sei pronto, scegli Crea fattoria.

Lo stato di avanzamento della creazione della tua fattoria viene visualizzato nella pagina Fattorie. Quando la fattoria è pronta per l'uso, viene visualizzato un messaggio di successo.

Configurazione di una workstation per sviluppatori per Deadline Cloud

In questo tutorial, lo utilizzerai AWS CloudShell per creare una semplice farm per sviluppatori ed eseguire il worker agent. Potrai quindi inviare ed eseguire un semplice lavoro con parametri e allegati, aggiungere una flotta gestita dai servizi e ripulire le risorse della fattoria quando hai finito.

Le sezioni seguenti ti introducono alle diverse funzionalità di Deadline Cloud e al modo in cui funzionano e interagiscono. Seguire questi passaggi è utile per sviluppare e testare nuovi carichi di lavoro e personalizzazioni.

Argomenti

Passaggio 1: creare una cloud farm di Deadline

Per creare la tua farm per sviluppatori e le risorse in coda in AWS Deadline Cloud, usa AWS Command Line Interface (AWS CLI), come mostrato nella procedura seguente. Inoltre, creerai un ruolo AWS Identity and Access Management (IAM) e una flotta gestita dai clienti (CMF) e assocerai la

flotta alla tua coda. Quindi puoi configurare AWS CLI e confermare che la tua farm sia configurata e funzioni come specificato.

Puoi utilizzare questa farm per esplorare le funzionalità di Deadline Cloud, quindi sviluppare e testare nuovi carichi di lavoro, personalizzazioni e integrazioni di pipeline.

Per creare una fattoria

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Crea un nome per la tua fattoria e aggiungi il nome della fattoria a`~/.bashrc`. In questo modo sarà disponibile per altre sessioni terminali.

   ```
   echo "DEV_FARM_NAME=DeveloperFarm" >> ~/.bashrc
   source ~/.bashrc
   ```

3. Crea la risorsa della fattoria e aggiungi il relativo ID della fattoria a`~/.bashrc`.

   ```
   aws deadline create-farm \
       --display-name "$DEV_FARM_NAME"

   echo "DEV_FARM_ID=\$(aws deadline list-farms \
           --query \"farms[?displayName=='\$DEV_FARM_NAME'].farmId \
           | [0]\" --output text)" >> ~/.bashrc
   source ~/.bashrc
   ```

4. Crea la risorsa della coda e aggiungi il relativo ID di coda a `~/.bashrc.`

   ```
   aws deadline create-queue \
       --farm-id $DEV_FARM_ID \
       --display-name "$DEV_FARM_NAME Queue" \
       --job-run-as-user '{"posix": {"user": "job-user", "group": "job-group"},
    "runAs":"QUEUE_CONFIGURED_USER"}'

   echo "DEV_QUEUE_ID=\$(aws deadline list-queues \
           --farm-id \$DEV_FARM_ID \
           --query \"queues[?displayName=='\$DEV_FARM_NAME Queue'].queueId \
           | [0]\" --output text)" >> ~/.bashrc
   source ~/.bashrc
   ```

5. Crea un ruolo IAM per la flotta. Questo ruolo fornisce agli host dei lavoratori del tuo parco macchine le credenziali di sicurezza necessarie per eseguire i lavori dalla tua coda.

```
aws iam create-role \
    --role-name "${DEV_FARM_NAME}FleetRole" \
    --assume-role-policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "credentials.deadline.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }'
aws iam put-role-policy \
    --role-name "${DEV_FARM_NAME}FleetRole" \
    --policy-name WorkerPermissions \
    --policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "deadline:AssumeFleetRoleForWorker",
                        "deadline:UpdateWorker",
                        "deadline:DeleteWorker",
                        "deadline:UpdateWorkerSchedule",
                        "deadline:BatchGetJobEntity",
                        "deadline:AssumeQueueRoleForWorker"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:PrincipalAccount": "${aws:ResourceAccount}"
                        }
                    }
                },
                {
                    "Effect": "Allow",
                    "Action": [
                        "logs:CreateLogStream"
```

```
                ],
                "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
                "Condition": {
                    "StringEquals": {
                        "aws:PrincipalAccount": "${aws:ResourceAccount}"
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "logs:PutLogEvents",
                    "logs:GetLogEvents"
                ],
                "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
                "Condition": {
                    "StringEquals": {
                        "aws:PrincipalAccount": "${aws:ResourceAccount}"
                    }
                }
            }
        ]
    }'
```

6. Crea la flotta gestita dal cliente (CMF) e aggiungi il relativo ID della flotta a. `~/.bashrc`

```
FLEET_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
        --query "Account" --output text):role/${DEV_FARM_NAME}FleetRole"
aws deadline create-fleet \
    --farm-id $DEV_FARM_ID \
    --display-name "$DEV_FARM_NAME CMF" \
    --role-arn $FLEET_ROLE_ARN \
    --max-worker-count 5 \
    --configuration \
        '{
            "customerManaged": {
                "mode": "NO_SCALING",
                "workerCapabilities": {
                    "vCpuCount": {"min": 1},
                    "memoryMiB": {"min": 512},
                    "osFamily": "linux",
                    "cpuArchitectureType": "x86_64"
                }
            }
```

```
        }'

echo "DEV_CMF_ID=\$(aws deadline list-fleets \
        --farm-id \$DEV_FARM_ID \
        --query \"fleets[?displayName=='\$DEV_FARM_NAME CMF'].fleetId \
        | [0]\" --output text)" >> ~/.bashrc
source ~/.bashrc
```

7. Assicurati di poter accedere a Deadline Cloud.

```
pip install deadline
```

8. Associa il CMF alla tua coda.

```
aws deadline create-queue-fleet-association \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --fleet-id $DEV_CMF_ID
```

9. Per impostare la farm predefinita sull'ID della fattoria e la coda sull'ID della coda creato in precedenza, utilizzate il comando seguente.

```
deadline config set defaults.farm_id $DEV_FARM_ID
deadline config set defaults.queue_id $DEV_QUEUE_ID
```

10. (Facoltativo) Per confermare che la fattoria è configurata in base alle specifiche, utilizzate i seguenti comandi:

    - Elenca tutte le fattorie — **`deadline farm list`**
    - Elenca tutte le code nella farm predefinita: **`deadline queue list`**
    - Elenca tutte le flotte nella fattoria predefinita: **`deadline fleet list`**
    - Ottieni la fattoria predefinita: **`deadline farm get`**
    - Ottieni la coda predefinita: **`deadline queue get`**
    - Ottieni tutte le flotte associate alla coda predefinita: **`deadline fleet get`**

Passaggio 2: esegui l'agente di lavoro in modalità sviluppatore in Deadline Cloud

Prima di poter eseguire i lavori che invii alla coda nella tua farm di sviluppatori, devi eseguire il worker agent di AWS Deadline Cloud in modalità sviluppatore su un worker host.

Nel resto di questo tutorial, eseguirai AWS CLI operazioni sulla tua farm di sviluppatori utilizzando due schede. AWS CloudShell Nella prima scheda, puoi inviare offerte di lavoro. Nella seconda scheda, puoi eseguire l'agente di lavoro.

> **Note**
>
> Se lasci la CloudShell sessione inattiva per più di 20 minuti, scatterà il timeout e interromperà l'agente di lavoro. Per riavviare l'agente di lavoro, segui le istruzioni nella procedura seguente.

Per eseguire l'agente di lavoro in modalità sviluppatore

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Con la fattoria ancora aperta nella prima CloudShell scheda, apri una seconda CloudShell scheda, quindi crea le `demoenv-persist` cartelle `demoenv-logs` e.

   ```
   mkdir ~/demoenv-logs
   mkdir ~/demoenv-persist
   ```

3. Scarica e installa i pacchetti Deadline Cloud worker agent da PyPI:

   > **Note**
   >
   > SìWindows, è necessario che i file dell'agente siano installati nella directory globale dei pacchetti del sito di Python. Gli ambienti virtuali Python non sono attualmente supportati.

   ```
   python -m pip install deadline-cloud-worker-agent
   ```

4. Per consentire all'agente di lavoro di creare le directory temporanee per i lavori in esecuzione, crea una directory:

```
sudo mkdir /sessions
sudo chmod 750 /sessions
sudo chown cloudshell-user /sessions
```

5. Esegui il worker agent Deadline Cloud in modalità sviluppatore con `DEV_FARM_ID` le variabili `DEV_CMF_ID` che hai aggiunto a. `~/.bashrc`

```
deadline-worker-agent \
    --farm-id $DEV_FARM_ID \
    --fleet-id $DEV_CMF_ID \
    --run-jobs-as-agent-user \
    --logs-dir ~/demoenv-logs \
    --persistence-dir ~/demoenv-persist
```

Quando l'agente di lavoro inizializza e quindi esegue il polling del funzionamento dell'`UpdateWorkerSchedule`API, viene visualizzato il seguente output:

```
INFO    Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] # Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] AgentInfo
Python Interpreter: /usr/bin/python3
Python Version: 3.9.16 (main, Sep  8 2023, 00:00:00)  - [GCC 11.4.1 20230605 (Red
 Hat 11.4.1-2)]
Platform: linux
...
[2024-03-27 15:51:02,528][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params={'assignedSessions': {}, 'cancelSessionActions': {},
 'updateIntervalSeconds': 15} ...
[2024-03-27 15:51:17,635][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
[2024-03-27 15:51:32,756][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
...
```

6. Seleziona la prima CloudShell scheda, quindi elenca i lavoratori della flotta.

```
deadline worker list --fleet-id $DEV_CMF_ID
```

Viene visualizzato un output come il seguente:

```
Displaying 1 of 1 workers starting at 0

- workerId: worker-8c9af877c8734e89914047111f
  status: STARTED
  createdAt: 2023-12-13 20:43:06+00:00
```

In una configurazione di produzione, il worker agent di Deadline Cloud richiede la configurazione di più utenti e directory di configurazione come utente amministrativo sulla macchina host. Puoi ignorare queste impostazioni perché stai eseguendo lavori nella tua farm di sviluppo, a cui solo tu puoi accedere.

Passaggio 3: invia ed esegui lavori con Deadline Cloud

Per utilizzare AWS Deadline Cloud per eseguire lavori, utilizza le seguenti procedure. Usa la prima AWS CloudShell scheda per inviare lavori alla tua farm di sviluppatori. Usa la seconda CloudShell scheda per visualizzare l'output del worker agent.

Argomenti

- Invia il simple_job campione
- Invia un messaggio simple_job con un parametro
- Crea un pacchetto di job simple_file_job con file I/O

Invia il simple_job campione

Dopo aver creato una fattoria e aver avviato l'agente operaio, puoi inviare il simple_job campione a Deadline Cloud.

Per inviare il simple_job campione a Deadline Cloud

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Scarica l'esempio da GitHub.

```
cd ~
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
```

3. Scegli la tua prima CloudShell scheda, quindi vai alla directory degli esempi del job bundle.

```
cd ~/deadline-cloud-samples/job_bundles/
```

4. Invia il simple_job campione.

```
deadline bundle submit simple_job
```

5. Scegli la seconda CloudShell scheda per visualizzare l'output di registrazione relativo alle chiamate`BatchGetJobEntities`, all'attivazione di una sessione e all'esecuzione di un'azione di sessione.

```
...
[2024-03-27 16:00:21,846][INFO    ] # Session.Starting
 # [session-053d77cef82648fe2] Starting new Session.
 [queue-3ba4ff683ff54db09b851a2ed8327d7b/job-d34cc98a6e234b6f82577940ab4f76c6]
[2024-03-27 16:00:21,853][INFO    ] # API.Req # [deadline:BatchGetJobEntity]
 resource={'farm-id': 'farm-3e24cfc9bbcd423e9c1b6754bc1',
 'fleet-id': 'fleet-246ee60f46d44559b6cce010d05', 'worker-id':
 'worker-75e0fce9c3c344a69bff57fcd83'} params={'identifiers': [{'jobDetails':
 {'jobId': 'job-d34cc98a6e234b6f82577940ab4'}}]} request_url=https://
scheduling.deadline.us-west-2.amazonaws.com/2023-10-12/farms/
farm-3e24cfc9bbcd423e /fleets/fleet-246ee60f46d44559b1 /workers/worker-
 75e0fce9c3c344a69b /batchGetJobEntity
[2024-03-27 16:00:22,013][INFO    ] # API.Resp # [deadline:BatchGetJobEntity](200)
 params={'entities': [{'jobDetails': {'jobId': 'job-d34cc98a6e234b6f82577940ab6',
 'jobRunAsUser': {'posix': {'user': 'job-user', 'group': 'job-group'},
 'runAs': 'QUEUE_CONFIGURED_USER'}, 'logGroupName': '/aws/deadline/
farm-3e24cfc9bbcd423e9c1b6754bc1/queue-3ba4ff683ff54db09b851a2ed83', 'parameters':
 '*REDACTED*', 'schemaVersion': 'jobtemplate-2023-09'}}], 'errors': []}
 request_id=a3f55914-6470-439e-89e5-313f0c6
[2024-03-27 16:00:22,013][INFO    ] # Session.Add #
 [session-053d77cef82648fea9c69827182] Appended new SessionActions.
 (ActionIds: ['sessionaction-053d77cef82648fea9c69827182-0'])
 [queue-3ba4ff683ff54db09b851a2ed8b/job-d34cc98a6e234b6f82577940ab6]
[2024-03-27 16:00:22,014][WARNING ] # Session.User #
 [session-053d77cef82648fea9c69827182] Running as the Worker Agent's
 user. (User: cloudshell-user) [queue-3ba4ff683ff54db09b851a2ed8b/job-
d34cc98a6e234b6f82577940ac6]
[2024-03-27 16:00:22,015][WARNING ] # Session.AWSCreds #
 [session-053d77cef82648fea9c69827182] AWS Credentials are not available: Queue has
 no IAM Role. [queue-3ba4ff683ff54db09b851a2ed8b/job-d34cc98a6e234b6f82577940ab6]
[2024-03-27 16:00:22,026][INFO    ] # Session.Logs #
 [session-053d77cef82648fea9c69827182] Logs streamed to: AWS CloudWatch
```

```
 Logs. (LogDestination: /aws/deadline/farm-3e24cfc9bbcd423e9c1b6754bc1/
queue-3ba4ff683ff54db09b851a2ed83/session-053d77cef82648fea9c69827181)
 [queue-3ba4ff683ff54db09b851a2ed83/job-d34cc98a6e234b6f82577940ab4]
[2024-03-27 16:00:22,026][INFO    ] # Session.Logs #
 [session-053d77cef82648fea9c69827182] Logs streamed to: local
 file. (LogDestination: /home/cloudshell-user/demoenv-logs/
queue-3ba4ff683ff54db09b851a2ed8b/session-053d77cef82648fea9c69827182.log)
 [queue-3ba4ff683ff54db09b851a2ed83/job-d34cc98a6e234b6f82577940ab4]
...
```

> **Note**
>
> Viene mostrato solo l'output di registrazione del worker agent. Esiste un registro separato per la sessione che esegue il lavoro.

6. Scegli la tua prima scheda, quindi controlla i file di registro scritti dal worker agent.

   a. Passa alla directory dei registri del worker agent e visualizzane il contenuto.

   ```
   cd ~/demoenv-logs
   ls
   ```

   b. Stampa il primo file di registro creato dal worker agent.

   ```
   cat worker-agent-bootstrap.log
   ```

   Questo file contiene l'output dell'agente di lavoro su come ha chiamato l'API Deadline Cloud per creare una risorsa worker nel parco macchine e poi ha assunto il ruolo del parco macchine.

   c. Stampa l'output del file di registro quando l'agente lavoratore si unisce alla flotta.

   ```
   cat worker-agent.log
   ```

   Questo registro contiene output su tutte le azioni intraprese dall'agente di lavoro, ma non contiene output sulle code da cui esegue i lavori, ad eccezione degli ID di tali risorse.

   d. Stampa i file di registro per ogni sessione in una directory con lo stesso nome dell'id della risorsa della coda.

```
cat $DEV_QUEUE_ID/session-*.log
```

Se il processo ha esito positivo, l'output del file di registro sarà simile al seguente:

```
 cat $DEV_QUEUE_ID/$(ls -t $DEV_QUEUE_ID | head -1)
2024-03-27 16:00:22,026 WARNING Session running with no AWS Credentials.
2024-03-27 16:00:22,404 INFO
2024-03-27 16:00:22,405 INFO ================================================
2024-03-27 16:00:22,405 INFO --------- Running Task
2024-03-27 16:00:22,405 INFO ================================================
2024-03-27 16:00:22,406 INFO ------------------------------------------------
2024-03-27 16:00:22,406 INFO Phase: Setup
2024-03-27 16:00:22,406 INFO ------------------------------------------------
2024-03-27 16:00:22,406 INFO Writing embedded files for Task to disk.
2024-03-27 16:00:22,406 INFO Mapping: Task.File.runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,406 INFO Wrote: runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,407 INFO ------------------------------------------------
2024-03-27 16:00:22,407 INFO Phase: Running action
2024-03-27 16:00:22,407 INFO ------------------------------------------------
2024-03-27 16:00:22,407 INFO Running command /sessions/
session-053d77cef82648fea9c698271812a/tmpzuzxpslm.sh
2024-03-27 16:00:22,414 INFO Command started as pid: 471
2024-03-27 16:00:22,415 INFO Output:
2024-03-27 16:00:22,420 INFO Welcome to AWS Deadline Cloud!
2024-03-27 16:00:22,571 INFO
2024-03-27 16:00:22,572 INFO ================================================
2024-03-27 16:00:22,572 INFO --------- Session Cleanup
2024-03-27 16:00:22,572 INFO ================================================
2024-03-27 16:00:22,572 INFO Deleting working directory: /sessions/
session-053d77cef82648fea9c698271812a
```

7. Stampa le informazioni sul lavoro.

```
deadline job get
```

Quando inviate il lavoro, il sistema lo salva come predefinito in modo da non dover inserire l'ID del lavoro.

Invia un messaggio simple_job con un parametro

Puoi inviare lavori con parametri. Nella procedura seguente, si modifica il simple_job modello per includere un messaggio personalizzato, si invia il file di registro della simple_job sessione e si stampa il file di registro della sessione per visualizzare il messaggio.

Per inviare l'simple_jobesempio con un parametro

1. Seleziona la tua prima CloudShell scheda, quindi vai alla directory degli esempi di job bundle.

   ```
   cd ~/deadline-cloud-samples/job_bundles/
   ```

2. Stampa il contenuto del simple_job modello.

   ```
   cat simple_job/template.yaml
   ```

   La `parameterDefinitions` sezione con il `Message` parametro dovrebbe avere l'aspetto seguente:

   ```
   parameterDefinitions:
   - name: Message
     type: STRING
     default: Welcome to AWS Deadline Cloud!
   ```

3. Inviate l'simple_jobesempio con un valore di parametro, quindi attendete che il processo finisca di funzionare.

   ```
   deadline bundle submit simple_job \
       -p "Message=Greetings from the developer getting started guide."
   ```

4. Per visualizzare il messaggio personalizzato, visualizza il file di registro della sessione più recente.

   ```
   cd ~/demoenv-logs
   cat $DEV_QUEUE_ID/$(ls -t $DEV_QUEUE_ID | head -1)
   ```

Crea un pacchetto di job simple_file_job con file I/O

Un lavoro di rendering deve leggere la definizione della scena, renderizzare un'immagine a partire da essa e quindi salvare l'immagine in un file di output. È possibile simulare questa azione facendo in modo che il job calcoli l'hash dell'input anziché renderizzare un'immagine.

Per creare un pacchetto di lavoro simple_file_job con file I/O

1. Seleziona la prima CloudShell scheda, quindi vai alla directory degli esempi di job bundle.

```
cd ~/deadline-cloud-samples/job_bundles/
```

2. Crea una copia `simple_job` con il nuovo nome`simple_file_job`.

```
cp -r simple_job simple_file_job
```

3. Modifica il modello di lavoro come segue:

> **Note**
>
> Ti consigliamo di utilizzarlo nano per questi passaggi. Se si preferisce utilizzareVim, è necessario impostarne la modalità di incolla utilizzando`:set paste`.

   a. Apri il modello in un editor di testo.

```
nano simple_file_job/template.yaml
```

   b. Aggiungi quanto segue `type`e `objectType`, e `dataFlow`e `parameterDefinitions`.

```
- name: InFile
  type: PATH
  objectType: FILE
  dataFlow: IN
- name: OutFile
  type: PATH
  objectType: FILE
  dataFlow: OUT
```

   c. Aggiungere il seguente comando di `bash` script alla fine del file che legge dal file di input e scrive nel file di output.

```
        # hash the input file, and write that to the output
        sha256sum "{{Param.InFile}}" > "{{Param.OutFile}}"
```

L'aggiornamento `template.yaml` dovrebbe corrispondere esattamente a quanto segue:

```
specificationVersion: 'jobtemplate-2023-09'
name: Simple File Job Bundle Example
parameterDefinitions:
- name: Message
  type: STRING
  default: Welcome to AWS Deadline Cloud!
- name: InFile
  type: PATH
  objectType: FILE
  dataFlow: IN
- name: OutFile
  type: PATH
  objectType: FILE
  dataFlow: OUT
steps:
- name: WelcomeToDeadlineCloud
  script:
    actions:
      onRun:
        command: '{{Task.File.runScript}}'
    embeddedFiles:
    - name: runScript
      type: TEXT
      runnable: true
      data: |
        #!/usr/bin/env bash
        echo "{{Param.Message}}"

        # hash the input file, and write that to the output
        sha256sum "{{Param.InFile}}" > "{{Param.OutFile}}"
```

> **Note**
>
> Se desideri regolare la spaziatura in`template.yaml`, assicurati di utilizzare spazi anziché rientri.

d. Salvate il file e uscite dall'editor di testo.

4. Fornite i valori dei parametri per i file di input e output per inviare il simple_file_job.

```
deadline bundle submit simple_file_job \
    -p "InFile=simple_job/template.yaml" \
    -p "OutFile=hash.txt"
```

5. Stampa le informazioni sul lavoro.

```
deadline job get
```

- Verrà visualizzato un output come il seguente:

```
parameters:
  Message:
    string: Welcome to AWS Deadline Cloud!
  InFile:
    path: /local/home/cloudshell-user/BundleFiles/JobBundle-Examples/simple_job/
template.yaml
  OutFile:
    path: /local/home/cloudshell-user/BundleFiles/JobBundle-Examples/hash.txt
```

- Sebbene abbiate fornito solo percorsi relativi, per i parametri è impostato il percorso completo. AWS CLI Unisce la directory di lavoro corrente a tutti i percorsi forniti come parametri quando i percorsi hanno il tipoPATH.
- L'agente di lavoro in esecuzione nell'altra finestra del terminale rileva ed esegue il lavoro. Questa azione crea il `hash.txt` file, che è possibile visualizzare con il seguente comando.

```
cat hash.txt
```

Questo comando stamperà un output simile al seguente.

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3 /local/home/
cloudshell-user/BundleFiles/JobBundle-Examples/simple_job/template.yaml
```

Passaggio 4: Esegui lavori con allegati di lavoro in Deadline Cloud

Molte farm utilizzano file system condivisi per condividere file tra gli host che inviano i lavori e quelli che eseguono i lavori. Ad esempio, nell'`simple_file_job`esempio precedente, il file system locale è condiviso tra le finestre del AWS CloudShell terminale, che vengono eseguite nella scheda uno in cui si invia il lavoro, e nella scheda due in cui si esegue il worker agent.

Un file system condiviso è vantaggioso quando la postazione di lavoro del mittente e gli host del lavoratore si trovano sulla stessa rete locale. Se memorizzi i dati in locale vicino alle workstation che vi accedono, l'utilizzo di una farm basata sul cloud significa dover condividere i file system tramite una VPN ad alta latenza o sincronizzare i file system nel cloud. Nessuna di queste opzioni è facile da configurare o utilizzare.

AWS Deadline Cloud offre una soluzione semplice con allegati di lavoro, simili agli allegati delle e-mail. Con gli allegati di lavoro, alleghi dati al tuo lavoro. Deadline Cloud gestisce quindi i dettagli del trasferimento e dell'archiviazione dei dati di lavoro nei bucket Amazon Simple Storage Service (Amazon S3).

I flussi di lavoro per la creazione di contenuti sono spesso iterativi, il che significa che un utente invia lavori con un piccolo sottoinsieme di file modificati. Poiché i bucket Amazon S3 archiviano gli allegati del lavoro in uno storage content-addressable, il nome di ogni oggetto si basa sull'hash dei dati dell'oggetto e il contenuto di un albero di directory viene archiviato in un formato di file manifesto allegato a un lavoro.

Per eseguire lavori con allegati di lavoro, completa i seguenti passaggi.

Argomenti

Aggiungi una configurazione degli allegati di lavoro alla tua coda

Per abilitare gli allegati dei lavori nella tua coda, aggiungi una configurazione degli allegati di lavoro alla risorsa di coda del tuo account.

Per aggiungere una configurazione degli allegati di lavoro alla tua coda

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Scegli la tua prima CloudShell scheda, quindi inserisci uno dei seguenti comandi per utilizzare un bucket Amazon S3 per gli allegati dei lavori.
   - Se non disponi di un bucket Amazon S3 privato esistente, puoi creare e utilizzare un nuovo bucket S3.

     ```
     DEV_FARM_BUCKET=$(echo $DEV_FARM_NAME \
         | tr '[:upper:]' '[:lower:]')-$(xxd -l 16 -p /dev/urandom)
     if [ "$AWS_REGION" == "us-east-1" ]; then LOCATION_CONSTRAINT=
     else LOCATION_CONSTRAINT="--create-bucket-configuration \
         LocationConstraint=${AWS_REGION}"
     fi
     aws s3api create-bucket \
         $LOCATION_CONSTRAINT \
         --acl private \
         --bucket ${DEV_FARM_BUCKET}
     ```

   - Se disponi già di un bucket Amazon S3 privato, puoi utilizzarlo sostituendolo *MY_BUCKET_NAME*con il nome del tuo bucket.

     ```
     DEV_FARM_BUCKET=MY_BUCKET_NAME
     ```

3. Dopo aver creato o scelto il bucket Amazon S3, aggiungi il nome del bucket a per renderlo disponibile `~/.bashrc` per altre sessioni di terminale.

   ```
   echo "DEV_FARM_BUCKET=$DEV_FARM_BUCKET" >> ~/.bashrc
   ```

4. Crea un ruolo AWS Identity and Access Management (IAM) per la coda.

   ```
   aws iam create-role --role-name "${DEV_FARM_NAME}QueueRole" \
       --assume-role-policy-document \
           '{
               "Version": "2012-10-17",
               "Statement": [
                   {
                       "Effect": "Allow",
                       "Principal": {
                           "Service": "credentials.deadline.amazonaws.com"
   ```

```
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }'
aws iam put-role-policy \
    --role-name "${DEV_FARM_NAME}QueueRole" \
    --policy-name S3BucketsAccess \
    --policy-document \
            '{
                "Version": "2012-10-17",
                "Statement": [
                {
                    "Action": [
                        "s3:GetObject*",
                        "s3:GetBucket*",
                        "s3:List*",
                        "s3:DeleteObject*",
                        "s3:PutObject",
                        "s3:PutObjectLegalHold",
                        "s3:PutObjectRetention",
                        "s3:PutObjectTagging",
                        "s3:PutObjectVersionTagging",
                        "s3:Abort*"
                    ],
                    "Resource": [
                        "arn:aws:s3:::'$DEV_FARM_BUCKET'",
                        "arn:aws:s3:::'$DEV_FARM_BUCKET'/*"
                    ],
                    "Effect": "Allow"
                }
            ]
            }'
```

5. Aggiorna la coda per includere le impostazioni degli allegati di lavoro e il ruolo IAM.

```
QUEUE_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
        --query "Account" --output text):role/${DEV_FARM_NAME}QueueRole"
aws deadline update-queue \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --role-arn $QUEUE_ROLE_ARN \
    --job-attachment-settings \
        '{
```

```
            "s3BucketName": "'$DEV_FARM_BUCKET'",
            "rootPrefix": "JobAttachments"
        }'
```

6. Conferma di aver aggiornato la coda.

```
deadline queue get
```

Viene visualizzato un output come il seguente:

```
...
jobAttachmentSettings:
  s3BucketName: DEV_FARM_BUCKET
  rootPrefix: JobAttachments
roleArn: arn:aws:iam::ACCOUNT_NUMBER:role/DeveloperFarmQueueRole
...
```

Invia simple_file_job con allegati di lavoro

Quando utilizzi gli allegati di lavoro, i pacchetti di lavoro devono fornire a Deadline Cloud informazioni sufficienti per determinare il flusso di dati del lavoro, ad esempio l'utilizzo dei parametri. PATH Nel caso disimple_file_job, hai modificato il `template.yaml` file per indicare a Deadline Cloud che il flusso di dati si trova nel file di input e nel file di output.

Dopo aver aggiunto la configurazione degli allegati di lavoro alla coda, puoi inviare l'esempio di simple_file_job con gli allegati del lavoro. Dopo aver eseguito questa operazione, è possibile visualizzare la registrazione e l'output del lavoro per confermare che l'operazione con gli allegati del lavoro funziona. simple_file_job

Per inviare il pacchetto di lavoro simple_file_job con gli allegati del lavoro

1. Scegli la tua prima CloudShell scheda, quindi apri la cartella. `JobBundle-Samples`
2.
```
cd ~/AmazonDeadlineCloud-DocumentationAndSamples/JobBundle-Samples
```
3. Invia simple_file_job alla coda. Quando ti viene richiesto di confermare il caricamento, inserisci. **y**

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```

4. Per visualizzare l'output del registro della sessione di trasferimento dati degli allegati del lavoro, scegliete la seconda CloudShell scheda.

```
JOB_ID=$(deadline config get defaults.job_id)
SESSION_ID=$(aws deadline list-sessions \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --job-id $JOB_ID \
        --query "sessions[0].sessionId" \
        --output text)
cat ~/demoenv-logs/$DEV_QUEUE_ID/$SESSION_ID.log
```

5. Elenca le azioni della sessione che sono state eseguite all'interno della sessione.

```
aws deadline list-session-actions \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --session-id $SESSION_ID
```

Viene mostrato un output come il seguente:

```
{
    "sessionactions": [
        {
            "sessionActionId": "sessionaction-123-0",
            "status": "SUCCEEDED",
            "startedAt": "<timestamp>",
            "endedAt": "<timestamp>",
            "progressPercent": 100.0,
            "definition": {
                "syncInputJobAttachments": {}
            }
        },
        {
            "sessionActionId": "sessionaction-123-1",
            "status": "SUCCEEDED",
            "startedAt": "<timestamp>",
            "endedAt": "<timestamp>",
            "progressPercent": 100.0,
            "definition": {
                "taskRun": {
```

```
                    "taskId": "task-abc-0",
                    "stepId": "step-def"
                }
            }
        }
    ]
}
```

La prima azione della sessione ha scaricato gli allegati del lavoro di input, mentre la seconda azione esegue l'attività come in precedenza e quindi ha caricato gli allegati del lavoro di output.

6. Elenca la directory di output.

```
ls *.txt
```

L'output come `hash.txt` quello è mostrato, ma `hash-jobattachments.txt` non esiste.

7. Scarica l'output del processo più recente.

```
deadline job download-output
```

8. Visualizza l'output del file scaricato.

```
cat hash-jobattachments.txt
```

Viene mostrato un output come il seguente:

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3  /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

Informazioni su come vengono archiviati gli allegati di lavoro in Amazon S3

Puoi utilizzare AWS Command Line Interface (AWS CLI) per caricare o scaricare dati per gli allegati di lavoro, che vengono archiviati nei bucket Amazon S3. Capire come Deadline Cloud archivia gli allegati di lavoro su Amazon S3 ti aiuterà a sviluppare carichi di lavoro e integrazioni di pipeline.

Per controllare come vengono archiviati gli allegati dei lavori di Deadline Cloud in Amazon S3

1. Scegli la tua prima CloudShell scheda, quindi apri la directory degli esempi di job bundle.

```
cd ~/AmazonDeadlineCloud-DocumentationAndSamples/JobBundle-Samples
```

2. Ispeziona le proprietà del lavoro.

```
deadline job get
```

Viene mostrato un output come il seguente:

```
parameters:
  Message:
    string: Welcome to Amazon Deadline Cloud!
  InFile:
    path: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
JobBundle-Samples/simple_job/template.yaml
  OutFile:
    path: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
JobBundle-Samples/hash-jobattachments.txt
attachments:
  manifests:
  - rootPath: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
JobBundle-Samples
    rootPathFormat: posix
    outputRelativeDirectories:
    - .
    inputManifestPath: farm-3040c59a5b9943d58052c29d907a645d/queue-
cde9977c9f4d4018a1d85f3e6c1a4e6e/Inputs/
f46af01ca8904cd8b514586671c79303/0d69cd94523ba617c731f29c019d16e8_input.xxh128
    inputManifestHash: f95ef91b5dab1fc1341b75637fe987ee
  fileSystem: COPIED
```

Il campo degli allegati contiene un elenco di strutture manifeste che descrivono i percorsi dei dati di input e output utilizzati dal job durante l'esecuzione. Guarda `rootPath` per vedere il percorso della directory locale sul computer che ha inviato il lavoro. Per vedere il suffisso dell'oggetto Amazon S3 che contiene un file manifesto, guarda. `inputManifestFile` Il file manifest contiene i metadati per un'istantanea ad albero di directory dei dati di input del processo.

3. Stampa bene l'oggetto manifest di Amazon S3 per vedere la struttura della directory di input per il lavoro.

```
MANIFEST_SUFFIX=$(aws deadline get-job \
```

```
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --query "attachments.manifests[0].inputManifestPath" \
    --output text)
 aws s3 cp s3://$DEV_FARM_BUCKET/JobAttachments/Manifests/$MANIFEST_SUFFIX - | jq .
```

Viene mostrato un output come il seguente:

```
{
    "hashAlg": "xxh128",
    "manifestVersion": "2023-03-03",
    "paths": [
    {
        "hash": "2ec297b04c59c4741ed97ac8fb83080c",
        "mtime": 1698186190000000,
        "path": "simple_job/template.yaml",
        "size": 445
    }
    ],
    "totalSize": 445
 }
```

4. Crea il prefisso Amazon S3 che contiene i manifest per gli allegati del processo di output ed elenca l'oggetto al suo interno.

```
SESSION_ACTION=$(aws deadline list-session-actions \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --session-id $SESSION_ID \
    --query "sessionActions[?definition.taskRun != null] | [0]")
STEP_ID=$(echo $SESSION_ACTION | jq -r .definition.taskRun.stepId)
TASK_ID=$(echo $SESSION_ACTION | jq -r .definition.taskRun.taskId)
TASK_OUTPUT_PREFIX=JobAttachments/Manifests/$DEV_FARM_ID/$DEV_QUEUE_ID/$JOB_ID/
$STEP_ID/$TASK_ID/
aws s3api list-objects-v2 --bucket $DEV_FARM_BUCKET --prefix $TASK_OUTPUT_PREFIX
```

Gli allegati del lavoro di output non sono referenziati direttamente dalla risorsa del lavoro, ma vengono invece inseriti in un bucket Amazon S3 basato sugli ID delle risorse agricole.

5. Ottieni la chiave dell'oggetto manifesto più recente per l'ID di azione della sessione specifica, quindi stampa in modo semplice gli oggetti del manifesto.

```
SESSION_ACTION_ID=$(echo $SESSION_ACTION | jq -r .sessionActionId)
 MANIFEST_KEY=$(aws s3api list-objects-v2 \
     --bucket $DEV_FARM_BUCKET \
     --prefix $TASK_OUTPUT_PREFIX \
     --query "Contents[*].Key" --output text \
     | grep $SESSION_ACTION_ID \
     | sort | tail -1)
 MANIFEST_OBJECT=$(aws s3 cp s3://$DEV_FARM_BUCKET/$MANIFEST_KEY -)
 echo $MANIFEST_OBJECT | jq .
```

`hash-jobattachments.txt`Nell'output vedrete le proprietà del file, come le seguenti:

```
{
     "hashAlg": "xxh128",
     "manifestVersion": "2023-03-03",
     "paths": [
     {
         "hash": "f60b8e7d0fabf7214ba0b6822e82e08b",
         "mtime": 1698785252554950,
         "path": "hash-jobattachments.txt",
         "size": 182
     }
     ],
     "totalSize": 182
 }
```

Il job avrà un solo oggetto manifesto per operazione eseguita, ma in generale è possibile avere più oggetti per operazione eseguita.

6. Visualizza l'output di storage Amazon S3 indirizzabile ai contenuti sotto il prefisso. `Data`

```
FILE_HASH=$(echo $MANIFEST_OBJECT | jq -r .paths[0].hash)
FILE_PATH=$(echo $MANIFEST_OBJECT | jq -r .paths[0].path)
aws s3 cp s3://$DEV_FARM_BUCKET/JobAttachments/Data/$FILE_HASH -
```

Viene mostrato un output come il seguente:

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3  /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

Passaggio 5: aggiungi una flotta gestita dai servizi alla tua farm di sviluppatori in Deadline Cloud

AWS CloudShell non fornisce una capacità di elaborazione sufficiente per testare carichi di lavoro più grandi. Inoltre, non è configurato per funzionare con lavori che distribuiscono le attività su più host di lavoro.

Invece di utilizzarla CloudShell, puoi aggiungere una flotta gestita dal servizio Auto Scaling (SMF) alla tua farm di sviluppatori. Un SMF offre una capacità di elaborazione sufficiente per carichi di lavoro più grandi ed è in grado di gestire lavori che richiedono la distribuzione delle attività lavorative su più host di lavoro. Lo scheduler utilizzerà sia i worker SMF che quelli CMF per eseguire i job, a meno che non si chiuda il worker CMF.

Per aggiungere una flotta gestita dai servizi alla tua farm di sviluppatori

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Scegli la tua prima AWS CloudShell scheda, quindi crea la flotta gestita dal servizio e aggiungi il relativo ID della flotta a `.bashrc`. Questa azione lo rende disponibile per altre sessioni terminali.

```
FLEET_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
         --query "Account" --output text):role/${DEV_FARM_NAME}FleetRole"
 aws deadline create-fleet \
     --farm-id $DEV_FARM_ID \
     --display-name "$DEV_FARM_NAME SMF" \
     --role-arn $FLEET_ROLE_ARN \
     --max-worker-count 5 \
     --configuration \
         '{
             "serviceManagedEc2": {
                 "instanceCapabilities": {
                     "vCpuCount": {
                         "min": 2,
                         "max": 4
                     },
```

```
                    "memoryMiB": {
                        "min": 512
                    },
                    "osFamily": "linux",
                    "cpuArchitectureType": "x86_64"
                },
                "instanceMarketOptions": {
                    "type": "spot"
                }
            }
        }'

 echo "DEV_SMF_ID=$(aws deadline list-fleets \
        --farm-id $DEV_FARM_ID \
        --query "fleets[?displayName=='$DEV_FARM_NAME SMF'].fleetId \
        | [0]" --output text)" >> ~/.bashrc
 source ~/.bashrc
```

3. Associate l'SMF alla vostra coda.

```
aws deadline create-queue-fleet-association \
     --farm-id $DEV_FARM_ID \
     --queue-id $DEV_QUEUE_ID \
     --fleet-id $DEV_SMF_ID
```

4.

> **Note**
>
> Lo scheduler utilizzerà sia i worker SMF che quelli CMF per eseguire i job, a meno che non si chiuda il worker CMF.

Invia alla codasimple_file_job. Quando ti viene richiesto di confermare il caricamento, inserisci. **y**

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```

5. Conferma che l'SMF funzioni correttamente.

```
deadline fleet get
```

- L'operatore potrebbe impiegare alcuni minuti per iniziare.
- `queueFleetAssociationsStatus`Per la tua flotta gestita dai clienti e la flotta gestita dai servizi lo sarannoACTIVE.
- La SMF `autoScalingStatus` cambierà da `GROWING` a. `STEADY`

Il tuo stato sarà simile al seguente:

```
fleetId: fleet-2cc78e0dd3f04d1db427e7dc1d51ea44
farmId: farm-63ee8d77cdab4a578b685be8c5561c4a
displayName: DeveloperFarm SMF
description: ''
status: ACTIVE
autoScalingStatus: STEADY
targetWorkerCount: 0
workerCount: 0
minWorkerCount: 0
maxWorkerCount: 5
```

6. Visualizza il registro del lavoro che hai inviato. Questo registro viene memorizzato in un registro in Amazon CloudWatch Logs, non nel CloudShell file system.

```
JOB_ID=$(deadline config get defaults.job_id)
SESSION_ID=$(aws deadline list-sessions \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --job-id $JOB_ID \
        --query "sessions[0].sessionId" \
        --output text)
aws logs tail /aws/deadline/$DEV_FARM_ID/$DEV_QUEUE_ID \
    --log-stream-names $SESSION_ID
```

Passaggio 6: ripulisci le risorse della tua azienda agricola in Deadline Cloud

Per sviluppare e testare nuovi carichi di lavoro e integrazioni di pipeline, puoi continuare a utilizzare la farm per sviluppatori di Deadline Cloud che hai creato per questo tutorial. Se non hai più bisogno della tua farm di sviluppatori, puoi eliminarne le risorse, tra cui farm, fleet, queue, ruoli AWS Identity and Access Management (IAM) e log in Amazon CloudWatch Logs. Dopo aver eliminato queste

risorse, dovrai ricominciare il tutorial per utilizzarle. Per ulteriori informazioni, consulta Configurazione di una workstation per sviluppatori per Deadline Cloud.

Per ripulire le risorse della farm degli sviluppatori

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare alla versione più recente di AWS CLI.
2. Scegli la tua prima CloudShell scheda, quindi interrompi tutte le associazioni tra coda e parco macchine per la tua coda.

```
FLEETS=$(aws deadline list-queue-fleet-associations \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --query "queueFleetAssociations[].fleetId" \
        --output text)
for FLEET_ID in $FLEETS; do
    aws deadline update-queue-fleet-association \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --fleet-id $FLEET_ID \
        --status STOP_SCHEDULING_AND_CANCEL_TASKS
done
```

3. Elenca le associazioni delle flotte in coda.

```
aws deadline list-queue-fleet-associations \
     --farm-id $DEV_FARM_ID \
     --queue-id $DEV_QUEUE_ID
```

Potrebbe essere necessario eseguire nuovamente il comando fino a quando l'output non riporta i risultati`"status": "STOPPED"`, quindi è possibile procedere al passaggio successivo. Il completamento di questo processo può richiedere diversi minuti.

```
{
    "queueFleetAssociations": [
        {
            "queueId": "queue-abcdefgh01234567890123456789012id",
            "fleetId": "fleet-abcdefgh01234567890123456789012id",
            "status": "STOPPED",
            "createdAt": "2023-11-21T20:49:19+00:00",
```

```
            "createdBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
            "updatedAt": "2023-11-21T20:49:38+00:00",
            "updatedBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName"
        },
        {
            "queueId": "queue-abcdefgh01234567890123456789012id",
            "fleetId": "fleet-abcdefgh01234567890123456789012id",
            "status": "STOPPED",
            "createdAt": "2023-11-21T20:32:06+00:00",
            "createdBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
            "updatedAt": "2023-11-21T20:49:39+00:00",
            "updatedBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName"
        }
    ]
}
```

4. Elimina tutte le associazioni queue-fleet per la tua coda.

```
for FLEET_ID in $FLEETS; do
     aws deadline delete-queue-fleet-association \
         --farm-id $DEV_FARM_ID \
         --queue-id $DEV_QUEUE_ID \
         --fleet-id $FLEET_ID
 done
```

5. Elimina tutte le flotte associate alla coda.

```
for FLEET_ID in $FLEETS; do
     aws deadline delete-fleet \
         --farm-id $DEV_FARM_ID \
         --fleet-id $FLEET_ID
 done
```

6. Elimina la coda.

```
aws deadline delete-queue \
     --farm-id $DEV_FARM_ID \
     --queue-id $DEV_QUEUE_ID
```

7. Eliminare la fattoria.

```
aws deadline delete-farm \
     --farm-id $DEV_FARM_ID
```

8. Elimina altre AWS risorse per la tua fattoria.

   a. Elimina il ruolo fleet AWS Identity and Access Management (IAM).

```
aws iam delete-role-policy \
     --role-name "${DEV_FARM_NAME}FleetRole" \
     --policy-name WorkerPermissions
aws iam delete-role \
     --role-name "${DEV_FARM_NAME}FleetRole"
```

   b. Elimina il ruolo IAM in coda.

```
aws iam delete-role-policy \
     --role-name "${DEV_FARM_NAME}QueueRole" \
     --policy-name S3BucketsAccess
aws iam delete-role \
     --role-name "${DEV_FARM_NAME}QueueRole"
```

   c. Elimina i gruppi di log di Amazon CloudWatch Logs. Ogni coda e flotta ha il proprio gruppo di log.

```
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_QUEUE_ID"
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_CMF_ID"
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_SMF_ID"
```

Configura i mittenti di Deadline Cloud

Questo processo è destinato agli amministratori e agli artisti che desiderano installare, configurare e avviare il mittente Deadline Cloud. AWS Un mittente di Deadline Cloud è un plug-in per la creazione di contenuti digitali (DCC). Gli artisti lo usano per inviare lavori da un'interfaccia DCC di terze parti con cui hanno familiarità.

> **Note**
>
> Questo processo deve essere completato su tutte le postazioni di lavoro che gli artisti utilizzeranno per inviare i rendering.

Argomenti

Passaggio 1: installa il mittente Deadline Cloud

Le seguenti sezioni ti guidano attraverso i passaggi per installare il mittente Deadline Cloud.

Scarica il programma di installazione del mittente

Prima di poter installare Deadline Cloud submitter, devi scaricare il programma di installazione del mittente. Attualmente, il programma di installazione del mittente di Deadline Cloud supporta solo e. Windows Linux

1. Accedi AWS Management Console e apri la console Deadline Cloud.
2. Dal pannello di navigazione laterale, scegli Download.
3. Individua la sezione del programma di installazione del mittente di Deadline Cloud.
4. Seleziona il programma di installazione per il sistema operativo del tuo computer, quindi scegli Scarica.

(Facoltativo) Verifica l'autenticità del software scaricato

Per verificare che il software scaricato sia autentico, utilizzate la procedura seguente per uno Windows o Linux più.

> **Note**
>
> Puoi utilizzare queste istruzioni per verificare prima il programma di installazione e quindi verificare il monitor Deadline Cloud dopo averlo scaricato nella sezione successiva (Fase 2).

Windows

Per verificare l'autenticità dei file scaricati, completa i seguenti passaggi.

1. Nel comando seguente, *file* sostituiscilo con il file che desideri verificare. Ad esempio, ***C:\PATH\TO\MY*DeadlineCloudSubmitter-windows-x64-installer.exe** . Inoltre, *signtool-sdk-version* sostituiscilo con la versione dell'SignToolSDK installata. Ad esempio, **10.0.22000.0**.

   ```
   "C:\Program Files (x86)\Windows Kits\10\bin\signtool-sdk-version\x86\signtool.exe" verify /vfile
   ```

2. Ad esempio, puoi verificare il file di installazione del submitter di Deadline Cloud eseguendo il seguente comando:

   ```
   "C:\Program Files (x86)\Windows Kits\10\bin
   \10.0.22000.0\x86\signtool.exe" verify /v DeadlineCloudSubmitter-
   windows-x64-installer.exe
   ```

Linux

Per verificare l'autenticità dei file scaricati, utilizza lo strumento da riga di comando. gpg

1. Importa la OpenPGP chiave per il programma di installazione di Deadline Cloud submitter eseguendo il seguente comando:

   ```
    gpg --import --armor <<EOF
   -----BEGIN PGP PUBLIC KEY BLOCK-----

   mQINBGX6GQsBEADduUtJgqSXI+q76O6fsFwEYKmbnlyL0xKvlq32EZuyv0otZo5L
   le4m5Gg52AzrvPvDiUTLooAlvYeozaYyirIGsK08Ydz0Ftdjroiuh/mw9JSJDJRI
   rnRn5yKet1JFezkjopA3pjsTBP6lW/mb1bDBDEwwwtH0x9lV7A03FJ9T7Uzu/qSh
   qO/UYdkafro3cPASvkqgDt2tCvURfBcUCAjZVFcLZcVD5iwXacxvKsxxS/e7kuVV
   I1+VGT8Hj8XzWYhjCZxOLZk/fvpYPMyEEujN0fYUp6RtMIXve0C9awwMCy5nBG2J
   eE2Ol5DsCpTaBd4Fdr3LWcSs8JFA/YfP9auL3NczOozPoVJt+fw8CBlVIXO0J7l5
   hvHDjcC+5v0wxqAlMG6+f/SX7CT8FXK+L3iOJ5gBYUNXqHSxUdv8kt76/KVmQa1B
   Akl+MPKpMq+lhw++S3G/lXqwWaDNQbRRw7dSZHymQVXvPp1nsqc3hV7KlOM+6s6g
   1g4mvFY4lf6DhptwZLWyQXU8rBQpojvQfiSmDFrFPWFi5BexesuVnkGIolQoklKx
   AVUSdJPVEJCteyy7td4FPhBaSqT5vW3+ANbr9b/uoRYWJvn17dN0cc9HuRh/Ai+I
   nkfECo2WUDLZ0fEKGjGyFX+todWvJXjvc5kmE9Ty5vJp+M9Vvb8jd6t+mwARAQAB
   tCxBV1MgRGVhZGxpbmUgQ2xvdWQgPGF3cy1kZWFkbGluZUBhbWF6b24uY29tPokC
   VwQTAQgAQRYhBLhAwIwpqQeWoHH6pfbNPOa3bzzvBQJl+hkLAxsvBAUJA8JnAAUL
   ```

```
CQgHAgIiAgYVCgkICwIDFgIBAh4HAheAAAoJEPbNPOa3bzzvKswQAJXzKSAY8sY8
F6Eas2oYwIDDdDurs8FiEnFghjUEO6MTt9AykF/jw+CQg2UzFtEyObHBymhgmhXE
3buVeom96tgM3ZDfZu+sxi5pGX6oAQnZ6riztN+VpkpQmLgwtMGpSMLl3KLwnv2k
WK8mrR/fPMkfdaewB7A6RIUYiW33GAL4KfMIs8/vIwIJw99NxHpZQVoU6dFpuDtE
1OuxGcCqGJ7mAmo6H/YawSNp2Ns80gyqIKYo7o3LJ+WRroIRlQyctq8gnR9JvYXX
42ASqLq5+OXKo4qh81blXKYqtc176BbbSNFjWnzIQgKDgNiHFZCdcOVgqDhwO15r
NICbqqwwNLj/Fr2kecYx180Ktpl0jOOw5IOyh3bf3MVGWnYRdjvA1v+/CO+55N4g
z0kf50Lcdu5RtqV10XBCifn28pecqPaSdYcssYSRl5DLiFktGbNzTGcZZwITTKQc
af8PPdTGtnnb6P+cdbW3bt9MVtN5/dgSHLThnS8MPEuNCtkTnpXshuVuBGgwBMdb
qUC+HjqvhZzbwns8dr5WI+6HWNBFgGANn6ageYl58vVp0UkuNP8wcWjRARciHXZx
ku6W2jPTHDWGNrBQO2Fx7fd2QYJheIPPAShHcfJO+xgWCof45D0vAxAJ8gGg9Eq+
gFWhsx4NSHn2gh1gDZ41Ou/4exJ1lwPM
=uVaX
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

2. Determina se fidarti della chiave. OpenPGP Alcuni fattori da considerare quando si decide se considerare attendibile la chiave di cui sopra sono i seguenti:

   - La connessione Internet che hai utilizzato per ottenere la chiave GPG da questo sito Web è sicura.
   - Il dispositivo da cui accedi a questo sito Web è sicuro.
   - AWS ha adottato misure per proteggere l'hosting della chiave OpenPGP pubblica su questo sito web.

3. Se decidi di considerare attendibile la OpenPGP chiave, modifica la chiave in modo affidabile con gpg un metodo simile al seguente esempio:

```
$ gpg --edit-key 0xB840C08C29A90796A071FAA5F6CD3CE6B76F3CEF

    gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
    This is free software: you are free to change and redistribute it.
    There is NO WARRANTY, to the extent permitted by law.


    pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                         trust: unknown       validity: unknown
    [ unknown] (1). AWS Deadline Cloud example@example.com

    gpg> trust
    pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                         trust: unknown       validity: unknown
    [ unknown] (1). AWS Deadline Cloud aws-deadline@amazon.com
```

```
   Please decide how far you trust this user to correctly verify other users'
keys
   (by looking at passports, checking fingerprints from different sources,
etc.)

     1 = I don't know or won't say
     2 = I do NOT trust
     3 = I trust marginally
     4 = I trust fully
     5 = I trust ultimately
     m = back to the main menu

   Your decision? 5
   Do you really want to set this key to ultimate trust? (y/N) y

   pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                        trust: ultimate      validity: unknown
   [ unknown] (1). AWS Deadline Cloud aws-deadline@amazon.com
   Please note that the shown key validity is not necessarily correct
   unless you restart the program.

   gpg> quit
```

4. Verifica il programma di installazione

   Per verificare il programma di installazione, completa i seguenti passaggi:

   a. Torna alla pagina dei download della console di Deadline Cloud e scarica il file della firma per il programma di installazione del mittente di Deadline Cloud.

   b. Verifica la firma del programma di installazione del mittente di Deadline Cloud eseguendo:

      ```
      gpg --verify ./DeadlineCloudSubmitter-linux-x64-
      installer.run.sig ./DeadlineCloudSubmitter-linux-x64-
      installer.run
      ```

5. Verifica Deadline Cloud Monitor

> **Note**
>
> Puoi verificare il download del monitor Deadline Cloud utilizzando file di firma o metodi specifici della piattaforma. Per i metodi specifici della piattaforma, consulta la Linux (DEB) scheda o la Linux (AppImage) scheda in base al tipo di file scaricato.

Per verificare l'applicazione desktop Deadline Cloud Monitor con i file di firma, completa i seguenti passaggi:

a. Torna alla pagina dei download della console Deadline Cloud e scarica il file.sig corrispondente, quindi esegui

   Per .deb:

   ```
   gpg --verify ./deadline-cloud-
   monitor_<APP_VERSION>_amd64.deb.sig ./deadline-cloud-
   monitor_<APP_VERSION>_amd64.deb
   ```

   Per. AppImage:

   ```
   gpg --verify ./deadline-cloud-
   monitor_<APP_VERSION>_amd64.AppImage.sig ./deadline-cloud-
   monitor_<APP_VERSION>_amd64.AppImage
   ```

b. Verificate che l'output sia simile al seguente:

   ```
   gpg: Signature made Mon Apr 1 21:10:14 2024 UTC

   gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
   ```

   Se l'output contiene la fraseGood `signature from "AWS Deadline Cloud"`, significa che la firma è stata verificata con successo e puoi eseguire lo script di installazione del monitor Deadline Cloud.

Linux (DEB)

Per verificare i pacchetti che utilizzano un Linux file binario.deb, completate prima i passaggi 1-3 nella scheda. Linux

dpkg è lo strumento di gestione dei pacchetti principale nella maggior parte delle distribuzioni basate. debian Linux È possibile verificare il file.deb con lo strumento.

1. Dalla pagina dei download della console di Deadline Cloud, scarica il file.deb del monitor di Deadline Cloud.
2. ***<APP_VERSION>***Sostituiscilo con la versione del file.deb che desideri verificare.

   ```
   dpkg-sig --verify deadline-cloud-monitor_<APP_VERSION>_amd64.deb
   ```
3. L'output sarà simile a:

   ```
   Processing deadline-cloud-monitor_1.1.1_amd64.deb... GOODSIG
   _gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
   ```
4. Per verificare il file.deb, verificate che `GOODSIG` sia presente nell'output.

Linux (AppImage)

Per verificare i pacchetti che utilizzano un. Linux AppImage binario, completa prima i passaggi 1-3 nella Linux scheda.

1. Dalla pagina dei download della console Deadline Cloud, scarica il monitor Deadline Cloud. AppImage file.
2. Da sostituire <APP_VERSION>con la versione di. AppImage il file che desideri verificare, completa i seguenti passaggi:

   a. Scrivi la firma dal. AppImage file in un file.sig.

      ```
      ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
      --appimage-signature > ./deadline-cloud-
      monitor_<APP_VERSION>_amd64_.AppImage.sig
      ```

   b. Utilizzate il file .sig generato per verificare utilizzando il comando seguente.

      ```
      gpg --verify ./deadline-cloud-
      monitor_<APP_VERSION>_amd64.AppImage.sig
      ```

c. (Facoltativo) Se viene visualizzato un errore di autorizzazione negata, utilizzate il comando seguente per aggiungere l'autorizzazione di esecuzione.

```
chmod +x ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
```

d. Verificate che l'output sia simile al seguente:

```
gpg: Signature made Mon Apr 1 21:10:14 2024 UTC

gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Se l'output contiene la frase`Good signature from "AWS Deadline Cloud"`, significa che la firma è stata verificata con successo e puoi eseguire lo script di installazione del monitor Deadline Cloud.

Installa il mittente Deadline Cloud

Puoi installare un mittente Deadline Cloud con o. Windows Linux Con il programma di installazione, puoi installare i seguenti mittenti:

- Maggio 2024
- Nuke 14.0 - 15.0
- Houdini 19.5
- Colpo chiave 12
- Frullatore 3.6
- Unreal Engine 5

Windows

1. In un browser di file, accedi alla cartella in cui è stato scaricato il programma di installazione, quindi seleziona. `DeadlineCloudSubmitter-windows-x64-installer.exe`

   a. Se viene visualizzato un popup protetto da Windows sul tuo PC, scegli Altre informazioni.

   b. Scegli comunque Esegui.

2. Dopo l'apertura della procedura guidata di configurazione di AWS Deadline Cloud Submitter, scegli Avanti.
3. Scegli l'ambito di installazione completando uno dei seguenti passaggi:

- Per eseguire l'installazione solo per l'utente corrente, scegli Utente.
- Per eseguire l'installazione per tutti gli utenti, scegli Sistema.

  Se scegli Sistema, devi uscire dal programma di installazione ed eseguirlo nuovamente come amministratore completando i seguenti passaggi:

  a. Fai clic con il pulsante destro del mouse su**`DeadlineCloudSubmitter-windows-x64-installer.exe`**, quindi scegli Esegui come amministratore.
  b. Inserisci le credenziali di amministratore, quindi scegli Sì.
  c. Scegli Sistema per l'ambito di installazione.

4. Dopo aver selezionato l'ambito di installazione, scegli Avanti.
5. Scegliete nuovamente Avanti per accettare la directory di installazione.
6. Seleziona Integrated Submitter per Nuke, o qualsiasi altro mittente che desideri installare.
7. Seleziona Successivo.
8. Controlla l'installazione e scegli Avanti.
9. Scegli di nuovo Avanti, quindi scegli Fine.

Linux

> **Note**
>
> Il programma di Nuke installazione integrato di Deadline Cloud Linux e il monitor Deadline Cloud possono essere installati solo su Linux distribuzioni con almeno GLIBC 2.31.

1. Apri una finestra del terminale.
2. Per eseguire un'installazione di sistema dell'installatore, inserisci il comando e premi Invio per diventare root. **`sudo -i`**
3. Vai alla posizione in cui hai scaricato il programma di installazione.

   Ad esempio, **`cd /home/`*`USER`*`/Downloads`**.
4. Per rendere eseguibile il programma di installazione, immettere. **`chmod +x DeadlineCloudSubmitter-linux-x64-installer.run`**
5. Per eseguire il programma di installazione del mittente di Deadline Cloud, inserisci. **`./DeadlineCloudSubmitter-linux-x64-installer.run`**

6. All'apertura del programma di installazione, segui le istruzioni sullo schermo per completare la procedura guidata di installazione.

Puoi installare altri mittenti non elencati qui. Utilizziamo le librerie Deadline Cloud per creare mittenti. Puoi trovare il codice sorgente di queste librerie e mittenti nell'organizzazione aws-deadline. GitHub

Passaggio 2: installa e configura Deadline Cloud Monitor

Puoi installare l'applicazione desktop di monitoraggio Deadline Cloud con Windows o. Linux

Windows

1. Se non l'hai già fatto, accedi AWS Management Console e apri la console Deadline Cloud.
2. Dal riquadro di navigazione a sinistra, scegli Download.
3. Nella sezione Deadline Cloud monitor, seleziona il file per il sistema operativo del tuo computer.
4. Per scaricare il monitor Deadline Cloud, scegli Scarica.

Linux

Per installare Deadline Cloud monitor AppImage su distribuzioni RPM

1. Scarica l'ultimo monitor Deadline Cloud. AppImage
2. Per rendere AppImage eseguibile, inserisci**`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**.
3. Per configurare il percorso corretto del certificato SSL, immettere. **`sudo ln -sf /etc/ssl/certs/ca-bundle.crt /etc/ssl/certs/ca-certificates.crt`**

Per installare Deadline Cloud Monitor AppImage su distribuzioni Debian

1. Scarica l'ultimo monitor Deadline Cloud. AppImage
2.
> **Note**
>
> Questo passaggio è per Ubuntu 22 e versioni successive. Per altre versioni di Ubuntu, salta questo passaggio.

Per installare libfuse2, inserisci **`sudo apt udpate`**

`sudo apt install libfuse2`.

3. Per rendere AppImage eseguibile, inserisci. **`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**

Per installare Deadline Cloud, monitora il pacchetto Debian sulle distribuzioni Debian

1. Scarica il pacchetto Debian Deadline Cloud monitor più recente.
2.

> **Note**
>
> Questo passaggio è per Ubuntu 22 e versioni successive. Per altre versioni di Ubuntu, salta questo passaggio.

Per installare libssl1.1, inserisci **`wget http://nz2.archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.<APP_VERSION>.1f-1ubuntu2.22_amd64.deb`**

`sudo dpkg -i libssl1.<APP_VERSION>.1f-1ubuntu2.22_amd64.deb`.

3. Per installare il pacchetto Deadline Cloud monitor Debian, immettere **`sudo apt update`**

`sudo apt install ./deadline-cloud-monitor_<APP_VERSION>_amd64.deb`.

4. Se l'installazione fallisce su pacchetti che hanno dipendenze non soddisfatte, correggi i pacchetti difettosi e poi esegui i seguenti comandi.

```
sudo apt --fix-missing update

sudo apt update

sudo apt install -f
```

Dopo aver completato il download, puoi verificare l'autenticità del software scaricato. Vedi Verifica dell'autenticità del software scaricato nel passaggio 1.

Dopo aver scaricato Deadline Cloud monitor e aver verificato l'autenticità, utilizza la seguente procedura per configurare il monitor Deadline Cloud.

Per configurare il monitor Deadline Cloud

1. Apri il monitor Deadline Cloud.
2. Quando ti viene richiesto di creare un nuovo profilo, completa i seguenti passaggi.

   a. Inserisci l'URL del monitor nell'input dell'URL, che appare come **`https://`*`MY-MONITOR`*`.deadlinecloud.amazonaws.com/`**

   b. Inserisci un nome per il profilo.

   c. Scegli Crea profilo.

   Il tuo profilo è stato creato e le tue credenziali sono ora condivise con qualsiasi software che utilizza il nome del profilo che hai creato.
3. Dopo aver creato il profilo di monitoraggio di Deadline Cloud, non puoi modificare il nome del profilo o l'URL dello studio. Se devi apportare modifiche, procedi invece come segue:

   a. Eliminare il profilo. Nel riquadro di navigazione a sinistra, scegli Deadline Cloud monitor, Impostazioni, Elimina.

   b. Crea un nuovo profilo con le modifiche che desideri.
4. Dal riquadro di navigazione a sinistra, utilizza l'opzione di monitoraggio >Deadline Cloud per effettuare le seguenti operazioni:

   - Modifica il profilo del monitor di Deadline Cloud per accedere a un monitor diverso.
   - Abilita l'accesso automatico in modo da non dover inserire l'URL del monitor nelle successive aperture del monitor di Deadline Cloud.
5. Chiudi la finestra di monitoraggio di Deadline Cloud. Continua a funzionare in background e sincronizza le tue credenziali ogni 15 minuti.
6. Per ogni applicazione DCC (Digital Content Creation) che intendi utilizzare per i tuoi progetti di rendering, completa i seguenti passaggi:

   a. Dal mittente di Deadline Cloud, apri la configurazione della workstation Deadline Cloud.

   b. Nella configurazione della workstation, seleziona il profilo che hai creato nel monitor Deadline Cloud. Le tue credenziali Deadline Cloud sono ora condivise con questo DCC e i tuoi strumenti dovrebbero funzionare come previsto.

Passaggio 3: avvia il mittente di Deadline Cloud

Le seguenti sezioni ti guidano attraverso i passaggi per avviare il plug-in di invio Deadline Cloud in,, e. Blender Nuke Maya Houdini

Per avviare il mittente Deadline Cloud in Blender

> **Note**
>
> Support for Blender viene fornito utilizzando l'Condaambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Ambiente di Conda coda predefinito.

1. Aprire Blender.
2. Aprite una Blender scena con dipendenze esistenti nella directory principale dell'asset.
3. Nel menu Render, selezionate la finestra di dialogo Deadline Cloud.
    a. Se non sei già autenticato nel mittente di Deadline Cloud, lo stato delle credenziali mostra NEEDS_LOGIN.
    b. Selezionare Login (Accesso).
    c. Viene visualizzata una finestra del browser di accesso. Accedi con le tue credenziali utente.
    d. Scegli Permetti. Ora hai effettuato l'accesso e lo stato delle credenziali verrà visualizzato come AUTENTICATO.
4. Scegli Invia.

Per avviare il mittente di Deadline Cloud in Foundry Nuke

> **Note**
>
> Support for Nuke viene fornito utilizzando l'Condaambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Ambiente di Conda coda predefinito.

1. Aprire Nuke.
2. Aprite uno Nuke script con dipendenze esistenti nella directory principale dell'asset.
3. Scegli Thinkbox, quindi scegli Invia a Deadline Cloud per avviare il mittente.

a. Se non sei già autenticato nel mittente di Deadline Cloud, lo stato delle credenziali verrà visualizzato come NEEDS_LOGIN.

b. Selezionare Login (Accesso).

c. Nella finestra di accesso del browser, accedi con le tue credenziali utente.

d. Scegli Permetti. Ora hai effettuato l'accesso e lo stato delle credenziali verrà visualizzato come AUTENTICATO.

4. Scegli Invia.

Per avviare il mittente di Deadline Cloud in Maya

> **Note**
>
> Support Maya e Arnold for Maya(MtoA) viene fornito utilizzando l'Condaambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Ambiente di Conda coda predefinito.

1. Aprire Maya.
2. Imposta il tuo progetto e apri un file che esiste nella directory principale dell'asset.
3. Scegliete Windows → Impostazioni/Preferenze → Plugin Manager.
4. Cerca Submitter. DeadlineCloud
5. Per caricare il plug-in di invio di Deadline Cloud, seleziona Loaded.

   a. Se non sei già autenticato nel mittente di Deadline Cloud, lo stato delle credenziali verrà visualizzato come NEEDS_LOGIN.

   b. Selezionare Login (Accesso).

   c. Viene visualizzata una finestra del browser di accesso. Accedi con le tue credenziali utente.

   d. Scegli Permetti. Ora hai effettuato l'accesso e lo stato delle credenziali viene visualizzato come AUTENTICATO.

6. (Facoltativo) Per caricare il plug-in di invio di Deadline Cloud ogni volta che lo apri, scegli Caricamento automatico. Maya
7. Seleziona lo scaffale Deadline Cloud, quindi seleziona il pulsante verde per avviare il mittente.

Per avviare il mittente di Deadline Cloud in Houdini

> **Note**
>
> Support for Houdini viene fornito utilizzando l'Condaambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Ambiente di Conda coda predefinito.

1. Aprire Houdini.
2. Nell'Editor di rete, seleziona la rete /out.
3. Premi il tasto tab e inserisci**`deadline`**.
4. Seleziona l'opzione Deadline Cloud e collegala alla tua rete esistente.
5. Fai doppio clic sul nodo Deadline Cloud.

Per avviare il mittente di Deadline Cloud in KeyShot

Ciò presuppone che tu abbia già scaricato Deadline Cloud e 2. PySide

1. Copia o collega il file Deadline-Cloud-for-Keyshot/keyshot_script/submit to AWS Deadline Cloud.py alla cartella degli script. KeyShot

   Ad esempio, on, la posizione della Windows cartella degli script sarebbe. **`C:/Users/USER/Documents/KeyShot 12/Scripts`**
2. Imposta le seguenti variabili di ambiente.

   a. Imposta la variabile di ambiente **`DEADLINE_PYTHON`** come percorso dell'installazione di Python in cui si trovano deadline-cloud e 2. PySide

      Ad esempio, onWindows, se si utilizza Python 3.10, il comando potrebbe essere. **`set DEADLINE_PYTHON=C:/Users/USER/AppData/Local/Programs/Python/Python310/python`**

   b. Imposta la variabile di ambiente **`DEADLINE_KEYSHOT`** come percorso della cartella keyshot_submitter.

      Ad esempio, attivoWindows, se l'origine si trova sul desktop, il comando potrebbe essere. **`set DEADLINE_KEYSHOT=C:/Users/USER/Desktop/deadline-cloud-for-keyshot/src/deadline/keyshot_submitter`**

3. Con le variabili di ambiente impostate, avvia KeyShot.
4. Per avviare il mittente KeyShot, scegli Scripting console Windows, Invia a AWS Deadline Cloud ed Esegui.

Per avviare il mittente di Deadline Cloud in Unreal Engine

Ciò presuppone che tu abbia già scaricato Deadline Cloud.

1. Crea o apri la cartella che usi per i tuoi Unreal Engine progetti.
2. Apri la riga di comando ed esegui i seguenti comandi:
   - `git clone https://github.com/aws-deadline/deadline-cloud-for-unreal-engine`
   - `cd deadline-cloud-for-unreal/test_projects`
   - `git lfs fetch –all`
3. Per scaricare il plugin perUnreal Engine, apri la cartella Unreal Engine del progetto e avvia deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat.

   Questo inserisce i file del plugin in C:// LocalProjectsUnrealDeadlineCloudTestUnrealDeadlineCloudService/Plugins/.
4. Per scaricare il mittente, apri la cartella ed esegui UnrealDeadlineCloudService . **`deadline-cloud-forunreal/ test_projects/Plugins/UnrealDeadlineCloudService/ install_unreal_submitter.bat`**
5. Per avviare il mittente daUnreal Engine, completa i seguenti passaggi:
   a. Scegliete Modifica, **>** Impostazioni del progetto.
   b. Nella barra di ricerca inserisci **`movie render pipeline`**.
   c. Regolate le seguenti impostazioni di Movie Render Pipeline:
      i. Per Default Remote Executor, immettere. **`MoviePipelineDeadlineCloudRemote Executor`**
      ii. Per Default Executor Job, immettere **`MoviePipelineDeadlineCloudExecutorJob`**
      iii. Per le classi Default Job Settings, scegliete il segno più, quindi immettete**`DeadlineCloudRenderStepSetting`**.

   Con queste impostazioni, puoi scegliere tra il plug-in Deadline Cloud. Unreal Engine

Usa la fattoria

Se hai seguito tutte le istruzioni per iniziare, hai impostato tutto ciò che ti serve per iniziare a inviare i lavori dalla tua postazione di lavoro locale alla tua azienda agricola e quindi monitorare tali lavori e risorse. Per ulteriori informazioni sull'invio di tutti i tipi di lavori o sul monitoraggio, consultate gli argomenti correlati riportati di seguito.

- Jobs
- Uso del monitor

Utilizzo del monitor Deadline Cloud

Il monitor AWS Deadline Cloud ti offre una visione generale dei tuoi lavori di elaborazione visiva. Puoi usarlo per monitorare e gestire i lavori, visualizzare l'attività dei lavoratori sulle flotte, tenere traccia dei budget e dell'utilizzo e scaricare i risultati di un lavoro.

Ogni coda ha un monitor dei lavori che mostra lo stato dei lavori, delle fasi e delle attività. Il monitor offre modi per gestire i lavori direttamente dal monitor. È possibile apportare modifiche alle priorità, annullare i lavori e richiederli.

Il monitor Deadline Cloud ha una tabella che mostra lo stato riepilogativo di un lavoro, oppure puoi selezionare un lavoro per visualizzare i registri dettagliati delle attività che aiutano a risolvere i problemi relativi a un lavoro.

Puoi utilizzare il monitor Deadline Cloud per scaricare i risultati nella posizione sulla tua workstation specificata al momento della creazione del lavoro.

Il monitor Deadline Cloud ti aiuta anche a monitorare l'utilizzo e a gestire i costi. Per ulteriori informazioni, consulta Gestione dei budget e dell'utilizzo per Deadline Cloud.

Argomenti

Condividi l'URL del monitor di Deadline Cloud

Quando configuri il servizio Deadline Cloud, per impostazione predefinita crei un URL che apre il monitor Deadline Cloud per il tuo account. Usa questo URL per aprire il monitor nel browser o sul desktop. Condividi l'URL con altri utenti in modo che possano accedere al monitor Deadline Cloud.

Prima che un utente possa aprire il monitor Deadline Cloud, devi concedere all'utente l'accesso. Per concedere l'accesso, aggiungi l'utente all'elenco degli utenti autorizzati per il monitor o aggiungilo a un gruppo con accesso al monitor. Per ulteriori informazioni, consulta Gestione degli utenti in Deadline Cloud.

Per condividere l'URL del monitor

1. Apri la console Deadline Cloud.
2. Da Inizia, scegli Vai alla dashboard di Deadline Cloud.
3. Nel riquadro di navigazione, selezionare Dashboard (Pannello di controllo).
4. Nella sezione Panoramica dell'account, scegli Dettagli dell'account.
5. Copia e invia in modo sicuro l'URL a chiunque debba accedere al monitor Deadline Cloud.

Apri il monitor Deadline Cloud

Puoi aprire il monitor Deadline Cloud in uno dei seguenti modi:

- Console: accedi AWS Management Console e apri la console Deadline Cloud.
- Web: vai all'URL di monitoraggio che hai creato quando hai configurato Deadline Cloud.
- Monitor: utilizza il monitor desktop Deadline Cloud.

Quando utilizzi la console, devi poter accedere AWS utilizzando un' AWS Identity and Access Management identità e quindi accedere al monitor con AWS IAM Identity Center le credenziali. Se disponi solo di credenziali IAM Identity Center, devi accedere utilizzando l'URL del monitor o l'applicazione desktop.

Per aprire il monitor Deadline Cloud (web)

1. Utilizzando un browser, apri l'URL del monitor che hai creato durante la configurazione di Deadline Cloud.
2. Accedi con le tue credenziali utente.

Per aprire il monitor Deadline Cloud (console)

1. Apri la console Deadline Cloud.
2. Nel riquadro di navigazione, seleziona Fattorie.

3. Seleziona una fattoria, quindi scegli Gestisci lavori per aprire la pagina di monitoraggio di Deadline Cloud.
4. Accedi con le tue credenziali utente.

Per aprire il monitor Deadline Cloud (desktop)

1. Apri la console Deadline Cloud.

   oppure

   Apri Deadline Cloud monitor - web dall'URL del monitor.

2. • Sulla console Deadline Cloud, procedi come segue:
   1. Nel monitor, scegli Vai alla dashboard di Deadline Cloud, quindi scegli Download dal menu a sinistra.
   2. Dal monitor Deadline Cloud, scegli la versione del monitor per il tuo desktop.
   3. Scegli Download (Scarica).
   - Sul monitor Deadline Cloud - web, procedi come segue:
     - Dal menu a sinistra, scegli Configurazione della workstation. Se l'elemento di configurazione della workstation non è visibile, usa la freccia per aprire il menu a sinistra.
     - Scegli Download (Scarica).
     - Da Seleziona un sistema operativo, scegli il tuo sistema operativo.
3. Scarica il monitor Deadline Cloud - desktop.
4. Dopo aver scaricato e installato il monitor, aprilo sul tuo computer.
   - Se è la prima volta che apri il monitor Deadline Cloud, devi fornire l'URL del monitor e creare un nome di profilo. Successivamente accedi al monitor con le tue credenziali Deadline Cloud.
   - Dopo aver creato un profilo, apri il monitor selezionando un profilo. Potrebbe essere necessario inserire le credenziali di Deadline Cloud.

Visualizza i dettagli della coda e della flotta in Deadline Cloud

Puoi utilizzare il monitor Deadline Cloud per visualizzare la configurazione delle code e delle flotte nella tua fattoria. Puoi anche utilizzare il monitor per visualizzare un elenco dei lavori in coda o dei lavoratori di una flotta.

È necessario disporre `VIEWING` dell'autorizzazione per visualizzare i dettagli della coda e della flotta. Se i dettagli non vengono visualizzati, contatta l'amministratore per ottenere le autorizzazioni corrette.

Per visualizzare i dettagli della coda

1. Apri il monitor Deadline Cloud.
2. Dall'elenco delle fattorie, scegli la fattoria che contiene la coda che ti interessa.
3. Nell'elenco delle code, scegli una coda per visualizzarne i dettagli. Per confrontare la configurazione di due o più code, seleziona più di una casella di controllo.
4. Per visualizzare un elenco di lavori in coda, scegli il nome della coda dall'elenco delle code o dal pannello dei dettagli.

Se il monitor è già aperto, puoi selezionare la coda dall'elenco delle code nel riquadro di navigazione a sinistra.

Per visualizzare i dettagli del parco istanze

1. Apri il monitor Deadline Cloud.
2. Dall'elenco delle aziende agricole, scegli la fattoria che contiene la flotta che ti interessa.
3. In Risorse agricole, scegli Flotte.
4. Nell'elenco delle flotte, scegli una flotta per visualizzarne i dettagli. Per confrontare la configurazione di due o più flotte, seleziona più di una casella di controllo.
5. Per visualizzare un elenco di lavoratori della flotta, scegli il nome della flotta dall'elenco delle flotte o dal pannello dei dettagli.

Se il monitor è già aperto, puoi selezionare la flotta dall'elenco Flotte nel riquadro di navigazione a sinistra.

Visualizza e gestisci lavori, passaggi e attività in Deadline Cloud

Quando selezioni una coda, la sezione di monitoraggio dei lavori del monitor Deadline Cloud mostra i lavori in quella coda, le fasi del lavoro e le attività in ogni fase. Quando selezioni un lavoro, un passaggio o un'attività, puoi utilizzare il menu Azioni per gestirli tutti.

Per aprire il monitor dei lavori, segui i passaggi per visualizzare una codaVisualizza i dettagli della coda e della flotta in Deadline Cloud, quindi seleziona il lavoro, il passaggio o l'attività su cui lavorare.

Per i lavori, le fasi e le attività, puoi fare quanto segue:

- Modifica lo stato in Richiesto, Operato con successo, Non riuscito o Annullato.
- Scarica l'output elaborato dal processo, dalla fase o dall'attività.
- Copia l'ID del lavoro, del passaggio o dell'attività.

Per il lavoro selezionato, puoi:

- Archiviare il lavoro.
- Modifica le proprietà del lavoro, ad esempio cambiando la priorità o visualizzando le dipendenze passo per passo.
- Visualizza dettagli aggiuntivi utilizzando i parametri del lavoro.

Per ulteriori informazioni, consulta Visualizza i dettagli del lavoro in Deadline Cloud.

Per ogni passaggio, puoi:

- Visualizzare le dipendenze per la fase. Le dipendenze di una fase devono essere completate prima dell'esecuzione della fase.

Per informazioni dettagliate, vedi Visualizza una fase in Deadline Cloud.

Per ogni attività, puoi:

- Visualizzare i registri dell'attività.
- Visualizza i parametri dell'attività.

Per ulteriori informazioni, consulta Visualizza un'attività in Deadline Cloud.

Visualizza i dettagli del lavoro in Deadline Cloud

La pagina Job monitor in Deadline Cloud monitor fornisce quanto segue:

- Una visione d'insieme dello stato di avanzamento di un lavoro.
- Una panoramica delle fasi e delle attività che compongono il lavoro.

Scegliete un lavoro dall'elenco per visualizzare un elenco dei passaggi del lavoro, quindi scegliete un passaggio dall'elenco dei passaggi per visualizzare le attività relative al lavoro. Dopo aver scelto un elemento, puoi utilizzare il menu Azioni relativo a quell'elemento per visualizzarne i dettagli.

Per visualizzare i dettagli del lavoro

1. Segui i passaggi per visualizzare una coda. Visualizza i dettagli della coda e della flotta in Deadline Cloud
2. Nel riquadro di navigazione, seleziona la coda in cui hai inviato il lavoro.
3. Seleziona un lavoro utilizzando uno dei seguenti metodi:

    a. Dall'elenco Lavori, selezionare un lavoro per visualizzarne i dettagli.

    b. Nel campo di ricerca, inserisci qualsiasi testo associato al lavoro, ad esempio il nome del lavoro o l'utente che ha creato il lavoro. Dai risultati visualizzati, seleziona il lavoro che desideri visualizzare.

I dettagli di un lavoro includono le fasi del lavoro e le attività in ogni fase. È possibile utilizzare il menu Azioni per effettuare le seguenti operazioni:

- Modificare lo stato del lavoro.
- Visualizza e modifica le proprietà di un lavoro. È possibile visualizzare le dipendenze tra le fasi del lavoro e modificare la priorità del lavoro. In genere, i lavori con una priorità più alta vengono completati prima.
- Visualizza i parametri per il lavoro che sono stati impostati al momento dell'invio del lavoro.
- Scarica l'output di un lavoro. Quando si scarica l'output di un lavoro, questo contiene tutto l'output generato dai passaggi e dalle attività del lavoro.

Visualizza una fase in Deadline Cloud

Utilizza il monitor AWS Deadline Cloud per visualizzare le fasi dei tuoi processi di elaborazione. Nel Job monitor, l'elenco Passaggi mostra l'elenco dei passaggi che compongono il lavoro selezionato. Quando si seleziona una fase, l'elenco Attività mostra le attività incluse nella fase.

Per visualizzare un passaggio

1. Segui i passaggi indicati Visualizza i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di lavori.

2. Selezionare un processo nell'elenco Jobs (Processi).
3. Seleziona un passaggio dall'elenco Passaggi.

È possibile utilizzare il menu Azioni per effettuare le seguenti operazioni:

- Modificare lo stato del passaggio.
- Scarica l'output del passaggio. Quando scaricate l'output di un passo, questo contiene tutto l'output generato dalle attività del passo.
- Visualizza le dipendenze di una fase. La tabella delle dipendenze mostra un elenco di passaggi che devono essere completati prima dell'inizio del passaggio selezionato e un elenco di passaggi in attesa del completamento di questo passaggio.

Visualizza un'attività in Deadline Cloud

Usa il monitor AWS Deadline Cloud per visualizzare le attività nei tuoi processi di elaborazione. Nel Job monitor, l'elenco Tasks mostra le attività che compongono la fase selezionata nell'elenco Steps.

Per visualizzare un'attività

1. Segui i passaggi indicati Visualizza i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di lavori.
2. Selezionare un processo nell'elenco Jobs (Processi).
3. Seleziona un passaggio dall'elenco Passaggi.
4. Seleziona un'attività dall'elenco Attività.

È possibile utilizzare il menu Azioni per effettuare le seguenti operazioni:

- Modificare lo stato dell'attività.
- Visualizza i registri delle attività. Per ulteriori informazioni, consulta Visualizza i log in Deadline Cloud.
- Visualizza i parametri che sono stati impostati al momento della creazione dell'attività.
- Scarica l'output dell'attività. Quando scarichi l'output di un'attività, contiene solo l'output generato dall'attività selezionata.

Visualizza i log in Deadline Cloud

I log forniscono informazioni dettagliate sullo stato e sull'elaborazione delle attività. Nel monitor AWS Deadline Cloud, puoi vedere i seguenti due tipi di log:

- I registri delle sessioni descrivono in dettaglio la sequenza temporale delle azioni, tra cui:
  - Azioni di configurazione, come la sincronizzazione degli allegati e il caricamento dell'ambiente software
  - Esecuzione di un'attività o di una serie di attività
  - Azioni di chiusura, come la chiusura dell'ambiente di lavoro di un lavoratore

  Una sessione include l'elaborazione di almeno un'attività e può includere più attività. I log di sessione mostrano anche informazioni sul tipo di istanza di Amazon Elastic Compute Cloud (Amazon EC2), vCPU e memoria. I log delle sessioni includono anche un collegamento al registro del lavoratore utilizzato nella sessione.
- I registri dei lavoratori forniscono dettagli sulla sequenza temporale delle azioni che un lavoratore elabora durante il suo ciclo di vita. I registri dei lavoratori possono contenere informazioni su più sessioni.

È possibile scaricare i registri delle sessioni e dei lavoratori in modo da poterli esaminare offline.

Per visualizzare i registri delle sessioni

1. Segui i passaggi indicati Visualizza i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di lavori.
2. Selezionare un processo nell'elenco Jobs (Processi).
3. Seleziona un passaggio dall'elenco Passaggi.
4. Seleziona un'attività dall'elenco Attività.
5. Dal menu Azioni, scegli Visualizza registri.

La sezione Cronologia mostra un riepilogo delle azioni relative all'attività. Per visualizzare altre attività eseguite nella sessione e per visualizzare le azioni di chiusura della sessione, scegli Visualizza i registri per tutte le attività.

Per visualizzare i registri dei lavoratori relativi a un'attività

1. Segui i passaggi indicati Visualizza i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di lavori.
2. Selezionare un processo nell'elenco Jobs (Processi).
3. Seleziona un passaggio dall'elenco Passaggi.
4. Seleziona un'attività dall'elenco Attività.
5. Dal menu Azioni, scegli Visualizza registri.
6. Scegli Informazioni sulla sessione.
7. Scegli Visualizza il registro dei lavoratori.

Per visualizzare i registri dei lavoratori dai dettagli della flotta

1. Segui i passaggi indicati Visualizza i dettagli della coda e della flotta in Deadline Cloud per visualizzare una flotta.
2. Seleziona un ID lavoratore dall'elenco Lavoratori.
3. Dal menu Azioni, scegli Visualizza i registri dei lavoratori.

Scarica l'output finito in Deadline Cloud

Al termine di un lavoro, puoi utilizzare il monitor AWS Deadline Cloud per scaricare i risultati sulla tua workstation. Il file di output viene archiviato con il nome e la posizione specificati al momento della creazione del lavoro.

I file di output vengono archiviati a tempo indeterminato. Per ridurre i costi di storage, prendi in considerazione la creazione di una configurazione del ciclo di vita S3 per il bucket Amazon S3 della coda. Per ulteriori informazioni, consulta Managing your storage lifecycle nella Amazon Simple Storage Service User Guide.

Per scaricare l'output finale di un lavoro, una fase o un'attività

1. Segui i passaggi indicati Visualizza i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di lavori.
2. Seleziona il lavoro, la fase o l'attività per cui desideri scaricare l'output.

- Se selezioni un lavoro, puoi scaricare tutto l'output per tutte le attività in tutti i passaggi di quel lavoro.
- Se si seleziona una fase, è possibile scaricare tutto l'output per tutte le attività di quella fase.
- Se si seleziona un'attività, è possibile scaricare l'output per quella singola attività.

3. Dal menu Azioni, scegli Scarica output.
4. L'output verrà scaricato nella posizione impostata al momento dell'invio del lavoro.

> **Note**
>
> Il download dell'output tramite il menu è attualmente supportato solo per Windows eLinux. Se avete un file Mac e scegliete la voce del menu Scarica output, una finestra mostra il AWS CLI comando che potete usare per scaricare l'output renderizzato.

Deadline Cloud farm

Una farm è un contenitore per le code che gestiscono i lavori e le flotte di risorse di elaborazione che eseguono attività.

Argomenti

Crea una fattoria

1. Dalla console Deadline Cloud, scegli Vai alla dashboard.
2. Nella sezione Farms della dashboard di Deadline Cloud, scegli Azioni → Crea fattoria.
   - In alternativa, nel pannello laterale sinistro scegli Fattorie e altre risorse, quindi scegli Crea fattoria.
3. Aggiungi un nome alla tua fattoria.
4. Per Descrizione, inserisci la descrizione dell'azienda. Una descrizione chiara può aiutarti a identificare rapidamente lo scopo della tua azienda.
5. (Facoltativo) Per impostazione predefinita, i tuoi dati sono crittografati con una chiave che AWS possiede e gestisce per la tua sicurezza. Puoi scegliere Personalizza le impostazioni di crittografia (avanzate) per utilizzare una chiave esistente o per crearne una nuova da gestire.

   Se scegli di personalizzare le impostazioni di crittografia utilizzando la casella di controllo, inserisci un AWS KMS ARN o creane uno AWS KMS nuovo scegliendo Crea nuova chiave KMS.
6. (Facoltativo) Scegli Aggiungi nuovo tag per aggiungere uno o più tag alla tua fattoria.
7. Scegli Crea fattoria. Dopo la creazione, la tua fattoria viene visualizzata.

Eliminare una fattoria

1. Dalla dashboard di Deadline Cloud, scegli Fattorie e altre risorse.
2. Nell'elenco delle fattorie, seleziona la fattoria o le fattorie che desideri eliminare, quindi scegli Elimina.

Modifica una fattoria

1. Dalla dashboard di Deadline Cloud, scegli Fattorie e altre risorse.
2. Nell'elenco delle fattorie, seleziona la fattoria o le fattorie che desideri eliminare, quindi scegli Modifica.
3. Nella finestra di modifica visualizzata, modifica il nome o la descrizione della fattoria, quindi scegli Salva modifiche.

Code Deadline Cloud

Una coda è una risorsa agricola che gestisce ed elabora i lavori.

Per utilizzare le code, è necessario disporre già di un monitor e di una farm configurati.

Argomenti

Crea una coda

1. Dalla dashboard della console Deadline Cloud, seleziona la fattoria per cui desideri creare una coda.
    - In alternativa, nel pannello laterale sinistro scegli Fattorie e altre risorse, quindi seleziona la fattoria per cui desideri creare una coda.
2. Nella scheda Code, scegli Crea coda.
3. Inserisci un nome per la coda.
4. In Descrizione, inserisci la descrizione della coda. Una descrizione consente di identificare lo scopo della coda.
5. Per gli allegati Job, puoi creare un nuovo bucket Amazon S3 o scegliere un bucket Amazon S3 esistente.
    a. Per creare un nuovo bucket Amazon S3
        i. Seleziona Crea nuovo job bucket.
        ii. Inserisci un nome per il bucket. Ti consigliamo di assegnare un nome al bucket. `deadlinecloud-job-attachments-[MONITORNAME]`
        iii. Inserisci un prefisso Root per definire o modificare la posizione principale della coda.
    b. Per scegliere un bucket Amazon S3 esistente

i. Seleziona Scegli un bucket S3 esistente > Sfoglia S3.

ii. Seleziona il bucket S3 per la tua coda dall'elenco dei bucket disponibili.

6. (Facoltativo) Per associare la coda a una flotta gestita dal cliente, seleziona Abilita l'associazione con flotte gestite dal cliente.

7. Se abiliti l'associazione con flotte gestite dal cliente, devi completare i seguenti passaggi.

> **Important**
>
> Consigliamo vivamente di specificare utenti e gruppi per la funzionalità run-as. In caso contrario, peggiorerà il livello di sicurezza della vostra azienda agricola, in quanto i dipendenti potranno così fare tutto ciò che può fare l'agente del lavoratore. Per ulteriori informazioni sui potenziali rischi per la sicurezza, consulta Esegui lavori come utenti e gruppi.

a. Per Esegui come utente:

   Per fornire le credenziali per i lavori della coda, seleziona Utente configurato dalla coda.

   In alternativa, per disattivare l'impostazione delle proprie credenziali ed eseguire i job come utente worker agent, seleziona Utente agente Worker.

b. (Facoltativo) Per Esegui come credenziali utente, inserisci un nome utente e un nome di gruppo per fornire le credenziali per i lavori della coda.

   Se si utilizza una Windows flotta, è necessario creare un AWS Secrets Manager segreto che contenga la password per l'utente Esegui come utente. Segui queste istruzioni per creare il segreto. Sostituisci *`jobuser`* con il nome di. `jobRunAsUser`

   i. Apri PowerShell o visualizza il prompt dei comandi come amministratore.

   ii. Creare l'utente.

   ```
   net user jobuser /add
   ```

   iii. Imposta la password.

   ```
   net user jobuser *
   ```

iv. Crea un profilo locale e una home directory per l'utente. Esegui il comando seguente e inserisci la password per l'utente quando richiesto.

```
runas /profile /user:jobuser "cmd.exe /C"
```

8. La richiesta di un budget consente di gestire i costi della coda. Seleziona Non richiedere un budget o Richiedi un budget.
9. La tua coda richiede l'autorizzazione per accedere ad Amazon S3 per tuo conto. Puoi creare un nuovo ruolo di servizio o utilizzare un ruolo di servizio esistente. Se non disponi di un ruolo di servizio esistente, crea e utilizza un nuovo ruolo di servizio.

    a. Per utilizzare un ruolo di servizio esistente, seleziona Scegli un ruolo di servizio, quindi seleziona un ruolo dal menu a discesa.

    b. Per creare un nuovo ruolo di servizio, seleziona Crea e utilizza un nuovo ruolo di servizio, quindi inserisci il nome e la descrizione del ruolo.
10. (Facoltativo) Per aggiungere variabili di ambiente per l'ambiente di coda, scegli Aggiungi nuova variabile di ambiente, quindi inserisci un nome e un valore per ogni variabile aggiunta.
11. (Facoltativo) Scegliete Aggiungi nuovo tag per aggiungere uno o più tag alla coda.
12. Per creare un ambiente di Conda coda predefinito, mantieni selezionata la casella di controllo. Per ulteriori informazioni sugli ambienti di coda, consulta Creare un ambiente di coda. Se stai creando una coda per un parco veicoli gestito dal cliente, deseleziona la casella di controllo.
13. Scegliere Crea coda.

Crea un ambiente di coda

Un ambiente di coda è un insieme di variabili e comandi di ambiente che configurano i lavoratori della flotta. È possibile utilizzare gli ambienti di coda per fornire applicazioni software, variabili di ambiente e altre risorse ai lavori in coda.

Quando si crea una coda, è possibile creare un ambiente di coda predefinitoConda. Questo ambiente fornisce alle flotte gestite dai servizi l'accesso ai pacchetti per le applicazioni e i renderer DCC dei partner. Per ulteriori informazioni, consulta Ambiente di Conda coda predefinito.

È possibile aggiungere ambienti di coda utilizzando la console o modificando direttamente il modello json o YAML. Questa procedura descrive come creare un ambiente con la console.

1. Per aggiungere un ambiente di coda a una coda, accedi alla coda e seleziona la scheda Ambienti di coda.
2. Scegli Azioni, quindi Crea nuovo con modulo.
3. Inserisci un nome e una descrizione per l'ambiente di coda.
4. Scegliete Aggiungi nuova variabile di ambiente, quindi immettete un nome e un valore per ogni variabile aggiunta.
5. (Facoltativo) Inserite una priorità per l'ambiente di coda. La priorità indica l'ordine in cui questo ambiente di coda verrà eseguito sul lavoratore. Gli ambienti di coda con priorità più elevata verranno eseguiti per primi.
6. Scegli Crea ambiente di coda.

Ambiente di Conda coda predefinito

Quando crei una coda associata a una flotta gestita dai servizi, hai la possibilità di aggiungere un ambiente di coda predefinito che supporti il download e l'installazione di pacchetti in un ambiente virtuale Condaper i tuoi lavori.

Condafornisce pacchetti dai canali. Un canale è una posizione in cui vengono archiviati i pacchetti. Deadline Cloud fornisce un canale che ospita pacchetti che supportano le applicazioni e i renderer DCC dei partner. `deadline-cloud` I pacchetti sono:

- Frullatore
  - `blender=3.6`
  - `blender-openjd`
- Houdini
  - `houdini=19.5`
  - `houdini-openjd`
- Maya
  - `maya=2024`
  - `maya-mtoa=2024.5.3`
  - `maya-openjd`
- Nuke
  - `nuke=15`
  - `nuke-openjd`

Quando si invia un lavoro a una coda con l'Condaambiente predefinito, l'ambiente aggiunge due parametri al lavoro. Questi parametri Conda specificano i pacchetti e i canali da utilizzare per configurare l'ambiente del lavoro prima dell'elaborazione delle attività. I parametri sono:

- `CondaPackages`— un elenco separato da spazi delle specifiche dei pacchetti che corrispondono, ad esempio `blender=3.6` o. `numpy>1.22` L'impostazione predefinita è vuota per ignorare la creazione di un ambiente virtuale.
- `CondaChannels`— un elenco di Condacanali separati da spazi come `deadline-cloudconda-forge`, `os3://DOC-EXAMPLE-BUCKET/conda/channel`. L'impostazione predefinita è `deadline-cloud` un canale disponibile per le flotte gestite dai servizi che fornisce applicazioni e renderer DCC partner.

Quando utilizzi un mittente integrato per inviare un lavoro a Deadline Cloud dal tuo DCC, il mittente inserisce il valore del parametro in base all'applicazione DCC e al mittente. `CondaPackages` Ad esempio, se si utilizza Blender, il parametro è impostato su. `CondaPackage` `blender=3.6.*` `blender-openjd=0.4.*`

Elimina una coda

> **Warning**
>
> Non puoi recuperare i lavori in coda se elimini la coda. L'eliminazione della coda elimina anche i lavori in quella coda.

1. Dalla dashboard di Deadline Cloud, scegli Fattorie e altre risorse.
2. Nell'elenco delle fattorie, seleziona la fattoria che contiene la coda da eliminare.
3. Seleziona la coda, quindi scegli Elimina.
4. Nella finestra di conferma scegli Delete (Elimina). La coda e tutti i lavori in coda vengono eliminati.

Modificare una coda

1. Dalla dashboard di Deadline Cloud, scegli Farms e altre risorse.
2. Nell'elenco delle fattorie, seleziona la fattoria che contiene la coda da modificare.

3. Seleziona la coda, quindi scegli Modifica.
4. È possibile modificare il nome, la descrizione, il requisito di budget, l'opzione Esegui come utente e il ruolo di servizio assegnato. Puoi anche associare una flotta esistente alla tua coda.
5. Seleziona Salvataggio delle modifiche.

Associa una coda e una flotta

1. Seleziona la coda da associare a una flotta.
2. Per selezionare una flotta da associare alla tua coda, scegli Associa flotte.
3. Scegli il menu a discesa Seleziona flotte. Viene visualizzato un elenco di flotte disponibili.
4. Dall'elenco delle flotte disponibili, seleziona la casella di controllo accanto alla flotta o alle flotte che desideri associare alla coda.
5. Selezionare Associate (Associa). Lo status di associazione della flotta dovrebbe ora essere Associato.

Gestisci le flotte Deadline Cloud

Questa sezione spiega come gestire flotte gestite dai servizi (SMF) e flotte gestite dai clienti (CMF) per Deadline Cloud.

Puoi configurare due tipi di flotte Deadline Cloud:

- Le flotte gestite dai servizi sono flotte di lavoratori con impostazioni predefinite fornite da questo servizio, Deadline Cloud. Queste impostazioni predefinite sono progettate per essere efficienti ed economiche.
- Le flotte gestite dai clienti (CMF) sono flotte di lavoratori gestite dall'utente. Un CMF può risiedere all'interno AWS dell'infrastruttura, in sede o in un data center condiviso. Un CMF fornisce il pieno controllo e la responsabilità della flotta. Ciò include il rifornimento, le operazioni, la gestione e lo smantellamento dei lavoratori della flotta.

Argomenti

Gestisci le flotte gestite dai servizi Deadline Cloud

Le flotte gestite dai servizi sono flotte di lavoratori con impostazioni predefinite fornite da Deadline Cloud. Queste impostazioni predefinite sono progettate per essere efficienti ed economiche.

1. Per creare una flotta gestita dai servizi (SMF), accedi alla farm in cui desideri creare la flotta.
2. Seleziona la scheda Flotte.
3. Scegliere Create Fleet (Crea parco istanze).
4. Inserisci un nome per la tua flotta.
5. Inserisci una Description (Descrizione). Una descrizione chiara può aiutarti a identificare rapidamente lo scopo della tua flotta.
6. Seleziona il tipo di flotta gestita dal servizio.
7. Scegli l'opzione di mercato con istanze Spot o On-Demand per la tua flotta. Le istanze Spot offrono una capacità non riservata che puoi utilizzare a un prezzo scontato, ma che possono

essere interrotte da richieste On-demand. Le istanze on demand hanno un prezzo al secondo, ma non hanno un impegno a lungo termine e non verranno interrotte. Per impostazione predefinita, le flotte utilizzano istanze Spot.

8. Facoltativo: imposta il numero massimo di istanze per scalare il parco istanze in modo che la capacità sia disponibile per i lavori in coda. Ti consigliamo di lasciare il numero minimo di istanze impostato su **0** per garantire che il parco istanze rilasci tutte le istanze quando non ci sono lavori in coda.
9. Per accedere al servizio per la tua flotta, seleziona un ruolo esistente o creane uno nuovo. Un ruolo di servizio fornisce le credenziali alle istanze del parco istanze, concedendo loro l'autorizzazione a elaborare i lavori, e agli utenti del monitor, in modo che possano leggere le informazioni di registro.
10. Seleziona Successivo.
11. Inserisci le vCPU minime e massime necessarie per la tua flotta.
12. Inserisci la memoria minima e massima di cui hai bisogno per il tuo parco macchine.
13. Facoltativo Puoi scegliere di consentire o escludere tipi di istanze specifici dal tuo parco istanze per assicurarti che solo quei tipi di istanze vengano utilizzati per questo parco istanze.
14. Facoltativo Puoi specificare la dimensione del volume gp3 di Amazon Elastic Block Store (Amazon EBS) che verrà collegato ai lavoratori di questa flotta. Per ulteriori informazioni, consulta la guida per l'utente di EBS.
15. Seleziona Successivo.
16. Facoltativo Definisci i requisiti personalizzati dei lavoratori che definiscono le caratteristiche di questa flotta che possono essere combinati con i requisiti personalizzati dell'host specificati negli invii di lavoro. Un esempio è un tipo di licenza particolare se prevedi di connettere la tua flotta al tuo server di licenze.
17. Seleziona Successivo.
18. Facoltativo Per associare la tua flotta a una coda, seleziona una coda dal menu a discesa. Se la coda è impostata con l'ambiente di Conda coda predefinito, alla flotta vengono automaticamente forniti pacchetti che supportano le applicazioni e i renderer DCC dei partner. Per un elenco dei pacchetti forniti, consulta. Ambiente di Conda coda predefinito
19. Seleziona Successivo.
20. Facoltativo Per aggiungere un tag alla tua flotta, scegli Aggiungi nuovo tag, quindi inserisci la chiave e il valore per quel tag.
21. Seleziona Successivo.

22. Controlla le impostazioni del parco veicoli, quindi scegli Crea flotta. Dopo la creazione, viene visualizzata la tua flotta.

Compatibilità VFX Reference Platform

VFX Reference PlatformÈ una piattaforma di destinazione comune per il settore degli effetti visivi. Per utilizzare l'istanza Amazon EC2 standard con flotta gestita dai servizi che esegue Amazon Linux 2023 con software che supporta VFX Reference Platform il, è necessario tenere a mente le seguenti considerazioni quando si utilizza una flotta gestita dai servizi.

Viene aggiornato ogni anno. VFX Reference Platform Queste considerazioni sull'utilizzo di un AL2023, che include le flotte gestite dai servizi Deadline Cloud, si basano sulle piattaforme di riferimento per l'anno solare (CY) dal 2022 al 2024. Per ulteriori informazioni, consulta VFX Reference Platform.

> **Note**
>
> Se stai creando una soluzione personalizzata Amazon Machine Image (AMI) per una flotta gestita dal cliente, puoi aggiungere questi requisiti quando prepari l'istanza Amazon EC2.

Per utilizzare il software VFX Reference Platform supportato su un'istanza Amazon EC2 AL2023, considera quanto segue:

- La versione glibc installata con AL2023 è compatibile per l'uso in fase di esecuzione, ma non per la creazione di software compatibile con CY2024 o versioni precedenti. VFX Reference Platform
- Python 3.9 e 3.11 sono forniti con la flotta gestita dai servizi che lo rende compatibile con CY2022 e CY2024. VFX Reference Platform Python 3.7 e 3.10 non sono forniti nella flotta gestita dai servizi. Il software che li richiede deve fornire l'installazione di Python nella coda o nell'ambiente di lavoro.
- Alcuni componenti della libreria Boost forniti nella flotta gestita dai servizi sono la versione 1.75, che non è compatibile con. VFX Reference Platform Se l'applicazione utilizza Boost, è necessario fornire la propria versione della libreria per motivi di compatibilità.
- L'aggiornamento Intel TBB 3 è fornito nella flotta gestita dai servizi. È compatibile con VFX Reference Platform CY2022, CY2023 e CY2024.

- Altre librerie con versioni specificate da non VFX Reference Platform sono fornite dalla flotta gestita dal servizio. È necessario fornire alla libreria qualsiasi applicazione utilizzata in una flotta gestita dai servizi. Per un elenco delle librerie, consulta la piattaforma di riferimento.

Gestisci le flotte gestite dai clienti di Deadline Cloud

Questa sezione spiega come gestire una flotta gestita dal cliente (CMF) per Deadline Cloud.

I CMF sono flotte di lavoratori che gestisci. Un CMF può risiedere all'interno AWS dell'infrastruttura, in sede o in un data center condiviso. Un CMF fornisce il pieno controllo e la responsabilità della flotta. Ciò include il rifornimento, le operazioni, la gestione e lo smantellamento dei lavoratori della flotta.

Argomenti

- Crea una flotta gestita dai clienti
- Configurazione e configurazione dell'host di lavoro
- Gestisci l'accesso ai segreti degli utenti dei job di Windows
- Installa e configura il software necessario per i lavori
- Configurazione delle credenziali AWS
- Creazione di un Amazon Machine Image
- Crea un'infrastruttura per il parco veicoli con un gruppo Amazon EC2 Auto Scaling
- Connect le flotte gestite dai clienti a un endpoint di licenza

Crea una flotta gestita dai clienti

Per creare una flotta gestita dal cliente (CMF), completa i seguenti passaggi.

Deadline Cloud console

Per utilizzare la console Deadline Cloud per creare una flotta gestita dal cliente

1. Apri la console Deadline Cloud.
2. Seleziona Fattorie. Viene visualizzato un elenco di fattorie disponibili.
3. Seleziona il nome della fattoria in cui vuoi lavorare.
4. Seleziona la scheda Flotte.
5. Scegliere Create Fleet (Crea parco istanze).

6. Inserisci un nome per la tua flotta.
7. (Facoltativo) Inserisci una descrizione per la tua flotta.
8. Seleziona Gestito dal cliente per il tipo di flotta.
9. Seleziona un tipo di Auto Scaling. Per ulteriori informazioni, consultate Utilizzare EventBridge per gestire gli eventi di Auto Scaling.

   - Nessuna scalabilità: stai creando una flotta locale e desideri rinunciare a Deadline Cloud Auto Scaling.
   - Consigli di scalabilità: stai creando una flotta Amazon Elastic Compute Cloud (Amazon EC2).

10. Seleziona l'accesso ai servizi del tuo parco veicoli.

    a. Ti consigliamo di utilizzare l'opzione Crea e utilizza un nuovo ruolo di servizio per ogni flotta per un controllo più granulare delle autorizzazioni. Questa opzione è selezionata per impostazione predefinita.

    b. Puoi anche utilizzare un ruolo di servizio esistente selezionando Scegli un ruolo di servizio.

11. Controlla le tue selezioni, quindi scegli Avanti.
12. Seleziona un sistema operativo per la tua flotta. Tutti i dipendenti della flotta devono disporre di un sistema operativo comune.
13. Seleziona l'architettura della CPU host.
14. Seleziona i seguenti requisiti hardware per gli host di lavoro di questo parco macchine.

    a. Seleziona i requisiti hardware minimi e massimi di vCPU e memoria per soddisfare le esigenze di carico di lavoro delle tue flotte.

    b. (Facoltativo) Seleziona i requisiti della GPU, quindi inserisci le GPU minime e massime.

15. Controlla le tue selezioni, quindi scegli Avanti.
16. (Facoltativo) Definisci i requisiti personalizzati dei lavoratori.
17. Utilizzando il menu a discesa, seleziona una o più code da associare alla flotta.

> **Note**
>
> Ti consigliamo di associare un parco veicoli solo a code che si trovano tutte all'interno dello stesso limite di trust. Ciò garantisce un forte limite di sicurezza tra l'esecuzione di lavori sullo stesso lavoratore.

18. Controlla le associazioni delle code, quindi seleziona Avanti.
19. (Facoltativo) Per l'ambiente di coda Conda predefinito, creeremo un ambiente per la coda che installerà i pacchetti Conda richiesti dai lavori.

> **Note**
>
> L'ambiente di coda Conda viene utilizzato per installare i pacchetti Conda richiesti dai lavori. In genere, è necessario deselezionare l'ambiente di coda Conda sulle code associate ai CMF perché nei CMF non verranno installati i comandi Conda richiesti per impostazione predefinita.

20. (Facoltativo) Aggiungi tag al tuo CMF. Per ulteriori informazioni, consulta Taggare le AWS risorse.
21. Rivedi la configurazione del tuo parco veicoli e apporta eventuali modifiche.
22. Scegliere Create Fleet (Crea parco istanze).
23. Seleziona la scheda Flotte, quindi annota l'ID della flotta.

AWS CLI

Da utilizzare per AWS CLI creare una flotta gestita dal cliente

1. Apri il. AWS CLI
2. Modificare `fleet-trust-policy.json`.
   a. Aggiungi la seguente politica IAM, sostituendo il testo IN *CORSIVO con l'*ID AWS dell'account e l'ID della fattoria Deadline Cloud.

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

```
            "Effect": "Allow",
            "Principal": {
                "Service": "credentials.deadline.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:deadline:*:ACCOUNT_ID:farm/FARM_ID"
                }
            }
        }
    ]
}
```

b. Salvare le modifiche.

3. Modificare `create-cmf-fleet.json`.

   a. Aggiungi la seguente politica IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "deadline:AssumeFleetRoleForWorker",
                "deadline:UpdateWorker",
                "deadline:DeleteWorker",
                "deadline:UpdateWorkerSchedule",
                "deadline:BatchGetJobEntity",
                "deadline:AssumeQueueRoleForWorker"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
            }
        }
    ]
}
```

b. Salvare le modifiche.

4. Aggiungi un ruolo IAM da utilizzare per i lavoratori della tua flotta.

```
aws iam create-role --role-name FleetWorkerRoleName --assume-role-policy-
document file://fleet-trust-policy.json
aws iam put-role-policy --role-name FleetWorkerRoleName --policy-name
 FleetWorkerPolicy --policy-document file://fleet-policy.json
```

5. Modificare `create-fleet-request.json`.

   a. Aggiungi la seguente policy IAM, sostituendo il testo IN CORSIVO con i valori del tuo CMF.

> **Note**
>
> Puoi trovare *ROLE_ARN* in. `create-cmf-fleet.json`
> Per *OS_FAMILY*, devi scegliere uno tra, o. `linux` `macos` `windows`

```
{
    "farmId": "FARM_ID",
    "displayName": "FLEET_NAME",
    "description": "FLEET_DESCRIPTION",
    "roleArn": "ROLE_ARN",
    "minWorkerCount": 0,
    "maxWorkerCount": 10,
    "configuration": {
        "customerManaged": {
            "mode": "NO_SCALING",
            "workerCapabilities": {
                "vCpuCount": {
                    "min": 1,
                    "max": 4
                },
                "memoryMiB": {
                    "min": 1024,
                    "max": 4096
                },
                "osFamily": "OS_FAMILY",
                "cpuArchitectureType": "x86_64",
            },
        },
    }
}
```

b. Salvare le modifiche.

6. Crea la tua flotta.

```
aws deadline create-fleet --cli-input-json file://create-fleet-request.json
```

Configurazione e configurazione dell'host di lavoro

Un worker host si riferisce a una macchina host che esegue un worker Deadline Cloud. Questa sezione spiega come configurare l'host di lavoro e configurarlo per esigenze specifiche. Ogni worker host esegue un programma chiamato worker agent. L'agente di lavoro è responsabile di:

- Gestione del ciclo di vita del lavoratore.
- Sincronizzazione del lavoro assegnato, dello stato di avanzamento e dei risultati.
- Monitoraggio del lavoro in corso.
- Inoltro dei log a destinazioni configurate.

Ti consigliamo di utilizzare l'agente di lavoro Deadline Cloud fornito. Il worker agent è open source e incoraggiamo la richiesta di funzionalità, ma puoi anche svilupparlo e personalizzarlo in base alle tue esigenze.

Per completare le attività descritte nelle seguenti sezioni, è necessario quanto segue:

Linux

- Un'istanza Amazon Elastic Compute Cloud (Amazon EC2) Linux basata su Amazon Elastic Compute Cloud (Amazon EC2). Consigliamo Amazon Linux 2023.
- `sudo`privilegi.
- Python 3.9 o versioni successive.

Windows

- Un'istanza Amazon Elastic Compute Cloud (Amazon EC2) Windows basata su Amazon Elastic Compute Cloud (Amazon EC2). Consigliamo. Windows Server 2022
- Accesso dell'amministratore all'host del lavoratore
- Python 3.9 o superiore installato per tutti gli utenti

Creare e configurare un ambiente virtuale Python

Puoi creare un ambiente virtuale Python su Linux se hai installato Python 3.9 o versione successiva e lo hai inserito nel tuo. `PATH`

Per creare e attivare un ambiente virtuale Python

1. Apri il. AWS CLI
2. Crea e attiva un ambiente virtuale Python.

```
python3 -m venv /opt/deadline/worker
source /opt/deadline/worker/bin/activate
pip install --upgrade pip
```

Installa l'agente di lavoro Deadline Cloud

Dopo aver configurato Python e creato un ambiente virtualeLinux, installa i pacchetti Python dell'agente di lavoro di Deadline Cloud.

Per installare i pacchetti Python dell'agente di lavoro

1. Apri un terminale.
   a. SìLinux, apri un terminale come `root` utente (o usa`sudo`/`su`)
   b. AttivatoWindows, apri il prompt dei comandi o il PowerShell terminale dell'amministratore.
2. Scarica e installa i pacchetti Deadline Cloud worker agent da PyPI:

> **Note**
>
> SìWindows, i file dell'agente devono essere installati nella directory globale dei pacchetti del sito di Python. Gli ambienti virtuali Python non sono attualmente supportati.

```
python -m pip install deadline-cloud-worker-agent
```

Configura l'agente di lavoro Deadline Cloud

Puoi configurare le impostazioni dell'agente Deadline Cloud Worker in tre modi. Ti consigliamo di utilizzare il sistema operativo configurato tramite`install-deadline-worker`.

Argomenti della riga di comando: puoi specificare gli argomenti quando esegui l'agente di lavoro Deadline Cloud dalla riga di comando. Alcune impostazioni di configurazione non sono disponibili tramite gli argomenti della riga di comando. Per visualizzare tutti gli argomenti disponibili nella riga di comando, digitare `deadline-worker-agent --help` per visualizzare tutti gli argomenti disponibili nella riga di comando.

Variabili di ambiente: puoi configurare l'agente di lavoro di Deadline Cloud impostando la variabile di ambiente che inizia con`DEADLINE_WORKER_`. Ad esempio, puoi utilizzare `export DEADLINE_WORKER_VERBOSE=true` per impostare l'output del worker agent su verboso. Per ulteriori esempi e informazioni, vedere `/etc/amazon/deadline/worker.toml.example` on Linux or `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` onWindows.

File di configurazione: quando si installa il worker agent, viene creato un file di configurazione che si trova in `/etc/amazon/deadline/worker.toml` on Linux o `C:\ProgramData\Amazon\Deadline\Config\worker.toml` onWindows. Il worker agent carica questo file di configurazione all'avvio. È possibile utilizzare il file di configurazione di esempio (`/etc/amazon/deadline/worker.toml.example`Linux`C:\ProgramData\Amazon\Deadline\Config\worker.toml.example`acceso o attivatoWindows) per personalizzare il file di configurazione del worker agent predefinito in base alle proprie esigenze specifiche.

Infine, ti consigliamo di abilitare lo spegnimento automatico per l'agente di lavoro. Ciò consente alla flotta di lavoratori di ampliarsi quando necessario e di arrestarsi al termine del lavoro di rendering. La scalabilità automatica aiuta a garantire l'utilizzo delle risorse solo se necessario.

Per abilitare lo spegnimento automatico

Come utente: **`root`**

- Installa l'agente di lavoro con i parametri**`--allow-shutdown`**.

  Linux

  Inserisci:

```
/opt/deadline/worker/bin/install-deadline-worker \
```

```
  --farm-id FARM_ID \
  --fleet-id FLEET_ID \
  --region REGION \
  --allow-shutdown
```

Windows

Inserisci:

```
install-deadline-worker ^
  --farm-id FARM_ID ^
  --fleet-id FLEET_ID ^
  --region REGION ^
  --allow-shutdown
```

Crea utenti e gruppi di lavoro

Questa sezione descrive la relazione utente e di gruppo richiesta tra l'utente agente e quella `jobRunAsUser` definita nelle code.

Il worker agent di Deadline Cloud deve funzionare come utente dedicato specifico dell'agente sull'host. È necessario configurare la `jobRunAsUser` proprietà delle code di Deadline Cloud in modo che i lavoratori eseguano i lavori in coda come utenti e gruppi specifici del sistema operativo. Ciò significa che puoi controllare le autorizzazioni condivise del file system di cui dispongono i tuoi lavori. Fornisce inoltre un importante limite di sicurezza tra i lavori e l'utente worker agent.

Linuxutenti e gruppi di lavoro

Per configurare il tuo agente-utente`jobRunAsUser`, assicurati di soddisfare i seguenti requisiti:

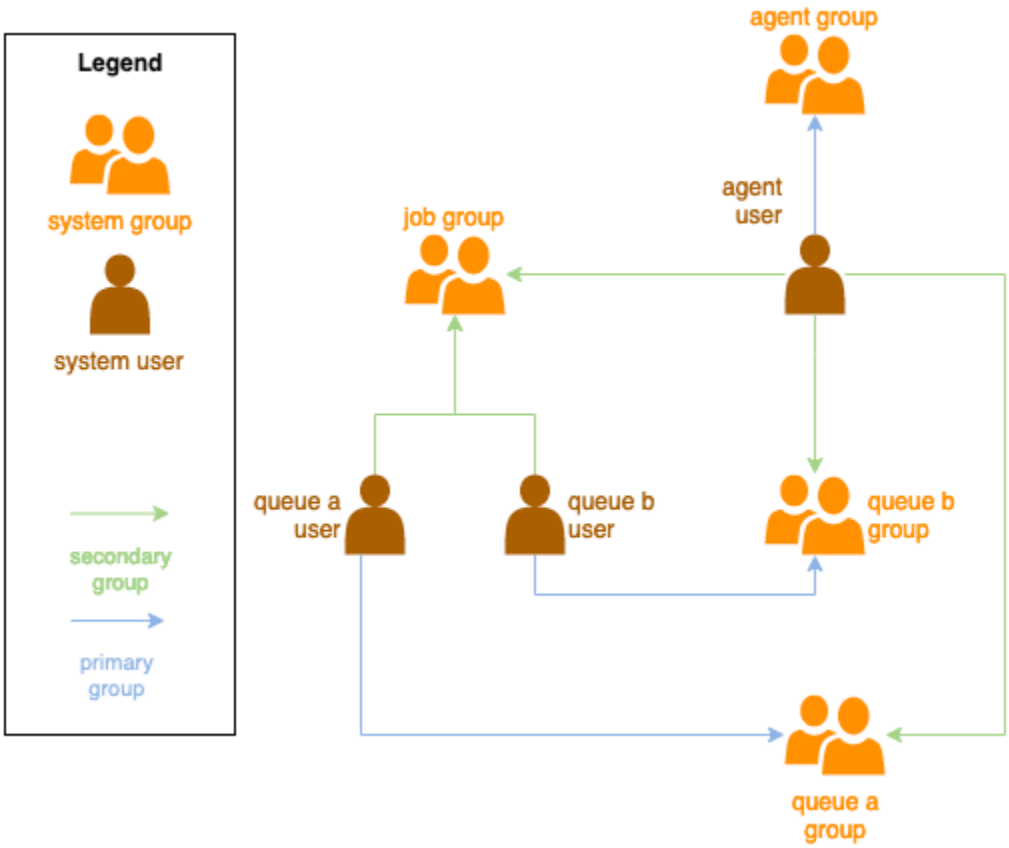
- Esiste un gruppo per ciascuno `jobRunAsUser` ed è il gruppo principale per il corrispondente. `jobRunAsUser`
- L'agente-utente appartiene al gruppo primario delle code in cui `jobRunAsUser` il lavoratore ottiene lavoro. Per le migliori pratiche di sicurezza, consigliamo questo gruppo come gruppo secondario di agente-utente. Questo gruppo condiviso consente all'agente di lavoro di rendere disponibili i file per il lavoro mentre è in esecuzione.
- A `jobRunAsUser` non appartiene al gruppo principale dell'agente-utente. Per le migliori pratiche di sicurezza:
  - I file sensibili scritti dall'agente di lavoro sono di proprietà del gruppo principale dell'agente.

  - Se un `jobRunAsUser` appartiene a questo gruppo, i file scritti dal worker agent possono essere accessibili dai lavori inviati alla coda in esecuzione sul worker.
- La AWS regione predefinita deve corrispondere alla regione dell'azienda agricola a cui appartiene il lavoratore. Per ulteriori informazioni, vedere Impostazioni dei file di configurazione e credenziali.

  Questo dovrebbe essere applicato a:

  - L'agente-utente
  - Tutti gli account in coda `jobRunAsUser` sul lavoratore
- L'agente-utente può eseguire `sudo` comandi come. `jobRunAsUser`

Il diagramma seguente illustra la relazione tra l'utente agente e `jobRunAsUser` gli utenti e i gruppi per le code associate alla flotta.



Utenti Windows

Per utilizzare un Windows utente come`jobRunAsUser`, deve soddisfare i seguenti requisiti:

- Tutti gli `jobRunAsUser` utenti della coda devono esistere.

- Le loro password devono corrispondere al valore del segreto specificato nel campo della coda. `JobRunAsUser` Per istruzioni, vedere il passaggio 7 in. Crea una coda
- L'utente-agente deve essere in grado di accedere come tali utenti.

Gestisci l'accesso ai segreti degli utenti dei job di Windows

Quando si configura una coda con Windows`jobRunAsUser`, è necessario specificare un segreto di AWS Secrets Manager. Il valore di questo segreto dovrebbe essere un oggetto del modulo con codifica JSON:

```
{
    "password": "JOB_USER_PASSWORD"
}
```

Affinché Workers esegua i job secondo la configurazione della coda`jobRunAsUser`, il ruolo IAM della flotta deve disporre delle autorizzazioni necessarie per ottenere il valore del segreto. Se il segreto è crittografato utilizzando una chiave KMS gestita dal cliente, anche il ruolo IAM della flotta deve disporre delle autorizzazioni per la decrittografia utilizzando la chiave KMS.

Si consiglia vivamente di seguire il principio del privilegio minimo per questi segreti. Ciò significa che l'accesso per recuperare il valore segreto di → → di una coda dovrebbe essere: `jobRunAsUser` `windows` `passwordArn`

- concesso a un ruolo di flotta quando viene creata un'associazione queue-fleet tra la flotta e la coda
- revocato da un ruolo di flotta quando viene eliminata un'associazione queue-fleet tra la flotta e la coda

Inoltre, il segreto di AWS Secrets Manager contenente la `jobRunAsUser` password deve essere eliminato quando non viene più utilizzato.

Concedi l'accesso a una password segreta

Le flotte Deadline Cloud richiedono l'accesso alla `jobRunAsUser` password memorizzata nella password segreta della coda quando coda e flotta sono associate. Ti consigliamo di utilizzare la politica delle risorse di AWS Secrets Manager per concedere l'accesso ai ruoli della flotta. Se ti attieni rigorosamente a queste linee guida, è più facile determinare quali ruoli della flotta hanno accesso al segreto.

Per concedere l'accesso al segreto

1. Apri la console AWS Secret Manager per accedere al segreto.
2. Nella sezione «Autorizzazioni per le risorse», aggiungi una dichiarazione politica nel modulo:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    // ...
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    // ...
  ]
}
```

Revoca l'accesso a una password segreta

Quando una flotta non richiede più l'accesso a una coda, rimuovi l'accesso alla password segreta per la coda. `jobRunAsUser` Ti consigliamo di utilizzare la politica delle risorse di AWS Secrets Manager per concedere l'accesso ai ruoli della flotta. Se ti attieni rigorosamente a queste linee guida, è più facile determinare quali ruoli della flotta hanno accesso al segreto.

Per revocare l'accesso al segreto

1. Apri la console AWS Secret Manager per accedere al segreto.
2. Nella sezione Autorizzazioni delle risorse, rimuovi la dichiarazione politica dal modulo:

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

```
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    // ...
  ]
}
```

Installa e configura il software necessario per i lavori

Dopo aver configurato l'agente di lavoro di Deadline Cloud, puoi preparare l'host di lavoro con qualsiasi software necessario per eseguire i lavori.

Quando invii un lavoro a una coda con un lavoro associato`jobRunAsUser`, il lavoro viene eseguito come tale utente. Tutti i comandi devono essere disponibili nella cartella `PATH` di quell'utente.

In Linux, è possibile specificare `PATH` per un utente in uno dei seguenti modi:

- loro `~/.bashrc` o `~/.bash_profile`
- file di configurazione del sistema come `/etc/profile.d/*` e `/etc/profile`
- script di avvio della shell:`/etc/bashrc`.

In Windows, è possibile specificare `PATH` per un utente in uno dei seguenti modi:

- le loro variabili di ambiente specifiche dell'utente
- le variabili di ambiente a livello di sistema

Installa gli adattatori per strumenti di creazione di contenuti digitali

Deadline Cloud fornisce applicazioni per la creazione di contenuti digitali (DCC) con supporto di integrazione di prime parti. Per utilizzare queste integrazioni su una flotta gestita dal cliente, è necessario installare il software DCC e gli adattatori.

Per installare gli adattatori DCC su una flotta gestita dal cliente

1. Apri il terminale a.

    a. Su Linux, apri un terminale come `root` utente (o usa`sudo`/`su`)

b. In Windows, apri il prompt dei comandi o il PowerShell terminale dell'amministratore.

2. Installa i pacchetti di adattatori Deadline Cloud.

```
pip install deadline deadline-cloud-for-maya deadline-cloud-for-nuke deadline-
cloud-for-blender
```

Configurazione delle credenziali AWS

Questa sezione spiega come configurare le AWS credenziali.

Questa fase iniziale del ciclo di vita del lavoratore è di tipo bootstrap. In questa fase, il software Worker Agent crea un lavoratore nella vostra flotta e ottiene AWS le credenziali del ruolo del parco macchine per ulteriori operazioni.

AWS credentials for Amazon EC2

Per configurare AWS le credenziali per Amazon EC2

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Seleziona Ruoli nel riquadro di navigazione, quindi Crea ruolo.
3. Seleziona AWS servizio.
4. Seleziona EC2 come servizio o caso d'uso, quindi seleziona Avanti.
5. Allega la politica `AWSDeadlineCloud-WorkerHost` AWS gestita.

On-premise AWS credentials

Per configurare le AWS credenziali locali

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Seleziona Ruoli nel riquadro di navigazione, quindi Crea ruolo.
3. Seleziona Account AWS, quindi seleziona Avanti.
4. Allega la politica `AWSDeadlineCloud-WorkerHost` AWS gestita.
5. Genera chiavi segrete e di accesso AWS IAM per l'utente IAM:

   a. Per IAM Role Anywhere, consulta IAM Roles Anywhere.

b. Per il modo più sicuro per configurare le credenziali sull'host, consulta Ottenere credenziali di sicurezza temporanee da AWS Identity and Access Management Roles Anywhere.

c. Puoi anche utilizzare la CLI come autenticazione alternativa, per maggiori informazioni consulta Autenticazione con le credenziali utente IAM.

6. Memorizza queste chiavi nel file delle AWS credenziali dell'agente-utente sul filesystem dell'host di lavoro.

   a. Su Linux, questo si trova in `~/.aws/credentials`

   b. Su Windows, si trova in `%USERPROFILE%\.aws\credentials`

> **Note**
>
> Le credenziali devono essere accessibili solo dal nome utente del sistema operativo (`deadline-worker-agent`) che ha installato il worker agent.

```
# Replace keys below
[default]
aws_access_key_id=ACCESS_KEY_ID
aws_secret_access_key=SECRET_ACCESSS_KEY
```

7. Cambia il `deadline-worker-agent` proprietario e le autorizzazioni.

> **Note**
>
> Se hai cambiato il nome utente del sistema operativo (`deadline-worker-agent`) quando hai installato il worker agent, usa invece quel nome.

Creazione di un Amazon Machine Image

Per creare un Amazon Machine Image (AMI) da utilizzare in una flotta Amazon Elastic Compute Cloud (Amazon EC2) gestita dai clienti (CMF), completa le attività in questa sezione. È necessario creare un'istanza Amazon EC2 prima di procedere. Per ulteriori informazioni, consulta Launch your istance nella Amazon EC2 User Guide for Linux Instances.

> **Important**
>
> La creazione e la AMI creazione di uno snapshot dei volumi collegati all'istanza Amazon EC2. Qualsiasi software installato sull'istanza persiste, così come le istanze, che vengono riutilizzate quando si avviano istanze da. AMI Ti consigliamo di adottare una strategia di patching e di aggiornare regolarmente qualsiasi nuovo software aggiornato prima di applicarlo AMI alla tua flotta.

Preparare l'istanza Amazon EC2

Prima di crearne unaAMI, devi eliminare lo stato del lavoratore. Lo stato del lavoratore persiste tra un avvio e l'altro del worker agent. Se questo stato persiste suAMI, tutte le istanze avviate da esso condivideranno lo stesso stato.

Ti consigliamo inoltre di eliminare tutti i file di registro esistenti. I file di log possono rimanere su un'istanza Amazon EC2 durante la preparazione dell'AMI. L'eliminazione di questi file riduce al minimo la confusione durante la diagnosi di possibili problemi nelle flotte di lavoratori che utilizzano l'AMI.

È inoltre necessario abilitare il servizio di sistema worker agent in modo che l'agente worker di Deadline Cloud venga avviato all'avvio di Amazon EC2.

Infine, ti consigliamo di abilitare lo spegnimento automatico dell'agente di lavoro. Ciò consente alla flotta di lavoratori di ampliarsi quando necessario e di arrestarsi al termine del lavoro di rendering. Questa scalabilità automatica aiuta a garantire l'utilizzo delle risorse solo se necessario.

Per preparare l'istanza Amazon EC2

1. Aprire la console Amazon EC2.
2. Avviare un'istanza Amazon EC2 Per ulteriori informazioni, consulta Launch your instance.
3. Configura l'host per la connessione al tuo provider di identità (IdP), quindi monta qualsiasi file system condiviso di cui ha bisogno.
4. Segui i tutorial per, quindi, e. Installa l'agente di lavoro Deadline Cloud Configura l'agente di lavoro Crea utenti e gruppi di lavoro
5. Se stai preparando un programma AMI basato su Amazon Linux 2023 per eseguire software compatibile con la piattaforma di riferimento VFX, devi aggiornare diversi requisiti. Per informazioni, consulta Compatibilità VFX Reference Platform.

6. Apri un terminale.

    a. Su Linux, apri un terminale come `root` utente (o usa`sudo`/`su`)

    b. In Windows, apri il prompt dei comandi o il PowerShell terminale dell'amministratore.

7. Assicurati che il servizio di lavoro non sia in esecuzione e configurato per l'avvio all'avvio:

    a. Su Linux, esegui

    ```
    systemctl stop deadline-worker
    systemctl enable deadline-worker
    ```

    b. Su Windows, esegui

    ```
    sc.exe stop DeadlineWorker
    sc.exe config DeadlineWorker start= auto
    ```

8. Eliminare lo stato del lavoratore.

    a. Su Linux, esegui

    ```
    rm -rf /var/lib/deadline/*
    ```

    b. Su Windows, esegui

    ```
    del /Q /S %PROGRAMDATA%\Amazon\Deadline\Cache\*
    ```

9. Eliminare i file di registro.

    a. Su Linux, esegui

    ```
    rm -rf /var/log/amazon/deadline/*
    ```

    b. Su Windows, esegui

    ```
    del /Q /S %PROGRAMDATA%\Amazon\Deadline\Logs\*
    ```

10. Su Windows, si consiglia di eseguire l'applicazione Amazon EC2Launch Settings disponibile nel menu Start per completare la preparazione finale dell'host e lo spegnimento dell'istanza.

> **Note**
>
> DEVI scegliere Shutdown senza Sysprep e non scegliere mai Shutdown with Sysprep. L'arresto con Sysprep renderà inutilizzabili tutti gli utenti locali. Per ulteriori informazioni, consulta la sezione Prima di iniziare dell'argomento Creare un'AMI personalizzata della Guida utente per le istanze di Windows.

Costruisci il AMI

Per costruire il AMI

1. Aprire la console Amazon EC2.
2. Seleziona Istanze nel riquadro di navigazione, quindi seleziona la tua istanza.
3. Scegli lo stato dell'istanza, quindi Arresta l'istanza.
4. Dopo che l'istanza è stata interrotta, scegli Azioni.
5. Scegli Immagine e modelli, quindi Crea immagine.
6. Inserisci un nome per l'immagine.
7. (Facoltativo) Inserisci una descrizione per l'immagine.
8. Scegliere Create Image (Crea immagine).

Crea un'infrastruttura per il parco veicoli con un gruppo Amazon EC2 Auto Scaling

Questa sezione spiega come creare una flotta Amazon EC2 Auto Scaling.

Utilizza il modello AWS CloudFormation YAML riportato di seguito per creare un gruppo Amazon EC2 Auto Scaling (Auto Scaling), un Amazon Virtual Private Cloud (Amazon VPC) con due sottoreti, un profilo di istanza e un ruolo di accesso all'istanza. Questi sono necessari per avviare l'istanza utilizzando Auto Scaling nelle sottoreti.

È necessario rivedere e aggiornare l'elenco dei tipi di istanze per adattarlo alle proprie esigenze di rendering.

Per creare una flotta Amazon EC2 Auto Scaling

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Crea un CloudFormation modello con parametri `Farm ID`, `Fleet ID`, e `AMI ID`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Amazon Deadline Cloud customer-managed fleet
Parameters:
  FarmId:
    Type: String
    Description: Farm ID
  FleetId:
    Type: String
    Description: Fleet ID
  AMIId:
    Type: String
    Description: AMI ID for launcing Workers
Resources:
  deadlineVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: 100.100.0.0/16
  deadlineWorkerSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: !Join
        - ' '
        - - Security Group created for deadline workers in fleet
          - !Ref FleetId
      GroupName: !Join
        - ''
        - - deadlineWorkerSecurityGroup-
          - !Ref FleetId
      SecurityGroupEgress:
        - CidrIp: 0.0.0.0/0
          IpProtocol: '-1'
      SecurityGroupIngress: []
      VpcId: !Ref deadlineVPC
  deadlineIGW:
    Type: 'AWS::EC2::InternetGateway'
    Properties: {}
  deadlineVPCGatewayAttachment:
    Type: 'AWS::EC2::VPCGatewayAttachment'
    Properties:
```

```
      VpcId: !Ref deadlineVPC
      InternetGatewayId: !Ref deadlineIGW
  deadlinePublicRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref deadlineVPC
  deadlinePublicRoute:
    Type: 'AWS::EC2::Route'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref deadlineIGW
    DependsOn:
      - deadlineIGW
      - deadlineVPCGatewayAttachment
  deadlinePublicSubnet0:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.16.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - a
  deadlineSubnetRouteTableAssociation0:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet0
  deadlinePublicSubnet1:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.20.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - c
  deadlineSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet1
  deadlineInstanceAccessAccessRole:
```

```
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Join
        - '-'
        - - deadline
          - InstanceAccess
          - !Ref FleetId
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      Path: /
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy'
        - 'arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore'
        - 'arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost'
  deadlineInstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Path: /
      Roles:
        - !Ref deadlineInstanceAccessAccessRole
  deadlineLaunchTemplate:
    Type: 'AWS::EC2::LaunchTemplate'
    Properties:
      LaunchTemplateName: !Join
        - ''
        - - deadline-LT-
          - !Ref FleetId
      LaunchTemplateData:
        NetworkInterfaces:
          - DeviceIndex: 0
            AssociatePublicIpAddress: true
            Groups:
              - !Ref deadlineWorkerSecurityGroup
            DeleteOnTermination: true
        ImageId: !Ref AMIId
        InstanceInitiatedShutdownBehavior: terminate
        IamInstanceProfile:
          Arn: !GetAtt
            - deadlineInstanceProfile
```

```
            - Arn
        MetadataOptions:
          HttpTokens: required
          HttpEndpoint: enabled

  deadlineAutoScalingGroup:
    Type: 'AWS::AutoScaling::AutoScalingGroup'
    Properties:
      AutoScalingGroupName: !Join
        - ''
        - - deadline-ASG-autoscalable-
          - !Ref FleetId
      MinSize: 0
      MaxSize: 10
      VPCZoneIdentifier:
        - !Ref deadlinePublicSubnet0
        - !Ref deadlinePublicSubnet1
      NewInstancesProtectedFromScaleIn: true
      MixedInstancesPolicy:
        InstancesDistribution:
          OnDemandBaseCapacity: 0
          OnDemandPercentageAboveBaseCapacity: 0
          SpotAllocationStrategy: capacity-optimized
          OnDemandAllocationStrategy: lowest-price
        LaunchTemplate:
          LaunchTemplateSpecification:
            LaunchTemplateId: !Ref deadlineLaunchTemplate
            Version: !GetAtt
              - deadlineLaunchTemplate
              - LatestVersionNumber
          Overrides:
            - InstanceType: m5.large
            - InstanceType: m5d.large
            - InstanceType: m5a.large
            - InstanceType: m5ad.large
            - InstanceType: m5n.large
            - InstanceType: m5dn.large
            - InstanceType: m4.large
            - InstanceType: m3.large
            - InstanceType: r5.large
            - InstanceType: r5d.large
            - InstanceType: r5a.large
            - InstanceType: r5ad.large
            - InstanceType: r5n.large
```

```
            - InstanceType: r5dn.large
            - InstanceType: r4.large
      MetricsCollection:
        - Granularity: 1Minute
          Metrics:
            - GroupMinSize
            - GroupMaxSize
            - GroupDesiredCapacity
            - GroupInServiceInstances
            - GroupTotalInstances
            - GroupInServiceCapacity
            - GroupTotalCapacity
```

3. Dopo aver creato i ruoli IAM, devi riconoscere quanto segue:

   - Le credenziali del ruolo IAM collegate all'istanza Amazon EC2 del lavoratore sono disponibili per tutti i processi in esecuzione su quel lavoratore, compresi i job. Il lavoratore deve avere i privilegi minimi per operare: e `deadline:CreateWorker` `deadline:AssumeFleetRoleForWorker.`
   - L'agente di lavoro ottiene le credenziali per il ruolo di coda e le configura per l'utilizzo da parte dell'esecuzione dei job. Il ruolo del profilo dell'istanza Amazon EC2 non dovrebbe includere le autorizzazioni necessarie per i tuoi lavori.

Ridimensiona automaticamente la tua flotta Amazon EC2 con la funzionalità di raccomandazione di scalabilità Deadline Cloud

Deadline Cloud sfrutta un gruppo Amazon EC2 Auto Scaling (Auto Scaling) per scalare automaticamente la flotta gestita dai clienti (CMF) di Amazon EC2. Devi configurare la modalità flotta e implementare l'infrastruttura richiesta nel tuo account per far crescere automaticamente la tua flotta. L'infrastruttura che hai implementato funzionerà per tutte le flotte, quindi dovrai configurarla una sola volta.

Il flusso di lavoro di base è: configuri la modalità flotta per la scalabilità automatica, quindi Deadline Cloud invierà un EventBridge evento per quella flotta ogni volta che la dimensione della flotta consigliata cambia (un evento contiene l'ID della flotta, la dimensione della flotta consigliata e altri metadati). Avrai una EventBridge regola per filtrare gli eventi rilevanti e avrai una Lambda per consumarli. Lambda si integrerà con Amazon EC2 Auto Scaling per scalare `AutoScalingGroup` automaticamente la flotta Amazon EC2.

Imposta la modalità flotta su **EVENT_BASED_AUTO_SCALING**

Configura la modalità flotta suEVENT_BASED_AUTO_SCALING. Puoi utilizzare la console per eseguire questa operazione oppure utilizzare la AWS CLI per chiamare direttamente l'UpdateFleetAPI CreateFleet or. Dopo aver configurato la modalità, Deadline Cloud inizia a inviare EventBridge eventi ogni volta che la dimensione della flotta consigliata cambia.

- UpdateFleetComando di esempio:

```
aws deadline update-fleet \
  --farm-id FARM_ID \
  --fleet-id FLEET_ID \
  --configuration file://configuration.json
```

- CreateFleetComando di esempio:

```
aws deadline create-fleet \
  --farm-id FARM_ID \
  --display-name "Fleet name" \
  --max-worker-count 10 \
  --configuration file://configuration.json
```

Di seguito è riportato un esempio di configuration.json utilizzo dei comandi CLI precedenti (--configuration file://configuration.json.

- Per abilitare Auto Scaling sulla tua flotta, devi impostare la modalità su. EVENT_BASED_AUTO_SCALING
- workerCapabilitiesSono i valori predefiniti assegnati al CMF al momento della sua creazione. È possibile modificare questi valori se è necessario aumentare le risorse disponibili per il CMF.

Dopo aver configurato la modalità flotta, Deadline Cloud inizia a emettere eventi di raccomandazione sulle dimensioni della flotta per quella flotta.

```
{
    "customerManaged": {
        "mode": "EVENT_BASED_AUTO_SCALING",
        "workerCapabilities": {
            "vCpuCount": {
                "min": 1,
```

```
                "max": 4
            },
            "memoryMiB": {
                "min": 1024,
                "max": 4096
            },
            "osFamily": "linux",
            "cpuArchitectureType": "x86_64",
        }
    }
}
```

Implementa lo stack Auto Scaling utilizzando il modello AWS CloudFormation

Puoi impostare una EventBridge regola per filtrare gli eventi, una Lambda per consumare gli eventi e controllare l'Auto Scaling e una coda SQS per archiviare gli eventi non elaborati. Usa il seguente AWS CloudFormation modello per distribuire tutto in uno stack. Dopo aver distribuito correttamente le risorse, puoi inviare un lavoro e la flotta aumenterà automaticamente.

```
Resources:
  AutoScalingLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |-
          """
          This lambda is configured to handle "Fleet Size Recommendation Change"
          messages. It will handle all such events, and requires
          that the ASG is named based on the fleet id. It will scale up/down the fleet
          based on the recommended fleet size in the message.

          Example EventBridge message:
          {
              "version": "0",
              "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
              "detail-type": "Fleet Size Recommendation Change",
              "source": "aws.deadline",
              "account": "111122223333",
              "time": "2017-12-22T18:43:48Z",
              "region": "us-west-1",
              "resources": [],
              "detail": {
                  "farmId": "farm-12345678900000000000000000000000",
```

```
                "fleetId": "fleet-12345678900000000000000000000000",
                "oldFleetSize": 1,
                "newFleetSize": 5,
            }
        }
        """

        import json
        import boto3
        import logging

        logger = logging.getLogger()
        logger.setLevel(logging.INFO)

        auto_scaling_client = boto3.client("autoscaling")

        def lambda_handler(event, context):
            logger.info(event)
            event_detail = event["detail"]
            fleet_id = event_detail["fleetId"]
            desired_capacity = event_detail["newFleetSize"]

            asg_name = f"deadline-ASG-autoscalable-{fleet_id}"
            auto_scaling_client.set_desired_capacity(
                AutoScalingGroupName=asg_name,
                DesiredCapacity=desired_capacity,
                HonorCooldown=False,
            )

            return {
                'statusCode': 200,
                'body': json.dumps(f'Successfully set desired_capacity for {asg_name}
to {desired_capacity}')
            }
     Handler: index.lambda_handler
     Role: !GetAtt
       - AutoScalingLambdaServiceRole
       - Arn
     Runtime: python3.11
   DependsOn:
     - AutoScalingLambdaServiceRoleDefaultPolicy
     - AutoScalingLambdaServiceRole
 AutoScalingEventRule:
   Type: 'AWS::Events::Rule'
```

```
    Properties:
      EventPattern:
        source:
          - aws.deadline
        detail-type:
          - Fleet Size Recommendation Change
      State: ENABLED
      Targets:
        - Arn: !GetAtt
            - AutoScalingLambda
            - Arn
          DeadLetterConfig:
            Arn: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
          Id: Target0
          RetryPolicy:
            MaximumRetryAttempts: 15
  AutoScalingEventRuleTargetPermission:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !GetAtt
        - AutoScalingLambda
        - Arn
      Principal: events.amazonaws.com
      SourceArn: !GetAtt
        - AutoScalingEventRule
        - Arn
  AutoScalingLambdaServiceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: 'sts:AssumeRole'
            Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
        Version: 2012-10-17
      ManagedPolicyArns:
        - !Join
          - ''
          - - 'arn:'
            - !Ref 'AWS::Partition'
```

```
          - ':iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  AutoScalingLambdaServiceRoleDefaultPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyDocument:
        Statement:
          - Action: 'autoscaling:SetDesiredCapacity'
            Effect: Allow
            Resource: '*'
        Version: 2012-10-17
      PolicyName: AutoScalingLambdaServiceRoleDefaultPolicy
      Roles:
        - !Ref AutoScalingLambdaServiceRole
  UnprocessedAutoScalingEventQueue:
    Type: 'AWS::SQS::Queue'
    Properties:
      QueueName: deadline-unprocessed-autoscaling-events
    UpdateReplacePolicy: Delete
    DeletionPolicy: Delete
  UnprocessedAutoScalingEventQueuePolicy:
    Type: 'AWS::SQS::QueuePolicy'
    Properties:
      PolicyDocument:
        Statement:
          - Action: 'sqs:SendMessage'
            Condition:
              ArnEquals:
                'aws:SourceArn': !GetAtt
                  - AutoScalingEventRule
                  - Arn
            Effect: Allow
            Principal:
              Service: events.amazonaws.com
            Resource: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
        Version: 2012-10-17
      Queues:
        - !Ref UnprocessedAutoScalingEventQueue
```

Connect le flotte gestite dai clienti a un endpoint di licenza

Il server di AWS licenze basato sull'utilizzo di Deadline Cloud (Deadline Cloud) fornisce licenze su richiesta per prodotti di terze parti selezionati. Ciò ti consente di pagare in base al consumo. Vieni cambiato solo per il tempo che utilizzi.

Il server di licenza basato sull'utilizzo di Deadline Cloud può essere utilizzato con qualsiasi tipo di flotta, purché gli addetti di Deadline Cloud possano comunicare con il server di licenza. Questo viene configurato automaticamente nelle flotte gestite dal servizio. Questa configurazione è necessaria solo per le flotte gestite dai clienti.

Per creare il server di licenza, è necessario quanto segue:

- Un gruppo di sicurezza per il VPC della tua azienda agricola che consente il traffico per licenze di terze parti.
- Un ruolo AWS Identity and Access Management (IAM) con una policy allegata che consente l'accesso alle operazioni degli endpoint della licenza Deadline Cloud.

Argomenti

Fase 1: Creare un gruppo di sicurezza

Usa la console Amazon VPC (https://console.aws.amazon.com/vpc/) per creare un gruppo di sicurezza per il VPC della tua fattoria. Configura il gruppo di sicurezza per consentire le seguenti regole in entrata:

- Autodesk Maya e Arnold — 2701 - 2702, TCP, IPv4
- Autodesk 3ds Max — 2704, TCP, IPv4
- Foundry Nuke — 6101, TCP, IPv4
- SideFX Houdini, Mantra e Karma — 1715-1717, TCP, IPv4

La fonte di ogni regola in entrata è il gruppo di sicurezza dei lavoratori della flotta.

Per ulteriori informazioni sulla creazione di un gruppo di sicurezza, consulta Creare un gruppo di sicurezza nella guida per l'utente di Amazon Virtual Private Cloud.

Passaggio 2: configura l'endpoint della licenza

Un endpoint di licenza fornisce l'accesso ai server di licenza per prodotti di terze parti. Le richieste di licenza vengono inviate all'endpoint di licenza. L'endpoint le indirizza al server di licenza appropriato. Il server delle licenze tiene traccia dei limiti di utilizzo e dei diritti. È previsto un costo per ogni endpoint di licenza creato. Per ulteriori informazioni, consulta la pagina Prezzi di Amazon VPC.

È possibile creare l'endpoint di licenza da qui AWS Command Line Interface con le autorizzazioni appropriate. Per la politica richiesta per creare un endpoint di licenza, vedi Politica per consentire la creazione di un endpoint di licenza.

È possibile utilizzare AWS CloudShell (https://console.aws.amazon.com/cloudshell/) o qualsiasi altro AWS CLI ambiente per configurare l'endpoint di licenza utilizzando i seguenti comandi. AWS Command Line Interface

1. Crea l'endpoint della licenza. Sostituisci l'ID del gruppo di sicurezza, l'ID di sottorete e l'ID VPC con i valori creati in precedenza. Se utilizzi più sottoreti, separale con spazi.

```
aws deadline create-license-endpoint \
  --security-group-id SECURITY_GROUP_ID \
  --subnet-ids SUBNET_ID1 SUBNET_ID2 \
  --vpc-id VPC_ID
```

2. Confermate che l'endpoint è stato creato correttamente con il seguente comando. Ricorda il nome DNS dell'endpoint VPC.

```
aws deadline get-license-endpoint \
  --license-endpoint-id LICENSE_ENDPOINT_ID
```

3. Visualizza un elenco di prodotti misurati disponibili:

```
aws deadline list-available-metered-products
```

4. Aggiungi i prodotti a consumo all'endpoint della licenza con il seguente comando.

```
aws deadline put-metered-product \
--license-endpoint-id LICENSE_ENDPOINT_ID \
--product-id PRODUCT_ID
```

È possibile rimuovere un prodotto da un endpoint di licenza con il comando: `remove-metered-product`

```
aws deadline remove-metered-product \
  --license-endpoint-id LICENSE_ENDPOINT_ID \
  --productId PRODUCT_ID
```

È possibile eliminare un endpoint di licenza con il `delete-license-endpoint` comando:

```
aws deadline delete-license-endpoint \
 --license-endpoint-id LICENSE_ENDPOINT_ID
```

Fase 3: Connettere un'applicazione di rendering a un endpoint

Dopo aver configurato l'endpoint di licenza, le applicazioni lo utilizzano nello stesso modo in cui utilizzano un server di licenze di terze parti. In genere si configura il server di licenza per l'applicazione impostando una variabile di ambiente o un'altra impostazione di sistema, ad esempio una chiave di registro di Microsoft Windows, su una porta e un indirizzo del server di licenza.

Per ottenere il nome DNS dell'endpoint della licenza, utilizzate il comando seguente AWS CLI .

```
aws deadline get-license-endpoint
```

Oppure puoi utilizzare la console Amazon VPC (https://console.aws.amazon.com/vpc/) per identificare l'endpoint VPC creato dall'API Deadline Cloud nel passaggio precedente.

Esempi di configurazione

Example — Autodesk Maya e Arnold

Imposta la variabile di ambiente su: `ADSKFLEX_LICENSE_FILE`

```
2702@VPC_Endpoint_DNS_Name:2701@VPC_Endpoint_DNS_Name
```

> **Note**
>
> Per Windows i lavoratori, utilizzate un punto e virgola (;) anziché i due punti (:) per separare gli endpoint.

Example — Autodesk 3ds Max

Imposta la variabile `ADSKFLEX_LICENSE_FILE` di ambiente su:

```
2704@VPC_Endpoint_DNS_Name
```

Example — Foundry Nuke

Imposta la variabile `foundry_LICENSE` di ambiente `6101@VPC_Endpoint_DNS_Name` su Per verificare che le licenze funzionino correttamente, puoi eseguire Nuke in un terminale:

```
~/nuke/Nuke14.0v5/Nuke14.0 -x
```

Example — SideFX Houdini, Mantra e Karma

Esegui il comando seguente:

```
/opt/hfs19.5.640/bin/hserver -S
 "http://VPC_Endpoint_DNS_Name:1715;http://VPC_Endpoint_DNS_Name:1716;http://
VPC_Endpoint_DNS_Name:1717;"
```

Per verificare che le licenze funzionino correttamente, puoi renderizzare una scena di Houdini tramite questo comando:

```
/opt/hfs19.5.640/bin/hython ~/forpentest.hip -c "hou.node('/out/mantra1').render()"
```

Gestione degli utenti in Deadline Cloud

AWS Deadline Cloud lo utilizza AWS IAM Identity Center per gestire utenti e gruppi. IAM Identity Center è un servizio Single Sign-On basato sul cloud che può essere integrato con il tuo provider Single Sign-On (SSO) aziendale. Grazie all'integrazione, gli utenti possono accedere con il proprio account aziendale.

Deadline Cloud abilita IAM Identity Center per impostazione predefinita ed è necessario per configurare e utilizzare Deadline Cloud. Per ulteriori informazioni, consulta Gestisci la tua fonte di identità.

Il proprietario dell'organizzazione AWS Organizations è responsabile della gestione degli utenti e dei gruppi che hanno accesso al monitor Deadline Cloud. Puoi creare e gestire questi utenti e gruppi utilizzando IAM Identity Center o la console Deadline Cloud. Per ulteriori informazioni, consulta Cos'è AWS Organizations.

Puoi creare e rimuovere utenti e gruppi che possono utilizzare il monitor per gestire fattorie, code e flotte utilizzando la console Deadline Cloud. Quando aggiungi un utente a Deadline Cloud, deve reimpostare la password utilizzando IAM Identity Center prima di poter accedere.

Argomenti

Gestisci utenti e gruppi per il monitor

Un proprietario di Organizations può utilizzare la console Deadline Cloud per gestire gli utenti e i gruppi che hanno accesso al monitor Deadline Cloud. Puoi scegliere tra utenti e gruppi IAM Identity Center esistenti oppure aggiungere nuovi utenti e gruppi dalla console.

1. Accedi AWS Management Console e apri la console Deadline Cloud. Dalla pagina principale, nella sezione Guida introduttiva, scegli Configura Deadline Cloud o Vai alla dashboard.
2. Nel riquadro di navigazione a sinistra, scegli Gestione utenti. Per impostazione predefinita, è selezionata la scheda Gruppi.

A seconda dell'azione da intraprendere, scegli la scheda Gruppi o la scheda Utenti.

Monitor groups

Creazione di un gruppo

1. Seleziona Crea gruppo.
2. Inserisci un nome per il gruppo. Il nome deve essere univoco tra i gruppi dell'organizzazione IAM Identity Center.

Per rimuovere un gruppo

1. Seleziona il gruppo da rimuovere.
2. Scegli Rimuovi.
3. Nella finestra di dialogo di conferma, scegli Rimuovi gruppo.

> **Note**
>
> Stai rimuovendo il gruppo da IAM Identity Center. I membri del gruppo non possono più accedere a Deadline Cloud o accedere alle risorse della fattoria.

Monitor users

Come aggiungere utenti

1. Scegli la scheda Users (Utenti);
2. Scegli Aggiungi utenti.
3. Inserisci il nome, l'indirizzo email e il nome utente del nuovo utente.
4. Se lo desideri, scegli uno o più gruppi IAM Identity Center a cui aggiungere il nuovo utente.
5. Scegli Invia invito per inviare al nuovo utente un'e-mail con le istruzioni per entrare a far parte della tua organizzazione IAM Identity Center.

Per rimuovere un utente

1. Seleziona l'utente da rimuovere dal monitor.
2. Scegli Rimuovi.
3. Nella finestra di dialogo di conferma, scegli Rimuovi utente.

> **Note**
>
> Stai rimuovendo l'utente da IAM Identity Center. L'utente non può più accedere al monitor Deadline Cloud o accedere alle risorse della fattoria.

Gestisci utenti e gruppi per fattorie, code e flotte

1. Se non l'hai già fatto, accedi AWS Management Console e apri la console Deadline Cloud.
2. Nel riquadro di navigazione a sinistra, scegli Fattorie e altre risorse.
3. Seleziona la fattoria da gestire. Scegli il nome della fattoria per aprire la pagina dei dettagli. Puoi cercare la fattoria usando la barra di ricerca.
4. Per gestire una coda o una flotta, scegli la scheda Code o Flotte, quindi scegli la coda o la flotta da gestire.
5. Scegli la scheda Gestione degli accessi. Per impostazione predefinita, è selezionata la scheda Gruppi. Per gestire gli utenti, sposta l'interruttore su Utenti.

A seconda dell'azione da intraprendere, scegli la scheda Gruppi o la scheda Utenti.

Per le definizioni dei livelli di accesso, consulta Autorizzazioni.

Groups

Per aggiungere gruppi

1. Seleziona l'interruttore Gruppi.
2. Scegliere Add Group (Aggiungi gruppo).
3. Dal menu a discesa, seleziona i gruppi da aggiungere.
4. Per il livello di accesso al gruppo, scegli una delle seguenti opzioni:
   - Visualizzatore
   - Collaboratore
   - Manager
   - Proprietario
5. Scegli Aggiungi.

Per rimuovere gruppi

1. Seleziona i gruppi da rimuovere.
2. Scegli Rimuovi.
3. Nella finestra di dialogo di conferma selezionare Remove (Rimuovi).

Users

Come aggiungere utenti

1. Per aggiungere un utente, scegli Aggiungi utente.
2. Dal menu a discesa, seleziona gli utenti da aggiungere alla tua fattoria.
3. Per il livello di accesso utente, scegli una delle seguenti opzioni:
   - Visualizzatore
   - Collaboratore
   - Manager
   - Proprietario
4. Scegli Aggiungi. Gli utenti vengono aggiunti alla tua fattoria.

Per rimuovere utenti

1. Seleziona l'utente da rimuovere.
2. Nella finestra di dialogo di conferma della rimozione, scegli Rimuovi. L'utente viene quindi rimosso dalla farm selezionata.

Puoi anche aggiungere o rimuovere le autorizzazioni della farm per utenti e gruppi utilizzando la console IAM Identity Center all'indirizzo https://console.aws.amazon.com/singlesignon/.

Offerte di lavoro Deadline Cloud

Un job è un insieme di istruzioni che AWS Deadline Cloud utilizza per pianificare ed eseguire il lavoro sui lavoratori disponibili. Quando crei un lavoro, scegli la fattoria e la coda a cui inviare il lavoro. Fornisci anche un file JSON o YAML che fornisce le istruzioni per l'elaborazione da parte dei lavoratori. Deadline Cloud accetta modelli di lavoro che seguono la specifica Open Job Description (OpenJD) per la descrizione dei lavori. Per ulteriori informazioni, consulta la documentazione di Open Job Description sul GitHub sito web.

Un lavoro è composto da:

- Fasi: definisce lo script da eseguire sui lavoratori. I passaggi possono avere requisiti come la memoria minima di lavoro o altri passaggi che devono essere completati prima. Ogni passaggio prevede una o più attività.
- Attività: un'unità di lavoro inviata a un lavoratore per eseguirla. Un'attività è una combinazione dello script di una fase e dei parametri, come il numero di frame, utilizzati nello script. Il processo è completo quando tutte le attività sono state completate per tutte le fasi.
- Ambienti: imposta e smonta istruzioni condivise da più passaggi o attività.

Puoi creare un lavoro in uno dei seguenti modi:

- Usa un mittente di Deadline Cloud.
- Crea un pacchetto di lavori e utilizza l'interfaccia a riga di comando di Deadline Cloud (Deadline Cloud CLI).
- Usa l'SDK. AWS
- Usa il AWS Command Line Interface (AWS CLI).

Un submitter è un plug-in per il software di creazione di contenuti digitali (DCC) che gestisce la creazione di un lavoro nell'interfaccia con il software DCC. Dopo aver creato il lavoro, usi il mittente per inviarlo a Deadline Cloud per l'elaborazione. Dietro le quinte, il mittente crea un modello di lavoro OpenJD che descrive il lavoro. Allo stesso tempo, carica i file degli asset in un bucket Amazon Simple Storage Service (Amazon S3). Per ridurre il tempo necessario per inviare i file, solo i file che sono stati modificati dall'ultima volta in cui sono stati caricati i file vengono inviati ad Amazon S3.

Per creare script e pipeline personalizzati per inviare lavori a Deadline Cloud, puoi utilizzare la CLI di Deadline Cloud, AWS l'SDK o AWS CLI chiamare le operazioni per creare, ottenere, visualizzare ed elencare lavori. I seguenti argomenti spiegano come utilizzare la CLI di Deadline Cloud.

La CLI Deadline Cloud viene installata insieme al mittente Deadline Cloud. Per ulteriori informazioni, consulta Configura i mittenti di Deadline Cloud.

Argomenti

Invio di lavori con la CLI di Deadline Cloud

Per inviare un lavoro utilizzando l'interfaccia a riga di comando di Deadline Cloud (CLI di Deadline Cloud), usa il comando. `deadline bundle submit`

I lavori vengono inviati alle code. Se non hai ancora configurato una farm e una coda, usa la console Deadline Cloud (https://console.aws.amazon.com/https://console.aws.amazon.com/deadlinecloud/home) per configurare una farm e una coda e per visualizzare l'ID della fattoria e della coda. Per ulteriori informazioni, consulta Definire i dettagli della fattoria e Definire i dettagli della coda.

Per impostare la farm e la coda predefinite per la CLI di Deadline Cloud, utilizzare il comando seguente. Quando imposti i valori predefiniti, puoi utilizzare i comandi CLI di Deadline Cloud senza specificare una farm o una coda. Nell'esempio seguente, sostituisci *farmId* e con le tue informazioni: *queueId*

```
deadline config set defaults.farm_id farmId
deadline config set defaults.queue_id queueId
```

Per specificare i passaggi e le attività di un job, create un modello di job OpenJD. Per ulteriori informazioni, vedere Schemi di modelli [versione: 2023-09] nell'archivio delle specifiche Open Job Description. GitHub

L'esempio seguente è un modello di lavoro YAML. Definisce un lavoro con due fasi e cinque attività per fase.

```
name: Sample Job
specificationVersion: jobtemplate-2023-09
steps:
- name: Sample Step 1
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
- name: Sample Step 2
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
```

Per creare un lavoro, crea una nuova cartella denominata`sample_job`, quindi salva il file modello nella nuova cartella come`template.yaml`. Invii il lavoro con il seguente comando CLI di Deadline Cloud:

```
deadline bundle submit path/to/sample_job
```

La risposta del comando contiene un identificatore per il lavoro. Ricorda l'ID in modo da poter controllare lo stato del lavoro in un secondo momento.

```
Submitting to Queue: test-queue
Waiting for Job to be created...
```

```
Submitted job bundle:
   sample_job
Job creation completed successfully
jobId
```

Ci sono opzioni aggiuntive che puoi utilizzare quando invii un lavoro. Per ulteriori informazioni, consulta Altre opzioni per l'invio di lavori con la CLI di Deadline Cloud.

Altre opzioni per l'invio di lavori con la CLI di Deadline Cloud

Il comando CLI `deadline bundle submit` Deadline Cloud fornisce opzioni che è possibile utilizzare per specificare informazioni aggiuntive per un lavoro. Gli esempi seguenti mostrano come:

- Specificate i parametri utilizzati durante l'elaborazione del modello di lavoro.
- Allega file e cartelle in un ambiente condiviso a un lavoro.
- Imposta il numero massimo di operazioni non riuscite prima che un lavoro venga annullato.
- Imposta il numero massimo di tentativi per un'attività.

Parametri del processo

L'`parameters`opzione imposta il valore di un parametro di lavoro quando si crea il lavoro. Il modello di lavoro definisce il campo e l'`parameters`opzione imposta il valore. Un parametro può avere un valore predefinito. Se viene specificato un valore per il parametro, il valore specificato sostituisce il valore predefinito.

Il seguente modello di lavoro definisce il `TestParameter` campo:

```
name: Sample Job With Job Parameter
parameterDefinitions:
- default: test
  name: TestParameter
  type: STRING
specificationVersion: jobtemplate-2023-09
steps:
- description: step description
  name: MyStep
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
```

```
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
```

Il comando seguente imposta il valore di «Hello AWS»: `TestParameter`

```
deadline bundle submit sample_job --parameter "TestParameter=Hello AWS"
```

Profili di archiviazione

I profili di archiviazione aiutano a condividere file tra lavoratori con sistemi operativi diversi. Crea un profilo di archiviazione utilizzando la console Deadline Cloud. Quindi, utilizza il `storage-profile-id` parametro per utilizzare il profilo di archiviazione. Per ulteriori informazioni, consulta Archiviazione condivisa in Deadline Cloud.

Per impostare il profilo di archiviazione per gli invii di lavoro, utilizzando la CLI di Deadline Cloud, utilizza il seguente comando per impostare il parametro di configurazione: `storage-profile-id`

```
deadline config set settings.storage_profile_id storageProfileId
```

Numero massimo di attività non riuscite

L'`max-failed-tasks-count`opzione imposta il numero massimo di attività che possono fallire prima che l'intero processo abbia esito negativo e tutte le attività rimanenti vengano contrassegnate`CANCELED`. Il valore predefinito è 100.

```
deadline bundle submit sample_job --max-failed-tasks-count 10
```

Numero massimo di tentativi di attività non riusciti

L'`max-retries-per-task`opzione imposta il numero massimo di volte in cui un'attività viene ritentata prima che abbia esito negativo. Quando un'operazione viene ritentata, viene messa nello `READY` stato. Il valore predefinito è 5.

```
deadline bundle submit sample_job --max-retries-per-task 10
```

Pianificazione dei lavori in Deadline Cloud

Dopo aver creato un lavoro, AWS Deadline Cloud ne pianifica l'elaborazione su una o più flotte associate a una coda. La flotta che elabora una particolare attività viene scelta in base alle funzionalità configurate per la flotta e ai requisiti dell'host di una fase specifica.

I lavori sono programmati secondo l'ordine di priorità più elevato, dal più alto al più basso. Quando due lavori hanno la stessa priorità, il lavoro più vecchio viene pianificato per primo.

Le seguenti sezioni forniscono dettagli sul processo di pianificazione di un lavoro.

Determina la compatibilità della flotta

Dopo la creazione di un lavoro, Deadline Cloud verifica i requisiti dell'host per ogni fase del lavoro rispetto alle capacità delle flotte associate alla coda a cui è stato inviato il lavoro. Se una flotta soddisfa i requisiti dell'host, il lavoro viene assegnato allo stato. `READY`

Se una fase del lavoro presenta requisiti che non possono essere soddisfatti da una flotta associata alla coda, lo stato della fase viene impostato `NOT_COMPATIBLE` su. Inoltre, gli altri passaggi del processo vengono annullati.

Le capacità di una flotta sono impostate a livello di flotta. Anche se un lavoratore di una flotta soddisfa i requisiti del lavoro, non gli verranno assegnati i compiti previsti dal lavoro se la flotta non soddisfa i requisiti del lavoro.

Il seguente modello di lavoro presenta una fase che specifica i requisiti dell'host per la fase:

```
name: Sample Job With Host Requirements
specificationVersion: jobtemplate-2023-09
steps:
- name: Step 1
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
  hostRequirements:
    amounts:
    # Capabilities starting with "amount." are amount capabilities. If they start with
 "amount.worker.",
```

```
    # they are defined by the OpenJD specification. Other names are free for custom
 usage.
    - name: amount.worker.vcpu
      min: 4
      max: 8
    attributes:
    - name: attr.worker.os.family
      anyOf:
      - linux
```

Questo lavoro può essere programmato per una flotta con le seguenti funzionalità:

```
{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
```

Questo lavoro non può essere programmato per una flotta con nessuna delle seguenti funzionalità:

```
{
    "vCpuCount": {"min": 4},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no maximum, so it exceeds the maximum vCPU host requirement.

{
    "vCpuCount": {"max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no minimum, so it doesn't satisfy the minimum vCPU host
 requirement.

{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "windows",
    "cpuArchitectureType": "x86_64"
```

```
}
    The osFamily doesn't match.
```

Scalabilità della flotta

Quando un lavoro viene assegnato a una flotta compatibile con service managed, la flotta viene ridimensionata automaticamente. Il numero di lavoratori della flotta varia in base al numero di attività disponibili per la flotta.

Quando un lavoro viene assegnato a una flotta gestita dal cliente, è possibile che i lavoratori esistano già o possano essere creati utilizzando la scalabilità automatica basata su eventi. Per ulteriori informazioni, consulta Use EventBridge to handle auto scaling events nella Amazon EC2 Auto Scaling User Guide.

Sessioni

Le attività di un job sono suddivise in una o più sessioni. I lavoratori eseguono le sessioni per configurare l'ambiente, eseguire le attività e quindi demolire l'ambiente. Ogni sessione è composta da una o più azioni che un lavoratore deve intraprendere.

Quando un lavoratore completa le azioni della sezione, al lavoratore possono essere inviate azioni di sessione aggiuntive. Il lavoratore riutilizza gli ambienti e gli allegati di lavoro esistenti nella sessione per completare le attività in modo più efficiente.

Gli allegati di lavoro vengono creati dal mittente che utilizzi, come parte del pacchetto di lavori CLI di Deadline Cloud. Puoi anche creare allegati di lavoro utilizzando l'opzione relativa al comando. `--attachments` `create-job` AWS CLI Gli ambienti sono definiti in due punti: ambienti di coda collegati a una coda specifica e ambienti di fase di lavoro definiti nel modello di lavoro.

Esistono quattro tipi di azioni di sessione:

- `syncInputJobAttachments`— Scarica gli allegati del lavoro di input per il lavoratore.
- `envEnter`— Esegue le `onEnter` azioni per un ambiente.
- `taskRun`— Esegue le `onRun` azioni relative a un'attività.
- `envExit`— Esegue le `onExit` azioni per un ambiente.

Il seguente modello di lavoro ha un ambiente a fasi. Ha una `onEnter` definizione per configurare l'ambiente delle fasi, una `onRun` definizione che definisce l'attività da eseguire e una `onExit`

definizione per eliminare l'ambiente delle fasi. Le sessioni create per questo lavoro includeranno un'`envEnter`azione, una o più `task`Run azioni e quindi un'`envExit`azione.

```
name: Sample Job with Maya Environment
specificationVersion: jobtemplate-2023-09
steps:
- name: Maya Step
  stepEnvironments:
  - name: Maya
    description: Runs Maya in the background.
    script:
      embeddedFiles:
      - name: initData
        filename: init-data.yaml
        type: TEXT
        data: |
          scene_file: MyAwesomeSceneFile
          renderer: arnold
          camera: persp
      actions:
        onEnter:
          command: MayaAdaptor
          args:
          - daemon
          - start
          - --init-data
          - file://{{Env.File.initData}}
        onExit:
          command: MayaAdaptor
          args:
          - daemon
          - stop
  parameterSpace:
    taskParameterDefinitions:
    - name: Frame
      range: 1-5
      type: INT
  script:
    embeddedFiles:
    - name: runData
      filename: run-data.yaml
      type: TEXT
      data: |
```

```
        frame: {{Task.Param.Frame}}
    actions:
      onRun:
        command: MayaAdaptor
        args:
        - daemon
        - run
        - --run-data
        - file://{{ Task.File.runData }}
```

Dipendenze tra fasi

Deadline Cloud supporta la definizione delle dipendenze tra i passaggi in modo che un passaggio attenda il completamento di un altro passaggio prima di iniziare. Puoi definire più di una dipendenza per un passaggio. Un passaggio con una dipendenza non è pianificato fino al completamento di tutte le relative dipendenze.

Se il modello di lavoro definisce una dipendenza circolare, il lavoro viene rifiutato e lo stato del processo viene impostato su. `CREATE_FAILED`

Il seguente modello di lavoro crea un lavoro con due passaggi. `StepB`dipende da`StepA`. `StepB`viene eseguito solo dopo essere stato `StepA` completato con successo.

Dopo la creazione del lavoro, `StepA` si trova nello `READY` stato e `StepB` si trova nello `PENDING` stato. Al `StepA` termine, `StepB` passa allo `READY` stato. Se `StepA` fallisce o se `StepA` viene annullato, `StepB` passa allo `CANCELED` stato.

È possibile impostare una dipendenza su più passaggi. Ad esempio, `StepC` dipende da entrambi `StepA` e`StepB`, `StepC` non inizierà fino al termine degli altri due passaggi.

```
name: Step-Step Dependency Test
specificationVersion: 'jobtemplate-2023-09'
steps:
- name: A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
```

```
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail

          sleep 1
          echo Task A Done!
- name: B
  dependencies:
  - dependsOn: A # This means Step B depends on Step A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail

          sleep 1
          echo Task B Done!
```

Job states nella CLI di Deadline Cloud

Questo argomento descrive come utilizzare l'interfaccia a riga di comando di AWS Deadline Cloud (CLI di Deadline Cloud) per visualizzare lo stato di un processo o di un passaggio. Se desideri utilizzare il monitor Deadline Cloud per visualizzare lo stato dei lavori o delle fasi, consulta. Visualizza e gestisci lavori, passaggi e attività in Deadline Cloud

Puoi vedere lo stato di un lavoro utilizzando il comando CLI `deadline job get --job-id` Deadline Cloud. La risposta ai comandi include lo stato del lavoro o della fase e il numero di attività in ogni stato di elaborazione.

Quando invii un lavoro per la prima volta, lo stato è`CREATE_IN_PROGRESS`. Se il lavoro supera i controlli di convalida, il suo stato cambia in`CREATE_COMPLETE`. In caso contrario, lo stato diventa. `CREATE_FAILED`

Alcuni possibili motivi per cui un lavoro può non superare i controlli di convalida includono i seguenti:

- Il modello di lavoro non segue le specifiche OpenJD.
- Il job contiene troppi passaggi.
- Il lavoro contiene troppe attività totali.

Per visualizzare le quote per il numero massimo di passaggi e attività in un processo, utilizza la console Service Quotas. Per ulteriori informazioni, consulta Quote per Deadline Cloud.

Potrebbe esserci anche un errore interno del servizio che impedisce la creazione di un lavoro. In tal caso, il codice di stato del lavoro è `INTERNAL_ERROR` e il campo del messaggio di stato fornisce una spiegazione più dettagliata.

Utilizza il seguente comando CLI di Deadline Cloud per visualizzare i dettagli di un lavoro. Nell'esempio seguente, sostituiscilo *jobID*con le tue informazioni:

```
deadline job get --job-id jobId
```

La risposta del `deadline job get` comando è la seguente:

```
jobId: jobId
name: Sample Job
lifecycleStatus: CREATE_COMPLETE
lifecycleStatusMessage: Job creation completed successfully
priority: 50
createdAt: 2024-03-26 18:11:19.065000+00:00
createdBy: Test User
startedAt: 2024-03-26 18:12:50.710000+00:00
taskRunStatus: STARTING
taskRunStatusCounts:
  PENDING: 0
  READY: 5
  RUNNING: 0
  ASSIGNED: 0
  STARTING: 0
  SCHEDULED: 0
  INTERRUPTING: 0
  SUSPENDED: 0
  CANCELED: 0
```

```
  FAILED: 0
  SUCCEEDED: 0
  NOT_COMPATIBLE: 0
maxFailedTasksCount: 100
maxRetriesPerTask: 5
```

Ogni attività di un processo o di una fase ha uno stato. Gli stati delle attività vengono combinati per fornire uno stato generale dei lavori e delle fasi. Il numero di attività in ogni stato è riportato nel `taskRunStatusCounts` campo della risposta.

Lo stato di una mansione o di una fase dipende dallo stato delle relative attività. Lo stato è determinato dalle attività che hanno questi stati, in ordine. Gli stati delle fasi sono determinati allo stesso modo dello stato del lavoro.

L'elenco seguente descrive gli stati:

`NOT_COMPATIBLE`

Il lavoro non è compatibile con l'azienda agricola perché non ci sono flotte in grado di completare una delle attività previste dal lavoro.

`RUNNING`

Uno o più lavoratori eseguono le attività del posto di lavoro. Finché c'è almeno un'attività in esecuzione, il lavoro è contrassegnato`RUNNING`.

`ASSIGNED`

A uno o più lavoratori vengono assegnati compiti nel lavoro come azione successiva. L'ambiente, se esiste, è configurato.

`STARTING`

Uno o più lavoratori stanno configurando l'ambiente per l'esecuzione delle attività.

`SCHEDULED`

Le attività relative alla mansione sono programmate su uno o più lavoratori come azione successiva del lavoratore.

`READY`

Almeno un'attività per il lavoro è pronta per essere elaborata.

`INTERRUPTING`

Almeno un'attività del lavoro viene interrotta. Le interruzioni possono verificarsi quando si aggiorna manualmente lo stato del lavoro. Può verificarsi anche in risposta a un'interruzione dovuta a variazioni di prezzo Spot di Amazon Elastic Compute Cloud (Amazon EC2).

`FAILED`

Una o più attività del lavoro non sono state completate correttamente.

`CANCELED`

Una o più attività del lavoro sono state annullate.

`SUSPENDED`

Almeno un'attività del lavoro è stata sospesa.

`PENDING`

Un'attività nel processo è in attesa della disponibilità di un'altra risorsa.

`SUCCEEDED`

Tutte le attività del processo sono state elaborate correttamente.

Modifica dei lavori in Deadline Cloud

Puoi utilizzare i seguenti `update` comandi AWS Command Line Interface (AWS CLI) per modificare la configurazione di un lavoro o per impostare lo stato di destinazione di un lavoro, un passaggio o un'attività:

- `aws deadline update-job`
- `aws deadline update-step`
- `aws deadline update-task`

Nei seguenti esempi di `update` comandi, sostituiteli *`user input placeholder`*con le vostre informazioni.

Puoi anche utilizzare il monitor Deadline Cloud per modificare la configurazione di un lavoro. Per ulteriori informazioni, consulta Visualizza e gestisci lavori, passaggi e attività in Deadline Cloud.

Example — Richiedi un lavoro

Tutte le attività del lavoro passano `READY` allo stato, a meno che non vi siano dipendenze tra fasi. I passaggi con dipendenze passano a uno o all'altro `READY` o `PENDING` man mano che vengono ripristinati.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status PENDING
```

Example — Annullare un lavoro

Tutte le attività del lavoro che non hanno lo stato `SUCCEEDED` o `FAILED` sono contrassegnate`CANCELED`.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status CANCELED
```

Example — Contrassegna un lavoro come non riuscito

Tutte le attività del lavoro che hanno lo stato `SUCCEEDED` rimangono invariate. Tutte le altre attività sono contrassegnate`FAILED`.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status FAILED
```

Example — Contrassegna un lavoro riuscito

Tutte le attività lavorative vengono trasferite allo `SUCCEEDED` stato.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
```

```
--job-id jobID \
--target-task-run-status SUCCEEDED
```

Example — Sospendere un lavoro

Le attività del lavoro nello `SUCCEEDED` `FAILED` stato o non cambiano. `CANCELED` Tutte le altre attività sono contrassegnate`SUSPENDED`.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status SUSPENDED
```

Example — Modificare la priorità di un lavoro

Aggiorna la priorità di un lavoro per modificare l'ordine in cui è pianificato. I lavori con priorità più alta vengono generalmente pianificati per primi.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--priority 100
```

Example — Modificare il numero di attività non riuscite consentite

Aggiorna il numero massimo di attività non riuscite che il lavoro può avere prima che le attività rimanenti vengano annullate.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-failed-tasks-count 200
```

Example — Modifica il numero di tentativi consentiti per le nuove attività

Aggiorna il numero massimo di tentativi per un'attività prima che l'operazione abbia esito negativo. Un'attività che ha raggiunto il numero massimo di tentativi non può essere richiesta finché questo valore non viene aumentato.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-retries-per-task 10
```

Example — Archivia un lavoro

Aggiorna lo stato del ciclo di vita del lavoro su. ARCHIVED I lavori archiviati non possono essere pianificati o modificati. È possibile archiviare solo un lavoro che si trova nello SUSPENDED stato FAILEDCANCELED,SUCCEEDED, o.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--lifecycle-status ARCHIVED
```

Example — Richiedere un passaggio

Tutte le attività della fase passano READY allo stato, a meno che non vi siano dipendenze tra fasi. Le attività in fasi con dipendenze passano a uno READY o all'altro e PENDING l'attività viene ripristinata.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status PENDING
```

Example — Annullare un passaggio

Tutte le attività del passaggio che non hanno lo stato SUCCEEDED o FAILED sono contrassegnateCANCELED.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
```

```
--target-task-run-status CANCELED
```

Example — Contrassegna un passaggio come fallito

Tutte le attività del passaggio che hanno lo stato `SUCCEEDED` rimangono invariate. Tutte le altre attività sono contrassegnate`FAILED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status FAILED
```

Example — Contrassegna un passaggio riuscito

Tutte le attività del passaggio sono contrassegnate`SUCCEEDED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUCCEEDED
```

Example — Sospendere un passaggio

Le attività del passaggio nello `SUCCEEDED` `FAILED` stato o non vengono modificate. `CANCELED` Tutte le altre attività sono contrassegnate`SUSPENDED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUSPENDED
```

Example — Modificare lo stato di un'attività

Quando si utilizza il comando CLI `update-task` Deadline Cloud, l'attività passa allo stato specificato.

```
aws deadline update-task \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--task-id taskID \
--target-task-run-status SUCCEEDED | SUSPENDED | CANCELED | FAILED | PENDING
```

Come Deadline Cloud elabora i lavori

Per elaborare un lavoro, AWS Deadline Cloud utilizza il modello di lavoro Open Job Description (OpenJD) per determinare le risorse necessarie. Deadline Cloud seleziona un lavoratore adatto per ogni fase tra le flotte associate alla tua coda. Il lavoratore selezionato soddisfa tutti gli attributi di capacità richiesti per la fase.

Successivamente, Deadline Cloud invia istruzioni ai lavoratori per impostare una sessione per la fase. Il software richiesto per la fase deve essere disponibile sull'istanza del lavoratore affinché il lavoro possa essere eseguito. Il servizio può aprire sessioni su più lavoratori se le impostazioni di scalabilità per la flotta sono sufficienti.

È possibile configurare il software in un file Amazon Machine Image (AMI) oppure l'operatore può caricare il software in fase di esecuzione da un repository o da un gestore di pacchetti. È possibile utilizzare un ambiente di coda, di lavoro o a fasi per distribuire il software che si preferisce.

Il servizio Deadline Cloud utilizza il modello OpenJD per determinare i passaggi necessari per il lavoro e le attività richieste per ogni passaggio. Alcuni passaggi dipendono da altri passaggi, quindi Deadline Cloud determina l'ordine di completamento dei passaggi. Quindi, Deadline Cloud invia le attività per ogni fase ai lavoratori affinché le elaborino. Al termine di un'attività, il servizio invia un'altra attività nella stessa sessione oppure il lavoratore può iniziare una nuova sessione.

Puoi tenere traccia dello stato di avanzamento del lavoro nel monitor Deadline Cloud, nell'interfaccia a riga di comando di Deadline Cloud (Deadline Cloud CLI) o nel. AWS CLI Per ulteriori informazioni sull'uso del monitor, consulta. Utilizzo del monitor Deadline Cloud Per ulteriori informazioni sull'utilizzo della CLI di Deadline Cloud, consulta. Job states nella CLI di Deadline Cloud

Una volta completate tutte le attività di ogni fase, il lavoro è completo e l'output è pronto per essere scaricato sulla workstation. Anche se il lavoro non è stato completato, l'output di ogni fase e attività completata è disponibile per il download.

Deadline Cloud rimuove i lavori 120 giorni dopo l'invio. Quando un lavoro viene rimosso, vengono rimossi anche tutti i passaggi e le attività associati al lavoro. Se hai bisogno di rieseguire il lavoro, invia nuovamente il modello OpenJD per il lavoro.

Risoluzione dei problemi relativi ai job di Deadline Cloud

Per informazioni sui problemi più comuni con i lavori in AWS Deadline Cloud, consulta i seguenti argomenti.

Argomenti

Perché la creazione del mio lavoro non è riuscita?

Alcuni possibili motivi per cui un lavoro può non superare i controlli di convalida includono i seguenti:

- Il modello di lavoro non segue le specifiche OpenJD.
- Il job contiene troppi passaggi.
- Il lavoro contiene troppe attività totali.
- Si è verificato un errore interno del servizio che impedisce la creazione del lavoro.

Per visualizzare le quote per il numero massimo di passaggi e attività in un processo, utilizza la console Service Quotas. Per ulteriori informazioni, consulta Quote per Deadline Cloud.

Perché il mio lavoro non è compatibile?

I motivi più comuni per cui i lavori non sono compatibili con le code includono i seguenti:

- Nessuna flotta è associata alla coda a cui è stato inviato il lavoro. Apri il monitor Deadline Cloud e verifica che la coda abbia flotte associate. Per ulteriori informazioni su come visualizzare le code, consulta. Visualizza i dettagli della coda e della flotta in Deadline Cloud

- Il lavoro presenta requisiti relativi all'host che non sono soddisfatti da nessuna delle flotte associate alla coda. Per verificarlo, confronta la `hostRequirements` voce inserita nel modello di lavoro con la configurazione delle flotte della tua fattoria. Assicurati che una delle flotte soddisfi i requisiti dell'host. Per ulteriori informazioni sulla compatibilità del parco veicoli, consulta. Determina la compatibilità della flotta Per visualizzare la configurazione del parco veicoli, vedereVisualizza i dettagli della coda e della flotta in Deadline Cloud.

Perché il mio lavoro è già pronto?

Le possibili ragioni per cui il tuo lavoro sembra essere bloccato nello `READY` stato includono le seguenti:

- Il numero massimo di lavoratori per le flotte associate alla coda è impostato su zero. Per verificare, vedere. Visualizza i dettagli della coda e della flotta in Deadline Cloud
- C'è un lavoro con priorità più alta in coda. Per verificare, vedereVisualizza i dettagli della coda e della flotta in Deadline Cloud.
- Per le flotte gestite dai clienti, controlla la configurazione della scalabilità automatica. Per ulteriori informazioni, consulta Ridimensiona automaticamente la tua flotta Amazon EC2 con la funzionalità di raccomandazione di scalabilità Deadline Cloud.

Perché il mio lavoro è fallito?

Un lavoro può fallire per molte ragioni. Per cercare il problema, apri il monitor Deadline Cloud e scegli il lavoro che non va a buon fine. Scegli un'attività che non è riuscita e quindi visualizza i registri dell'attività. Per istruzioni, consulta Visualizza i log in Deadline Cloud.

- Se visualizzi errori di licenza o se viene visualizzata una filigrana perché il software non dispone di una licenza valida, assicurati che l'operatore possa connettersi al server di licenza richiesto. Per ulteriori informazioni, consulta Connect le flotte gestite dai clienti a un endpoint di licenza.

Perché il mio passo è in sospeso?

I passaggi possono rimanere `PENDING` invariati quando una o più dipendenze non sono complete. Puoi controllare lo stato delle dipendenze utilizzando il monitor Deadline Cloud. Per istruzioni, consulta Visualizza una fase in Deadline Cloud.

Archiviazione di file per Deadline Cloud

I lavoratori devono avere accesso alle posizioni di archiviazione che contengono i file di input necessari per elaborare un lavoro e alle posizioni che archiviano l'output. AWS Deadline Cloud offre due opzioni per le posizioni di archiviazione:

- Con gli allegati dei lavori, Deadline Cloud trasferisce i file di input e output dei lavori avanti e indietro tra una workstation e i lavoratori di Deadline Cloud. Per abilitare i trasferimenti di file, Deadline Cloud utilizza un bucket Amazon Simple Storage Service (Amazon S3) nel tuo. Account AWS

  Quando utilizzi Job Attachments con una flotta gestita dal servizio, puoi configurare un file system virtuale (VFS) nella tua rete privata virtuale (VPN). Quindi i lavoratori possono caricare i file solo quando necessario.
- Con lo storage condiviso, si utilizza la condivisione di file con il sistema operativo per fornire l'accesso ai file.

  Quando si utilizza lo storage condiviso multipiattaforma, è possibile creare un profilo di archiviazione in modo che gli operatori possano mappare il percorso dei file tra due diversi sistemi operativi.

Argomenti

Allegati di lavoro in Deadline Cloud

Gli allegati Job ti consentono di trasferire file avanti e indietro tra la tua workstation e AWS Deadline Cloud. Con gli allegati dei lavori, non è necessario configurare manualmente un bucket Amazon S3 per i file. Invece, quando crei una coda con la console Deadline Cloud, scegli il bucket per i tuoi allegati di lavoro.

La prima volta che invii un lavoro a Deadline Cloud, tutti i file relativi al lavoro vengono trasferiti su Deadline Cloud. Per gli invii successivi, vengono trasferiti solo i file modificati, risparmiando tempo e larghezza di banda.

Una volta completata l'elaborazione, puoi scaricare il risultato dalla pagina dei dettagli del lavoro o utilizzando il comando `deadline job download-output` CLI di Deadline Cloud.

Puoi utilizzare lo stesso bucket S3 per più code. Imposta un prefisso root diverso per ogni coda per organizzare gli allegati nel bucket.

Quando crei una coda con la console, puoi scegliere un ruolo esistente AWS Identity and Access Management (IAM) oppure puoi fare in modo che la console crei un nuovo ruolo. Se la console crea il ruolo, imposta le autorizzazioni per accedere al bucket specificato per la coda. Se scegli un ruolo esistente, devi concedere al ruolo le autorizzazioni per accedere al bucket S3.

Crittografia per i bucket S3 di Job Attachment

Per impostazione predefinita, i file degli allegati Job vengono crittografati automaticamente nel bucket S3. Questo approccio aiuta a proteggere le informazioni da accessi non autorizzati. Non devi fare nulla per crittografare i tuoi file con le chiavi fornite da Deadline Cloud. Per ulteriori informazioni, consulta Amazon S3 ora crittografa automaticamente tutti i nuovi oggetti nella Amazon S3 User Guide.

Puoi utilizzare la tua AWS Key Management Service chiave gestita dal cliente per crittografare il bucket S3 che contiene i tuoi allegati di lavoro. A tale scopo, è necessario modificare il ruolo IAM per la coda associata al bucket per consentire l'accesso a. AWS KMS key

Per aprire l'editor delle politiche IAM per il ruolo di coda

1. Accedi AWS Management Console e apri la console Deadline Cloud. Dalla pagina principale, nella sezione Guida introduttiva, scegli Visualizza fattorie.
2. Dall'elenco delle fattorie, scegli la fattoria che contiene la coda da modificare.
3. Dall'elenco delle code, scegli la coda da modificare.
4. Nella sezione Dettagli sulla coda, scegli il ruolo di servizio per aprire la console IAM per il ruolo di servizio.

Quindi, completa la seguente procedura.

Per aggiornare la politica dei ruoli con l'autorizzazione per AWS KMS

1. Dall'elenco delle politiche di autorizzazione, scegli la politica per il ruolo.
2. Nella sezione Autorizzazioni definite in questa politica, scegli Modifica.

3. Scegli Aggiungi nuova dichiarazione.
4. Copia e incolla la seguente politica nell'editor. Modificate il *RegionaccountID*, e *keyID*adattatelo ai vostri valori.

```
{
   "Effect": "Allow",
   "Action": [
       "kms:Decrypt",
       "kms:DescribeKey",
       "kms:GenerateDataKey"
   ],
   "Resource": [
       "arn:aws:kms:Region:accountID:key/keyID"
   ]
}
```

5. Seleziona Successivo.
6. Controlla le modifiche alla politica e, quando sei soddisfatto, scegli Salva modifiche.

Gestione degli allegati di lavoro nei bucket S3

Deadline Cloud archivia i file allegati del lavoro necessari per il tuo lavoro in un bucket S3. Questi file si accumulano nel tempo, con conseguente aumento dei costi di Amazon S3. Per ridurre i costi, puoi applicare una configurazione S3 Lifecycle al tuo bucket S3. Questa configurazione può eliminare automaticamente i file nel bucket. Poiché il bucket S3 è nel tuo account, puoi scegliere di modificare o rimuovere la configurazione di S3 Lifecycle in qualsiasi momento. Per ulteriori informazioni, consulta Esempi di configurazione del ciclo di vita di S3 nella Amazon S3 User Guide.

Per una soluzione di gestione dei bucket S3 più granulare, puoi impostare gli oggetti con scadenza in un bucket S3 in base Account AWS all'ultima volta in cui sono stati utilizzati. Per ulteriori informazioni, consulta la sezione relativa alla scadenza degli oggetti Amazon S3 in base alla data dell'ultimo accesso per ridurre i costi sul AWS blog di architettura.

File system virtuale Deadline Cloud

Il supporto del file system virtuale per gli allegati di lavoro in AWS Deadline Cloud consente al software client sui lavoratori di comunicare direttamente con Amazon Simple Storage Service. I lavoratori possono caricare i file solo quando necessario invece di scaricare tutti i file prima

dell'elaborazione. I file vengono archiviati localmente. Questo approccio evita di scaricare le risorse utilizzate più di una volta più volte. Tutti i file vengono rimossi al termine del processo.

- Il file system virtuale offre un significativo incremento delle prestazioni per profili professionali specifici. In generale, i sottoinsiemi più piccoli di file totali con flotte di lavoratori più grandi offrono i maggiori vantaggi. Un numero limitato di file con un minor numero di addetti ha tempi di elaborazione all'incirca equivalenti.
- Il supporto dei file system virtuali è disponibile solo per Linux i lavoratori delle flotte gestite dai servizi.
- Il file system virtuale Deadline Cloud supporta le seguenti operazioni, ma non è conforme a POSIX:
  - File`create`,`delete`,,`open`,`close`,`read`,`write`,`append`,,`truncate`, `renamemove`, e `copy` `stat` `fsync` `falloc`
  - Directory `createdelete`,`rename`,`move`,`copy`, e `stat`
- Il file system virtuale è progettato per ridurre il trasferimento di dati e migliorare le prestazioni quando le attività accedono solo a una parte di un set di dati di grandi dimensioni e non è ottimizzato per tutti i carichi di lavoro. È necessario testare il carico di lavoro prima di eseguire i lavori di produzione.

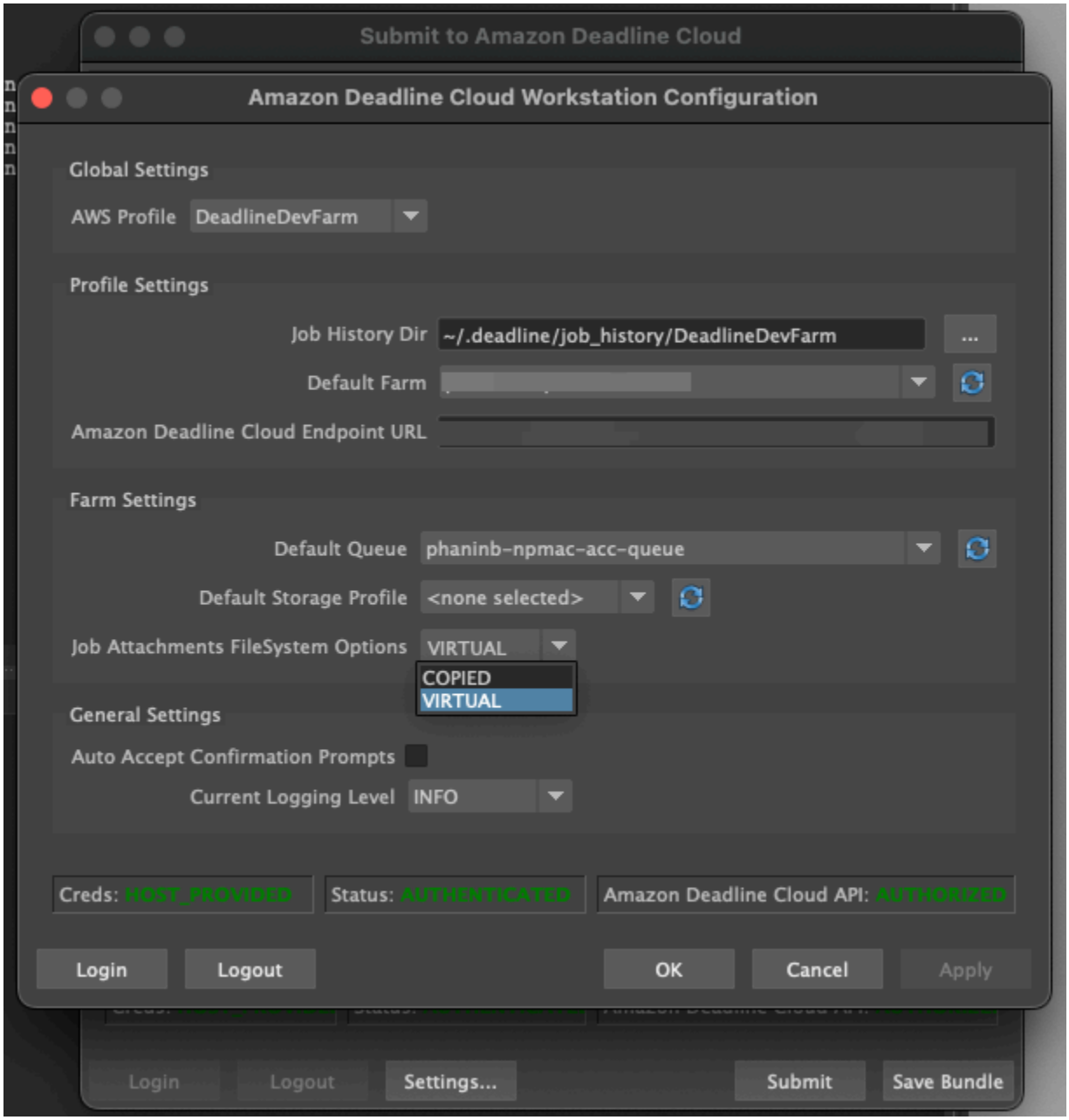
Abilita il supporto VFS

Il supporto per i file system virtuali (VFS) è abilitato per ogni processo. Un job torna al framework predefinito dei job attachments nei seguenti casi:

- Un profilo di istanza di lavoro non supporta un file system virtuale.
- I problemi impediscono l'avvio del processo del file system virtuale.
- Il file system virtuale non può essere montato.

Per abilitare il supporto del file system virtuale utilizzando il mittente

1. Quando invii un lavoro, scegli il pulsante Impostazioni per aprire il pannello di configurazione della workstation AWS Deadline Cloud.
2. Dal menu a discesa delle opzioni del file system Job attachments, scegli VIRTUAL.



3. Per salvare le modifiche, scegli OK.

Per abilitare il supporto del file system virtuale utilizzando AWS CLI

- Utilizzate il seguente comando quando inviate un lavoro salvato:

```
deadline bundle submit-job --job-attachments-file-system VIRTUAL
```

Per verificare che il file system virtuale sia stato avviato correttamente per un determinato lavoro, esamina i log in Amazon CloudWatch Logs. Cerca i seguenti messaggi:

```
Using mount_point mount_point
Launching vfs with command command
Launched vfs as pid PID number
```

Se il registro contiene il seguente messaggio, il supporto del file system virtuale è disabilitato:

```
Virtual File System not found, falling back to COPIED for JobAttachmentsFileSystem.
```

Risoluzione dei problemi relativi al supporto dei file system virtuali

Puoi visualizzare i log del tuo file system virtuale utilizzando il monitor Deadline Cloud. Per istruzioni, consulta Visualizza i log in Deadline Cloud.

I log del file system virtuale vengono inoltre inviati al gruppo CloudWatch Logs associato alla coda condivisa con l'output del worker agent.

Archiviazione condivisa in Deadline Cloud

Per utilizzare l'archiviazione condivisa, i lavoratori utilizzano il sistema di condivisione dei file del sistema operativo per accedere a uno spazio di archiviazione condiviso per l'input e l'output dei lavori.

Il metodo effettivo utilizzato per condividere i file dipende dal sistema operativo e dal modo in cui si implementa lo storage condiviso sulla rete. Sei responsabile della configurazione della condivisione dei file e della garanzia che soddisfi le tue esigenze.

Se utilizzi una soluzione di condivisione di file tra sistemi, puoi utilizzare i profili di archiviazione per mappare le posizioni dei file tra Linux i diversi Windows file system.

Profili di archiviazione in Deadline Cloud

Un profilo di archiviazione consente di configurare le farm utilizzando uno storage condiviso multipiattaforma. Un profilo di archiviazione mappa i percorsi tra i sistemi operativi per i lavori elaborati su lavoratori con un sistema operativo diverso da quello da cui sono stati inviati.

I profili di storage sono necessari quando si utilizza una flotta gestita dal cliente con una combinazione di sistemi operativi tra workstation e lavoratori. I profili di storage non sono supportati nelle flotte gestite dai servizi.

Dopo aver creato un profilo di archiviazione, è necessario concedere l'accesso alle code e alle flotte che utilizzano il profilo.

Per creare un profilo di archiviazione

1. Apri la console Deadline Cloud.
2. Da Inizia, scegli Vai alla dashboard di Deadline Cloud.
3. Scegli una fattoria, quindi scegli la scheda Profili di archiviazione.
4. Scegli Crea profilo di archiviazione.
5. Scegli un sistema operativo dal menu a discesa.
6. Fornisci un nome per il profilo. Un nome chiaro consente di scegliere il profilo di archiviazione da utilizzare per l'invio dei lavori.
7. Per il nome del percorso, inserisci la posizione principale dei dati del lavoro sulla workstation da cui invii i lavori.
8. Scegli un tipo di archiviazione:
   - Locale si riferisce alle posizioni dei file che non sono condivise tra il lavoratore e la workstation. Vengono caricati come allegati di lavoro.
   - Condiviso si riferisce allo storage condiviso tra il lavoratore e la workstation. I file nella memoria condivisa non vengono caricati come allegati di lavoro.
9. Fornisci un percorso di posizione del file system. Questa è la directory principale per i dati del lavoro.
10. Scegli Crea.

Dopo aver creato un profilo di archiviazione, è necessario modificare le code e le flotte gestite dai clienti per utilizzare il nuovo profilo. Per consentire l'accesso a un profilo di archiviazione, utilizzare la procedura seguente dopo aver completato la procedura precedente.

Per consentire alle code e alle flotte gestite dai clienti di utilizzare un profilo di archiviazione

1. Scegli la scheda Code o Flotte.
2. Scegli la coda o la flotta da modificare.
3. Scegli Modifica profili di archiviazione.
4. Seleziona il profilo di archiviazione da consentire e le posizioni del file system da quel profilo.
5. Scegli Save changes (Salva modifiche).

Gestione dei budget e dell'utilizzo per Deadline Cloud

Il budget manager e l'usage explorer di AWS Deadline Cloud sono strumenti di gestione dei costi che forniscono il costo approssimativo dell'utilizzo di Deadline Cloud sulla base delle informazioni disponibili sulle variabili di costo. Gli strumenti di gestione dei costi non garantiscono l'importo dovuto per l'uso effettivo di Deadline Cloud e di altri servizi. AWS

Per aiutarti a gestire i costi di Deadline Cloud, puoi utilizzare le seguenti funzionalità:

- Gestione del budget: con il gestore del budget di Deadline Cloud, puoi creare e modificare budget per aiutare a gestire i costi del progetto.
- Usage explorer: con Deadline Cloud usage explorer, puoi visualizzare quante AWS risorse vengono utilizzate e i costi stimati per tali risorse.

Ipotesi di costo

Il calcolo di base utilizzato dagli strumenti di gestione dei costi di Deadline Cloud è:

```
Cost per job =
    (CMF run time x CMF compute rate) +
    (SMF run time x SMF compute rate) +
    (License run time x license rate)
```

- Il tempo di esecuzione è la somma di tutte le attività di un processo, dall'ora di inizio all'ora di fine.
- La velocità di elaborazione è determinata dai prezzi di AWS Deadline Cloud per le flotte gestite dai servizi. Per le flotte gestite dai clienti, la velocità di elaborazione è stimata in 1 USD per lavoratore all'ora.
- La tariffa di licenza è determinata dal prezzo della licenza base di Deadline Cloud. I livelli aggiuntivi non sono inclusi. Per ulteriori informazioni sui prezzi delle licenze, consulta i prezzi di AWS Deadline Cloud.

La stima dei costi fornita dagli strumenti di gestione dei costi di Deadline Cloud può variare dai costi effettivi per una serie di motivi. I motivi più comuni includono:

- Risorse di proprietà del cliente e relativi prezzi. Puoi scegliere di portare le tue risorse, da AWS o esternamente da fornitori di servizi cloud locali o di altro tipo. I costi effettivi di queste risorse non vengono calcolati.
- Costi dei lavoratori inattivi. Per le flotte con un numero minimo di istanze superiore a zero, i lavoratori inattivi non vengono presi in considerazione nei calcoli.
- Crediti promozionali, sconti e accordi sui prezzi personalizzati. Gli strumenti di gestione dei costi non tengono conto di crediti promozionali, accordi tariffari privati o altri sconti. Potresti avere diritto ad altri sconti che non fanno parte della stima.
- Archiviazione delle risorse. Lo storage degli asset non è incluso nelle stime dei costi e dell'utilizzo.
- Variazioni di prezzo. AWS offre pay-as-you-go prezzi per la maggior parte dei servizi. I prezzi possono cambiare nel tempo. Gli strumenti di gestione dei costi utilizzano la maggior parte dei up-to-date prezzi disponibili al pubblico, ma potrebbero verificarsi ritardi in seguito alle modifiche.
- Imposte. Gli strumenti di gestione dei costi non includono le tasse applicate all'acquisto del servizio da parte nostra.
- Arrotondamento. Lo strumento di gestione dei costi esegue l'arrotondamento matematico dei dati sui prezzi.
- Valuta. Le stime dei costi sono espresse in dollari USA. I tassi di cambio globali variano nel tempo. Se si traducono le stime in una base valutaria diversa sulla valuta corrente, le variazioni del tasso di cambio influiscono sulla stima.
- Licenze esterne. Se scegli di utilizzare licenze preacquistate (porta la tua licenza), gli strumenti di gestione dei costi di Deadline Cloud non possono tenere conto di questo costo.

Utilizzo del gestore del budget Deadline Cloud

Il budget manager di Deadline Cloud ti aiuta a controllare la spesa per una determinata risorsa, come una coda, una flotta o una fattoria. Puoi creare importi e limiti di budget e impostare azioni automatizzate per ridurre o bloccare le spese aggiuntive rispetto al budget.

Le sezioni seguenti forniscono i passaggi per utilizzare il gestore di budget di Deadline Cloud.

Argomenti

- Modifica un budget
- Disattiva un budget

Prerequisito

Per utilizzare il gestore del budget di Deadline Cloud, devi disporre del livello di `OWNER` accesso. Per concedere `OWNER` l'autorizzazione, segui i passaggi indicatiGestione degli utenti in Deadline Cloud.

Accedi al gestore del budget

Per accedere al gestore del budget di Deadline Cloud, utilizza la seguente procedura.

1. Accedi AWS Management Console e apri la console Deadline Cloud.
2. Scegli Visualizza fattorie.
3. Individua la fattoria su cui desideri ottenere informazioni, quindi scegli Gestisci lavori. Il monitor Deadline Cloud si apre in una nuova scheda.
4. Nel monitor Deadline Cloud, nel riquadro di navigazione a sinistra, scegli Budget.

La pagina di riepilogo del gestore del budget mostra un elenco di budget attivi e inattivi:

- I budget attivi vengono confrontati con la risorsa selezionata (una coda).
- I budget inattivi sono scaduti o sono stati annullati da un utente e non tengono più traccia dei costi rispetto ai limiti di questo budget.

Dopo aver scelto un budget, la pagina di riepilogo del budget contiene informazioni di base sul budget. Le informazioni fornite includono il nome del budget, lo stato, le risorse, la percentuale rimanente, l'importo rimanente, il budget totale, la data di inizio e la data di fine.

Creazione di un budget

Per creare un budget, utilizzare la procedura seguente.

1. Se non l'hai già fatto, accedi a AWS Management Console, apri la console Deadline Cloud, scegli una fattoria, quindi scegli Gestisci lavori.
2. Dalla pagina Gestione del budget, scegli Crea budget.
3. Nella sezione dei dettagli, inserisci un nome per il budget.

4. (Facoltativo) Nel campo della descrizione, inserisci una descrizione chiara e breve per il budget.
5. Da Risorsa, scegli il menu a discesa Coda per trovare e selezionare la coda per cui desideri creare un budget.
6. Per Periodo, imposta la data di inizio e di fine del budget completando i seguenti passaggi:

    a. Per Data di inizio, inserisci la prima data del monitoraggio del budget nel formato YYYY/MM/GG oppure scegli l'icona del calendario e seleziona una data.

    La data di inizio predefinita è la data di creazione del budget.

    b. Per Data di fine, inserisci l'ultima data del monitoraggio del budget nel formato AAAA/MM/GG oppure scegli l'icona del calendario e seleziona una data.

    La data di fine predefinita è 120 giorni dalla data di inizio.
7. Per Importo del budget, inserisci l'importo in dollari del budget.
8. (Facoltativo) Ti consigliamo di creare avvisi relativi ai limiti. Nella sezione Limita le azioni, puoi implementare azioni automatiche che si verificano quando nel budget rimangono importi specifici. Per farlo, completa le seguenti fasi.

    a. Scegli Aggiungi nuova azione.

    b. In Importo rimanente, inserisci l'importo in dollari con cui desideri avviare l'azione.

    c. Nel menu a discesa Azione, scegli l'azione che desideri. Le azioni includono:

    - Interrompi dopo aver terminato il lavoro corrente: tutto il lavoro attualmente in esecuzione quando viene raggiunto l'importo della soglia continua a funzionare (e comporta costi) fino al termine.
    - Interruzione immediata del lavoro: tutto il lavoro viene annullato immediatamente quando viene raggiunto l'importo della soglia.

    d. Per creare avvisi di limite aggiuntivi, scegli Aggiungi nuova azione e ripeti i due passaggi precedenti.
9. Scegli Crea budget. Viene visualizzata la pagina di gestione del budget. Il budget appena creato viene visualizzato nella scheda Budget attivi.

Visualizza un budget

Dopo aver creato un budget, puoi visualizzarlo nella pagina Gestione del budget. Da qui, è possibile visualizzare l'importo totale del budget e il costo complessivo assegnato al budget specifico.

Per visualizzare un budget, utilizzare la procedura seguente.

1. Se non l'hai già fatto, accedi a AWS Management Console, apri la console Deadline Cloud, scegli una fattoria, quindi scegli Gestisci lavori.
2. Scegli Budget dal riquadro di navigazione a sinistra. Viene visualizzata la pagina Budget Manager.
3. Per visualizzare un budget attivo, scegli la scheda Budget attivi e scegli il nome del budget che desideri visualizzare. Viene visualizzata la pagina dei dettagli del budget.
4. Per visualizzare i dettagli del budget per un budget scaduto, scegli la scheda Budget inattivi. Quindi, scegli il nome del budget che desideri visualizzare. Viene visualizzata la pagina dei dettagli del budget.

Modifica un budget

Puoi modificare qualsiasi budget attivo. Per modificare un budget attivo, utilizzare la procedura seguente.

1. Se non l'hai già fatto, accedi a AWS Management Console, apri la console Deadline Cloud, scegli una fattoria, quindi scegli Gestisci lavori.
2. Dalla pagina Budget Manager, nella scheda Budget attivi, scegli il pulsante accanto al budget che desideri modificare.
3. Dal menu a discesa Azioni nell'angolo in alto a destra, seleziona Modifica budget.
4. Apporta le modifiche desiderate, quindi scegli Aggiorna budget.

Disattiva un budget

Puoi disattivare qualsiasi budget attivo. La disattivazione di un budget ne modifica lo stato da Attivo a Inattivo. Quando un budget viene disattivato, non tiene più traccia di una risorsa in base all'importo del budget.

Per disattivare un budget, utilizzare la procedura seguente.

1. Se non l'hai già fatto, accedi a AWS Management Console, apri la console Deadline Cloud, scegli una fattoria, quindi scegli Gestisci lavori.
2. Dalla pagina Gestione del budget, nella scheda Budget attivi, scegli il pulsante accanto al budget che desideri disattivare.

3. Dal menu a discesa Azioni nell'angolo in alto a destra, seleziona Disattiva budget. In pochi istanti, il budget selezionato passerà da Attivo a Inattivo e passerà dalla scheda Budget attivi alla scheda Budget inattivi.

Utilizzo dell'esploratore di utilizzo di Deadline Cloud

Con l'esploratore di utilizzo di Deadline Cloud, puoi visualizzare le metriche in tempo reale sull'attività che si svolge in ogni azienda agricola. Puoi esaminare i costi dell'azienda agricola in base a diverse variabili, ad esempio coda, lavoro, prodotto in licenza o tipi di istanza. Seleziona vari intervalli di tempo per visualizzare l'utilizzo in un determinato periodo di tempo e osserva le tendenze di utilizzo nel corso del tempo. Puoi anche visualizzare una suddivisione dettagliata dei punti dati selezionati, che consente di esaminare più da vicino le metriche. L'utilizzo può essere visualizzato in base al tempo (minuti e ore) o al costo ($ USD).

Le seguenti sezioni mostrano i passaggi per accedere e utilizzare l'esploratore di utilizzo di Deadline Cloud.

Argomenti

Prerequisito

Per utilizzare l'esploratore di utilizzo di Deadline Cloud, devi disporre delle autorizzazioni `MANAGER` o dell'`OWNER`azienda agricola. Per ulteriori informazioni, consulta Gestisci utenti e gruppi per fattorie, code e flotte.

Apri lo strumento di esplorazione dell'utilizzo

Per aprire l'esploratore di utilizzo di Deadline Cloud, utilizzare la seguente procedura.

1. Accedi AWS Management Console e apri la console Deadline Cloud.
2. Per vedere tutte le fattorie disponibili, scegli Visualizza fattorie.
3. Individua la fattoria sulla quale desideri ottenere informazioni, quindi scegli Gestisci lavori. Il monitor Deadline Cloud si apre in una nuova scheda.

4. Nel monitor Deadline Cloud, dal menu a sinistra, seleziona Usage explorer.

Usa lo strumento di esplorazione dell'utilizzo

Dalla pagina Usage Explorer, è possibile selezionare parametri specifici in cui è possibile visualizzare i dati. Per impostazione predefinita, viene visualizzato l'utilizzo totale in termini di tempo (ore e minuti) negli ultimi 7 giorni. È possibile modificare questi parametri e le informazioni visualizzate cambiano dinamicamente in base alle impostazioni dei parametri.

È possibile raggruppare i risultati in base alla coda, al processo, all'utilizzo del calcolo, al tipo di istanza o al prodotto in licenza. Se scegli un prodotto in licenza, i costi vengono calcolati per licenze specifiche. Per tutti gli altri gruppi, il tempo viene calcolato sommando il tempo impiegato per l'esecuzione di ciascuna attività.

L'Usage Explorer restituisce solo 100 risultati in base ai criteri di filtro impostati. I risultati sono elencati in ordine decrescente in base al timestamp della data di creazione. Se sono presenti più di 100 risultati, viene visualizzato un messaggio di errore. Puoi affinare la tua query per ridurre il numero di risultati:

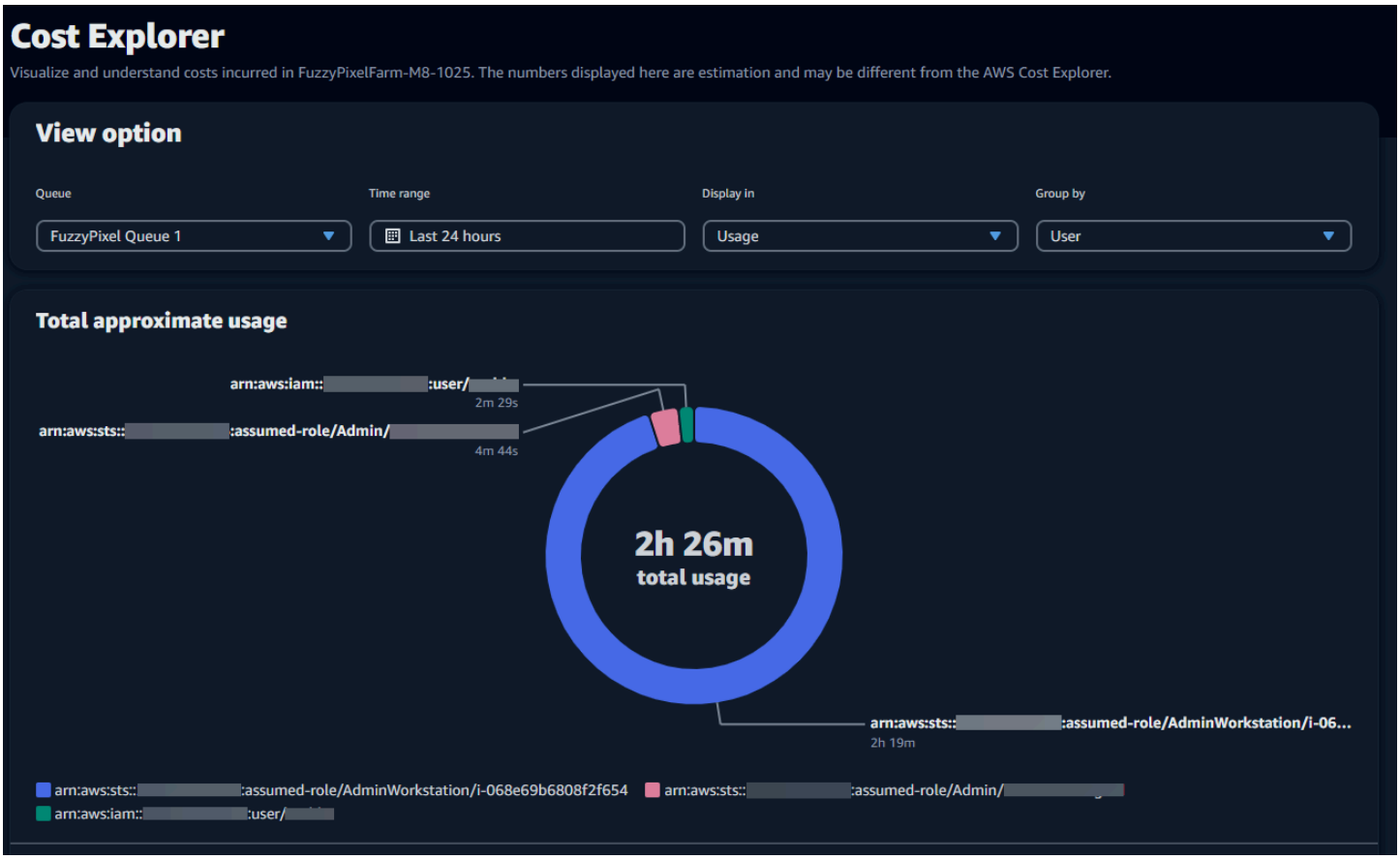
- Seleziona un intervallo di tempo più piccolo
- Seleziona meno code
- Seleziona un raggruppamento diverso, ad esempio il raggruppamento per coda anziché per lavoro

Argomenti

Usa grafici visivi per esaminare i dati

Puoi esaminare i dati in un formato visivo per identificare tendenze e aree potenziali che potrebbero richiedere maggiore analisi o attenzione. Usage explorer offre un grafico a torta che mostra l'utilizzo e i costi complessivi con la possibilità di raggruppare i totali in subtotali più piccoli.

> **Note**
>
> Il grafico mostra solo i primi cinque risultati con altri risultati combinati in una sezione «altri». Puoi visualizzare tutti i risultati nella sezione suddivisa sotto il grafico.



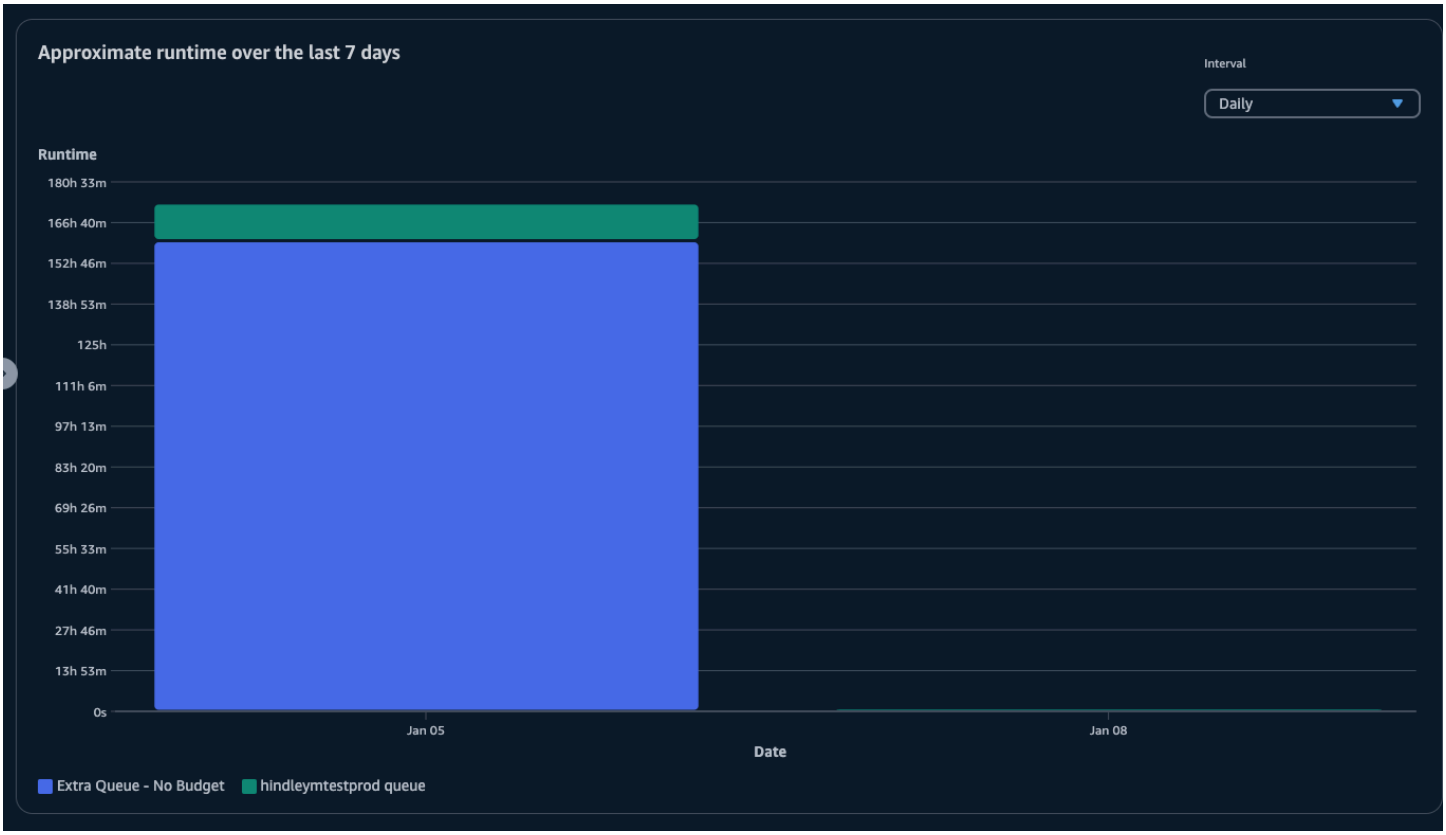
Visualizza una suddivisione delle metriche

Sotto il grafico a torta, Usage Explorer offre un'analisi più dettagliata di metriche specifiche, che cambieranno al variare dei parametri. Per impostazione predefinita, nell'Usage Explorer vengono visualizzati cinque risultati. Puoi scorrere i risultati utilizzando le frecce di impaginazione nella sezione di suddivisione.

La suddivisione è ridotta al minimo per impostazione predefinita. Per espandere e visualizzare i risultati, seleziona la freccia di ripartizione Visualizza tutto. Per scaricare la suddivisione, scegli Scarica dati.

Visualizza la durata approssimativa delle code

È inoltre possibile visualizzare la durata approssimativa delle code in base a diversi intervalli specificati. Le opzioni di intervallo sono orarie, giornaliere, settimanali e mensili. Dopo aver selezionato un intervallo, il grafico mostra la durata approssimativa delle code.



Gestione dei costi

AWS Deadline Cloud fornisce i budget e lo strumento di esplorazione dell'utilizzo per aiutarti a controllare e visualizzare i costi dei tuoi lavori. Tuttavia, Deadline Cloud utilizza altri AWS servizi, come Amazon S3. I costi di tali servizi non si riflettono nei budget di Deadline Cloud o nell'Usage Explorer e vengono addebitati separatamente in base all'utilizzo. A seconda di come configuri Deadline Cloud, puoi utilizzare i seguenti AWS servizi, oltre ad altri:

Servizio	Pagina dei prezzi
CloudWatch Registri Amazon	Prezzi di Amazon CloudWatch Logs
Amazon Elastic Compute Cloud	Prezzi di Amazon Elastic Compute Cloud

Servizio	Pagina dei prezzi
AWS Key Management Service	Prezzi di AWS Key Management Service
AWS PrivateLink	Prezzi di AWS PrivateLink
Amazon Simple Storage Service	Prezzi di Amazon S3
Amazon Virtual Private Cloud	Prezzi di Amazon Virtual Private Cloud

Best practice per la gestione dei costi

L'utilizzo delle seguenti best practice può aiutarti a comprendere e controllare i costi quando utilizzi Deadline Cloud e i compromessi che puoi fare tra costi ed efficienza.

> **Note**
>
> Il costo finale dell'utilizzo di Deadline Cloud dipende dall'interazione tra una serie di AWS servizi, dalla quantità di lavoro che elabori e dal Regione AWS luogo in cui esegui i lavori. Le seguenti best practice sono linee guida e potrebbero non ridurre in modo significativo i costi.

Procedure consigliate per i CloudWatch log

Deadline Cloud invia i registri dei lavoratori e delle attività a Logs. CloudWatch La raccolta, l'archiviazione e l'analisi di questi registri sono a carico dell'utente. È possibile ridurre i costi registrando solo la quantità minima di dati necessaria per monitorare le attività.

Quando crei una coda o una flotta, Deadline Cloud crea un gruppo di log CloudWatch Logs con i seguenti nomi:

- `aws/deadline/<FARM_ID>/<FLEET_ID>`
- `aws/deadline/<FARM_ID>/<QUEUE_ID>`

Per impostazione predefinita, questi registri non scadono mai. È possibile modificare la politica di conservazione dei gruppi di log per rimuovere i vecchi log e contribuire a ridurre i costi di archiviazione. Puoi anche esportare i log in Amazon S3. I costi di storage di Amazon S3 sono inferiori a quelli di. CloudWatch Per ulteriori informazioni, consulta Esportazione di dati di log su Amazon S3.

Best practice per Amazon EC2

Puoi utilizzare le istanze Amazon EC2 sia per flotte gestite dal servizio che per quelle gestite dai clienti. Esistono tre considerazioni:

- Per le flotte gestite dai servizi, puoi scegliere di avere una o più istanze sempre disponibili impostando il numero minimo di lavoratori per il parco macchine. Quando si imposta il numero minimo di lavoratori su un valore superiore a 0, il parco macchine ha sempre questo numero di lavoratori in funzione. Ciò può ridurre il tempo impiegato da Deadline Cloud per avviare l'elaborazione dei lavori, tuttavia ti verrà addebitato il tempo di inattività dell'istanza.
- Per le flotte gestite dai servizi, imposta una dimensione massima per la flotta. Ciò limita il numero di istanze su cui una flotta può scalare automaticamente. Le flotte non supereranno queste dimensioni anche se ci sono più posti di lavoro in attesa di essere elaborati.
- Sia per le flotte gestite dal servizio che per quelle gestite dal cliente, puoi specificare i tipi di istanze Amazon EC2 nelle tue flotte. L'utilizzo di istanze più piccole costa meno al minuto, ma può richiedere più tempo per completare un processo. Al contrario, un'istanza più grande costa di più al minuto, ma può ridurre il tempo necessario per completare un processo. Comprendere le esigenze che i vostri lavori impongono a un'istanza può aiutarvi a ridurre i costi.
- Quando possibile, scegli le istanze Spot di Amazon EC2 per la tua flotta. Le istanze Spot sono disponibili a un prezzo ridotto, ma possono essere interrotte da richieste on-demand. Le istanze on demand vengono addebitate al secondo e non vengono interrotte.

Le migliori pratiche per AWS KMS

Per impostazione predefinita, Deadline Cloud crittografa i tuoi dati con una chiave AWS proprietaria. Non ti viene addebitato alcun costo per questa chiave.

Puoi scegliere di utilizzare una chiave gestita dal cliente per crittografare i tuoi dati. Quando utilizzi la tua chiave, ti viene addebitato un costo in base a come viene utilizzata la chiave. Se utilizzi una chiave esistente, questo sarà un costo incrementale per l'uso aggiuntivo.

Le migliori pratiche per AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione tra il tuo VPC e Deadline Cloud utilizzando un endpoint di interfaccia. Quando crei una connessione, puoi chiamare tutte le azioni dell'API Deadline Cloud. Ti viene addebitato un costo orario per ogni endpoint che crei. Se lo utilizzi PrivateLink, devi creare almeno tre endpoint e, a seconda della configurazione, potrebbero essere necessari fino a cinque.

Le migliori pratiche per Amazon S3

Deadline Cloud utilizza Amazon S3 per archiviare risorse per l'elaborazione, gli allegati di lavoro, l'output e i log. Per ridurre i costi associati ad Amazon S3, riduci la quantità di dati archiviati. Alcuni suggerimenti:

- Archivia solo le risorse attualmente in uso o che verranno utilizzate a breve.
- Utilizza una configurazione S3 Lifecycle per eliminare automaticamente i file inutilizzati da un bucket S3.

Le migliori pratiche per Amazon VPC

Quando utilizzi licenze basate sull'utilizzo per la tua flotta gestita dal cliente, crei un endpoint di licenza Deadline Cloud, ovvero un endpoint Amazon VPC creato nel tuo account. Questo endpoint viene addebitato in base a una tariffa oraria. Per ridurre i costi, rimuovi gli endpoint quando non utilizzi licenze basate sull'utilizzo.

Sicurezza in Deadline Cloud

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità applicabili AWS Deadline Cloud, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal Servizio AWS materiale che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo Deadline Cloud. I seguenti argomenti mostrano come eseguire la configurazione Deadline Cloud per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere Deadline Cloud le tue risorse.

Argomenti

Protezione dei dati in Deadline Cloud

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Deadline Cloud. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi la console, l'API Deadline Cloud o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

Crittografia dei dati a riposo

AWS Deadline Cloud protegge i dati sensibili crittografandoli quando sono inattivi utilizzando le chiavi di crittografia memorizzate in AWS Key Management Service ()AWS KMS. La crittografia a riposo è disponibile Regioni AWS ovunque Deadline Cloud sia disponibile.

La crittografia dei dati significa che i dati sensibili salvati su disco non sono leggibili da un utente o da un'applicazione senza una chiave valida. Solo chi dispone di una chiave gestita valida può decrittografare i dati.

Per informazioni sulle modalità di Deadline Cloud utilizzo della crittografia AWS KMS dei dati inattivi, consulta. Gestione delle chiavi

Crittografia in transito

Per i dati in transito, AWS Deadline Cloud utilizza Transport Layer Security (TLS) 1.2 o 1.3 per crittografare i dati inviati tra il servizio e i lavoratori. È richiesto TLS 1.2 ed è consigliato TLS 1.3. Inoltre, se utilizzi un cloud privato virtuale (VPC), puoi utilizzare AWS PrivateLink per stabilire una connessione privata tra il tuo VPC e. Deadline Cloud

Gestione delle chiavi

Quando crei una nuova farm, puoi scegliere una delle seguenti chiavi per crittografare i dati della tua fattoria:

- AWS chiave KMS proprietaria: tipo di crittografia predefinito se non si specifica una chiave quando si crea la farm. La chiave KMS è di proprietà di. AWS Deadline Cloud Non puoi visualizzare, gestire o utilizzare chiavi AWS di proprietà. Tuttavia, non è necessario intraprendere alcuna azione per proteggere le chiavi che crittografano i dati. Per ulteriori informazioni, consulta le chiavi AWS possedute nella guida per gli AWS Key Management Service sviluppatori.
- Chiave KMS gestita dal cliente: si specifica una chiave gestita dal cliente quando si crea una farm. Tutto il contenuto all'interno della farm è crittografato con la chiave KMS. La chiave è memorizzata

nel tuo account e viene creata, posseduta e gestita da te e vengono applicati dei AWS KMS costi. Hai il pieno controllo sulla chiave KMS. Puoi eseguire attività come:

- Stabilire e mantenere le politiche chiave
- Stabilire e mantenere le policy e le sovvenzioni IAM
- Abilitare e disabilitare le policy delle chiavi
- Aggiungere tag
- Creare alias delle chiavi

Non è possibile ruotare manualmente una chiave di proprietà del cliente utilizzata in un' Deadline Cloud azienda agricola. È supportata la rotazione automatica della chiave.

Per ulteriori informazioni, consulta Customer Owned keys nella AWS Key Management Service Developer Guide.

Per creare una chiave gestita dal cliente, segui i passaggi per la creazione di chiavi gestite dal cliente simmetriche nella Guida per gli AWS Key Management Service sviluppatori.

Come utilizzare le sovvenzioni Deadline CloudAWS KMS

Deadline Cloud richiede una concessione per utilizzare la chiave gestita dal cliente. Quando crei una farm crittografata con una chiave gestita dal cliente, Deadline Cloud crea una concessione per tuo conto inviando una `CreateGrant` richiesta AWS KMS per ottenere l'accesso alla chiave KMS specificata.

Deadline Cloud utilizza più sovvenzioni. Ogni concessione viene utilizzata da una parte diversa Deadline Cloud che deve crittografare o decrittografare i dati. Deadline Cloud utilizza anche sovvenzioni per consentire l'accesso ad altri AWS servizi utilizzati per archiviare dati per tuo conto, come Amazon Simple Storage Service, Amazon Elastic Block Store o OpenSearch.

Le sovvenzioni che consentono Deadline Cloud di gestire le macchine in un parco macchine gestito dai servizi includono un numero di Deadline Cloud account e un ruolo `GranteePrincipal` anziché un responsabile del servizio. Sebbene non sia tipico, ciò è necessario per crittografare i volumi Amazon EBS per i lavoratori delle flotte gestite dai servizi utilizzando la chiave KMS gestita dal cliente specificata per la farm.

Policy delle chiavi gestite dal cliente

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave deve avere esattamente una policy chiave che contenga istruzioni che determinano chi può utilizzare la chiave e come può usarla. Quando si crea la chiave gestita dal cliente, è possibile specificare una politica chiave. Per ulteriori informazioni, consulta Gestione dell'accesso alle chiavi gestite dal cliente nella Guida per gli sviluppatori di AWS Key Management Service .

Policy IAM minima per CreateFarm

Per utilizzare la chiave gestita dal cliente per creare farm utilizzando la console o il funzionamento dell'`CreateFarm`API, devono essere consentite le seguenti operazioni AWS KMS API:

- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso della console a una AWS KMS chiave specificata. Per maggiori informazioni, consulta Using grants nella guida per AWS Key Management Service sviluppatori.
- `kms:Decrypt`— Consente di Deadline Cloud decrittografare i dati nella fattoria.
- `kms:DescribeKey`— Fornisce i dettagli chiave gestiti dal cliente per consentire Deadline Cloud la convalida della chiave.
- `kms:GenerateDataKey`— Consente di Deadline Cloud crittografare i dati utilizzando una chiave dati unica.

La seguente dichiarazione politica concede le autorizzazioni necessarie per l'operazione. `CreateFarm`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineCreateGrants",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/1234567890abcdef0",
            "Condition": {
                "StringEquals": {
```

```
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Policy IAM minima per operazioni di sola lettura

Utilizzare la chiave gestita dal cliente per Deadline Cloud operazioni di sola lettura, ad esempio per ottenere informazioni su fattorie, code e flotte. Le seguenti operazioni AWS KMS API devono essere consentite:

- `kms:Decrypt`— Consente di Deadline Cloud decrittografare i dati nella farm.
- `kms:DescribeKey`— Fornisce i dettagli chiave gestiti dal cliente per consentire Deadline Cloud la convalida della chiave.

La seguente dichiarazione politica concede le autorizzazioni necessarie per le operazioni di sola lettura.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineReadOnly",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Policy IAM minima per le operazioni di lettura/scrittura

Utilizzare la chiave gestita dal cliente per Deadline Cloud operazioni di lettura/scrittura, come la creazione e l'aggiornamento di fattorie, code e flotte. Le seguenti operazioni AWS KMS API devono essere consentite:

- `kms:Decrypt`— Consente di Deadline Cloud decrittografare i dati nella farm.
- `kms:DescribeKey`— Fornisce i dettagli chiave gestiti dal cliente per consentire Deadline Cloud la convalida della chiave.
- `kms:GenerateDataKey`— Consente di Deadline Cloud crittografare i dati utilizzando una chiave dati unica.

La seguente dichiarazione politica concede le autorizzazioni necessarie per l'operazione. `CreateFarm`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineReadWrite",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey",
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Monitoraggio delle chiavi di crittografia

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue Deadline Cloud farm, puoi utilizzare AWS CloudTrailAmazon CloudWatch Logs per tenere traccia delle richieste Deadline Cloud inviate a AWS KMS.

CloudTrail evento per borse di studio

L' CloudTrail evento di esempio seguente si verifica quando vengono create le sovvenzioni, in genere quando si chiama l'`CreateFarm`operazione`CreateMonitor`, or`CreateFleet`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T02:05:26Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T02:05:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "operations": [
```

```
            "CreateGrant",
            "Decrypt",
            "DescribeKey",
            "Encrypt",
            "GenerateDataKey"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
                "aws:deadline:accountId": "111122223333"
            }
        },
        "granteePrincipal": "deadline.amazonaws.com",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "retiringPrincipal": "deadline.amazonaws.com"
    },
    "responseElements": {
        "grantId": "6bbe819394822a400fe5e3a75d0e9ef16c1733143fff0c1fc00dc7ac282a18a0",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE44444"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


CloudTrail evento per la decrittografia

L' CloudTrail evento di esempio seguente si verifica quando si decrittografano i valori utilizzando la chiave KMS gestita dal cliente.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:51:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeffffff",
```

```
    "eventID": "ffffffff-eeee-dddd-cccc-bbbbbbaaaaaa",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CloudTrail evento per la crittografia

L' CloudTrail evento di esempio seguente si verifica quando si crittografano i valori utilizzando la chiave KMS gestita dal cliente.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
```

```
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "keyId": "arn:aws::kms:us-
west-2:111122223333:key/abcdef12-3456-7890-0987-654321fedcba"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Eliminazione di una chiave KMS gestita dal cliente

L'eliminazione di una chiave KMS gestita dal cliente in AWS Key Management Service (AWS KMS) è distruttiva e potenzialmente pericolosa. Elimina in modo irreversibile il materiale chiave e tutti i metadati associati alla chiave. Dopo l'eliminazione di una chiave KMS gestita dal cliente, non è

più possibile decrittografare i dati crittografati con quella chiave. Ciò significa che i dati diventano irrecuperabili.

Questo è il motivo per cui AWS KMS offre ai clienti un periodo di attesa fino a 30 giorni prima di eliminare la chiave KMS. Il periodo di attesa predefinito è di 30 giorni.

Informazioni sul periodo di attesa

Poiché eliminare una chiave KMS gestita dal cliente è distruttivo e potenzialmente pericoloso, ti chiediamo di impostare un periodo di attesa di 7—30 giorni. Il periodo di attesa predefinito è di 30 giorni.

Tuttavia, il periodo di attesa effettivo potrebbe essere fino a 24 ore più lungo del periodo pianificato. Per ottenere la data e l'ora effettive in cui la chiave verrà eliminata, utilizzare l'DescribeKeyoperazione. È inoltre possibile visualizzare la data di eliminazione pianificata di una chiave nella AWS KMS console nella pagina di dettaglio della chiave, nella sezione Configurazione generale. Nota il fuso orario.

Durante il periodo di attesa, lo stato e lo stato della chiave gestita dal cliente sono In attesa di eliminazione.

- Una chiave KMS gestita dal cliente in attesa di eliminazione non può essere utilizzata in alcuna operazione crittografica.
- AWS KMS non ruota le chiavi di supporto delle chiavi KMS gestite dal cliente in attesa di eliminazione.

Per ulteriori informazioni sull'eliminazione di una chiave KMS gestita dal cliente, consulta Eliminazione delle chiavi principali del cliente nella Guida per gli sviluppatori.AWS Key Management Service

Riservatezza del traffico Internet

AWS Deadline Cloud supporta Amazon Virtual Private Cloud (Amazon VPC) per proteggere le connessioni. Amazon VPC offre funzionalità che puoi utilizzare per aumentare e monitorare la sicurezza del tuo cloud privato virtuale (VPC).

Puoi configurare una flotta gestita dal cliente (CMF) con istanze Amazon Elastic Compute Cloud (Amazon EC2) eseguite all'interno di un VPC. Implementando gli endpoint Amazon VPC da AWS PrivateLink utilizzare, il traffico tra i lavoratori del tuo CMF e l'endpoint rimane all'interno Deadline

Cloud del tuo VPC. Inoltre, puoi configurare il tuo VPC per limitare l'accesso a Internet alle tue istanze.

Nelle flotte gestite dai servizi, i lavoratori non sono raggiungibili da Internet, ma hanno accesso a Internet e si connettono al servizio tramite Internet. Deadline Cloud

Rifiuta il consenso

AWS Deadline Cloud raccoglie determinate informazioni operative per aiutarci a svilupparci e migliorare Deadline Cloud. I dati raccolti includono elementi come l'ID del tuo AWS account e l'ID utente, in modo che possiamo identificarti correttamente in caso di problemi con. Deadline Cloud Raccogliamo anche informazioni Deadline Cloud specifiche, come i Resource ID (un FarmID o QueueID se applicabile), il nome del prodotto (ad esempio, JobAttachments WorkerAgent, e altro) e la versione del prodotto.

Puoi scegliere di rinunciare a questa raccolta di dati utilizzando la configurazione dell'applicazione. Ogni computer con cui interagisce Deadline Cloud, sia le postazioni di lavoro dei clienti che gli addetti alla flotta, deve disattivarlo separatamente.

Deadline Cloud monitor - desktop

Deadline Cloud monitor - desktop raccoglie informazioni operative, ad esempio quando si verificano arresti anomali e quando l'applicazione viene aperta, per aiutarci a sapere quando si verificano problemi con l'applicazione. Per disattivare la raccolta di queste informazioni operative, vai alla pagina delle impostazioni e deseleziona Attiva la raccolta dei dati per misurare le prestazioni di Deadline Cloud Monitor.

Dopo la disattivazione, il monitor desktop non invia più i dati operativi. Tutti i dati raccolti in precedenza vengono conservati e possono ancora essere utilizzati per migliorare il servizio. Per ulteriori informazioni, consulta le Domande frequenti sulla privacy dei dati in .

AWS Deadline Cloud CLI e strumenti

La AWS Deadline Cloud CLI, i mittenti e l'agente di lavoro raccolgono tutti informazioni operative, ad esempio quando si verificano arresti anomali e quando vengono inviati lavori, per aiutarci a sapere quando si verificano problemi con queste applicazioni. Per rinunciare alla raccolta di queste informazioni operative, utilizza uno dei seguenti metodi:

- Nel terminale, inserisci**`deadline config set telemetry.opt_out true`**.

  Ciò disattiverà la CLI, i mittenti e il worker agent quando viene eseguito come utente corrente.

- Quando installi il Deadline Cloud worker agent, aggiungi l'argomento della **`--telemetry-opt-out`** riga di comando. Ad esempio, **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**.
- Prima di eseguire l'agente di lavoro, la CLI o il mittente, imposta una variabile di ambiente: **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

Dopo la disattivazione, gli Deadline Cloud strumenti non inviano più i dati operativi. Tutti i dati raccolti in precedenza vengono conservati e possono ancora essere utilizzati per migliorare il servizio. Per ulteriori informazioni, consulta le Domande frequenti sulla privacy dei dati in .

Identity and Access Management in Deadline Cloud

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Deadline Cloud. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona Deadline Cloud con IAM
- Esempi di policy basate sull'identità per Deadline Cloud
- AWS politiche gestite per Deadline Cloud
- Risoluzione dei problemi relativi all'identità e all'accesso a AWS Deadline Cloud

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Deadline Cloud.

Utente del servizio: se utilizzi il servizio Deadline Cloud per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità

di Deadline Cloud per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Deadline Cloud, consulta. Risoluzione dei problemi relativi all'identità e all'accesso a AWS Deadline Cloud

Amministratore del servizio: se sei responsabile delle risorse di Deadline Cloud presso la tua azienda, probabilmente hai pieno accesso a Deadline Cloud. È tuo compito determinare a quali funzionalità e risorse di Deadline Cloud gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Deadline Cloud, consulta. Come funziona Deadline Cloud con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a Deadline Cloud. Per visualizzare esempi di policy basate sull'identità di Deadline Cloud che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Deadline Cloud

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del

metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali

temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni,

crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo

`Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Deadline Cloud con IAM

Prima di utilizzare IAM per gestire l'accesso a Deadline Cloud, scopri quali funzionalità IAM sono disponibili per l'uso con Deadline Cloud.

Funzionalità IAM che puoi utilizzare con AWS Deadline Cloud

Funzionalità IAM	Supporto Deadline Cloud
Policy basate su identità	Sì
Policy basate su risorse	No

Funzionalità IAM	Supporto Deadline Cloud
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come Deadline Cloud e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Deadline Cloud

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy

JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Deadline Cloud

Per visualizzare esempi di politiche basate sull'identità di Deadline Cloud, consulta. Esempi di policy basate sull'identità per Deadline Cloud

Politiche basate sulle risorse all'interno di Deadline Cloud

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per Deadline Cloud

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Deadline Cloud, consulta Azioni definite da AWS Deadline Cloud nel Service Authorization Reference.

Le azioni politiche in Deadline Cloud utilizzano il seguente prefisso prima dell'azione:

```
deadline
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "deadline:action1",
      "deadline:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di Deadline Cloud, consulta. Esempi di policy basate sull'identità per Deadline Cloud

Risorse politiche per Deadline Cloud

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN).

Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse Deadline Cloud e dei relativi ARN, consulta Risorse definite da AWS Deadline Cloud nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, vedi Azioni definite da AWS Deadline Cloud.

Per visualizzare esempi di politiche basate sull'identità di Deadline Cloud, consulta. Esempi di policy basate sull'identità per Deadline Cloud

Chiavi relative alle condizioni delle policy per Deadline Cloud

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome

utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di Deadline Cloud, consulta Condition keys for AWS Deadline Cloud nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Deadline Cloud.

Per visualizzare esempi di politiche basate sull'identità di Deadline Cloud, consulta. Esempi di policy basate sull'identità per Deadline Cloud

ACL in Deadline Cloud

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Deadline Cloud

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Deadline Cloud

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Deadline Cloud

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS,

in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Deadline Cloud

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Deadline Cloud. Modifica i ruoli di servizio solo quando Deadline Cloud fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Deadline Cloud

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Deadline Cloud

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Deadline Cloud. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l' AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da Deadline Cloud, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per AWS Deadline Cloud nel Service Authorization Reference.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Deadline Cloud nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni

che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Deadline Cloud

Per accedere alla console AWS Deadline Cloud, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Deadline Cloud presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console Deadline Cloud, collega anche Deadline Cloud *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Politica per l'invio di lavori a una coda

In questo esempio, si crea una politica ristretta che concede l'autorizzazione a inviare lavori a una coda specifica in una fattoria specifica.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SubmitJobsFarmAndQueue",
            "Effect": "Allow",
            "Action": "deadline:CreateJob",
            "Resource": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_A/queue/QUEUE_B/
job/*"
        }
    ]
}
```

Politica per consentire la creazione di un endpoint di licenza

In questo esempio, si crea una policy ristretta che concede le autorizzazioni necessarie per creare e gestire gli endpoint di licenza. Utilizza questa politica per creare l'endpoint di licenza per il VPC associato alla tua farm.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "SID": "CreateLicenseEndpoint",
        "Effect": "Allow",
        "Action": [
            "deadline:CreateLicenseEndpoint",
            "deadline:DeleteLicenseEndpoint",
            "deadline:GetLicenseEndpoint",
            "deadline:UpdateLicenseEndpoint",
            "deadline:ListLicenseEndpoints",
            "deadline:PutMeteredProduct",
            "deadline:DeleteMeteredProduct",
```

```
            "deadline:ListMeteredProducts",
            "deadline:ListAvailableMeteredProducts",
            "ec2:CreateVpcEndpoint",
            "ec2:DescribeVpcEndpoints",
            "ec2:DeleteVpcEndpoints"
        ],
        "Resource": "*"
    }]
}
```

Politica per consentire il monitoraggio di una coda specifica della fattoria

In questo esempio, si crea una politica ristretta che concede l'autorizzazione a monitorare i lavori in una coda specifica per una determinata azienda agricola.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "MonitorJobsFarmAndQueue",
        "Effect": "Allow",
        "Action": [
            "deadline:SearchJobs",
            "deadline:ListJobs",
            "deadline:GetJob",
            "deadline:SearchSteps",
            "deadline:ListSteps",
            "deadline:ListStepConsumers",
            "deadline:ListStepDependencies",
            "deadline:GetStep",
            "deadline:SearchTasks",
            "deadline:ListTasks",
            "deadline:GetTask",
            "deadline:ListSessions",
            "deadline:GetSession",
            "deadline:ListSessionActions",
            "deadline:GetSessionAction"
        ],
        "Resource": [
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B",
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B/*"
        ]
    }]
}
```

AWS politiche gestite per Deadline Cloud

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSDeadlineCloud-FleetWorker

Puoi allegare la `AWSDeadlineCloud-FleetWorker` policy alle tue identità AWS Identity and Access Management (IAM).

Questa politica concede ai lavoratori di questa flotta le autorizzazioni necessarie per connettersi e ricevere attività dal servizio.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente ai dirigenti di gestire i lavoratori di una flotta.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud la guida di riferimento di AWS Managed Policy. FleetWorker

AWS politica gestita: AWSDeadlineCloud-WorkerHost

È possibile allegare la policy `AWSDeadlineCloud-WorkerHost`alle identità IAM.

Questa politica concede le autorizzazioni necessarie per connettersi inizialmente al servizio. Può essere usato come profilo di istanza Amazon Elastic Compute Cloud (Amazon EC2).

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente ai dirigenti di creare lavoratori.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud la guida di riferimento di AWS Managed Policy. WorkerHost

AWS politica gestita: AWSDeadlineCloud-UserAccessFarms

È possibile allegare la policy `AWSDeadlineCloud-UserAccessFarms`alle identità IAM.

Questa politica consente agli utenti di accedere ai dati delle aziende agricole in base alle aziende agricole di cui sono membri e al loro livello di iscrizione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente all'utente di accedere ai dati dell'azienda agricola.
- `ec2`— Consente agli utenti di visualizzare i dettagli sui tipi di istanze Amazon EC2.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud- UserAccess Farms in the AWS Managed Policy reference guide.

AWS politica gestita: AWSDeadlineCloud-UserAccessFleets

È possibile allegare la policy `AWSDeadlineCloud-UserAccessFleets`alle identità IAM.

Questa politica consente agli utenti di accedere ai dati della flotta in base alle aziende agricole di cui sono membri e al loro livello di iscrizione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente all'utente di accedere ai dati dell'azienda agricola.
- `ec2`— Consente agli utenti di visualizzare i dettagli sui tipi di istanze Amazon EC2.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud- UserAccess Fleets in the AWS Managed Policy reference guide.

AWS politica gestita: AWSDeadlineCloud-UserAccessJobs

È possibile allegare la policy `AWSDeadlineCloud-UserAccessJobs`alle identità IAM.

Questa politica consente agli utenti di accedere ai dati sulle offerte di lavoro in base alle aziende agricole di cui sono membri e al loro livello di iscrizione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente all'utente di accedere ai dati dell'azienda agricola.
- `ec2`— Consente agli utenti di visualizzare i dettagli sui tipi di istanze Amazon EC2.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud- UserAccess Jobs in the AWS Managed Policy reference guide.

AWS politica gestita: AWSDeadlineCloud-UserAccessQueues

È possibile allegare la policy `AWSDeadlineCloud-UserAccessQueues`alle identità IAM.

Questa politica consente agli utenti di accedere ai dati delle code in base alle farm di cui sono membri e al loro livello di iscrizione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `deadline`— Consente all'utente di accedere ai dati dell'azienda agricola.

- `ec2`— Consente agli utenti di visualizzare i dettagli sui tipi di istanze Amazon EC2.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-UserAccessQueues in the AWS Managed Policy reference guide.

Aggiornamenti di Deadline Cloud alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Deadline Cloud da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Deadline Cloud.

Modifica	Descrizione	Data
Deadline Cloud ha iniziato a tracciare le modifiche	Deadline Cloud ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	2 aprile 2024

Risoluzione dei problemi relativi all'identità e all'accesso a AWS Deadline Cloud

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Deadline Cloud e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Deadline Cloud
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Deadline Cloud

Non sono autorizzato a eseguire un'azione in Deadline Cloud

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `deadline:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 deadline:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `deadline:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Deadline Cloud.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Deadline Cloud. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Deadline Cloud

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Deadline Cloud supporta queste funzionalità, consulta. Come funziona Deadline Cloud con IAM
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Convalida della conformità per Deadline Cloud

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Deadline Cloud

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

AWS Deadline Cloud non esegue il backup dei dati memorizzati nel bucket S3 degli allegati di lavoro. Puoi abilitare i backup dei dati dei tuoi allegati di lavoro utilizzando qualsiasi meccanismo di backup standard di Amazon S3, come S3 Versioning o. AWS Backup

Sicurezza dell'infrastruttura in Deadline Cloud

In quanto servizio gestito, AWS Deadline Cloud è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Deadline Cloud attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Deadline Cloud non supporta l'utilizzo di policy per gli endpoint del cloud privato AWS PrivateLink virtuale (VPC). Utilizza la politica AWS PrivateLink predefinita, che garantisce l'accesso completo all'endpoint. Per ulteriori informazioni, consulta la policy predefinita per gli endpoint nella guida per l'AWS PrivateLink utente.

Configurazione e analisi delle vulnerabilità in Deadline Cloud

AWS gestisce le attività di sicurezza di base come l'applicazione di patch al sistema operativo guest (OS) e al database, la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori dettagli, consulta le seguenti risorse :

- Modello di responsabilità condivisa
- Amazon Web Services: panoramica dei processi di sicurezza (whitepaper)

AWS Deadline Cloud gestisce le attività su flotte gestite dai servizi o dai clienti:

- Per le flotte gestite dai servizi, Deadline Cloud gestisce il sistema operativo ospite.
- Per le flotte gestite dai clienti, sei responsabile della gestione del sistema operativo.

Per ulteriori informazioni sulla configurazione e l'analisi delle vulnerabilità per AWS Deadline Cloud, consulta

- Best practice di sicurezza per Deadline Cloud

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare aws:SourceArnle chiavi di contesto della condizione aws:SourceAccountglobale nelle politiche delle risorse per limitare le autorizzazioni che AWS Deadline Cloud forniscono un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'Amazon Resource Name (ARN) completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:deadline:*:`*`123456789012`*`:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition Deadline Cloud per evitare il confuso problema del vice.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "deadline.amazonaws.com"
    },
    "Action": "deadline:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:deadline:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Accesso AWS Deadline Cloud tramite un'interfaccia endpoint ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. AWS Deadline Cloud Puoi accedere Deadline Cloud come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. Deadline Cloud

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a Deadline Cloud.

Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida di AWS PrivateLink .

Considerazioni per Deadline Cloud

Prima di configurare un endpoint di interfaccia per Deadline Cloud, consulta Accedere a un servizio AWS utilizzando un endpoint VPC di interfaccia nella Guida.AWS PrivateLink

Deadline Cloud supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Per impostazione predefinita, l'accesso completo a Deadline Cloud è consentito tramite l'endpoint dell'interfaccia. In alternativa, è possibile associare un gruppo di sicurezza alle interfacce di rete dell'endpoint per controllare il traffico che Deadline Cloud attraversa l'endpoint dell'interfaccia.

Deadline Cloud non supporta le policy degli endpoint VPC. Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Guida.AWS PrivateLink

Deadline Cloud endpoint

Deadline Cloud utilizza due endpoint per l'accesso al servizio utilizzando. AWS PrivateLink

I lavoratori utilizzano l'`com.amazonaws.`*`region`*`.deadline.scheduling`endpoint per prelevare le attività dalla coda, segnalarne lo stato di avanzamento e rispedirne l'output. Deadline Cloud Se

si utilizza una flotta gestita dal cliente, l'endpoint di pianificazione è l'unico endpoint da creare, a meno che non si utilizzino operazioni di gestione. Ad esempio, se un job crea più lavori, è necessario abilitare l'endpoint di gestione a richiamare l'operazione. `CreateJob`

Il Deadline Cloud monitor utilizza il `com.amazonaws.`*`region`*`.deadline.management` per gestire le risorse della fattoria, ad esempio per creare e modificare code e flotte o ottenere elenchi di lavori, fasi e attività.

Deadline Cloud richiede anche endpoint per i seguenti endpoint di servizio: AWS

- Deadline Cloud utilizza AWS STS per autenticare i lavoratori in modo che possano accedere alle risorse lavorative. Per ulteriori informazioni in merito AWS STS, consulta Credenziali di sicurezza temporanee in IAM nella Guida per l'AWS Identity and Access Management utente.
- Se configuri la tua flotta gestita dai clienti in una sottorete senza connessione Internet, devi creare un endpoint VPC per CloudWatch Amazon Logs in modo che gli operatori possano scrivere i log. Per ulteriori informazioni, consulta Monitoraggio con. CloudWatch
- Se utilizzi gli allegati di lavoro, devi creare un endpoint VPC per Amazon Simple Storage Service (Amazon S3) Let's Amazon S3) in modo che i lavoratori possano accedere agli allegati. Per ulteriori informazioni, vedere Job attachments in Deadline Cloud.

Crea endpoint per Deadline Cloud

Puoi creare endpoint di interfaccia per Deadline Cloud utilizzare la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea endpoint di gestione e pianificazione per l' Deadline Cloud utilizzo dei seguenti nomi di servizio. Sostituisci la *`regione`* con quella Regione AWS in cui hai distribuito. Deadline Cloud

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Se abiliti il DNS privato per gli endpoint dell'interfaccia, puoi effettuare richieste API Deadline Cloud utilizzando il nome DNS regionale predefinito. Ad esempio, `worker.deadline.us-east-1.amazonaws.com` per le operazioni dei lavoratori o `management.deadline.us-east-1.amazonaws.com` per tutte le altre operazioni.

È inoltre necessario creare un endpoint per l' AWS STS utilizzo del seguente nome di servizio:

```
com.amazonaws.region.sts
```

Se la flotta gestita dal cliente si trova su una sottorete senza una connessione Internet, è necessario creare un endpoint CloudWatch Logs utilizzando il seguente nome di servizio:

```
com.amazonaws.region.logs
```

Se utilizzi gli allegati di lavoro per trasferire file, devi creare un endpoint Amazon S3 utilizzando il seguente nome di servizio:

```
com.amazonaws.region.s3
```

Best practice di sicurezza per Deadline Cloud

AWS Deadline Cloud (Deadline Cloud) offre una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

> **Note**
>
> Per ulteriori informazioni sull'importanza di molti argomenti relativi alla sicurezza, consulta il Modello di responsabilità condivisa.

Protezione dei dati

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare account individuali con AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.

- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza servizi di sicurezza gestiti avanzati come Amazon Macie, che aiuta a scoprire e proteggere i dati personali archiviati in Amazon Simple Storage Service (Amazon S3).
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Consigliamo di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero come un campo Nome. Ciò include quando lavori con AWS Deadline Cloud o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS Tutti i dati che inserisci in Deadline Cloud o in altri servizi potrebbero essere raccolti per essere inclusi nei registri di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

AWS Identity and Access Management autorizzazioni

Gestisci l'accesso alle AWS risorse utilizzando utenti, ruoli AWS Identity and Access Management (IAM) e concedendo il minimo privilegio agli utenti. Stabilisci politiche e procedure di gestione delle credenziali per creare, distribuire, ruotare e revocare le credenziali di accesso. AWS Per ulteriori informazioni, consulta Best practice IAM nella Guida per l'utente di IAM.

Esegui lavori come utenti e gruppi

Quando si utilizza la funzionalità di coda in Deadline Cloud, è consigliabile specificare un utente del sistema operativo (OS) e il relativo gruppo primario in modo che l'utente del sistema operativo disponga delle autorizzazioni con privilegi minimi per i lavori della coda.

Quando specifichi un «Esegui come utente» (e gruppo), tutti i processi per i lavori inviati alla coda verranno eseguiti utilizzando quell'utente del sistema operativo e erediteranno le autorizzazioni del sistema operativo associate a quell'utente.

Le configurazioni della flotta e della coda si combinano per stabilire un livello di sicurezza. Sul lato della coda, è possibile specificare il ruolo «Job run as user» e IAM per utilizzare il sistema operativo e AWS le autorizzazioni per i lavori della coda. La flotta definisce l'infrastruttura (worker host, reti, storage condiviso montato) che, se associata a una particolare coda, esegue i lavori all'interno della

coda. I job di una o più code associate devono accedere ai dati disponibili sugli host dei worker. Specificare un utente o un gruppo aiuta a proteggere i dati nei lavori da altre code, da altri software installati o da altri utenti con accesso agli host di lavoro. Quando una coda è priva di un utente, viene eseguita come utente agente che può impersonare () `sudo` qualsiasi utente della coda. In questo modo, una coda senza utente può trasferire i privilegi a un'altra coda.

Rete

Per evitare che il traffico venga intercettato o reindirizzato, è essenziale proteggere come e dove viene instradato il traffico di rete.

Ti consigliamo di proteggere il tuo ambiente di rete nei seguenti modi:

- Proteggi le tabelle di routing delle sottoreti di Amazon Virtual Private Cloud (Amazon VPC) per controllare come viene instradato il traffico a livello IP.
- Se utilizzi Amazon Route 53 (Route 53) come provider DNS nella configurazione della tua farm o workstation, accedi in modo sicuro all'API Route 53.
- Se ti connetti a Deadline Cloud all'esterno, AWS ad esempio utilizzando workstation locali o altri data center, proteggi qualsiasi infrastruttura di rete locale. Ciò include server DNS e tabelle di routing su router, switch e altri dispositivi di rete.

Lavori e dati sui lavori

I job di Deadline Cloud vengono eseguiti all'interno delle sessioni sugli host dei lavoratori. Ogni sessione esegue uno o più processi sull'host di lavoro, che in genere richiedono l'immissione di dati per produrre l'output.

Per proteggere questi dati, è possibile configurare gli utenti del sistema operativo con code. L'agente di lavoro utilizza l'utente del sistema operativo in coda per eseguire i sottoprocessi della sessione. Questi sottoprocessi ereditano le autorizzazioni dell'utente del sistema operativo di coda.

Ti consigliamo di seguire le migliori pratiche per proteggere l'accesso ai dati a cui accedono questi sottoprocessi. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

Struttura dell'azienda

Puoi organizzare le flotte e le code di Deadline Cloud in molti modi. Tuttavia, alcune disposizioni hanno implicazioni in termini di sicurezza.

Una farm ha uno dei confini più sicuri perché non può condividere le risorse di Deadline Cloud con altre aziende agricole, tra cui flotte, code e profili di archiviazione. Tuttavia, puoi condividere AWS risorse esterne all'interno di una farm, il che compromette i limiti di sicurezza.

È inoltre possibile stabilire limiti di sicurezza tra le code all'interno della stessa farm utilizzando la configurazione appropriata.

Segui queste best practice per creare code sicure nella stessa farm:

- Associa una flotta solo alle code all'interno dello stesso limite di sicurezza. Tieni presente quanto segue:
  - Dopo l'esecuzione del processo sull'host del lavoratore, i dati potrebbero rimanere indietro, ad esempio in una directory temporanea o nella home directory dell'utente in coda.
  - Lo stesso utente del sistema operativo esegue tutti i lavori su un host Fleet Worker di proprietà del servizio, indipendentemente dalla coda a cui viene inviato il lavoro.
  - Un job può lasciare i processi in esecuzione su un worker host, permettendo ai job di altre code di osservare altri processi in esecuzione.
- Assicurati che solo le code all'interno dello stesso limite di sicurezza condividano un bucket Amazon S3 per gli allegati dei lavori.
- Assicurati che solo le code all'interno dello stesso limite di sicurezza condividano un utente del sistema operativo.
- Proteggi tutte AWS le altre risorse integrate nella farm fino al limite.

Code di allegati Job

Gli allegati Job sono associati a una coda, che utilizza il tuo bucket Amazon S3.

- Gli allegati di lavoro scrivono e leggono da un prefisso root nel bucket Amazon S3. È necessario specificare questo prefisso root nella chiamata API. `CreateQueue`
- Il bucket ha un corrispondente`Queue Role`, che specifica il ruolo che concede agli utenti della coda l'accesso al bucket e al prefisso root. Quando crei una coda, specifichi l'`Queue Role`Amazon Resource Name (ARN) insieme al bucket degli allegati del lavoro e al prefisso root.
- Le chiamate autorizzate a `AssumeQueueRoleForReadAssumeQueueRoleForUser`, e le operazioni `AssumeQueueRoleForWorker` API restituiscono una serie di credenziali di sicurezza temporanee per. `Queue Role`

Se crei una coda e riutilizzi un bucket Amazon S3 e un prefisso root, c'è il rischio che le informazioni vengano divulgate a parti non autorizzate. Ad esempio, QueueA e QueueB condividono lo stesso bucket e lo stesso prefisso root. In un flusso di lavoro sicuro, Artista ha accesso a QueueA ma non a QueueB. Tuttavia, quando più code condividono un bucket, Artista può accedere ai dati nei dati di QueueB perché utilizza lo stesso bucket e lo stesso prefisso root di QueueA.

La console imposta code sicure per impostazione predefinita. Assicurati che le code abbiano una combinazione distinta di bucket Amazon S3 e prefisso root, a meno che non facciano parte di un limite di sicurezza comune.

Per isolare le code, devi configurare per consentire l'accesso alla coda solo `Queue Role` al bucket e al prefisso root. Nell'esempio seguente, sostituisci ogni *`segnaposto`* con le informazioni specifiche della risorsa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME",
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME/JOB_ATTACHMENTS_ROOT_PREFIX/*"
      ],
      "Condition": {
        "StringEquals": { "aws:ResourceAccount": "ACCOUNT_ID" }
      }
    },
    {
      "Action": ["logs:GetLogEvents"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:REGION:ACCOUNT_ID:log-group:/aws/deadline/FARM_ID/*"
    }
  ]
}
```

È inoltre necessario impostare una politica di fiducia per il ruolo. Nell'esempio seguente, sostituisci il testo *segnaposto* con le informazioni specifiche della risorsa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    },
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "credentials.deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    }
  ]
}
```

Bucket Amazon S3 software personalizzati

Puoi aggiungere la seguente dichiarazione alla tua richiesta di accesso `Queue Role` al software personalizzato nel tuo bucket Amazon S3. Nell'esempio seguente, sostituisci *SOFTWARE_BUCKET_NAME con il nome del tuo bucket S3*.

```
"Statement": [
    {
        "Action": [
            "s3:GetObject",
            "s3:ListBucket"
```

```
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME",
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME/*"
        ]
    }
]
```

Per ulteriori informazioni sulle best practice di sicurezza di Amazon S3, consulta la sezione Best practice di sicurezza per Amazon S3 nella Amazon Simple Storage Service User Guide.

Operatori ospitanti

Proteggi gli host per i lavoratori per garantire che ogni utente possa eseguire operazioni solo per il ruolo assegnato.

Consigliamo le seguenti best practice per proteggere gli host dei lavoratori:

- Non utilizzare lo stesso `jobRunAsUser` valore con più code a meno che i lavori inviati a tali code non rientrino nello stesso limite di sicurezza.
- Non impostate la coda `jobRunAsUser` sul nome dell'utente del sistema operativo con cui viene eseguito il worker agent.
- Concedi agli utenti della coda le autorizzazioni del sistema operativo con i privilegi minimi necessarie per i carichi di lavoro in coda previsti. Assicurati che non dispongano delle autorizzazioni di scrittura del filesystem per i file di programma Work Agent o altro software condiviso.
- Assicurati che solo l'utente root Linux e il suo account siano `Administrator` proprietari e che possano modificare Windows i file di programma del worker agent.
- Sugli host Linux worker, valuta la possibilità di configurare un `umask` override `/etc/sudoers` che consenta all'utente worker agent di avviare i processi come utenti in coda. Questa configurazione aiuta a garantire che altri utenti non possano accedere ai file scritti nella coda.
- Concedi a persone fidate l'accesso con i privilegi minimi agli host dei lavoratori.
- Limita le autorizzazioni al DNS locale, sostituisci i file di configurazione (`/etc/hosts`accesi e attivi) Linux e instrada le tabelle `C:\Windows\system32\etc\hosts` sulle Windows workstation e sui sistemi operativi degli host di lavoro.
- Limita le autorizzazioni alla configurazione DNS sulle workstation e sui sistemi operativi degli host di lavoro.

- Applicate regolarmente patch al sistema operativo e a tutto il software installato. Questo approccio include software utilizzati specificamente con Deadline Cloud, come mittenti, adattatori, agenti di lavoro, OpenJD pacchetti e altro.
- Usa password complesse per la coda. Windows `jobRunAsUser`
- Ruota regolarmente le password per la coda. `jobRunAsUser`
- Garantisci l'accesso con il minimo privilegio alle password segrete ed elimina le Windows password segrete non utilizzate.
- Non `jobRunAsUser` autorizzate la coda a eseguire i comandi di pianificazione in futuro:
  - SìLinux, nega a questi account l'accesso a `cron` e. `at`
  - SìWindows, nega a questi account l'accesso al Windows task scheduler.

> **Note**
>
> Per ulteriori informazioni sull'importanza di applicare regolarmente patch al sistema operativo e al software installato, consulta il Modello di responsabilità condivisa.

Workstation

È importante proteggere le postazioni di lavoro con accesso a Deadline Cloud. Questo approccio aiuta a garantire che tutti i lavori che invii a Deadline Cloud non possano eseguire carichi di lavoro arbitrari fatturati a te. Account AWS

Consigliamo le seguenti best practice per proteggere le postazioni di lavoro degli artisti. Per ulteriori informazioni, consultare il Shared Responsibility Model (Modello di responsabilità condivisa).

- Proteggi tutte le credenziali permanenti che forniscono l'accesso a AWS, incluso Deadline Cloud. Per ulteriori informazioni, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM .
- Installa solo software affidabile e sicuro.
- Richiedi agli utenti di federarsi con un provider di identità per accedere AWS con credenziali temporanee.
- Utilizza autorizzazioni sicure sui file di programma del mittente di Deadline Cloud per impedirne la manomissione.
- Concedi alle persone fidate l'accesso meno privilegiato alle postazioni di lavoro degli artisti.

- Utilizza solo i mittenti e gli adattatori che ottieni tramite Deadline Cloud Monitor.
- Limita le autorizzazioni e indirizza le tabelle sulle workstation `/etc/hosts` e sui sistemi operativi host dei lavoratori.
- Limita le autorizzazioni alle workstation e `/etc/resolv.conf` ai sistemi operativi host dei lavoratori.
- Applicate regolarmente patch al sistema operativo e a tutto il software installato. Questo approccio include software utilizzati specificamente con Deadline Cloud, come mittenti, adattatori, agenti di lavoro, OpenJD pacchetti e altro.

Monitoraggio di AWS Deadline Cloud

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Deadline Cloud (Deadline Cloud) e delle tue soluzioni. AWS Raccogli i dati di monitoraggio da tutte le parti della tua AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Prima di iniziare a monitorare Deadline Cloud, devi creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Quali risorse verranno monitorate?
- Con quale frequenza eseguirai il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno usati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

AWS e Deadline Cloud forniscono strumenti che puoi utilizzare per monitorare le tue risorse e rispondere a potenziali incidenti. Alcuni di questi strumenti eseguono il monitoraggio al posto tuo, altri richiedono un intervento manuale. È necessario automatizzare il più possibile le attività di monitoraggio.

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

  Deadline Cloud ha tre CloudWatch metriche.
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre CloudTrail fonti. CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- Amazon EventBridge può essere utilizzato per automatizzare i AWS servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o

modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta Amazon EventBridge User Guide.

- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Argomenti

Registrazione delle chiamate con CloudTrail

AWS Deadline Cloud è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Deadline Cloud. CloudTrail acquisisce tutte le chiamate API per Deadline Cloud come eventi. Le chiamate acquisite includono chiamate dalla console Deadline Cloud e chiamate in codice alle operazioni dell'API Deadline Cloud.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Deadline Cloud. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata a Deadline Cloud, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni su Deadline Cloud in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Deadline Cloud, tale attività viene registrata in un CloudTrail evento insieme ad

altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

CloudTrail registra anche gli eventi quando gli utenti accedono al monitor Deadline Cloud e ricevono AWS le credenziali. Quando un utente accede, c'è un CloudTrail evento con l'origine `signin.amazonaws.com` e il nome. `UserAuthentication` C'è un secondo evento in cui all'utente che ha effettuato l'accesso vengono fornite AWS le credenziali dall'origine `sts.amazonaws.com` e dal nome. `AssumeRole` L'ID dell'utente viene registrato nel secondo evento all'interno del nome della sessione del ruolo.

Per una registrazione continua degli eventi nel tuo Account AWS, compresi gli eventi per Deadline Cloud, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail

Per ulteriori informazioni, consulta gli argomenti seguenti:

Panoramica della creazione di un percorso

CloudTrail servizi e integrazioni supportati

Configurazione delle notifiche Amazon SNS per CloudTrail

Ricezione di file di CloudTrail registro da più regioni

Ricezione di file di CloudTrail registro da più account

Deadline Cloud supporta la registrazione delle seguenti azioni come eventi nei CloudTrail file di registro:

- associate-member-to-farm
- associate-member-to-fleet
- associate-member-to-job
- associate-member-to-queue
- assume-fleet-role-for-leggi

- assume-fleet-role-for-lavoratore
- assume-queue-role-for-leggi
- assume-queue-role-for-utente
- assume-queue-role-for-lavoratore
- creare un budget
- crea-fattoria
- create-fleet
- create-license-endpoint
- crea-monitora
- crea coda
- create-queue-environment
- create-queue-fleet-association
- create-storage-profile
- create-worker
- elimina-budget
- elimina-farm
- delete-fleet
- delete-license-endpoint
- delete-metered-product
- elimina-monitora
- cancella coda
- delete-queue-environment
- delete-queue-fleet-association
- delete-storage-profile
- delete-worker
- disassociate-member-from-farm
- disassociate-member-from-fleet
- disassociate-member-from-job
- disassociate-member-from-queue

- get-application-version
- ottenere un budget
- prendere in fattoria
- get-feature-map
- prendi una flotta
- get-license-endpoint
- tieniti monitorato
- get-queue
- get-queue-environment
- get-queue-fleet-association
- get-sessions-statistics-aggregation
- get-storage-profile
- get-storage-profile-for-coda
- list-available-metered-products
- elenca-budget
- list-farm-members
- elenca-fattorie
- list-fleet-members
- list-flotte
- list-job-members
- list-license-endpoints
- list-metered-products
- list-monitor
- list-queue-environments
- list-queue-fleet-associations
- list-queue-members
- code di elenchi
- list-storage-profiles
- list-storage-profiles-for-coda

- list-tags-for-resource
- put-metered-product
- start-sessions-statistics-aggregation
- tag-resource
- untag-resource
- aggiorna il budget
- update-farm
- aggiorna la flotta
- aggiorna e monitora
- coda di aggiornamento
- update-queue-environment
- update-queue-fleet-association
- update-storage-profile
- update-worker

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio .

Per ulteriori informazioni, vedete l'elemento CloudTrail user Identity.

Comprendere le voci dei file di registro di Deadline Cloud

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di

registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Questo esempio JSON mostra il log generato da una chiamata all'**`CreateFarm`**API:


```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "deadline.amazonaws.com",
    "eventName": "CreateFarm",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "example-farm",
        "kmsKeyArn": "arn:aws:kms:us-west-2:111122223333:key/111122223333",
        "X-Amz-Client-Token": "12abc12a-1234-1abc-123a-1a11bc1111a",
        "description": "example-description",
        "tags": {
            "purpose_1": "e2e"
            "purpose_2": "tag_test"
        }
```

```
    },
    "responseElements": {
        "farmId": "EXAMPLE-farmID"
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
    "eventCategory": "Management",
}
```

L'esempio mostra la AWS regione, l'indirizzo IP e altri `requestParameters` "" come "edisplayName" kmsKeyArn "che possono aiutarti a identificare l'evento.

Monitoraggio con CloudWatch

Amazon CloudWatch (CloudWatch) raccoglie dati grezzi e li elabora in parametri leggibili quasi in tempo reale. Puoi aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/ per visualizzare e filtrare i parametri di Deadline Cloud.

- In una flotta gestita dai clienti di Deadline Cloud, CloudWatch ti invia due metriche e: `UnhealthyWorkerCount` `RecommendedFleetSize`
- Il namespace per queste metriche è `AWS/DeadlineCloud`.
- Puoi utilizzare le dimensioni `farmID` e filtrare le metriche`fleetID`.
- Entrambe le metriche utilizzano l'unità. `count`

Queste statistiche vengono conservate per 15 mesi in modo da poter accedere alle informazioni storiche per avere una prospettiva migliore sulle prestazioni dell'applicazione o del servizio Web. 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.

Deadline Cloud ha due tipi di registri: i registri delle attività e i registri dei lavoratori. Un registro delle attività si verifica quando si eseguono i registri di esecuzione come script o come esecuzione di DCC. Un registro delle attività potrebbe mostrare eventi come il caricamento delle risorse, il rendering dei riquadri o il mancato rilevamento delle texture.

Un registro dei lavoratori mostra i processi degli agenti di lavoro. Questi potrebbero includere elementi come l'avvio degli agenti di lavoro, la registrazione, i report sullo stato di avanzamento, il caricamento delle configurazioni o il completamento delle attività.

Per Deadline Cloud, i lavoratori caricano questi registri in Logs. CloudWatch Per impostazione predefinita, i log non scadono mai. Se un lavoro produce un volume elevato di dati, è possibile incorrere in costi aggiuntivi. Per ulteriori informazioni, consulta i CloudWatch prezzi di Amazon.

Puoi modificare la politica di conservazione per ogni gruppo di log. Una conservazione più breve rimuove i vecchi log e può aiutare a ridurre i costi di archiviazione. Per conservare i log, puoi archiviarli su Amazon Simple Storage Service prima di rimuoverli. Per ulteriori informazioni, consulta Esportazione dei dati di registro in Amazon S3 utilizzando la console nella guida per l' CloudWatch utente di Amazon.

> **Note**
>
> CloudWatch le letture dei log sono limitate da. AWS Se hai intenzione di inserire molti artisti, ti suggeriamo di contattare l'assistenza AWS clienti e richiedere un aumento della `GetLogEvents` quota di iscrizione. CloudWatch Inoltre, ti consigliamo di chiudere il portale di log tailing quando non stai eseguendo il debug.

Per ulteriori informazioni, consulta CloudWatch Logs quotas nella guida per CloudWatch l'utente di Amazon.

Agire in base agli eventi EventBridge

Deadline Cloud invia eventi EventBridge ad Amazon per informarti delle modifiche allo stato del servizio. Puoi utilizzare EventBridge questi eventi per scrivere regole che agiscano, ad esempio avvisandoti quando c'è un cambiamento nella tua flotta. Per ulteriori informazioni, consulta Cos'è Amazon EventBridge

Modifica dei consigli sulle dimensioni del parco veicoli

Quando configuri la tua flotta per utilizzare la scalabilità automatica basata sugli eventi, Deadline Cloud invia eventi che puoi utilizzare per gestire le tue flotte. Ciascuno di questi eventi contiene informazioni sulla dimensione attuale e sulla dimensione richiesta di una flotta. Per un esempio di utilizzo di un EventBridge evento e di una funzione Lambda di esempio per gestire l'evento, vedere.

Ridimensiona automaticamente la tua flotta Amazon EC2 con la funzionalità di raccomandazione di scalabilità Deadline Cloud

L'evento di modifica dei consigli sulle dimensioni del parco veicoli viene inviato quando si verifica quanto segue:

- Quando la dimensione del parco veicoli consigliata cambia e `oldFleetSize` differisce da`newFleetSize`.
- Quando il servizio rileva che la dimensione effettiva della flotta non corrisponde alla dimensione della flotta consigliata. È possibile ottenere le dimensioni effettive della flotta dalla `workerCount` risposta dell'GetFleetoperazione. Ciò può accadere quando un'istanza Amazon EC2 attiva non riesce a registrarsi come operatore Deadline Cloud.

L'evento ha il seguente formato:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "Fleet Size Recommendation Change",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-west-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "fleetId": "fleet-12345678900000000000000000000000",
        "oldFleetSize": 1,
        "newFleetSize": 5,
    }
}
```

I seguenti campi definiscono lo schema dell'evento:

`"source": "aws.deadline"`

Indica che l'origine di questo evento è Deadline Cloud.

`"detail-type": "Fleet Size Recommendation Change"`

Identifica il tipo di evento.

"detail": { }

Fornisce informazioni sulle modifiche consigliate alla dimensione del parco veicoli.

"farmId": "farm-12345678900000000000000000000000"

L'identificatore dell'azienda agricola che contiene la flotta.

"fleetId": "fleet-12345678900000000000000000000000"

L'identificatore della flotta che necessita di un cambio di dimensione.

"oldFleetSize": 1

Le dimensioni attuali della flotta.

"newFleetSize": 5

La nuova dimensione della flotta consigliata.

Quote per Deadline Cloud

AWS Deadline Cloud fornisce risorse, come fattorie, flotte e code, che è possibile utilizzare per elaborare i lavori. Quando crei le tue Account AWS, impostiamo quote predefinite su queste risorse per ciascuna. Regione AWS

Service Quotas è una posizione centrale in cui è possibile visualizzare e gestire le quote per. Servizi AWS Puoi anche richiedere un aumento della quota per molte delle risorse che utilizzi.

Per visualizzare le quote per Deadline Cloud, apri la console Service Quotas. Nel riquadro di navigazione, scegli Servizi AWS, quindi seleziona Deadline Cloud.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di aumento della quota di servizio.

Creazione di risorse AWS Deadline Cloud con AWS CloudFormation

AWS Deadline Cloud è integrato con AWS CloudFormation un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come fattorie, code e flotte) e fornisce e AWS CloudFormation configura tali risorse per te.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Deadline Cloud in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più regioni Account AWS .

Deadline Cloud e modelli AWS CloudFormation

Per fornire e configurare le risorse per Deadline Cloud e i servizi correlati, devi conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire nei tuoi AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

Deadline Cloud supporta la creazione di fattorie, code e flotte. AWS CloudFormationPer ulteriori informazioni, inclusi esempi di modelli JSON e YAML per fattorie, code e flotte, consulta Deadline Cloud nella Guida per l'utente.AWS AWS CloudFormation

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Documentazione di riferimento delle API
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Cronologia dei documenti per la guida utente di Deadline Cloud

La tabella seguente descrive le modifiche importanti in ogni versione della guida per l'utente di AWS Deadline Cloud.

Modifica	Descrizione	Data
Versione iniziale	Questa è la versione iniziale della guida per l'utente di Deadline Cloud.	2 aprile 2024

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.