Panduan Pengguna

AWS Batas Waktu Cloud

Versi latest

AWS Batas Waktu Cloud: Panduan Pengguna

Table of Contents

Apa itu AWS Deadline Cloud?

Deadline Cloud Layanan AWS dapat digunakan untuk membuat dan mengelola proyek dan pekerjaan rendering di instans Amazon Elastic Compute Cloud (Amazon EC2) langsung dari pipeline pembuatan konten digital dan workstation.

Deadline Cloud menyediakan antarmuka konsol, aplikasi lokal, alat baris perintah, dan API. Dengan Deadline Cloud, Anda dapat membuat, mengelola, dan memantau peternakan, armada, pekerjaan, grup pengguna, dan penyimpanan. Anda juga dapat menentukan kemampuan perangkat keras, membuat lingkungan untuk beban kerja tertentu, dan mengintegrasikan alat pembuatan konten yang diperlukan produksi Anda ke dalam pipeline Deadline Cloud Anda.

Deadline Cloud menyediakan antarmuka terpadu untuk mengelola semua proyek rendering Anda di satu tempat. Anda dapat mengelola pengguna, menetapkan proyek kepada mereka, dan memberikan izin untuk peran pekerjaan.

Topik

Fitur Deadline Cloud

Berikut adalah beberapa cara utama Deadline Cloud dapat membantu Anda menjalankan dan mengelola beban kerja komputasi visual:

- Buat peternakan, antrian, dan armada Anda dengan cepat. Pantau status mereka, dan dapatkan wawasan tentang pengoperasian pertanian dan pekerjaan Anda.
- Kelola pengguna dan grup Deadline Cloud secara terpusat, dan tetapkan izin.
- Kelola keamanan masuk untuk pengguna proyek dan penyedia identitas eksternal dengan AWS IAM Identity Center.

- Mengelola akses ke sumber daya proyek dengan aman AWS Identity and Access Management (IAM) kebijakan dan peran.
- Gunakan tag untuk mengatur dan menemukan sumber daya proyek dengan cepat.
- Kelola penggunaan sumber daya proyek dan perkiraan biaya untuk proyek Anda.
- Menyediakan berbagai pilihan manajemen komputasi untuk mendukung rendering di cloud atau secara langsung.

Konsep dan terminologi untuk Deadline Cloud

Untuk membantu Anda memulai dengan AWS Deadline Cloud, topik ini menjelaskan beberapa konsep dan terminologi utamanya.

Manajer anggaran

: Manajer anggaran adalah bagian dari monitor Deadline Cloud. Gunakan manajer anggaran untuk membuat dan mengelola anggaran. Anda juga dapat menggunakannya untuk membatasi aktivitas agar tetap sesuai anggaran.

Pustaka Klien Cloud Batas Waktu

: Pustaka Klien menyertakan antarmuka baris perintah dan pustaka untuk mengelola Deadline Cloud. Fungsionalitas termasuk mengirimkan bundel pekerjaan berdasarkan spesifikasi Open Job Description ke Deadline Cloud, mengunduh output lampiran pekerjaan, dan memantau pertanian Anda menggunakan antarmuka baris perintah.

Aplikasi pembuatan konten digital (DCC)

: Aplikasi pembuatan konten digital (DCCs) adalah produk pihak ketiga tempat Anda membuat konten digital. Contohnya DCCs adalah Maya, Nuke, dan Houdini. Deadline Cloud menyediakan plugin terintegrasi pengirim pekerjaan untuk spesifik. DCCs

Peternakan

: Peternakan adalah tempat sumber daya proyek Anda berada. Ini terdiri dari antrian dan armada.

Armada

: Armada adalah sekelompok node pekerja yang melakukan rendering. Node pekerja memproses pekerjaan. Armada dapat dikaitkan dengan beberapa antrian, dan antrian dapat dikaitkan dengan beberapa armada.

Pekerjaan

Pekerjaan adalah permintaan rendering. Pengguna mengirimkan pekerjaan. Pekerjaan berisi properti pekerjaan tertentu yang diuraikan sebagai langkah dan tugas.

Lampiran Job

Lampiran pekerjaan adalah fitur Deadline Cloud yang dapat Anda gunakan untuk mengelola input dan output untuk pekerjaan. File Job diunggah sebagai lampiran pekerjaan selama proses rendering. File-file ini dapat berupa tekstur, model 3D, rig pencahayaan, dan item serupa lainnya.

Prioritas Job

Prioritas Job adalah perkiraan urutan Deadline Cloud memproses pekerjaan dalam antrian. Anda dapat menetapkan prioritas pekerjaan antara 1 dan 100, pekerjaan dengan prioritas angka yang lebih tinggi umumnya diproses terlebih dahulu. Pekerjaan dengan prioritas yang sama diproses dalam urutan yang diterima.

Properti Job

Properti Job adalah pengaturan yang Anda tentukan saat mengirimkan pekerjaan render. Beberapa contoh termasuk rentang bingkai, jalur keluaran, lampiran pekerjaan, kamera yang dapat dirender, dan banyak lagi. Properti bervariasi berdasarkan DCC tempat render dikirimkan.

Templat Job

Template pekerjaan mendefinisikan lingkungan runtime dan semua proses yang berjalan sebagai bagian dari pekerjaan Deadline Cloud.

Antrean

Antrian adalah tempat pekerjaan yang diajukan berada dan dijadwalkan akan diberikan. Antrian harus dikaitkan dengan armada untuk membuat render yang berhasil. Antrian dapat dikaitkan dengan beberapa armada.

Asosiasi antrian armada

Ketika antrian dikaitkan dengan armada, ada asosiasi antrian-armada. Gunakan asosiasi untuk menjadwalkan pekerja dari armada ke pekerjaan dalam antrian itu. Anda dapat memulai dan menghentikan asosiasi untuk mengontrol penjadwalan kerja.

Sesi

Sesi adalah lingkungan runtime sementara pada host pekerja yang dibuat untuk menjalankan serangkaian tugas dari pekerjaan yang sama. Sesi berakhir ketika host pekerja selesai menjalankan tugas untuk pekerjaan itu.

Sesi ini menyediakan cara untuk mengonfigurasi lingkungan dengan sumber daya yang dibagikan di beberapa tugas yang dijalankan, seperti mendefinisikan variabel lingkungan atau memulai proses latar belakang atau wadah.

Tindakan sesi

Tindakan sesi adalah unit kerja diskrit yang dijalankan oleh pekerja dalam suatu sesi. Ini dapat mencakup operasi tugas inti dari suatu tugas, atau mungkin termasuk langkah-langkah persiapan seperti pengaturan lingkungan dan proses pasca-eksekusi seperti pembongkaran dan pembersihan.

Langkah

Langkah adalah salah satu proses khusus untuk dijalankan dalam pekerjaan.

Batas waktu pengirim Cloud

Submitter Deadline Cloud adalah plugin pembuatan konten digital (DCC). Artis menggunakannya untuk mengirimkan pekerjaan dari antarmuka DCC pihak ketiga yang mereka kenal.

Tanda

Tag adalah label yang dapat Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional yang Anda tentukan.

Dengan tag, Anda dapat mengkategorikan AWS sumber daya Anda dengan berbagai cara. Misalnya, Anda dapat menentukan satu set tag untuk EC2 instans Amazon akun Anda yang membantu Anda melacak setiap pemilik instans dan tingkat tumpukan.

Anda juga dapat mengkategorikan AWS sumber daya Anda berdasarkan tujuan, pemilik, atau lingkungan. Pendekatan ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama. Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan padanya.

Tugas

Tugas adalah komponen tunggal dari langkah render.

Lisensi berbasis penggunaan (UBL)

Usage-based licensing (UBL) adalah model lisensi on-demand yang tersedia untuk produk pihak ketiga tertentu. Model ini dibayar sesuai keinginan Anda, dan Anda dikenakan biaya untuk jumlah jam dan menit yang Anda gunakan.

Penjelajah penggunaan

Penjelajah penggunaan adalah fitur monitor Deadline Cloud. Ini memberikan perkiraan perkiraan biaya dan penggunaan Anda.

Pekerja

Pekerja termasuk dalam armada dan menjalankan tugas yang diberikan Deadline Cloud untuk menyelesaikan langkah dan pekerjaan. Pekerja menyimpan log dari operasi tugas di Amazon CloudWatch Logs. Pekerja juga dapat menggunakan fitur lampiran pekerjaan untuk menyinkronkan input dan output ke bucket Amazon Simple Storage Service (Amazon S3).

Memulai dengan Deadline Cloud

Gunakan Deadline Cloud untuk membuat farm render dengan cepat dengan setelan dan sumber daya default, seperti konfigurasi EC2 instans Amazon dan bucket Amazon Simple Storage Service (Amazon S3).

Anda juga dapat menentukan pengaturan dan sumber daya saat membuat render farm. Metode ini membutuhkan lebih banyak waktu daripada menggunakan pengaturan dan sumber daya default tetapi memberi Anda lebih banyak kontrol.

Setelah Anda terbiasa dengan Deadline Cloud Concepts dan terminologi, lihat Memulai step-by-step petunjuk untuk membuat farm Anda, menambahkan pengguna, dan link ke informasi bermanfaat.

Mengakses Deadline Cloud

Anda dapat mengakses Deadline Cloud dengan salah satu cara berikut:

- Konsol Cloud Deadline — Akses konsol di browser untuk membuat pertanian dan sumber dayanya, dan mengelola akses pengguna. Untuk informasi selengkapnya, lihat Memulai.
- Monitor Cloud Deadline — Kelola pekerjaan render Anda, termasuk memperbarui prioritas dan status pekerjaan. Pantau pertanian Anda dan lihat log dan status pekerjaan. Untuk pengguna dengan izin Pemilik, monitor Deadline Cloud juga menyediakan akses untuk mengeksplorasi penggunaan dan membuat anggaran. Monitor Deadline Cloud tersedia sebagai browser web dan aplikasi desktop.
- AWS SDK dan AWS CLI — Gunakan AWS Command Line Interface (AWS CLI) untuk memanggil operasi Deadline Cloud API dari baris perintah pada sistem lokal Anda. Untuk informasi selengkapnya, lihat Menyiapkan stasiun kerja pengembang.

Layanan terkait

Deadline Cloud bekerja dengan yang berikut: Layanan AWS

- Amazon CloudWatch — Dengan CloudWatch, Anda dapat memantau proyek dan AWS sumber daya terkait. Untuk informasi selengkapnya, lihat Memantau dengan CloudWatch di Panduan Pengembang Cloud Deadline.
- Amazon EC2 — Ini Layanan AWS menyediakan server virtual yang menjalankan aplikasi Anda di cloud. Anda dapat mengonfigurasi proyek untuk menggunakan EC2 instans Amazon untuk beban kerja Anda. Untuk informasi selengkapnya, lihat EC2 instans Amazon.
- EC2 Auto Scaling Amazon — Dengan Auto Scaling, Anda dapat secara otomatis menambah atau mengurangi jumlah instans saat permintaan instans Anda berubah. Auto Scaling membantu memastikan bahwa Anda menjalankan jumlah instans yang diinginkan, meskipun instans gagal. Jika Anda mengaktifkan Auto Scaling dengan Deadline Cloud, instance yang diluncurkan oleh Auto Scaling secara otomatis terdaftar dengan beban kerja. Demikian juga, instance yang dihentikan oleh Auto Scaling secara otomatis tidak terdaftar dari beban kerja. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2 Auto Scaling.
- AWS PrivateLink— AWS PrivateLink menyediakan konektivitas pribadi antara virtual private cloud (VPCs), Layanan AWS, dan jaringan lokal Anda, tanpa mengekspos lalu lintas Anda ke internet publik. AWS PrivateLink membuatnya mudah untuk menghubungkan layanan di berbagai akun dan VPCs. Untuk informasi selengkapnya, lihat AWS PrivateLink.
- Amazon S3 - Amazon S3 adalah layanan penyimpanan objek. Deadline Cloud menggunakan bucket Amazon S3 untuk menyimpan lampiran pekerjaan. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon S3.
- IAM Identity Center - IAM Identity Center adalah Layanan AWS tempat Anda dapat memberi pengguna akses masuk tunggal ke semua akun dan aplikasi yang ditugaskan dari satu tempat. Anda juga dapat mengelola akses multi-akun dan izin pengguna secara terpusat ke semua akun Anda. AWS Organizations Untuk informasi selengkapnya, lihat AWS IAM Identity Center FAQs.

Bagaimana Deadline Cloud bekerja

Dengan Deadline Cloud, Anda dapat membuat dan mengelola proyek dan pekerjaan rendering langsung dari pipeline dan workstation pembuatan konten digital (DCC).

Anda mengirimkan lowongan ke Deadline Cloud menggunakan pengirim pekerjaan AWS SDK, AWS Command Line Interface (AWS CLI), atau Deadline Cloud. Deadline Cloud mendukung Open Job

Description (OpenJD) untuk spesifikasi template pekerjaan. Untuk informasi selengkapnya, lihat Open Job Description di GitHub situs web.

Deadline Cloud menyediakan pengirim pekerjaan. Pengirim pekerjaan adalah plugin DCC untuk mengirimkan pekerjaan render dari antarmuka DCC pihak ketiga, seperti Maya atau Nuke. Dengan submitter, artis dapat mengirimkan pekerjaan rendering dari antarmuka pihak ketiga ke Deadline Cloud di mana sumber daya proyek dikelola dan pekerjaan dipantau, semuanya di satu lokasi.

Dengan Deadline Cloud farm, Anda dapat membuat antrian dan armada, mengelola pengguna, dan mengelola penggunaan dan biaya sumber daya proyek. Sebuah peternakan terdiri dari antrian dan armada. Antrian adalah tempat pekerjaan yang diajukan berada dan dijadwalkan akan diberikan. Armada adalah sekelompok node pekerja yang menjalankan tugas untuk menyelesaikan pekerjaan. Antrian harus dikaitkan dengan armada sehingga pekerjaan dapat dibuat. Sebuah armada tunggal dapat mendukung beberapa antrian dan antrian dapat didukung oleh beberapa armada.

Pekerjaan terdiri dari langkah-langkah, dan setiap langkah terdiri dari tugas-tugas tertentu. Dengan monitor Deadline Cloud, Anda dapat mengakses status, log, dan metrik pemecahan masalah lainnya untuk pekerjaan, langkah, dan tugas.

Izin di Deadline Cloud

Deadline Cloud mendukung hal-hal berikut:

- Mengelola akses ke operasi API-nya menggunakan AWS Identity and Access Management (IAM)
- Mengelola akses pengguna tenaga kerja menggunakan integrasi dengan AWS IAM Identity Center

Sebelum ada yang dapat mengerjakan proyek, mereka harus memiliki akses ke proyek itu dan pertanian terkait. Deadline Cloud terintegrasi dengan IAM Identity Center untuk mengelola otentikasi dan otorisasi tenaga kerja. Pengguna dapat ditambahkan langsung ke IAM Identity Center, atau izin dapat dihubungkan ke penyedia identitas (IDP) Anda yang sudah ada seperti Okta atau Active Directory. Administrator TI dapat memberikan izin akses kepada pengguna dan grup pada tingkat yang berbeda. Setiap level berikutnya mencakup izin untuk level sebelumnya. Daftar berikut menjelaskan empat tingkat akses dari tingkat terendah ke tingkat tertinggi:

- Penampil — Izin untuk melihat sumber daya di peternakan, antrian, armada, dan pekerjaan yang dapat mereka akses. Penampil tidak dapat mengirimkan atau membuat perubahan pada pekerjaan.

- Kontributor — Sama seperti pemirsa, tetapi dengan izin untuk mengirimkan pekerjaan ke antrian atau peternakan.
- Manajer — Sama seperti kontributor, tetapi dengan izin untuk mengedit pekerjaan dalam antrian yang dapat mereka akses, dan memberikan izin pada sumber daya yang dapat mereka akses.
- Pemilik — Sama seperti manajer, tetapi dapat melihat dan membuat anggaran dan melihat penggunaan.

> **Note**
>
> Izin ini tidak memberi pengguna akses ke AWS Management Console atau izin untuk mengubah infrastruktur Deadline Cloud.

Pengguna harus memiliki akses ke peternakan sebelum mereka dapat mengakses antrian dan armada terkait. Akses pengguna ditetapkan ke antrian dan armada secara terpisah di dalam peternakan.

Anda dapat menambahkan pengguna sebagai individu atau sebagai bagian dari grup. Menambahkan grup ke peternakan, armada, atau antrian dapat mempermudah pengelolaan izin akses untuk sekelompok besar orang. Misalnya, jika Anda memiliki tim yang mengerjakan proyek tertentu, Anda dapat menambahkan setiap anggota tim ke grup. Kemudian, Anda dapat memberikan izin akses ke seluruh grup untuk pertanian, armada, atau antrian yang sesuai.

Dukungan perangkat lunak dengan Deadline Cloud

Deadline Cloud bekerja dengan aplikasi perangkat lunak apa pun yang dapat dijalankan dari antarmuka baris perintah dan dikendalikan dengan menggunakan nilai parameter. Deadline Cloud mendukung OpenJD spesifikasi untuk menggambarkan pekerjaan sebagai pekerjaan dengan langkah-langkah skrip perangkat lunak yang diparameterisasi (seperti melintasi rentang bingkai) ke dalam tugas. Merakit OpenJD instruksi pekerjaan ke dalam bundel pekerjaan dengan alat dan fitur Deadline Cloud untuk membuat, menjalankan, dan melisensikan langkah-langkah dari aplikasi perangkat lunak pihak ketiga.

Pekerjaan membutuhkan lisensi untuk dirender. Deadline Cloud menawarkan usage-based-licensing (UBL) untuk pilihan lisensi aplikasi perangkat lunak yang ditagih per jam per menit berdasarkan penggunaan. Dengan Deadline Cloud, Anda juga dapat menggunakan lisensi perangkat lunak Anda

sendiri jika Anda mau. Jika suatu pekerjaan tidak dapat mengakses lisensi, itu tidak akan dirender dan menghasilkan kesalahan yang ditampilkan di log tugas di monitor Deadline Cloud.

Memulai dengan Deadline Cloud

Untuk membuat farm di AWS Deadline Cloud, Anda dapat menggunakan konsol Deadline Cloud atau AWS Command Line Interface ()AWS CLI. Gunakan konsol untuk pengalaman terpandu menciptakan pertanian, termasuk antrian dan armada. Gunakan AWS CLI untuk bekerja secara langsung dengan layanan, atau untuk mengembangkan alat Anda sendiri yang bekerja dengan Deadline Cloud.

Untuk membuat farm dan menggunakan monitor Deadline Cloud, siapkan akun Anda untuk Deadline Cloud. Anda hanya perlu menyiapkan infrastruktur monitor Deadline Cloud sekali per akun. Dari peternakan Anda, Anda dapat mengelola proyek Anda, termasuk akses pengguna ke pertanian Anda dan sumber dayanya.

Untuk membuat farm tanpa menyiapkan infrastruktur monitor Deadline Cloud, siapkan workstation pengembang untuk Deadline Cloud.

Untuk membuat peternakan dengan sumber daya minimal untuk menerima pekerjaan, pilih Mulai cepat di halaman beranda konsol. Siapkan monitor Cloud Deadlinememandu Anda melalui langkah-langkah itu. Peternakan ini dimulai dengan antrian dan armada yang secara otomatis terkait. Pendekatan ini adalah cara mudah untuk membuat peternakan gaya kotak pasir untuk bereksperimen.

Topik

- Siapkan Akun AWS
- Siapkan monitor Cloud Deadline
- Mengatur Deadline Pengirim Cloud

Siapkan Akun AWS

Siapkan Akun AWS untuk menggunakan AWS Deadline Cloud.

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun.

> **Important**
>
> Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Siapkan monitor Cloud Deadline

Untuk memulai, Anda harus membuat infrastruktur monitor Deadline Cloud dan menentukan pertanian Anda. Anda juga dapat melakukan langkah-langkah opsional tambahan termasuk menambahkan grup dan pengguna, memilih peran layanan, dan menambahkan tag ke sumber daya Anda.

Langkah 1: Buat monitor Anda

Monitor Deadline Cloud digunakan AWS IAM Identity Center untuk mengotorisasi pengguna. Instance IAM Identity Center yang Anda gunakan untuk Deadline Cloud harus Wilayah AWS sama dengan monitor. Jika konsol Anda menggunakan Wilayah yang berbeda saat membuat monitor, Anda akan mendapatkan pengingat untuk mengubah ke Wilayah Pusat Identitas IAM.

Infrastruktur monitor Anda terdiri dari komponen-komponen berikut:

- Nama monitor: Nama Monitor adalah bagaimana Anda dapat mengidentifikasi monitor Anda - misalnya AnyCompany monitor. Nama monitor Anda juga menentukan URL monitor Anda.
- URL Monitor: Anda dapat mengakses monitor Anda dengan menggunakan URL Monitor. URL didasarkan pada nama Monitor — misalnya https://anycompanymonitor.awsapps.com.
- Wilayah AWS: Wilayah AWSIni adalah lokasi fisik untuk pengumpulan pusat AWS data. Ketika Anda mengatur monitor Anda, Region default ke lokasi terdekat dengan Anda. Kami merekomendasikan untuk mengubah Wilayah sehingga letaknya paling dekat dengan pengguna Anda. Ini mengurangi lag dan meningkatkan kecepatan transfer data. AWS IAM Identity Center harus diaktifkan sama Wilayah AWS dengan Deadline Cloud.

> **Important**
>
> Anda tidak dapat mengubah Wilayah setelah selesai menyiapkan Deadline Cloud.

Selesaikan tugas di bagian ini untuk mengonfigurasi infrastruktur monitor Anda.

Untuk mengkonfigurasi infrastruktur monitor

1. Masuk ke AWS Management Consoleuntuk memulai penyiapan Welcome to Deadline Cloud, lalu pilih Berikutnya.
2. Masukkan nama Monitor — misalnya**`AnyCompany Monitor`**.
3. (Opsional) Untuk mengubah URL Monitor, pilih Edit URL.
4. (Opsional) Untuk mengubah Wilayah AWSagar paling dekat dengan pengguna Anda, pilih Ubah Wilayah.
   a. Pilih Wilayah yang paling dekat dengan pengguna Anda.
   b. Pilih Terapkan Wilayah.
5. (Opsional) Untuk lebih menyesuaikan pengaturan monitor Anda, pilih Pengaturan tambahan.
6. Jika Anda siapLangkah 2: Tentukan detail pertanian, pilih Berikutnya.

Pengaturan tambahan

Deadline Cloud setup mencakup pengaturan tambahan. Dengan pengaturan ini, Anda dapat melihat semua perubahan yang dilakukan Deadline Cloud setup untuk Anda Akun AWS, mengonfigurasi peran pengguna monitor Anda, dan mengubah jenis kunci enkripsi Anda.

AWS IAM Identity Center

AWS IAM Identity Center adalah layanan masuk tunggal berbasis cloud untuk mengelola pengguna dan grup. Pusat Identitas IAM juga dapat diintegrasikan dengan penyedia sistem masuk tunggal (SSO) perusahaan Anda sehingga pengguna dapat masuk dengan akun perusahaan mereka.

Deadline Cloud mengaktifkan IAM Identity Center secara default, dan diperlukan untuk mengatur dan menggunakan Deadline Cloud. Instance IAM Identity Center yang Anda gunakan untuk Deadline Cloud harus Wilayah AWS sama dengan monitor. Untuk informasi lebih lanjut, lihat Apa itu AWS IAM Identity Center.

Konfigurasikan peran akses layanan

AWS Layanan dapat mengambil peran layanan untuk melakukan tindakan atas nama Anda. Deadline Cloud memerlukan peran pengguna monitor agar dapat memberi pengguna akses ke sumber daya di monitor Anda.

Anda dapat melampirkan kebijakan terkelola AWS Identity and Access Management (IAM) ke peran pengguna monitor. Kebijakan tersebut memberi pengguna izin untuk melakukan tindakan tertentu, seperti membuat pekerjaan di aplikasi Deadline Cloud tertentu. Karena aplikasi bergantung pada kondisi tertentu dalam kebijakan terkelola, jika Anda tidak menggunakan kebijakan terkelola, aplikasi mungkin tidak berfungsi seperti yang diharapkan.

Anda dapat mengubah peran pengguna monitor setelah Anda menyelesaikan penyiapan, kapan saja. Untuk informasi selengkapnya tentang peran pengguna, lihat Peran IAM.

Tab berikut berisi instruksi untuk dua kasus penggunaan yang berbeda. Untuk membuat dan menggunakan peran layanan baru, pilih tab Peran layanan baru. Untuk menggunakan peran layanan yang ada, pilih tab Peran layanan yang ada.

New service role

Untuk membuat dan menggunakan peran layanan baru

1. Pilih Buat dan gunakan peran layanan baru.
2. (Opsional) Masukkan nama peran pengguna Layanan.
3. Pilih Lihat detail izin untuk informasi selengkapnya tentang peran tersebut.

Existing service role

Untuk menggunakan peran layanan yang ada

1. Pilih Gunakan peran layanan yang ada.
2. Buka daftar dropdown untuk memilih peran layanan yang ada.
3. (Opsional) Pilih Lihat di konsol IAM untuk informasi selengkapnya tentang peran tersebut.

Langkah 2: Tentukan detail pertanian

Kembali ke konsol Deadline Cloud, selesaikan langkah-langkah berikut untuk menentukan detail pertanian.

1. Di detail Pertanian, tambahkan Nama untuk pertanian.
2. Untuk Deskripsi, masukkan deskripsi pertanian. Deskripsi dapat membantu Anda mengidentifikasi tujuan pertanian Anda.
3. Buat grup dan tambahkan kegunaan untuk peternakan Anda. Setelah menyiapkan farm, Anda dapat menggunakan konsol manajemen Deadline Cloud untuk menambah atau mengubah grup dan pengguna.
4. (Opsional) Pilih Pengaturan pertanian tambahan.

    a. (Opsional) Secara default, data Anda dienkripsi dengan kunci yang AWS memiliki dan mengelola keamanan Anda. Anda dapat memilih Sesuaikan pengaturan enkripsi (lanjutan) untuk menggunakan kunci yang ada atau untuk membuat kunci baru yang Anda kelola.

    Jika Anda memilih untuk menyesuaikan pengaturan enkripsi menggunakan kotak centang, masukkan AWS KMS ARN, atau buat yang AWS KMS baru dengan memilih Buat kunci KMS baru.

    b. (Opsional) Pilih Tambahkan tag baru untuk menambahkan satu atau beberapa tag ke peternakan Anda.
5. Pilih salah satu opsi berikut:

    - Pilih Lewati untuk Meninjau dan Buat untuk meninjau dan membuat peternakan Anda.
    - Pilih Berikutnya untuk melanjutkan ke langkah-langkah tambahan dan opsional.

(Opsional) Langkah 3: Tentukan detail antrian

Antrian bertanggung jawab untuk melacak kemajuan dan penjadwalan pekerjaan untuk pekerjaan Anda.

1. Mulai dari detail Antrian, berikan Nama untuk antrian.
2. Untuk Deskripsi, masukkan deskripsi antrian. Deskripsi yang jelas dapat membantu Anda mengidentifikasi tujuan antrian dengan cepat.
3. Untuk lampiran Job, Anda dapat membuat bucket Amazon S3 baru atau memilih bucket Amazon S3 yang sudah ada. Jika Anda tidak memiliki bucket Amazon S3 yang ada, Anda harus membuatnya.

    a. Untuk membuat bucket Amazon S3 baru, pilih Buat bucket pekerjaan baru. Anda dapat menentukan nama bucket pekerjaan di bidang awalan Root. Kami merekomendasikan memanggil ember**`deadlinecloud-job-attachments-[MONITORNAME]`**.

    Anda hanya dapat menggunakan huruf kecil dan tanda hubung. Tidak ada spasi atau karakter khusus.

    b. Untuk mencari dan memilih bucket Amazon S3 yang ada, pilih Pilih dari bucket Amazon S3 yang ada. Kemudian, cari bucket yang ada dengan memilih Browse S3. Saat daftar bucket Amazon S3 yang tersedia ditampilkan, pilih bucket Amazon S3 yang ingin Anda gunakan untuk antrian Anda.
4. (Opsional) Pilih Pengaturan pertanian tambahan.

    a. Jika Anda menggunakan armada yang dikelola pelanggan, pilih Aktifkan asosiasi dengan armada yang dikelola pelanggan.

        i. Untuk armada yang dikelola pelanggan, tambahkan pengguna yang dikonfigurasi antrian, lalu atur kredensialnya POSIX dan/atau Windows. Atau, Anda dapat melewati fungsionalitas run-as dengan memilih kotak centang.

        ii. Jika Anda ingin menetapkan anggaran untuk antrian, pilih Memerlukan anggaran untuk antrian ini. Jika Anda memerlukan anggaran, Anda harus membuat anggaran menggunakan konsol Deadline Cloud untuk menjadwalkan pekerjaan dalam antrian.

    b. Antrian Anda memerlukan izin untuk mengakses Amazon S3 atas nama Anda. Kami menyarankan Anda membuat peran layanan baru untuk setiap antrian.

        i. Untuk peran baru, selesaikan langkah-langkah berikut.

A. Pilih Buat dan gunakan peran layanan baru.

B. Masukkan nama Peran untuk peran antrian Anda atau gunakan nama peran yang disediakan.

C. (Opsional) Tambahkan peran antrian Deskripsi.

D. Anda dapat melihat izin IAM untuk peran antrian dengan memilih Lihat detail izin.

ii. Atau, Anda dapat memilih peran layanan yang ada.

c. (Opsional) Tambahkan variabel lingkungan untuk lingkungan antrian menggunakan nama dan pasangan nilai.

d. (Opsional) Tambahkan tag untuk antrian menggunakan pasangan kunci dan nilai.

Pilih salah satu opsi berikut:

- Pilih Lewati untuk Meninjau dan Buat untuk meninjau dan membuat peternakan Anda.
- Pilih Berikutnya untuk melanjutkan ke langkah-langkah tambahan dan opsional.

(Opsional) Langkah 4: Tentukan detail armada

Armada mengalokasikan pekerja untuk melaksanakan tugas rendering Anda. Jika Anda membutuhkan armada untuk tugas rendering Anda, centang kotak untuk Buat armada.

1. Rincian armada

   a. Berikan Nama dan Deskripsi opsional untuk armada Anda.

   b. Tinjau jenis armada dan sistem operasi untuk kesadaran.

2. Di bagian Jenis pasar Instans, pilih Instans Spot atau Instans Sesuai Permintaan. Instans Amazon EC2 On-Demand menyediakan ketersediaan yang lebih cepat dan instans Amazon EC2 Spot lebih baik untuk upaya penghematan biaya.
3. Untuk Penskalaan otomatis jumlah instans dalam armada Anda, pilih jumlah Instans Minimum dan Jumlah instans Maksimum.

   Kami sangat menyarankan untuk selalu menetapkan jumlah minimum instans **`0`** untuk menghindari biaya tambahan.
4. Tinjau kemampuan pekerja untuk kesadaran.
5. (opsional) Pilih Pengaturan armada tambahan

a. Armada Anda memerlukan izin untuk CloudWatch menulis atas nama Anda. Kami menyarankan Anda membuat peran layanan baru untuk setiap armada.

   i. Untuk peran baru, selesaikan langkah-langkah berikut.

      A. Pilih Buat dan gunakan peran layanan baru.

      B. Masukkan nama Peran untuk peran armada Anda atau gunakan nama peran yang disediakan.

      C. (Opsional) Tambahkan peran armada Deskripsi.

      D. Untuk melihat izin IAM untuk peran armada, pilih Lihat detail izin.

   ii. Atau, Anda dapat menggunakan peran layanan yang ada.

b. (Opsional) Tambahkan tag untuk armada menggunakan pasangan kunci dan nilai.

Setelah Anda memasukkan semua detail armada, pilih Berikutnya.

Langkah 5: Tinjau dan buat

Tinjau informasi yang dimasukkan untuk membuat peternakan Anda. Saat Anda siap, pilih Buat peternakan.

Kemajuan pembuatan peternakan Anda ditampilkan di halaman Peternakan. Pesan sukses ditampilkan saat peternakan Anda siap digunakan.

Mengatur Deadline Pengirim Cloud

Proses ini untuk administrator dan artis yang ingin menginstal, menyiapkan, dan meluncurkan submitter AWS Deadline Cloud. Submitter Deadline Cloud adalah plugin pembuatan konten digital (DCC). Artis menggunakannya untuk mengirimkan pekerjaan dari antarmuka DCC pihak ketiga yang mereka kenal.

> **Note**
>
> Proses ini harus diselesaikan di semua workstation yang akan digunakan seniman untuk mengirimkan render.

Setiap workstation harus memiliki DCC diinstal sebelum menginstal submitter yang sesuai. Misalnya, jika Anda ingin mengunduh submitter Deadline Cloud untuk Blender, Anda harus memiliki Blender sudah diinstal pada workstation Anda.

Kami menyediakan default yang wajar untuk menjaga workstation tetap aman. Untuk informasi selengkapnya tentang mengamankan workstation Anda, lihat Praktik terbaik keamanan - workstation.

Topik

Langkah 1: Instal pengirim Cloud Deadline

Bagian berikut memandu Anda melalui langkah-langkah untuk menginstal submitter Deadline Cloud.

Unduh penginstal pengirim

Sebelum Anda dapat menginstal submitter Deadline Cloud, Anda harus mengunduh penginstal pengirim.

1. Masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Dari panel navigasi samping, pilih Unduhan.
3. Dari bagian Deadline Cloud submitter installer, pilih installer untuk sistem operasi komputer Anda, lalu pilih Unduh.
4. (Opsional)Verifikasi keaslian perangkat lunak yang diunduh.

Instal Deadline Cloud submitter

Dengan installer, Anda dapat menginstal pengirim berikut:

Perangkat lunak	Versi yang didukung	Penginstal Windows	Penginstal Linux	Penginstal macOS
Adobe Setelah Efek	2024 - 2025	Termasuk	Tidak termasuk	Termasuk

Perangkat lunak	Versi yang didukung	Penginstal Windows	Penginstal Linux	Penginstal macOS
Autodesk Arnold untuk Maya	7.1 - 7.2	Termasuk	Termasuk	Termasuk
Autodesk Maya	2023 - 2025	Termasuk	Termasuk	Termasuk
Blender	3.6 - 4.2	Termasuk	Termasuk	Termasuk
Pengecoran Nuke	15 - 16	Termasuk	Termasuk	Tidak termasuk
KeyShot Studio	2023 - 2024	Termasuk	Tidak termasuk	Termasuk
Bioskop Maxon 4D	2024 - 2025	Termasuk	Tidak termasuk	Termasuk
SidFX Houdini	19.5 - 20.5	Termasuk	Termasuk	Termasuk

Anda dapat menginstal pengirim lain yang tidak tercantum di sini. Kami menggunakan pustaka Deadline Cloud untuk membangun submitter. Beberapa pengirim termasuk Unreal Engine, 3ds Max dan Rhino. Anda dapat menemukan kode sumber untuk pustaka dan pengirim ini di organisasi aws-deadline. GitHub

Windows

1. Di browser file, navigasikan ke folder tempat penginstal diunduh, lalu pilih`DeadlineCloudSubmitter-windows-x64-installer.exe`.
   a. Jika Windows melindungi tampilan pop-up PC Anda, pilih Info lebih lanjut.
   b. Pilih Run pula.
2. Setelah AWS Deadline Cloud Submitter Setup Wizard terbuka, pilih Berikutnya.
3. Pilih ruang lingkup instalasi dengan menyelesaikan salah satu langkah berikut:
   - Untuk menginstal hanya untuk pengguna saat ini, pilih Pengguna.
   - Untuk menginstal untuk semua pengguna, pilih Sistem.

Jika Anda memilih Sistem, Anda harus keluar dari penginstal dan menjalankannya kembali sebagai administrator dengan menyelesaikan langkah-langkah berikut:

a. Klik kanan pada**DeadlineCloudSubmitter-windows-x64-installer.exe**, dan kemudian pilih Run as administrator.

b. Masukkan kredensi administrator Anda, lalu pilih Ya.

c. Pilih Sistem untuk ruang lingkup instalasi.

4. Setelah memilih ruang lingkup instalasi, pilih Berikutnya.
5. Pilih Berikutnya lagi untuk menerima direktori instalasi.
6. Pilih Integrated submitter untuk Nuke, atau pengirim mana pun yang ingin Anda instal.
7. Pilih Berikutnya.
8. Tinjau instalasi, dan pilih Berikutnya.
9. Pilih Berikutnya lagi, lalu pilih Selesai.

Linux

> **Note**
>
> The Deadline Cloud terintegrasi Nuke installer untuk Linux dan monitor Deadline Cloud hanya dapat diinstal pada Linux distribusi dengan setidaknya GLIBC 2.31.

1. Buka jendela terminal.
2. Untuk melakukan instalasi sistem installer, masukkan perintah **sudo -i** dan tekan Enter untuk menjadi root.
3. Arahkan ke lokasi tempat Anda mengunduh penginstal.

   Misalnya, **cd /home/*USER*/Downloads**.
4. Untuk membuat installer dapat dieksekusi, masukkan. **chmod +x DeadlineCloudSubmitter-linux-x64-installer.run**
5. Untuk menjalankan installer submitter Deadline Cloud, masukkan. **./DeadlineCloudSubmitter-linux-x64-installer.run**
6. Ketika installer terbuka, ikuti petunjuk di layar Anda untuk menyelesaikan Setup Wizard.

MacOS

1. Di browser file, navigasikan ke folder tempat penginstal diunduh, lalu pilih file.
2. Setelah AWS Deadline Cloud Submitter Setup Wizard terbuka, pilih Berikutnya.
3. Pilih Berikutnya lagi untuk menerima direktori instalasi.
4. Pilih Integrated submitter untuk Maya, atau pengirim mana pun yang ingin Anda instal.
5. Pilih Berikutnya.
6. Tinjau instalasi, dan pilih Berikutnya.
7. Pilih Berikutnya lagi, lalu pilih Selesai.

Langkah 2: Instal dan atur monitor Deadline Cloud

Anda dapat menginstal aplikasi desktop monitor Deadline Cloud dengan Windows, Linux, atau macOS.

Windows

1. Jika Anda belum melakukannya, masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Dari panel navigasi kiri, pilih Unduhan.
3. Di bagian Monitor Deadline Cloud, pilih yang terbaru Windows File, dan pilih Download.

   Untuk melakukan instalasi diam, gunakan perintah berikut:

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

   Secara default monitor dipasang di`C:\Users{username}\AppData\Local\DeadlineCloudMonitor`. Untuk mengubah direktori instalasi, gunakan perintah ini sebagai gantinya:

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

Linux (AppImage)

Untuk menginstal monitor Deadline Cloud AppImage di distro Debian

1. Unduh monitor AppImage Deadline Cloud terbaru.

2.
> **Note**
>
> Langkah ini untuk Ubuntu 22 dan yang lebih tinggi. Untuk versi Ubuntu lainnya, lewati langkah ini.

   Untuk menginstal libfuse2, masukkan:

```
sudo apt update
sudo apt install libfuse2
```

3. Untuk membuat AppImage executable, masukkan:

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

Linux (Debian)

Untuk menginstal Deadline Cloud monitor paket Debian pada distro Debian

1. Unduh paket Debian monitor Deadline Cloud terbaru.
2.
> **Note**
>
> Langkah ini untuk Ubuntu 22 dan yang lebih tinggi. Untuk versi Ubuntu lainnya, lewati langkah ini.

   Untuk menginstal libssl1.1, masukkan:

```
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. Untuk menginstal paket Debian monitor Deadline Cloud, masukkan:

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

4. Jika instalasi gagal pada paket yang memiliki dependensi yang tidak terpenuhi, perbaiki paket yang rusak dan kemudian jalankan perintah berikut.

```
sudo apt --fix-missing update
sudo apt update
sudo apt install -f
```

Linux (RPM)

Untuk menginstal Deadline Cloud monitor RPM aktif Rocky Linux 9 atau Alma Linux 9

1. Unduh monitor Deadline Cloud terbaru RPM.
2. Tambahkan paket tambahan untuk Enterprise Linux 9 repositori:

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

3. Instal compat-openssl11 untuk ketergantungan libssl.so.1.1:

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

Untuk menginstal Deadline Cloud monitor RPM aktif Red Hat Linux 9

1. Unduh monitor Deadline Cloud terbaru RPM.
2. Aktifkan CodeReady Linux Builder repositori:

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

3. Instal paket tambahan untuk Enterprise RPM:

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

4. Instal compat-openssl11 untuk ketergantungan libssl.so.1.1:

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

Untuk menginstal Deadline Cloud monitor RPM aktif Rocky Linux 8, Alma Linux 8, atau Red Hat Linux 8

1. Unduh monitor Deadline Cloud terbaru RPM.
2. Instal monitor Cloud Deadline:

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

macOS

1. Jika Anda belum melakukannya, masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Dari panel navigasi kiri, pilih Unduhan.
3. Di bagian Monitor Deadline Cloud, pilih yang terbaru macOS File, dan pilih Download.
4. Buka file yang diunduh. Saat jendela ditampilkan, pilih dan seret ikon monitor Deadline Cloud ke folder Aplikasi.

Setelah Anda menyelesaikan unduhan, Anda dapat memverifikasi keaslian perangkat lunak yang diunduh. Anda mungkin ingin melakukan ini untuk memastikan tidak ada yang merusak file selama atau setelah proses pengunduhan. Lihat Verifikasi keaslian perangkat lunak yang diunduh di Langkah 1.

Setelah mengunduh monitor Deadline Cloud dan memverifikasi keasliannya, gunakan prosedur berikut untuk mengatur monitor Deadline Cloud.

Untuk mengatur monitor Cloud Deadline

1. Buka Monitor Cloud Deadline.
2. Saat diminta untuk membuat profil baru, selesaikan langkah-langkah berikut.
   a. Masukkan URL monitor Anda ke input URL, yang terlihat seperti **`https://MY-MONITOR.deadlinecloud.amazonaws.com/`**
   b. Masukkan nama Profil.
   c. Pilih Buat Profil.

      Profil Anda dibuat dan kredensyal Anda sekarang dibagikan dengan perangkat lunak apa pun yang menggunakan nama profil yang Anda buat.

3. Setelah membuat profil monitor Deadline Cloud, Anda tidak dapat mengubah nama profil atau URL studio. Jika Anda perlu melakukan perubahan, lakukan hal berikut sebagai gantinya:

   a. Hapus profil. Di panel navigasi kiri, pilih Deadline Cloud monitor > Settings > Delete.

   b. Buat profil baru dengan perubahan yang Anda inginkan.

4. Dari panel navigasi kiri, gunakan opsi >Deadline Cloud monitor untuk melakukan hal berikut:

   - Ubah profil monitor Deadline Cloud untuk masuk ke monitor lain.
   - Aktifkan Autologin sehingga Anda tidak perlu memasukkan URL monitor Anda pada monitor Deadline Cloud berikutnya.

5. Tutup jendela monitor Deadline Cloud. Ini terus berjalan di latar belakang dan menyinkronkan kredensialmu setiap 15 menit.

6. Untuk setiap aplikasi pembuatan konten digital (DCC) yang Anda rencanakan untuk digunakan untuk proyek rendering Anda, selesaikan langkah-langkah berikut:

   a. Dari submitter Deadline Cloud Anda, buka konfigurasi workstation Deadline Cloud.

   b. Dalam konfigurasi workstation, pilih profil yang Anda buat di monitor Deadline Cloud. Kredensi Cloud Deadline Anda sekarang dibagikan dengan DCC ini dan alat Anda harus berfungsi seperti yang diharapkan.

Langkah 3: Luncurkan submitter Deadline Cloud

Contoh berikut menunjukkan cara menginstal Blender pengirim. Anda dapat menginstal pengirim lain menggunakan instruksi di. Pengirim yang didukung

Untuk meluncurkan submitter Deadline Cloud di Blender

> **Note**
>
> Support untuk Blender disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Blender.
2. Pilih Edit, lalu Preferensi. Di bawah Jalur File pilih Direktori Skrip, lalu pilih Tambah. Tambahkan direktori skrip untuk folder python tempat Blender pengirim diinstal:

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

3. Mulai ulang Blender.
4. Pilih Edit, lalu Preferensi. Selanjutnya, pilih Add-on, lalu cari Deadline Cloud untuk Blender. Pilih kotak centang untuk mengaktifkan add-on.
5. Buka a Blender adegan dengan dependensi yang ada di dalam direktori root aset.
6. Di menu Render, pilih dialog Deadline Cloud.
    a. Jika Anda belum diautentikasi di pengirim Deadline Cloud, Status Kredensial ditampilkan sebagai NEEDS_LOGIN.
    b. Pilih Login.
    c. Jendela browser login ditampilkan. Masuk dengan kredensi pengguna Anda.
    d. Pilih Izinkan. Anda sekarang masuk dan Status Kredensial ditampilkan sebagai AUTENTIKASI.
7. Pilih Kirim.

Pengirim yang didukung

Bagian berikut memandu Anda melalui langkah-langkah untuk meluncurkan plugin pengirim Deadline Cloud yang tersedia.

Anda dapat menginstal pengirim lain yang tidak tercantum di sini. Kami menggunakan pustaka Deadline Cloud untuk membangun submitter. Beberapa pengirim termasuk Unreal Engine, 3ds Max and Rhino. Anda dapat menemukan kode sumber untuk pustaka dan pengirim ini di organisasi aws-deadline. GitHub

Perangkat lunak	Versi yang didukung	Penginstal Windows	Penginstal Linux	Penginstal macOS
Adobe Setelah Efek	2024 - 2025	Termasuk	Tidak termasuk	Termasuk

Perangkat lunak	Versi yang didukung	Penginstal Windows	Penginstal Linux	Penginstal macOS
Autodesk Arnold untuk Maya	7.1 - 7.2	Termasuk	Termasuk	Termasuk
Autodesk Maya	2023 - 2025	Termasuk	Termasuk	Termasuk
Blender	3.6 - 4.2	Termasuk	Termasuk	Termasuk
Pengecoran Nuke	15 - 16	Termasuk	Termasuk	Tidak termasuk
KeyShot Studio	2023 - 2024	Termasuk	Tidak termasuk	Termasuk
Bioskop Maxon 4D	2024 - 2025	Termasuk	Tidak termasuk	Termasuk
SidFX Houdini	19.5 - 20.5	Termasuk	Termasuk	Termasuk

After Effects

Untuk meluncurkan submitter Deadline Cloud di After Effects

1. Buka After Effects.
2. Pilih Edit, lalu Preferensi, lalu Skrip & Ekspresi.
3. Pilih Izinkan skrip untuk menulis file dan mengakses jaringan.
4. Mulai Ulang Setelah Efek
5. Pilih Window, lalu DeadlineCloudSubmitterpilih.jsx.

Untuk menggunakan pengirim After Effects

1. Pilih Buka antrian render pada panel pengirim.
2. Tambahkan komposisi ke antrian render Anda dan atur pengaturan render, modul output, dan jalur keluaran.
3. Pilih Refresh pada panel submitter.

4. Pilih komposisi Anda dari daftar dan kemudian pilih Kirim. Anda dapat memilih Refresh lagi ketika Anda menambahkan atau menghapus komposisi dari antrian render Anda.

Anda dapat memasang pengirim ke panel samping dengan memilih sudut kanan atas pengirim dan menjatuhkannya di bagian yang disorot di After Effects.

Blender

Untuk meluncurkan submitter Deadline Cloud di Blender

> **Note**
>
> Support untuk Blender disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Blender.
2. Pilih Edit, lalu Preferensi. Di bawah Jalur File pilih Direktori Skrip, lalu pilih Tambah. Tambahkan direktori skrip untuk folder python tempat Blender pengirim diinstal:

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

3. Mulai ulang Blender.
4. Pilih Edit, lalu Preferensi. Selanjutnya, pilih Add-on, lalu cari Deadline Cloud untuk Blender. Pilih kotak centang untuk mengaktifkan add-on.
5. Buka a Blender adegan dengan dependensi yang ada di dalam direktori root aset.
6. Di menu Render, pilih dialog Deadline Cloud.
    a. Jika Anda belum diautentikasi di pengirim Deadline Cloud, Status Kredensial ditampilkan sebagai NEEDS_LOGIN.
    b. Pilih Login.
    c. Jendela browser login ditampilkan. Masuk dengan kredensi pengguna Anda.
    d. Pilih Izinkan. Anda sekarang masuk dan Status Kredensial ditampilkan sebagai AUTENTIKASI.

7. Pilih Kirim.

Cinema 4D

Untuk meluncurkan submitter Deadline Cloud di Cinema 4D

> **Note**
>
> Support untuk Cinema 4D disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Bioskop 4D.
2. Jika diminta untuk menginstal komponen GUI untuk AWS Deadline Cloud, selesaikan langkah-langkah berikut:
   a. Saat prompt ditampilkan, pilih Ya, dan tunggu dependensi dipasang.
   b. Mulai ulang Cinema 4D untuk memastikan perubahan diterapkan.
3. Pilih Ekstensi > AWS Deadline Cloud Submitter.

Houdini

Untuk meluncurkan submitter Deadline Cloud di Houdini

> **Note**
>
> Support untuk Houdini disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Houdini.
2. Di Network Editor, pilih jaringan /out.
3. Tekan tab, dan masukkan**`deadline`**.
4. Pilih opsi Deadline Cloud, dan sambungkan ke jaringan yang ada.
5. Klik dua kali node Deadline Cloud.

KeyShot

Untuk meluncurkan submitter Deadline Cloud di KeyShot

1. Buka KeyShot.
2. Pilih Windows> Konsol scripting > Kirim ke AWS Deadline Cloud dan Run.

Ada dua mode pengiriman untuk KeyShot pengirim. Pilih mode pengiriman untuk membuka pengirim.

- Lampirkan file BIP adegan dan semua referensi file eksternal - File adegan terbuka dan semua file eksternal yang direferensikan dalam BIP disertakan sebagai lampiran pekerjaan.
- Lampirkan hanya file BIP adegan - Hanya file adegan terbuka yang dilampirkan ke kiriman. Setiap file eksternal yang direferensikan dalam adegan harus tersedia untuk pekerja melalui penyimpanan jaringan atau metode lain.

Maya and Arnold for Maya

Untuk meluncurkan submitter Deadline Cloud di Maya

> **Note**
>
> Support untuk Maya and Arnold for Maya (MtoA) disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Maya.
2. Tetapkan proyek Anda, dan buka file yang ada di dalam direktori root aset.
3. Pilih Windows → Pengaturan/Preferensi → Pengelola Plugin.
4. Cari DeadlineCloudSubmitter.
5. Untuk memuat plugin pengirim Deadline Cloud, pilih Loaded.
    a. Jika Anda belum diautentikasi di pengirim Deadline Cloud, Status Kredensial ditampilkan sebagai NEEDS_LOGIN.
    b. Pilih Login.
    c. Jendela browser login ditampilkan. Masuk dengan kredensi pengguna Anda.

   d. Pilih Izinkan. Anda sekarang masuk dan Status Kredensial ditampilkan sebagai AUTENTIKASI.

6. (Opsional) Untuk memuat plugin pengirim Deadline Cloud setiap kali Anda membuka Maya, pilih Muat otomatis.
7. Pilih rak Deadline Cloud, lalu pilih tombol hijau untuk meluncurkan submitter.

Nuke

Untuk meluncurkan submitter Deadline Cloud di Nuke

> **Note**
>
> Support untuk Nuke disediakan dengan menggunakan Conda lingkungan untuk armada yang dikelola layanan. Untuk informasi selengkapnya, lihat Default Conda lingkungan antrian.

1. Buka Nuke.
2. Buka a Nuke script dengan dependensi yang ada dalam direktori root aset.
3. Pilih AWS Deadline, lalu pilih Kirim ke Deadline Cloud untuk meluncurkan submitter.

   a. Jika Anda belum diautentikasi di pengirim Deadline Cloud, Status Kredensial ditampilkan sebagai NEEDS_LOGIN.

   b. Pilih Login.

   c. Di jendela browser login, masuk dengan kredensi pengguna Anda.

   d. Pilih Izinkan. Anda sekarang masuk dan Status Kredensial ditampilkan sebagai AUTENTIKASI.

4. Pilih Kirim.

Menggunakan monitor Deadline Cloud

Monitor AWS Deadline Cloud memberi Anda tampilan keseluruhan pekerjaan komputasi visual Anda. Anda dapat menggunakannya untuk memantau dan mengelola pekerjaan, melihat aktivitas pekerja di armada, melacak anggaran dan penggunaan, dan untuk mengunduh hasil pekerjaan.

Setiap antrian memiliki monitor pekerjaan yang menunjukkan status pekerjaan, langkah, dan tugas. Monitor menyediakan cara untuk mengelola pekerjaan langsung dari monitor. Anda dapat membuat perubahan prioritas, membatalkan pekerjaan, meminta pekerjaan, dan mengirim ulang pekerjaan.

Monitor Deadline Cloud memiliki tabel yang menunjukkan status ringkasan untuk suatu pekerjaan, atau Anda dapat memilih pekerjaan untuk melihat log tugas terperinci yang membantu memecahkan masalah dengan pekerjaan.

Anda dapat menggunakan monitor Deadline Cloud untuk mengunduh hasil ke lokasi di workstation Anda yang ditentukan saat pekerjaan dibuat.

Monitor Deadline Cloud juga membantu Anda memantau penggunaan dan mengelola biaya. Untuk informasi selengkapnya, lihat Lacak pengeluaran dan penggunaan untuk Deadline Cloud farm.

Topik

Bagikan URL monitor Cloud Deadline

Saat menyiapkan layanan Deadline Cloud, secara default Anda membuat URL yang membuka monitor Deadline Cloud untuk akun Anda. Gunakan URL ini untuk membuka monitor di browser

Anda atau di desktop Anda. Bagikan URL dengan pengguna lain sehingga mereka dapat mengakses monitor Deadline Cloud.

Sebelum pengguna dapat membuka monitor Deadline Cloud, Anda harus memberikan akses kepada pengguna. Untuk memberikan akses, tambahkan pengguna ke daftar pengguna yang berwenang untuk monitor atau tambahkan mereka ke grup dengan akses ke monitor. Untuk informasi selengkapnya, lihat Mengelola pengguna di Deadline Cloud.

Untuk berbagi URL monitor

1. Buka konsol Deadline Cloud.
2. Dari Mulai, pilih Go to Deadline Cloud dashboard.
3. Di panel navigasi, pilih Dashboard (Dasbor).
4. Di bagian Ikhtisar akun, pilih Detail akun.
5. Salin dan kemudian kirim URL dengan aman ke siapa saja yang perlu mengakses monitor Deadline Cloud.

Buka monitor Deadline Cloud

Anda dapat membuka monitor Deadline Cloud dengan salah satu cara berikut:

- Konsol — Masuk ke AWS Management Console dan buka konsol Deadline Cloud.
- Web — Buka URL monitor yang Anda buat saat menyiapkan Deadline Cloud.
- Monitor — Gunakan monitor Cloud Deadline desktop.

Saat menggunakan konsol, Anda harus dapat masuk AWS menggunakan AWS Identity and Access Management identitas, lalu masuk ke monitor dengan AWS IAM Identity Center kredensil. Jika Anda hanya memiliki kredenal Pusat Identitas IAM, Anda harus masuk menggunakan URL monitor atau aplikasi desktop.

Untuk membuka monitor Deadline Cloud (web)

1. Menggunakan browser, buka URL monitor yang Anda buat saat menyiapkan Deadline Cloud.
2. Masuk dengan kredensi pengguna Anda.

Untuk membuka monitor Deadline Cloud (konsol)

1. Buka konsol Deadline Cloud.
2. Di panel navigasi, pilih Peternakan.
3. Pilih peternakan, lalu pilih Kelola pekerjaan untuk membuka halaman monitor Deadline Cloud.
4. Masuk dengan kredensi pengguna Anda.

Untuk membuka monitor Deadline Cloud (desktop)

1. Buka konsol Deadline Cloud.

   -atau-

   Buka monitor Deadline Cloud - web dari URL monitor.
2. - Pada konsol Deadline Cloud, lakukan hal berikut:
     1. Di monitor, pilih Buka dasbor Deadline Cloud, lalu pilih Unduhan dari menu sebelah kiri.
     2. Dari monitor Deadline Cloud, pilih versi monitor untuk desktop Anda.
     3. Pilih Unduh.
   - Pada monitor Deadline Cloud - web, lakukan hal berikut:
     - Dari menu sebelah kiri, pilih Pengaturan Workstation. Jika item pengaturan Workstation tidak terlihat, gunakan panah untuk membuka menu kiri.
     - Pilih Unduh.
     - Dari Pilih OS, pilih sistem operasi Anda.
3. Unduh monitor Cloud Deadline - desktop.
4. Setelah Anda mengunduh dan menginstal monitor, buka di komputer Anda.

   - Jika ini adalah pertama kalinya Anda membuka monitor Deadline Cloud, Anda harus memberikan URL monitor dan membuat nama profil. Selanjutnya Anda masuk ke monitor dengan kredensi Deadline Cloud Anda.
   - Setelah Anda membuat profil, Anda membuka monitor dengan memilih profil. Anda mungkin perlu memasukkan kredensi Deadline Cloud Anda.

Mengubah setelan bahasa Anda

Setelah Anda membuat dan membuka monitor Deadline Cloud Anda, Anda dapat mengubah pengaturan bahasa Anda. Secara default, bahasa monitor diatur ke pengaturan bahasa sistem Anda.

Untuk mengubah pengaturan bahasa Anda dari monitor Deadline Cloud (desktop)

1. Dari profil pengguna Anda, pilih Pengaturan, lalu pilih Bahasa.
2. Dari menu tarik-turun, pilih salah satu bahasa yang tersedia.
3. Konfirmasikan bahwa bahasa yang Anda pilih adalah opsi yang tercantum, lalu pilih Konfirmasi dan terapkan untuk menerapkan perubahan.

   Setelah monitor menyegarkan, monitor ditampilkan dalam bahasa yang dipilih.

   Setelah Anda mengubah pengaturan bahasa, itu adalah default saat membuka dan tetap default sampai Anda mengubahnya lagi atau menghapus instalasi aplikasi desktop.

Untuk mengubah bahasa monitor Deadline Cloud di web, ubah bahasa pilihan di pengaturan browser Anda.

> **Note**
>
> Jika browser atau sistem operasi Anda diatur ke bahasa yang tidak didukung oleh Deadline Cloud, bahasa Inggris menjadi bahasa default untuk monitor Deadline Cloud.

Lihat detail antrian dan armada di Deadline Cloud

Anda dapat menggunakan monitor Deadline Cloud untuk melihat konfigurasi antrian dan armada di peternakan Anda. Anda juga dapat menggunakan monitor untuk melihat daftar pekerjaan dalam antrian atau pekerja dalam armada.

Anda harus memiliki `VIEWING` izin untuk melihat detail antrian dan armada. Jika detail tidak ditampilkan, hubungi administrator Anda untuk mendapatkan izin yang benar.

Untuk melihat detail antrian

1. Buka monitor Deadline Cloud.

2. Dari daftar peternakan, pilih peternakan yang berisi antrian yang Anda minati.
3. Dalam daftar antrian, pilih antrian untuk menampilkan detailnya. Untuk membandingkan konfigurasi dua antrian atau lebih, pilih lebih dari satu kotak centang.
4. Untuk melihat daftar pekerjaan dalam antrian, pilih nama antrian dari daftar antrian atau dari panel detail.

Jika monitor sudah terbuka, Anda dapat memilih antrian dari daftar Antrian di panel navigasi kiri.

Untuk melihat detail armada

1. Buka monitor Deadline Cloud.
2. Dari daftar peternakan, pilih peternakan yang berisi armada yang Anda minati.
3. Di sumber daya Pertanian, pilih Armada.
4. Dalam daftar armada, pilih armada untuk menampilkan detailnya. Untuk membandingkan konfigurasi dua armada atau lebih, pilih lebih dari satu kotak centang.
5. Untuk melihat daftar pekerja di armada, pilih nama armada dari daftar armada atau dari panel detail.

Jika monitor sudah terbuka, Anda dapat memilih armada dari daftar Armada di panel navigasi kiri.

Kelola pekerjaan, langkah, dan tugas di Deadline Cloud

Saat Anda memilih antrian, bagian monitor pekerjaan pada monitor Deadline Cloud menunjukkan pekerjaan dalam antrian tersebut, langkah-langkah dalam pekerjaan, dan tugas di setiap langkah. Ketika Anda memilih pekerjaan, langkah, atau tugas, Anda dapat menggunakan menu Tindakan untuk mengelola masing-masing.

Untuk membuka monitor pekerjaan, ikuti langkah-langkah untuk melihat antrianLihat detail antrian dan armada di Deadline Cloud, lalu pilih pekerjaan, langkah, atau tugas yang akan dikerjakan.

Untuk pekerjaan, langkah, dan tugas, Anda dapat melakukan hal berikut:

- Ubah status menjadi Requeued, Succeeded, Failed, atau Canceled.
- Unduh output yang diproses dari pekerjaan, langkah, atau tugas.
- Salin ID pekerjaan, langkah, atau tugas.

Untuk pekerjaan yang dipilih, Anda dapat:

- Arsipkan pekerjaan.
- Ubah properti pekerjaan, seperti mengubah prioritas atau melihat dependensi langkah ke langkah.
- Lihat detail tambahan menggunakan parameter pekerjaan.
- Kirim ulang pekerjaan.

Untuk informasi lebih lanjut, lihatLihat dan kelola detail pekerjaan di Deadline Cloud.

Untuk setiap langkah, Anda dapat:

- Lihat dependensi untuk langkah tersebut. Dependensi untuk langkah harus diselesaikan sebelum langkah berjalan.

Lihat perinciannya di Lihat langkah di Deadline Cloud.

Untuk setiap tugas, Anda dapat:

- Lihat log untuk tugas tersebut.
- Lihat parameter tugas.

Untuk informasi selengkapnya, lihat Melihat tugas di Deadline Cloud.

Lihat dan kelola detail pekerjaan di Deadline Cloud

Halaman monitor Job di monitor Deadline Cloud memberi Anda hal-hal berikut:

- Pandangan keseluruhan tentang kemajuan suatu pekerjaan.
- Pandangan tentang langkah-langkah dan tugas yang membentuk pekerjaan.

Pilih pekerjaan dari daftar untuk melihat daftar langkah untuk pekerjaan itu, lalu pilih langkah dari daftar langkah untuk melihat tugas untuk pekerjaan itu. Setelah memilih item, Anda dapat menggunakan menu Tindakan untuk item tersebut untuk melihat detail.

Untuk melihat detail pekerjaan

1. Ikuti langkah-langkah untuk melihat antrian diLihat detail antrian dan armada di Deadline Cloud.

2. Di panel navigasi, pilih antrian tempat Anda mengirimkan pekerjaan.
3. Pilih pekerjaan menggunakan salah satu metode berikut:

    a. Dari daftar Pekerjaan, pilih pekerjaan untuk melihat detailnya.
    b. Dari bidang pencarian, masukkan teks apa pun yang terkait dengan pekerjaan, seperti nama pekerjaan atau pengguna yang membuat pekerjaan. Dari hasil yang ditampilkan, pilih pekerjaan yang ingin Anda lihat.

Rincian pekerjaan mencakup langkah-langkah dalam pekerjaan dan tugas di setiap langkah. Anda dapat menggunakan menu Tindakan untuk melakukan hal berikut:

- Ubah status pekerjaan.
- Melihat dan memodifikasi properti pekerjaan.
    - Anda dapat melihat dependensi di antara langkah-langkah dalam pekerjaan.
    - Anda dapat mengubah prioritas pekerjaan dalam antrian. Pekerjaan dengan prioritas angka yang lebih tinggi diproses sebelum pekerjaan dengan prioritas angka yang lebih rendah. Pekerjaan dapat memiliki prioritas antara 1 dan 100. Ketika dua pekerjaan memiliki prioritas yang sama, pekerjaan tertua dijadwalkan terlebih dahulu.
- Lihat parameter untuk pekerjaan yang ditetapkan saat pekerjaan dikirimkan.
- Unduh output dari suatu pekerjaan. Ketika Anda men-download output dari pekerjaan, itu berisi semua output yang dihasilkan oleh langkah-langkah dan tugas dalam pekerjaan.

Arsipkan pekerjaan

Untuk mengarsipkan pekerjaan, itu harus dalam keadaan terminal,`FAILED`,`SUCCEEDED`,`SUSPENDED`, atau`CANCELED`. `ARCHIVED`Negara adalah final. Setelah pekerjaan diarsipkan, pekerjaan tidak dapat diulang atau dimodifikasi.

Data pekerjaan tidak terpengaruh oleh pengarsipan pekerjaan. Data dihapus ketika batas waktu tidak aktif tercapai, atau ketika antrian yang berisi pekerjaan dihapus.

Hal-hal lain yang terjadi pada pekerjaan yang diarsipkan:

- Pekerjaan yang diarsipkan disembunyikan di monitor Deadline Cloud.
- Pekerjaan yang diarsipkan terlihat dalam status hanya-baca dari Deadline Cloud CLI selama 120 hari sebelum penghapusan.

Meminta pekerjaan

Saat Anda meminta ulang pekerjaan, semua tugas tanpa dependensi langkah beralih ke. `READY` Status langkah-langkah dengan dependensi beralih ke `READY` atau `PENDING` saat dipulihkan.

- Semua pekerjaan, langkah, dan tugas beralih ke`PENDING`.
- Jika sebuah langkah tidak memiliki ketergantungan, itu beralih ke`READY`.

Kirim ulang pekerjaan

Mungkin ada saat-saat ketika Anda ingin menjalankan pekerjaan lagi, tetapi dengan properti dan pengaturan yang berbeda. Misalnya, Anda dapat mengirimkan pekerjaan untuk merender subset frame pengujian, memverifikasi output, lalu menjalankan pekerjaan lagi dengan rentang bingkai penuh. Untuk melakukan ini, kirimkan kembali pekerjaan.

Saat Anda mengirim ulang pekerjaan, tugas baru tanpa dependensi menjadi. `READY` Tugas baru dengan dependensi menjadi. `PENDING`

- Semua pekerjaan, langkah, dan tugas baru menjadi`PENDING`.
- Jika langkah baru tidak memiliki ketergantungan, itu menjadi`READY`.

Saat mengirim ulang pekerjaan, Anda hanya dapat mengubah properti yang didefinisikan sebagai dapat dikonfigurasi saat pekerjaan pertama kali dibuat. Misalnya, jika nama pekerjaan tidak didefinisikan sebagai properti pekerjaan yang dapat dikonfigurasi saat pertama kali dikirimkan, maka nama tersebut tidak dapat diedit pada pengiriman ulang.

Lihat langkah di Deadline Cloud

Gunakan monitor AWS Deadline Cloud untuk melihat langkah-langkah dalam pekerjaan pemrosesan Anda. Di monitor Job, daftar Langkah menunjukkan daftar langkah yang membentuk pekerjaan yang dipilih. Saat Anda memilih langkah, daftar Tugas menunjukkan tugas di langkah tersebut.

Untuk melihat langkah

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.
2. Pilih sebuah tugas dari daftar Tugas.

3. Pilih langkah dari daftar Langkah.

Anda dapat menggunakan menu Tindakan untuk melakukan hal berikut:

- Ubah status langkah.
- Unduh output dari langkah tersebut. Saat Anda mengunduh output dari sebuah langkah, itu berisi semua output yang dihasilkan oleh tugas di langkah tersebut.
- Lihat dependensi dari sebuah langkah. Tabel dependensi menunjukkan daftar langkah yang harus diselesaikan sebelum langkah yang dipilih dimulai, dan daftar langkah yang menunggu langkah ini selesai.

Melihat tugas di Deadline Cloud

Gunakan monitor AWS Deadline Cloud untuk melihat tugas dalam pekerjaan pemrosesan Anda. Di monitor Job, daftar Tugas menampilkan tugas yang membentuk langkah yang dipilih dalam daftar Langkah.

Untuk melihat tugas

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.
2. Pilih sebuah tugas dari daftar Tugas.
3. Pilih langkah dari daftar Langkah.
4. Pilih tugas dari daftar Tugas.

Anda dapat menggunakan menu Tindakan untuk melakukan hal berikut:

- Ubah status tugas.
- Lihat log tugas. Untuk informasi selengkapnya, lihat Lihat sesi dan log pekerja di Deadline Cloud.
- Lihat parameter yang ditetapkan saat tugas dibuat.
- Unduh output tugas. Saat Anda mengunduh output tugas, itu hanya berisi output yang dihasilkan oleh tugas yang dipilih.

Lihat sesi dan log pekerja di Deadline Cloud

Log memberi Anda informasi terperinci tentang status dan pemrosesan tugas. Di monitor AWS Deadline Cloud, Anda dapat melihat dua jenis log berikut:

- Log sesi merinci garis waktu tindakan, termasuk:
  - Tindakan pengaturan, seperti sinkronisasi lampiran dan memuat lingkungan perangkat lunak
  - Menjalankan tugas atau serangkaian tugas
  - Tindakan penutupan, seperti mematikan lingkungan pada pekerja

  Sesi mencakup pemrosesan setidaknya satu tugas, dan dapat mencakup banyak tugas. Log sesi juga menampilkan informasi tentang jenis instans Amazon Elastic Compute Cloud (Amazon EC2), vCPU, dan memori. Log sesi juga menyertakan tautan ke log untuk pekerja yang digunakan dalam sesi.
- Log pekerja memberikan detail untuk timeline tindakan yang diproses pekerja selama siklus hidupnya. Log pekerja dapat berisi informasi tentang beberapa sesi.

Anda dapat mengunduh log sesi dan pekerja sehingga Anda dapat memeriksanya secara offline.

Untuk melihat log sesi

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.
2. Pilih sebuah tugas dari daftar Tugas.
3. Pilih langkah dari daftar Langkah.
4. Pilih tugas dari daftar Tugas.
5. Dari menu Tindakan, pilih Lihat log.

Bagian Garis Waktu menunjukkan ringkasan tindakan untuk tugas tersebut. Untuk melihat lebih banyak tugas yang dijalankan dalam sesi dan untuk melihat tindakan shutdown untuk sesi, pilih Lihat log untuk semua tugas.

Untuk melihat log pekerja dari tugas

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.

2. Pilih sebuah tugas dari daftar Tugas.
3. Pilih langkah dari daftar Langkah.
4. Pilih tugas dari daftar Tugas.
5. Dari menu Tindakan, pilih Lihat log.
6. Pilih Info sesi.
7. Pilih Lihat log pekerja.

Untuk melihat log pekerja dari detail armada

1. Ikuti langkah-langkah Lihat detail antrian dan armada di Deadline Cloud untuk melihat armada.
2. Pilih ID Pekerja dari daftar Pekerja.
3. Dari menu Tindakan, pilih Lihat log pekerja.

Lihat detail pekerja di dasbor pekerja

Dasbor pekerja memberikan detail untuk pekerja yang memproses tugas. Anda dapat melihat:

- Metadata, seperti tipe instance, untuk pekerja
- Tindakan sesi yang dilakukan pekerja
- Kinerja pekerja, termasuk CPU, memori, dan penggunaan disk
- Grafik penggunaan CPU, memori, dan disk dari waktu ke waktu
- Grafik kecepatan disk dari waktu ke waktu
- Log pekerja untuk tugas tersebut

Untuk melihat dasbor pekerja dari tugas

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.
2. Pilih sebuah tugas dari daftar Tugas.
3. Pilih langkah dari daftar Langkah.
4. Pilih tugas dari daftar Tugas.
5. Di tabel tugas, dari menu Tindakan, pilih Lihat dasbor pekerja.

Untuk melihat dasbor pekerja dari detail armada

1. Ikuti langkah-langkah Lihat detail antrian dan armada di Deadline Cloud untuk melihat armada.
2. Pilih Pekerja dari daftar Pekerja.
3. Dari menu Tindakan, pilih Lihat dasbor pekerja.

Kasus penggunaan

Mendeteksi instance yang kurang disediakan

Ketika render memakan waktu lebih lama dari yang diharapkan, dasbor pekerja dapat membantu menentukan apakah instance Anda berukuran cukup untuk beban kerja Anda. Meskipun pemanfaatan vCPU 100% normal untuk banyak penyaji, penggunaan memori yang tinggi secara konsisten mendekati kapasitas maksimum dan pemanfaatan ruang disk yang meningkat dapat menunjukkan bahwa instance Anda kurang disediakan. Dalam kasus seperti itu, memutakhirkan konfigurasi instance armada Anda dapat mengurangi kesalahan render dan secara signifikan meningkatkan waktu render. Namun, penting untuk terus memantau kinerja pekerja setelah melakukan upgrade untuk memastikan Anda telah menemukan keseimbangan optimal - peningkatan yang terlalu agresif dapat menyebabkan biaya yang tidak perlu melalui penyediaan berlebihan.

Mendeteksi instance yang disediakan secara berlebihan

Bahkan ketika tugas selesai dengan sukses, mungkin ada peluang untuk mengoptimalkan biaya Anda. Dasbor pekerja dapat mengungkapkan jika Anda membayar lebih banyak daya komputasi daripada yang dibutuhkan beban kerja Anda. Jika Anda melihat bahwa pekerja memiliki penggunaan vCPU rata-rata yang rendah, pemanfaatan memori minimal, dan kelebihan ruang disk yang tidak digunakan, Anda dapat mengurangi konfigurasi instance armada Anda.

Pemecahan masalah tugas yang gagal

Saat menyelidiki tugas yang gagal, dasbor pekerja berfungsi sebagai alat diagnostik yang berharga. Berikan perhatian khusus pada penggunaan memori puncak dan pemanfaatan ruang disk - jika metrik ini mendekati atau mencapai 100%, kemungkinan besar merupakan akar penyebab kegagalan tugas Anda. Kelelahan sumber daya seperti itu menunjukkan bahwa instans Anda saat ini tidak memiliki kapasitas untuk menangani beban kerja Anda secara efektif. Dalam kasus ini, penyediaan instance dengan peningkatan memori atau ruang disk akan membantu memastikan penyelesaian tugas yang berhasil.

Tingkat pemanfaatan instans optimal

Pemanfaatan vCPU

Kisaran target: 70— 90%

- Di bawah 70%: Kemungkinan kurang memanfaatkan sumber daya komputasi, artinya Anda membayar lebih banyak CPU daripada kebutuhan beban kerja Anda
- 70— 90%: Rentang optimal di mana Anda menggunakan sumber daya secara efisien tanpa mengalami kemacetan
- Secara konsisten pada 100%: Dapat menunjukkan kemacetan CPU yang mungkin memperlambat render

Ingatlah bahwa beberapa tugas render secara alami akan lebih intensif CPU daripada yang lain, dan penggunaan vCPU 100% mungkin tidak menjadi masalah. Tugas visualisasi real-time mungkin menunjukkan pemanfaatan CPU yang lebih konsisten, sementara tugas dengan perubahan persyaratan komputasi mungkin memiliki pola yang bervariasi.

Pemanfaatan Memori

Kisaran target: 70— 85%

- Di bawah 50%: Instans yang berpotensi besar untuk beban kerja Anda
- 70— 85%: Pemanfaatan optimal dengan ruang kepala yang cukup untuk paku
- Di atas 90%: Risiko penurunan kinerja atau kesalahan out-of-memory

Persyaratan memori dapat sangat bervariasi tergantung pada kompleksitas pemandangan, resolusi tekstur, dan data simulasi. Memantau tren memori dari waktu ke waktu penting untuk mengidentifikasi apakah beban kerja Anda bertambah dalam kebutuhan memori.

Pemanfaatan Ruang Disk

Kisaran target: 60— 80%

- Di bawah 40%: Kemungkinan penyimpanan yang disediakan secara berlebihan
- 60-85%: Pemanfaatan yang baik dengan ruang untuk file sementara dan cache
- Di atas 85%: Risiko kehabisan ruang selama render besar

Ingat bahwa I/O kinerja disk bisa sama pentingnya dengan kapasitas, terutama untuk beban kerja yang tekstur read/write besar atau file cache selama rendering.

Unduh hasil jadi di Deadline Cloud

Setelah pekerjaan selesai, Anda dapat menggunakan monitor AWS Deadline Cloud untuk mengunduh hasilnya ke workstation Anda. File output disimpan dengan nama dan lokasi yang Anda tentukan saat Anda membuat pekerjaan.

File output disimpan tanpa batas waktu. Untuk mengurangi biaya penyimpanan, pertimbangkan untuk membuat konfigurasi Siklus Hidup S3 untuk bucket Amazon S3 antrian Anda. Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk mengunduh hasil akhir dari pekerjaan, langkah, atau tugas

1. Ikuti langkah-langkah Lihat dan kelola detail pekerjaan di Deadline Cloud untuk melihat daftar pekerjaan.
2. Pilih pekerjaan, langkah, atau tugas yang ingin Anda unduh hasilnya.
   - Jika Anda memilih pekerjaan, Anda dapat mengunduh semua output untuk semua tugas di semua langkah untuk pekerjaan itu.
   - Jika Anda memilih langkah, Anda dapat mengunduh semua output untuk semua tugas di langkah itu.
   - Jika Anda memilih tugas, Anda dapat mengunduh output untuk tugas individual tersebut.
3. Dari menu Tindakan, pilih Unduh output.
4. Output akan diunduh ke lokasi yang ditetapkan saat pekerjaan dikirimkan.

> **Note**
>
> Mengunduh output menggunakan menu saat ini hanya didukung untuk Windows danLinux. Jika Anda memiliki Mac dan Anda memilih item menu keluaran Unduh, sebuah jendela menunjukkan AWS CLI perintah yang dapat Anda gunakan untuk mengunduh output yang dirender.

Batas waktu Cloud farm

Dengan Deadline Cloud farm, Anda dapat mengelola pengguna dan sumber daya proyek. Peternakan adalah tempat sumber daya proyek Anda berada. Peternakan Anda terdiri dari antrian dan armada. Antrian adalah tempat pekerjaan yang diajukan berada dan dijadwalkan akan diberikan. Armada adalah sekelompok node pekerja yang menjalankan tugas untuk menyelesaikan pekerjaan. Setelah Anda membuat peternakan, Anda dapat membuat antrian dan armada untuk memenuhi kebutuhan proyek Anda.

Buat peternakan

1. Dari konsol Cloud Deadline, pilih Buka Dasbor.
2. Di bagian Farms di dasbor Deadline Cloud, pilih Actions → Create farm.
   - Atau, di panel sebelah kiri pilih Farms dan sumber daya lainnya, lalu pilih Create Farm.
3. Tambahkan Nama untuk peternakan Anda.
4. Untuk Deskripsi, masukkan deskripsi pertanian. Deskripsi yang jelas dapat membantu Anda mengidentifikasi tujuan pertanian Anda dengan cepat.
5. (Opsional) Secara default, data Anda dienkripsi dengan kunci yang AWS memiliki dan mengelola keamanan Anda. Anda dapat memilih Sesuaikan pengaturan enkripsi (lanjutan) untuk menggunakan kunci yang ada atau untuk membuat kunci baru yang Anda kelola.

   Jika Anda memilih untuk menyesuaikan pengaturan enkripsi menggunakan kotak centang, masukkan AWS KMS ARN, atau buat yang AWS KMS baru dengan memilih Buat kunci KMS baru.
6. (Opsional) Pilih Tambahkan tag baru untuk menambahkan satu atau beberapa tag ke peternakan Anda.
7. Pilih Buat pertanian. Setelah pembuatan, pertanian Anda ditampilkan.

Batas waktu antrian Cloud

Antrian adalah sumber daya pertanian yang mengelola dan memproses pekerjaan.

Untuk bekerja dengan antrian, Anda harus sudah memiliki monitor dan pertanian.

Topik

Membuat antrean

1. Dari dasbor konsol Deadline Cloud, pilih farm yang ingin Anda buat antrean.
    - Atau, di panel sisi kiri pilih Peternakan dan sumber daya lainnya, lalu pilih peternakan yang ingin Anda buat antrean.
2. Di tab Antrian, pilih Buat antrian.
3. Masukkan nama untuk antrian Anda.
4. Untuk Deskripsi, masukkan deskripsi antrian. Deskripsi membantu Anda mengidentifikasi tujuan antrian Anda.
5. Untuk lampiran Job, Anda dapat membuat bucket Amazon S3 baru atau memilih bucket Amazon S3 yang sudah ada.
    a. Untuk membuat bucket Amazon S3 baru
        i. Pilih Buat keranjang pekerjaan baru.
        ii. Masukkan nama untuk ember. Kami merekomendasikan penamaan emberdeadlinecloud-job-attachments-[MONITORNAME].
        iii. Masukkan awalan Root untuk menentukan atau mengubah lokasi root antrian Anda.
    b. Untuk memilih bucket Amazon S3 yang ada
        i. Pilih Pilih bucket S3 yang ada > Jelajahi S3.
        ii. Pilih bucket S3 untuk antrian Anda dari daftar bucket yang tersedia.

6. (Opsional) Untuk mengaitkan antrian Anda dengan armada yang dikelola pelanggan, pilih Aktifkan asosiasi dengan armada yang dikelola pelanggan.
7. Jika Anda mengaktifkan asosiasi dengan armada yang dikelola pelanggan, Anda harus menyelesaikan langkah-langkah berikut.

> **Important**
>
> Kami sangat menyarankan untuk menentukan pengguna dan grup untuk fungsionalitas run-as. Jika tidak, itu akan menurunkan postur keamanan peternakan Anda karena pekerjaan kemudian dapat melakukan semua yang dapat dilakukan agen pekerja. Untuk informasi selengkapnya tentang potensi risiko keamanan, lihat Menjalankan lowongan sebagai pengguna dan grup.

   a. Untuk Jalankan sebagai pengguna:

      Untuk memberikan kredensi untuk pekerjaan antrian, pilih Pengguna yang dikonfigurasi antrian.

      Atau, untuk memilih keluar dari pengaturan kredensional Anda sendiri dan menjalankan pekerjaan sebagai pengguna agen pekerja, pilih Pengguna agen pekerja.

   b. (Opsional) Untuk Run as user credentials, masukkan nama pengguna dan nama grup untuk memberikan kredensi untuk pekerjaan antrian.

      Jika Anda menggunakan Windows armada, Anda harus membuat AWS Secrets Manager rahasia yang berisi kata sandi untuk Run sebagai pengguna. Jika Anda tidak memiliki rahasia yang ada dengan kata sandi, pilih Buat rahasia untuk membuka konsol Secrets Manager untuk membuat rahasia. Untuk informasi selengkapnya, lihat Mengelola akses ke Windows rahasia pengguna pekerjaan di Panduan Pengembang Cloud Deadline.

8. Membutuhkan anggaran membantu mengelola biaya untuk antrian Anda. Pilih salah satu Jangan memerlukan anggaran atau Memerlukan anggaran.
9. Antrian Anda memerlukan izin untuk mengakses Amazon S3 atas nama Anda. Anda dapat membuat peran layanan baru atau menggunakan peran layanan yang ada. Jika Anda tidak memiliki peran layanan yang ada, buat dan gunakan peran layanan baru.

   a. Untuk menggunakan peran layanan yang ada, pilih Pilih peran layanan, lalu pilih peran dari menu tarik-turun.

   b. Untuk membuat peran layanan baru, pilih Buat dan gunakan peran layanan baru, lalu masukkan nama peran dan deskripsi.

10. (Opsional) Untuk menambahkan variabel lingkungan untuk lingkungan antrian, pilih Tambahkan variabel lingkungan baru, lalu masukkan nama dan nilai untuk setiap variabel yang Anda tambahkan.
11. (Opsional) Pilih Tambahkan tag baru untuk menambahkan satu atau beberapa tag ke antrian Anda.
12. Untuk membuat default Conda lingkungan antrian, pertahankan kotak centang yang dipilih. Untuk mempelajari lebih lanjut tentang lingkungan antrian, lihat Membuat lingkungan antrian. Jika Anda membuat antrian untuk armada yang dikelola pelanggan, kosongkan kotak centang.
13. Pilih Buat antrean.

Buat lingkungan antrian

Lingkungan antrian adalah seperangkat variabel lingkungan dan perintah yang mengatur pekerja armada. Anda dapat menggunakan lingkungan antrian untuk menyediakan aplikasi perangkat lunak, variabel lingkungan, dan sumber daya lainnya untuk pekerjaan dalam antrian.

Saat Anda membuat antrian, Anda memiliki opsi untuk membuat default Conda lingkungan antrian. Lingkungan ini menyediakan akses armada yang dikelola layanan ke paket untuk aplikasi dan penyaji DCC mitra. Lingkungan default Untuk informasi selengkapnya, lihatDefault Conda lingkungan antrian.

Anda dapat menambahkan lingkungan antrian menggunakan konsol, atau dengan mengedit template json atau YAMAL secara langsung. Prosedur ini menjelaskan cara membuat lingkungan dengan konsol.

1. Untuk menambahkan lingkungan antrian ke antrian, navigasikan ke antrian dan pilih tab Lingkungan antrian.
2. Pilih Tindakan, lalu Buat baru dengan formulir.
3. Masukkan nama dan deskripsi untuk lingkungan antrian.
4. Pilih Tambahkan variabel lingkungan baru, lalu masukkan nama dan nilai untuk setiap variabel yang Anda tambahkan.
5. (Opsional) Masukkan prioritas untuk lingkungan antrian. Prioritas menunjukkan urutan bahwa lingkungan antrian ini akan berjalan pada pekerja. Lingkungan antrian prioritas yang lebih tinggi akan berjalan terlebih dahulu.

6. Pilih Buat lingkungan antrian.

Default Conda lingkungan antrian

Saat membuat antrian yang terkait dengan armada yang dikelola layanan, Anda memiliki opsi untuk menambahkan lingkungan antrian default yang mendukung Condauntuk mengunduh dan menginstal paket di lingkungan virtual untuk pekerjaan Anda.

Jika Anda menambahkan lingkungan antrian default dengan konsol Deadline Cloud, lingkungan akan dibuat untuk Anda. Jika Anda menambahkan antrian dengan cara lain, seperti AWS CLI atau dengan AWS CloudFormation, Anda harus membuat lingkungan antrian sendiri. Untuk memastikan Anda memiliki konten yang benar untuk lingkungan, Anda dapat merujuk ke file YAMAL template lingkungan antrian. GitHub Untuk konten lingkungan antrian default, lihat file YAMAL lingkungan antrian default aktif. GitHub

Ada templat lingkungan antrian lain yang tersedia GitHub yang dapat Anda gunakan sebagai titik awal untuk kebutuhan Anda sendiri.

Conda menyediakan paket dari saluran. Saluran adalah lokasi di mana paket disimpan. Deadline Cloud menyediakan saluran,`deadline-cloud`, yang menjadi tuan rumah Conda paket yang mendukung aplikasi dan penyaji DCC mitra. Pilih setiap tab di bawah ini untuk melihat paket yang tersedia Linux atau Windows.

Linux

- Blender
  - `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`

- Nuklir
  - `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`

Saat Anda mengirimkan pekerjaan ke antrian dengan default Conda lingkungan, lingkungan menambahkan dua parameter ke pekerjaan. Parameter ini menentukan Conda paket dan saluran yang akan digunakan untuk mengkonfigurasi lingkungan pekerjaan sebelum tugas diproses. Parameternya adalah:

- `CondaPackages`— daftar spesifikasi kecocokan paket yang dipisahkan ruang, seperti `blender=3.6` atau. `numpy>1.22` Defaultnya kosong untuk melewatkan pembuatan lingkungan virtual.
- `CondaChannels`— daftar spasi terpisah dari Conda saluran sepertideadline-cloud,conda-forge, ataus3://*amzn-s3-demo-bucket*/conda/channel. Defaultnya adalahdeadline-

`cloud`, saluran yang tersedia untuk armada yang dikelola layanan yang menyediakan aplikasi dan penyaji DCC mitra.

Saat Anda menggunakan pengirim terintegrasi untuk mengirim pekerjaan ke Deadline Cloud dari DCC Anda, pengirim mengisi nilai `CondaPackages` parameter berdasarkan aplikasi dan pengirim DCC. Misalnya, jika Anda menggunakan Blender `CondaPackage` parameter diatur ke`blender=3.6.* blender-openjd=0.4.*`.

Kami menyarankan Anda menyematkan setiap kiriman hanya ke versi yang tercantum dalam tabel di atas, misalnya blender=3.6. Ini karena rilis patch mempengaruhi paket yang tersedia. Misalnya, ketika kami merilis Blender 3.6.17, kami tidak akan lagi mendistribusikan Blender 3.6.16. Setiap kiriman yang disematkan ke blender=3.6.16 akan gagal. Jika Anda pin ke blender=3.6, maka Anda akan mendapatkan versi patch terdistribusi terbaru dan pekerjaan tidak akan terpengaruh. Secara default, pengirim DCC menyematkan ke versi saat ini yang tercantum dalam tabel di atas, tidak termasuk nomor tambalan, seperti blender = 3.6.

Kaitkan antrian dan armada

Untuk memproses pekerjaan, Anda harus mengaitkan antrian dengan armada. Anda dapat mengaitkan satu armada dengan beberapa antrian dan satu antrian dengan beberapa armada. Ketika Anda mengasosiasikan armada dengan beberapa antrian, itu membagi pekerjanya secara merata di antara mereka. Demikian pula, ketika Anda mengaitkan antrian dengan beberapa armada, itu mendistribusikan pekerjaan secara merata di seluruh armada tersebut. Ikuti langkah-langkah berikut untuk mengaitkan antrian yang ada dengan armada yang ada:

1. Dari Deadline Cloud farm Anda, pilih Antrian yang ingin Anda kaitkan dengan armada. Antrian ditampilkan.
2. Untuk memilih armada yang akan dikaitkan dengan antrian Anda, pilih Armada asosiasi.
3. Pilih dropdown Pilih armada. Daftar tampilan armada yang tersedia.
4. Dari daftar armada yang tersedia, pilih kotak centang di sebelah armada atau armada yang ingin Anda kaitkan dengan antrian Anda.
5. Pilih Kaitkan. Status asosiasi armada sekarang harus Terkait.

Batas waktu Armada Cloud

Bagian ini menjelaskan cara mengelola armada yang dikelola layanan dan armada yang dikelola pelanggan (CMF) untuk Deadline Cloud.

Anda dapat mengatur dua jenis armada Deadline Cloud:

- Armada yang dikelola layanan adalah armada pekerja yang memiliki pengaturan default yang disediakan oleh Deadline Cloud. Pengaturan default ini dirancang agar efisien dan hemat biaya.
- Armada yang dikelola pelanggan (CMFs) memberi Anda kontrol penuh atas saluran pemrosesan Anda. CMF dapat berada di dalam AWS infrastruktur, di tempat, atau di pusat data yang terletak bersama. Ini termasuk penyediaan, operasi, manajemen, dan penonaktifan pekerja di armada.

Ketika Anda mengasosiasikan armada dengan beberapa antrian, ia membagi pekerjanya secara merata di antara antrian tersebut.

Topik

Armada yang dikelola layanan

Service-managed fleet (SMF) adalah armada pekerja yang memiliki pengaturan default yang disediakan oleh Deadline Cloud. Pengaturan default ini dirancang agar efisien dan hemat biaya.

Beberapa pengaturan default membatasi jumlah waktu yang dapat dijalankan oleh pekerja dan tugas. Seorang pekerja hanya dapat berlari selama tujuh hari dan tugas hanya dapat berjalan selama lima hari. Ketika batas tercapai, tugas atau pekerja berhenti. Jika ini terjadi, Anda mungkin kehilangan pekerjaan yang sedang dijalankan oleh pekerja atau tugas. Untuk menghindari hal ini, pantau pekerja dan tugas Anda untuk memastikan mereka tidak melebihi batas durasi maksimum. Untuk mempelajari lebih lanjut tentang memantau pekerja Anda, lihatMenggunakan monitor Deadline Cloud.

Buat armada yang dikelola layanan

1. Dari konsol Deadline Cloud, navigasikan ke peternakan tempat Anda ingin membuat armada.

2. Pilih tab Armada, lalu pilih Buat armada.
3. Masukkan Nama untuk armada Anda.
4. (Opsional) Masukkan Deskripsi. Deskripsi yang jelas dapat membantu Anda mengidentifikasi tujuan armada Anda dengan cepat.
5. Pilih jenis armada yang dikelola layanan.
6. Pilih opsi pasar instans Spot atau On-Demand untuk armada Anda. Instans spot adalah kapasitas tanpa reservasi yang dapat Anda gunakan dengan harga diskon, tetapi dapat terganggu oleh permintaan sesuai permintaan. Instans sesuai permintaan dihargai oleh yang kedua, tetapi tidak memiliki komitmen jangka panjang, dan tidak akan terganggu. Secara default, armada menggunakan instance Spot.
7. Untuk akses layanan armada Anda, pilih peran yang ada atau buat peran baru. Peran layanan memberikan kredensi untuk instance di armada, memberi mereka izin untuk memproses pekerjaan, dan kepada pengguna di monitor sehingga mereka dapat membaca informasi log.
8. Pilih Berikutnya.
9. Pilih antara instance CPU saja atau instans yang dipercepat GPU. Instans yang dipercepat GPU mungkin dapat memproses pekerjaan Anda lebih cepat, tetapi bisa lebih mahal.
10. Pilih sistem operasi untuk pekerja Anda. Anda dapat meninggalkan default, Linux atau memilih Windows.
11. (Opsional) Jika Anda memilih instans yang dipercepat GPU, tetapkan jumlah maksimum dan minimum GPUs di setiap instans. Untuk tujuan pengujian Anda terbatas pada satu GPU. Untuk meminta lebih banyak beban kerja produksi Anda, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.
12. Masukkan vCPU minimum dan maksimum yang Anda butuhkan untuk armada Anda.
13. Masukkan memori minimum dan maksimum yang Anda butuhkan untuk armada Anda.
14. (Opsional) Anda dapat memilih untuk mengizinkan atau mengecualikan jenis instans tertentu dari armada Anda untuk memastikan hanya jenis instans yang digunakan untuk armada ini.
15. (Opsional) Tetapkan jumlah maksimum instans untuk skala armada sehingga kapasitas tersedia untuk pekerjaan dalam antrian. Kami menyarankan Anda meninggalkan jumlah minimum instans di **0** untuk memastikan armada melepaskan semua instance ketika tidak ada pekerjaan yang diantrian.
16. (Opsional) Anda dapat menentukan ukuran volume Amazon Elastic Block Store (Amazon EBS) gp3 yang akan dilampirkan ke pekerja di armada ini. Untuk informasi selengkapnya, lihat panduan pengguna EBS.

17. Pilih Berikutnya.
18. (Opsional) Tentukan kemampuan pekerja khusus yang menentukan fitur armada ini yang dapat digabungkan dengan kemampuan host khusus yang ditentukan pada pengiriman pekerjaan. Salah satu contohnya adalah jenis lisensi tertentu jika Anda berencana untuk menghubungkan armada Anda ke server lisensi Anda sendiri.
19. Pilih Berikutnya.
20. (Opsional) Untuk mengaitkan armada Anda dengan antrian, pilih antrian dari dropdown. Jika antrian diatur dengan lingkungan Conda antrian default, armada Anda secara otomatis dilengkapi dengan paket yang mendukung aplikasi dan perender DCC mitra. Untuk daftar paket yang disediakan, lihatDefault Conda lingkungan antrian.
21. Pilih Berikutnya.
22. (Opsional) Untuk menambahkan tag ke armada Anda, pilih Tambahkan tag baru, lalu masukkan kunci dan nilai untuk tag tersebut.
23. Pilih Berikutnya.
24. Tinjau pengaturan armada Anda, lalu pilih Buat armada.

Gunakan akselerator GPU

Anda dapat mengonfigurasi host pekerja di armada yang dikelola layanan untuk menggunakan satu atau lebih GPUs untuk mempercepat pemrosesan pekerjaan Anda. Menggunakan akselerator dapat mengurangi waktu yang diperlukan untuk memproses pekerjaan, tetapi dapat meningkatkan biaya setiap contoh pekerja. Anda harus menguji beban kerja Anda untuk memahami trade off antara armada menggunakan akselerator GPU dan armada yang tidak.

> **Note**
>
> Untuk tujuan pengujian Anda terbatas pada satu GPU. Untuk meminta lebih banyak beban kerja produksi Anda, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Anda memutuskan apakah armada Anda akan menggunakan akselerator GPU saat Anda menentukan kemampuan instance pekerja. Jika Anda memutuskan untuk menggunakan GPUs, Anda dapat menentukan jumlah minimum dan maksimum GPUs untuk setiap instance, jenis chip GPU yang akan digunakan, dan driver runtime untuk. GPUs

Akselerator GPU yang tersedia adalah:

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

Anda dapat memilih dari driver runtime berikut:

- `Latest`- Gunakan runtime terbaru yang tersedia untuk chip. Jika Anda menentukan `latest` dan versi baru runtime dirilis, versi baru runtime akan digunakan.
- `grid:r570`- Perangkat lunak NVIDIA vGPU 18
- `grid:r550`- Perangkat lunak NVIDIA vGPU 17
- `grid:r535`- Perangkat lunak NVIDIA vGPU 16

Jika Anda tidak menentukan runtime, Deadline Cloud akan digunakan `latest` sebagai default. Namun, jika Anda memiliki beberapa akselerator dan menentukan `latest` untuk beberapa dan membiarkan yang lain kosong, Deadline Cloud memunculkan pengecualian.

Lisensi perangkat lunak untuk armada yang dikelola layanan

Deadline Cloud menyediakan lisensi berbasis penggunaan (UBL) untuk paket perangkat lunak yang umum digunakan. Paket perangkat lunak yang didukung secara otomatis dilisensikan ketika mereka berjalan pada armada yang dikelola layanan. Anda tidak perlu mengkonfigurasi atau memelihara server lisensi perangkat lunak. Skala lisensi sehingga Anda tidak akan kehabisan pekerjaan yang lebih besar.

Anda dapat menginstal paket perangkat lunak yang mendukung UBL menggunakan saluran Conda Cloud Deadline bawaan, atau Anda dapat menggunakan paket Anda sendiri. Untuk informasi selengkapnya tentang saluran conda, lihatBuat lingkungan antrian.

Untuk daftar paket perangkat lunak yang didukung dan informasi tentang harga untuk UBL, lihat Harga AWS Deadline Cloud.

Bawa lisensi Anda sendiri dengan armada yang dikelola layanan

Dengan Deadline Cloud usage-based licensing (UBL) Anda tidak perlu mengelola perjanjian lisensi terpisah dengan vendor perangkat lunak. Namun, jika Anda memiliki lisensi yang ada atau perlu menggunakan perangkat lunak yang tidak tersedia melalui UBL, Anda dapat menggunakan lisensi

perangkat lunak Anda sendiri dengan armada yang dikelola layanan Deadline Cloud Anda. Anda menghubungkan SMF Anda ke server lisensi perangkat lunak melalui internet untuk memeriksa lisensi untuk setiap pekerja di armada.

Untuk contoh menghubungkan ke server lisensi menggunakan proxy, lihat Connect service-managed fleet ke server lisensi kustom di Panduan Pengembang Cloud Deadline.

VFX Reference Platformkompatibilitas

VFX Reference PlatformIni adalah platform target umum untuk industri VFX. Untuk menggunakan EC2 instance Amazon armada terkelola layanan standar yang menjalankan Amazon Linux 2023 dengan perangkat lunak yang mendukungVFX Reference Platform, Anda harus memperhatikan pertimbangan berikut saat menggunakan armada yang dikelola layanan.

VFX Reference PlatformItu diperbarui setiap tahun. Pertimbangan untuk menggunakan AL2 023 termasuk armada yang dikelola layanan Deadline Cloud didasarkan pada tahun kalender (CY) 2022 hingga 2024 Platform Referensi. Untuk informasi selengkapnya, lihat VFX Reference Platform.

> **Note**
>
> Jika Anda membuat custom Amazon Machine Image (AMI) untuk armada yang dikelola pelanggan, Anda dapat menambahkan persyaratan ini saat menyiapkan instans Amazon EC2 .

Untuk menggunakan perangkat lunak yang VFX Reference Platform didukung pada EC2 instans Amazon AL2 023, pertimbangkan hal berikut:

- Versi glibc yang diinstal dengan AL2 023 kompatibel untuk penggunaan runtime, tetapi tidak untuk membangun perangkat lunak yang kompatibel dengan 024 atau sebelumnya. VFX Reference Platform CY2
- Python 3.9 dan 3.11 dilengkapi dengan armada yang dikelola layanan sehingga kompatibel dengan 022 dan 024. VFX Reference Platform CY2 CY2 Python 3.7 dan 3.10 tidak disediakan dalam armada yang dikelola layanan. Perangkat lunak yang membutuhkan mereka harus menyediakan instalasi Python dalam antrian atau lingkungan kerja.
- Beberapa komponen pustaka Boost yang disediakan dalam armada yang dikelola layanan adalah versi 1.75, yang tidak kompatibel dengan file. VFX Reference Platform Jika aplikasi Anda menggunakan Boost, Anda harus menyediakan versi pustaka Anda sendiri untuk kompatibilitas.

- Pembaruan Intel TBB 3 disediakan dalam armada yang dikelola layanan. Ini kompatibel dengan VFX Reference Platform CY2 022, CY2 023, dan CY2 024.
- Pustaka lain dengan versi yang ditentukan oleh tidak VFX Reference Platform disediakan oleh armada yang dikelola layanan. Anda harus menyediakan perpustakaan dengan aplikasi apa pun yang digunakan pada armada yang dikelola layanan. Untuk daftar pustaka, lihat platform referensi.

Armada yang dikelola pelanggan

Ketika Anda ingin menggunakan armada pekerja yang Anda kelola, Anda dapat membuat armada yang dikelola pelanggan (CMF) yang digunakan Deadline Cloud untuk memproses pekerjaan Anda. Gunakan CMF saat:

- Anda memiliki pekerja lokal yang sudah ada untuk diintegrasikan dengan Deadline Cloud.
- Anda memiliki pekerja di pusat data yang berlokasi bersama.
- Anda ingin kontrol langsung dari pekerja Amazon Elastic Compute Cloud (Amazon EC2).

Saat Anda menggunakan CMF, Anda memiliki kendali penuh dan tanggung jawab atas armada. Ini termasuk penyediaan, operasi, manajemen, dan penonaktifan pekerja di armada.

Untuk informasi selengkapnya, lihat Membuat dan menggunakan armada yang dikelola pelanggan Deadline Cloud di Panduan Pengembang Cloud Deadline.

Mengelola pengguna di Deadline Cloud

AWS Deadline Cloud digunakan AWS IAM Identity Center untuk mengelola pengguna dan grup. IAM Identity Center adalah layanan single sign-on berbasis cloud yang dapat diintegrasikan dengan penyedia single-sign on (SSO) perusahaan Anda. Dengan integrasi, pengguna dapat masuk dengan akun perusahaan mereka.

Deadline Cloud mengaktifkan IAM Identity Center secara default, dan diperlukan untuk mengatur dan menggunakan Deadline Cloud. Untuk informasi selengkapnya, lihat Mengelola sumber identitas Anda.

Pemilik organisasi untuk Anda AWS Organizations bertanggung jawab untuk mengelola pengguna dan grup yang memiliki akses ke monitor Deadline Cloud Anda. Anda dapat membuat dan mengelola pengguna dan grup ini menggunakan IAM Identity Center atau konsol Deadline Cloud. Untuk informasi lebih lanjut, lihat Apa yang dimaksud dengan AWS Organizations.

Anda membuat dan menghapus pengguna dan grup yang dapat mengelola farm, antrian, dan armada menggunakan konsol Deadline Cloud. Ketika Anda menambahkan pengguna ke Deadline Cloud, mereka harus mengatur ulang kata sandi mereka menggunakan IAM Identity Center sebelum mereka mendapatkan akses.

Topik

Kelola pengguna dan grup untuk monitor

Pemilik Organizations dapat menggunakan konsol Deadline Cloud untuk mengelola pengguna dan grup yang memiliki akses ke monitor Deadline Cloud. Anda dapat memilih dari pengguna dan grup Pusat Identitas IAM yang ada, atau Anda dapat menambahkan pengguna dan grup baru dari konsol.

1. Masuk ke AWS Management Console dan buka konsol Deadline Cloud. Dari halaman utama, di bagian Memulai, pilih Atur Batas Waktu Cloud atau Buka dasbor.
2. Di panel navigasi kiri, pilih Manajemen pengguna. Secara default, tab Grup dipilih.

Bergantung pada tindakan yang akan diambil, pilih tab Grup atau tab Pengguna.

Groups

Untuk membuat grup

1. Pilih Buat grup.
2. Masukkan nama grup. Nama harus unik di antara kelompok-kelompok di organisasi Pusat Identitas IAM Anda.

Untuk menghapus grup

1. Pilih grup yang akan dihapus.
2. Pilih Hapus.
3. Dalam dialog konfirmasi, pilih Hapus grup.

> **Note**
>
> Anda menghapus grup dari IAM Identity Center. Anggota grup tidak dapat lagi masuk ke Deadline Cloud atau mengakses sumber daya pertanian.

Users

Untuk menambahkan pengguna

1. Pilih tab Pengguna.
2. Pilih Add Users (Tambahkan pengguna).
3. Masukkan nama, alamat email, dan nama pengguna untuk pengguna baru.
4. (Opsional) Pilih satu atau beberapa grup Pusat Identitas IAM untuk menambahkan pengguna baru.
5. Pilih Kirim undangan untuk mengirim email kepada pengguna baru dengan instruksi untuk bergabung dengan organisasi Pusat Identitas IAM Anda.

Untuk menghapus pengguna

1. Pilih pengguna yang akan Anda hapus.
2. Pilih Hapus.

3. Dalam dialog konfirmasi, pilih Hapus pengguna.

> **Note**
>
> Anda menghapus pengguna dari IAM Identity Center. Pengguna tidak dapat lagi masuk ke monitor Deadline Cloud atau mengakses sumber daya pertanian.

Kelola pengguna dan grup untuk peternakan, antrian, dan armada

Sebagai bagian dari mengelola pengguna dan grup, Anda dapat memberikan izin akses pada tingkat yang berbeda. Setiap level berikutnya mencakup izin untuk level sebelumnya. Daftar berikut menjelaskan empat tingkat akses dari tingkat terendah ke tingkat tertinggi:

- Penampil — Izin untuk melihat sumber daya di peternakan, antrian, armada, dan pekerjaan yang dapat mereka akses. Penampil tidak dapat mengirimkan atau membuat perubahan pada pekerjaan.
- Kontributor — Sama seperti pemirsa, tetapi dengan izin untuk mengirimkan pekerjaan ke antrian atau peternakan.
- Manajer — Sama seperti kontributor, tetapi dengan izin untuk mengedit pekerjaan dalam antrian yang dapat mereka akses, dan memberikan izin pada sumber daya yang dapat mereka akses.
- Pemilik — Sama seperti manajer, tetapi dapat melihat dan membuat anggaran dan melihat penggunaan.

> **Note**
>
> Perubahan izin akses dapat memakan waktu hingga 10 menit untuk tercermin dalam sistem.

1. Jika Anda belum melakukannya, masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Di panel navigasi kiri, pilih Peternakan dan sumber daya lainnya.
3. Pilih peternakan untuk dikelola. Pilih nama pertanian untuk membuka halaman detail. Anda dapat mencari peternakan menggunakan bilah pencarian.
4. Untuk mengelola antrian atau armada, pilih tab Antrian atau Armada, lalu pilih antrian atau armada yang akan dikelola.

5. Pilih tab Manajemen akses. Secara default, tab Grup dipilih. Untuk mengelola pengguna, pilih Pengguna.

Bergantung pada tindakan yang akan diambil, pilih tab Grup atau tab Pengguna.

Groups

Untuk menambahkan grup

1. Pilih sakelar Grup.
2. Pilih Tambah grup.
3. Dari dropdown, pilih grup yang akan ditambahkan.
4. Untuk tingkat akses grup, pilih salah satu opsi berikut:
   - Penampil
   - Kontributor
   - Manajer
   - Pemilik
5. Pilih Tambahkan.

Untuk menghapus grup

1. Pilih grup yang akan dihapus.
2. Pilih Hapus.
3. Dalam dialog konfirmasi, pilih Hapus grup.

Users

Untuk menambahkan pengguna

1. Untuk menambahkan pengguna, pilih Tambah pengguna.
2. Dari dropdown, pilih pengguna yang akan ditambahkan.
3. Untuk tingkat akses pengguna, pilih salah satu opsi berikut:
   - Penampil
   - Kontributor

- Manajer
- Pemilik

4. Pilih Tambahkan.

Untuk menghapus pengguna

1. Pilih pengguna yang akan dihapus.
2. Pilih Hapus.
3. Dalam dialog konfirmasi, pilih Hapus pengguna.

Lowongan kerja Deadline Cloud

Pekerjaan adalah serangkaian instruksi yang digunakan AWS Deadline Cloud untuk menjadwalkan dan menjalankan pekerjaan pada pekerja yang tersedia. Saat Anda membuat pekerjaan, Anda memilih pertanian dan antrian untuk mengirim pekerjaan.

Submitter adalah plugin untuk aplikasi pembuatan konten digital (DCC) Anda yang mengelola pembuatan pekerjaan di antarmuka aplikasi DCC Anda. Setelah Anda membuat pekerjaan, Anda menggunakan pengirim mengirimkannya ke Deadline Cloud untuk diproses.

Submitter membuat template Open Job Specification (OpenJD) yang menjelaskan pekerjaan. Pada saat yang sama, ia mengunggah file aset Anda ke bucket Amazon Simple Storage Service (Amazon S3). Untuk mengurangi waktu unggah, pengirim hanya mengirim file yang telah berubah sejak unggahan terakhir ke Amazon S3

Anda juga dapat membuat pekerjaan dengan cara berikut.

- Dari terminal — untuk pengguna mengirimkan pekerjaan yang nyaman menggunakan baris perintah.
- Dari skrip - untuk menyesuaikan dan mengotomatiskan beban kerja.
- Dari aplikasi — untuk saat pekerjaan pengguna berada dalam aplikasi, atau ketika konteks aplikasi penting.

Untuk informasi selengkapnya, lihat Cara mengirimkan lowongan ke Deadline Cloud di Panduan Pengembang Cloud Deadline.

Pekerjaan terdiri dari:

- Prioritas — Perkiraan urutan Deadline Cloud memproses pekerjaan dalam antrian. Anda dapat mengatur prioritas pekerjaan antara 0 dan 100, pekerjaan dengan prioritas angka yang lebih tinggi umumnya diproses terlebih dahulu. Pekerjaan dengan prioritas yang sama diproses dalam urutan yang diterima.
- Langkah - Mendefinisikan skrip untuk dijalankan pada pekerja. Langkah-langkah dapat memiliki persyaratan seperti memori pekerja minimum atau langkah-langkah lain yang perlu diselesaikan terlebih dahulu. Setiap langkah memiliki satu atau lebih tugas.

- Tugas — Unit kerja yang dikirim ke pekerja untuk melakukan. Tugas adalah kombinasi skrip dan parameter langkah, seperti nomor bingkai, yang digunakan dalam skrip. Pekerjaan selesai ketika semua tugas selesai untuk semua langkah.
- Lingkungan - Siapkan dan hancurkan instruksi yang dibagikan oleh beberapa langkah atau tugas.

Menggunakan submitter Deadline Cloud

Submitter adalah alat yang terintegrasi dengan pembuatan konten digital Anda sehingga Anda dapat mengirim pekerjaan render langsung ke Deadline Cloud. Integrasi ini merampingkan alur kerja Anda dengan menghilangkan kebutuhan untuk beralih antar aplikasi atau mentransfer file secara manual. Ini menghemat waktu dan mengurangi potensi kesalahan.

Pengirim tersedia untuk banyak aplikasi DCC populer. Menginstal submitter, menambahkan opsi khusus Deadline Cloud ke antarmuka aplikasi Anda, biasanya di pengaturan render atau menu ekspor.

Dengan submitter Deadline Cloud Anda dapat:

- Konfigurasikan parameter pekerjaan render di lingkungan DCC yang Anda kenal
- Kirim pekerjaan ke Deadline Cloud tanpa meninggalkan aplikasi Anda
- Mengurangi potensi kesalahan yang terkait dengan transfer file manual
- Hemat waktu karena Anda tidak perlu beralih antar aplikasi

Untuk menemukan pengirim aplikasi DCC Anda, periksa daftar pengirim yang didukung. Kemudian ikuti instruksi Mengatur Deadline Pengirim Cloud untuk menginstal pengirim.

Jika aplikasi Anda tidak memiliki pengirim yang didukung, Anda masih dapat menjalankan pekerjaan untuk aplikasi Anda. Mungkin ada contoh bundel pekerjaan yang tersedia untuk itu, atau Anda dapat membuat pengirim sederhana untuk perintah CLI render aplikasi. Untuk informasi selengkapnya, lihat template Open Job Description (OpenJD) untuk Deadline Cloud di Panduan Pengembangan Cloud Deadline.

Contoh dalam topik ini menggunakan Blender pengirim, tetapi langkah-langkah untuk menggunakan pengirim lain serupa.

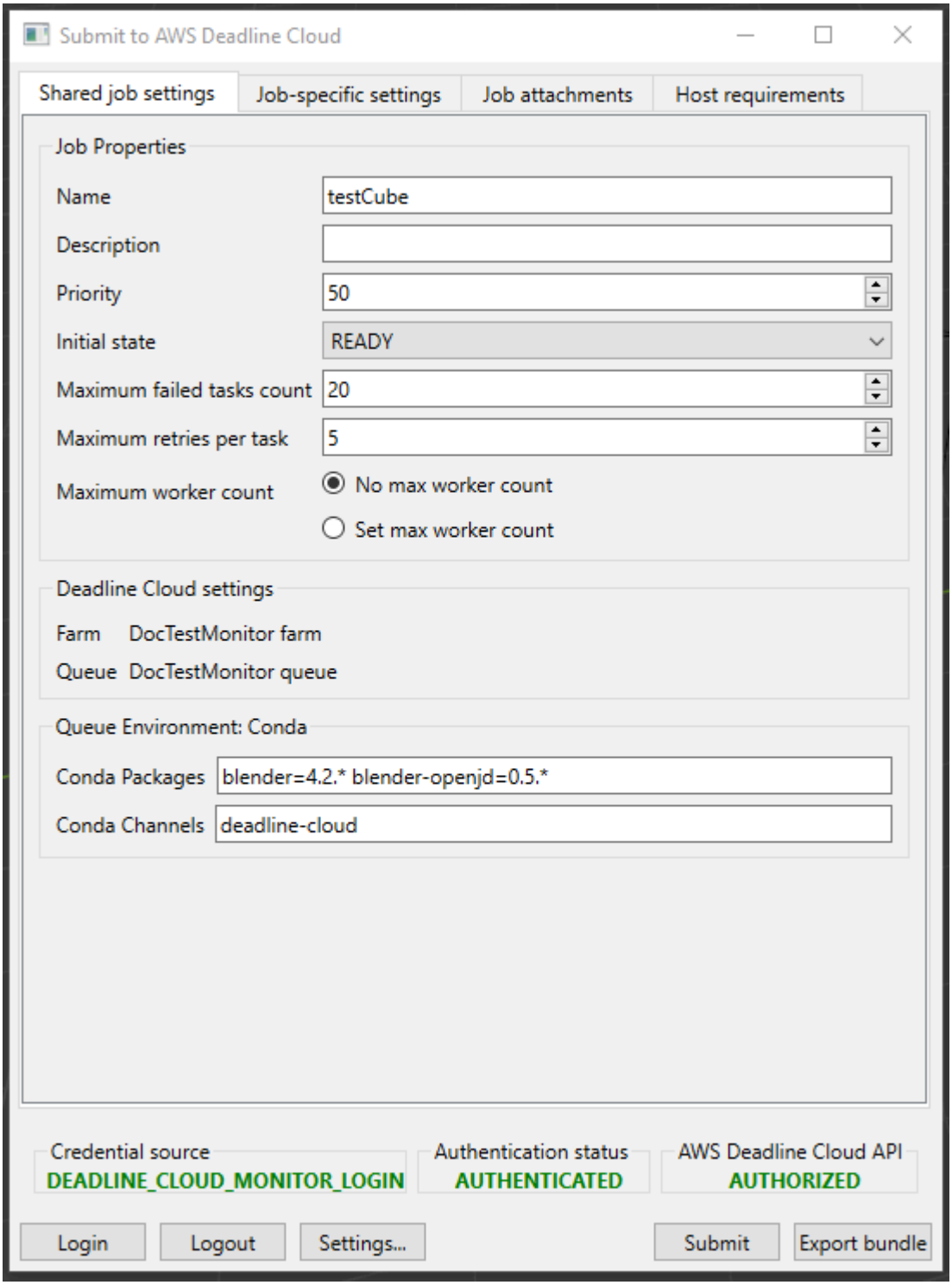
> **Note**
>
> Untuk menggunakan submitter, Anda harus masuk ke monitor Deadline Cloud.

Pengirim memiliki empat tab:

Topik

- Tab pengaturan pekerjaan bersama
- Tab pengaturan khusus pekerjaan
- Tab lampiran Job
- Tab persyaratan host

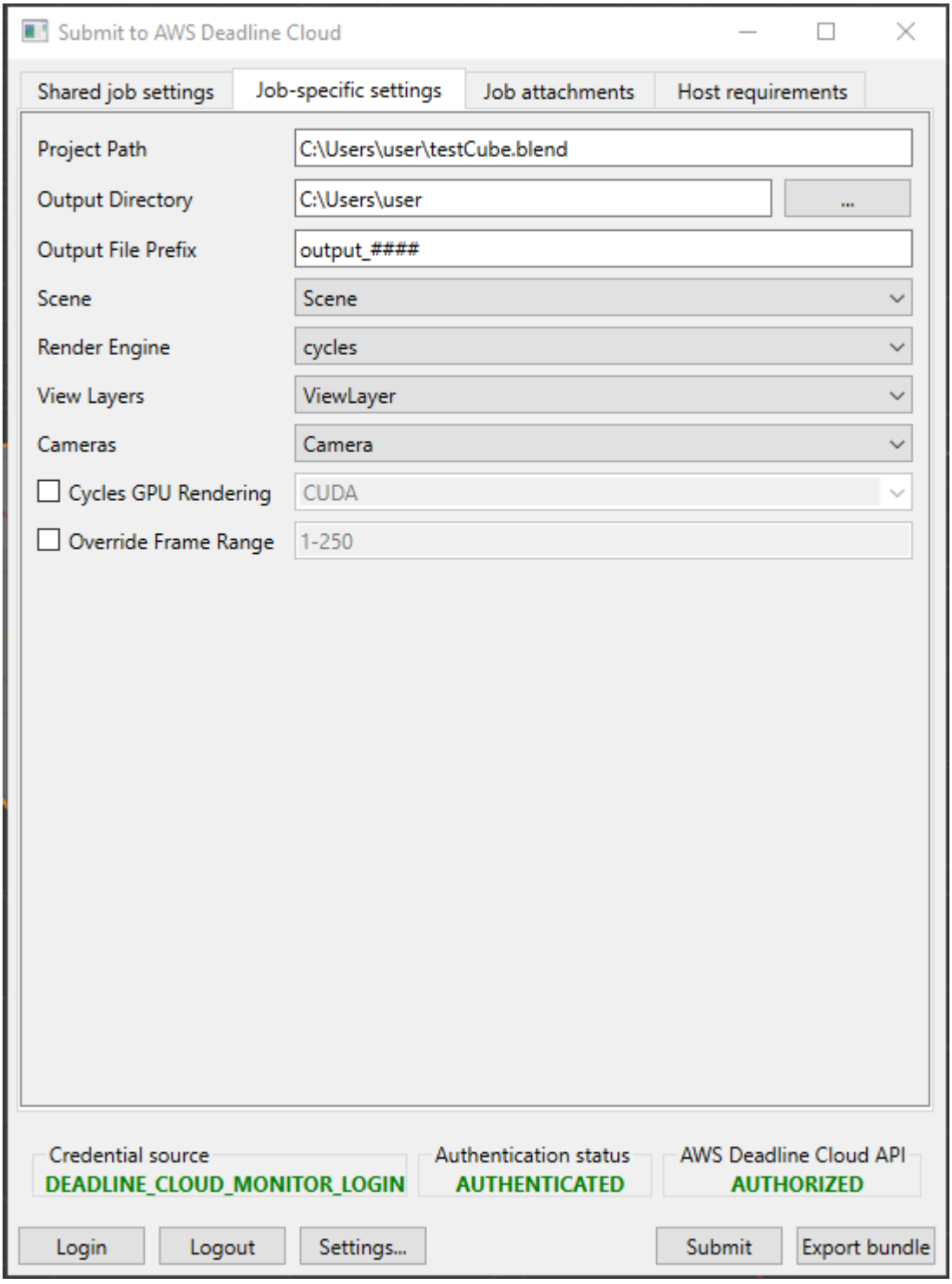
Tab pengaturan pekerjaan bersama



Tab pengaturan pekerjaan bersama berisi pengaturan yang umum untuk semua pekerjaan yang dikirim ke Deadline Cloud menggunakan pengirim. Tiga bagian tersebut adalah:

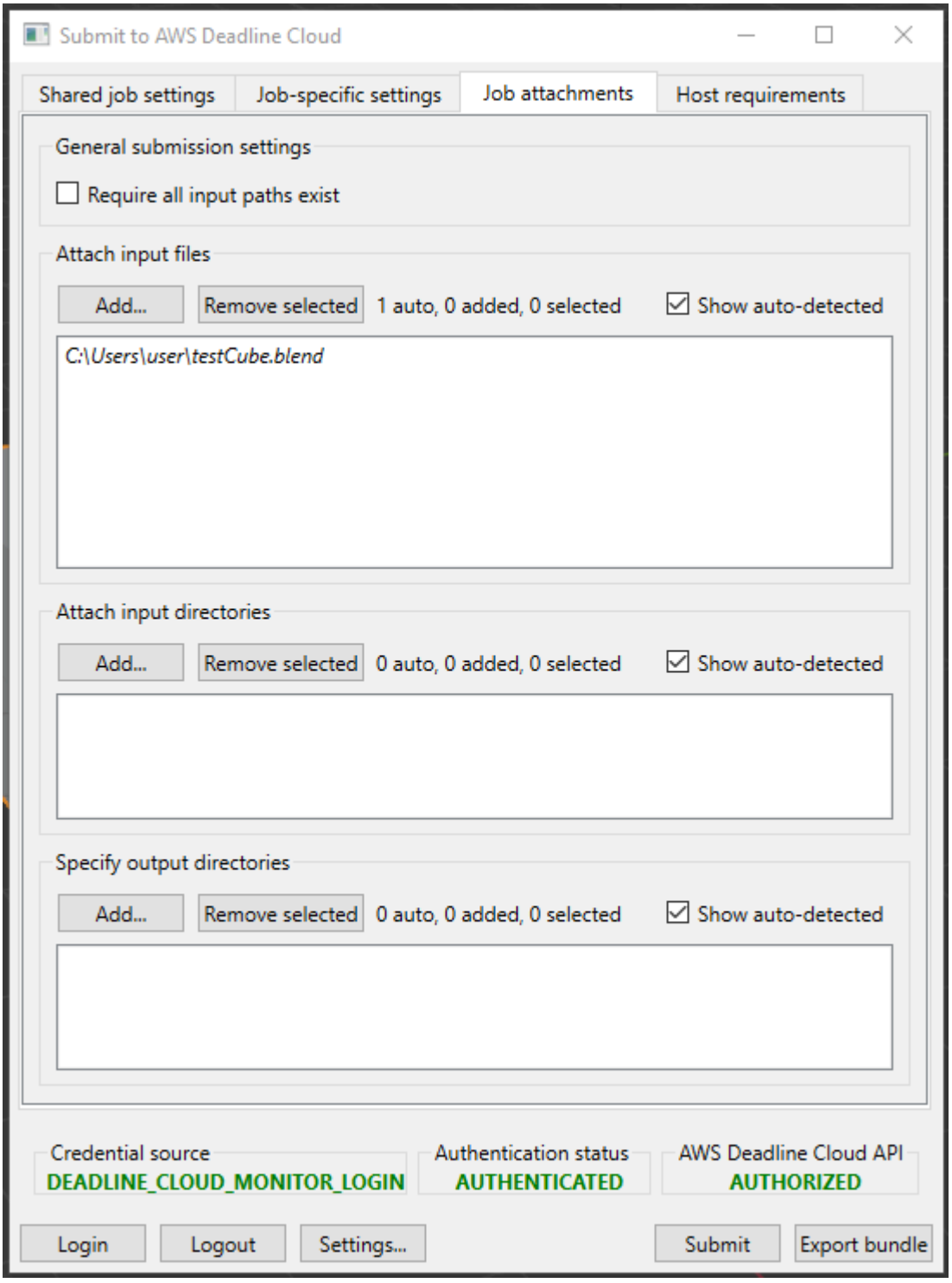
- Properti Job - Menetapkan properti keseluruhan pekerjaan. Properti ini hadir di pengirim untuk semua aplikasi DCC.
- Pengaturan Deadline Cloud — Menampilkan pertanian dan antrian tempat pekerjaan dikirim. Untuk mengubah pertanian dan antrian, gunakan Pengaturan... tombol di bagian bawah pengirim.
- Lingkungan antrian - Menetapkan nilai parameter yang ditentukan dalam lingkungan antrian. Deadline Cloud menambahkan nilai parameter default untuk aplikasi DCC Anda, Anda dapat menambahkan nilai tambahan jika perlu.

Tab pengaturan khusus pekerjaan



Tab pengaturan khusus pekerjaan berisi pengaturan khusus untuk aplikasi DCC Anda. Tentukan pengaturan ini berdasarkan opsi yang tersedia di aplikasi Anda.

Tab lampiran Job

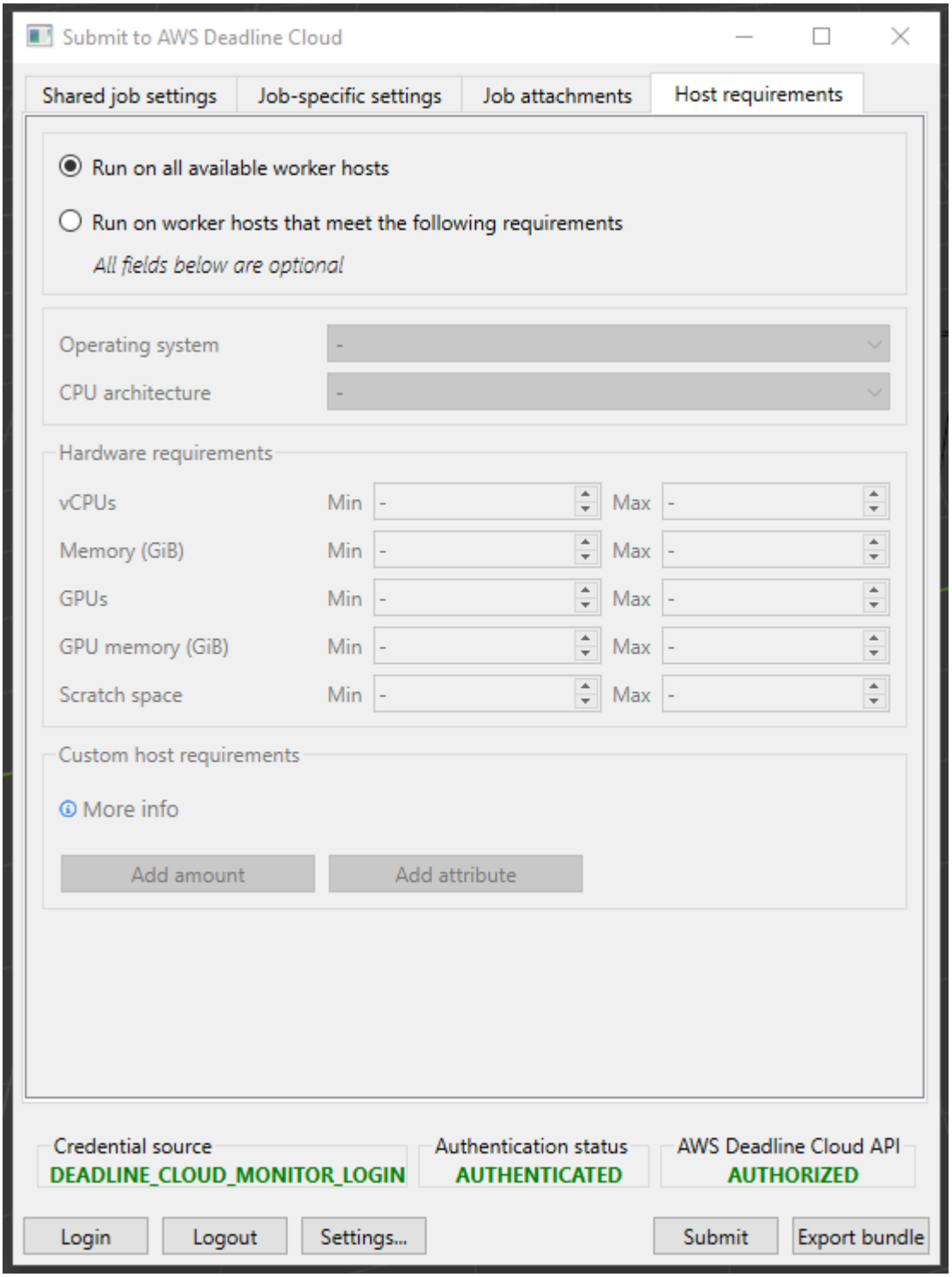


Tab lampiran pekerjaan menunjukkan semua file yang diperlukan untuk menyelesaikan render. Submitter mencoba untuk menemukan semua file yang diperlukan untuk render. File yang diidentifikasi muncul dalam daftar dengan huruf miring.

Anda dapat menambahkan file input dan direktori tambahan yang berisi aset lain yang diperlukan untuk render yang tidak terdeteksi secara otomatis.

Jika pekerjaan Anda menulis file ke beberapa direktori output, Anda harus menentukan direktori di sini sehingga merupakan bagian dari download pekerjaan.

Tab persyaratan host



Tab persyaratan host menetapkan kemampuan armada yang diperlukan untuk memproses pekerjaan. Kemampuan ditentukan untuk seluruh armada, bukan pekerja individu dalam armada.

Jika antrian Anda memiliki batas sumber daya terkait, gunakan tombol Tambah jumlah untuk menentukan batas. Untuk informasi selengkapnya, lihat Membuat batas sumber daya untuk lowongan

Lowongan kerja Processing Deadline Cloud

Ketika pekerjaan memasuki antrian, Deadline Cloud menjadwalkannya pada satu atau lebih armada yang terkait dengan antrian. Armada dipilih berdasarkan kemampuan yang dikonfigurasi untuk armada dan persyaratan tuan rumah dari langkah tertentu. Jika pekerjaan memiliki persyaratan yang tidak dapat dipenuhi oleh salah satu armada yang terkait dengan antrian, status pekerjaan diatur ke “Tidak kompatibel” dan langkah-langkah lainnya dalam pekerjaan dibatalkan.

Selanjutnya, Deadline Cloud mengirimkan instruksi kepada pekerja untuk mengatur sesi untuk langkah tersebut. Perangkat lunak yang diperlukan untuk langkah tersebut harus tersedia pada instance pekerja agar pekerjaan dapat dijalankan. Layanan membuka sesi pada beberapa pekerja jika pengaturan penskalaan armada memungkinkan.

Anda dapat mengatur perangkat lunak di Amazon Machine Image (AMI), atau pekerja Anda dapat memuat perangkat lunak saat runtime dari repositori atau manajer paket. Anda dapat menggunakan lingkungan antrian, pekerjaan, atau langkah untuk menyebarkan perangkat lunak yang Anda inginkan.

Layanan Deadline Cloud menggunakan template OpenJD untuk mengidentifikasi langkah-langkah yang diperlukan untuk pekerjaan itu, dan tugas yang diperlukan untuk setiap langkah. Beberapa langkah memiliki ketergantungan pada langkah lain, jadi Deadline Cloud menentukan urutan untuk menyelesaikan langkah-langkah tersebut. Kemudian, Deadline Cloud mengirimkan tugas untuk setiap langkah ke pekerja untuk diproses. Ketika tugas selesai, layanan mengirimkan tugas lain dalam sesi yang sama, atau pekerja dapat memulai sesi baru.

Setelah semua tugas di setiap langkah selesai, pekerjaan selesai dan output siap diunduh ke workstation Anda. Bahkan jika pekerjaan tidak selesai, output dari setiap langkah dan tugas yang selesai tersedia untuk diunduh.

> **Note**
>
> Deadline Cloud menghapus pekerjaan 120 hari setelah diserahkan. Ketika pekerjaan dihapus, semua langkah dan tugas yang terkait dengan pekerjaan juga dihapus. Jika Anda perlu menjalankan kembali pekerjaan, kirimkan template OpenJD untuk pekerjaan itu lagi.

Lowongan kerja Monitoring Deadline Cloud

Monitor AWS Deadline Cloud memberi Anda gambaran keseluruhan tentang pekerjaan Anda. Gunakan untuk:

- Memantau dan mengelola pekerjaan
- Lihat aktivitas pekerja di armada
- Lacak anggaran dan penggunaan
- Unduh hasil pekerjaan.

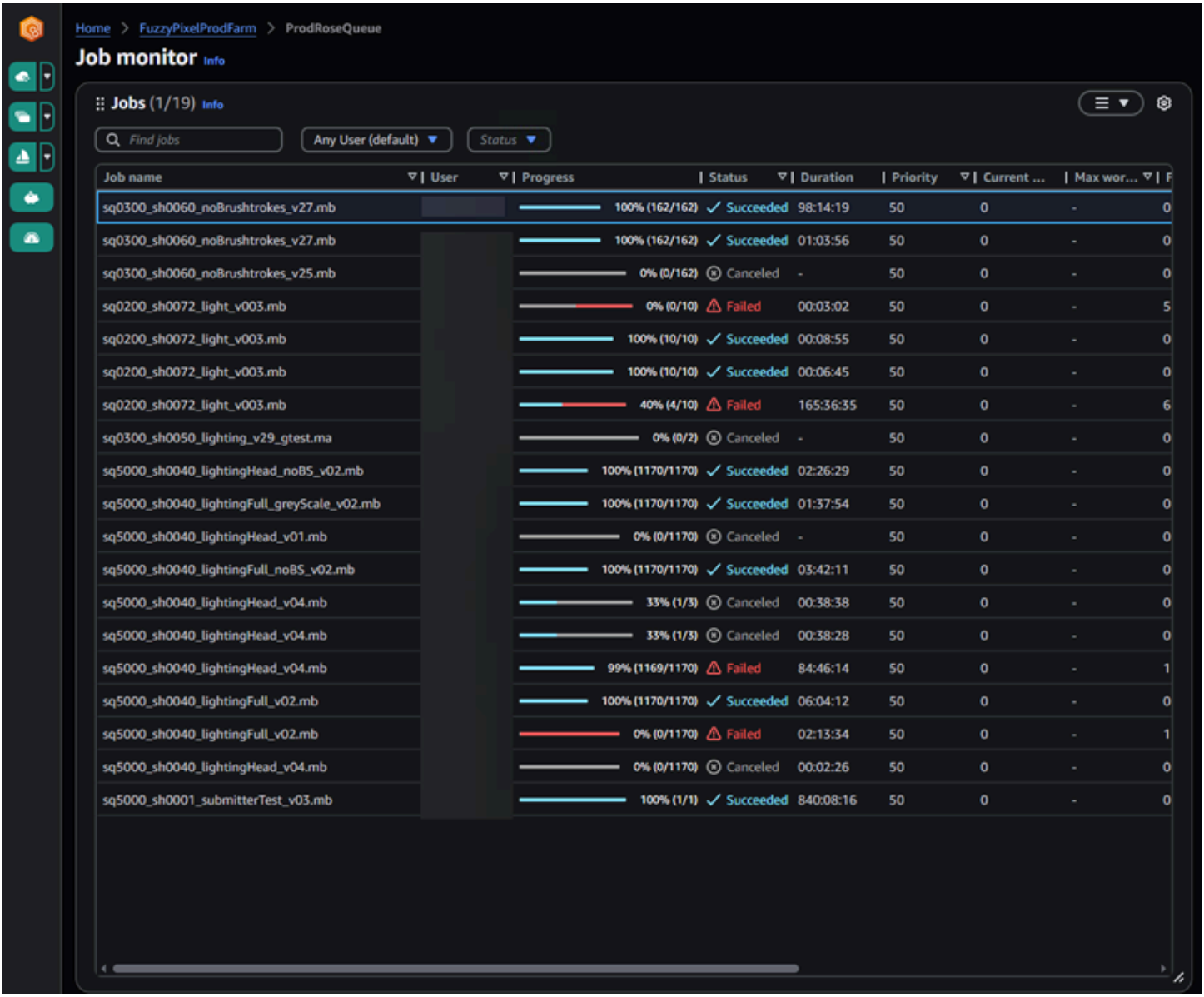
Untuk memantau pekerjaan tertentu, pilih pertanian dan antrian yang berisi pekerjaan, lalu pilih pekerjaan dari daftar. Anda dapat menggunakan kotak pencarian untuk menemukan pekerjaan atau pekerjaan tertentu dalam antrian.

Klik kanan pada pekerjaan, langkah, atau tugas untuk melihat opsi untuk item tersebut. Anda dapat:

- Ubah status
- Tangguhkan dan lanjutkan item
- Meminta ulang item
- Unduh outputnya
- Untuk tugas: Lihat log tugas dan pekerja.

Untuk informasi selengkapnya, lihat Menggunakan monitor Deadline Cloud.

Setiap tugas dalam pekerjaan atau langkah memiliki status. Status pekerjaan atau langkah tergantung pada status tugasnya. Status ditentukan oleh tugas-tugas yang memiliki status ini, secara berurutan. Status langkah ditentukan sama dengan status pekerjaan.



Daftar berikut menjelaskan status:

`NOT_COMPATIBLE`

Pekerjaan itu tidak kompatibel dengan pertanian karena tidak ada armada yang dapat menyelesaikan salah satu tugas dalam pekerjaan itu.

`RUNNING`

Satu atau lebih pekerja menjalankan tugas dari pekerjaan itu. Selama setidaknya ada satu tugas yang berjalan, pekerjaan itu ditandai`RUNNING`.

`ASSIGNED`

Satu atau lebih pekerja diberi tugas dalam pekerjaan sebagai tindakan mereka selanjutnya. Lingkungan, jika ada, sudah diatur.

`STARTING`

Satu atau lebih pekerja sedang menyiapkan lingkungan untuk menjalankan tugas.

`SCHEDULED`

Tugas untuk pekerjaan dijadwalkan pada satu atau lebih pekerja sebagai tindakan pekerja selanjutnya.

`READY`

Setidaknya satu tugas untuk pekerjaan itu siap diproses.

`INTERRUPTING`

Setidaknya satu tugas dalam pekerjaan sedang terganggu. Gangguan dapat terjadi ketika Anda memperbarui status pekerjaan secara manual. Ini juga dapat terjadi sebagai respons terhadap gangguan karena perubahan harga Spot Amazon Elastic Compute Cloud EC2 (Amazon).

`FAILED`

Satu atau lebih tugas dalam pekerjaan itu tidak berhasil diselesaikan.

`CANCELED`

Satu atau lebih tugas dalam pekerjaan telah dibatalkan.

`SUSPENDED`

Setidaknya satu tugas dalam pekerjaan telah ditangguhkan.

`PENDING`

Tugas dalam pekerjaan sedang menunggu ketersediaan sumber daya lain.

`SUCCEEDED`

Semua tugas dalam pekerjaan berhasil diproses.

Penyimpanan file untuk Deadline Cloud

Pekerja harus memiliki akses ke lokasi penyimpanan yang berisi file input yang diperlukan untuk memproses pekerjaan, dan ke lokasi yang menyimpan output. AWS Deadline Cloud menyediakan dua opsi untuk lokasi penyimpanan:

- Dengan lampiran pekerjaan, Deadline Cloud mentransfer file input dan output untuk pekerjaan Anda bolak-balik antara workstation dan pekerja Deadline Cloud. Untuk mengaktifkan transfer file, Deadline Cloud menggunakan bucket Amazon Simple Storage Service (Amazon S3) di bucket Anda. Akun AWS

  Saat Anda menggunakan lampiran pekerjaan dengan armada yang dikelola layanan, Anda dapat mengatur sistem file virtual (VFS) di jaringan pribadi virtual (VPN) Anda. Kemudian pekerja dapat memuat file hanya bila diperlukan.
- Dengan penyimpanan bersama, Anda menggunakan berbagi file dengan sistem operasi Anda untuk menyediakan akses ke file.

  Saat Anda menggunakan penyimpanan bersama lintas platform, Anda dapat membuat profil penyimpanan sehingga pekerja dapat memetakan jalur ke file di antara dua sistem operasi yang berbeda.

Topik

Lampiran Job di Deadline Cloud

Lampiran Job memungkinkan Anda mentransfer file bolak-balik antara workstation dan AWS Deadline Cloud. Dengan lampiran pekerjaan, Anda tidak perlu menyiapkan bucket Amazon S3 secara manual untuk file Anda. Sebagai gantinya, saat membuat antrian dengan konsol Deadline Cloud, Anda memilih bucket untuk lampiran pekerjaan Anda.

Pertama kali Anda mengirimkan pekerjaan ke Deadline Cloud, semua file untuk pekerjaan tersebut ditransfer ke Deadline Cloud. Untuk pengiriman berikutnya, hanya file yang telah berubah ditransfer, menghemat waktu dan bandwidth.

Setelah pemrosesan selesai, Anda dapat mengunduh hasilnya dari halaman detail pekerjaan, atau dengan menggunakan perintah Deadline Cloud `deadline job download-output` CLI.

Anda dapat menggunakan bucket S3 yang sama untuk beberapa antrian. Tetapkan awalan root yang berbeda untuk setiap antrian untuk mengatur lampiran di bucket.

Saat membuat antrian dengan konsol, Anda dapat memilih peran AWS Identity and Access Management (IAM) yang sudah ada atau membuat konsol membuat peran baru. Jika konsol membuat peran, konsol akan menetapkan izin untuk mengakses bucket yang ditentukan untuk antrian. Jika memilih peran yang ada, Anda harus memberikan izin peran untuk mengakses bucket S3.

Enkripsi untuk bucket S3 lampiran pekerjaan

File lampiran Job dienkripsi di bucket S3 Anda secara default. Ini membantu mengamankan informasi Anda dari akses yang tidak sah. Anda tidak perlu melakukan apa pun agar file Anda dienkripsi dengan kunci yang disediakan oleh Deadline Cloud. Untuk informasi selengkapnya, lihat Amazon S3 sekarang secara otomatis mengenkripsi semua objek baru di Panduan Pengguna Amazon S3.

Anda dapat menggunakan AWS Key Management Service kunci yang dikelola pelanggan Anda sendiri untuk mengenkripsi bucket S3 yang berisi lampiran pekerjaan Anda. Untuk melakukannya, Anda harus mengubah peran IAM untuk antrian yang terkait dengan bucket agar memungkinkan akses ke. AWS KMS key

Untuk membuka editor kebijakan IAM untuk peran antrian

1. Masuk ke AWS Management Console dan buka konsol Deadline Cloud. Dari halaman utama, di bagian Memulai, pilih Lihat peternakan.
2. Dari daftar peternakan, pilih peternakan yang berisi antrian untuk dimodifikasi.
3. Dari daftar antrian, pilih antrian yang akan dimodifikasi.
4. Di bagian Detail antrian, pilih peran Layanan untuk membuka konsol IAM untuk peran layanan.

Selanjutnya, selesaikan prosedur berikut.

Untuk memperbarui kebijakan peran dengan izin AWS KMS

1. Dari daftar kebijakan Izin, pilih kebijakan untuk peran tersebut.
2. Di bagian Izin yang ditentukan di bagian kebijakan ini, pilih Edit.
3. Pilih Tambahkan pernyataan baru.
4. Salin dan tempel kebijakan berikut ke editor. Ubah *Region*,*accountID*, dan *keyID* nilai-nilai Anda sendiri.

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

5. Pilih Berikutnya.
6. Tinjau perubahan pada kebijakan, lalu setelah puas, pilih Simpan perubahan.

Mengelola lampiran pekerjaan di bucket S3

Deadline Cloud menyimpan file lampiran pekerjaan yang diperlukan untuk pekerjaan Anda di bucket S3. File-file ini terakumulasi dari waktu ke waktu, yang menyebabkan peningkatan biaya Amazon S3. Untuk mengurangi biaya, Anda dapat menerapkan konfigurasi Siklus Hidup S3 ke bucket S3 Anda. Konfigurasi ini dapat secara otomatis menghapus file di bucket. Karena bucket S3 ada di akun Anda, Anda dapat memilih untuk memodifikasi atau menghapus konfigurasi Siklus Hidup S3 kapan saja. Untuk informasi selengkapnya, lihat Contoh konfigurasi Siklus Hidup S3 di Panduan Pengguna Amazon S3.

Untuk solusi manajemen bucket S3 yang lebih terperinci, Anda dapat mengatur objek yang Akun AWS kedaluwarsa dalam bucket S3 berdasarkan waktu terakhir mereka diakses. Untuk informasi selengkapnya, lihat Objek Amazon S3 kedaluwarsa berdasarkan tanggal akses terakhir untuk mengurangi biaya di AWS Blog Arsitektur.

Tenggat waktu Cloud sistem file virtual

Dukungan sistem file virtual untuk lampiran pekerjaan di AWS Deadline Cloud memungkinkan perangkat lunak klien pada pekerja untuk berkomunikasi langsung dengan Amazon Simple Storage Service. Pekerja dapat memuat file hanya bila diperlukan alih-alih mengunduh semua file sebelum diproses. File disimpan secara lokal. Pendekatan ini menghindari pengunduhan aset yang digunakan lebih dari sekali beberapa kali. Semua file dihapus setelah pekerjaan selesai.

- Sistem file virtual memberikan peningkatan kinerja yang signifikan untuk profil pekerjaan tertentu. Secara umum, himpunan bagian yang lebih kecil dari total file dengan armada pekerja yang lebih besar menunjukkan manfaat paling besar. Sejumlah kecil file dengan lebih sedikit pekerja memiliki waktu pemrosesan yang kira-kira setara.
- Dukungan sistem file virtual hanya tersedia untuk Linux pekerja di armada yang dikelola layanan.
- Sistem file virtual Deadline Cloud mendukung operasi berikut, tetapi tidak sesuai dengan POSIX:
  - File`create`,,,,`delete`,,`open`,,`close`,,,`read`,,`write`,,`append`,,`truncate`,,`rename`,,,`move`,,`copy`,,`stat` `falloc`
  - Direktori `createdelete`,`rename`,,`move`,`copy`, dan `stat`
- Sistem file virtual dirancang untuk mengurangi transfer data dan meningkatkan kinerja ketika tugas Anda hanya mengakses sebagian dari kumpulan data besar, dan tidak dioptimalkan untuk semua beban kerja. Anda harus menguji beban kerja Anda sebelum menjalankan pekerjaan produksi.

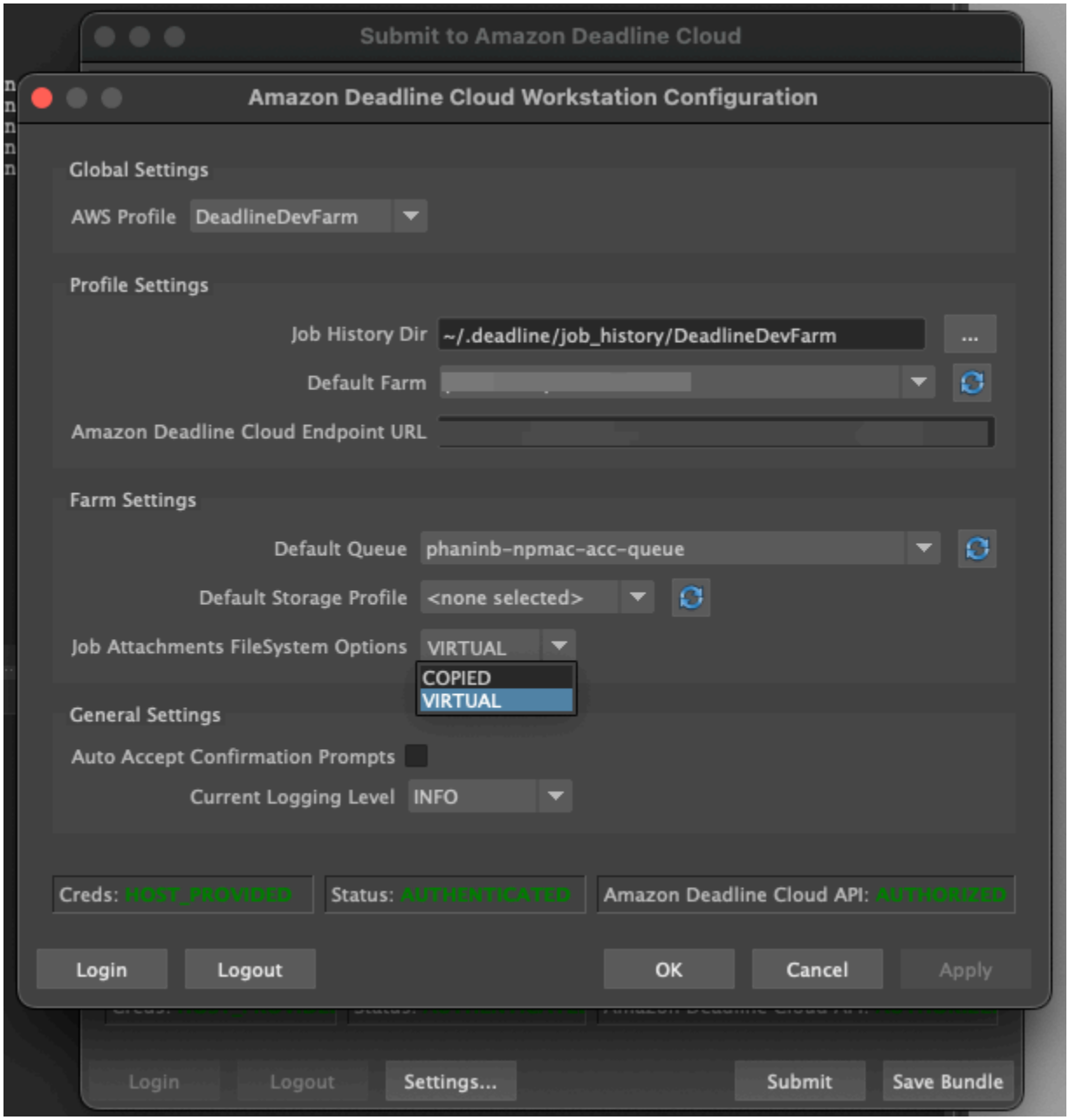
Aktifkan dukungan VFS

Dukungan sistem file virtual (VFS) diaktifkan untuk setiap pekerjaan. Pekerjaan kembali ke kerangka kerja lampiran pekerjaan default dalam kasus ini:

- Profil instance pekerja tidak mendukung sistem file virtual.
- Masalah mencegah peluncuran proses sistem file virtual.
- Sistem file virtual tidak dapat dipasang.

Untuk mengaktifkan dukungan sistem file virtual menggunakan submitter

1. Saat mengirimkan pekerjaan, pilih tombol Pengaturan untuk membuka panel konfigurasi workstation AWS Deadline Cloud.
2. Dari tarik-turun opsi sistem file lampiran Job, pilih VIRTUAL.



3. Untuk menyimpan perubahan Anda, pilih OK.

Untuk mengaktifkan dukungan sistem file virtual menggunakan AWS CLI

- Gunakan perintah berikut saat Anda mengirimkan pekerjaan yang disimpan:

```
deadline bundle submit-job --job-attachments-file-system VIRTUAL
```

Untuk memverifikasi bahwa sistem file virtual berhasil diluncurkan untuk pekerjaan tertentu, tinjau log Anda di Amazon CloudWatch Logs. Cari pesan-pesan berikut:

```
Using mount_point mount_point
Launching vfs with command command
Launched vfs as pid PID number
```

Jika log berisi pesan berikut, dukungan sistem file virtual dinonaktifkan:

```
Virtual File System not found, falling back to COPIED for JobAttachmentsFileSystem.
```

Memecahkan masalah dukungan sistem file virtual

Anda dapat melihat log untuk sistem file virtual Anda menggunakan monitor Deadline Cloud. Untuk petunjuk, silakan lihat Lihat sesi dan log pekerja di Deadline Cloud.

Log sistem file virtual juga dikirim ke grup CloudWatch Log yang terkait dengan antrian yang dibagikan dengan output agen pekerja.

Lacak pengeluaran dan penggunaan untuk Deadline Cloud farm

Manajer anggaran dan penjelajah penggunaan AWS Deadline Cloud adalah alat manajemen biaya yang menyediakan perkiraan biaya penggunaan Deadline Cloud berdasarkan informasi yang tersedia tentang variabel biaya. Alat manajemen biaya tidak menjamin jumlah yang terutang untuk penggunaan Deadline Cloud dan layanan lainnya AWS yang sebenarnya.

Untuk membantu Anda mengelola biaya untuk Deadline Cloud, Anda dapat menggunakan fitur berikut:

- Manajer anggaran — Dengan manajer anggaran Deadline Cloud, Anda dapat membuat dan mengedit anggaran untuk membantu mengelola biaya proyek.
- Penjelajah penggunaan — Dengan penjelajah penggunaan Deadline Cloud, Anda dapat melihat berapa banyak AWS sumber daya yang digunakan dan perkiraan biaya untuk sumber daya tersebut.
- AWS tag alokasi biaya — Dengan tag alokasi biaya, Anda dapat melacak biaya terperinci untuk semua layanan Anda AWS . Untuk informasi selengkapnya, lihat Mengatur dan melacak AWS biaya menggunakan tag alokasi biaya.

Asumsi biaya

Perhitungan dasar yang digunakan oleh alat manajemen biaya Deadline Cloud adalah:

```
Cost per job =
    (CMF run time x CMF compute rate) +
    (SMF run time x SMF compute rate) +
    (License run time x license rate)
```

- Run time adalah jumlah dari semua tugas dalam suatu pekerjaan, dari waktu mulai hingga waktu akhir.
- Tingkat komputasi ditentukan oleh harga AWS Deadline Cloud untuk armada yang dikelola layanan. Untuk armada yang dikelola pelanggan, tingkat komputasi diperkirakan $1 per jam pekerja.

- Tarif lisensi ditentukan oleh harga lisensi basis Deadline Cloud dan hanya tersedia untuk armada yang dikelola layanan. Tingkatan tambahan tidak termasuk. Untuk informasi selengkapnya tentang harga lisensi, lihat harga AWS Deadline Cloud.

Perkiraan biaya dari alat manajemen biaya Deadline Cloud dapat bervariasi dari biaya aktual Anda karena sejumlah alasan. Alasan umum meliputi:

- Sumber daya milik pelanggan dan harganya. Anda dapat memilih untuk membawa sumber daya Anda sendiri, baik dari AWS atau eksternal dari lokal atau penyedia cloud lainnya. Biaya aktual dari sumber daya ini tidak dihitung.
- Biaya pekerja menganggur. Biaya pekerja menganggur tidak termasuk ketika status pekerja dalam keadaan IDLE. Hal ini dapat terjadi untuk armada dengan jumlah instans minimum lebih besar dari nol, atau ketika pekerja bertransisi antar pekerjaan. Biaya pekerja menganggur tidak termasuk dalam perhitungan.
- Pekerja berhenti dan mulai waktu. Setelah pekerja menyelesaikan pekerjaan, biaya untuk pindah dari IDLE ke STOPING dan dari STOPING ke STOPTED tidak termasuk dalam perkiraan biaya Deadline Cloud.
- Kredit promosi, diskon, dan perjanjian harga khusus. Alat manajemen biaya tidak memperhitungkan kredit promosi, perjanjian harga pribadi, atau diskon lainnya. Anda mungkin memenuhi syarat untuk diskon lain yang bukan bagian dari perkiraan.
- Penyimpanan aset. Penyimpanan aset tidak termasuk dalam perkiraan biaya dan penggunaan.
- Perubahan harga. AWS menawarkan pay-as-you-go harga untuk sebagian besar layanan. Harga dapat berubah seiring waktu. Alat manajemen biaya menggunakan up-to-date harga terbanyak yang tersedia untuk umum, tetapi mungkin ada penundaan setelah perubahan.
- Pajak. Alat manajemen biaya tidak termasuk pajak yang diterapkan untuk pembelian layanan kami.
- Pembulatan. Alat manajemen biaya melakukan pembulatan matematis data penetapan harga.
- Mata uang. Perkiraan biaya dibuat dalam dolar AS. Nilai tukar global bervariasi dari waktu ke waktu. Jika Anda menerjemahkan perkiraan ke basis mata uang yang berbeda pada pertukaran saat ini, perubahan nilai tukar mempengaruhi perkiraan.
- Lisensi luar. Jika Anda memilih untuk menggunakan lisensi yang telah dibeli sebelumnya (Lisensi perangkat lunak untuk armada yang dikelola layanan), alat manajemen biaya Deadline Cloud tidak dapat memperhitungkan biaya ini.

Kontrol biaya dengan anggaran

Manajer anggaran Deadline Cloud membantu Anda mengontrol pengeluaran untuk sumber daya tertentu, seperti antrian, armada, atau pertanian. Anda dapat membuat jumlah dan batasan anggaran, dan menetapkan tindakan otomatis untuk membantu mengurangi atau menghentikan pengeluaran tambahan terhadap anggaran.

Bagian berikut memberi Anda langkah-langkah untuk menggunakan manajer anggaran Deadline Cloud.

Topik

Prasyarat

Untuk menggunakan manajer anggaran Deadline Cloud, Anda harus memiliki tingkat `OWNER` akses. Untuk memberikan `OWNER` izin, ikuti langkah-langkahnyaMengelola pengguna di Deadline Cloud.

Buka manajer anggaran Deadline Cloud

Untuk membuka manajer anggaran Deadline Cloud, gunakan prosedur berikut.

1. Masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Pilih Lihat peternakan.
3. Temukan peternakan yang ingin Anda dapatkan informasinya, lalu pilih Kelola pekerjaan.
4. Di monitor Deadline Cloud, di panel navigasi kiri, pilih Anggaran.

Halaman ringkasan pengelola anggaran menampilkan daftar anggaran aktif dan tidak aktif:

- Anggaran aktif melacak sumber daya yang dipilih (antrian).
- Anggaran tidak aktif telah kedaluwarsa atau dibatalkan oleh pengguna, dan tidak lagi melacak biaya terhadap batas anggaran ini.

Setelah Anda memilih anggaran, halaman ringkasan anggaran berisi informasi dasar tentang anggaran. Informasi yang diberikan meliputi nama anggaran, status, sumber daya, persentase yang tersisa, jumlah yang tersisa, total anggaran, tanggal mulai, dan tanggal akhir.

Buat anggaran untuk antrian Deadline Cloud

Untuk membuat anggaran, gunakan prosedur berikut.

1. Jika Anda belum melakukannya, masuk ke AWS Management Console, buka konsol Cloud Deadline, pilih pertanian, lalu pilih Kelola pekerjaan.
2. Dari halaman Manajer anggaran, pilih Buat anggaran.
3. Di bagian detail, masukkan nama Anggaran untuk anggaran.
4. (Opsional) Di bidang deskripsi, masukkan deskripsi singkat tentang anggaran.
5. Dari Resource, gunakan dropdown Antrian untuk memilih antrian yang ingin Anda buat anggaran.
6. Untuk Periode, tetapkan tanggal mulai dan berakhirnya anggaran dengan menyelesaikan langkah-langkah berikut:

    a. Untuk Tanggal mulai, masukkan tanggal pertama pelacakan anggaran dalam YYYY/MM/DD format, atau pilih ikon kalender dan pilih tanggal.

    Tanggal mulai default adalah tanggal pembuatan anggaran.

    b. Untuk Tanggal akhir, masukkan tanggal terakhir pelacakan anggaran dalam YYYY/MM/DD format atau pilih ikon kalender dan pilih tanggal.

    Tanggal akhir default adalah 120 hari dari tanggal mulai.
7. Untuk jumlah Anggaran, masukkan jumlah dolar dari anggaran.
8. (Opsional) Kami menyarankan Anda membuat peringatan batas. Di bagian Batasi tindakan, Anda dapat menerapkan tindakan otomatis yang terjadi ketika jumlah tertentu tetap ada dalam anggaran. Caranya, lakukan langkah-langkah berikut:

    a. Pilih Tambahkan tindakan baru.

b. Untuk jumlah yang tersisa, masukkan jumlah dolar yang Anda inginkan untuk memulai tindakan.

c. Di dropdown Action, pilih tindakan yang Anda inginkan. Tindakan meliputi:

- Berhenti setelah menyelesaikan pekerjaan saat ini — Semua pekerjaan yang sedang berjalan saat jumlah ambang terpenuhi terus berjalan (dan mengeluarkan biaya) hingga selesai.
- Segera berhenti bekerja - Semua pekerjaan dibatalkan segera ketika jumlah ambang batas terpenuhi.

d. Untuk membuat peringatan batas tambahan, pilih Tambahkan tindakan baru dan ulangi langkah sebelumnya.

9. Pilih Buat anggaran.

Melihat anggaran antrian Deadline Cloud

Setelah Anda membuat anggaran, Anda dapat melihat anggaran di halaman Manajer anggaran. Dari sana, Anda dapat melihat jumlah total anggaran dan keseluruhan biaya yang dialokasikan untuk anggaran tertentu.

Untuk melihat anggaran, gunakan prosedur berikut.

1. Jika Anda belum melakukannya, masuk ke AWS Management Console, buka konsol Cloud Deadline, pilih pertanian, lalu pilih Kelola pekerjaan.
2. Pilih Anggaran dari panel navigasi sisi kiri. Halaman Manajer Anggaran muncul.
3. Untuk melihat anggaran aktif, pilih tab Anggaran aktif, dan pilih nama anggaran yang ingin Anda lihat. Halaman detail anggaran muncul.
4. Untuk melihat detail anggaran untuk anggaran kedaluwarsa, pilih tab Anggaran tidak aktif. Kemudian, pilih nama anggaran yang ingin Anda lihat. Halaman detail anggaran muncul.

Mengedit anggaran untuk antrean Deadline Cloud

Anda dapat mengedit anggaran aktif apa pun. Untuk mengedit anggaran aktif, gunakan prosedur berikut.

1. Jika Anda belum melakukannya, masuk ke AWS Management Console, buka konsol Cloud Deadline, pilih pertanian, lalu pilih Kelola pekerjaan.

2. Dari halaman Manajer Anggaran, di tab Anggaran aktif, pilih tombol di sebelah anggaran yang ingin Anda edit.
3. Dari menu tarik-turun Tindakan, pilih Edit anggaran.
4. Buat perubahan yang Anda inginkan, lalu pilih Perbarui anggaran.

Nonaktifkan anggaran untuk antrian Deadline Cloud

Anda dapat menonaktifkan anggaran aktif apa pun. Menonaktifkan anggaran mengubah statusnya dari Aktif menjadi Tidak Aktif. Ketika anggaran dinonaktifkan, itu tidak lagi melacak sumber daya ke jumlah anggaran itu.

Untuk menonaktifkan anggaran, gunakan prosedur berikut.

1. Jika Anda belum melakukannya, masuk ke AWS Management Console, buka konsol Cloud Deadline, pilih pertanian, lalu pilih Kelola pekerjaan.
2. Dari halaman Manajer anggaran, di tab Anggaran Aktif, pilih tombol di sebelah anggaran yang ingin Anda nonaktifkan.
3. Dari menu tarik-turun Tindakan, pilih Nonaktifkan anggaran. Dalam beberapa saat, anggaran yang dipilih akan berubah dari Aktif menjadi Tidak Aktif dan akan berpindah dari tab Anggaran Aktif ke tab Anggaran Tidak Aktif.

Pantau anggaran dengan EventBridge acara

Deadline Cloud mengirimkan acara terkait anggaran, menggunakan Amazon EventBridge, ke bus acara default Anda. EventBridge Anda dapat membuat fungsi khusus yang menerima acara dan menindaklanjutinya untuk mengirim pemberitahuan untuk memberi tahu pengguna secara otomatis melalui email, Slack, atau saluran lain ketika anggaran mencapai tingkat yang telah ditentukan. Misalnya, Anda dapat mengirim pesan SMS ketika anggaran mencapai ambang batas tertentu. Ini membantu Anda tetap di atas pengeluaran Anda dan membuat keputusan berdasarkan informasi sebelum anggaran Anda habis.

Deadline Cloud secara berkala mengumpulkan data penggunaan dan biaya untuk setiap render farm. Kemudian memeriksa untuk melihat apakah ada ambang anggaran yang telah dilewati. Jika ambang batas dilintasi, Deadline Cloud memicu peristiwa untuk mengingatkan Anda sehingga Anda dapat mengambil tindakan yang sesuai. Suatu peristiwa dipicu setiap kali anggaran melewati salah satu ambang batas ini, ditentukan dalam persen dari anggaran yang digunakan:

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

Ambang batas penggunaan anggaran semakin dekat karena anggaran mendekati penggunaan 100 persen. Ini membantu Anda memantau penggunaan dengan cermat saat anggaran mencapai batasnya. Anda juga dapat menetapkan ambang anggaran Anda sendiri. Deadline Cloud mengirimkan peristiwa saat penggunaan melewati ambang batas kustom Anda. Setelah anggaran Anda mencapai 100 persen, Deadline Cloud berhenti mengirim acara. Jika Anda menyesuaikan anggaran, Deadline Cloud mengirimkan acara untuk ambang batas Anda berdasarkan jumlah anggaran baru.

Anda dapat menggunakan EventBridge console (https://console.aws.amazon.com/events/) untuk membuat aturan untuk mengirim peristiwa Deadline Cloud ke target yang sesuai untuk acara tersebut. Misalnya, Anda dapat mengirim acara ke antrian Amazon Simple Queue Service dan dari sana ke beberapa target, seperti AWS End User Messaging SMS atau database Amazon Relational Database Service untuk logging.

Untuk contoh EventBridge aturan, lihat topik berikut:

- Kirim email saat peristiwa terjadi menggunakan Amazon EventBridge.
- Membuat EventBridge aturan Amazon yang mengirimkan pemberitahuan ke Pengembang Amazon Q di aplikasi obrolan.
- Memulai dengan Amazon EventBridge

Untuk informasi selengkapnya tentang peristiwa anggaran, lihat acara Ambang Batas Anggaran Tercapai di Panduan Pengembang Cloud Tenggat Waktu.

Lacak penggunaan dan biaya dengan penjelajah penggunaan Deadline Cloud

Dengan penjelajah penggunaan Deadline Cloud, Anda dapat melihat metrik real-time pada aktivitas yang terjadi di setiap farm. Anda dapat melihat biaya pertanian dengan variabel yang berbeda, seperti antrian, pekerjaan, produk lisensi, atau jenis instance. Pilih berbagai kerangka waktu untuk melihat penggunaan selama periode waktu tertentu, dan lihat tren penggunaan selama waktu. Anda juga dapat melihat rincian rinci dari titik data yang dipilih, memungkinkan untuk melihat lebih dekat ke metrik. Penggunaan dapat ditunjukkan berdasarkan waktu (menit dan jam) atau dengan biaya ($ USD).

Bagian berikut menunjukkan langkah-langkah untuk mengakses dan menggunakan penjelajah penggunaan Deadline Cloud.

Topik

Prasyarat

Untuk menggunakan penjelajah penggunaan Deadline Cloud, Anda harus memiliki salah satu `MANAGER` atau izin `OWNER` pertanian. Untuk informasi selengkapnya, lihat Kelola pengguna dan grup untuk peternakan, antrian, dan armada.

> **Note**
>
> Jika zona waktu Anda tidak sejajar dengan satu jam penuh, seperti Waktu Standar India (UTC+ 5:30), penjelajah penggunaan tidak menampilkan metrik penggunaan. Untuk melihat metrik, atur zona waktu Anda ke zona yang sejajar dengan satu jam penuh.

Buka penjelajah penggunaan

Untuk membuka penjelajah penggunaan Deadline Cloud, gunakan prosedur berikut.

1. Masuk ke AWS Management Console dan buka konsol Deadline Cloud.
2. Untuk melihat semua peternakan yang tersedia, pilih Lihat peternakan.
3. Temukan peternakan yang ingin Anda dapatkan informasinya, lalu pilih Kelola pekerjaan. Monitor Deadline Cloud terbuka di tab baru.
4. Di monitor Deadline Cloud, dari menu kiri, pilih Usage explorer.

Gunakan penjelajah penggunaan

Dari halaman penjelajah penggunaan, Anda dapat memilih parameter tertentu di mana data dapat ditampilkan. Secara default, Anda melihat total penggunaan dalam waktu (jam dan menit) dalam 7

hari terakhir. Anda dapat mengubah parameter ini, dan informasi yang ditampilkan berubah secara dinamis sesuai dengan pengaturan parameter.

Anda dapat mengelompokkan hasil berdasarkan antrian, pekerjaan, penggunaan komputasi, jenis instans, atau produk lisensi. Jika Anda memilih produk lisensi, biaya dihitung untuk lisensi tertentu. Untuk semua grup lain, waktu dihitung dengan menjumlahkan waktu yang dibutuhkan untuk setiap tugas untuk dijalankan.

Penjelajah penggunaan hanya mengembalikan 100 hasil berdasarkan kriteria filter yang Anda tetapkan. Hasilnya tercantum dalam urutan menurun berdasarkan tanggal yang dibuat stempel waktu. Jika ada lebih dari 100 hasil, Anda mendapatkan pesan kesalahan. Anda dapat menyempurnakan kueri untuk mengurangi jumlah hasil:

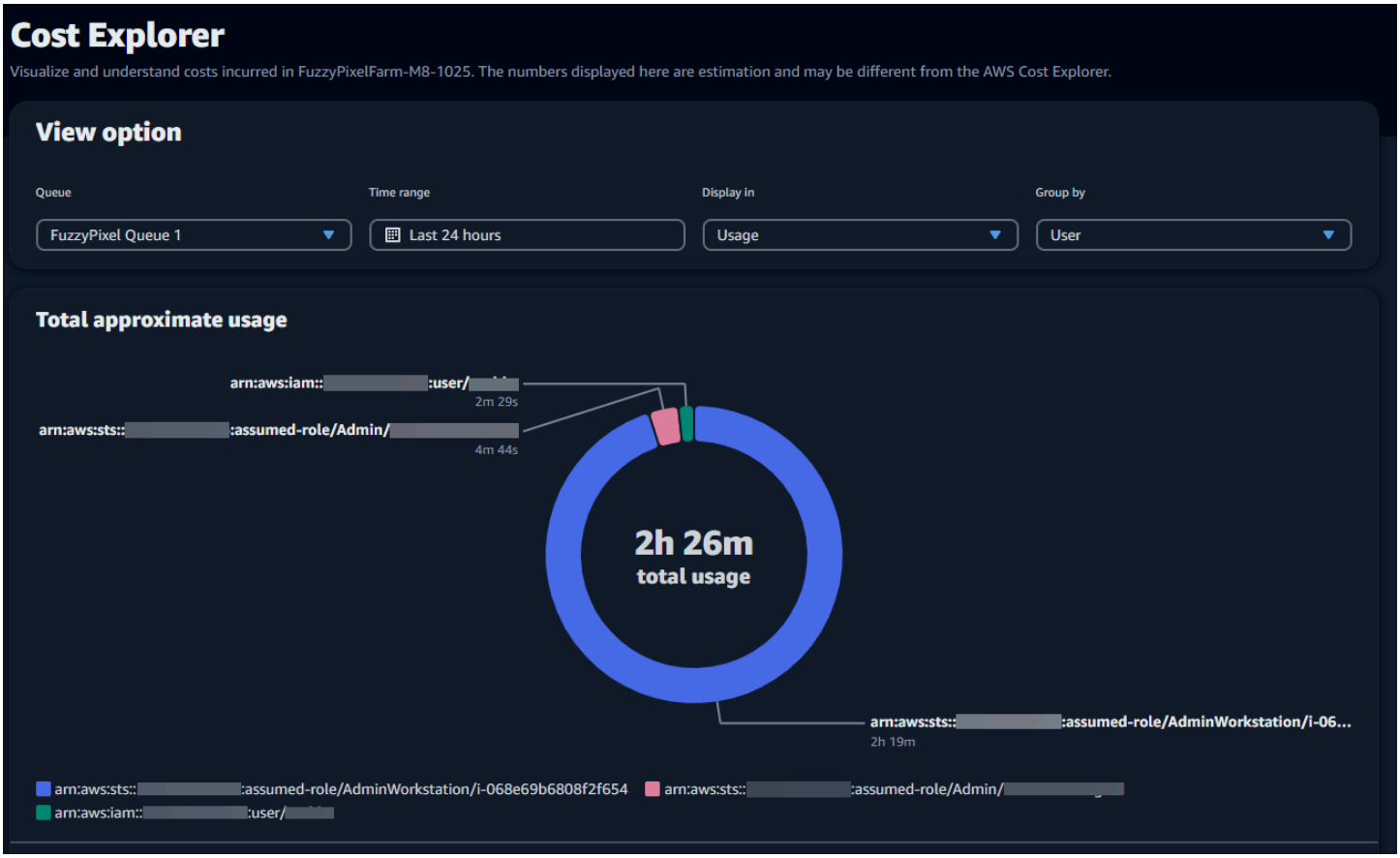
- Pilih rentang waktu yang lebih kecil
- Pilih antrian yang lebih sedikit
- Pilih pengelompokan yang berbeda, seperti pengelompokan berdasarkan antrian, bukan pekerjaan

Topik

Gunakan grafik visual untuk meninjau data

Anda dapat meninjau data dalam format visual untuk mengidentifikasi tren dan area potensial yang mungkin memerlukan lebih banyak analisis atau perhatian. Penjelajah penggunaan menawarkan diagram lingkaran yang menampilkan penggunaan dan biaya keseluruhan dengan opsi untuk mengelompokkan total menjadi subtotal yang lebih kecil.

> **Note**
>
> Bagan hanya menampilkan lima hasil teratas dengan hasil lain yang digabungkan dalam bagian “lainnya”. Anda dapat melihat semua hasil di bagian rincian di bawah grafik.



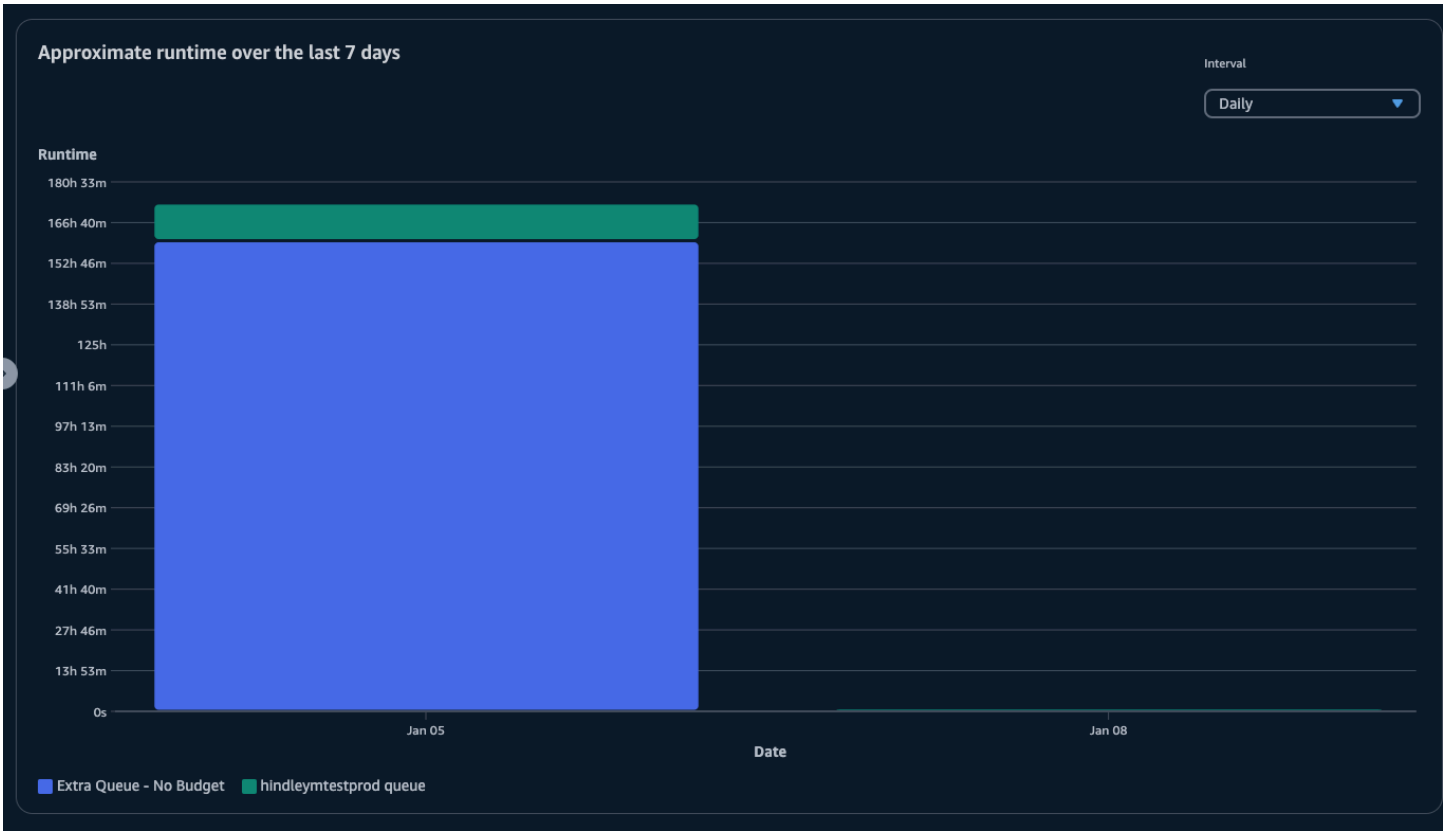
Lihat rincian metrik

Di bawah diagram lingkaran, penjelajah penggunaan menawarkan rincian metrik tertentu yang lebih rinci, yang akan berubah saat parameter berubah. Secara default, lima hasil ditampilkan di penjelajah penggunaan. Anda dapat menggulir hasil menggunakan panah pagination di bagian breakdown.

Kerusakan diminimalkan secara default. Untuk memperluas dan menampilkan hasilnya, pilih panah Lihat semua kerusakan. Untuk mengunduh rincian, pilih Unduh data.

Lihat perkiraan runtime antrian

Anda juga dapat melihat perkiraan runtime antrian Anda berdasarkan interval berbeda yang Anda tentukan. Opsi interval adalah per jam, harian, mingguan, dan bulanan. Setelah Anda memilih interval, grafik menampilkan perkiraan runtime antrian Anda.



Manajemen biaya

AWS Deadline Cloud menyediakan anggaran dan penjelajah penggunaan untuk membantu Anda mengontrol dan memvisualisasikan biaya untuk pekerjaan Anda. Namun, Deadline Cloud menggunakan AWS layanan lain, seperti Amazon S3. Biaya untuk layanan tersebut tidak tercermin dalam anggaran Deadline Cloud atau penjelajah penggunaan dan dibebankan secara terpisah berdasarkan penggunaan. Bergantung pada cara Anda mengonfigurasi Deadline Cloud, Anda dapat menggunakan AWS layanan berikut, serta layanan lainnya:

Layanan	Halaman harga
CloudWatch Log Amazon	Harga Amazon CloudWatch Logs
Amazon Elastic Compute Cloud	Harga Amazon Elastic Compute Cloud
AWS Key Management Service	AWS Key Management Service harga
AWS PrivateLink	AWS PrivateLink harga

Layanan	Halaman harga
Amazon Simple Storage Service	Harga Amazon Simple Storage Service
Amazon Virtual Private Cloud	Harga Amazon Virtual Private Cloud

Praktik terbaik manajemen biaya

Menggunakan praktik terbaik berikut dapat membantu Anda memahami dan mengontrol biaya saat menggunakan Deadline Cloud dan pengorbanan yang dapat Anda lakukan antara biaya dan efisiensi.

> **Note**
>
> Biaya akhir menggunakan Deadline Cloud tergantung pada interaksi antara sejumlah AWS layanan, jumlah pekerjaan yang Anda proses, dan Wilayah AWS di mana Anda menjalankan pekerjaan Anda. Praktik terbaik berikut adalah pedoman dan mungkin tidak mengurangi biaya secara signifikan.

Praktik terbaik untuk CloudWatch Log

Deadline Cloud mengirimkan log pekerja dan tugas ke CloudWatch Log. Anda dikenakan biaya untuk mengumpulkan, menyimpan, dan menganalisis log ini. Anda dapat mengurangi biaya dengan mencatat hanya jumlah minimum data yang diperlukan untuk memantau tugas Anda.

Saat Anda membuat antrian atau armada, Deadline Cloud membuat grup CloudWatch log Log dengan nama berikut:

- `/aws/deadline/<FARM_ID>/<FLEET_ID>`
- `/aws/deadline/<FARM_ID>/<QUEUE_ID>`

Secara default, log ini tidak pernah kedaluwarsa. Anda dapat menyesuaikan kebijakan penyimpanan grup log untuk menghapus log lama dan membantu mengurangi biaya penyimpanan. Anda juga dapat mengekspor log ke Amazon S3. Biaya penyimpanan Amazon S3 lebih rendah daripada biaya penyimpanan. CloudWatch Untuk informasi lebih lanjut, lihat Mengekspor data log ke Amazon S3.

Praktik terbaik untuk Amazon EC2

Anda dapat menggunakan EC2 instans Amazon untuk armada yang dikelola layanan dan yang dikelola pelanggan. Ada tiga pertimbangan:

- Untuk armada yang dikelola layanan, Anda dapat memilih untuk memiliki satu atau beberapa instance yang tersedia setiap saat dengan menetapkan jumlah pekerja minimum untuk armada. Ketika Anda menetapkan jumlah pekerja minimum di atas 0, armada selalu memiliki banyak pekerja yang berjalan. Ini dapat mengurangi jumlah waktu yang dibutuhkan Deadline Cloud untuk mulai memproses pekerjaan, namun Anda dikenakan biaya untuk waktu idle instans.
- Untuk armada yang dikelola layanan, tetapkan ukuran maksimum untuk armada. Ini membatasi jumlah instance yang dapat ditskalakan secara otomatis oleh armada. Armada tidak akan tumbuh melewati ukuran ini bahkan jika ada lebih banyak pekerjaan yang menunggu untuk diproses.
- Untuk armada yang dikelola layanan dan yang dikelola pelanggan, Anda dapat menentukan jenis EC2 instans Amazon di armada Anda. Menggunakan contoh yang lebih kecil harganya lebih murah per menit, tetapi mungkin membutuhkan waktu lebih lama untuk menyelesaikan pekerjaan. Sebaliknya, contoh yang lebih besar harganya lebih per menit, tetapi dapat mengurangi waktu untuk menyelesaikan pekerjaan. Memahami tuntutan yang ditempatkan pekerjaan Anda pada sebuah contoh dapat membantu mengurangi biaya Anda.
- Jika memungkinkan, pilih instans Amazon EC2 Spot untuk armada Anda. Instans spot tersedia dengan harga yang lebih murah, tetapi dapat terganggu oleh permintaan sesuai permintaan. Instans sesuai permintaan dibebankan oleh yang kedua dan tidak terganggu.

Praktik terbaik untuk AWS KMS

Secara default, Deadline Cloud mengenkripsi data Anda dengan kunci yang AWS dimiliki. Anda tidak dikenakan biaya untuk kunci ini.

Anda dapat memilih untuk menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data Anda. Ketika Anda menggunakan kunci Anda sendiri, Anda akan dikenakan biaya berdasarkan bagaimana kunci Anda digunakan. Jika Anda menggunakan kunci yang ada, ini akan menjadi biaya tambahan untuk penggunaan tambahan.

Praktik terbaik untuk AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi antara VPC dan Deadline Cloud menggunakan endpoint antarmuka. Saat membuat koneksi, Anda dapat memanggil semua tindakan

Deadline Cloud API. Anda dikenakan biaya per jam untuk setiap titik akhir yang Anda buat. Jika Anda menggunakan PrivateLink, Anda harus membuat setidaknya tiga titik akhir, dan tergantung pada konfigurasi Anda, Anda mungkin memerlukan sebanyak lima.

Praktik terbaik untuk Amazon S3

Deadline Cloud menggunakan Amazon S3 untuk menyimpan aset untuk diproses, lampiran pekerjaan, output, dan log. Untuk mengurangi biaya yang terkait dengan Amazon S3, kurangi jumlah data yang Anda simpan. Beberapa saran:

- Hanya menyimpan aset yang sedang digunakan atau yang akan segera digunakan.
- Gunakan konfigurasi Siklus Hidup S3 untuk menghapus file yang tidak digunakan secara otomatis dari bucket S3.

Praktik terbaik untuk Amazon VPC

Saat Anda menggunakan lisensi berbasis penggunaan untuk armada yang dikelola pelanggan, Anda membuat titik akhir lisensi Deadline Cloud, yang merupakan titik akhir Amazon VPC yang dibuat di akun Anda. Titik akhir ini dikenakan tarif per jam. Untuk mengurangi biaya, hapus titik akhir saat Anda tidak menggunakan lisensi berbasis penggunaan.

Keamanan di Deadline Cloud

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Deadline Cloud, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Deadline Cloud. Topik berikut menunjukkan cara mengonfigurasi Deadline Cloud untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan Layanan AWS yang lain yang membantu Anda memantau dan mengamankan Deadline Cloud sumber daya Anda.

Topik

- Praktik terbaik keamanan untuk Deadline Cloud

Perlindungan data di Deadline Cloud

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Deadline Cloud. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti

bidang Nama. Ini termasuk saat Anda bekerja dengan Deadline Cloud atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Data yang dimasukkan ke dalam bidang nama dalam templat Deadline Cloud pekerjaan juga dapat dimasukkan dalam log penagihan atau diagnostik dan tidak boleh berisi informasi rahasia atau sensitif.

Topik

Enkripsi diam

AWS Deadline Cloud melindungi data sensitif dengan mengenkripsinya saat istirahat menggunakan kunci enkripsi yang disimpan di AWS Key Management Service ()AWS KMS. Enkripsi saat istirahat tersedia di semua Wilayah AWS tempat Deadline Cloud yang tersedia.

Mengenkripsi data berarti data sensitif yang disimpan pada disk tidak dapat dibaca oleh pengguna atau aplikasi tanpa kunci yang valid. Hanya pihak dengan kunci terkelola yang valid yang dapat mendekripsi data.

Untuk informasi tentang cara Deadline Cloud penggunaan AWS KMS untuk mengenkripsi data saat istirahat, lihat. Manajemen kunci

Enkripsi bergerak

Untuk data dalam perjalanan, AWS Deadline Cloud gunakan Transport Layer Security (TLS) 1.2 atau 1.3 untuk mengenkripsi data yang dikirim antara layanan dan pekerja. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3. Selain itu, jika Anda menggunakan virtual private cloud (VPC), Anda

dapat menggunakannya AWS PrivateLink untuk membuat koneksi pribadi antara VPC dan VPC Anda. Deadline Cloud

Manajemen kunci

Saat membuat peternakan baru, Anda dapat memilih salah satu kunci berikut untuk mengenkripsi data pertanian Anda:

- AWS kunci KMS yang dimiliki — Jenis enkripsi default jika Anda tidak menentukan kunci saat membuat peternakan. Kunci KMS dimiliki oleh AWS Deadline Cloud. Anda tidak dapat melihat, mengelola, atau menggunakan kunci AWS yang dimiliki. Namun, Anda tidak perlu mengambil tindakan apa pun untuk melindungi kunci yang mengenkripsi data Anda. Untuk informasi selengkapnya, lihat kunci yang AWS dimiliki di panduan AWS Key Management Service pengembang.
- Kunci KMS yang dikelola pelanggan — Anda menentukan kunci yang dikelola pelanggan saat membuat peternakan. Semua konten di dalam peternakan dienkripsi dengan kunci KMS. Kunci disimpan di akun Anda dan dibuat, dimiliki, dan dikelola oleh Anda dan AWS KMS dikenakan biaya. Anda memiliki kontrol penuh atas tombol KMS. Anda dapat melakukan tugas-tugas seperti:
  - Menetapkan dan memelihara kebijakan utama
  - Menetapkan dan memelihara kebijakan dan hibah IAM
  - Mengaktifkan dan menonaktifkan kebijakan utama
  - Menambahkan tanda
  - Membuat alias kunci

  Anda tidak dapat memutar kunci milik pelanggan secara manual yang digunakan dengan Deadline Cloud peternakan. Rotasi otomatis tombol didukung.

  Untuk informasi selengkapnya, lihat Kunci milik pelanggan di Panduan AWS Key Management Service Pengembang.

  Untuk membuat kunci terkelola pelanggan, ikuti langkah-langkah untuk Membuat kunci terkelola pelanggan simetris di Panduan AWS Key Management Service Pengembang.

Bagaimana Deadline Cloud menggunakan AWS KMS hibah

Deadline Cloud membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda. Saat Anda membuat peternakan yang dienkripsi dengan kunci yang dikelola pelanggan, Deadline Cloud

buat hibah atas nama Anda dengan mengirimkan `CreateGrant` permintaan untuk mendapatkan akses AWS KMS ke kunci KMS yang Anda tentukan.

Deadline Cloud menggunakan beberapa hibah. Setiap hibah digunakan oleh bagian yang berbeda Deadline Cloud yang perlu mengenkripsi atau mendekripsi data Anda. Deadline Cloud juga menggunakan hibah untuk memungkinkan akses ke AWS layanan lain yang digunakan untuk menyimpan data atas nama Anda, seperti Amazon Simple Storage Service, Amazon Elastic Block Store, atau OpenSearch.

Hibah yang memungkinkan Deadline Cloud untuk mengelola mesin dalam armada yang dikelola layanan mencakup nomor Deadline Cloud akun dan peran dalam `GranteePrincipal` alih-alih prinsip layanan. Meskipun tidak khas, ini diperlukan untuk mengenkripsi volume Amazon EBS untuk pekerja dalam armada yang dikelola layanan menggunakan kunci KMS terkelola pelanggan yang ditentukan untuk pertanian.

Kebijakan kunci yang dikelola pelanggan

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci harus memiliki persis satu kebijakan kunci yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi selengkapnya, lihat Mengelola akses ke kunci terkelola pelanggan di Panduan AWS Key Management Service Pengembang.

Kebijakan IAM minimal untuk CreateFarm

Untuk menggunakan kunci terkelola pelanggan Anda untuk membuat farm menggunakan konsol atau operasi `CreateFarm` API, operasi AWS KMS API berikut harus diizinkan:

- `kms:CreateGrant`— Menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses konsol ke AWS KMS kunci tertentu. Untuk informasi selengkapnya, lihat Menggunakan hibah di panduan AWS Key Management Service pengembang.
- `kms:Decrypt`— Memungkinkan Deadline Cloud untuk mendekripsi data di peternakan.
- `kms:DescribeKey`— Memberikan detail kunci yang dikelola pelanggan untuk memungkinkan Deadline Cloud memvalidasi kunci.
- `kms:GenerateDataKey`— Memungkinkan Deadline Cloud untuk mengenkripsi data menggunakan kunci data yang unik.

Pernyataan kebijakan berikut memberikan izin yang diperlukan untuk operasi. `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"
                }
            }
        }
    ]
}
```

Kebijakan IAM minimal untuk operasi hanya-baca

Untuk menggunakan kunci yang dikelola pelanggan Anda untuk Deadline Cloud operasi hanya-baca, seperti mendapatkan informasi tentang peternakan, antrian, dan armada. Operasi AWS KMS API berikut harus diizinkan:

- `kms:Decrypt`— Memungkinkan Deadline Cloud untuk mendekripsi data di peternakan.
- `kms:DescribeKey`— Memberikan detail kunci yang dikelola pelanggan untuk memungkinkan Deadline Cloud memvalidasi kunci.

Pernyataan kebijakan berikut memberikan izin yang diperlukan untuk operasi hanya-baca.

```
{
    "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"
                }
            }
        }
    ]
}
```

Kebijakan IAM minimal untuk operasi baca-tulis

Untuk menggunakan kunci terkelola pelanggan Anda untuk Deadline Cloud operasi baca-tulis, seperti membuat dan memperbarui peternakan, antrian, dan armada. Operasi AWS KMS API berikut harus diizinkan:

- `kms:Decrypt`— Memungkinkan Deadline Cloud untuk mendekripsi data di peternakan.
- `kms:DescribeKey`— Memberikan detail kunci yang dikelola pelanggan untuk memungkinkan Deadline Cloud memvalidasi kunci.
- `kms:GenerateDataKey`— Memungkinkan Deadline Cloud untuk mengenkripsi data menggunakan kunci data yang unik.

Pernyataan kebijakan berikut memberikan izin yang diperlukan untuk operasi. `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"
                }
            }
        }
    ]
}
```

Memantau kunci enkripsi Anda

Saat menggunakan kunci terkelola AWS KMS pelanggan dengan Deadline Cloud peternakan, Anda dapat menggunakan AWS CloudTrailatau Amazon CloudWatch Logs untuk melacak permintaan yang Deadline Cloud dikirim AWS KMS.

CloudTrail acara untuk hibah

Contoh CloudTrail peristiwa berikut terjadi ketika hibah dibuat, biasanya ketika Anda memanggil`CreateFarm`,`CreateMonitor`, atau `CreateFleet` operasi.

```
{
    "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 acara untuk dekripsi

Contoh CloudTrail peristiwa berikut terjadi ketika mendekripsi nilai menggunakan kunci KMS yang dikelola pelanggan.

```
{
    "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 acara untuk enkripsi

Contoh CloudTrail peristiwa berikut terjadi ketika mengenkripsi nilai menggunakan kunci KMS yang dikelola pelanggan.

```
{
    "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"
```

```
}
```

Menghapus kunci KMS yang dikelola pelanggan

Menghapus kunci KMS yang dikelola pelanggan di AWS Key Management Service (AWS KMS) bersifat merusak dan berpotensi berbahaya. Ini secara permanen menghapus materi kunci dan semua metadata yang terkait dengan kunci. Setelah kunci KMS yang dikelola pelanggan dihapus, Anda tidak dapat lagi mendekripsi data yang dienkripsi oleh kunci itu. Ini berarti bahwa data menjadi tidak dapat dipulihkan.

Inilah sebabnya mengapa AWS KMS memberi pelanggan masa tunggu hingga 30 hari sebelum menghapus kunci KMS. Masa tunggu default adalah 30 hari.

Tentang masa tunggu

Karena menghapus kunci KMS yang dikelola pelanggan merusak dan berpotensi berbahaya, kami mengharuskan Anda menetapkan masa tunggu 7-30 hari. Masa tunggu default adalah 30 hari.

Namun, masa tunggu sebenarnya mungkin hingga 24 jam lebih lama dari periode yang Anda jadwalkan. Untuk mendapatkan tanggal dan waktu aktual ketika kunci akan dihapus, gunakan DescribeKeyoperasi. Anda juga dapat melihat tanggal penghapusan kunci yang dijadwalkan di AWS KMS konsol pada halaman detail kunci, di bagian Konfigurasi umum. Perhatikan zona waktu.

Selama masa tunggu, status dan status kunci yang dikelola pelanggan adalah Penghapusan tertunda.

- Kunci KMS yang dikelola pelanggan yang menunggu penghapusan tidak dapat digunakan dalam operasi kriptografi apa pun.
- AWS KMS tidak memutar kunci dukungan kunci KMS yang dikelola pelanggan yang sedang menunggu penghapusan.

Untuk informasi selengkapnya tentang menghapus kunci KMS yang dikelola pelanggan, lihat Menghapus kunci master pelanggan di Panduan Pengembang AWS Key Management Service .

Privasi lalu lintas antar jaringan

AWS Deadline Cloud mendukung Amazon Virtual Private Cloud (Amazon VPC) untuk mengamankan koneksi. Amazon VPC menyediakan fitur yang dapat Anda gunakan untuk meningkatkan dan memantau keamanan virtual private cloud (VPC) Anda.

Anda dapat menyiapkan armada yang dikelola pelanggan (CMF) dengan instans Amazon Elastic Compute Cloud (Amazon EC2) yang berjalan di dalam VPC. Dengan menerapkan titik akhir VPC Amazon untuk AWS PrivateLink digunakan, lalu lintas antar pekerja di CMF Anda dan Deadline Cloud titik akhir tetap berada dalam VPC Anda. Selanjutnya, Anda dapat mengonfigurasi VPC Anda untuk membatasi akses internet ke instans Anda.

Dalam armada yang dikelola layanan, pekerja tidak dapat dijangkau dari internet, tetapi mereka memiliki akses internet dan terhubung ke layanan melalui internet. Deadline Cloud

Menyisih

AWS Deadline Cloud mengumpulkan informasi operasional tertentu untuk membantu kami mengembangkan dan meningkatkan Deadline Cloud. Data yang dikumpulkan mencakup hal-hal seperti ID AWS akun dan ID pengguna Anda, sehingga kami dapat mengidentifikasi Anda dengan benar jika Anda memiliki masalah dengan Deadline Cloud. Kami juga mengumpulkan informasi Deadline Cloud spesifik, seperti Resource IDs (FarmId atau QueueID bila berlaku), nama produk (misalnya,, JobAttachments WorkerAgent, dan lainnya) dan versi produk.

Anda dapat memilih untuk memilih keluar dari pengumpulan data ini menggunakan konfigurasi aplikasi. Setiap komputer yang berinteraksi dengan Deadline Cloud, baik workstation klien dan pekerja armada, perlu memilih keluar secara terpisah.

Deadline Cloud monitor - desktop

Deadline Cloud monitor - desktop mengumpulkan informasi operasional, seperti ketika crash terjadi dan ketika aplikasi dibuka, untuk membantu kami mengetahui kapan Anda mengalami masalah dengan aplikasi. Untuk memilih keluar dari pengumpulan informasi operasional ini, buka halaman pengaturan dan hapus Aktifkan pengumpulan data untuk mengukur kinerja Deadline Cloud Monitor.

Setelah Anda memilih keluar, monitor desktop tidak lagi mengirimkan data operasional. Setiap data yang dikumpulkan sebelumnya disimpan dan masih dapat digunakan untuk meningkatkan layanan. Untuk informasi selengkapnya, lihat FAQ Privasi Data.

AWS Deadline Cloud CLI dan Alat

AWS Deadline Cloud CLI, pengirim, dan agen pekerja semuanya mengumpulkan informasi operasional seperti kapan crash terjadi dan kapan pekerjaan dikirimkan untuk membantu kami mengetahui kapan Anda mengalami masalah dengan aplikasi ini. Untuk memilih keluar dari pengumpulan informasi operasional ini, gunakan salah satu metode berikut:

- Di terminal, masukkan**`deadline config set telemetry.opt_out true`**.

  Ini akan memilih keluar dari CLI, pengirim, dan agen pekerja saat berjalan sebagai pengguna saat ini.
- Saat menginstal agen Deadline Cloud pekerja, tambahkan argumen baris **`--telemetry-opt-out`** perintah. Misalnya, **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**.
- Sebelum menjalankan agen pekerja, CLI, atau submitter, tetapkan variabel lingkungan: **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

Setelah Anda memilih keluar, Deadline Cloud alat tidak lagi mengirim data operasional. Setiap data yang dikumpulkan sebelumnya disimpan dan masih dapat digunakan untuk meningkatkan layanan. Untuk informasi selengkapnya, lihat FAQ Privasi Data.

Identity and Access Management di Deadline Cloud

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Deadline Cloud. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Deadline Cloud bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Deadline Cloud
- AWS kebijakan terkelola untuk Deadline Cloud
- Pemecahan Masalah AWS Batas Waktu Identitas dan akses Cloud

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Deadline Cloud.

Pengguna layanan — Jika Anda menggunakan layanan Deadline Cloud untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Deadline Cloud untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Deadline Cloud, lihatPemecahan Masalah AWS Batas Waktu Identitas dan akses Cloud.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Deadline Cloud di perusahaan Anda, Anda mungkin memiliki akses penuh ke Deadline Cloud. Tugas Anda adalah menentukan fitur dan sumber daya Deadline Cloud mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Deadline Cloud, lihat. Bagaimana Deadline Cloud bekerja dengan IAM

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Deadline Cloud. Untuk melihat contoh Kebijakan berbasis identitas Cloud Batas waktu yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Deadline Cloud

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara

kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk

menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensyal sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan

antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Deadline Cloud bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Deadline Cloud, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Deadline Cloud.

Fitur IAM yang dapat Anda gunakan dengan AWS Deadline Cloud

Fitur IAM	Dukungan Batas Waktu Cloud
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS kerja Deadline Cloud dan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Deadline Cloud

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Deadline Cloud

Untuk melihat contoh kebijakan berbasis identitas Deadline Cloud, lihat. Contoh kebijakan berbasis identitas untuk Deadline Cloud

Kebijakan berbasis sumber daya dalam Deadline Cloud

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada

entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Deadline Cloud

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Cloud Deadline, lihat Tindakan yang ditentukan oleh AWS Deadline Cloud di Referensi Otorisasi Layanan.

Tindakan kebijakan di Deadline Cloud menggunakan awalan berikut sebelum tindakan:

```
awsdeadlinecloud
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "awsdeadlinecloud:action1",
      "awsdeadlinecloud:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Deadline Cloud, lihat. Contoh kebijakan berbasis identitas untuk Deadline Cloud

Sumber daya kebijakan untuk Deadline Cloud

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Cloud Deadline dan jenisnya ARNs, lihat Sumber Daya yang ditentukan oleh AWS Deadline Cloud di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Deadline Cloud.

Untuk melihat contoh kebijakan berbasis identitas Deadline Cloud, lihat. Contoh kebijakan berbasis identitas untuk Deadline Cloud

Kunci kondisi kebijakan untuk Deadline Cloud

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Deadline Cloud, lihat Kunci kondisi untuk AWS Deadline Cloud di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Deadline Cloud.

Untuk melihat contoh kebijakan berbasis identitas Deadline Cloud, lihat. Contoh kebijakan berbasis identitas untuk Deadline Cloud

ACLs di Deadline Cloud

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Deadline Cloud

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensil sementara dengan Deadline Cloud

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Deadline Cloud

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah

tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Deadline Cloud

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Deadline Cloud. Edit peran layanan hanya jika Deadline Cloud memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Deadline Cloud

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Deadline Cloud

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Deadline Cloud. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS

Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Deadline Cloud, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Deadline Cloud di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Cloud Deadline
- Kebijakan untuk mengirimkan pekerjaan ke antrian
- Kebijakan untuk mengizinkan pembuatan titik akhir lisensi
- Kebijakan untuk memungkinkan pemantauan antrian pertanian tertentu

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Deadline Cloud di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi

tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Cloud Deadline

Untuk mengakses konsol AWS Deadline Cloud, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Cloud Deadline di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Deadline Cloud, lampirkan juga Deadline Cloud *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Kebijakan untuk mengirimkan pekerjaan ke antrian

Dalam contoh ini, Anda membuat kebijakan cakupan bawah yang memberikan izin untuk mengirimkan pekerjaan ke antrian tertentu di peternakan tertentu.

```
{
    "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/*"
        }
    ]
}
```

Kebijakan untuk mengizinkan pembuatan titik akhir lisensi

Dalam contoh ini, Anda membuat kebijakan cakupan bawah yang memberikan izin yang diperlukan untuk membuat dan mengelola titik akhir lisensi. Gunakan kebijakan ini untuk membuat titik akhir lisensi untuk VPC yang terkait dengan farm Anda.

```
{
    "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": "*"
    }]
}
```

Kebijakan untuk memungkinkan pemantauan antrian pertanian tertentu

Dalam contoh ini, Anda membuat kebijakan cakupan bawah yang memberikan izin untuk memantau pekerjaan dalam antrian tertentu untuk peternakan tertentu.

```
{
    "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 kebijakan terkelola untuk Deadline Cloud

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSDeadlineCloud-FleetWorker

Anda dapat melampirkan `AWSDeadlineCloud-FleetWorker` kebijakan ke identitas AWS Identity and Access Management (IAM) Anda.

Kebijakan ini memberi pekerja di armada ini izin yang diperlukan untuk terhubung dan menerima tugas dari layanan.

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan kepala sekolah untuk mengelola pekerja dalam armada.

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-FleetWorkerdi panduan referensi Kebijakan Terkelola AWS.

AWS kebijakan terkelola: AWSDeadlineCloud-WorkerHost

Anda dapat melampirkan kebijakan `AWSDeadlineCloud-WorkerHost` ke identitas IAM Anda.

Kebijakan ini memberikan izin yang diperlukan untuk awalnya terhubung ke layanan. Ini dapat digunakan sebagai profil instans Amazon Elastic Compute Cloud (Amazon EC2).

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan pengguna untuk membuat pekerja, mengambil peran armada untuk pekerja, dan menerapkan tag untuk pekerja

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-WorkerHostdi panduan referensi Kebijakan Terkelola AWS.

AWS kebijakan terkelola: AWSDeadlineCloud-UserAccessFarms

Anda dapat melampirkan kebijakan `AWSDeadlineCloud-UserAccessFarms` ke identitas IAM Anda.

Kebijakan ini memungkinkan pengguna untuk mengakses data pertanian berdasarkan peternakan tempat mereka menjadi anggota dan tingkat keanggotaan mereka.

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan pengguna untuk mengakses data pertanian.
- `ec2`— Memungkinkan pengguna untuk melihat detail tentang jenis EC2 instans Amazon.
- `identitystore`— Memungkinkan pengguna untuk melihat nama pengguna dan grup.

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-UserAccessFarmsdi panduan referensi Kebijakan Terkelola AWS.

AWS kebijakan terkelola: AWSDeadlineCloud-UserAccessFleets

Anda dapat melampirkan kebijakan `AWSDeadlineCloud-UserAccessFleets` ke identitas IAM Anda.

Kebijakan ini memungkinkan pengguna untuk mengakses data armada berdasarkan peternakan tempat mereka menjadi anggota dan tingkat keanggotaan mereka.

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan pengguna untuk mengakses data pertanian.
- `ec2`— Memungkinkan pengguna untuk melihat detail tentang jenis EC2 instans Amazon.
- `identitystore`— Memungkinkan pengguna untuk melihat nama pengguna dan grup.

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-UserAccessFleetsdi panduan referensi Kebijakan Terkelola AWS.

AWS kebijakan terkelola: AWSDeadlineCloud-UserAccessJobs

Anda dapat melampirkan kebijakan `AWSDeadlineCloud-UserAccessJobs` ke identitas IAM Anda.

Kebijakan ini memungkinkan pengguna untuk mengakses data pekerjaan berdasarkan peternakan tempat mereka menjadi anggota dan tingkat keanggotaan mereka.

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan pengguna untuk mengakses data pertanian.
- `ec2`— Memungkinkan pengguna untuk melihat detail tentang jenis EC2 instans Amazon.
- `identitystore`— Memungkinkan pengguna untuk melihat nama pengguna dan grup.

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-UserAccessJobsdi panduan referensi Kebijakan Terkelola AWS.

AWS kebijakan terkelola: AWSDeadlineCloud-UserAccessQueues

Anda dapat melampirkan kebijakan `AWSDeadlineCloud-UserAccessQueues` ke identitas IAM Anda.

Kebijakan ini memungkinkan pengguna untuk mengakses data antrian berdasarkan peternakan tempat mereka menjadi anggota dan tingkat keanggotaan mereka.

Detail izin

Kebijakan ini mencakup izin berikut:

- `deadline`— Memungkinkan pengguna untuk mengakses data pertanian.
- `ec2`— Memungkinkan pengguna untuk melihat detail tentang jenis EC2 instans Amazon.
- `identitystore`— Memungkinkan pengguna untuk melihat nama pengguna dan grup.

Untuk daftar JSON tentang detail kebijakan, lihat AWSDeadlineCloud-UserAccessQueuesdi panduan referensi Kebijakan Terkelola AWS.

Pembaruan Cloud batas waktu ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Deadline Cloud sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Cloud Batas Waktu.

Perubahan	Deskripsi	Tanggal
AWSDeadlineCloud-WorkerHost— Ubah	Deadline Cloud menambahkan tindakan baru `deadline:TagResource` dan `deadline:ListTagsForResource` memungkinkan Anda menambahkan dan melihat tag yang terkait dengan pekerja di armada Anda.	30 Mei 2025
AWSDeadlineCloud-UserAccessFarms— Ubah AWSDeadlineCloud-UserAccessJobs— Ubah	Deadline Cloud menambahkan tindakan baru `deadline:GetJobTemplate` dan `deadline:ListJobParameterDefinitions` memungkinkan Anda	Oktober 7, 2024

Perubahan	Deskripsi	Tanggal
AWSDeadlineCloud-UserAccessQueues— Ubah	mengirimkan kembali pekerjaan.	
Deadline Cloud mulai melacak perubahan	Deadline Cloud mulai melacak perubahan pada kebijakan AWS terkelolanya.	April 2, 2024

Pemecahan Masalah AWS Batas Waktu Identitas dan akses Cloud

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Deadline Cloud dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Deadline Cloud
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Deadline Cloud saya

Saya tidak berwenang untuk melakukan tindakan di Deadline Cloud

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `awsdeadlinecloud:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awsdeadlinecloud:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `awsdeadlinecloud:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Deadline Cloud.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Deadline Cloud. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Deadline Cloud saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Deadline Cloud mendukung fitur-fitur ini, lihatBagaimana Deadline Cloud bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk Deadline Cloud

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.

- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Deadline Cloud

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

AWS Deadline Cloud tidak mencadangkan data yang disimpan di bucket S3 lampiran pekerjaan Anda. Anda dapat mengaktifkan pencadangan data lampiran pekerjaan Anda menggunakan mekanisme pencadangan Amazon S3 standar apa pun, seperti Pembuatan Versi S3 atau. AWS Backup

Keamanan infrastruktur di Deadline Cloud

Sebagai layanan terkelola, AWS Deadline Cloud dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat

Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Deadline Cloud melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Deadline Cloud tidak mendukung penggunaan kebijakan titik akhir AWS PrivateLink virtual private cloud (VPC). Ini menggunakan kebijakan AWS PrivateLink default, yang memberikan akses penuh ke titik akhir. Untuk informasi selengkapnya, lihat Kebijakan titik akhir default di panduan AWS PrivateLink pengguna.

Analisis konfigurasi dan kerentanan di Deadline Cloud

AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patching database, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk detail selengkapnya, lihat sumber daya berikut:

- Model Tanggung Jawab Bersama
- Amazon Web Services: Gambaran Umum Proses Keamanan (whitepaper)

AWS Deadline Cloud mengelola tugas pada armada yang dikelola layanan atau yang dikelola pelanggan:

- Untuk armada yang dikelola layanan, Deadline Cloud mengelola sistem operasi tamu.
- Untuk armada yang dikelola pelanggan, Anda bertanggung jawab untuk mengelola sistem operasi.

Untuk informasi tambahan tentang konfigurasi dan analisis kerentanan untuk AWS Deadline Cloud, lihat

- Praktik terbaik keamanan untuk Deadline Cloud

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang memilik hak akses lebih tinggi untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi aws:SourceAccountglobal aws:SourceArndan dalam kebijakan sumber daya untuk membatasi izin yang AWS Deadline Cloud memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan kunci konteks kondisi `aws:SourceArn` global dengan Nama Sumber Daya Amazon (ARN) lengkap dari sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks global `aws:SourceArn` dengan karakter wildcard (`*`) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:awsdeadlinecloud:*:123456789012:*`.

Jika nilai `aws:SourceArn` tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global tersebut untuk membatasi izin.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan Deadline Cloud untuk mencegah masalah wakil yang membingungkan.

```
{
```

```
  "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"
      }
    }
  }
}
```

Akses AWS Deadline Cloud menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. AWS Deadline Cloud Anda dapat mengakses Deadline Cloud seolah-olah itu ada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses. Deadline Cloud

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. Deadline Cloud

Deadline Cloud juga memiliki titik akhir dual-stack yang tersedia. Titik akhir dual-stack mendukung permintaan over dan. IPv6 IPv4

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink .

Pertimbangan untuk Deadline Cloud

Sebelum Anda menyiapkan titik akhir antarmuka Deadline Cloud, lihat Mengakses layanan AWS menggunakan titik akhir VPC antarmuka dalam Panduan.AWS PrivateLink

Deadline Cloud mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Secara default, akses penuh ke Deadline Cloud diizinkan melalui titik akhir antarmuka. Atau, Anda dapat mengaitkan grup keamanan dengan antarmuka jaringan titik akhir untuk mengontrol lalu lintas Deadline Cloud melalui titik akhir antarmuka.

Deadline Cloud juga mendukung kebijakan titik akhir VPC. Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir di Panduan.AWS PrivateLink

Deadline Cloud titik akhir

Deadline Cloud menggunakan empat titik akhir untuk akses ke layanan menggunakan AWS PrivateLink - dua untuk IPv4 dan dua untuk IPv6.

Pekerja menggunakan `scheduling.deadline.region.amazonaws.com` endpoint untuk mendapatkan tugas dari antrian, melaporkan kemajuan ke Deadline Cloud, dan mengirim output tugas kembali. Jika Anda menggunakan armada yang dikelola pelanggan, titik akhir penjadwalan adalah satu-satunya titik akhir yang perlu Anda buat kecuali Anda menggunakan operasi manajemen. Misalnya, jika pekerjaan menciptakan lebih banyak pekerjaan, Anda perlu mengaktifkan titik akhir manajemen untuk memanggil `CreateJob` operasi.

Deadline Cloud Monitor menggunakan `management.deadline.region.amazonaws.com` untuk mengelola sumber daya di peternakan Anda, seperti membuat dan memodifikasi antrian dan armada atau mendapatkan daftar pekerjaan, langkah, dan tugas.

Deadline Cloud juga membutuhkan titik akhir untuk titik akhir AWS layanan berikut:

- Deadline Cloud digunakan AWS STS untuk mengautentikasi pekerja sehingga mereka dapat mengakses aset pekerjaan. Untuk informasi selengkapnya AWS STS, lihat Kredensyal keamanan sementara di IAM di Panduan Pengguna.AWS Identity and Access Management
- Jika Anda menyiapkan armada yang dikelola pelanggan di subnet tanpa koneksi internet, Anda harus membuat titik akhir VPC untuk CloudWatch Amazon Logs agar pekerja dapat menulis log. Untuk informasi selengkapnya, lihat Memantau dengan CloudWatch.

- Jika Anda menggunakan lampiran pekerjaan, Anda harus membuat titik akhir VPC untuk Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) sehingga pekerja dapat mengakses lampiran. Untuk informasi selengkapnya, lihat Lampiran Job di Deadline Cloud.

Buat titik akhir untuk Deadline Cloud

Anda dapat membuat titik akhir antarmuka untuk Deadline Cloud menggunakan konsol VPC Amazon atau () AWS Command Line Interface .AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat endpoint manajemen dan penjadwalan untuk Deadline Cloud menggunakan nama layanan berikut. Ganti *region* dengan Wilayah AWS tempat yang Anda gunakan. Deadline Cloud

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

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

Deadline Cloud mendukung titik akhir dual-stack.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API untuk Deadline Cloud menggunakan nama DNS Regional default. Misalnya, `scheduling.deadline.us-east-1.amazonaws.com` untuk operasi pekerja, atau `management.deadline.us-east-1.amazonaws.com` untuk semua operasi lainnya.

Anda juga harus membuat endpoint untuk AWS STS menggunakan nama layanan berikut:

```
com.amazonaws.region.sts
```

Jika armada yang dikelola pelanggan Anda berada di subnet tanpa koneksi internet, Anda harus membuat titik akhir CloudWatch Log menggunakan nama layanan berikut:

```
com.amazonaws.region.logs
```

Jika Anda menggunakan lampiran pekerjaan untuk mentransfer file, Anda harus membuat titik akhir Amazon S3 menggunakan nama layanan berikut:

```
com.amazonaws.region.s3
```

Praktik terbaik keamanan untuk Deadline Cloud

AWS Deadline Cloud (Deadline Cloud) menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

> **Note**
>
> Untuk informasi selengkapnya tentang pentingnya banyak topik keamanan, lihat Model Tanggung Jawab Bersama.

Perlindungan data

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensyal dan menyiapkan akun individual dengan AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon Simple Storage Service (Amazon S3).
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak memasukkan informasi identifikasi sensitif apapun, seperti nomor rekening pelanggan Anda, ke dalam kolom isian teks bebas seperti kolom Nama. Ini

termasuk saat Anda bekerja dengan AWS Deadline Cloud atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke Deadline Cloud atau layanan lain mungkin diambil untuk dimasukkan dalam log diagnostik. Saat Anda memberikan URL ke server eksternal, jangan sertakan informasi kredensyal di URL untuk memvalidasi permintaan Anda ke server tersebut.

AWS Identity and Access Management izin

Kelola akses ke AWS sumber daya menggunakan pengguna, peran AWS Identity and Access Management (IAM), dan dengan memberikan hak istimewa paling sedikit kepada pengguna. Menetapkan kebijakan dan prosedur manajemen kredensyal untuk membuat, mendistribusikan, memutar, dan mencabut AWS kredensyal akses. Untuk informasi selengkapnya, lihat Praktik Terbaik IAM dalam Panduan Pengguna IAM.

Jalankan pekerjaan sebagai pengguna dan grup

Saat menggunakan fungsionalitas antrian di Deadline Cloud, ini adalah praktik terbaik untuk menentukan pengguna sistem operasi (OS) dan grup utamanya sehingga pengguna OS memiliki izin hak istimewa paling sedikit untuk pekerjaan antrian.

Saat Anda menentukan “Jalankan sebagai pengguna” (dan grup), proses apa pun untuk pekerjaan yang dikirimkan ke antrian akan dijalankan menggunakan pengguna OS tersebut dan akan mewarisi izin OS terkait pengguna tersebut.

Konfigurasi armada dan antrian bergabung untuk membangun postur keamanan. Di sisi antrian, peran “Job run as user” dan IAM dapat ditentukan untuk menggunakan OS dan AWS izin untuk pekerjaan antrian. Armada mendefinisikan infrastruktur (host pekerja, jaringan, penyimpanan bersama yang dipasang) yang, ketika dikaitkan dengan antrian tertentu, menjalankan pekerjaan dalam antrian. Data yang tersedia pada host pekerja perlu diakses oleh pekerjaan dari satu atau lebih antrian terkait. Menentukan pengguna atau grup membantu melindungi data dalam pekerjaan dari antrian lain, perangkat lunak lain yang diinstal, atau pengguna lain dengan akses ke host pekerja. Ketika antrian tanpa pengguna, itu berjalan sebagai pengguna agen yang dapat meniru (`sudo`) setiap pengguna antrian. Dengan cara ini, antrian tanpa pengguna dapat meningkatkan hak istimewa ke antrian lain.

Jaringan

Untuk mencegah lalu lintas dicegat atau dialihkan, penting untuk mengamankan bagaimana dan di mana lalu lintas jaringan Anda diarahkan.

Kami menyarankan Anda mengamankan lingkungan jaringan Anda dengan cara berikut:

- Amankan tabel rute subnet Amazon Virtual Private Cloud (Amazon VPC) untuk mengontrol bagaimana lalu lintas lapisan IP dirutekan.
- Jika Anda menggunakan Amazon Route 53 (Route 53) sebagai penyedia DNS di penyiapan farm atau workstation Anda, amankan akses ke API Route 53.
- Jika Anda tersambung ke Deadline Cloud di luar AWS seperti menggunakan workstation lokal atau pusat data lainnya, amankan infrastruktur jaringan lokal. Ini termasuk server DNS dan tabel rute pada router, switch, dan perangkat jaringan lainnya.

Pekerjaan dan data pekerjaan

Tenggat waktu pekerjaan Cloud berjalan dalam sesi di host pekerja. Setiap sesi menjalankan satu atau lebih proses pada host pekerja, yang umumnya mengharuskan Anda memasukkan data untuk menghasilkan output.

Untuk mengamankan data ini, Anda dapat mengonfigurasi pengguna sistem operasi dengan antrian. Agen pekerja menggunakan pengguna OS antrian untuk menjalankan sub-proses sesi. Sub-proses ini mewarisi izin pengguna OS antrian.

Kami menyarankan Anda mengikuti praktik terbaik untuk mengamankan akses ke data akses sub-proses ini. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

Struktur pertanian

Anda dapat mengatur armada Deadline Cloud dan antrian banyak cara. Namun, ada implikasi keamanan dengan pengaturan tertentu.

Sebuah peternakan memiliki salah satu batas paling aman karena tidak dapat berbagi sumber daya Deadline Cloud dengan peternakan lain, termasuk armada, antrian, dan profil penyimpanan. Namun, Anda dapat berbagi AWS sumber daya eksternal di dalam peternakan, yang membahayakan batas keamanan.

Anda juga dapat menetapkan batas keamanan antara antrian dalam peternakan yang sama menggunakan konfigurasi yang sesuai.

Ikuti praktik terbaik ini untuk membuat antrian aman di peternakan yang sama:

- Kaitkan armada hanya dengan antrian dalam batas keamanan yang sama. Perhatikan hal berikut:

  - Setelah pekerjaan berjalan di host pekerja, data mungkin tetap tertinggal, seperti di direktori sementara atau direktori home pengguna antrian.
  - Pengguna OS yang sama menjalankan semua pekerjaan pada host pekerja armada milik layanan, terlepas dari antrian mana Anda mengirimkan pekerjaan.
  - Pekerjaan mungkin membiarkan proses berjalan pada host pekerja, sehingga memungkinkan pekerjaan dari antrian lain untuk mengamati proses berjalan lainnya.
- Pastikan hanya antrian dalam batas keamanan yang sama yang berbagi bucket Amazon S3 untuk lampiran pekerjaan.
- Pastikan bahwa hanya antrian dalam batas keamanan yang sama berbagi pengguna OS.
- Amankan AWS sumber daya lain yang terintegrasi ke dalam pertanian hingga batas.

Antrian lampiran pekerjaan

Lampiran Job dikaitkan dengan antrian, yang menggunakan bucket Amazon S3 Anda.

- Lampiran Job menulis dan membaca dari awalan root di bucket Amazon S3. Anda menentukan awalan root ini dalam panggilan `CreateQueue` API.
- Bucket memiliki kode yang sesuai`Queue Role`, yang menentukan peran yang memberi pengguna antrian akses ke awalan bucket dan root. Saat membuat antrian, Anda menentukan Nama Sumber Daya `Queue Role` Amazon (ARN) di samping bucket lampiran pekerjaan dan awalan root.
- Panggilan resmi ke`AssumeQueueRoleForRead`,`AssumeQueueRoleForUser`, dan operasi `AssumeQueueRoleForWorker` API mengembalikan satu set kredensil keamanan sementara untuk. `Queue Role`

Jika Anda membuat antrian dan menggunakan kembali bucket Amazon S3 dan awalan root, ada risiko informasi diungkapkan kepada pihak yang tidak berwenang. Misalnya, QueueA dan QueueB berbagi bucket dan awalan root yang sama. Dalam alur kerja yang aman, ArtisTa memiliki akses ke QueueA tetapi tidak QueueB. Namun, ketika beberapa antrian berbagi bucket, ArtisTA dapat mengakses data dalam data QueueB karena menggunakan bucket dan awalan root yang sama dengan QueueA.

Konsol mengatur antrian yang aman secara default. Pastikan antrian memiliki kombinasi yang berbeda antara bucket Amazon S3 dan awalan root kecuali mereka merupakan bagian dari batas keamanan umum.

Untuk mengisolasi antrian Anda, Anda harus mengonfigurasi `Queue Role` untuk hanya mengizinkan akses antrian ke bucket dan awalan root. Dalam contoh berikut, ganti masing-masing *placeholder* dengan informasi spesifik sumber daya Anda.

```
{
  "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/*"
    }
  ]
}
```

Anda juga harus menetapkan kebijakan kepercayaan tentang peran tersebut. Dalam contoh berikut, ganti *placeholder* teks dengan informasi spesifik sumber daya Anda.

```
{
  "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 perangkat lunak khusus

Anda dapat menambahkan pernyataan berikut ke perangkat lunak khusus `Queue Role` untuk mengakses perangkat lunak khusus di bucket Amazon S3 Anda. Dalam contoh berikut, ganti *SOFTWARE_BUCKET_NAME* dengan nama bucket S3 Anda.

```
"Statement": [
    {
        "Action": [
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME",
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME/*"
        ]
    }
]
```

Untuk informasi selengkapnya tentang praktik terbaik keamanan Amazon S3, lihat Praktik terbaik keamanan untuk Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Tuan rumah pekerja

Host pekerja aman untuk membantu memastikan bahwa setiap pengguna hanya dapat melakukan operasi untuk peran yang ditetapkan.

Kami merekomendasikan praktik terbaik berikut untuk mengamankan host pekerja:

- Menggunakan skrip konfigurasi host dapat mengubah keamanan dan operasi pekerja. Konfigurasi yang salah dapat menyebabkan pekerja menjadi tidak stabil atau berhenti bekerja. Adalah tanggung jawab Anda untuk men-debug kegagalan tersebut.
- Jangan gunakan `jobRunAsUser` nilai yang sama dengan beberapa antrian kecuali pekerjaan yang dikirimkan ke antrian tersebut berada dalam batas keamanan yang sama.
- Jangan atur antrian `jobRunAsUser` ke nama pengguna OS yang dijalankan oleh agen pekerja.
- Berikan izin OS dengan hak istimewa paling sedikit kepada pengguna antrian yang diperlukan untuk beban kerja antrian yang dimaksud. Pastikan bahwa mereka tidak memiliki izin menulis sistem file untuk bekerja file program agen atau perangkat lunak bersama lainnya.
- Pastikan hanya pengguna root yang aktif Linux dan `Administrator` memiliki akun sendiri Windows dan dapat memodifikasi file program agen pekerja.
- Pada host Linux pekerja, pertimbangkan untuk mengonfigurasi `umask` penggantian `/etc/sudoers` yang memungkinkan pengguna agen pekerja meluncurkan proses sebagai pengguna antrian. Konfigurasi ini membantu memastikan pengguna lain tidak dapat mengakses file yang ditulis ke antrian.
- Berikan individu tepercaya akses paling tidak memiliki hak istimewa ke host pekerja.
- Batasi izin untuk mengganti file konfigurasi DNS lokal (`/etc/hosts`aktif dan aktifWindows), Linux dan untuk merutekan tabel `C:\Windows\system32\etc\hosts` di workstation dan sistem operasi host pekerja.
- Batasi izin untuk konfigurasi DNS pada workstation dan sistem operasi host pekerja.
- Secara teratur menambal sistem operasi dan semua perangkat lunak yang diinstal. Pendekatan ini mencakup perangkat lunak yang khusus digunakan dengan Deadline Cloud seperti submitter, adaptor, agen pekerja, OpenJD paket, dan lain-lain.
- Gunakan kata sandi yang kuat untuk Windows antrian`jobRunAsUser`.
- Putar kata sandi untuk antrian `jobRunAsUser` Anda secara teratur.
- Pastikan akses hak istimewa paling sedikit ke rahasia Windows kata sandi dan hapus rahasia yang tidak digunakan.

- Jangan berikan `jobRunAsUser` izin antrian perintah jadwal untuk dijalankan di masa mendatang:
  - PadaLinux, tolak akses akun ini ke `cron` dan`at`.
  - OnWindows, tolak akses akun ini ke penjadwal Windows tugas.

> **Note**
>
> Untuk informasi selengkapnya tentang pentingnya menambal sistem operasi dan perangkat lunak yang diinstal secara teratur, lihat Model Tanggung Jawab Bersama.

Skrip konfigurasi host

- Menggunakan skrip konfigurasi host dapat mengubah keamanan dan operasi pekerja. Konfigurasi yang salah dapat menyebabkan pekerja menjadi tidak stabil atau berhenti bekerja. Adalah tanggung jawab Anda untuk men-debug kegagalan tersebut.

Workstation

Sangat penting untuk mengamankan workstation dengan akses ke Deadline Cloud. Pendekatan ini membantu memastikan bahwa pekerjaan apa pun yang Anda kirimkan ke Deadline Cloud tidak dapat menjalankan beban kerja sewenang-wenang yang ditagih ke Anda. Akun AWS

Kami merekomendasikan praktik terbaik berikut untuk mengamankan workstation artis. Untuk informasi selengkapnya, lihat Model Tanggung Jawab Bersama.

- Amankan semua kredensil tetap yang menyediakan akses ke AWS, termasuk Deadline Cloud. Untuk informasi lebih lanjut, lihat Mengelola access key untuk pengguna IAM dalam Panduan Pengguna IAM.
- Hanya instal perangkat lunak tepercaya dan aman.
- Mengharuskan pengguna berfederasi dengan penyedia identitas untuk mengakses AWS dengan kredensi sementara.
- Gunakan izin aman pada file program submitter Deadline Cloud untuk mencegah gangguan.
- Berikan individu tepercaya akses paling tidak istimewa ke workstation artis.
- Hanya gunakan pengirim dan adaptor yang Anda dapatkan melalui Deadline Cloud Monitor.

- Batasi izin ke DNS lokal mengganti file konfigurasi (`/etc/hosts`on Linux danmacOS, dan `C:\Windows\system32\etc\hosts` onWindows), dan untuk merutekan tabel pada workstation dan sistem operasi host pekerja.
- Batasi izin `/etc/resolve.conf` pada workstation dan sistem operasi host pekerja.
- Secara teratur menambal sistem operasi dan semua perangkat lunak yang diinstal. Pendekatan ini mencakup perangkat lunak yang khusus digunakan dengan Deadline Cloud seperti submitter, adaptor, agen pekerja, OpenJD paket, dan lain-lain.

Verifikasi keaslian perangkat lunak yang diunduh

Verifikasi keaslian perangkat lunak Anda setelah mengunduh penginstal untuk melindungi dari gangguan file. Prosedur ini berfungsi untuk keduanya Windows dan Linux sistem.

Windows

Untuk memverifikasi keaslian file yang Anda unduh, selesaikan langkah-langkah berikut.

1. Dalam perintah berikut, ganti *`file`* dengan file yang ingin Anda verifikasi. Misalnya, ***`C:\PATH\TO\MY\`*`DeadlineCloudSubmitter-windows-x64-installer.exe`** . Juga, ganti *`signtool-sdk-version`* dengan versi SignTool SDK yang diinstal. Misalnya, **`10.0.22000.0`**.

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

2. Misalnya, Anda dapat memverifikasi file installer submitter Deadline Cloud dengan menjalankan perintah berikut:

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

Linux

Untuk memverifikasi keaslian file yang Anda unduh, gunakan alat baris gpg perintah.

1. Impor OpenPGP kunci dengan menjalankan perintah berikut:

   ```
   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. Tentukan apakah akan mempercayai OpenPGP kuncinya. Beberapa faktor yang perlu dipertimbangkan ketika memutuskan apakah akan mempercayai kunci di atas termasuk yang berikut:

   - Koneksi internet yang Anda gunakan untuk mendapatkan kunci GPG dari situs web ini aman.
   - Perangkat tempat Anda mengakses situs web ini aman.
   - AWS telah mengambil langkah-langkah untuk mengamankan hosting kunci OpenPGP publik di situs web ini.

3. Jika Anda memutuskan untuk mempercayai OpenPGP kunci, edit kunci untuk dipercaya dengan gpg mirip dengan contoh berikut:

```
$ 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. Verifikasi penginstal pengirim Cloud Deadline

   Untuk memverifikasi installer submitter Deadline Cloud, selesaikan langkah-langkah berikut:

a. Kembali ke halaman Unduhan konsol Cloud Deadline dan unduh file tanda tangan untuk penginstal pengirim Deadline Cloud.

b. Verifikasi tanda tangan penginstal submitter Deadline Cloud dengan menjalankan:

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

5. Verifikasi monitor Cloud Deadline

> **Note**
>
> Anda dapat memverifikasi unduhan monitor Deadline Cloud menggunakan file tanda tangan atau metode khusus platform. Untuk metode khusus platform, lihat Linux (Debian) tab, tab Linux (RPM), atau Linux (AppImage) tab berdasarkan jenis file yang Anda unduh.

Untuk memverifikasi aplikasi desktop monitor Deadline Cloud dengan file tanda tangan, selesaikan langkah-langkah berikut:

a. Kembali ke halaman Unduhan konsol Cloud Deadline dan unduh file.sig yang sesuai, lalu jalankan

Untuk.deb:

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

Untuk.rpm:

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

Untuk. AppImage:

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

b. Konfirmasikan bahwa output terlihat mirip dengan yang berikut:

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

gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Jika output berisi frasa`Good signature from "AWS Deadline Cloud"`, itu berarti tanda tangan telah berhasil diverifikasi dan Anda dapat menjalankan skrip instalasi monitor Deadline Cloud.

Linux (AppImage)

Untuk memverifikasi paket yang menggunakan fileLinux. AppImage biner, pertama selesaikan langkah 1-3 di Linux tab, lalu selesaikan langkah-langkah berikut.

1. Dari AppImageUpdate halaman di GitHub, unduh validate-x86_64. AppImageberkas.
2. Setelah mengunduh file, untuk menambahkan izin eksekusi, jalankan perintah berikut.

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

3. Untuk menambahkan izin eksekusi, jalankan perintah berikut.

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

4. Untuk memverifikasi tanda tangan monitor Deadline Cloud, jalankan perintah berikut.

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

Jika output berisi frasa`Validation successful`, itu berarti tanda tangan telah berhasil diverifikasi dan Anda dapat menjalankan skrip instalasi monitor Deadline Cloud dengan aman.

Linux (Debian)

Untuk memverifikasi paket yang menggunakan Linux biner.deb, pertama-tama selesaikan langkah 1-3 di tab. Linux

dpkg adalah alat manajemen paket inti di sebagian besar distribusi debian berbasisLinux. Anda dapat memverifikasi file.deb dengan alat ini.

1. Dari halaman Unduhan Konsol Cloud Deadline, unduh file Deadline Cloud monitor .deb.
2. Ganti *<APP_VERSION>* dengan versi file.deb yang ingin Anda verifikasi.

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

3. Outputnya akan mirip dengan:

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

4. Untuk memverifikasi file.deb, konfirmasikan bahwa `GOODSIG` ada dalam output.

Linux (RPM)

Untuk memverifikasi paket yang menggunakan Linux biner.rpm, pertama-tama selesaikan langkah 1-3 di Linux tab.

1. Dari halaman Unduhan Konsol Cloud Deadline, unduh file monitor Deadline Cloud .rpm.
2. Ganti *<APP_VERSION>* dengan versi file.rpm untuk memverifikasi.

```
gpg --export --armor "Deadline Cloud" > key.pub
sudo rpm --import key.pub
rpm -K deadline-cloud-monitor-<APP_VERSION>-1.x86_64.rpm
```

3. Outputnya akan mirip dengan:

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

4. Untuk memverifikasi file.rpm, konfirmasikan yang `digests signatures OK` ada di output.

AWS Batas Waktu Pemantauan Cloud

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS Deadline Cloud (Deadline Cloud) dan solusi Anda AWS . Kumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. Sebelum Anda mulai memantau Deadline Cloud, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan-pertanyaan berikut:

- Apa tujuan pemantauan Anda?
- Sumber daya manakah yang akan Anda pantau?
- Seberapa seringkah Anda akan memantau sumber daya ini?
- Apa sajakah alat pemantauan yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

AWS dan Deadline Cloud menyediakan alat yang dapat Anda gunakan untuk memantau sumber daya Anda dan menanggapi potensi insiden. Beberapa alat ini melakukan pemantauan untuk Anda, beberapa alat memerlukan intervensi manual. Anda harus mengotomatiskan tugas pemantauan sebanyak mungkin.

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari EC2 instans Amazon Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

  Deadline Cloud memiliki tiga CloudWatch metrik.

- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari EC2 instans Amazon CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.

- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengembang Cloud Deadline:

- CloudTraillog
- Mengelola acara menggunakan EventBridge
- Monitoring dengan CloudWatch

Kuota untuk Deadline Cloud

AWS Deadline Cloud menyediakan sumber daya, seperti peternakan, armada, dan antrian, yang dapat Anda gunakan untuk memproses pekerjaan. Saat Anda membuat Akun AWS, kami menetapkan kuota default pada sumber daya ini untuk masing-masing Wilayah AWS.

Service Quotas adalah lokasi pusat di mana Anda dapat melihat dan mengelola kuota Anda. Layanan AWS Anda juga dapat meminta peningkatan kuota untuk banyak sumber daya yang Anda gunakan.

Untuk melihat kuota Deadline Cloud, buka konsol Service Quotas. Di panel navigasi, pilih Layanan AWSdan pilih Deadline Cloud.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas. Jika kuota belum tersedia di Service Quotas, gunakan formulir peningkatan kuota layanan.

AWS Akun Anda memiliki kuota berikut yang terkait Deadline Cloud dengan.

Nama	Default	Dapat disesuaikan	Deskripsi
Anggota terkait per peternakan	Setiap Wilayah yang didukung: 75	Tidak	Jumlah maksimum anggota yang dapat dikaitkan dengan setiap peternakan di AWS Wilayah saat ini.
Anggota terkait per armada	Setiap Wilayah yang didukung: 75	Tidak	Jumlah maksimum anggota yang dapat dikaitkan dengan setiap armada di AWS Wilayah saat ini.
Anggota terkait per pekerjaan	Setiap Wilayah yang didukung: 75	Tidak	Jumlah maksimum anggota yang dapat dikaitkan dengan setiap pekerjaan di AWS Wilayah saat ini.

Nama	Default	Dapat disesuaikan	Deskripsi
Anggota terkait per antrian	Setiap Wilayah yang didukung: 75	Tidak	Jumlah maksimum anggota yang dapat dikaitkan dengan setiap antrian di AWS Wilayah saat ini.
Anggaran per peternakan	Setiap Wilayah yang didukung: 20	Ya	Jumlah maksimum anggaran per peternakan di Wilayah saat ini AWS
Peternakan per wilayah	Setiap Wilayah yang didukung: 2	Ya	Jumlah maksimum peternakan yang dapat dibuat di AWS Wilayah saat ini.
Armada per peternakan	Setiap Wilayah yang didukung: 5	Ya	Jumlah maksimum armada yang dapat dibuat untuk setiap peternakan di AWS Wilayah saat ini.
Pekerjaan per peternakan	Setiap Wilayah yang didukung: 100.000	Ya	Jumlah maksimum pekerjaan per pertanian di AWS Wilayah saat ini.
Titik akhir lisensi per wilayah	Setiap Wilayah yang didukung: 5	Ya	Jumlah maksimum titik akhir lisensi di AWS Wilayah saat ini.
Sesi lisensi per titik akhir lisensi	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum sesi lisensi per titik akhir lisensi di AWS Wilayah saat ini.

Nama	Default	Dapat disesuaikan	Deskripsi
Batas per peternakan	Setiap Wilayah yang didukung: 50	Ya	Jumlah maksimum batas yang dapat dibuat untuk setiap peternakan di AWS Wilayah saat ini.
Monitor per wilayah	Setiap Wilayah yang didukung: 1	Tidak	Jumlah maksimum monitor di AWS Wilayah saat ini.
OnDemand G contoh GPUs per wilayah	Setiap Wilayah yang didukung: 1	Ya	Jumlah maksimum instans G sesuai permintaan GPUs yang dapat disediakan di semua armada yang dikelola layanan di Wilayah saat ini. AWS
OnDemand v CPUs per wilayah	Setiap Wilayah yang didukung: 50	Ya	Jumlah maksimum on-demand v CPUs yang dapat disediakan di semua armada yang dikelola layanan di Wilayah saat ini. AWS
Lingkungan antrian per antrian	Setiap Wilayah yang didukung: 10	Tidak	Jumlah maksimum lingkungan antrian yang dapat dibuat untuk setiap antrian di Wilayah saat ini AWS .
Asosiasi armada antrian per peternakan	Setiap Wilayah yang didukung: 100	Ya	Jumlah maksimum asosiasi armada antrian per peternakan di Wilayah saat ini AWS

Nama	Default	Dapat disesuaikan	Deskripsi
Asosiasi batas antrian per antrian	Setiap Wilayah yang didukung: 10	Ya	Jumlah maksimum batas yang dapat dikaitkan dengan setiap antrian di AWS Wilayah saat ini.
Antrian per peternakan	Setiap Wilayah yang didukung: 20	Ya	Jumlah maksimum antrian yang dapat dibuat untuk setiap peternakan di Wilayah saat ini AWS .
Instans Spot G GPUs per wilayah	Setiap Wilayah yang didukung: 1	Ya	Jumlah maksimum instans G spot GPUs yang dapat disediakan di semua armada yang dikelola layanan di Wilayah saat ini. AWS
Spot v CPUs per wilayah	Setiap Wilayah yang didukung: 500	Ya	Jumlah maksimum spot v CPUs yang dapat disediakan di semua armada yang dikelola layanan di Wilayah saat ini. AWS
Langkah per pekerjaan	Setiap Wilayah yang didukung: 200	Ya	Jumlah maksimum langkah per pekerjaan di AWS Wilayah saat ini.
Penyimpanan untuk volume SSD Tujuan Umum (gp3) dalam TiB	Setiap Wilayah yang didukung: 50	Ya	Jumlah agregat maksimum penyimpanan EBS, diukur dalam TiB, yang dapat digunakan di semua armada di Wilayah saat ini. AWS

Nama	Default	Dapat disesuaikan	Deskripsi
Profil penyimpanan per peternakan	Setiap Wilayah yang didukung: 50	Tidak	Jumlah maksimum profil penyimpanan yang dapat dibuat untuk setiap peternakan di AWS Wilayah saat ini.
Tugas per pekerjaan	Setiap Wilayah yang didukung: 10.000	Ya	Jumlah maksimum tugas per pekerjaan di AWS Wilayah saat ini.
Tugas per langkah	Setiap Wilayah yang didukung: 10.000	Ya	Jumlah maksimum tugas per langkah di AWS Wilayah saat ini.
Pekerja per peternakan	Setiap Wilayah yang didukung: 7.500	Tidak	Jumlah maksimum pekerja per peternakan di AWS Wilayah saat ini.

Membuat sumber daya Cloud AWS Deadline dengan AWS CloudFormation

AWS Deadline Cloud terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti peternakan, antrian, dan armada), serta menyediakan serta mengonfigurasi sumber AWS CloudFormation daya tersebut untuk Anda.

Bila Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya Deadline Cloud Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Tenggat waktu Cloud dan template AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk Deadline Cloud dan layanan terkait, Anda harus memahami AWS CloudFormation templat. Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi selengkapnya, lihat Apa itu AWS CloudFormation Designer? di Panduan Pengguna AWS CloudFormation .

Deadline Cloud mendukung pembuatan peternakan, antrian, dan armada. AWS CloudFormationUntuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk farm, antrian, dan armada, lihat AWS Deadline Cloud di Panduan Pengguna.AWS CloudFormation

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation Referensi API

- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Pemecahan Masalah

Prosedur dan tips berikut dapat membantu Anda memecahkan masalah dengan pertanian dan sumber daya AWS Deadline Cloud Anda.

Topik

Mengapa pengguna tidak dapat melihat peternakan, armada, atau antrian saya?

Akses pengguna

Saat pengguna Anda tidak melihat peternakan, armada, atau antrian Anda di monitor Deadline Cloud, mungkin ada masalah dengan akses mereka ke pertanian dan sumber daya Anda.

Pengguna tanpa akses ke peternakan apa pun menerima pesan “Tidak ada peternakan yang tersedia” di monitor Deadline Cloud.

Untuk mengonfirmasi bahwa Anda memiliki pengguna atau grup yang benar yang ditetapkan ke peternakan, armada, atau antrian Anda

1. Di konsol AWS Deadline Cloud, temukan farm, armada, atau antrian Anda, lalu pilih Manajemen akses.
2. Tab grup dipilih secara default. Jika Anda menetapkan izin berdasarkan grup, yang direkomendasikan, grup Anda harus ditampilkan dalam daftar dan memiliki tingkat akses yang ditetapkan.

   Jika grup tidak ada dalam daftar, pilih Tambahkan grup untuk menetapkan izin untuk grup.
3. Jika Anda menetapkan izin oleh pengguna, pilih tab Pengguna. Pengguna Anda harus ditampilkan dalam daftar dan memiliki tingkat akses yang ditetapkan.

Jika pengguna Anda tidak ada dalam daftar, pilih Tambahkan pengguna untuk menetapkan izin bagi pengguna.

Untuk mengonfirmasi bahwa Anda telah menetapkan pengguna ke grup Anda

1. Di konsol AWS Deadline Cloud, temukan farm, armada, atau antrian Anda, lalu pilih Manajemen akses.
2. Tab grup dipilih secara default. Pilih nama grup untuk melihat anggotanya.
3. Jika pengguna tidak terdaftar dalam grup, mereka harus ditambahkan.

   Jika Anda menggunakan pengaturan identitas default, Anda dapat langsung menambahkan pengguna ke grup di konsol Pusat Identitas. Jika Anda terhubung ke penyedia identitas eksternal seperti Okta atau Google Workspace, Anda dapat menambahkan pengguna Anda ke grup di penyedia identitas Anda.

   > **Note**
   >
   > Beberapa penyedia identitas eksternal menyinkronkan pengguna tetapi tidak mengelompokkan ke Pusat Identitas. Dalam hal ini, pertimbangkan untuk menetapkan izin kepada pengguna secara langsung, bukan berdasarkan grup.

Untuk informasi selengkapnya tentang mengelola akses pengguna ke Deadline Cloud, lihatMengelola pengguna di Deadline Cloud.

Mengapa pekerja tidak mengambil pekerjaan saya?

Konfigurasi peran armada

Terkadang ketika pekerja dibuat tetapi tidak menyelesaikan inisialisasi dan tidak mulai mengerjakan pekerjaan, itu karena peran armada tidak dikonfigurasi dengan benar.

Untuk memverifikasi ini adalah apa yang terjadi, periksa CloudTrail log Anda untuk setiap kesalahan akses ditolak. Setelah Anda mengonfirmasi masalah akses ditolak, buka armada Anda dan perbarui konfigurasi peran ke izin yang benar. Untuk informasi selengkapnya, lihat CloudTraillog di panduan pengembang Deadline Cloud.

Mengapa pekerja saya terjebak berlari?

Pekerja terjebak keluar dari lingkungan OpenJD

Pekerja bisa terjebak dalam tindakan `envExit` sesi yang berjalan lama. Ini mungkin terjadi jika Anda menggunakan template pekerjaan yang mengganti template OpenJD dan menetapkan batas waktu tindakan keluar lingkungan menjadi lebih dari 5 menit. Monitor Deadline Cloud memberikan beberapa visibilitas ke pekerja yang terjebak dalam situasi ini, tetapi membutuhkan `RUNNING` pekerja referensi silang terhadap pekerjaan yang tersedia dalam antrian terkait.

Untuk menemukan pekerja yang macet, telusuri semua armada di monitor Deadline Cloud dan selesaikan langkah-langkah berikut:

1. Di kolom status pekerja, temukan `RUNNING` pekerja.
2. Dari bagian Detail Armada, arahkan ke setiap antrian terkait.
3. Di setiap antrian terkait, cari pekerjaan yang`RUNNING`,`READY`, atau`PENDING`. Jika semua antrian terkait tidak memiliki pekerjaan di negara bagian tersebut, maka pekerja tersebut menjalankan jalan keluar lingkungan.

Untuk menghentikan pekerja terjebak dalam status ini, gunakan AWS CLI perintah berikut:

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

Setelah menjalankan perintah, agen pekerja memulai ulang saat program keluar. Pekerja kemudian kembali online dan menjalankan lebih banyak pekerjaan dari antrian terkait. Jika antrian berisi lebih banyak pekerjaan dengan batas waktu tindakan keluar lingkungan lebih dari 5 menit, pekerja akan macet lagi. Jika ini terjadi, Anda harus mengulangi proses ini sampai tidak ada lagi pekerja yang terjebak keluar.

Untuk menghindari masalah ini, setel opsi batas waktu tidak lebih dari 5 menit saat menggunakan templat pekerjaan.

Memecahkan masalah Deadline pekerjaan Cloud

Untuk informasi tentang masalah umum dengan pekerjaan di AWS Deadline Cloud, lihat topik berikut.

Mengapa membuat pekerjaan saya gagal?

Beberapa kemungkinan alasan bahwa pekerjaan dapat gagal dalam pemeriksaan validasi meliputi:

- Template pekerjaan tidak mengikuti spesifikasi OpenJD.
- Pekerjaan itu mengandung terlalu banyak langkah.
- Pekerjaan itu mengandung terlalu banyak tugas total.
- Ada kesalahan layanan internal yang mencegah pekerjaan dibuat.

Untuk melihat kuota untuk jumlah maksimum langkah dan tugas dalam suatu pekerjaan, gunakan konsol Service Quotas. Untuk informasi selengkapnya, lihat Kuota untuk Deadline Cloud.

Mengapa pekerjaan saya tidak kompatibel?

Alasan umum bahwa pekerjaan tidak kompatibel dengan antrian meliputi:

- Tidak ada armada yang terkait dengan antrian tempat pekerjaan itu diserahkan. Buka monitor Deadline Cloud, dan periksa apakah antrian memiliki armada terkait. Untuk informasi selengkapnya tentang cara melihat antrian, lihat. Lihat detail antrian dan armada di Deadline Cloud
- Pekerjaan tersebut memiliki persyaratan tuan rumah yang tidak dipenuhi oleh armada mana pun yang terkait dengan antrian. Untuk memeriksanya, bandingkan `hostRequirements` entri dalam templat pekerjaan dengan konfigurasi armada di peternakan Anda. Pastikan salah satu armada memenuhi persyaratan tuan rumah. Untuk informasi selengkapnya tentang kompatibilitas armada, lihat Menentukan kompatibilitas armada. Untuk melihat konfigurasi armada, lihatLihat detail antrian dan armada di Deadline Cloud.

Mengapa pekerjaan saya terjebak siap?

Kemungkinan alasan pekerjaan Anda tampak macet di `READY` negara bagian termasuk yang berikut:

- Jumlah pekerja maksimum untuk armada yang terkait dengan antrian diatur ke nol. Untuk memeriksa, lihatLihat detail antrian dan armada di Deadline Cloud.

- Ada pekerjaan prioritas yang lebih tinggi dalam antrian. Untuk memeriksa, lihatLihat detail antrian dan armada di Deadline Cloud.
- Untuk armada yang dikelola pelanggan, periksa konfigurasi penskalaan otomatis. Untuk informasi selengkapnya, lihat Membuat infrastruktur armada dengan grup Amazon EC2 Auto Scaling di Panduan Pengembang Cloud Batas Waktu.

Mengapa pekerjaan saya gagal?

Pekerjaan bisa gagal karena berbagai alasan. Untuk mencari masalah, buka monitor Deadline Cloud dan pilih pekerjaan yang gagal. Pilih tugas yang gagal lalu lihat log untuk tugas tersebut. Untuk petunjuk, lihat Lihat sesi dan log pekerja di Deadline Cloud.

- Jika Anda melihat kesalahan lisensi atau jika Anda mendapatkan tanda air yang terjadi karena perangkat lunak tidak memiliki lisensi yang valid, pastikan pekerja dapat terhubung ke server lisensi yang diperlukan. Untuk informasi selengkapnya, lihat Connect armada yang dikelola pelanggan ke titik akhir lisensi di Panduan Pengembang Cloud Deadline.
- Pesan tindakan sesi terakhir atau kode keluar proses dapat memberikan informasi tentang mengapa pekerjaan Anda gagal. Jika Anda menggunakan Windows dan kode keluar Anda negatif, coba cari versi kode keluar Anda yang tidak ditandatangani:

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

Mengapa langkah saya tertunda?

Langkah-langkah mungkin tetap dalam `PENDING` keadaan ketika satu atau lebih dependensi mereka tidak lengkap. Anda dapat memeriksa status dependensi menggunakan monitor Deadline Cloud. Untuk petunjuk, lihat Lihat langkah di Deadline Cloud.

Sumber daya tambahan

Anda dapat menemukan informasi dan sumber daya tambahan di GitHub.

Riwayat dokumen untuk panduan pengguna Deadline Cloud

Tabel berikut menjelaskan perubahan penting dalam setiap rilis panduan pengguna AWS Deadline Cloud.

Perubahan	Deskripsi	Tanggal
AWS Pembaruan kebijakan terkelola	Memperbarui kebijakan AWS AWSDeadlineCloud-WorkerHostterkelola yang ada. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk Deadline Cloud.	30 Mei 2025
Penginstal pengirim Adobe After Effects	Menambahkan instruksi untuk menambahkan penginstal pengirim Adobe After Effects ke perangkat lunak pembuatan konten digital Anda. Untuk informasi selengkapnya, lihat Adobe After Effects.	Februari 13, 2025
Pemecahan Masalah	Menambahkan informasi untuk memecahkan masalah Deadline Cloud. Untuk informasi selengkapnya, lihat Pemecahan Masalah.	Februari 7, 2025
Batas sumber daya Job	Menambahkan dokumentasi untuk batas sumber daya pekerjaan baru dan jumlah maksimum host pekerja. Untuk informasi selengkapnya, lihat Membuat batas sumber daya untuk pekerjaan.	Januari 30, 2025

Adobe Setelah Efek UBL	Menambahkan informasi tentang lisensi berbasis penggunaan Adobe After Effects (UBL) untuk Deadline Cloud. Untuk informasi selengkapnya, lihat Connect ke titik akhir lisensi.	Januari 30, 2025
Konten yang direorganisasi dari panduan pengguna	Memindahkan konten yang berfokus pada pengemban g dari panduan pengguna ke panduan pengembang: • Memindahkan instruksi untuk membuat armada yang dikelola pelanggan ke chapter armada baru yang dikelola Pelanggan dalam panduan pengembang. • Memindahkan informasi tentang penggunaan lisensi Anda sendiri ke bagian baru Menggunakan lisensi perangkat lunak dalam panduan pengembang. • Memindahkan detail tentang pemantauan dengan CloudTrail CloudWatch,, dan EventBridge ke bagian Pemantauan di panduan pengembang.	Januari 6, 2025

Acara ambang anggaran	Menambahkan EventBridge acara ambang anggaran baru. Untuk informasi selengkapnya, lihat referensi detail peristiwa Deadline Cloud.	Oktober 30, 2024
Acara status Job	Menambahkan pekerjaan baru dan EventBridge acara status tugas. Untuk informasi selengkapnya, lihat referensi detail peristiwa Deadline Cloud.	Oktober 24, 2024
Kirim ulang pekerjaan	Menambahkan informasi tentang cara mengirimkan kembali pekerjaan. Untuk informasi selengkapnya, lihat Mengirim ulang pekerjaan.	Oktober 7, 2024
AWS Pembaruan kebijakan terkelola	Memperbarui kebijakan AWS terkelola yang ada. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk Deadline Cloud.	Oktober 7, 2024
Bawa lisensi Anda sendiri	Menambahkan informasi tentang bagaimana Anda dapat menggunakan server lisensi atau instance proxy lisensi Anda sendiri dengan Deadline Cloud. Untuk informasi selengkapnya, lihat Armada yang dikelola layanan.	Juli 26, 2024

Autodesk 3ds Maks UBL	Menambahkan informasi tentang lisensi berbasis penggunaan Autodesk 3ds Max (UBL) untuk Deadline Cloud. Untuk informasi selengkapnya, lihat Connect ke titik akhir lisensi.	Juni 18, 2024
Fitur pemantauan dan manajemen biaya	Anda dapat menggunak an EventBridge untuk mendukung pemantauan di Deadline Cloud. Untuk informasi selengkapnya, lihat Bertindak atas EventBrid ge acara. Deadline Cloud menyediakan anggaran dan penjelajah penggunaan untuk membantu Anda mengontrol dan memvisualisasikan biaya untuk pekerjaan Anda. Pelajari tentang beberapa praktik terbaik untuk membantu mengelola biaya tersebut. Untuk informasi selengkapnya, lihat Manajemen biaya.	23 Mei 2024
Rilis awal	Ini adalah rilis awal panduan pengguna Deadline Cloud.	April 2, 2024

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.