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 EC2 (Amazon) 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 le funzionalità 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

Funzionalità 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 (DCCs) sono prodotti di terze parti in cui è possibile creare contenuti digitali. Esempi di DCCs sono Maya, Nukee Houdini. Deadline Cloud fornisce plugin integrati per Job Submitter per scopi specifici. DCCs

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.

Priorità del lavoro

La priorità del lavoro è l'ordine approssimativo in cui Deadline Cloud elabora un lavoro in una coda. È possibile impostare la priorità del lavoro tra 1 e 100, i lavori con una priorità numerica più alta vengono generalmente elaborati per primi. I lavori con la stessa priorità vengono elaborati nell'ordine di ricezione.

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.

Sessione

Una sessione è un ambiente di runtime temporaneo su un host di lavoro creato per eseguire una serie di attività dallo stesso lavoro. La sessione termina quando l'host di lavoro termina l'esecuzione delle attività per quel lavoro.

La sessione consente di configurare l'ambiente con risorse condivise tra più esecuzioni di attività, ad esempio la definizione di variabili di ambiente o l'avvio di un processo o di un contenitore in background.

Azione della sessione

Un'azione di sessione è un'unità di lavoro discreta eseguita da un lavoratore all'interno di una sessione. Può comprendere le operazioni principali di esecuzione di un'attività oppure può includere fasi preparatorie come la configurazione dell'ambiente e processi post-esecuzione come lo smontaggio e la pulizia.

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 EC2 istanze Amazon 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 hanno 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 che utilizzi.

Esplora l'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 delle EC2 istanze Amazon 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.

Accedere 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 Monitoring with CloudWatch nella Deadline Cloud Developer Guide.
- Amazon EC2: Servizio AWS fornisce server virtuali che eseguono le tue applicazioni nel cloud. Puoi configurare i tuoi progetti per utilizzare le EC2 istanze Amazon per i tuoi carichi di lavoro. Per ulteriori informazioni, consulta le EC2 istanze di Amazon.
- 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 guasto 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 Amazon EC2 Auto Scaling User Guide.
- AWS PrivateLink— AWS PrivateLink fornisce connettività privata tra cloud privati virtuali (VPCs) e reti locali Servizi AWS, senza esporre il traffico alla rete Internet pubblica. AWS PrivateLink semplifica la connessione di servizi tra diversi account e. VPCs 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. Per ulteriori informazioni, consulta la Amazon S3 User Guide.
- 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 AWS IAM Identity Center FAQs.

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, vedere Open Job Description sul GitHub sito web.

Deadline Cloud fornisce candidature. Un job submitter è un plug-in DCC per l'invio di lavori di rendering da un'interfaccia DCC di terze parti, come Maya oppure 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 vengono 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 è possibile collegare l'autorizzazione al provider di identità (IdP) esistente, ad esempio Okta oppure Active Directory. Gli amministratori IT possono concedere 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 OpenJD specifica per descrivere il lavoro come un lavoro con istruzioni di script software parametrizzate (ad esempio in un intervallo di frame) in attività. Assemblare OpenJD le istruzioni di 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 usage-based-licensing (UBL) una selezione di licenze per 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.

Guida introduttiva a 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

Configura il tuo 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 https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla 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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

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 l'aggiunta di gruppi e utenti, la scelta di un ruolo di servizio e l'aggiunta di tag alle tue risorse.

Passaggio 1: crea il tuo monitor

Il monitor Deadline Cloud utilizza 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 del monitor: Il nome del monitor è il modo in cui è possibile identificare il monitor, ad esempio AnyCompany monitor. Il nome del monitor determina anche l'URL del monitor.

- URL di monitoraggio: puoi accedere al monitor utilizzando l'URL del monitor. L'URL è basato sul nome del Monitor, ad esempio https://anycompanymonitor.awsapps.com.
- Regione AWS: Regione AWSè la posizione fisica per un insieme di data center. AWS 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 del monitor, ad esempio**`AnyCompany Monitor`**.
3. (Facoltativo) Per modificare l'URL del monitor, scegli 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.
5. (Facoltativo) Per personalizzare ulteriormente la configurazione del monitor, seleziona Impostazioni aggiuntive.
6. Se sei pronto perFase 2: Definizione dei dettagli della fattoria, scegli Avanti.

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 politiche forniscono agli utenti le autorizzazioni per 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 della fattoria

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 può aiutarti a identificare lo scopo della tua fattoria.
3. Crea un gruppo e aggiungi usi per la tua fattoria. Dopo aver configurato la tua fattoria, puoi utilizzare la console di gestione Deadline Cloud per aggiungere o modificare gruppi e utenti.
4. (Facoltativo) Scegli Impostazioni aggiuntive della fattoria.

   a. (Facoltativo) Per impostazione predefinita, i tuoi dati sono crittografati con una chiave che AWS possiede e gestisce 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.

   b. (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 dell'avanzamento 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. (Facoltativo) Scegli Impostazioni aggiuntive della fattoria.

    a. Se utilizzi flotte gestite dal cliente, seleziona Abilita l'associazione con flotte gestite dal cliente.

        i. 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.

        ii. Se desideri impostare un budget per una coda, scegli Richiedi un budget per questa coda. Se hai bisogno di un budget, devi crearlo utilizzando la console Deadline Cloud per pianificare i lavori in coda.

    b. 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.

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

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

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

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

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

ii. In alternativa, puoi selezionare un ruolo di servizio esistente.

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

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

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 4: Definizione dei dettagli del parco veicoli

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. Controlla il tipo di flotta e il sistema operativo per maggiori informazioni.

2. Nella sezione Tipo di mercato dell'istanza, scegli Istanza Spot o Istanza on demand. Le istanze Amazon EC2 On-demand offrono una disponibilità più rapida e le istanze Amazon EC2 Spot 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. Esamina le capacità dei lavoratori per sensibilizzarli.
5. (opzionale) Scegli Impostazioni aggiuntive del parco veicoli

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

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

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

B. Inserisci un nome di ruolo per il ruolo del tuo parco veicoli o usa il nome del ruolo fornito.

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

D. Per visualizzare le autorizzazioni IAM per il ruolo della flotta, scegli Visualizza i dettagli delle autorizzazioni.

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

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

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

Passaggio 5: revisione e creazione

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

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

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.

Su ogni workstation deve essere installato il DCC prima di installare il mittente corrispondente. Ad esempio, se desideri scaricare il mittente Deadline Cloud per Blender, devi avere Blender già installato sulla workstation.

Forniamo impostazioni predefinite ragionevoli per proteggere le postazioni di lavoro. Per ulteriori informazioni sulla protezione della postazione di lavoro, consulta Best practice di sicurezza - workstation.

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.

1. Accedi e apri la console Deadline AWS Management Console Cloud.
2. Dal pannello di navigazione laterale, scegli Download.
3. Dalla sezione del programma di installazione del mittente di Deadline Cloud, seleziona il programma di installazione per il sistema operativo del tuo computer, quindi scegli Scarica.
4. Verifica l'autenticità del software scaricato(Facoltativo).

Installa il mittente Deadline Cloud

Con il programma di installazione, puoi installare i seguenti mittenti:

Software	Versioni supportate	Programma di installazione di Windows	programma di installazione Linux	Programma di installazione macOS
Adobe After Effects	2024 - 2025	Incluso	Non incluso	Incluso

Software	Versioni supportate	Programma di installazione di Windows	programma di installazione Linux	Programma di installazione macOS
Autodesk Arnold per Maya	7.1 - 7.2	Incluso	Incluso	Incluso
Autodesk Maya	2023 - 2025	Incluso	Incluso	Incluso
Frullatore	3,6 - 4,2	Incluso	Incluso	Incluso
Foundry Nuke	15 - 16	Incluso	Incluso	Non incluso
KeyShot Studio	2023 - 2024	Incluso	Non incluso	Incluso
Maxon Cinema 4D	2024 - 2025	Incluso	Non incluso	Incluso
SideFX Houdini	19,5 - 20,5	Incluso	Incluso	Incluso

È possibile installare altri mittenti non elencati qui. Utilizziamo le librerie Deadline Cloud per creare mittenti. Alcuni dei mittenti includono Unreal Engine, 3ds Max e Rhino. Puoi trovare il codice sorgente di queste librerie e mittenti nell'organizzazione aws-deadline. GitHub

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. Scegli Next (Successivo).
8. Controllate l'installazione e scegliete Avanti.
9. Scegli di nuovo Avanti, quindi scegli Fine.

Linux

> **Note**
>
> Deadline Cloud integrato Nuke installatore per Linux e Deadline Cloud monitor può essere installato 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 **`sudo -i`** e premi Invio per diventare root.
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.

MacOS

1. In un browser di file, accedi alla cartella in cui è stato scaricato il programma di installazione, quindi seleziona il file.
2. Dopo l'apertura della procedura guidata di configurazione di AWS Deadline Cloud Submitter, scegli Avanti.
3. Scegli nuovamente Avanti per accettare la directory di installazione.
4. Seleziona Integrated Submitter per Maya, o qualsiasi altro mittente che desideri installare.
5. Scegli Next (Successivo).
6. Controllate l'installazione e scegliete Avanti.
7. Scegli di nuovo Avanti, quindi scegli Fine.

Passaggio 2: installa e configura Deadline Cloud Monitor

Puoi installare l'applicazione desktop di monitoraggio Deadline Cloud con Windows, Linux, oppure macOS.

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 l'ultima Windows file e scegli Scarica.

   Per eseguire un'installazione invisibile, utilizzate il seguente comando:

   ```
   DeadlineCloudMonitor_VERSION_x64-setup.exe /S
   ```

   Per impostazione predefinita, il monitor è installato in`C:\Users{username}\AppData\Local\DeadlineCloudMonitor`. Per cambiare la directory di installazione, usate invece questo comando:

   ```
   DeadlineCloudMonitor_VERSION_x64-setup.exe /S /D={InstallDirectory}
   ```

Linux (AppImage)

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 update
   sudo apt install libfuse2
   ```
3. Per rendere l' AppImage eseguibile, inserisci:

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

Linux (Debian)

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://archive.ubuntu.com/ubuntu/pool/main/o/openssl/
   libssl1.1_1.1.1f-1ubuntu2_amd64.deb
   sudo apt install ./libssl1.1_1.1.1f-1ubuntu2_amd64.deb
   ```
3. Per installare il pacchetto Deadline Cloud monitor Debian, inserisci:

```
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
```

Linux (RPM)

Per installare Deadline Cloud, monitora RPM su Rocky Linux 9 oppure Alma Linux 9

1. Scarica l'ultima versione del monitor RPM di Deadline Cloud.
2. Aggiungi i pacchetti extra per Enterprise Linux 9 archivio:

```
sudo dnf install epel-release
```

3. Installa compat-openssl11 per la dipendenza libssl.so.1.1:

```
sudo dnf install compat-openssl11 deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

Per installare Deadline Cloud, monitora RPM su Red Hat Linux 9

1. Scarica l'ultima versione del monitor RPM di Deadline Cloud.
2. Abilita il CodeReady Linux Builder archivio:

```
subscription-manager repos --enable codeready-builder-for-rhel-9-x86_64-rpms
```

3. Installa i pacchetti aggiuntivi per Enterprise RPM:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-9.noarch.rpm
```

4. Installa compat-openssl11 per la dipendenza libssl.so.1.1:

```
sudo dnf install compat-openssl11 deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

Per installare Deadline Cloud, monitora RPM su Rocky Linux 8, Alma Linux 8, oppure Red Hat Linux 8

1. Scarica l'ultimo RPM del monitor Deadline Cloud.
2. Installa il monitor Deadline Cloud:

```
sudo dnf install deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

macOS

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 l'ultima macOS file e scegli Scarica.
4. Apri il file scaricato. Quando viene visualizzata la finestra, seleziona e trascina l'icona del monitor di Deadline Cloud nella cartella Applicazioni.

Dopo aver completato il download, puoi verificare l'autenticità del software scaricato. È consigliabile eseguire questa operazione per assicurarsi che nessuno abbia manomesso i file durante o dopo il processo di download. 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

L'esempio seguente mostra come installare Blender mittente. È possibile installare altri mittenti utilizzando le istruzioni in. Inviatori supportati

Per avviare il mittente di Deadline Cloud in Blender

> **Note**
>
> Supporto per Blender viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

1. Aprire Blender.
2. Scegli Modifica, quindi Preferenze. In Percorsi dei file scegli Directory di script, quindi scegli Aggiungi. Aggiungi una directory di script per la cartella python in cui Blender submitter è stato installato:

```
Windows:
   %USERPROFILE%\DeadlineCloudSubmitter\Submitters\Blender\python\
Linux:
   ~/DeadlineCloudSubmitter/Submitters/Blender/python/
MacOS:
   ~/DeadlineCloudSubmitter/Submitters/Blender/python/
```

3. Restart (Riavvia) Blender.
4. Scegli Modifica, quindi Preferenze. Quindi, scegli Componenti aggiuntivi, quindi cerca Deadline Cloud per Blender. Seleziona la casella di controllo per abilitare il componente aggiuntivo.
5. Apri un Blender scena con dipendenze che esistono all'interno della directory principale dell'asset.
6. 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 viene 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.
7. Scegli Invia.

Inviatori supportati

Le seguenti sezioni ti guidano attraverso i passaggi per avviare i plugin di invio di Deadline Cloud disponibili.

Puoi installare altri mittenti non elencati qui. Utilizziamo le librerie Deadline Cloud per creare mittenti. Alcuni dei mittenti includono Unreal Engine, 3ds Max e Rhino. Puoi trovare il codice sorgente di queste librerie e mittenti nell'organizzazione GitHubaws-deadline.

Software	Versioni supportate	Programma di installazione di Windows	programma di installazione Linux	Programma di installazione macOS
Adobe After Effects	2024 - 2025	Incluso	Non incluso	Incluso
Autodesk Arnold per Maya	7.1 - 7.2	Incluso	Incluso	Incluso
Autodesk Maya	2023 - 2025	Incluso	Incluso	Incluso
Frullatore	3,6 - 4,2	Incluso	Incluso	Incluso
Foundry Nuke	15 - 16	Incluso	Incluso	Non incluso
KeyShot Studio	2023 - 2024	Incluso	Non incluso	Incluso
Maxon Cinema 4D	2024 - 2025	Incluso	Non incluso	Incluso
SideFX Houdini	19,5 - 20,5	Incluso	Incluso	Incluso

After Effects

Per avviare il mittente di Deadline Cloud in After Effects

1. Aprire After Effects.
2. Scegli Modifica, quindi Preferenze, quindi Scripting ed espressioni.
3. Scegli Consenti agli script di scrivere file e accedere alle reti.
4. Riavviate After Effects
5. Selezionate Finestra, quindi scegliete DeadlineCloudSubmitter.jsx.

Per usare il programma di invio di After Effects

1. Scegliete Apri coda di rendering nel pannello del mittente.

2. Aggiungete una composizione alla coda di rendering e configurate le impostazioni di rendering, il modulo di output e il percorso di output.
3. Scegliete Aggiorna nel pannello del mittente.
4. Scegli la tua composizione dall'elenco, quindi scegli Invia. Puoi scegliere nuovamente Aggiorna quando aggiungi o rimuovi composizioni dalla coda di rendering.

Puoi agganciare il mittente ai pannelli laterali scegliendo l'angolo in alto a destra del mittente e rilasciandolo in qualsiasi sezione evidenziata in After Effects.

Blender

Per avviare il mittente di Deadline Cloud in Blender

> **Note**
>
> Supporto per Blender viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

1. Aprire Blender.
2. Scegli Modifica, quindi Preferenze. In Percorsi dei file scegli Directory di script, quindi scegli Aggiungi. Aggiungi una directory di script per la cartella python in cui Blender submitter è stato installato:

```
Windows:
   %USERPROFILE%\DeadlineCloudSubmitter\Submitters\Blender\python\
Linux:
   ~/DeadlineCloudSubmitter/Submitters/Blender/python/
```

3. Restart (Riavvia) Blender.
4. Scegli Modifica, quindi Preferenze. Quindi, scegli Componenti aggiuntivi, quindi cerca Deadline Cloud per Blender. Seleziona la casella di controllo per abilitare il componente aggiuntivo.
5. Apri un Blender scena con dipendenze che esistono all'interno della directory principale dell'asset.
6. 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 viene 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.

7. Scegli Invia.

Cinema 4D

Per avviare il mittente di Deadline Cloud in Cinema 4D

> **Note**
>
> Supporto per Cinema 4D viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

1. Apri Cinema 4D.
2. Se viene richiesto di installare i componenti della GUI per AWS Deadline Cloud, completate i seguenti passaggi:
   a. Quando viene visualizzato il prompt, scegli Sì e attendi l'installazione delle dipendenze.
   b. Restart (Riavvia) Cinema 4D per garantire che le modifiche vengano applicate.
3. Scegli Estensioni > AWS Deadline Cloud Submitter.

Houdini

Per avviare Deadline Cloud Submitter in Houdini

> **Note**
>
> Supporto per Houdini viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

1. Aprire Houdini.
2. Nel Network Editor, 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.

KeyShot

Per avviare il mittente di Deadline Cloud in KeyShot

1. Aperta KeyShot.
2. Scegliere Windows> Console di scripting > Invia a AWS Deadline Cloud ed esegui.

Esistono due modalità di invio per il mittente. KeyShot Seleziona la modalità di invio per aprire il mittente.

- Allega il file BIP della scena e tutti i riferimenti ai file esterni: il file di scena aperto e tutti i file esterni a cui fa riferimento il BIP sono inclusi come allegati del lavoro.
- Allega solo il file BIP della scena: all'invio viene allegato solo il file di scena aperto. Tutti i file esterni a cui si fa riferimento nella scena devono essere disponibili per i lavoratori tramite l'archiviazione di rete o un altro metodo.

Maya and Arnold for Maya

Per avviare il mittente Deadline Cloud in Maya

> **Note**
>
> Supporto per Maya e Arnold for Maya (MtoA) viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

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. Cercare DeadlineCloudSubmitter.
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 viene 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 apri Maya, scegli Caricamento automatico.
7. Seleziona lo scaffale Deadline Cloud, quindi seleziona il pulsante verde per avviare il mittente.

Nuke

Per avviare il mittente di Deadline Cloud in Nuke

> **Note**
>
> Supporto per Nuke viene fornito utilizzando il Conda ambiente per flotte gestite dai servizi. Per ulteriori informazioni, consulta Predefinita Conda ambiente di coda.

1. Aprire Nuke.
2. Aprire un Nuke script con dipendenze che esistono all'interno della directory principale dell'asset.
3. Scegliere AWS Deadline, 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 viene 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 viene visualizzato come AUTENTICATO.
4. Scegli Invia.

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, richiederli e inviare nuovamente i lavori.

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 Tieni traccia della spesa e dell'utilizzo per le fattorie 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 abbia bisogno di 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 essere in grado di 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.

Modifica le impostazioni della lingua

Dopo aver creato e aperto il monitor Deadline Cloud, puoi modificare le impostazioni della lingua. Per impostazione predefinita, la lingua del monitor è impostata sulle impostazioni della lingua del sistema.

Per modificare le impostazioni della lingua dal monitor Deadline Cloud (desktop)

1. Dal tuo profilo utente, seleziona Impostazioni, quindi scegli Lingua.
2. Dal menu a discesa, seleziona una delle lingue disponibili.
3. Conferma che la lingua scelta è l'opzione elencata, quindi scegli Conferma e applica per applicare la modifica.

   Dopo l'aggiornamento, il monitor viene visualizzato nella lingua scelta.

   Dopo aver modificato l'impostazione della lingua, questa diventa quella predefinita all'apertura e rimane tale fino a quando non la si modifica nuovamente o si disinstalla l'applicazione desktop.

Per cambiare la lingua del monitor di Deadline Cloud sul Web, modifica la lingua preferita nelle impostazioni del browser.

> **Note**
>
> Se il browser o il sistema operativo è impostato su una lingua non supportata da Deadline Cloud, l'inglese diventa la lingua predefinita per Deadline Cloud monitor.

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.

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.
- Invia nuovamente il lavoro.

Per ulteriori informazioni, consulta Visualizza e gestisci 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, consultare 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 e gestisci i dettagli del lavoro in Deadline Cloud

La pagina Job monitor nel monitor Deadline Cloud 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 in Visualizza i dettagli della coda e della flotta in Deadline Cloud arrivo.
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.
    - È possibile modificare la priorità del lavoro in una coda. I lavori con priorità numerica più alta vengono elaborati prima dei lavori con priorità numerica inferiore. I lavori possono avere una priorità compresa tra 1 e 100. Quando due lavori hanno la stessa priorità, il lavoro più vecchio viene pianificato per primo.
- 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.

Archivia un lavoro

Per archiviare un lavoro, deve trovarsi in uno stato terminale`FAILED`,`SUCCEEDED`,`SUSPENDED`, o`CANCELED`. Lo `ARCHIVED` stato è definitivo. Una volta archiviato, un lavoro non può essere richiesto o modificato.

I dati del lavoro non sono influenzati dall'archiviazione del lavoro. I dati vengono eliminati quando viene raggiunto il timeout di inattività o quando viene eliminata la coda contenente il lavoro.

Altre cose che accadono ai lavori archiviati:

- I lavori archiviati sono nascosti nel monitor Deadline Cloud.
- I lavori archiviati sono visibili in uno stato di sola lettura dalla CLI di Deadline Cloud per 120 giorni prima dell'eliminazione.

Richiedi un lavoro

Quando richiedi un lavoro, tutte le attività senza dipendenze tra fasi passano a. `READY` Lo stato dei passaggi con dipendenze passa a `READY` o `PENDING` man mano che vengono ripristinati.

- Tutti i lavori, i passaggi e le attività passano a`PENDING`.
- Se un passaggio non ha una dipendenza, passa a. `READY`

Invia nuovamente un lavoro

In alcuni momenti potresti voler eseguire nuovamente un lavoro, ma con proprietà e impostazioni diverse. Ad esempio, potreste inviare un lavoro per eseguire il rendering di un sottoinsieme di frame di test, verificare l'output, quindi eseguire nuovamente il lavoro con l'intera gamma di frame. A tale scopo, invia nuovamente il lavoro.

Quando invii nuovamente un lavoro, diventano nuove attività senza dipendenze. `READY` Le nuove attività con dipendenze diventano. `PENDING`

- Tutti i nuovi lavori, passaggi e attività diventano`PENDING`.
- Se un nuovo passaggio non ha una dipendenza, lo diventa`READY`.

Quando invii nuovamente un lavoro, puoi modificare solo le proprietà che erano state definite come configurabili quando il lavoro è stato creato per la prima volta. Ad esempio, se il nome di un lavoro non è definito come proprietà configurabile del lavoro al momento dell'invio per la prima volta, il nome non può essere modificato al momento del nuovo invio.

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 e gestisci i dettagli del lavoro in Deadline Cloud per visualizzare un elenco di offerte di lavoro.
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 e gestisci 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 registri delle sessioni e dei lavoratori 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 registri delle sessioni e dei lavoratori 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 EC2 (Amazon), 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 e gestisci 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 e gestisci 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.

Visualizza i dettagli del lavoratore nella dashboard del lavoratore

La dashboard del lavoratore fornisce dettagli per il lavoratore che elabora un'attività. Puoi vedere:

- Metadati, come il tipo di istanza, per il lavoratore
- Le azioni di sessione eseguite dal lavoratore
- Prestazioni del lavoratore, incluso l'utilizzo di CPU, memoria e disco
- Un grafico dell'utilizzo di CPU, memoria e disco nel tempo
- Un grafico della velocità del disco nel tempo
- Il registro del lavoratore relativo all'attività

Per visualizzare il pannello di controllo del lavoratore da un'attività

1. Segui i passaggi indicati Visualizza e gestisci 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. Nella tabella delle attività, dal menu Azioni, scegli Visualizza dashboard del lavoratore.

Per visualizzare la dashboard 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 lavoratore dall'elenco Lavoratori.
3. Dal menu Azioni, scegli Visualizza il pannello di controllo del lavoratore.

Casi d'uso

Rilevamento di istanze con provisioning insufficiente

Quando i rendering richiedono più tempo del previsto, la dashboard di lavoro può aiutarti a determinare se le istanze sono di dimensioni adeguate per i tuoi carichi di lavoro. Sebbene l'utilizzo del 100% della vCPU sia normale per molti renderer, un utilizzo costante della memoria vicino alla capacità massima e un utilizzo elevato dello spazio su disco possono indicare che le istanze non dispongono di un provisioning sufficiente. In questi casi, l'aggiornamento della configurazione delle istanze del parco istanze può ridurre gli errori di rendering e migliorare significativamente i tempi di rendering. Tuttavia, è importante continuare a monitorare le prestazioni degli operatori dopo l'aggiornamento per assicurarsi di aver trovato l'equilibrio ottimale: un upgrade troppo aggressivo può portare a costi inutili a causa dell'over-provisioning.

Rilevamento di istanze con sovra-provisioning

Anche quando le attività vengono completate con successo, potrebbero esserci opportunità per ottimizzare i costi. La dashboard dei lavoratori può rivelare se stai pagando per una potenza di elaborazione superiore a quella richiesta dai tuoi carichi di lavoro. Se noti che il worker ha un utilizzo

medio basso della vCPU, un utilizzo minimo della memoria e uno spazio su disco inutilizzato in eccesso, puoi ridimensionare la configurazione delle istanze del tuo parco istanze.

Risoluzione dei problemi delle attività non riusc

Quando si esaminano le attività non riuscite, il dashboard del lavoratore funge da prezioso strumento diagnostico. Presta particolare attenzione ai picchi di utilizzo della memoria e dello spazio su disco: se questi parametri si avvicinano o raggiungono il 100%, sono probabilmente la causa principale degli errori delle attività. Tale esaurimento delle risorse indica che le istanze attuali non sono in grado di gestire efficacemente i carichi di lavoro. In questi casi, il provisioning delle istanze con maggiore memoria o spazio su disco contribuirà a garantire il corretto completamento delle attività.

Tasso di utilizzo ottimale delle istanze

Utilizzo della vCPU

Intervallo obiettivo: 70-90%

- Meno del 70%: probabilmente stai sottoutilizzando le risorse di elaborazione, il che significa che stai pagando per una CPU superiore a quella necessaria per il tuo carico di lavoro
- 70— 90%: intervallo ottimale in cui è possibile utilizzare le risorse in modo efficiente senza incorrere in intoppi
- Coerentemente al 100%: potrebbe indicare colli di bottiglia della CPU che potrebbero rallentare il rendering

Tieni presente che alcune attività di rendering richiederanno naturalmente un utilizzo più intensivo della CPU rispetto ad altre e l'utilizzo al 100% della vCPU potrebbe non essere un problema. Le attività di visualizzazione in tempo reale potrebbero mostrare un utilizzo più coerente della CPU, mentre le attività con requisiti di calcolo variabili potrebbero avere modelli diversi.

Utilizzo della memoria

Intervallo obiettivo: 70-85%

- Inferiore al 50%: istanze potenzialmente sovradimensionate per il carico di lavoro
- 70-85%: utilizzo ottimale con sufficiente margine di crescita per i picchi
- Oltre il 90%: rischio di peggioramento delle prestazioni o di errori out-of-memory

I requisiti di memoria possono variare in modo significativo a seconda della complessità della scena, della risoluzione delle texture e dei dati di simulazione. Il monitoraggio delle tendenze della memoria nel tempo è importante per identificare se i carichi di lavoro stanno aumentando in termini di requisiti di memoria.

Utilizzo dello spazio su disco

Intervallo obiettivo: 60-80%

- Inferiore al 40%: probabilmente un eccesso di provisioning di storage
- 60-85%: buon utilizzo con spazio per file temporanei e cache
- Oltre l'85%: rischio di esaurimento dello spazio durante i rendering di grandi dimensioni

Ricorda che I/O le prestazioni del disco possono essere importanti tanto quanto la capacità, specialmente per i carichi di lavoro che richiedono texture di read/write grandi dimensioni o la cache dei file durante il rendering.

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 e gestisci 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

Con una Deadline Cloud farm, puoi gestire gli utenti e le risorse del progetto. Una farm è il luogo in cui si trovano le risorse del progetto. La tua 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. Dopo aver creato una fattoria, puoi creare code e flotte per soddisfare le esigenze del tuo progetto.

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.

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 di Deadline Cloud, seleziona la farm 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 un Windows fleet, è necessario creare un AWS Secrets Manager segreto che contenga la password per l'utente Run as. Se non disponi di un segreto esistente con la password, scegli Crea segreto per aprire la console Secrets Manager e creare un segreto. Per ulteriori informazioni, consulta Gestire l'accesso a Windows segreti per gli utenti del lavoro nella Deadline Cloud Developer Guide.

8. La richiesta di un budget aiuta a gestire i costi della coda. Seleziona Non richiedere un budget o Richiedi un budget.
9. La 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 valore predefinito Conda ambiente di coda, 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 una coda predefinita Conda ambiente di coda. Questo ambiente fornisce alle flotte gestite dai servizi l'accesso ai pacchetti per le applicazioni e i renderer DCC dei partner. L'ambiente predefinito Per ulteriori informazioni, vedere. Predefinita Conda ambiente di coda

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.

Predefinita Conda ambiente di coda

Quando si crea una coda associata a una flotta gestita dal servizio, è possibile aggiungere un ambiente di coda predefinito che supporti Condaper scaricare e installare pacchetti in un ambiente virtuale per i tuoi lavori.

Se aggiungi un ambiente di coda predefinito con la console Deadline Cloud, l'ambiente viene creato per te. Se aggiungi una coda in un altro modo, ad esempio con AWS CLI o with AWS CloudFormation, dovrai creare tu stesso l'ambiente di coda. Per assicurarti di avere i contenuti corretti per l'ambiente, puoi fare riferimento ai file YAML del modello di ambiente di coda sui file YAML. GitHub Per i contenuti dell'ambiente di coda predefinito, consultate il file YAML dell'ambiente di coda predefinito su. GitHub

Sono disponibili altri modelli di ambiente di coda GitHub che è possibile utilizzare come punto di partenza per le proprie esigenze.

Conda fornisce pacchetti provenienti dai canali. Un canale è una posizione in cui vengono archiviati i pacchetti. Deadline Cloud fornisce un canale `deadline-cloud` che ospita Conda pacchetti che supportano le applicazioni e i renderer DCC dei partner. Seleziona ciascuna scheda qui sotto per visualizzare i pacchetti disponibili per Linux oppure Windows.

Linux

- Frullatore
  - `blender=3.6`
  - `blender=4.2`
  - `blender-openjd`
- Houdini
  - `houdini=19.5`
  - `houdini=20.0`
  - `houdini=20.5`
  - `houdini-openjd`
- Maya
  - `maya=2024`

    `maya=2025`
  - `maya-mtoa=2024.5.3`

    maya-mtoa=2025.5.4
  - maya-openjd
- Nuke
  - nuke=15
  - nuke-openjd

Windows

- After Effects
  - aftereffects=24.6
  - aftereffects=25.1
- Cinema 4D
  - cinema4d=2024
  - cinema4d=2025
  - cinema4d-openjd
- KeyShot
  - keyshot=2024
  - keyshot-openjd

Quando invii un lavoro a una coda con l'impostazione predefinita Conda ambiente, l'ambiente aggiunge due parametri al lavoro. Questi parametri specificano il Conda pacchetti e 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 separato da spazi di Conda canali come `deadline-cloud` `conda-forge`, `s3://amzn-s3-demo-bucket/conda/channel`. L'impostazione predefinita è `deadline-cloud` un canale disponibile per le flotte gestite dai servizi che fornisce applicazioni e renderer DCC dei 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.*`

Ti consigliamo di associare qualsiasi invio solo alle versioni elencate nella tabella precedente, ad esempio blender=3.6. Questo perché le versioni delle patch influiscono sui pacchetti disponibili. Ad esempio, quando rilasciamo Blender 3.6.17, non distribuiremo più Blender 3.6.16. Tutti gli invii bloccati su blender=3.6.16 falliranno. Se aggiungi blender=3.6, otterrai l'ultima versione della patch distribuita e i lavori non ne risentiranno. Per impostazione predefinita, i mittenti di DCC si collegano alle versioni correnti elencate nella tabella precedente, escluso il numero di patch, ad esempio blender=3.6.

Associa una coda e una flotta

Per elaborare i lavori, è necessario associare una coda a una flotta. È possibile associare una singola flotta a più code e una singola coda a più flotte. Quando si associa una flotta a più code, i lavoratori vengono suddivisi equamente tra loro. Allo stesso modo, quando si associa una coda a più flotte, i lavori vengono distribuiti in modo uniforme tra tali flotte. Segui questi passaggi per associare una coda esistente a una flotta esistente:

1. Dalla tua Deadline Cloud farm, seleziona la coda che desideri associare a una flotta. Viene visualizzata la coda.
2. Per selezionare una flotta da associare alla 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.

Flotte Deadline Cloud

Questa sezione spiega come gestire flotte gestite dai servizi 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 Deadline Cloud. Queste impostazioni predefinite sono progettate per essere efficienti e convenienti.
- Le flotte gestite dal cliente (CMFs) offrono il pieno controllo sulla pipeline di elaborazione. Un CMF può risiedere all'interno AWS dell'infrastruttura, in sede o in un data center condiviso. Ciò include il rifornimento, le operazioni, la gestione e lo smantellamento dei lavoratori della flotta.

Quando si associa una flotta a più code, il parco macchine divide i lavoratori in modo uniforme tra tali code.

Argomenti

Flotte gestite dai servizi

Una flotta gestita dai servizi (SMF) è una flotta di lavoratori con impostazioni predefinite fornite da Deadline Cloud. Queste impostazioni predefinite sono progettate per essere efficienti ed economiche.

Alcune impostazioni predefinite limitano la quantità di tempo in cui i lavoratori e le attività possono essere eseguiti. Un lavoratore può lavorare solo per sette giorni e un'attività può essere eseguita solo per cinque giorni. Quando viene raggiunto il limite, l'attività o il lavoratore si interrompe. In tal caso, potresti perdere il lavoro svolto dal lavoratore o dall'attività. Per evitare ciò, monitora i lavoratori e le attività per assicurarti che non superino i limiti di durata massima. Per ulteriori informazioni sul monitoraggio dei lavoratori, consultaUtilizzo del monitor Deadline Cloud.

Crea una flotta gestita dai servizi

1. Dalla console Deadline Cloud, accedi alla fattoria in cui vuoi creare la flotta.
2. Seleziona la scheda Flotte, quindi scegli Crea flotta.

3. Inserisci un nome per la tua flotta.
4. (Facoltativo) Inserisci una descrizione. Una descrizione chiara può aiutarti a identificare rapidamente lo scopo della tua flotta.
5. Seleziona il tipo di flotta gestita dal servizio.
6. 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.
7. 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.
8. Scegli Next (Successivo).
9. Scegli tra istanze con sola CPU o istanze accelerate da GPU. Le istanze con accelerazione GPU possono essere in grado di elaborare i tuoi lavori più velocemente, ma possono essere più costose.
10. Seleziona il sistema operativo per i tuoi dipendenti. Puoi lasciare l'impostazione predefinita, Linux o scegliere Windows.
11. (Facoltativo) Se hai selezionato istanze con accelerazione GPU, imposta il numero massimo e minimo di istanze GPUs in ciascuna istanza. A scopo di test, sei limitato a una GPU. Per richiedere di più per i tuoi carichi di lavoro di produzione, consulta Richiedere un aumento delle quote nella Service Quotas User Guide.
12. Inserisci le vCPU minime e massime necessarie per la tua flotta.
13. Inserisci la memoria minima e massima di cui hai bisogno per la tua flotta.
14. (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.
15. (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 impostato il numero minimo di istanze **0** per garantire che il parco istanze rilasci tutte le istanze quando nessun lavoro è in coda.
16. (Facoltativo) Puoi specificare la dimensione del volume Amazon Elastic Block Store (Amazon EBS) gp3 che verrà collegato ai lavoratori di questa flotta. Per ulteriori informazioni, consulta la guida per l'utente di EBS.

17. Scegli Next (Successivo).
18. (Facoltativo) Definisci funzionalità personalizzate per i lavoratori che definiscono le caratteristiche di questa flotta che possono essere combinate con le funzionalità host personalizzate specificate negli invii di lavoro. Un esempio è un tipo di licenza particolare se prevedi di connettere la tua flotta al tuo server di licenze.
19. Scegli Next (Successivo).
20. (Facoltativo) Per associare la tua flotta a una coda, seleziona una coda dal menu a discesa. Se la coda è configurata 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, vedere. Predefinita Conda ambiente di coda
21. Scegli Next (Successivo).
22. (Facoltativo) Per aggiungere un tag alla tua flotta, scegli Aggiungi nuovo tag, quindi inserisci la chiave e il valore per quel tag.
23. Scegli Next (Successivo).
24. Controlla le impostazioni del parco veicoli, quindi scegli Crea flotta.

Usa un acceleratore GPU

Puoi configurare gli host dei lavoratori nelle tue flotte gestite dai servizi in modo che utilizzino uno o più GPUs host per accelerare l'elaborazione dei lavori. L'uso di un acceleratore può ridurre il tempo necessario per elaborare un lavoro, ma può aumentare il costo di ogni istanza di worker. Dovresti testare i tuoi carichi di lavoro per comprendere i compromessi tra una flotta che utilizza acceleratori GPU e flotte che non lo fanno.

> **Note**
>
> A scopo di test, sei limitato a una GPU. Per richiedere di più per i tuoi carichi di lavoro di produzione, consulta Richiedere un aumento delle quote nella Service Quotas User Guide.

Sei tu a decidere se la tua flotta utilizzerà gli acceleratori GPU quando specifichi le funzionalità delle istanze di lavoro. Se decidi di utilizzarli GPUs, puoi specificare il numero minimo e massimo di GPUs per ogni istanza, i tipi di chip GPU da utilizzare e il driver di runtime per. GPUs

Gli acceleratori GPU disponibili sono:

- `T4`- GPU NVIDIA T4 Tensor Core
- `A10G`- GPU NVIDIA A10G Tensor Core
- `L4`- GPU NVIDIA L4 Tensor Core
- `L40s`- GPU NVIDIA L40S Tensor Core

È possibile scegliere tra i seguenti driver di runtime:

- `Latest`- Utilizza il runtime più recente disponibile per il chip. Se si specifica `latest` e viene rilasciata una nuova versione del runtime, viene utilizzata la nuova versione del runtime.
- `grid:r570`- Software NVIDIA vGPU 18
- `grid:r550`- Software NVIDIA vGPU 17
- `grid:r535`- Software NVIDIA vGPU 16

Se non si specifica un runtime, Deadline Cloud lo utilizza `latest` come predefinito. Tuttavia, se disponi di più acceleratori e ne specifichi `latest` alcuni e lasci vuoti altri, Deadline Cloud solleva un'eccezione.

Licenze software per flotte gestite dai servizi

Deadline Cloud fornisce licenze basate sull'utilizzo (UBL) per pacchetti software di uso comune. I pacchetti software supportati vengono automaticamente concessi in licenza quando vengono eseguiti su una flotta gestita dai servizi. Non è necessario configurare o gestire un server di licenze software. Le licenze sono scalabili in modo da non esaurirle per lavori più grandi.

Puoi installare pacchetti software che supportano UBL utilizzando il canale conda integrato di Deadline Cloud oppure puoi utilizzare i tuoi pacchetti. Per ulteriori informazioni sul canale conda, consulta. Crea un ambiente di coda

Per un elenco dei pacchetti software supportati e informazioni sui prezzi di UBL, consulta i prezzi di AWS Deadline Cloud.

Porta la tua licenza con flotte gestite dai servizi

Con le licenze basate sull'utilizzo (UBL) di Deadline Cloud non è necessario gestire contratti di licenza separati con i fornitori di software. Tuttavia, se disponi di licenze esistenti o devi utilizzare software non disponibile tramite UBL, puoi utilizzare le tue licenze software con le flotte gestite dai

servizi Deadline Cloud. Collegate la vostra SMF al server delle licenze software via Internet per richiedere una licenza per ogni lavoratore della flotta.

Per un esempio di connessione a un server di licenze utilizzando un proxy, consulta Connect flotte gestite dal servizio a un server di licenze personalizzato nella Deadline Cloud Developer Guide.

Compatibilità VFX Reference Platform

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

Viene aggiornato ogni anno. VFX Reference Platform Queste considerazioni sull'utilizzo di una piattaforma di riferimento AL2 023 che include 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' EC2 istanza Amazon AL2 023, considera quanto segue:

- La versione glibc installata con AL2 023 è compatibile per l'uso in fase di esecuzione, ma non per la creazione di software compatibile con la VFX Reference Platform CY2 024 o versioni precedenti.
- Python 3.9 e 3.11 sono forniti con la flotta gestita dai servizi che lo rende compatibile con 022 e 024. VFX Reference Platform CY2 CY2 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 CY2 022, 023 e CY2 024. CY2

- Altre librerie con versioni specificate da non VFX Reference Platform sono fornite dal parco giochi gestito 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.

Flotte gestite dai clienti

Se desideri utilizzare una flotta di lavoratori che gestisci, puoi creare una flotta gestita dal cliente (CMF) che Deadline Cloud utilizza per elaborare i tuoi lavori. Usa un CMF quando:

- Hai già dipendenti locali da integrare con Deadline Cloud.
- Hai lavoratori in un data center condiviso.
- Desideri il controllo diretto dei lavoratori di Amazon Elastic Compute Cloud (Amazon EC2).

Quando utilizzi un CMF, hai il pieno controllo e la responsabilità della flotta. Ciò include il rifornimento, le operazioni, la gestione e lo smantellamento dei lavoratori della flotta.

Per ulteriori informazioni, consulta Creare e utilizzare flotte gestite dai clienti di Deadline Cloud nella Deadline Cloud Developer Guide.

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 in grado di 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.

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.

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. (Facoltativo) 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.
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

Nell'ambito della gestione di utenti e gruppi, puoi concedere autorizzazioni di accesso 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**
>
> Le modifiche alle autorizzazioni di accesso possono richiedere fino a 10 minuti per essere applicate al sistema.

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, scegli Utenti.

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

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, scegli Rimuovi gruppo.

Users

Come aggiungere utenti

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

4. Scegli Aggiungi.

Per rimuovere utenti

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

Offerte di lavoro Deadline Cloud

Un lavoro 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.

Un mittente è un plug-in per l'applicazione DCC (Digital Content Creation) che gestisce la creazione di un lavoro nell'interfaccia dell'applicazione DCC. Dopo aver creato il lavoro, usi il mittente per inviarlo a Deadline Cloud per l'elaborazione.

Il mittente crea un modello Open Job Specification (OpenJD) che descrive il lavoro. Allo stesso tempo carica i file delle risorse in un bucket Amazon Simple Storage Service (Amazon S3). Per ridurre i tempi di caricamento, il mittente invia solo i file che sono stati modificati dall'ultimo caricamento su Amazon S3

Puoi anche creare un lavoro nei seguenti modi.

- Da terminale: per gli utenti che inviano un lavoro e che si sentono a proprio agio utilizzando la riga di comando.
- Da uno script: per personalizzare e automatizzare i carichi di lavoro.
- Da un'applicazione: per quando il lavoro dell'utente è in un'applicazione o quando il contesto di un'applicazione è importante.

Per ulteriori informazioni, consulta Come inviare un lavoro a Deadline Cloud nella Deadline Cloud Developer Guide.

Un lavoro è composto da:

- Priorità: l'ordine approssimativo in cui Deadline Cloud elabora un lavoro in coda. È possibile impostare la priorità del lavoro tra 0 e 100, i lavori con una priorità numerica più alta vengono generalmente elaborati per primi. I lavori con la stessa priorità vengono elaborati nell'ordine di ricezione.
- 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, ad esempio un numero di frame, utilizzati nello script. Il processo è completo quando tutte le attività sono state completate per tutte le fasi.
- Ambiente: imposta e smonta le istruzioni condivise da più passaggi o attività.

Utilizzo di un mittente Deadline Cloud

Un mittente è uno strumento che si integra con la creazione di contenuti digitali in modo da poter inviare lavori di rendering direttamente a Deadline Cloud. Questa integrazione semplifica il flusso di lavoro eliminando la necessità di passare da un'applicazione all'altra o di trasferire manualmente i file. In questo modo si risparmia tempo e si riduce il rischio di errori.

I mittenti sono disponibili per molte delle applicazioni DCC più diffuse. L'installazione di un mittente aggiunge opzioni specifiche di Deadline Cloud all'interfaccia dell'applicazione, in genere nelle impostazioni di rendering o nel menu di esportazione.

Con un mittente di Deadline Cloud puoi:

- Configura i parametri del processo di rendering nel tuo ambiente DCC familiare
- Invia offerte di lavoro a Deadline Cloud senza uscire dalla tua candidatura
- Riduci il rischio di errori associati ai trasferimenti manuali di file
- Risparmia tempo perché non è necessario passare da un'applicazione all'altra

Per trovare un mittente per la tua applicazione DCC, controlla l'elenco dei mittenti supportati. Quindi segui le istruzioni riportate per installare il mittenteConfigura i mittenti di Deadline Cloud.

Se la tua applicazione non dispone di un mittente supportato, puoi comunque eseguire i job per la tua applicazione. Potrebbe essere disponibile un job bundle di esempio oppure puoi creare un semplice submitter per il comando render CLI dell'applicazione. Per ulteriori informazioni, consulta i modelli Open Job Description (OpenJD) per Deadline Cloud nella Deadline Cloud Developor Guide.

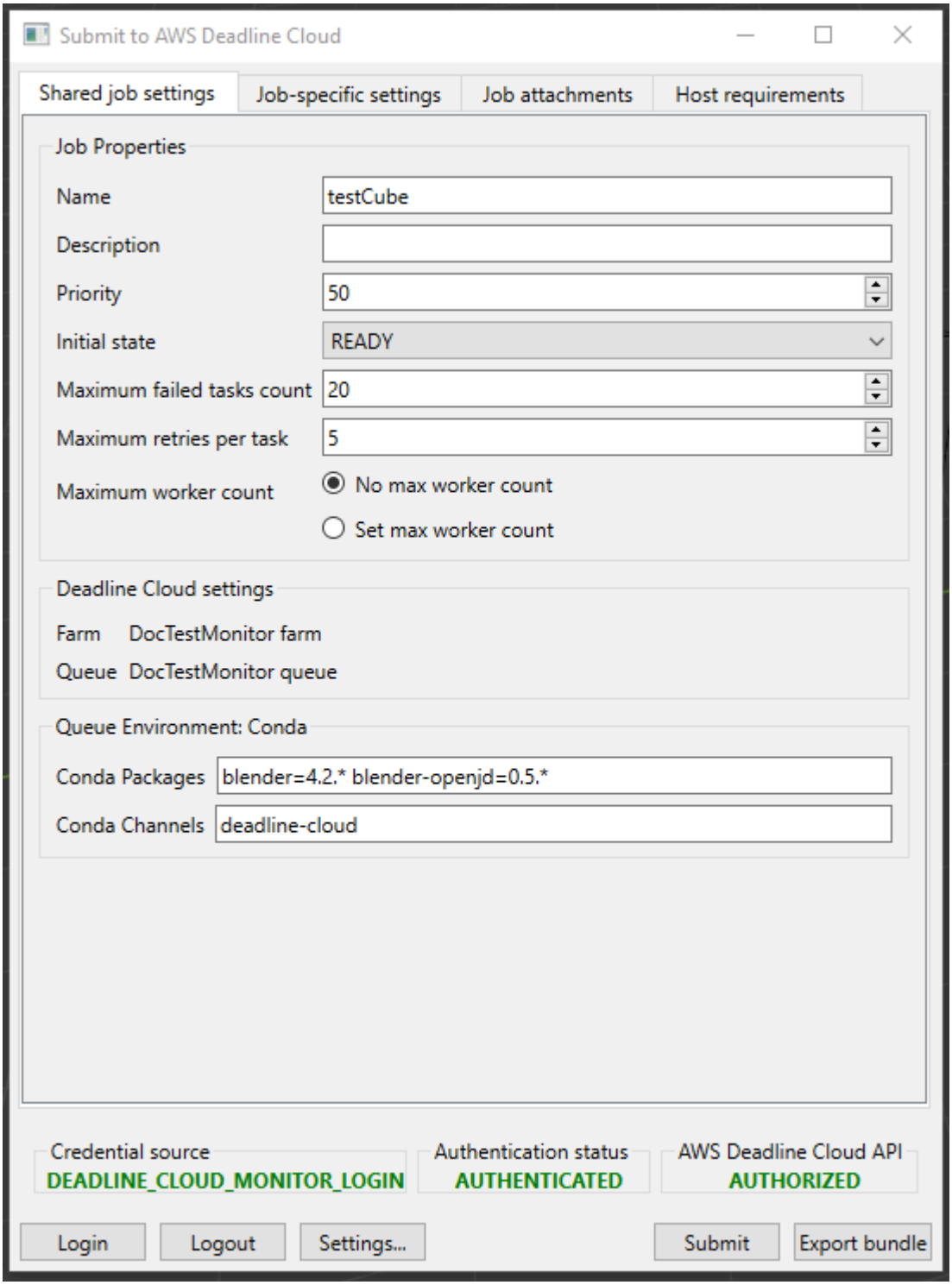
Gli esempi in questo argomento utilizzano il Blender submitter, ma i passaggi per utilizzare altri mittenti sono simili.

> **Note**
>
> Per utilizzare un mittente, devi aver effettuato l'accesso al monitor Deadline Cloud.

Il mittente ha quattro schede:

Argomenti

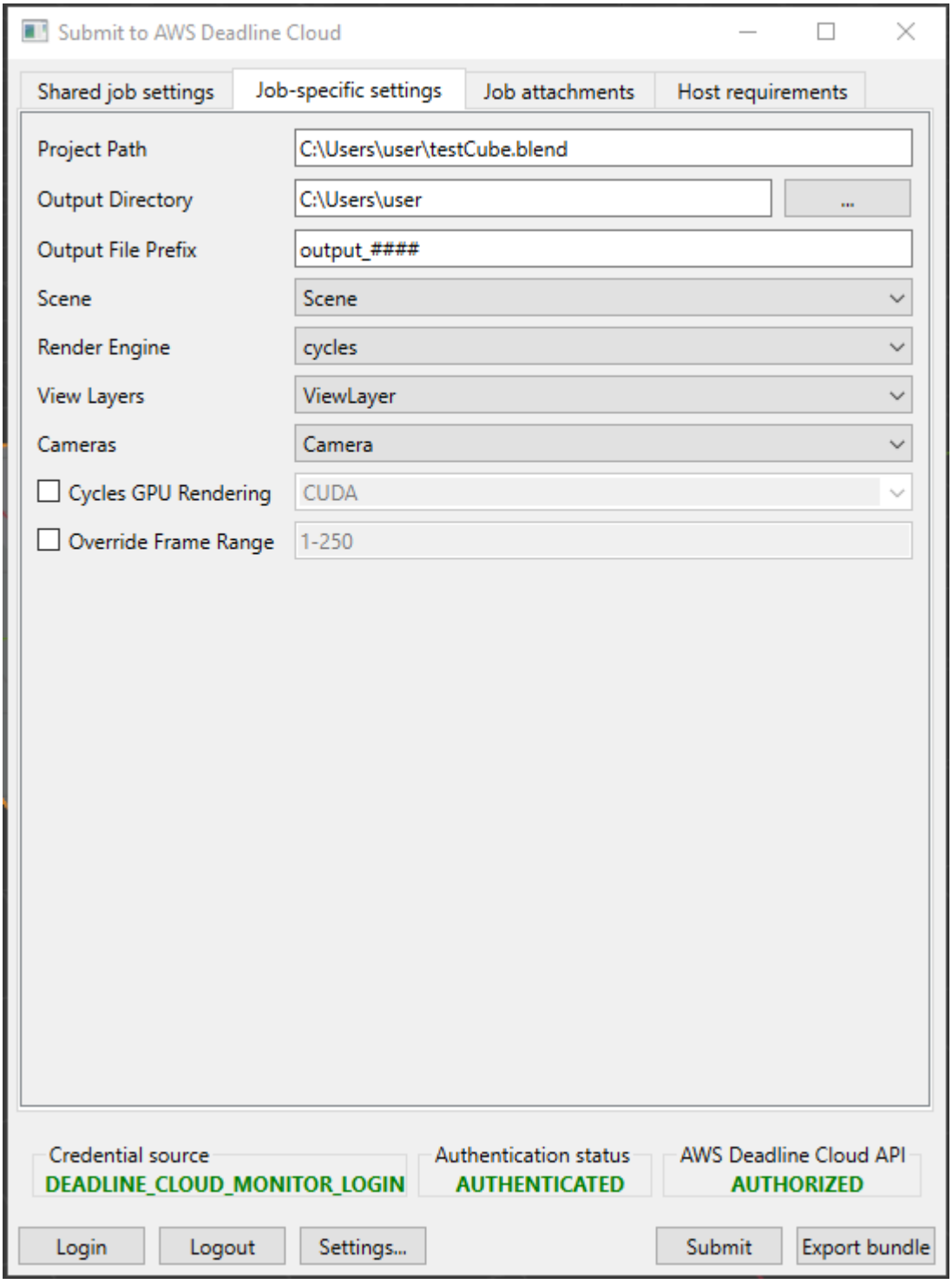
Scheda delle impostazioni dei lavori condivisi



La scheda delle impostazioni dei lavori condivisi contiene le impostazioni comuni a tutti i lavori inviati a Deadline Cloud utilizzando il mittente. Le tre sezioni sono:

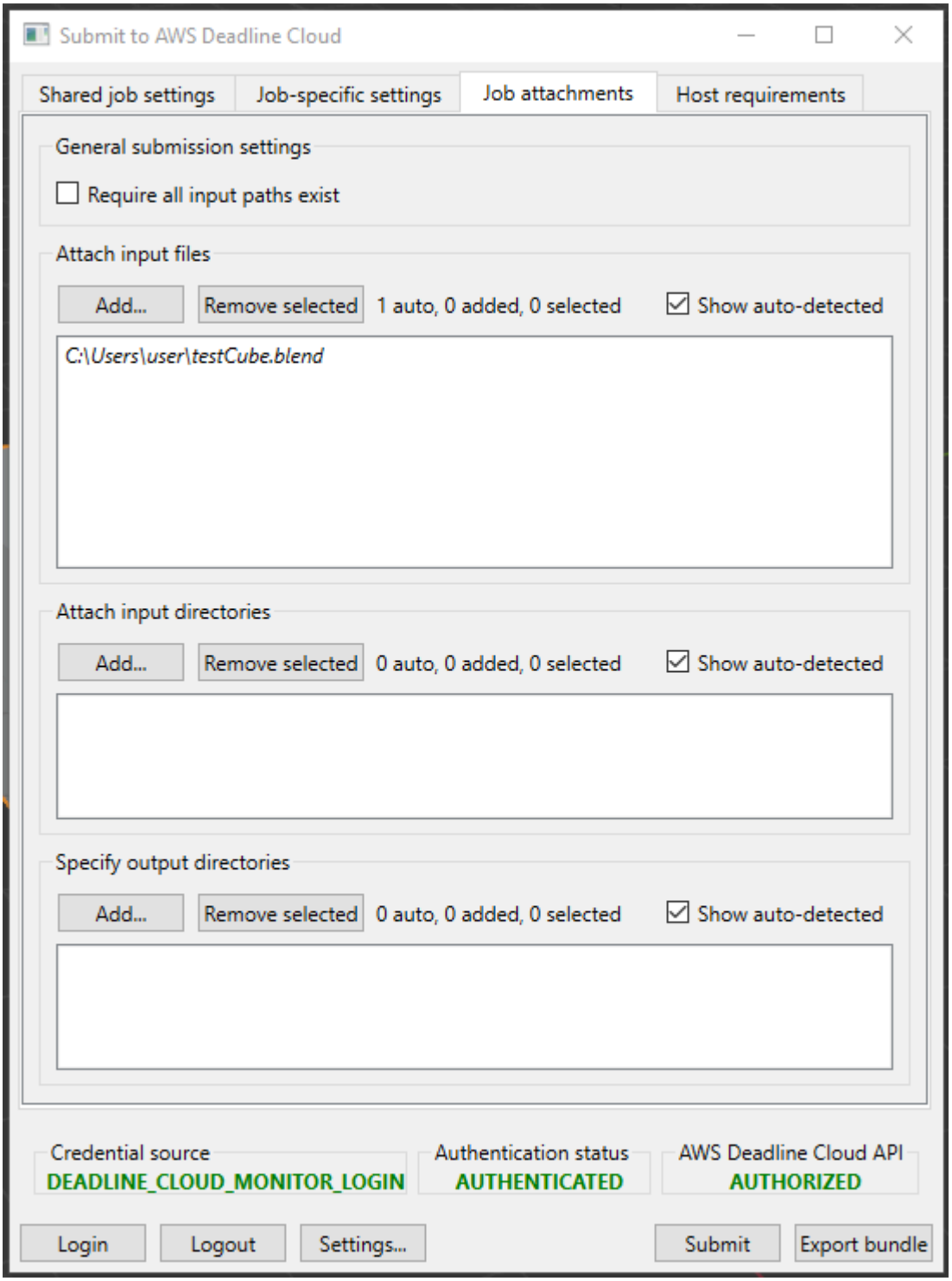
- Proprietà del lavoro: imposta le proprietà generali del lavoro. Queste proprietà sono presenti nei mittenti per tutte le applicazioni DCC.
- Impostazioni Deadline Cloud: mostra la farm e la coda a cui viene inviato il lavoro. Per modificare la fattoria e la coda, usa le Impostazioni... pulsante nella parte inferiore del mittente.
- Ambiente di coda: imposta i valori dei parametri definiti nell'ambiente di coda. Deadline Cloud aggiunge i valori dei parametri predefiniti per la tua applicazione DCC, puoi aggiungere valori aggiuntivi se necessario.

Scheda delle impostazioni specifiche del lavoro



La scheda delle impostazioni specifiche del lavoro contiene le impostazioni specifiche dell'applicazione DCC. Specificate queste impostazioni in base alle opzioni disponibili nell'applicazione.

Scheda Job attachments

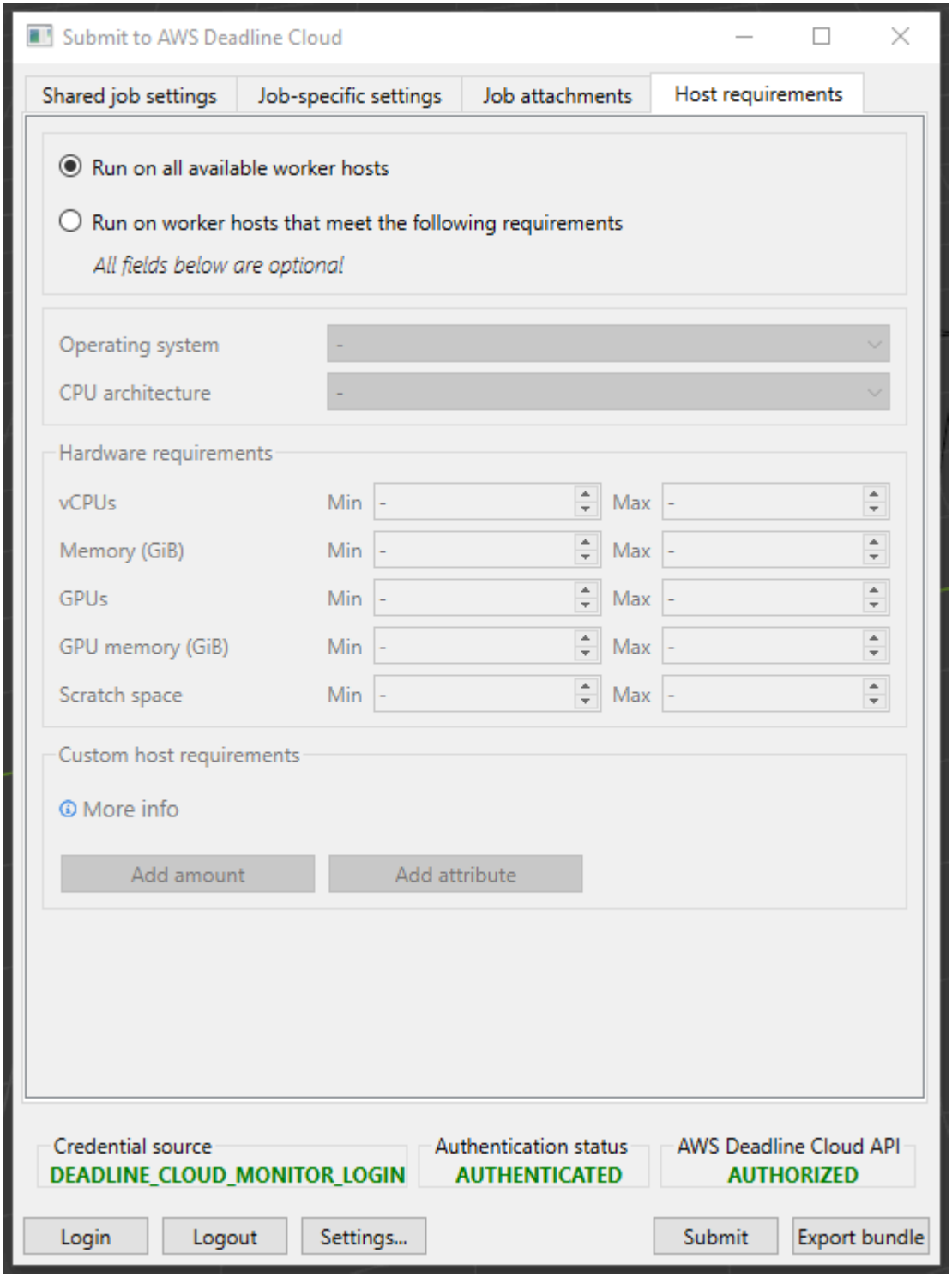


La scheda degli allegati del lavoro mostra tutti i file necessari per completare un rendering. Il mittente cerca di trovare tutti i file necessari per il rendering. I file che identifica appaiono negli elenchi in corsivo.

Potete aggiungere file e directory di input aggiuntivi che contengono altre risorse necessarie per il rendering che non sono state rilevate automaticamente.

Se il lavoro scrive file in più directory di output, è necessario specificare le directory qui in modo che facciano parte del download del lavoro.

Scheda Requisiti dell'host



Le schede dei requisiti dell'host impostano le funzionalità della flotta necessarie per elaborare il lavoro. Le capacità sono specificate per l'intera flotta, non per i singoli lavoratori della flotta.

Se alla coda sono associati limiti di risorse, utilizza il pulsante Aggiungi importo per specificare il limite. Per ulteriori informazioni, consulta Creare limiti di risorse per i lavori

Elaborazione dei lavori di Deadline Cloud

Quando un lavoro entra in coda, Deadline Cloud lo pianifica su una o più flotte associate alle code. La flotta viene scelta in base alle funzionalità configurate per la flotta e ai requisiti dell'host di una fase specifica. Se un lavoro presenta un requisito che non può essere soddisfatto da nessuna delle flotte associate alla coda, lo stato del lavoro viene impostato su «Non compatibile» e le altre fasi del lavoro vengono annullate.

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 apre sessioni su più lavoratori se le impostazioni di ridimensionamento delle flotte lo consentono.

È possibile configurare il software in un Amazon Machine Image (AMI), oppure l'operatore può caricare il software in fase di esecuzione da un repository o da un gestore di pacchetti. Puoi utilizzare ambienti queue, job o step per distribuire il software che preferisci.

Il servizio Deadline Cloud utilizza il modello OpenJD per identificare 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.

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.

> **Note**
>
> 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.

Monitoraggio dei lavori di Deadline Cloud

Il monitor AWS Deadline Cloud ti offre una visione generale dei tuoi lavori. Usalo per:

- Monitora e gestisci i lavori
- Visualizza l'attività dei lavoratori sulle flotte
- Tieni traccia dei budget e dell'utilizzo
- Scarica i risultati di un lavoro.

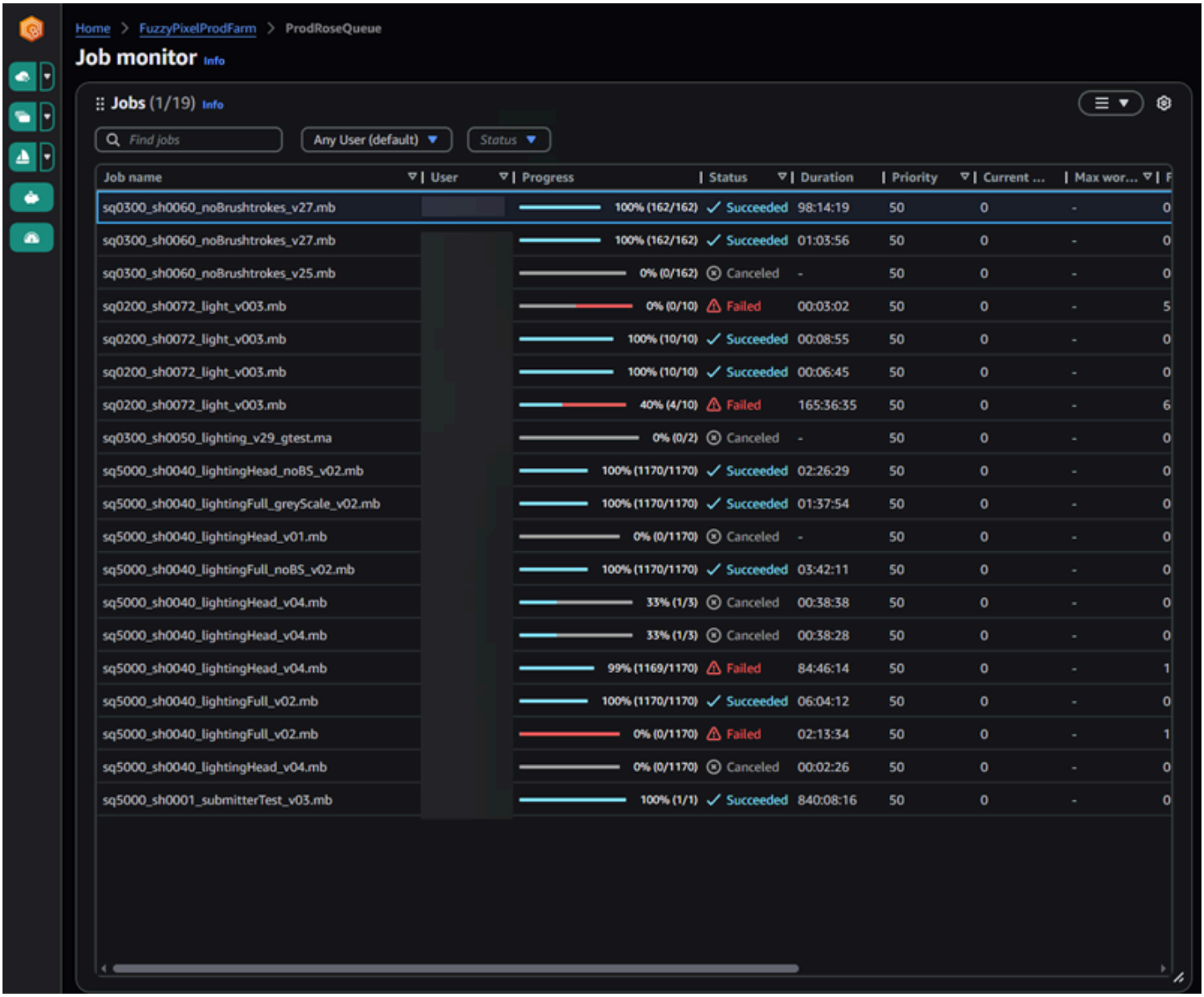
Per monitorare un lavoro specifico, seleziona la fattoria e la coda che contengono il lavoro, quindi seleziona il lavoro dall'elenco. È possibile utilizzare la casella di ricerca per individuare uno o più lavori specifici in coda.

Fai clic con il pulsante destro del mouse su un lavoro, un passaggio o un'attività per visualizzare le opzioni relative all'elemento. È possibile:

- Modificare lo stato
- Sospendere e riprendere l'elemento
- Richiedi l'articolo
- Scarica l'output
- Per le attività: visualizza i registri delle attività e dei lavoratori.

Per ulteriori informazioni, consulta Utilizzo del monitor Deadline Cloud.

Ogni attività di un processo o di una fase ha uno stato. Lo stato di un processo o di un'operazione 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 EC2 (Amazon).

`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.

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 dai servizi, 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 sono crittografati nel bucket S3. Questo aiuta a proteggere le tue 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 *Region* *accountID*, e *keyID* adattatelo ai vostri valori.

```
{
   "Effect": "Allow",
   "Action": [
       "kms:Decrypt",
       "kms:DescribeKey",
       "kms:GenerateDataKey"
   ],
   "Resource": [
       "arn:aws:kms:Region:accountID:key/keyID"
   ]
}
```

5. Scegli Next (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 per i file system virtuali è disponibile solo per Linux lavoratori in 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.

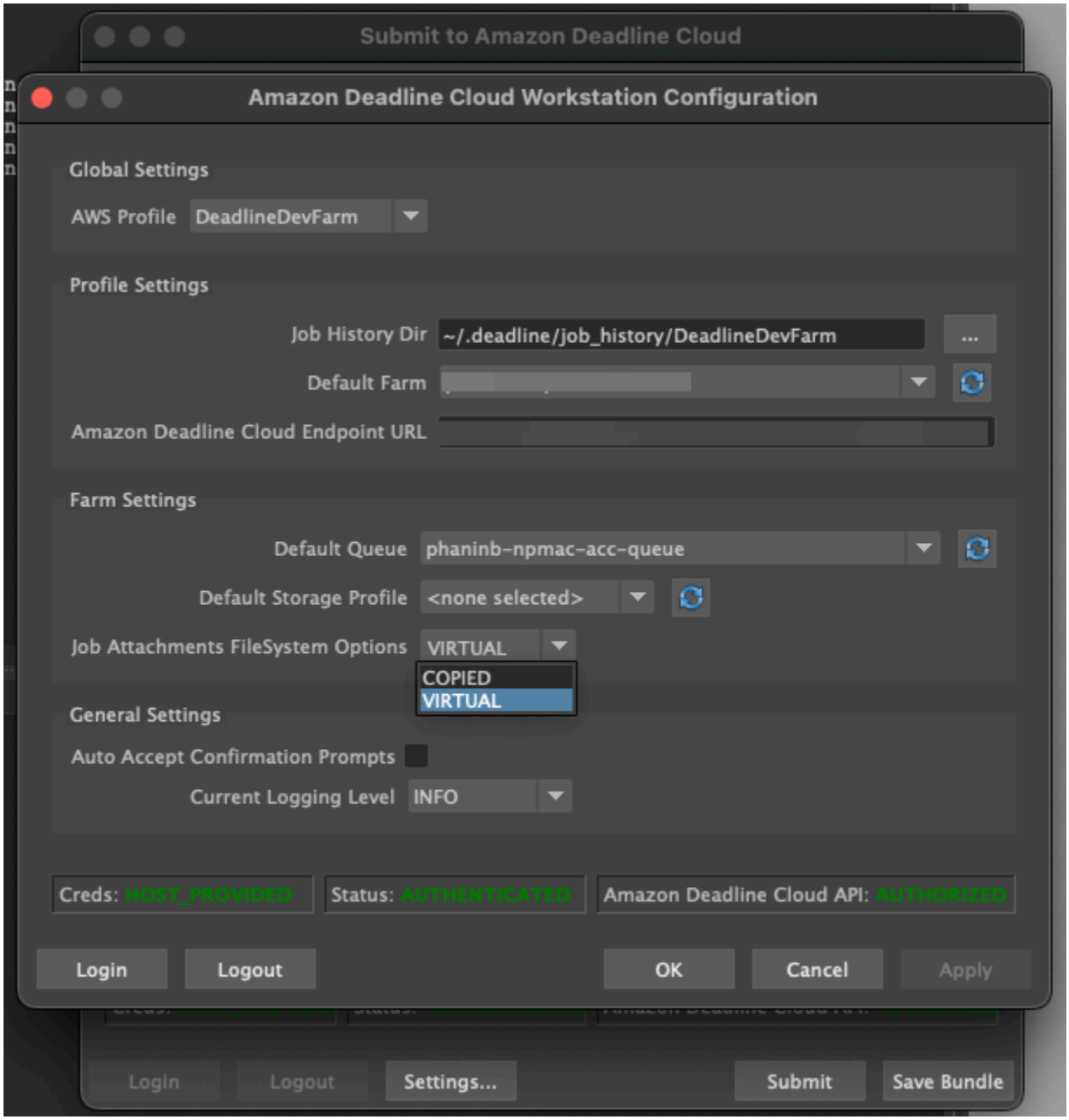
Abilita il supporto VFS

Il supporto del file system virtuale (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 il 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 registri delle sessioni e dei lavoratori 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.

Tieni traccia della spesa e dell'utilizzo per le fattorie 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.
- AWS tag di allocazione dei costi: con i tag di allocazione dei costi, puoi tenere traccia dei costi dettagliati per tutti i tuoi servizi. AWS Per ulteriori informazioni, consulta Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione AWS dei costi.

Ipotesi relative ai costi

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 ed è disponibile solo per le flotte gestite dai servizi. 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 provider di servizi cloud locali o di altro tipo. I costi effettivi di queste risorse non vengono calcolati.
- Costi dei lavoratori inattivi. I costi del lavoratore inattivo non sono inclusi quando lo stato del lavoratore è INATTIVO. Ciò può accadere per le flotte con un numero minimo di istanze superiore a zero o quando i lavoratori passano da un lavoro all'altro. I costi dei lavoratori inattivi non sono inclusi nei calcoli.
- Ora di arresto e inizio del lavoratore. Dopo che i lavoratori hanno completato un lavoro, il costo per il passaggio da IDLE a STOPPING e da STOPPING a STOPPING non è incluso nelle stime dei costi di Deadline Cloud.
- 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 (Licenze software per flotte gestite dai servizi), gli strumenti di gestione dei costi di Deadline Cloud non possono tenere conto di questo costo.

Controlla i costi con un budget

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

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.

Apri il gestore del budget di Deadline Cloud

Per aprire il 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.
4. Nel monitor di 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.

Crea un budget per una coda di Deadline Cloud

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 il nome del budget per il budget.
4. (Facoltativo) Nel campo della descrizione, inserisci una breve descrizione del budget.
5. Da Risorsa, utilizza il menu a discesa Queue per 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 YYYY/MM/DD formato di tracciamento del budget 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 YYYY/MM/DD formato di tracciamento del budget o 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 passaggi precedenti.

9. Scegli Crea budget.

Visualizza un budget per la coda di Deadline Cloud

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 per una coda di Deadline Cloud

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, seleziona Modifica budget.
4. Apporta le modifiche desiderate, quindi scegli Aggiorna budget.

Disattiva un budget per una coda di Deadline Cloud

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, seleziona Disattiva budget. In pochi istanti, il budget selezionato passerà da Attivo a Inattivo e passerà dalla scheda Budget attivi alla scheda Budget inattivi.

Monitora un budget con eventi EventBridge

Deadline Cloud invia eventi relativi al budget, tramite Amazon EventBridge, al tuo bus eventi predefinito EventBridge . Puoi creare funzioni personalizzate che ricevono gli eventi e agiscono di conseguenza per inviare notifiche e avvisare automaticamente gli utenti via e-mail, Slack o altri canali quando un budget raggiunge livelli predefiniti. Ad esempio, puoi inviare messaggi SMS quando un budget raggiunge una determinata soglia. Questo ti aiuta a tenere sotto controllo le tue spese e a prendere decisioni informate prima che il budget sia esaurito.

Deadline Cloud aggrega periodicamente i dati di utilizzo e costo per ogni render farm. Quindi controlla se una delle soglie di budget è stata superata. Se viene superata una soglia, Deadline Cloud attiva un evento per avvisarti in modo che tu possa intraprendere le azioni appropriate. Un evento viene attivato ogni volta che un budget supera una di queste soglie, specificate in percentuale del budget utilizzato:

- 10, 20, 30, 40, 50, 60, 70, 75, 80, 85, 90, 95, 96, 97, 98, 99, 100

Le soglie di utilizzo del budget si avvicinano man mano che un budget si avvicina all'utilizzo del 100%. Ciò consente di monitorare attentamente l'utilizzo man mano che il budget raggiunge il limite.

Puoi anche impostare soglie di budget personalizzate. Deadline Cloud invia un evento quando l'utilizzo supera le soglie personalizzate. Quando il budget raggiunge il 100%, Deadline Cloud interrompe l'invio di eventi. Se modifichi il budget, Deadline Cloud invia gli eventi corrispondenti alle tue soglie in base al nuovo importo del budget.

Puoi utilizzare la EventBridge console (https://console.aws.amazon.com/events/) per creare regole per inviare gli eventi Deadline Cloud al target appropriato per l'evento. Ad esempio, puoi inviare l'evento a una coda di Amazon Simple Queue Service e da lì a più destinazioni, come AWS End User Messaging SMS o un database Amazon Relational Database Service per la registrazione.

Per esempi di EventBridge regola, consulta i seguenti argomenti:

- Invia un'e-mail quando si verificano eventi utilizzando Amazon EventBridge.
- Creazione di una EventBridge regola Amazon che invii notifiche ad Amazon Q Developer nelle applicazioni di chat.
- Guida introduttiva ad Amazon EventBridge.

Per ulteriori informazioni sugli eventi relativi al budget, consulta l'evento Budget Threshold Reached nella Deadline Cloud Developer Guide.

Tieni traccia dell'utilizzo e dei costi con l'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
- Apri lo strumento di esplorazione dell'utilizzo

- Usa lo strumento di esplorazione dell'utilizzo

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.

> **Note**
>
> Se il fuso orario non si allinea a un'ora intera, ad esempio l'ora solare dell'India (UTC+ 5:30), lo strumento di esplorazione dell'utilizzo non mostra le metriche di utilizzo. Per visualizzare le metriche, imposta il fuso orario su un fuso orario che corrisponda a un'ora intera.

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:

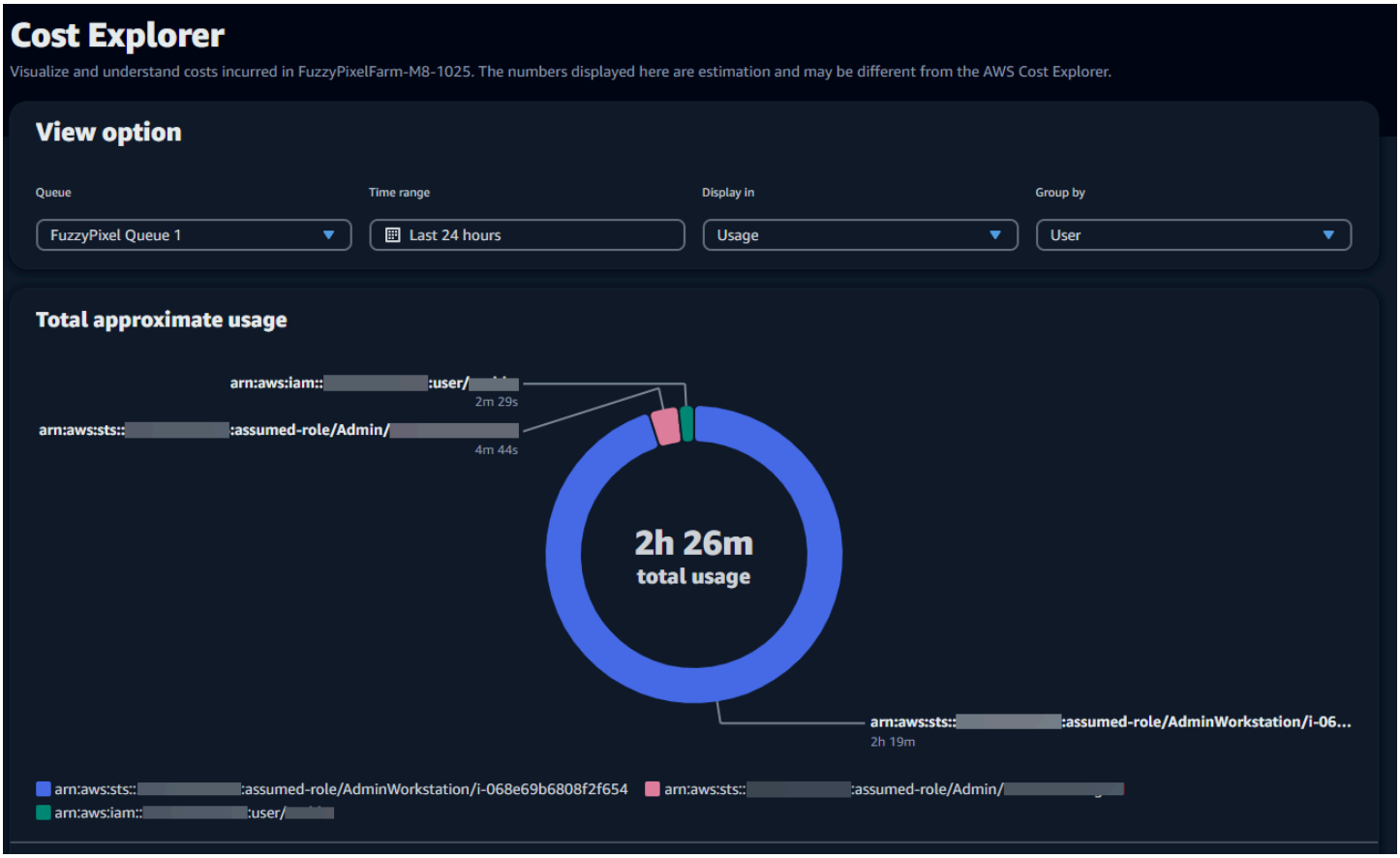
- Seleziona un intervallo di tempo più piccolo
- Seleziona un minor numero di code
- Seleziona un raggruppamento diverso, ad esempio il raggruppamento per coda anziché per lavoro

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.



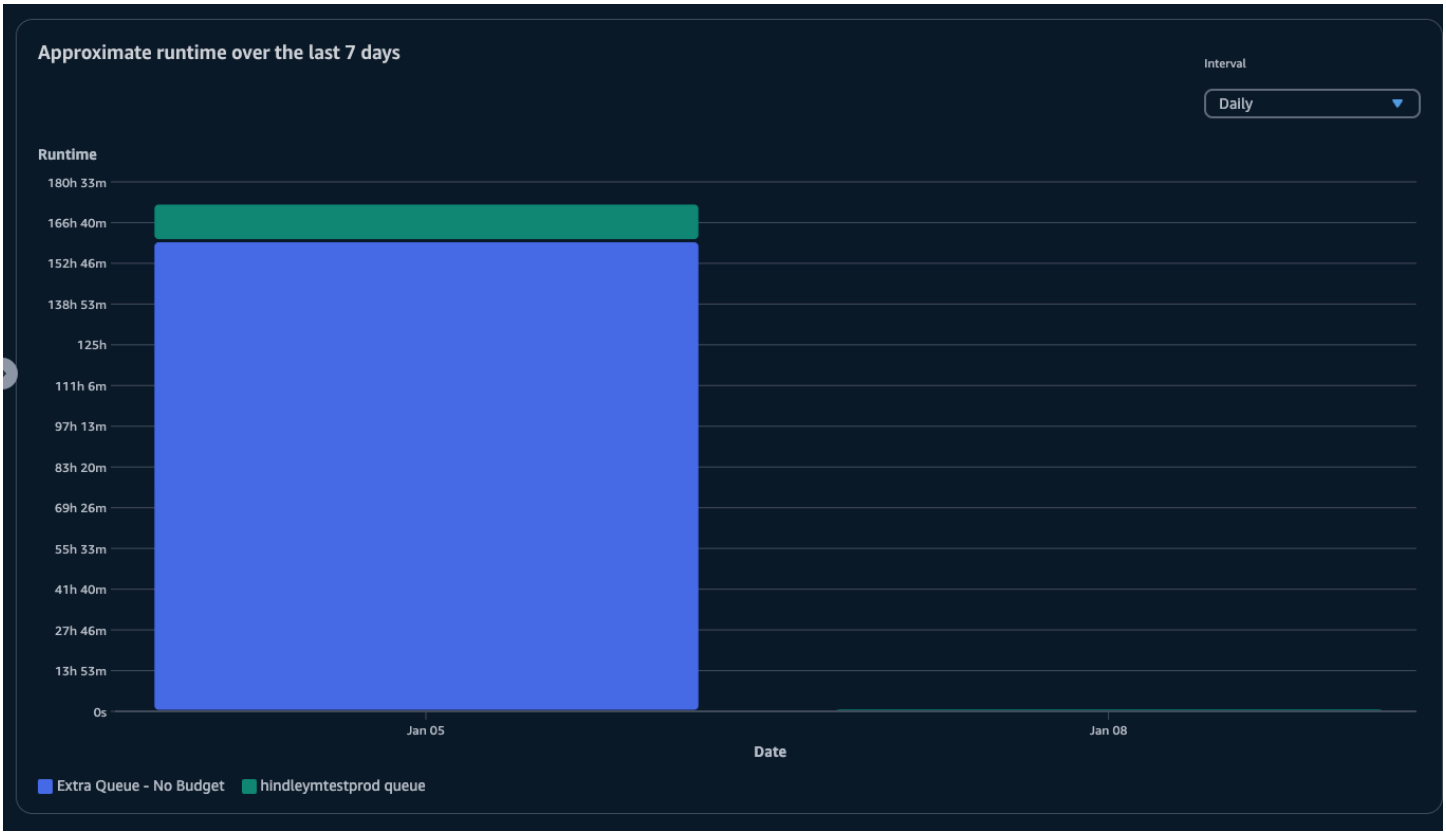
Visualizza una suddivisione delle metriche

Sotto il grafico a torta, Usage Explorer offre un'analisi più dettagliata di metriche specifiche, che cambieranno man mano che i parametri cambiano. Per impostazione predefinita, nell'Usage Explorer vengono visualizzati cinque risultati. È possibile 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
AWS Key Management Service	Prezzi di AWS Key Management Service
AWS PrivateLink	Prezzi di AWS PrivateLink
Amazon Simple Storage Service	Prezzi di Amazon S3

Servizio	Pagina dei prezzi
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.

Le migliori pratiche per Amazon EC2

Puoi utilizzare EC2 le istanze Amazon 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 dai clienti, puoi specificare i tipi di EC2 istanze Amazon 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 Amazon EC2 Spot 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. Negli argomenti seguenti viene illustrato 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.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo 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 Deadline Cloud o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. 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.

I dati inseriti nei campi dei nomi nei modelli di Deadline Cloud lavoro possono essere inclusi anche nei registri di fatturazione o diagnostica e non devono contenere informazioni riservate o sensibili.

Argomenti

Crittografia 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`— Permette di Deadline Cloud decifrare 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-abcdef1234567890098765432 1fedcba",
                "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-abcdef12345678900987654321fedcba",
            "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 della chiave gestita dal cliente e lo stato della chiave 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 Resource IDs (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 sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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)AWS in IAM nella 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 Casi d'uso per utenti IAM 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. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). 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 Create a role for a third-party identity provider (federation) 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 informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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 inoltrato (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 Forward access sessions.
  - Ruolo di servizio: 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 Create a role to delegate permissions to an Servizio AWS nella 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' EC2 istanza e che AWS CLI effettuano

richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

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 operazioni 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 sull'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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente 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 sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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 operazioni 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 () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

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 del servizio (SCPs): SCPs 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 di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- 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 o meno una richiesta quando sono coinvolti più tipi di policy, consulta la 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
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente 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. Esempi di policy basate sulle 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 operazioni 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 Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Deadline Cloud

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni 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 operazioni 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:

```
awsdeadlinecloud
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "awsdeadlinecloud:action1",
      "awsdeadlinecloud: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. In altre parole, 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). È possibile eseguire questa operazione per operazioni 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 relativi ARNs, 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. In altre parole, quale principale può eseguire operazioni 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. È possibile 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.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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

ACLs in Deadline Cloud

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle 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 Definizione delle autorizzazioni con autorizzazione 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 Passaggio da un ruolo utente a un ruolo IAM (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 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 Create a role to delegate permissions to an Servizio AWS nella 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 (console) nella Guida per l'utente IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da Deadline Cloud, incluso il formato di ARNs 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. È possibile 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 è possibile 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 il Sistema di analisi degli accessi IAM 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 Protezione dell'accesso API 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: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-FleetWorkerla guida di riferimento di AWS Managed Policy.

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 all'utente di creare lavoratori, assumere il ruolo della flotta per i lavoratori e applicare tag ai lavoratori

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-WorkerHostla guida di riferimento di AWS Managed Policy.

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 EC2 istanze Amazon.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-UserAccessFarmsla guida di riferimento di AWS Managed Policy.

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 EC2 istanze Amazon.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-UserAccessFleetsla guida di riferimento di AWS Managed Policy.

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 EC2 istanze Amazon.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-UserAccessJobsla guida di riferimento di AWS Managed Policy.

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 EC2 istanze Amazon.
- `identitystore`— Consente agli utenti di visualizzare i nomi di utenti e gruppi.

Per un elenco in JSON dei dettagli della policy, consulta AWSDeadlineCloud-UserAccessQueuesla guida di riferimento di AWS Managed Policy.

Deadline Cloud aggiorna le policy 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
AWSDeadlineCloud-WorkerHost— Modifica	Deadline Cloud ha aggiunto nuove azioni `deadline:TagResource` e ti ha `deadline:ListTagsForResource` permesso di aggiungere e visualizzare i tag associati ai lavoratori della tua flotta.	30 maggio 2025
AWSDeadlineCloud-UserAccessFarms— Modifica AWSDeadlineCloud-UserAccessJobs— Cambiare AWSDeadlineCloud-UserAccessQueues— Cambiare	Deadline Cloud ha aggiunto nuove azioni `deadline:GetJobTemplate` e ti ha consentito di `deadline:ListJobParameterDefinitions` inviare nuovamente i lavori.	7 ottobre 2024
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 `awsdeadlinecloud:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awsdeadlinecloud: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 `awsdeadlinecloud:`*`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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche 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 scoprire 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 informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

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:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa 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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: 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

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. 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:awsdeadlinecloud:*: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": "awsdeadlinecloud.amazonaws.com"
    },
    "Action": "awsdeadlinecloud:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:awsdeadlinecloud:*: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.

Deadline Cloud dispone anche di endpoint dual-stack. Gli endpoint dual-stack supportano le richieste di assistenza su e. IPv6 IPv4

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 supporta anche 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 quattro endpoint per l'accesso al servizio utilizzando AWS PrivateLink : due per IPv4 e due per. IPv6

I lavoratori utilizzano l'`scheduling.deadline.`*`region`*`.amazonaws.com`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 `management.deadline.`*`region`*`.amazonaws.com` 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. *`region`*Sostituiscilo con quello Regione AWS che hai distribuito. Deadline Cloud

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Deadline Cloud supporta endpoint dual-stack.

Se abiliti il DNS privato per gli endpoint dell'interfaccia, puoi effettuare richieste API Deadline Cloud utilizzando il nome DNS regionale predefinito. Ad esempio, `scheduling.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.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. 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. AWS CLI AWS SDKs 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 `AssumeQueueRoleForRead`AssumeQueueRoleForUser, 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 ciascuno *`placeholder`* di essi 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 *`placeholder`* testo 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, sostituiscilo *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:

- L'utilizzo di uno script di configurazione dell'host può modificare la sicurezza e le operazioni di un lavoratore. Una configurazione errata può causare l'instabilità o l'interruzione del lavoro del lavoratore. È responsabilità dell'utente eseguire il debug di tali errori.
- 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`attivati e attivatiWindows) Linux e instrada le tabelle `C:\Windows\system32\etc\hosts` sulle 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 Windows password segrete ed elimina quelle inutilizzate.
- 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.

Script di configurazione dell'host

- L'utilizzo di uno script di configurazione dell'host può modificare la sicurezza e le operazioni di un lavoratore. Una configurazione errata può causare l'instabilità o l'interruzione del lavoro del lavoratore. È responsabilità dell'utente eseguire il debug di tali errori.

Workstation

È importante proteggere le workstation 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 al DNS localemacOS, sostituisci i file di configurazione (attivati e `/etc/hosts` attivatiWindows) Linux e instrada le tabelle `C:\Windows\system32\etc\hosts` sulle workstation e sui sistemi operativi host dei lavoratori.
- Limita le autorizzazioni alle workstation e ai `/etc/resolve.conf` 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.

Verifica l'autenticità del software scaricato

Verifica l'autenticità del software dopo aver scaricato il programma di installazione per proteggerlo dalla manomissione dei file. Questa procedura funziona per entrambi i sistemi. Windows Linux

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 0penPGP chiave 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 OpenPGP chiave. 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 base all'attendibilità con un metodo gpg 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 del mittente di Deadline Cloud

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

   a. Torna alla pagina di download della console Deadline Cloud e scarica il file di 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 il monitor Deadline Cloud

   > **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 (Debian) scheda, la scheda Linux (RPM) 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 .rpm:

```
gpg --verify ./deadline-cloud-monitor_<APP_VERSION>_x86_64.deb.sig ./
deadline-cloud-monitor_<APP_VERSION>_x86_64.rpm
```

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 che puoi eseguire lo script di installazione del monitor Deadline Cloud.

Linux (AppImage)

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

1. Dalla AppImageUpdate pagina in poi GitHub, scarica il validate-x86_64. AppImagefile.
2. Dopo aver scaricato il file, per aggiungere i permessi di esecuzione, esegui il seguente comando.

```
chmod a+x ./validate-x86_64.AppImage
```

3. Per aggiungere i permessi di esecuzione, esegui il comando seguente.

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

4. Per verificare la firma del monitor di Deadline Cloud, esegui il seguente comando.

```
./validate-x86_64.AppImage ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
```

Se l'output contiene la fraseValidation successful, significa che la firma è stata verificata con successo e puoi eseguire in sicurezza lo script di installazione del monitor di Deadline Cloud.

Linux (Debian)

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

dpkg è lo strumento principale per la gestione dei pacchetti 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:

```
ProcessingLinux deadline-cloud-monitor_<APP_VERSION>_amd64.deb...
GOODSIG _gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
```

4. Per verificare il file.deb, verificate che GOODSIG sia presente nell'output.

Linux (RPM)

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

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

```
gpg --export --armor "Deadline Cloud" > key.pub
sudo rpm --import key.pub
```

```
rpm -K deadline-cloud-monitor-<APP_VERSION>-1.x86_64.rpm
```

3. L'output sarà simile a:

```
deadline-cloud-monitor-deadline-cloud-
monitor-<APP_VERSION>-1.x86_64.rpm-1.x86_64.rpm: digests signatures OK
```

4. Per verificare il file.rpm, verificate che `digests signatures OK` sia presente nell'output.

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, dovresti 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 per te, 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 EC2 istanze Amazon 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 registro da EC2 istanze Amazon e altre fonti. CloudTrail 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.

Per ulteriori informazioni, consulta i seguenti argomenti nella Deadline Cloud Developer Guide:

- CloudTrail log
- Gestione degli eventi utilizzando EventBridge
- Monitoraggio con CloudWatch

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.

Il tuo AWS account ha le seguenti quote relative a. Deadline Cloud

Nome	Predefinita	Adatta e	Descrizione
Membri associati per azienda	Ogni regione supportata: 75	No	Il numero massimo di membri che possono essere associati a ciascuna azienda agricola nella AWS regione corrente.
Membri associati per flotta	Ogni regione supportata: 75	No	Il numero massimo di membri che possono essere associati a ciascuna flotta nella AWS regione corrente.
Membri associati per mansione	Ogni regione supportata: 75	No	Il numero massimo di membri che possono essere associati a

Nome	Predefinita	Adatta e	Descrizione
			ciascun lavoro nella AWS regione corrente.
Membri associati per coda	Ogni regione supportata: 75	No	Il numero massimo di membri che possono essere associati a ciascuna coda nella regione corrente AWS .
Budget per azienda	Ogni regione supportata: 20	Sì	Il numero massimo di budget per azienda agricola nella regione attuale AWS
Aziende agricole per regione	Ogni regione supportata: 2	Sì	Il numero massimo di aziende agricole che è possibile creare nella AWS regione corrente.
Flotte per azienda	Ogni regione supportata: 5	Sì	Il numero massimo di flotte che è possibile creare per ogni azienda agricola nella regione corrente AWS .
Posti di lavoro per azienda	Ogni regione supportata: 100.000	Sì	Il numero massimo di posti di lavoro per azienda agricola nella AWS regione attuale.
Endpoint di licenza per regione	Ogni regione supportata: 5	Sì	Il numero massimo di endpoint di licenza nella regione corrente AWS .

Nome	Predefinita	Adatta e	Descrizione
Sessioni di licenza per endpoint di licenza	Ogni regione supportata: 500	Sì	Il numero massimo di sessioni di licenza per endpoint di licenza nella regione corrente AWS .
Limiti per azienda	Ogni Regione supportata: 50	Sì	Il numero massimo di limiti che è possibile creare per ogni azienda agricola nella AWS regione corrente.
Monitor per regione	Ogni regione supportata: 1	No	Il numero massimo di monitor nella regione corrente AWS .
OnDemand Istanza G GPUs per regione	Ogni regione supportata: 1	Sì	Il numero massimo di istanze G on-demand di GPUs cui è possibile effettuare il provisioning in tutte le flotte gestite dai servizi nella regione corrente. AWS
OnDemand v per regione CPUs	Ogni Regione supportata: 50	Sì	Il numero massimo di v on demand di CPUs cui è possibile effettuare il provisioning in tutte le flotte gestite dai servizi nella regione corrente. AWS

Nome	Predefinita	Adatta e	Descrizione
Ambienti di coda per coda	Ogni regione supportata: 10	No	Il numero massimo di ambienti di coda che è possibile creare per ogni coda nella regione corrente. AWS
Metti in coda le associazioni di flotte per azienda	Ogni regione supportata: 100	Sì	Il numero massimo di associazioni di flotte in coda per azienda agricola nella regione corrente AWS
Associazioni di limiti di coda per coda	Ogni regione supportata: 10	Sì	Il numero massimo di limiti che possono essere associati a ciascuna coda nella regione corrente. AWS
Code per azienda	Ogni regione supportata: 20	Sì	Il numero massimo di code che è possibile creare per ogni azienda agricola nella regione corrente AWS .
Istanza Spot G GPUs per regione	Ogni regione supportata: 1	Sì	Il numero massimo di istanze spot G di GPUs cui è possibile effettuare il provisioning in tutte le flotte gestite dai servizi nella regione corrente. AWS

Nome	Predefinita	Adatta e	Descrizione
Spot v per regione CPUs	Ogni regione supportata: 500	Sì	Il numero massimo di spot v di CPUs cui è possibile effettuare il provisioning in tutte le flotte gestite dai servizi nella regione corrente. AWS
Fasi per lavoro	Ogni Regione supportata: 200	Sì	Il numero massimo di passaggi per processo nella AWS regione corrente.
Archiviazione per volumi SSD a scopo generico (gp3) in TiB	Ogni Regione supportata: 50	Sì	La quantità massima aggregata di storage EBS, misurata in TiB, che può essere utilizzata in tutte le flotte della regione corrente. AWS
Profili di archiviazione per farm	Ogni Regione supportata: 50	No	Il numero massimo di profili di archiviazione che è possibile creare per ogni farm nella AWS regione corrente.
Attività per mansione	Ogni regione supportata: 10.000	Sì	Il numero massimo di attività per mansione nella AWS regione corrente.
Attività per fase	Ogni regione supportata: 10.000	Sì	Il numero massimo di attività per fase nella AWS regione corrente.

Nome	Predefinita	Adatta e	Descrizione
Lavoratori per azienda	Ogni regione supportata: 7.500	No	Il numero massimo di lavoratori per azienda agricola nella regione attuale AWS .

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 API
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Risoluzione dei problemi

Le seguenti procedure e suggerimenti possono aiutarti a risolvere i problemi con le tue farm e risorse AWS Deadline Cloud.

Argomenti

Perché un utente non può vedere la mia fattoria, la mia flotta o la mia coda?

Accesso utente

Se i tuoi utenti non vedono le tue fattorie, le tue flotte o le tue code nel monitor Deadline Cloud, potrebbe esserci un problema con l'accesso alla tua fattoria e alle tue risorse.

Gli utenti che non hanno accesso a nessuna fattoria ricevono il messaggio «Nessuna azienda agricola disponibile» nel monitor Deadline Cloud.

Per confermare di avere assegnato l'utente o il gruppo corretto alla fattoria, alla flotta o alla coda

1. Nella console AWS Deadline Cloud, trova la tua fattoria, flotta o coda, quindi scegli Gestione degli accessi.
2. La scheda dei gruppi è selezionata per impostazione predefinita. Se si assegnano le autorizzazioni per gruppi, operazione consigliata, il gruppo dovrebbe essere visualizzato nell'elenco e avere un livello di accesso assegnato.

   Se il gruppo non è nell'elenco, scegli Aggiungi gruppo per assegnare l'autorizzazione al gruppo.
3. Se stai assegnando le autorizzazioni per utente, seleziona la scheda Utenti. Il tuo utente dovrebbe apparire nell'elenco e avere un livello di accesso assegnato.

Se il tuo utente non è nell'elenco, scegli Aggiungi utente per assegnare l'autorizzazione all'utente.

Per confermare che l'utente è stato assegnato al gruppo

1. Nella console AWS Deadline Cloud, trova la tua fattoria, la tua flotta o la tua coda, quindi scegli Gestione degli accessi.
2. La scheda dei gruppi è selezionata per impostazione predefinita. Seleziona il nome del gruppo per visualizzarne i membri.
3. Se l'utente non è elencato nel gruppo, deve essere aggiunto.

   Se utilizzi la configurazione di identità predefinita, puoi aggiungere direttamente l'utente al gruppo nella console di Identity Center. Se sei connesso a un provider di identità esterno come Okta oppure Google Workspace, puoi aggiungere il tuo utente al gruppo del tuo provider di identità.

   > **Note**
   >
   > Alcuni provider di identità esterni sincronizzano gli utenti ma non i gruppi con Identity Center. In questo caso, valuta la possibilità di assegnare le autorizzazioni a un utente direttamente anziché per gruppo.

Per ulteriori informazioni sulla gestione dell'accesso degli utenti a Deadline Cloud, consulta. Gestione degli utenti in Deadline Cloud

Perché i lavoratori non vengono a ritirare il mio lavoro?

Configurazione dei ruoli della flotta

A volte, quando i lavoratori vengono creati ma non completano l'inizializzazione e non iniziano a lavorare sui lavori, è perché il ruolo della flotta non è stato configurato correttamente.

Per verificare che ciò stia accadendo, controlla CloudTrail i registri per eventuali errori di accesso negato. Dopo aver confermato il problema di accesso negato, accedi alla tua flotta e aggiorna la configurazione dei ruoli con le autorizzazioni corrette. Per ulteriori informazioni, consulta CloudTrailil log nella guida per sviluppatori di Deadline Cloud.

Perché il mio lavoratore è bloccato a correre?

Il lavoratore è bloccato mentre esce dall'ambiente OpenJD

I lavoratori possono rimanere bloccati in sessioni di lunga duratae`envExit`. Ciò potrebbe accadere se si utilizza un modello di lavoro che sostituisce il modello OpenJD e imposta il timeout delle azioni di uscita dall'ambiente su più di 5 minuti. Il monitor Deadline Cloud offre una certa visibilità sui lavoratori bloccati in questa situazione, ma richiede il confronto tra i `RUNNING` lavoratori e il lavoro disponibile nelle code associate.

Per trovare lavoratori bloccati, esamina tutte le flotte del monitor Deadline Cloud e completa i seguenti passaggi:

1. Nella colonna relativa allo stato del lavoratore, trova `RUNNING` i lavoratori.
2. Dalla sezione Dettagli della flotta, accedi a ciascuna coda associata.
3. In ogni coda associata, cerca i lavori che sono `RUNNINGREADY`, o. `PENDING` Se in tutte le code associate non è presente alcun lavoro in tali stati, il lavoratore sta eseguendo un'uscita dall'ambiente.

Per fermare un lavoratore bloccato in questo stato, utilizzate il seguente AWS CLI comando:

```
aws deadline update-worker \
    --farm-id $FARM_ID     \
    --fleet-id $FLEET_ID   \
    --worker-id $WORKER_ID \
    --status STOPPED
```

Dopo aver eseguito il comando, l'agente di lavoro si riavvia all'uscita del programma. I lavoratori tornano quindi online ed eseguono altri lavori dalle code associate. Se la coda contiene più lavori con tempi di uscita dall'ambiente superiori a 5 minuti, il lavoratore rimarrà nuovamente bloccato. In tal caso, sarà necessario ripetere la procedura fino a quando non ci saranno più lavoratori bloccati all'uscita.

Per evitare questo problema, impostate l'opzione di timeout su non più di 5 minuti quando utilizzate un modello di 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.

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 Determinare la compatibilità del parco veicoli. Per visualizzare la configurazione del parco veicoli, consultaVisualizza 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 Creare un'infrastruttura per il parco veicoli con un gruppo Amazon EC2 Auto Scaling nella Deadline Cloud Developer Guide.

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, consultare Visualizza i registri delle sessioni e dei lavoratori 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 flotte gestite dai clienti a un endpoint di licenza nella Deadline Cloud Developer Guide.
- Il messaggio relativo all'azione dell'ultima sessione o il codice di uscita del processo possono fornire informazioni sul motivo per cui il processo non è riuscito. Se stai usando Windows e il tuo codice di uscita è negativo, prova a cercare la versione non firmata del codice di uscita:

```
2,147,483,647 - |your exit code|
```

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, consultare Visualizza una fase in Deadline Cloud.

Risorse aggiuntive

Puoi trovare ulteriori informazioni e risorse su. GitHub

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
AWS Aggiornamento della policy gestita	Politica AWS AWSDeadlineCloud-WorkerHostgestita esistente aggiornata. Per ulteriori informazioni, consulta le politiche AWS gestite per Deadline Cloud.	30 maggio 2025
Programma di installazione di Adobe After Effects Submitter	Sono state aggiunte istruzioni per aggiungere il programma di installazione di Adobe After Effects Submitter al software per la creazione di contenuti digitali. Per ulteriori informazioni, vedete Adobe After Effects.	13 febbraio 2025
Risoluzione dei problemi	Sono state aggiunte informazioni per la risoluzione dei problemi di Deadline Cloud. Per ulteriori informazioni, consulta Risoluzione dei problemi.	7 febbraio 2025
Limiti delle risorse Job	È stata aggiunta la documentazione relativa al nuovo limite di risorse lavorative e al numero massimo di host di lavoratori. Per ulteriori informazioni,	30 gennaio 2025

	consulta Creare limiti di risorse per i lavori.	
Adobe After Effects UBL	Sono state aggiunte informazioni sulle licenze basate sull'utilizzo di Adobe After Effects (UBL) per Deadline Cloud. Per ulteriori informazioni, consulta Connect to a license endpoint.	30 gennaio 2025
Contenuto riorganizzato della guida per l'utente	I contenuti dedicati agli sviluppatori sono stati spostati dalla guida per l'utente alla guida per sviluppatori: • Le istruzioni per la creazione di una flotta gestita dal cliente sono state spostate in un nuovo capitolo sulle flotte gestite dai clienti nella guida per gli sviluppatori. • Le informazioni sull'utilizzo delle proprie licenze sono state spostate nel nuovo capitolo Utilizzo delle licenze software della guida per gli sviluppatori. • Sono stati spostati i dettagli sul monitoraggio con CloudTrail e nel capitolo Monitoraggio della guida EventBridge per gli sviluppatori. CloudWatch	6 gennaio 2025

Evento sulla soglia di budget	Aggiunto un nuovo EventBridge evento relativo alla soglia di budget. Per ulteriori informazioni, consulta il riferimento dettagliato agli eventi di Deadline Cloud.	30 ottobre 2024
Eventi Job status	Aggiunti nuovi EventBridge eventi sullo stato del lavoro e dell'attività. Per ulteriori informazioni, consulta il riferimento dettagliato agli eventi di Deadline Cloud.	24 ottobre 2024
Invia nuovamente il lavoro	Sono state aggiunte informazioni su come inviare nuovamente un'offerta di lavoro. Per ulteriori informazioni, consulta Reinvia un lavoro.	7 ottobre 2024
AWS Aggiornamenti gestiti delle politiche	Politiche AWS gestite esistenti aggiornate. Per ulteriori informazioni, consulta le politiche AWS gestite per Deadline Cloud.	7 ottobre 2024
Porta la tua licenza	Sono state aggiunte informazioni su come utilizzare il proprio server di licenza o l'istanza proxy di licenza con Deadline Cloud. Per ulteriori informazioni, consulta Flotte gestite dai servizi.	26 luglio 2024

Autodesk 3ds Max UBL	Sono state aggiunte informazioni sulle licenze basate sull'utilizzo (UBL) di Autodesk 3ds Max per Deadline Cloud. Per ulteriori informazioni, consulta Connect to a license endpoint.	18 giugno 2024
Funzionalità di monitoraggio e gestione dei costi	Puoi utilizzarle EventBridge per supportare il monitoraggio in Deadline Cloud. Per ulteriori informazioni, consulta Agire sugli EventBridge eventi. Deadline Cloud fornisce i budget e lo strumento di esplorazione dell'utilizzo per aiutarti a controllare e visualizzare i costi dei tuoi lavori. Scopri alcune best practice per aiutarti a gestire questi costi. Per ulteriori informazioni, consulta Gestione dei costi.	23 maggio 2024
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.