사용자 가이드

AWS 기한 클라우드

버전 latest

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 기한 클라우드: 사용자 가이드

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

Deadline Cloud란 무엇입니까? 1
Deadline Cloud의 기능 1
개념 및 용어 2
Deadline Cloud 시작하기 4
기한 클라우드 액세스 5
관련 서비스 5
Deadline Cloud 작동 방식 6
..... 6
Deadline Cloud의 권한 6
Deadline Cloud를 통한 소프트웨어 지원 7
시작 9
설정 AWS 계정 9
모니터 설정 10
모니터 생성 10
팜 세부 정보 정의 12
대기열 세부 정보 정의 13
플릿 세부 정보 정의 14
검토 및 생성 15
제출자 설정 15
1단계: Deadline Cloud 제출자 설치 16
2단계: Deadline Cloud Monitor 설치 및 설정 19
3단계: Deadline Cloud 제출자 시작 23
지원되는 제출자 24
모니터 사용 30
Deadline Cloud Monitor URL 공유 30
Deadline Cloud 모니터 열기 31
언어 설정 변경 32
대기열 및 플릿 세부 정보 보기 33
작업, 단계 및 작업 관리 34
작업 세부 정보 보기 35
작업 아카이브 36
작업 다시 대기열에 추가 36
작업 다시 제출 36
단계 보기 37

작업 보기 ... 37
세션 및 작업자 로그 보기 ... 38
작업자 대시보드 보기 ... 39
사용 사례 ... 40
완료된 출력 다운로드 ... 42
팜 ... 43
팜 생성 ... 43
대기열 ... 44
대기열 생성 ... 44
대기열 환경 생성 ... 46
기본 Conda 대기열 환경 ... 46
대기열과 플릿 연결 ... 48
플릿 ... 50
서비스 관리형 플릿 ... 50
SMF 생성 ... 50
GPU 액셀러레이터 사용 ... 52
소프트웨어 라이선스 ... 53
VFX 플랫폼 ... 53
고객 관리형 플릿 ... 54
사용자 관리 ... 56
모니터의 사용자 관리 ... 56
팜 사용자 관리 ... 58
작업 ... 61
제출자 사용 ... 62
공유 작업 설정 탭 ... 63
작업별 설정 탭 ... 65
작업 첨부 파일 탭 ... 66
호스트 요구 사항 탭 ... 68
처리 작업 ... 69
작업 모니터링 ... 69
스토리지 ... 73
작업 첨부 파일 ... 73
작업 연결 S3 버킷에 대한 암호화 ... 74
S3 버킷에서 작업 연결 관리 ... 75
가상 파일 시스템 ... 75
지출 및 사용량 추적 ... 79

비용 가정 ... 79
예산으로 비용 제어 ... 80
전제 조건 ... 81
Deadline Cloud 예산 관리자 열기 ... 81
예산 생성 ... 81
예산 보기 ... 82
예산 편집 ... 83
예산 비활성화 ... 83
EventBridge 이벤트를 사용하여 예산 모니터링 ... 83
사용량 및 비용 추적 ... 84
전제 조건 ... 85
사용량 탐색기 열기 ... 85
사용량 탐색기 사용 ... 84
비용 관리 ... 88
비용 관리 모범 사례 ... 89
보안 ... 92
데이터 보호 ... 93
저장 시 암호화 ... 94
전송 중 암호화 ... 94
키 관리 ... 94
인터네트워크 트래픽 개인 정보 보호 ... 104
옵트아웃 ... 104
ID 및 액세스 관리 ... 105
대상 ... 106
ID를 통한 인증 ... 106
정책을 사용하여 액세스 관리 ... 109
Deadline Cloud와 IAM의 작동 방식 ... 112
자격 증명 기반 정책 예제 ... 118
AWS 관리형 정책 ... 121
문제 해결 ... 125
규정 준수 확인 ... 127
복원성 ... 128
인프라 보안 ... 128
구성 및 취약성 분석 ... 129
교차 서비스 혼동된 대리인 방지 ... 129
AWS PrivateLink ... 131

고려 사항 ... 131
Deadline Cloud 엔드포인트 ... 131
엔드포인트 생성 ... 132
보안 모범 사례 ... 133
데이터 보호 ... 133
IAM 권한 ... 134
사용자 및 그룹으로 작업 실행 ... 134
네트워킹 ... 134
작업 데이터 ... 135
팜 구조 ... 135
작업 연결 대기열 ... 136
사용자 지정 소프트웨어 버킷 ... 138
작업자 호스트 ... 138
호스트 구성 스크립트 ... 140
워크스테이션 ... 140
다운로드한 소프트웨어 확인 ... 140
모니터링 ... 147
할당량 ... 149
AWS CloudFormation 리소스 ... 153
기한 클라우드 및 AWS CloudFormation 템플릿 ... 153
에 대해 자세히 알아보기 AWS CloudFormation ... 153
문제 해결 ... 154
사용자가 내 팜, 플릿 또는 대기열을 볼 수 없는 이유는 무엇입니까? ... 154
사용자 액세스 ... 154
작업자가 내 작업을 선택하지 않는 이유는 무엇입니까? ... 155
플릿 역할 구성 ... 155
작업자의 실행이 멈춘 이유는 무엇입니까? ... 155
작업자가 OpenJD 환경에서 나가지 못함 ... 155
작업 문제 해결 ... 156
작업 생성이 실패한 이유는 무엇입니까? ... 156
내 작업이 호환되지 않는 이유는 무엇입니까? ... 156
내 작업이 준비된 이유는 무엇입니까? ... 157
내 작업이 실패한 이유는 무엇입니까? ... 157
내 단계가 보류 중인 이유는 무엇입니까? ... 158
추가 리소스 ... 158
문서 기록 ... 159

AWS 용어집 163
..... clxiv

AWS Deadline Cloud란 무엇인가요?

Deadline Cloud는 디지털 콘텐츠 생성 파이프라인 및 워크스테이션에서 직접 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 렌더링 프로젝트 및 작업을 생성하고 관리하는 데 사용할 AWS 서비스 수 있는 입니다.

Deadline Cloud는 콘솔 인터페이스, 로컬 애플리케이션, 명령줄 도구 및 API를 제공합니다. Deadline Cloud를 사용하면 팜, 플릿, 작업, 사용자 그룹 및 스토리지를 생성, 관리 및 모니터링할 수 있습니다. 또한 하드웨어 기능을 지정하고, 특정 워크로드에 대한 환경을 생성하고, 프로덕션에 필요한 콘텐츠 생성 도구를 Deadline Cloud 파이프라인에 통합할 수 있습니다.

Deadline Cloud는 모든 렌더링 프로젝트를 한 곳에서 관리할 수 있는 통합 인터페이스를 제공합니다. 사용자를 관리하고, 사용자에게 프로젝트를 할당하고, 작업 역할에 대한 권한을 부여할 수 있습니다.

주제

- Deadline Cloud의 기능
- Deadline Cloud의 개념 및 용어
- Deadline Cloud 시작하기
- 기한 클라우드 액세스
- 관련 서비스
- Deadline Cloud 작동 방식

Deadline Cloud의 기능

다음은 Deadline Cloud가 시각적 컴퓨팅 워크로드를 실행하고 관리하는 데 도움이 되는 몇 가지 주요 방법입니다.

- 팜, 대기열 및 플릿을 빠르게 생성합니다. 상태를 모니터링하고 팜 및 작업 운영에 대한 인사이트를 얻습니다.
- Deadline Cloud 사용자 및 그룹을 중앙에서 관리하고 권한을 할당합니다.
- 를 사용하여 프로젝트 사용자 및 외부 자격 증명 공급자의 로그인 보안을 관리합니다 AWS IAM Identity Center.
- AWS Identity and Access Management (IAM) 정책 및 역할을 사용하여 프로젝트 리소스에 대한 액세스를 안전하게 관리합니다.
- 태그를 사용하여 프로젝트 리소스를 구성하고 빠르게 찾을 수 있습니다.

- 프로젝트의 프로젝트 리소스 사용량 및 예상 비용을 관리합니다.
- 클라우드 또는 직접 렌더링을 지원하는 다양한 컴퓨팅 관리 옵션을 제공합니다.

Deadline Cloud의 개념 및 용어

AWS Deadline Cloud를 시작하는 데 도움이 되도록이 주제에서는 몇 가지 주요 개념과 용어를 설명합니다.

예산 관리자

예산 관리자는 Deadline Cloud 모니터의 일부입니다. 예산 관리자를 사용하여 예산을 생성하고 관리합니다. 또한 이를 사용하여 예산 내에서 유지되도록 활동을 제한할 수 있습니다.

기한 클라우드 클라이언트 라이브러리

클라이언트 라이브러리에는 Deadline Cloud를 관리하기 위한 명령줄 인터페이스와 라이브러리가 포함되어 있습니다. 이 기능에는 Open Job Description 사양을 기반으로 Deadline Cloud에 작업 번들 제출, 작업 연결 출력 다운로드, 명령줄 인터페이스를 사용한 팜 모니터링이 포함됩니다.

디지털 콘텐츠 생성 애플리케이션(DCC)

디지털 콘텐츠 생성 애플리케이션(DCCs)은 디지털 콘텐츠를 생성하는 타사 제품입니다. DCCs가 있습니다Houdini. Maya Nuke Deadline Cloud는 특정 DCCs 제공합니다.

팜

팜은 프로젝트 리소스가 있는 입니다. 대기열과 플릿으로 구성됩니다.

플릿

플릿은 렌더링을 수행하는 작업자 노드 그룹입니다. 작업자 노드는 작업을 처리합니다. 플릿은 여러 대기열에 연결할 수 있으며 대기열은 여러 플릿에 연결할 수 있습니다.

작업

작업은 렌더링 요청입니다. 사용자는 작업을 제출합니다. 작업에는 단계 및 작업으로 요약된 특정 작업 속성이 포함됩니다.

작업 첨부 파일

작업 연결은 작업에 대한 입력 및 출력을 관리하는 데 사용할 수 있는 Deadline Cloud 기능입니다. 작업 파일은 렌더링 프로세스 중에 작업 첨부 파일로 업로드됩니다. 이러한 파일은 텍스처, 3D 모델, 조명 리그 및 기타 유사한 항목일 수 있습니다.

작업 우선 순위

작업 우선 순위는 Deadline Cloud가 대기열에서 작업을 처리하는 대략적인 순서입니다. 작업 우선 순위를 1~100으로 설정할 수 있으며, 일반적으로 우선 순위가 높은 작업이 먼저 처리됩니다. 우선 순위가 동일한 작업은 수신된 순서대로 처리됩니다.

작업 속성

작업 속성은 렌더링 작업을 제출할 때 정의하는 설정입니다. 프레임 범위, 출력 경로, 작업 연결, 렌더링 가능한 카메라 등을 예로 들 수 있습니다. 속성은 렌더링이 제출되는 DCC에 따라 달라집니다.

작업 템플릿

작업 템플릿은 런타임 환경과 Deadline Cloud 작업의 일부로 실행되는 모든 프로세스를 정의합니다.

대기열

대기열은 제출된 작업이 위치하고 렌더링되도록 예약된 곳입니다. 성공적인 렌더링을 생성하려면 대기열을 플릿과 연결해야 합니다. 대기열은 여러 플릿과 연결할 수 있습니다.

대기열-플릿 연결

대기열이 플릿과 연결된 경우 대기열-플릿 연결이 있습니다. 연결을 사용하여 플릿에서 해당 대기열의 작업으로 작업자를 예약합니다. 연결을 시작하고 중지하여 작업 일정을 제어할 수 있습니다.

세션

세션은 동일한 작업에서 작업 세트를 실행하기 위해 생성된 작업자 호스트의 임시 런타임 환경입니다. 작업자 호스트가 해당 작업에 대한 작업 실행을 완료하면 세션이 종료됩니다.

세션은 환경 변수를 정의하거나 백그라운드 프로세스 또는 컨테이너를 시작하는 등 여러 작업 실행에서 공유되는 리소스로 환경을 구성하는 방법을 제공합니다.

세션 작업

세션 작업은 세션 내에서 작업자가 실행하는 개별 작업 단위입니다. 작업의 핵심 작업 실행 작업을 포함하거나 환경 설정과 같은 준비 단계와 해체 및 정리와 같은 실행 후 프로세스를 포함할 수 있습니다.

단계

단계는 작업에서 실행할 특정 프로세스 중 하나입니다.

Deadline Cloud 제출자

Deadline Cloud 제출자는 디지털 콘텐츠 생성(DCC) 플러그인입니다. 아티스트는 이를 사용하여 익숙한 타사 DCC 인터페이스에서 작업을 제출합니다.

Tags

태그는 AWS 리소스에 할당할 수 있는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다.

태그를 사용하면 AWS 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어, 계정의 Amazon EC2 인스턴스에 대해 각 인스턴스의 소유자나 스택 수준을 추적하는 데 도움이 되는 태그 세트를 정의할 수 있습니다.

용도, 소유자 또는 환경별로 AWS 리소스를 분류할 수도 있습니다. 이 접근 방식은 동일한 유형의 리소스가 많을 때 유용합니다. 할당한 태그를 기반으로 특정 리소스를 빠르게 식별할 수 있습니다.

Task

작업은 렌더링 단계의 단일 구성 요소입니다.

사용량 기반 라이선스(UBL)

사용량 기반 라이선스(UBL)는 일부 타사 제품에 사용할 수 있는 온디맨드 라이선스 모델입니다. 이 모델은 사용한 만큼 지불되며 사용한 시간과 분에 대한 요금이 부과됩니다.

사용량 탐색기

Usage Explorer는 Deadline Cloud Monitor의 기능입니다. 대략적인 예상 비용 및 사용량을 제공합니다.

작업자

작업자는 플릿에 속하며 Deadline Cloud 할당 작업을 실행하여 단계와 작업을 완료합니다. 작업자는 작업 작업의 로그를 Amazon CloudWatch Logs에 저장합니다. 작업자는 작업 연결 기능을 사용하여 입력 및 출력을 Amazon Simple Storage Service(Amazon S3) 버킷에 동기화할 수도 있습니다.

Deadline Cloud 시작하기

Deadline Cloud를 사용하여 Amazon EC2 인스턴스 구성 및 Amazon Simple Storage Service(Amazon S3) 버킷과 같은 기본 설정 및 리소스를 사용하여 렌더 팜을 빠르게 생성할 수 있습니다.

렌더 팜을 생성할 때 설정과 리소스를 정의할 수도 있습니다. 이 방법은 기본 설정 및 리소스를 사용하는 것보다 시간이 더 걸리지만 더 많은 제어 기능을 제공합니다.

Deadline Cloud 개념 및 용어를 숙지한 후에는 팜 생성, 사용자 추가 및 유용한 정보에 대한 링크에 대한 step-by-step 지침은 시작하기를 참조하세요.

기한 클라우드 액세스

다음 방법 중 하나로 Deadline Cloud에 액세스할 수 있습니다.

- 기한 클라우드 콘솔 - 브라우저에서 콘솔에 액세스하여 팜과 리소스를 생성하고 사용자 액세스를 관리합니다. 자세한 내용은 시작하기를 참조하세요.
- Deadline Cloud Monitor - 우선순위 및 작업 상태 업데이트를 포함하여 렌더링 작업을 관리합니다. 팜을 모니터링하고 로그 및 작업 상태를 확인합니다. 소유자 권한이 있는 사용자의 경우 Deadline Cloud Monitor는 사용량을 탐색하고 예산을 생성할 수 있는 액세스 권한도 제공합니다. Deadline Cloud 모니터는 웹 브라우저와 데스크톱 애플리케이션으로 사용할 수 있습니다.
- AWS SDK 및 AWS CLI - AWS Command Line Interface (AWS CLI)를 사용하여 로컬 시스템의 명령줄에서 Deadline Cloud API 작업을 호출합니다. 자세한 내용은 개발자 워크스테이션 설정을 참조하세요.

관련 서비스

Deadline Cloud는 AWS 서비스다음과 함께 작동합니다.

- Amazon CloudWatch - CloudWatch를 사용하면 프로젝트 및 관련 AWS 리소스를 모니터링할 수 있습니다. 자세한 내용은 Deadline Cloud Developer Guide의 Monitoring with CloudWatch를 참조하세요.
- Amazon EC2 - 클라우드에서 애플리케이션을 실행하는 가상 서버를 AWS 서비스 제공합니다. 워크로드에 Amazon EC2 인스턴스를 사용하도록 프로젝트를 구성할 수 있습니다. 자세한 내용은 Amazon EC2 인스턴스를 참조하세요.
- Amazon EC2 Auto Scaling - Auto Scaling을 사용하면 인스턴스에 대한 수요가 변경되면 인스턴스 수를 자동으로 늘리거나 줄일 수 있습니다. Auto Scaling을 사용하면 인스턴스가 실패하더라도 원하는 수의 인스턴스를 실행할 수 있습니다. Deadline Cloud로 Auto Scaling을 활성화하면 Auto Scaling에서 시작한 인스턴스가 워크로드에 자동으로 등록됩니다. 마찬가지로 Auto Scaling에 의해 종료된 인스턴스는 워크로드에서 자동으로 등록 취소됩니다. 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서를 참조하세요.
- AWS PrivateLink- 트래픽을 퍼블릭 인터넷에 노출하지 않고 Virtual Private Cloud(VPCs) AWS 서비스와 온프레미스 네트워크 간에 프라이빗 연결을 AWS PrivateLink 제공합니다.를 AWS PrivateLink 사용하면 다양한 계정과 VPCs. 자세한 내용은 AWS PrivateLink 단원을 참조하십시오.
- Amazon S3 - Amazon S3는 객체 스토리지 서비스입니다. Deadline Cloud는 Amazon S3 버킷을 사용하여 작업 첨부 파일을 저장합니다. 자세한 내용은 Amazon S3 사용 설명서를 참조하세요.

- IAM Identity Center - IAM Identity Center는 사용자에게 할당된 모든 계정 및 애플리케이션에 대한 Single Sign-On 액세스를 한 곳에서 제공할 수 AWS 서비스 있는 입니다. 또한 AWS Organizations에서 모든 계정에 대한 다중 계정 액세스 및 사용자 권한을 중앙에서 관리할 수 있습니다. 자세한 내용은 AWS IAM Identity Center FAQ를 참조하세요.

Deadline Cloud 작동 방식

Deadline Cloud를 사용하면 디지털 콘텐츠 생성(DCC) 파이프라인 및 워크스테이션에서 직접 렌더링 프로젝트 및 작업을 생성하고 관리할 수 있습니다.

AWS SDK, AWS Command Line Interface (AWS CLI) 또는 Deadline Cloud 작업 제출자를 사용하여 Deadline Cloud에 작업을 제출합니다. Deadline Cloud는 작업 템플릿 사양에 대한 Open Job Description(OpenJD)을 지원합니다. 자세한 내용은 GitHub 웹 사이트의 Open Job Description을 참조하세요.

Deadline Cloud는 작업 제출자를 제공합니다. 작업 제출자는 Maya 또는와 같은 타사 DCC 인터페이스에서 렌더링 작업을 제출하기 위한 DCC 플러그인입니다Nuke. 제출자를 사용하면 아티스트는 프로젝트 리소스가 관리되고 작업이 모니터링되는 Deadline Cloud에 타사 인터페이스의 렌더링 작업을 한 곳에서 제출할 수 있습니다.

Deadline Cloud 팜을 사용하면 대기열과 플릿을 생성하고, 사용자를 관리하고, 프로젝트 리소스 사용량과 비용을 관리할 수 있습니다. 팜은 대기열과 플릿으로 구성됩니다. 대기열은 제출된 작업이 위치하고 렌더링되도록 예약된 곳입니다. 플릿은 작업을 실행하여 작업을 완료하는 작업자 노드 그룹입니다. 작업이 렌더링될 수 있도록 대기열을 플릿과 연결해야 합니다. 단일 플릿은 여러 대기열을 지원할 수 있으며 대기열은 여러 플릿에서 지원할 수 있습니다.

작업은 단계로 구성되며 각 단계는 특정 작업으로 구성됩니다. Deadline Cloud 모니터를 사용하면 작업, 단계 및 작업에 대한 상태, 로그 및 기타 문제 해결 지표에 액세스할 수 있습니다.

Deadline Cloud의 권한

Deadline Cloud는 다음을 지원합니다.

- AWS Identity and Access Management (IAM)을 사용하여 API 작업에 대한 액세스 관리
- 와의 통합을 사용하여 작업 인력 사용자의 액세스 관리 AWS IAM Identity Center

누구나 프로젝트에서 작업하려면 먼저 해당 프로젝트와 관련 팜에 액세스할 수 있어야 합니다. Deadline Cloud는 IAM Identity Center와 통합되어 인력 인증 및 권한 부여를 관리합니다. 사용자를

IAM Identity Center에 직접 추가하거나 Okta 또는와 같은 기존 ID 제공업체(IdP)에 권한을 연결할 수 있습니다Active Directory. IT 관리자는 다양한 수준의 사용자 및 그룹에 액세스 권한을 부여할 수 있습니다. 각 후속 수준에는 이전 수준에 대한 권한이 포함됩니다. 다음 목록은 가장 낮은 수준에서 가장 높은 수준까지 네 가지 액세스 수준을 설명합니다.

- 뷰어 - 액세스할 수 있는 팜, 대기열, 플릿 및 작업의 리소스를 볼 수 있는 권한입니다. 최종 사용자는 작업을 제출하거나 변경할 수 없습니다.
- 기고자 - 최종 사용자와 동일하지만 대기열 또는 팜에 작업을 제출할 수 있는 권한이 있습니다.
- 관리자 - 기고자와 동일하지만 액세스 권한이 있는 대기열에서 작업을 편집하고 액세스 권한이 있는 리소스에 대한 권한을 부여할 수 있는 권한이 있습니다.
- 소유자 - 관리자와 동일하지만 예산을 보고 생성하고 사용량을 확인할 수 있습니다.

> **Note**
>
> 이러한 권한은 사용자에게에 대한 액세스 권한을 부여 AWS Management Console 하거나 Deadline Cloud 인프라를 수정할 수 있는 권한을 부여하지 않습니다.

사용자는 연결된 대기열 및 플릿에 액세스하려면 먼저 팜에 액세스할 수 있어야 합니다. 사용자 액세스는 팜 내에서 대기열과 플릿에 별도로 할당됩니다.

사용자를 개인 또는 그룹의 일부로 추가할 수 있습니다. 팜, 플릿 또는 대기열에 그룹을 추가하면 대규모 그룹의 액세스 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 특정 프로젝트에서 작업하는 팀이 있는 경우 각 팀원을 그룹에 추가할 수 있습니다. 그런 다음 해당 팜, 플릿 또는 대기열에 대한 전체 그룹에 액세스 권한을 부여할 수 있습니다.

Deadline Cloud를 통한 소프트웨어 지원

Deadline Cloud는 명령줄 인터페이스에서 실행하고 파라미터 값을 사용하여 제어할 수 있는 모든 소프트웨어 애플리케이션에서 작동합니다. Deadline Cloud는 작업으로 파라미터화된 소프트웨어 스크립트 단계(예: 프레임 범위)를 사용하여 작업으로 설명하는 OpenJD 사양을 지원합니다. Deadline Cloud 도구 및 기능을 사용하여 OpenJD 작업 지침을 작업 번들에 통합하여 타사 소프트웨어 애플리케이션의 단계를 생성, 실행 및 라이선스를 부여합니다.

작업을 렌더링하려면 라이선스가 필요합니다. Deadline Cloud는 usage-based-licensing(UBL)를 제공하여 사용량에 따라 시간 단위로 요금이 청구되는 소프트웨어 애플리케이션 라이선스를 선택할 수 있습니다. Deadline Cloud를 사용하면 원하는 경우 자체 소프트웨어 라이선스를 사용할 수도 있습니다.

작업이 라이선스에 액세스할 수 없는 경우를 렌더링하지 않고 Deadline Cloud 모니터의 작업 로그에 표시되는 오류를 생성합니다.

Deadline Cloud 시작하기

AWS Deadline Cloud에서 팜을 생성하려면 Deadline Cloud 콘솔 또는 ()를 AWS Command Line Interface 사용할 수 있습니다AWS CLI. 콘솔을 사용하여 대기열 및 플릿을 포함하여 팜을 생성하는 방법을 안내합니다. AWS CLI 를 사용하여 서비스와 직접 작업하거나 Deadline Cloud와 함께 작동하는 자체 도구를 개발할 수 있습니다.

팜을 생성하고 Deadline Cloud 모니터를 사용하려면 Deadline Cloud에 대한 계정을 설정합니다. 계정당 한 번만 Deadline Cloud Monitor 인프라를 설정하면 됩니다. 팜에서 팜 및 해당 리소스에 대한 사용자 액세스를 포함하여 프로젝트를 관리할 수 있습니다.

Deadline Cloud 모니터 인프라를 설정하지 않고 팜을 생성하려면 Deadline Cloud용 개발자 워크스테이션을 설정합니다.

작업을 수락할 최소한의 리소스로 팜을 생성하려면 콘솔 홈 페이지에서 빠른 시작을 선택합니다.에서 해당 단계를 Deadline Cloud 모니터 설정 안내합니다. 이러한 팜은 대기열과 자동으로 연결된 플릿으로 시작합니다. 이 접근 방식은 실험할 샌드박스 스타일 팜을 생성하는 편리한 방법입니다.

주제

- 설정 AWS 계정
- Deadline Cloud 모니터 설정
- Deadline Cloud 제출자 설정

설정 AWS 계정

AWS Deadline Cloud AWS 계정 를 사용하도록를 설정합니다.

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

를 처음 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다.

> **Important**
>
> 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

Deadline Cloud 모니터 설정

시작하려면 Deadline Cloud 모니터 인프라를 생성하고 팜을 정의해야 합니다. 그룹 및 사용자 추가, 서비스 역할 선택, 리소스에 태그 추가 등 선택적 단계를 추가로 수행할 수도 있습니다.

1단계: 모니터 생성

Deadline Cloud 모니터는 AWS IAM Identity Center 를 사용하여 사용자에게 권한을 부여합니다. Deadline Cloud에 사용하는 IAM Identity Center 인스턴스는 모니터 AWS 리전 와 동일한에 있어야 합니다. 모니터를 생성할 때 콘솔에서 다른 리전을 사용하는 경우 IAM Identity Center 리전으로 변경하라는 알림을 받게 됩니다.

모니터의 인프라는 다음 구성 요소로 구성됩니다.

- 모니터 이름: 모니터 이름은 AnyCompany 모니터와 같이 모니터를 식별하는 방법입니다. 모니터 이름에 따라 모니터 URL도 결정됩니다.
- 모니터 URL: 모니터 URL을 사용하여 모니터에 액세스할 수 있습니다. URL은 모니터 이름을 기반으로 합니다. 예: https://anycompanymonitor.awsapps.com.
- AWS 리전: AWS 리전는 AWS 데이터 센터 모음의 물리적 위치입니다. 모니터를 설정할 때 리전은 기본적으로 가장 가까운 위치로 설정됩니다. 사용자와 가장 가까운 곳에 위치하도록 리전을 변경하

는 것이 좋습니다. 이렇게 하면 지연이 줄어들고 데이터 전송 속도가 향상됩니다. Deadline Cloud AWS 리전 와 동일한에서 활성화해야 AWS IAM Identity Center 합니다.

> **Important**
>
> Deadline Cloud 설정을 완료한 후에는 리전을 변경할 수 없습니다.

이 섹션의 작업을 완료하여 모니터의 인프라를 구성합니다.

모니터의 인프라를 구성하려면

1. 에 로그인하여 Welcome to Deadline Cloud 설정을 AWS Management Console 시작한 후 다음을 선택합니다.
2. 모니터 이름을 입력합니다. 예: **`AnyCompany Monitor`**.
3. (선택 사항) 모니터 URL을 변경하려면 URL 편집을 선택합니다.
4. (선택 사항) 사용자에게 가장 가깝AWS 리전도록를 변경하려면 리전 변경을 선택합니다.
   a. 사용자들과 가장 가까운 리전을 선택합니다.
   b. 리전 적용을 선택합니다.
5. (선택 사항) 모니터 설정을 추가로 사용자 지정하려면를 선택합니다추가 설정.
6. 를 사용할 준비가 되면 다음을 2단계: 팜 세부 정보 정의선택합니다.

추가 설정

Deadline Cloud 설정에는 추가 설정이 포함됩니다. 이러한 설정을 사용하면에 대한 Deadline Cloud 설정의 모든 변경 사항을 보고 AWS 계정, 모니터 사용자 역할을 구성하고, 암호화 키 유형을 변경할 수 있습니다.

AWS IAM Identity Center

AWS IAM Identity Center 는 사용자 및 그룹을 관리하기 위한 클라우드 기반 Single Sign-On 서비스입니다. IAM Identity Center를 엔터프라이즈 Single Sign-On(SSO) 공급자와 통합하면 사용자가 회사 계정으로 로그인할 수도 있습니다.

Deadline Cloud는 기본적으로 IAM Identity Center를 활성화하며 Deadline Cloud를 설정하고 사용해야 합니다. Deadline Cloud에 사용하는 IAM Identity Center 인스턴스는 모니터 AWS 리전 와 동일한에 있어야 합니다. 자세한 내용은 란 AWS IAM Identity Center 무엇입니까?를 참조하십시오.

서비스 액세스 역할 구성

AWS 서비스는 서비스 역할을 수임하여 사용자를 대신하여 작업을 수행할 수 있습니다. Deadline Cloud는 사용자에게 모니터의 리소스에 대한 액세스 권한을 부여하려면 모니터 사용자 역할이 필요합니다.

모니터 사용자 역할에 AWS Identity and Access Management (IAM) 관리형 정책을 연결할 수 있습니다. 정책은 사용자에게 특정 Deadline Cloud 애플리케이션에서 작업 생성과 같은 특정 작업을 수행할 수 있는 권한을 부여합니다. 애플리케이션은 관리형 정책의 특정 조건에 의존하므로 관리형 정책을 사용하지 않으면 애플리케이션이 예상대로 작동하지 않을 수 있습니다.

설정을 완료한 후 언제든지 모니터 사용자 역할을 변경할 수 있습니다. 사용자 역할에 대한 자세한 내용은 IAM 역할을 참조하세요.

다음 탭에는 두 가지 사용 사례에 대한 지침이 포함되어 있습니다. 새 서비스 역할을 생성하고 사용하려면 새 서비스 역할 탭을 선택합니다. 기존 서비스 역할을 사용하려면 기존 서비스 역할 탭을 선택합니다.

New service role

새 서비스 역할을 생성하고 사용하려면

1. 새 서비스 역할 생성 및 사용을 선택합니다.
2. (선택 사항) 서비스 사용자 역할 이름을 입력합니다.
3. 역할에 대한 자세한 내용을 보려면 권한 세부 정보 보기를 선택합니다.

Existing service role

기존 서비스 역할을 사용하려면

1. 기존 서비스 역할 사용을 선택합니다.
2. 드롭다운 목록을 열어 기존 서비스 역할을 선택합니다.
3. (선택 사항) 역할에 대한 자세한 내용을 보려면 IAM 콘솔에서 보기를 선택합니다.

2단계: 팜 세부 정보 정의

Deadline Cloud 콘솔로 돌아가서 다음 단계를 완료하여 팜 세부 정보를 정의합니다.

1. 팜 세부 정보에서 팜의 이름을 추가합니다.

2. 설명에 팜 설명을 입력합니다. 설명은 팜의 목적을 식별하는 데 도움이 될 수 있습니다.
3. 그룹을 생성하고 팜에 대한 사용을 추가합니다. 팜을 설정한 후 Deadline Cloud 관리 콘솔을 사용하여 그룹 및 사용자를 추가하거나 변경할 수 있습니다.
4. (선택 사항) 추가 팜 설정을 선택합니다.
   a. (선택 사항) 기본적으로 데이터는 보안을 위해가 AWS 소유하고 관리하는 키로 암호화됩니다. 암호화 설정 사용자 지정(고급)을 선택하여 기존 키를 사용하거나 관리하는 새 키를 생성할 수 있습니다.

      확인란을 사용하여 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS ARN을 입력하거나 새 KMS 키 생성을 AWS KMS 선택하여 새를 생성합니다.
   b. (선택 사항) 새 태그 추가를 선택하여 팜에 하나 이상의 태그를 추가합니다.
5. 다음 옵션 중 하나를 선택하세요.
   - 검토 및 생성으로 건너뛰기를 선택하여 팜을 검토하고 생성합니다.
   - 다음을 선택하여 추가 선택적 단계로 진행합니다.

(선택 사항) 3단계: 대기열 세부 정보 정의

대기열은 진행 상황을 추적하고 작업에 대한 작업을 예약할 책임이 있습니다.

1. 대기열 세부 정보부터 시작하여 대기열의 이름을 입력합니다.
2. 설명에 대기열 설명을 입력합니다. 명확한 설명은 대기열의 목적을 빠르게 식별하는 데 도움이 될 수 있습니다.
3. 작업 연결의 경우 새 Amazon S3 버킷을 생성하거나 기존 Amazon S3 버킷을 선택할 수 있습니다. 기존 Amazon S3 버킷이 없는 경우 버킷을 생성해야 합니다.
   a. 새 Amazon S3 버킷을 생성하려면 새 작업 버킷 생성을 선택합니다. 루트 접두사 필드에서 작업 버킷의 이름을 정의할 수 있습니다. 버킷을 호출하는 것이 좋습니다**deadlinecloud-job-attachments-[MONITORNAME]**.

      소문자와 대시만 사용할 수 있습니다. 공백이나 특수 문자는 사용할 수 없습니다.
   b. 기존 Amazon S3 버킷을 검색하고 선택하려면 기존 Amazon S3 버킷에서 선택을 선택합니다. 그런 다음 S3 찾아보기를 선택하여 기존 버킷을 검색합니다. 사용 가능한 Amazon S3 버킷 목록이 표시되면 대기열에 사용할 Amazon S3 버킷을 선택합니다.
4. (선택 사항) 추가 팜 설정을 선택합니다.

a. 고객 관리형 플릿을 사용하는 경우 고객 관리형 플릿과의 연결 활성화를 선택합니다.

   i. 고객 관리형 플릿의 경우 대기열 구성 사용자를 추가한 다음 POSIX 및/또는 Windows 자격 증명을 설정합니다. 또는 확인란을 선택하여 run-as 기능을 우회할 수 있습니다.

   ii. 대기열에 대한 예산을 설정하려면 이 대기열에 대한 예산 필요를 선택합니다. 예산이 필요한 경우 Deadline Cloud 콘솔을 사용하여 예산을 생성하여 대기열에서 작업을 예약해야 합니다.

b. 대기열에는 사용자를 대신하여 Amazon S3에 액세스할 수 있는 권한이 필요합니다. 모든 대기열에 대해 새 서비스 역할을 생성하는 것이 좋습니다.

   i. 새 역할의 경우 다음 단계를 완료합니다.

      A. 새 서비스 역할 생성 및 사용을 선택합니다.

      B. 대기열 역할의 역할 이름을 입력하거나 제공된 역할 이름을 사용합니다.

      C. (선택 사항) 대기열 역할 설명을 추가합니다.

      D. 권한 세부 정보 보기를 선택하여 대기열 역할에 대한 IAM 권한을 볼 수 있습니다.

   ii. 또는 기존 서비스 역할을 선택할 수 있습니다.

c. (선택 사항) 이름 및 값 페어를 사용하여 대기열 환경에 대한 환경 변수를 추가합니다.

d. (선택 사항) 키 및 값 페어를 사용하여 대기열의 태그를 추가합니다.

다음 옵션 중 하나를 선택하세요.

- 검토 및 생성으로 건너뛰기를 선택하여 팜을 검토하고 생성합니다.
- 다음을 선택하여 추가 선택적 단계로 진행합니다.

(선택 사항) 4단계: 플릿 세부 정보 정의

플릿은 렌더링 작업을 실행할 작업자를 할당합니다. 렌더링 작업에 플릿이 필요한 경우 플릿 생성 확인란을 선택합니다.

1. 플릿 세부 정보

   a. 플릿의 이름과 선택적 설명을 모두 입력합니다.

   b. 플릿 유형 및 운영 체제를 검토하여 인지합니다.

2. 인스턴스 시장 유형 섹션에서 스팟 인스턴스 또는 온디맨드 인스턴스를 선택합니다. Amazon EC2 온디맨드 인스턴스는 더 빠른 가용성을 제공하고 Amazon EC2 스팟 인스턴스는 비용 절감 노력에 더 적합합니다.
3. 플릿의 인스턴스 수 자동 조정에서 최소 인스턴스 수와 최대 인스턴스 수를 모두 선택합니다.

   추가 비용이 발생하지 않도록 항상 최소 인스턴스 수**0**를 로 설정하는 것이 좋습니다.
4. 작업자 기능을 검토하여 인식합니다.
5. (선택 사항) 추가 플릿 설정 선택
   a. 플릿에는 사용자를 대신하여 CloudWatch에 쓸 수 있는 권한이 필요합니다. 모든 플릿에 대해 새 서비스 역할을 생성하는 것이 좋습니다.
      i. 새 역할의 경우 다음 단계를 완료합니다.
         A. 새 서비스 역할 생성 및 사용을 선택합니다.
         B. 플릿 역할의 역할 이름을 입력하거나 제공된 역할 이름을 사용합니다.
         C. (선택 사항) 플릿 역할 설명을 추가합니다.
         D. 플릿 역할에 대한 IAM 권한을 보려면 권한 세부 정보 보기를 선택합니다.
      ii. 또는 기존 서비스 역할을 사용할 수 있습니다.
   b. (선택 사항) 키 및 값 페어를 사용하여 플릿의 태그를 추가합니다.

모든 플릿 세부 정보를 입력한 후 다음을 선택합니다.

5단계: 검토 및 생성

입력한 정보를 검토하여 팜을 생성합니다. 준비가 되면 팜 생성을 선택합니다.

팜 생성 진행 상황이 팜 페이지에 표시됩니다. 팜을 사용할 준비가 되면 성공 메시지가 표시됩니다.

Deadline Cloud 제출자 설정

이 프로세스는 AWS Deadline Cloud 제출자를 설치, 설정 및 시작하려는 관리자와 아티스트를 위한 것입니다. Deadline Cloud 제출자는 디지털 콘텐츠 생성(DCC) 플러그인입니다. 아티스트는 이를 사용하여 익숙한 타사 DCC 인터페이스에서 작업을 제출합니다.

> **Note**
> 아티스트가 렌더를 제출하는 데 사용할 모든 워크스테이션에서이 프로세스를 완료해야 합니다.

각 워크스테이션에는 해당 제출자를 설치하기 전에 DCC가 설치되어 있어야 합니다. 예를 들어에 대한 Deadline Cloud 제출자를 다운로드하려면 워크스테이션에가 Blender 이미 설치되어 Blender있어야 합니다.

워크스테이션을 안전하게 유지하기 위한 합리적인 기본값을 제공합니다. 워크스테이션 보안에 대한 자세한 내용은 보안 모범 사례 - 워크스테이션을 참조하세요.

주제

- 1단계: Deadline Cloud 제출자 설치
- 2단계: Deadline Cloud Monitor 설치 및 설정
- 3단계: Deadline Cloud 제출자 시작
- 지원되는 제출자

1단계: Deadline Cloud 제출자 설치

다음 섹션에서는 Deadline Cloud 제출자를 설치하는 단계를 안내합니다.

제출자 설치 프로그램 다운로드

Deadline Cloud 제출자를 설치하려면 먼저 제출자 설치 관리자를 다운로드해야 합니다.

1. 에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 측면 탐색 창에서 다운로드를 선택합니다.
3. 기한 클라우드 제출자 설치 관리자 섹션에서 컴퓨터 운영 체제의 설치 관리자를 선택한 다음 다운로드를 선택합니다.
4. (선택 사항) 다운로드한 소프트웨어의 신뢰성 확인.

Deadline Cloud 제출자 설치

설치 관리자를 사용하여 다음 제출자를 설치할 수 있습니다.

소프트웨어	지원되는 버전	Windows 설치 관리자	Linux 설치 관리자	MacOS 설치 관리자
Adobe After Effects	2024~2025	포함	포함되지 않음	포함
Autodesk Arnold for Maya	7.1 - 7.2	포함	포함	포함
Autodesk Maya	2023~2025	포함	포함	포함
블렌더	3.6 - 4.2	포함	포함	포함
Foundry Nuke	15~16	포함	포함	포함되지 않음
KeyShot Studio	2023~2024	포함	포함되지 않음	포함
Maxon 시네마 4D	2024~2025	포함	포함되지 않음	포함
SideFX Houdini	19.5~20.5	포함	포함	포함

여기에 나열되지 않은 다른 제출자를 설치할 수 있습니다. Deadline Cloud 라이브러리를 사용하여 제출자를 빌드합니다. 일부 제출자에는 Unreal Engine, 3ds Max 및 Rhino가 포함됩니다. aws-deadline GitHub 조직에서 이러한 라이브러리 및 제출자의 소스 코드를 찾을 수 있습니다.

Windows

1. 파일 브라우저에서 설치 관리자가 다운로드한 폴더로 이동한 다음를 선택합니다`DeadlineCloudSubmitter-windows-x64-installer.exe`.
   a. Windows에서 PC를 보호한 팝업이 표시되면 추가 정보를 선택합니다.
   b. 그래도 실행을 선택합니다.
2. AWS Deadline Cloud Submitter Setup Wizard가 열리면 다음을 선택합니다.
3. 다음 단계 중 하나를 완료하여 설치 범위를 선택합니다.
   - 현재 사용자에 대해서만를 설치하려면 사용자를 선택합니다.
   - 모든 사용자에 대해를 설치하려면 시스템을 선택합니다.

시스템을 선택하는 경우 설치 관리자를 종료하고 다음 단계를 완료하여 관리자로 다시 실행해야 합니다.

a. 를 마우스 오른쪽 버튼으로 클릭한 **DeadlineCloudSubmitter-windows-x64-installer.exe**다음 관리자로 실행을 선택합니다.

b. 관리자 자격 증명을 입력한 다음 예를 선택합니다.

c. 설치 범위로 시스템을 선택합니다.

4. 설치 범위를 선택한 후 다음을 선택합니다.
5. 다음을 다시 선택하여 설치 디렉터리를 수락합니다.
6. 에 대한 통합 제출자 Nuke또는 설치하려는 제출자를 선택합니다.
7. 다음을 선택합니다.
8. 설치를 검토하고 다음을 선택합니다.
9. 다음을 다시 선택한 후 완료를 선택합니다.

Linux

> **Note**
>
> 및 Deadline Cloud 모니터용 Linux Deadline Cloud 통합 Nuke 설치 관리자는 GLIBC 2.31 이상이 설치된 Linux 배포에만 설치할 수 있습니다.

1. 터미널 창을 엽니다.
2. 설치 프로그램의 시스템 설치를 수행하려면 명령을 **sudo -i** 입력하고 Enter 키를 눌러 루트가 됩니다.
3. 설치 프로그램을 다운로드한 위치로 이동합니다.

   예를 들어 **cd /home/*USER*/Downloads**입니다.
4. 설치 관리자를 실행 가능하게 만들려면를 입력합니다**chmod +x DeadlineCloudSubmitter-linux-x64-installer.run**.
5. Deadline Cloud 제출자 설치 프로그램을 실행하려면를 입력합니다**./DeadlineCloudSubmitter-linux-x64-installer.run**.
6. 설치 프로그램이 열리면 화면의 프롬프트에 따라 Setup Wizard를 완료합니다.

MacOS

1. 파일 브라우저에서 설치 관리자가 다운로드한 폴더로 이동한 다음 파일을 선택합니다.
2. AWS Deadline Cloud Submitter Setup Wizard가 열리면 다음을 선택합니다.
3. 다음을 다시 선택하여 설치 디렉터리를 수락합니다.
4. 의 통합 제출자 Maya또는 설치하려는 제출자를 선택합니다.
5. 다음을 선택합니다.
6. 설치를 검토하고 다음을 선택합니다.
7. 다음을 다시 선택한 후 완료를 선택합니다.

2단계: Deadline Cloud Monitor 설치 및 설정

Windows, Linux또는를 사용하여 Deadline Cloud Monitor 데스크톱 애플리케이션을 설치할 수 있습니다macOS.

Windows

1. 아직 로그인하지 않았다면에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 다운로드를 선택합니다.
3. Deadline Cloud monitor 섹션에서 최신 Windows 파일을 선택하고 다운로드를 선택합니다.

자동 설치를 수행하려면 다음 명령을 사용합니다.

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

기본적으로 모니터는에 설치됩니다`C:\Users{username}\AppData\Local\DeadlineCloudMonitor`. 설치 디렉터리를 변경하려면 대신 다음 명령을 사용합니다.

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

Linux (AppImage)

Deadline Cloud Monitor AppImage on Debian 배포판을 설치하려면

1. 최신 Deadline Cloud Monitor AppImage를 다운로드합니다.

2.

> **Note**
> 이 단계는 Ubuntu 22 이상을 위한 것입니다. Ubuntu의 다른 버전의 경우이 단계를 건너뜁니다.

libfuse2를 설치하려면 다음을 입력합니다.

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

3. AppImage 실행 파일을 만들려면 다음을 입력합니다.

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

Linux (Debian)

Debian 배포판에 Deadline Cloud Monitor Debian 패키지를 설치하려면

1. 최신 Deadline Cloud Monitor Debian 패키지를 다운로드합니다.
2.

> **Note**
> 이 단계는 Ubuntu 22 이상을 위한 것입니다. Ubuntu의 다른 버전의 경우이 단계를 건너뜁니다.

libssl1.1을 설치하려면 다음을 입력합니다.

```
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. Deadline Cloud Monitor Debian 패키지를 설치하려면 다음을 입력합니다.

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

4. 종속성이 충족되지 않은 패키지에 대한 설치가 실패하면 손상된 패키지를 수정한 다음 다음 명령을 실행합니다.

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

Linux (RPM)

Rocky Linux 9 또는에 Deadline Cloud Monitor RPM을 설치하려면 Alma Linux 9

1. 최신 Deadline Cloud Monitor RPM을 다운로드합니다.
2. Enterprise Linux 9 리포지토리에 대한 추가 패키지를 추가합니다.

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

3. libssl.so.1.1 종속성을 위해 compat-openssl11을 설치합니다.

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

에 Deadline Cloud Monitor RPM을 설치하려면 Red Hat Linux 9

1. 최신 Deadline Cloud Monitor RPM을 다운로드합니다.
2. CodeReady Linux Builder 리포지토리를 활성화합니다.

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

3. 에 대한 추가 패키지를 설치합니다Enterprise RPM.

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

4. libssl.so.1.1 종속성을 위해 compat-openssl11을 설치합니다.

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

Rocky Linux 8, Alma Linux 8또는에 Deadline Cloud Monitor RPM을 설치하려면 Red Hat Linux 8

1. 최신 Deadline Cloud Monitor RPM을 다운로드합니다.
2. Deadline Cloud 모니터를 설치합니다.

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

macOS

1. 아직 로그인하지 않았다면에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 다운로드를 선택합니다.
3. Deadline Cloud monitor 섹션에서 최신 macOS 파일을 선택하고 다운로드를 선택합니다.
4. 다운로드한 파일을 엽니다. 창이 표시되면 Deadline Cloud monitor 아이콘을 선택하고 Applications 폴더로 드래그합니다.

다운로드를 완료한 후 다운로드한 소프트웨어의 신뢰성을 확인할 수 있습니다. 다운로드 프로세스 도중 또는 이후에 아무도 파일을 변조하지 않도록 하려면 이렇게 해야 할 수 있습니다. 1단계에서 다운로드한 소프트웨어의 신뢰성 확인을 참조하세요.

Deadline Cloud 모니터를 다운로드하고 신뢰성을 확인한 후 다음 절차에 따라 Deadline Cloud 모니터를 설정합니다.

Deadline Cloud Monitor를 설정하려면

1. Deadline Cloud Monitor를 엽니다.
2. 새 프로필을 생성하라는 메시지가 표시되면 다음 단계를 완료합니다.
   a. 다음과 같이 URL 입력에 모니터 URL을 입력합니다. **`https://MY-MONITOR.deadlinecloud.amazonaws.com/`**
   b. 프로필 이름을 입력합니다.
   c. 프로필 생성을 선택합니다.

      이제 프로필이 생성되고 생성한 프로필 이름을 사용하는 모든 소프트웨어와 자격 증명이 공유됩니다.

3. Deadline Cloud 모니터 프로파일을 생성한 후에는 프로파일 이름 또는 스튜디오 URL을 변경할 수 없습니다. 변경해야 하는 경우 대신 다음을 수행합니다.

   a. 프로필을 삭제합니다. 왼쪽 탐색 창에서 Deadline Cloud Monitor > 설정 > 삭제를 선택합니다.

   b. 원하는 변경 사항이 포함된 새 프로필을 생성합니다.

4. 왼쪽 탐색 창에서 >Deadline Cloud monitor 옵션을 사용하여 다음을 수행합니다.

   - Deadline Cloud 모니터 프로파일을 변경하여 다른 모니터에 로그인합니다.
   - Deadline Cloud Monitor의 후속 열기에서 모니터 URL을 입력할 필요가 없도록 자동 로그인을 활성화합니다.

5. Deadline Cloud Monitor 창을 닫습니다. 백그라운드에서 계속 실행되며 15분마다 자격 증명을 동기화합니다.

6. 렌더링 프로젝트에 사용할 각 디지털 콘텐츠 생성(DCC) 애플리케이션에 대해 다음 단계를 완료합니다.

   a. Deadline Cloud 제출자에서 Deadline Cloud 워크스테이션 구성을 엽니다.

   b. 워크스테이션 구성에서 Deadline Cloud 모니터에서 생성한 프로파일을 선택합니다. 이제 Deadline Cloud 자격 증명이이 DCC와 공유되며 도구가 예상대로 작동해야 합니다.

3단계: Deadline Cloud 제출자 시작

다음 예제에서는 Blender 제출자를 설치하는 방법을 보여줍니다. 의 지침에 따라 다른 제출자를 설치할 수 있습니다지원되는 제출자.

에서 Deadline Cloud 제출자를 시작하려면 Blender

> **Note**
>
> 에 대한 지원Blender은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Blender를 엽니다.

2. 편집을 선택한 다음 기본 설정을 선택합니다. 파일 경로에서 스크립트 디렉터리를 선택한 다음 추가를 선택합니다. Blender 제출자가 설치된 python 폴더의 스크립트 디렉터리를 추가합니다.

```
Windows:
```

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

3. Blender을 다시 시작합니다.
4. 편집을 선택한 다음 기본 설정을 선택합니다. 그런 다음 추가 기능을 선택한 다음의 Deadline Cloud를 Blender검색합니다. 확인란을 선택하여 추가 기능을 활성화합니다.
5. 자산 루트 디렉터리 내에 종속성이 있는 Blender 장면을 엽니다.
6. 렌더링 메뉴에서 Deadline Cloud 대화 상자를 선택합니다.
   a. Deadline Cloud 제출자에서 아직 인증되지 않은 경우 자격 증명 상태가 NEEDS_LOGIN으로 표시됩니다.
   b. 로그인을 선택합니다.
   c. 로그인 브라우저 창이 표시됩니다. 사용자 자격 증명으로 로그인합니다.
   d. 허용을 선택합니다. 이제 로그인되고 자격 증명 상태가 AUTHENTICATED로 표시됩니다.
7. 제출을 선택합니다.

지원되는 제출자

다음 섹션에서는 사용 가능한 Deadline Cloud 제출자 플러그인을 시작하는 단계를 안내합니다.

여기에 나열되지 않은 다른 제출자를 설치할 수 있습니다. Deadline Cloud 라이브러리를 사용하여 제출자를 빌드합니다. 일부 제출자에는 Unreal Engine, 3ds Max 및가 포함됩니다Rhino. aws-deadline GitHub 조직에서 이러한 라이브러리 및 제출자의 소스 코드를 찾을 수 있습니다.

소프트웨어	지원되는 버전	Windows 설치 관리자	Linux 설치 관리자	MacOS 설치 관리자
Adobe After Effects	2024~2025	포함	포함되지 않음	포함
Autodesk Arnold for Maya	7.1 - 7.2	포함	포함	포함
Autodesk Maya	2023~2025	포함	포함	포함

소프트웨어	지원되는 버전	Windows 설치 관리자	Linux 설치 관리자	MacOS 설치 관리자
블렌더	3.6 - 4.2	포함	포함	포함
Foundry Nuke	15~16	포함	포함	포함되지 않음
KeyShot Studio	2023~2024	포함	포함되지 않음	포함
Maxon 시네마 4D	2024~2025	포함	포함되지 않음	포함
SideFX Houdini	19.5~20.5	포함	포함	포함

After Effects

에서 Deadline Cloud 제출자를 시작하려면 After Effects

1. After Effects를 엽니다.
2. 편집, 기본 설정, 스크립팅 및 표현식을 차례로 선택합니다.
3. 스크립트가 파일을 쓰고 네트워크에 액세스하도록 허용을 선택합니다.
4. 효과 후 다시 시작
5. 창을 선택한 다음 DeadlineCloudSubmitter.jsx를 선택합니다.

After Effects 제출자를 사용하려면

1. 제출자 패널에서 렌더링 대기열 열기를 선택합니다.
2. 렌더링 대기열에 구성을 추가하고 렌더링 설정, 출력 모듈 및 출력 경로를 설정합니다.
3. 제출자 패널에서 새로 고침을 선택합니다.
4. 목록에서 구성을 선택한 다음 제출을 선택합니다. 렌더링 대기열에서 구성을 추가하거나 제거할 때 새로 고침을 다시 선택할 수 있습니다.

제출자의 오른쪽 상단 모서리를 선택하고의 강조 표시된 섹션에 놓아 제출자를 사이드 패널에 도킹할 수 있습니다After Effects.

Blender

에서 Deadline Cloud 제출자를 시작하려면 Blender

> **Note**
>
> 에 대한 지원Blender은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Blender를 엽니다.
2. 편집을 선택한 다음 기본 설정을 선택합니다. 파일 경로에서 스크립트 디렉터리를 선택한 다음 추가를 선택합니다. Blender 제출자가 설치된 python 폴더의 스크립트 디렉터리를 추가합니다.

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

3. Blender을 다시 시작합니다.
4. 편집을 선택한 다음 기본 설정을 선택합니다. 그런 다음 추가 기능을 선택한 다음 Deadline Cloud for Blender를 검색합니다. 확인란을 선택하여 추가 기능을 활성화합니다.
5. 자산 루트 디렉터리 내에 종속성이 있는 Blender 장면을 엽니다.
6. 렌더링 메뉴에서 Deadline Cloud 대화 상자를 선택합니다.
   a. Deadline Cloud 제출자에서 아직 인증되지 않은 경우 자격 증명 상태가 NEEDS_LOGIN으로 표시됩니다.
   b. 로그인을 선택합니다.
   c. 로그인 브라우저 창이 표시됩니다. 사용자 자격 증명으로 로그인합니다.
   d. 허용을 선택합니다. 이제 로그인되고 자격 증명 상태가 AUTHENTICATED로 표시됩니다.
7. 제출을 선택합니다.

Cinema 4D

에서 Deadline Cloud 제출자를 시작하려면 Cinema 4D

> **Note**
> 에 대한 지원Cinema 4D은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Cinema 4D를 엽니다.
2. AWS Deadline Cloud용 GUI 구성 요소를 설치하라는 메시지가 표시되면 다음 단계를 완료합니다.
   a. 프롬프트가 표시되면 예를 선택하고 종속성이 설치될 때까지 기다립니다.
   b. 변경 사항이 적용Cinema 4D되도록 다시 시작합니다.
3. 확장 > AWS Deadline Cloud Submitter를 선택합니다.

Houdini

에서 Deadline Cloud 제출자를 시작하려면 Houdini

> **Note**
> 에 대한 지원Houdini은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Houdini를 엽니다.
2. 네트워크 편집기에서 /out 네트워크를 선택합니다.
3. 탭을 누르고를 입력합니다**`deadline`**.
4. Deadline Cloud 옵션을 선택하고 기존 네트워크에 연결합니다.
5. Deadline Cloud 노드를 두 번 클릭합니다.

KeyShot

에서 Deadline Cloud 제출자를 시작하려면 KeyShot

1. KeyShot를 엽니다.
2. Windows > 스크립팅 콘솔 > AWS 기한 클라우드에 제출 및 실행을 선택합니다.

KeyShot 제출자에는 두 가지 제출 모드가 있습니다. 제출 모드를 선택하여 제출자를 엽니다.

- 장면 BIP 파일 및 모든 외부 파일 참조 연결 - 열려 있는 장면 파일과 BIP에서 참조되는 모든 외부 파일이 작업 첨부 파일로 포함됩니다.
- 장면 BIP 파일만 첨부 - 열린 장면 파일만 제출에 첨부됩니다. 장면에서 참조되는 모든 외부 파일은 네트워크 스토리지 또는 다른 방법을 통해 작업자가 사용할 수 있어야 합니다.

Maya and Arnold for Maya

에서 Deadline Cloud 제출자를 시작하려면 Maya

> **Note**
>
> Maya 및에 대한 지원Arnold for Maya (MtoA)은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Maya를 엽니다.
2. 프로젝트를 설정하고 자산 루트 디렉터리 내에 있는 파일을 엽니다.
3. Windows → 설정/기본 설정 → 플러그인 관리자를 선택합니다.
4. DeadlineCloudSubmitter를 검색합니다.
5. Deadline Cloud 제출자 플러그인을 로드하려면 로드를 선택합니다.
   a. Deadline Cloud 제출자에서 아직 인증되지 않은 경우 자격 증명 상태가 NEEDS_LOGIN으로 표시됩니다.
   b. 로그인을 선택합니다.
   c. 로그인 브라우저 창이 표시됩니다. 사용자 자격 증명으로 로그인합니다.
   d. 허용을 선택합니다. 이제 로그인되고 자격 증명 상태가 AUTHENTICATED로 표시됩니다.

6. (선택 사항)를 열 때마다 Deadline Cloud 제출자 플러그인을 로드하려면 자동 로드를 Maya선택합니다.
7. Deadline Cloud shelf를 선택한 다음 녹색 버튼을 선택하여 제출자를 시작합니다.

Nuke

에서 Deadline Cloud 제출자를 시작하려면 Nuke

> **Note**
>
> 에 대한 지원Nuke은 서비스 관리형 플릿의 Conda 환경을 사용하여 제공됩니다. 자세한 내용은 기본 Conda 대기열 환경 단원을 참조하십시오.

1. Nuke를 엽니다.
2. 자산 루트 디렉터리 내에 종속성이 있는 Nuke 스크립트를 엽니다.
3. AWS Deadline를 선택한 다음 Deadline Cloud에 제출을 선택하여 제출자를 시작합니다.
   a. Deadline Cloud 제출자에서 아직 인증되지 않은 경우 자격 증명 상태는 NEEDS_LOGIN으로 표시됩니다.
   b. 로그인을 선택합니다.
   c. 로그인 브라우저 창에서 사용자 자격 증명으로 로그인합니다.
   d. 허용을 선택합니다. 이제 로그인되고 자격 증명 상태가 AUTHENTICATED로 표시됩니다.
4. 제출을 선택합니다.

Deadline Cloud 모니터 사용

AWS Deadline Cloud 모니터는 시각적 컴퓨팅 작업에 대한 전체 보기를 제공합니다. 이를 사용하여 작업을 모니터링 및 관리하고, 플릿에 대한 작업자 활동을 보고, 예산 및 사용량을 추적하고, 작업 결과를 다운로드할 수 있습니다.

각 대기열에는 작업, 단계 및 작업의 상태를 보여주는 작업 모니터가 있습니다. 모니터는 모니터에서 직접 작업을 관리하는 방법을 제공합니다. 우선 순위를 변경하고, 작업을 취소하고, 작업을 다시 대기열에 추가하고, 작업을 다시 제출할 수 있습니다.

Deadline Cloud 모니터에는 작업의 요약 상태를 보여주는 테이블이 있습니다. 또는 작업을 선택하여 작업 관련 문제를 해결하는 데 도움이 되는 세부 작업 로그를 볼 수 있습니다.

Deadline Cloud 모니터를 사용하여 작업이 생성될 때 지정된 워크스테이션의 위치로 결과를 다운로드할 수 있습니다.

또한 Deadline Cloud 모니터는 사용량을 모니터링하고 비용을 관리하는 데 도움이 됩니다. 자세한 내용은 Deadline Cloud 팜의 지출 및 사용량 추적 단원을 참조하십시오.

주제

- Deadline Cloud Monitor URL 공유
- Deadline Cloud 모니터 열기
- Deadline Cloud에서 대기열 및 플릿 세부 정보 보기
- Deadline Cloud에서 작업, 단계 및 작업 관리
- Deadline Cloud에서 작업 세부 정보 보기 및 관리
- Deadline Cloud에서 단계 보기
- Deadline Cloud에서 작업 보기
- Deadline Cloud에서 세션 및 작업자 로그 보기
- 작업자 대시보드에서 작업자 세부 정보 보기
- Deadline Cloud에서 완료된 출력 다운로드

Deadline Cloud Monitor URL 공유

Deadline Cloud 서비스를 설정할 때 기본적으로 계정의 Deadline Cloud 모니터를 여는 URL을 생성합니다. 이 URL을 사용하여 브라우저 또는 데스크톱에서 모니터를 엽니다. Deadline Cloud 모니터에 액세스할 수 있도록 URL을 다른 사용자와 공유합니다.

사용자가 Deadline Cloud 모니터를 열려면 먼저 사용자에게 액세스 권한을 부여해야 합니다. 액세스 권한을 부여하려면 모니터의 승인된 사용자 목록에 사용자를 추가하거나 모니터에 액세스할 수 있는 그룹에 사용자를 추가합니다. 자세한 내용은 Deadline Cloud에서 사용자 관리 단원을 참조하십시오.

모니터 URL을 공유하려면

1. Deadline Cloud 콘솔을 엽니다.
2. 시작하기에서 Deadline Cloud 대시보드로 이동을 선택합니다.
3. 탐색 창에서 대시보드를 선택합니다.
4. 계정 개요 섹션에서 계정 세부 정보를 선택합니다.
5. Deadline Cloud 모니터에 액세스해야 하는 모든 사용자에게 URL을 복사한 다음 안전하게 전송합니다.

Deadline Cloud 모니터 열기

다음 방법 중 하나를 사용하여 Deadline Cloud 모니터를 열 수 있습니다.

- 콘솔 -에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
- 웹 - Deadline Cloud를 설정할 때 생성한 모니터 URL로 이동합니다.
- 모니터 - 데스크톱 Deadline Cloud 모니터를 사용합니다.

콘솔을 사용하는 경우 자격 증명을 AWS 사용하여 AWS Identity and Access Management 에 로그인한 다음 자격 AWS IAM Identity Center 증명으로 모니터에 로그인할 수 있어야 합니다. IAM Identity Center 자격 증명만 있는 경우 모니터 URL 또는 데스크톱 애플리케이션을 사용하여 로그인해야 합니다.

Deadline Cloud Monitor를 열려면(웹)

1. 브라우저를 사용하여 Deadline Cloud를 설정할 때 생성한 모니터 URL을 엽니다.
2. 사용자 자격 증명으로 로그인합니다.

Deadline Cloud 모니터를 열려면(콘솔)

1. Deadline Cloud 콘솔을 엽니다.
2. 탐색 창에서 팜을 선택합니다.
3. 팜을 선택한 다음 작업 관리를 선택하여 Deadline Cloud Monitor 페이지를 엽니다.

4. 사용자 자격 증명으로 로그인합니다.

Deadline Cloud 모니터(데스크톱)를 열려면

1. Deadline Cloud 콘솔을 엽니다.

   -또는-

   모니터 URL에서 Deadline Cloud monitor - 웹을 엽니다.
2. • Deadline Cloud 콘솔에서 다음을 수행합니다.
     1. 모니터에서 Deadline Cloud 대시보드로 이동을 선택한 다음 왼쪽 메뉴에서 다운로드를 선택합니다.
     2. Deadline Cloud Monitor에서 데스크톱의 모니터 버전을 선택합니다.
     3. 다운로드를 선택합니다.
   • Deadline Cloud Monitor - 웹에서 다음을 수행합니다.
     • 왼쪽 메뉴에서 워크스테이션 설정을 선택합니다. 워크스테이션 설정 항목이 표시되지 않으면 화살표를 사용하여 왼쪽 메뉴를 엽니다.
     • 다운로드를 선택합니다.
     • OS 선택에서 운영 체제를 선택합니다.
3. Deadline Cloud Monitor - 데스크톱을 다운로드합니다.
4. 모니터를 다운로드하여 설치한 후 컴퓨터에서 엽니다.

   • Deadline Cloud 모니터를 처음 여는 경우 모니터 URL을 제공하고 프로필 이름을 생성해야 합니다. 그런 다음 Deadline Cloud 자격 증명을 사용하여 모니터에 로그인합니다.
   • 프로필을 생성한 후 프로필을 선택하여 모니터를 엽니다. Deadline Cloud 자격 증명을 입력해야 할 수 있습니다.

언어 설정 변경

Deadline Cloud 모니터를 생성하고 연 후 언어 설정을 변경할 수 있습니다. 기본적으로 모니터 언어는 시스템의 언어 설정으로 설정됩니다.

Deadline Cloud Monitor(데스크톱)에서 언어 설정을 변경하려면

1. 사용자 프로필에서 설정을 선택한 다음 언어를 선택합니다.
2. 드롭다운 메뉴에서 사용 가능한 언어 중 하나를 선택합니다.

3. 선택한 언어가 나열된 옵션인지 확인한 다음 확인 및 적용을 선택하여 변경 사항을 적용합니다.

   모니터가 새로 고쳐지면 선택한 언어로 표시됩니다.

   언어 설정을 변경한 후에는 열 때 기본값이며 다시 변경하거나 데스크톱 애플리케이션을 제거할 때까지 기본값으로 유지됩니다.

웹에서 Deadline Cloud Monitor 언어를 변경하려면 브라우저 설정에서 원하는 언어를 변경합니다.

> **Note**
>
> 브라우저 또는 운영 체제가 Deadline Cloud에서 지원하지 않는 언어로 설정된 경우 영어가 Deadline Cloud 모니터의 기본 언어가 됩니다.

Deadline Cloud에서 대기열 및 플릿 세부 정보 보기

Deadline Cloud 모니터를 사용하여 팜의 대기열 및 플릿 구성을 볼 수 있습니다. 또한 모니터를 사용하여 대기열의 작업 또는 플릿의 작업자 목록을 볼 수 있습니다.

대기열 및 플릿 세부 정보를 볼 수 있는 `VIEWING` 권한이 있어야 합니다. 세부 정보가 표시되지 않으면 관리자에게 문의하여 올바른 권한을 얻으십시오.

대기열 세부 정보를 보려면

1. Deadline Cloud 모니터 열기.
2. 팜 목록에서 관심 있는 대기열이 포함된 팜을 선택합니다.
3. 대기열 목록에서 세부 정보를 표시할 대기열을 선택합니다. 둘 이상의 대기열 구성을 비교하려면 둘 이상의 확인란을 선택합니다.
4. 대기열의 작업 목록을 보려면 대기열 목록 또는 세부 정보 패널에서 대기열 이름을 선택합니다.

모니터가 이미 열려 있는 경우 왼쪽 탐색 창의 대기열 목록에서 대기열을 선택할 수 있습니다.

플릿 세부 정보를 보려면

1. Deadline Cloud 모니터 열기.
2. 팜 목록에서 관심 있는 플릿이 포함된 팜을 선택합니다.
3. 팜 리소스에서 플릿을 선택합니다.

4. 플릿 목록에서 세부 정보를 표시할 플릿을 선택합니다. 둘 이상의 플릿 구성을 비교하려면 둘 이상의 확인란을 선택합니다.
5. 플릿의 작업자 목록을 보려면 플릿 목록 또는 세부 정보 패널에서 플릿 이름을 선택합니다.

모니터가 이미 열려 있는 경우 왼쪽 탐색 창의 플릿 목록에서 플릿을 선택할 수 있습니다.

Deadline Cloud에서 작업, 단계 및 작업 관리

대기열을 선택하면 Deadline Cloud 모니터의 작업 모니터 섹션에 해당 대기열의 작업, 작업의 단계 및 각 단계의 작업이 표시됩니다. 작업, 단계 또는 작업을 선택할 때 작업 메뉴를 사용하여 각 작업을 관리할 수 있습니다.

작업 모니터를 열려면 단계에 따라에서 대기열을 확인한 Deadline Cloud에서 대기열 및 플릿 세부 정보 보기다음 작업할 작업, 단계 또는 작업을 선택합니다.

작업, 단계 및 작업의 경우 다음을 수행할 수 있습니다.

- 상태를 Requeued, Succeeded, Failed 또는 Canceled로 변경합니다.
- 작업, 단계 또는 작업에서 처리된 출력을 다운로드합니다.
- 작업, 단계 또는 작업의 ID를 복사합니다.

선택한 작업의 경우 다음을 수행할 수 있습니다.

- 작업을 아카이브합니다.
- 우선순위 변경 또는 단계 종속성에 대한 보기 단계와 같은 작업 속성을 수정합니다.
- 작업의 파라미터를 사용하여 추가 세부 정보를 봅니다.
- 작업을 다시 제출합니다.

자세한 내용은 Deadline Cloud에서 작업 세부 정보 보기 및 관리 단원을 참조하세요.

각 단계에 대해 다음을 수행할 수 있습니다.

- 단계의 종속성을 봅니다. 단계가 실행되기 전에 단계의 종속성을 완료해야 합니다.

자세한 내용은 Deadline Cloud에서 단계 보기을 참조하세요.

각 작업에 대해 다음을 수행할 수 있습니다.

- 작업에 대한 로그를 봅니다.
- 작업 파라미터를 봅니다.

자세한 내용은 Deadline Cloud에서 작업 보기 단원을 참조하십시오.

Deadline Cloud에서 작업 세부 정보 보기 및 관리

Deadline Cloud Monitor의 작업 모니터 페이지에서는 다음을 제공합니다.

- 작업 진행 상황에 대한 전체 보기입니다.
- 작업을 구성하는 단계 및 작업의 보기입니다.

목록에서 작업을 선택하여 작업의 단계 목록을 확인한 다음 단계 목록에서 단계를 선택하여 작업의 작업을 봅니다. 항목을 선택한 후 해당 항목에 대한 작업 메뉴를 사용하여 세부 정보를 볼 수 있습니다.

작업 세부 정보를 보려면

1. 단계에 따라에서 대기열을 봅니다Deadline Cloud에서 대기열 및 플릿 세부 정보 보기.
2. 탐색 창에서 작업을 제출한 대기열을 선택합니다.
3. 다음 방법 중 하나를 사용하여 작업을 선택합니다.
   a. 작업 목록에서 세부 정보를 볼 작업을 선택합니다.
   b. 검색 필드에서 작업을 생성한 작업 이름 또는 사용자와 같이 작업과 연결된 텍스트를 입력합니다. 표시되는 결과에서 보려는 작업을 선택합니다.

작업 세부 정보에는 작업의 단계와 각 단계의 작업이 포함됩니다. 작업 메뉴를 사용하여 다음을 수행할 수 있습니다.

- 작업 상태를 변경합니다.
- 작업의 속성을 보고 수정합니다.
  - 작업의 단계 간 종속성을 볼 수 있습니다.
  - 대기열에서 작업의 우선 순위를 변경할 수 있습니다. 우선 순위가 높은 작업은 우선 순위가 낮은 작업보다 먼저 처리됩니다. 작업의 우선 순위는 1~100입니다. 두 작업의 우선 순위가 같으면 가장 오래된 작업이 먼저 예약됩니다.

- 작업이 제출될 때 설정된 작업의 파라미터를 봅니다.
- 작업의 출력을 다운로드합니다. 작업의 출력을 다운로드하면 작업의 단계와 작업에서 생성된 모든 출력이 포함됩니다.

작업 아카이브

작업을 아카이브하려면 작업이 터미널 상태, , FAILED, SUCCEEDED SUSPENDED또는에 있어야 합니다CANCELED. ARCHIVED 상태는 최종입니다. 작업이 아카이브된 후에는 다시 대기열에 추가하거나 수정할 수 없습니다.

작업의 데이터는 작업을 아카이빙해도 영향을 받지 않습니다. 비활성 제한 시간에 도달하거나 작업이 포함된 대기열이 삭제되면 데이터가 삭제됩니다.

아카이브된 작업에 발생하는 기타 상황:

- 보관된 작업은 Deadline Cloud 모니터에 숨겨집니다.
- 보관된 작업은 삭제 전 120일 동안 Deadline Cloud CLI의 읽기 전용 상태로 표시됩니다.

작업 다시 대기열에 추가

작업을 다시 대기열에 추가하면 단계 종속성이 없는 모든 작업이 로 전환됩니다READY. 종속성이 있는 단계의 상태는 복원PENDING될 때 READY 또는 로 전환됩니다.

- 모든 작업, 단계 및 작업이 로 전환됩니다PENDING.
- 단계에 종속성이 없는 경우 로 전환됩니다READY.

작업 다시 제출

작업을 다시 실행하고 싶지만 속성과 설정이 다른 경우가 있을 수 있습니다. 예를 들어 테스트 프레임의 하위 집합을 렌더링하고 출력을 확인한 다음 전체 프레임 범위로 작업을 다시 실행하는 작업을 제출할 수 있습니다. 이렇게 하려면 작업을 다시 제출합니다.

작업을 다시 제출하면 종속성이 없는 새 작업이이 됩니다READY. 종속성이 있는 새 태스크는이 됩니다PENDING.

- 모든 새 작업, 단계 및 작업은이 됩니다PENDING.
- 새 단계에 종속성이 없는 경우가 됩니다READY.

작업을 다시 제출할 때 작업이 처음 생성될 때 구성 가능한 것으로 정의된 속성만 변경할 수 있습니다. 예를 들어, 작업 이름이 처음 제출될 때 작업의 구성 가능한 속성으로 정의되지 않은 경우 재제출 시 이름을 편집할 수 없습니다.

Deadline Cloud에서 단계 보기

AWS Deadline Cloud 모니터를 사용하여 처리 작업의 단계를 봅니다. 작업 모니터의 단계 목록에는 선택한 작업을 구성하는 단계 목록이 표시됩니다. 단계를 선택하면 작업 목록에 단계의 작업이 표시됩니다.

단계를 보려면

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.
2. 작업 목록에서 작업을 선택합니다.
3. 단계 목록에서 단계를 선택합니다.

작업 메뉴를 사용하여 다음을 수행할 수 있습니다.

- 단계의 상태를 변경합니다.
- 단계의 출력을 다운로드합니다. 단계의 출력을 다운로드하면 단계의 작업에서 생성된 모든 출력이 포함됩니다.
- 단계의 종속성을 봅니다. 종속성 테이블에는 선택한 단계가 시작되기 전에 완료해야 하는 단계 목록과이 단계가 완료될 때까지 대기 중인 단계 목록이 표시됩니다.

Deadline Cloud에서 작업 보기

AWS Deadline Cloud 모니터를 사용하여 처리 작업의 작업을 봅니다. 작업 모니터의 작업 목록에는 단계 목록에서 선택한 단계를 구성하는 작업이 표시됩니다.

작업 보기

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.
2. 작업 목록에서 작업을 선택합니다.
3. 단계 목록에서 단계를 선택합니다.
4. 작업 목록에서 작업을 선택합니다.

작업 메뉴를 사용하여 다음을 수행할 수 있습니다.

- 작업의 상태를 변경합니다.
- 작업 로그를 봅니다. 자세한 내용은 Deadline Cloud에서 세션 및 작업자 로그 보기 단원을 참조하십시오.
- 작업이 생성될 때 설정된 파라미터를 봅니다.
- 작업의 출력을 다운로드합니다. 작업의 출력을 다운로드하면 선택한 작업에서 생성된 출력만 포함됩니다.

Deadline Cloud에서 세션 및 작업자 로그 보기

로그는 작업의 상태 및 처리에 대한 자세한 정보를 제공합니다. AWS Deadline Cloud 모니터에서 다음 두 가지 유형의 로그를 볼 수 있습니다.

- 세션 로그는 다음을 포함한 작업 타임라인을 자세히 설명합니다.
  - 연결 동기화 및 소프트웨어 환경 로드와 같은 설정 작업
  - 작업 또는 작업 세트 실행
  - 작업자의 환경 종료와 같은 종결 작업

  세션에는 하나 이상의 작업 처리가 포함되며 여러 작업을 포함할 수 있습니다. 세션 로그에는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 유형, vCPU 및 메모리에 대한 정보도 표시됩니다. 세션 로그에는 세션에 사용된 작업자의 로그에 대한 링크도 포함됩니다.
- 작업자 로그는 작업자가 수명 주기 동안 처리하는 작업의 타임라인에 대한 세부 정보를 제공합니다. 작업자 로그에는 여러 세션에 대한 정보가 포함될 수 있습니다.

세션 및 작업자 로그를 다운로드하여 오프라인으로 검사할 수 있습니다.

세션 로그를 보려면

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.
2. 작업 목록에서 작업을 선택합니다.
3. 단계 목록에서 단계를 선택합니다.
4. 작업 목록에서 작업을 선택합니다.
5. 작업 메뉴에서 로그 보기를 선택합니다.

타임라인 섹션에는 작업에 대한 작업 요약이 표시됩니다. 세션에서 더 많은 작업이 실행되는지 확인하고 세션에 대한 종료 작업을 보려면 모든 작업에 대한 로그 보기를 선택합니다.

작업의 작업자 로그를 보려면

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.
2. 작업 목록에서 작업을 선택합니다.
3. 단계 목록에서 단계를 선택합니다.
4. 작업 목록에서 작업을 선택합니다.
5. 작업 메뉴에서 로그 보기를 선택합니다.
6. 세션 정보를 선택합니다.
7. 작업자 로그 보기를 선택합니다.

플릿 세부 정보에서 작업자 로그를 보려면

1. 의 단계에 따라 Deadline Cloud에서 대기열 및 플릿 세부 정보 보기 플릿을 봅니다.
2. 작업자 목록에서 작업자 ID를 선택합니다.
3. 작업 메뉴에서 작업자 로그 보기를 선택합니다.

작업자 대시보드에서 작업자 세부 정보 보기

작업자 대시보드는 작업을 처리하는 작업자에 대한 세부 정보를 제공합니다. 다음을 확인할 수 있습니다.

- 작업자의 인스턴스 유형과 같은 메타데이터
- 작업자가 수행한 세션 작업
- CPU, 메모리 및 디스크 사용량을 포함한 작업자 성능
- 시간 경과에 따른 CPU, 메모리 및 디스크 사용량 그래프
- 시간 경과에 따른 디스크 속도 그래프
- 작업에 대한 작업자 로그

작업에서 작업자 대시보드를 보려면

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.

2. 작업 목록에서 작업을 선택합니다.
3. 단계 목록에서 단계를 선택합니다.
4. 작업 목록에서 작업을 선택합니다.
5. 작업 테이블의 작업 메뉴에서 작업자 대시보드 보기를 선택합니다.

플릿 세부 정보에서 작업자 대시보드를 보려면

1. 의 단계에 따라 Deadline Cloud에서 대기열 및 플릿 세부 정보 보기 플릿을 봅니다.
2. 작업자 목록에서 작업자를 선택합니다.
3. 작업 메뉴에서 작업자 대시보드 보기를 선택합니다.

사용 사례

과소 프로비저닝된 인스턴스 감지

렌더링이 예상보다 오래 걸리는 경우 작업자 대시보드를 통해 인스턴스가 워크로드에 적합한 크기인지 확인할 수 있습니다. 많은 렌더러의 경우 vCPU 사용률이 100% 정상이지만 최대 용량에 가까운 메모리 사용량이 지속적으로 높고 디스크 공간 사용률이 높아지면 인스턴스가 과소 프로비저닝된 것일 수 있습니다. 이러한 경우 플릿의 인스턴스 구성을 업그레이드하면 렌더링 오류를 줄이고 렌더링 시간을 크게 개선할 수 있습니다. 그러나 업그레이드 후 작업자 성능을 계속 모니터링하여 최적의 균형을 찾았는지 확인하는 것이 중요합니다. 너무 적극적으로 업그레이드하면 오버프로비저닝으로 인해 불필요한 비용이 발생할 수 있습니다.

과다 프로비저닝된 인스턴스 감지

작업이 성공적으로 완료되더라도 비용을 최적화할 기회가 있을 수 있습니다. 작업자 대시보드를 통해 워크로드에 필요한 것보다 더 많은 컴퓨팅 성능에 대해 비용을 지불하고 있는지 확인할 수 있습니다. 작업자가 평균 vCPU 사용량이 낮고 메모리 사용률이 최소화되며 사용되지 않는 디스크 공간이 초과되는 경우 플릿의 인스턴스 구성을 축소할 수 있습니다.

실패한 작업 문제 해결

실패한 작업을 조사할 때 작업자 대시보드는 중요한 진단 도구 역할을 합니다. 최대 메모리 사용량 및 디스크 공간 사용률에 특히 주의하십시오. 이러한 지표가 100%에 가깝거나 도달하면 작업 실패의 근본 원인일 수 있습니다. 이러한 리소스 소진은 현재 인스턴스에 워크로드를 효과적으로 처리할 수 있는 용량이 부족함을 나타냅니다. 이러한 경우 메모리 또는 디스크 공간이 늘어난 인스턴스를 프로비저닝하면 성공적인 작업 완료를 보장하는 데 도움이 됩니다.

최적의 인스턴스 사용률

vCPU 사용률

목표 범위: 70~90%

- 70% 미만: 컴퓨팅 리소스 사용률이 낮을 수 있습니다. 즉, 워크로드에 필요한 것보다 더 많은 CPU 비용을 지불하고 있습니다.
- 70~90%: 병목 현상 없이 리소스를 효율적으로 사용하는 최적의 범위
- 일관되게 100%: 렌더링 속도가 느려질 수 있는 CPU 병목 현상을 나타낼 수 있음

일부 렌더링 작업은 자연스럽게 다른 렌더링 작업보다 CPU 집약적이며 100% vCPU 사용량은 문제가 되지 않을 수 있습니다. 실시간 시각화 작업에서는 CPU 사용률이 더 일관되게 표시될 수 있지만, 컴퓨팅 요구 사항이 변화하는 작업에는 다양한 패턴이 있을 수 있습니다.

메모리 사용률

목표 범위: 70~85%

- 50% 미만: 워크로드에 대해 잠재적으로 크기가 큰 인스턴스
- 70~85%: 스파이크에 충분한 헤드룸을 갖춘 최적의 사용률
- 90% 초과: 성능 저하 또는 out-of-memory 오류 위험

메모리 요구 사항은 장면 복잡성, 텍스처 해상도 및 시뮬레이션 데이터에 따라 크게 달라질 수 있습니다. 시간 경과에 따른 메모리 추세를 모니터링하는 것은 워크로드의 메모리 요구 사항이 증가하고 있는지 식별하는 데 중요합니다.

디스크 공간 사용률

목표 범위: 60~80%

- 40% 미만: 과다 프로비저닝된 스토리지 가능성
- 60~85%: 임시 파일 및 캐시를 위한 공간을 통한 우수한 사용률
- 85% 초과: 대규모 렌더링 중에 공간이 부족할 위험

특히 렌더링 중에 대용량 텍스처 또는 캐시 파일을 읽거나 쓰는 워크로드의 경우 디스크 I/O 성능이 용량만큼 중요할 수 있습니다.

Deadline Cloud에서 완료된 출력 다운로드

작업이 완료되면 AWS Deadline Cloud 모니터를 사용하여 결과를 워크스테이션에 다운로드할 수 있습니다. 출력 파일은 작업을 생성할 때 지정한 이름과 위치와 함께 저장됩니다.

출력 파일은 무기한 저장됩니다. 스토리지 비용을 줄이려면 대기열의 Amazon S3 버킷에 대한 S3 수명 주기 구성을 생성하는 것이 좋습니다. Amazon S3 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 스토리지 수명 주기 관리를 참조하세요.

작업, 단계 또는 작업의 완료된 출력을 다운로드하려면

1. 의 단계에 따라 작업 목록을 Deadline Cloud에서 작업 세부 정보 보기 및 관리 봅니다.
2. 출력을 다운로드할 작업, 단계 또는 작업을 선택합니다.
   - 작업을 선택하면 해당 작업의 모든 단계에서 모든 작업에 대한 모든 출력을 다운로드할 수 있습니다.
   - 단계를 선택하면 해당 단계의 모든 작업에 대한 모든 출력을 다운로드할 수 있습니다.
   - 작업을 선택하면 해당 개별 작업에 대한 출력을 다운로드할 수 있습니다.
3. 작업 메뉴에서 출력 다운로드를 선택합니다.
4. 출력은 작업이 제출될 때 설정된 위치로 다운로드됩니다.

> **Note**
>
> 메뉴를 사용한 출력 다운로드는 현재 Windows 및 에서만 지원됩니다Linux. 가 Mac 있고 출력 다운로드 메뉴 항목을 선택하면 창에 렌더링된 출력을 다운로드하는 데 사용할 수 있는 AWS CLI 명령이 표시됩니다.

기한 클라우드 팜

Deadline Cloud 팜을 사용하면 사용자와 프로젝트 리소스를 관리할 수 있습니다. 팜은 프로젝트 리소스가 있는 입니다. 팜은 대기열과 플릿으로 구성됩니다. 대기열은 제출된 작업이 위치하고 렌더링되도록 예약된 곳입니다. 플릿은 작업을 실행하여 작업을 완료하는 작업자 노드 그룹입니다. 팜을 생성한 후 프로젝트의 요구 사항에 맞게 대기열과 플릿을 생성할 수 있습니다.

팜 생성

1. 기한 클라우드 콘솔에서 대시보드로 이동을 선택합니다.
2. Deadline Cloud 대시보드의 팜 섹션에서 작업 → 팜 생성을 선택합니다.
   - 또는 왼쪽 패널에서 팜 및 기타 리소스를 선택한 다음 팜 생성을 선택합니다.
3. 팜의 이름을 추가합니다.
4. 설명에 팜 설명을 입력합니다. 명확한 설명은 팜의 목적을 빠르게 식별하는 데 도움이 될 수 있습니다.
5. (선택 사항) 기본적으로 데이터는 보안을 위해가 AWS 소유하고 관리하는 키로 암호화됩니다. 암호화 설정 사용자 지정(고급)을 선택하여 기존 키를 사용하거나 관리하는 새 키를 생성할 수 있습니다.

   확인란을 사용하여 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS ARN을 입력하거나 새 KMS 키 생성을 AWS KMS 선택하여 새를 생성합니다.
6. (선택 사항) 새 태그 추가를 선택하여 팜에 하나 이상의 태그를 추가합니다.
7. 팜 생성을 선택합니다. 생성 후 팜이 표시됩니다.

기한 클라우드 대기열

대기열은 작업을 관리하고 처리하는 팜 리소스입니다.

대기열을 사용하려면 모니터와 팜이 이미 설정되어 있어야 합니다.

주제

- 대기열 생성
- 대기열 환경 생성
- 대기열과 플릿 연결

대기열 생성

1. Deadline Cloud 콘솔 대시보드에서 대기열을 생성할 팜을 선택합니다.
   - 또는 왼쪽 패널에서 팜 및 기타 리소스를 선택한 다음 대기열을 생성할 팜을 선택합니다.
2. 대기열 탭에서 대기열 생성을 선택합니다.
3. 대기열의 이름을 입력합니다.
4. 설명에 대기열 설명을 입력합니다. 설명은 대기열의 목적을 식별하는 데 도움이 됩니다.
5. 작업 연결의 경우 새 Amazon S3 버킷을 생성하거나 기존 Amazon S3 버킷을 선택할 수 있습니다.
   a. 새 Amazon S3 버킷을 생성하려면
      i. 새 작업 버킷 생성을 선택합니다.
      ii. 버킷의 이름을 입력합니다. 버킷의 이름을 로 지정하는 것이 좋습니다`deadlinecloud-job-attachments-[MONITORNAME]`.
      iii. 루트 접두사를 입력하여 대기열의 루트 위치를 정의하거나 변경합니다.
   b. 기존 Amazon S3 버킷을 선택하려면
      i. 기존 S3 버킷 선택 > S3 찾아보기를 선택합니다.
      ii. 사용 가능한 버킷 목록에서 대기열의 S3 버킷을 선택합니다.
6. (선택 사항) 대기열을 고객 관리형 플릿과 연결하려면 고객 관리형 플릿과의 연결 활성화를 선택합니다.
7. 고객 관리형 플릿과의 연결을 활성화하는 경우 다음 단계를 완료해야 합니다.

> **Important**
>
> 실행 기능을 위한 사용자 및 그룹을 지정하는 것이 좋습니다. 그렇지 않으면 작업이 작업자의 에이전트가 수행할 수 있는 모든 작업을 수행할 수 있으므로 팜의 보안 태세가 저하됩니다. 잠재적 보안 위험에 대한 자세한 내용은 사용자 및 그룹으로 작업 실행을 참조하세요.

a. 사용자로 실행의 경우:

   대기열 작업에 대한 자격 증명을 제공하려면 대기열로 구성된 사용자를 선택합니다.

   또는 자체 자격 증명 설정을 옵트아웃하고 작업자 에이전트 사용자로 작업을 실행하려면 작업자 에이전트 사용자를 선택합니다.

b. (선택 사항) 사용자 자격 증명으로 실행에 사용자 이름과 그룹 이름을 입력하여 대기열 작업에 대한 자격 증명을 제공합니다.

   Windows 플릿을 사용하는 경우 사용자로 실행에 대한 암호가 포함된 보안 암호를 생성 AWS Secrets Manager 해야 합니다. 암호가 있는 기존 보안 암호가 없는 경우 보안 암호 생성을 선택하여 Secrets Manager 콘솔을 열어 보안 암호를 생성합니다. 자세한 내용은 Deadline Cloud 개발자 안내서의 Windows 작업 사용자 보안 암호에 대한 액세스 관리를 참조하세요.

8. 예산을 요구하면 대기열 비용을 관리하는 데 도움이 됩니다. 예산 필요 없음 또는 예산 필요 중 하나를 선택합니다.

9. 대기열에 사용자를 대신하여 Amazon S3에 액세스할 수 있는 권한이 필요합니다. 새 서비스 역할을 생성하거나 기존 서비스 역할을 사용할 수 있습니다. 기존 서비스 역할이 없는 경우 새 서비스 역할을 생성하고 사용합니다.

   a. 기존 서비스 역할을 사용하려면 서비스 역할 선택을 선택한 다음 드롭다운에서 역할을 선택합니다.

   b. 새 서비스 역할을 생성하려면 새 서비스 역할 생성 및 사용을 선택한 다음 역할 이름과 설명을 입력합니다.

10. (선택 사항) 대기열 환경에 대한 환경 변수를 추가하려면 새 환경 변수 추가를 선택한 다음 추가하는 각 변수의 이름과 값을 입력합니다.

11. (선택 사항) 새 태그 추가를 선택하여 대기열에 하나 이상의 태그를 추가합니다.

12. 기본 Conda 대기열 환경을 생성하려면 확인란을 선택한 상태로 유지합니다. 대기열 환경에 대한 자세한 내용은 대기열 환경 생성을 참조하세요. 고객 관리형 플릿에 대한 대기열을 생성하는 경우 확인란의 선택을 취소합니다.
13. 대기열 생성을 선택합니다.

대기열 환경 생성

대기열 환경은 플릿 작업자를 설정하는 환경 변수 및 명령 세트입니다. 대기열 환경을 사용하여 대기열의 작업에 소프트웨어 애플리케이션, 환경 변수 및 기타 리소스를 제공할 수 있습니다.

대기열을 생성할 때 기본 Conda 대기열 환경을 생성할 수 있습니다. 이 환경은 파트너 DCC 애플리케이션 및 렌더러용 패키지에 대한 서비스 관리형 플릿 액세스를 제공합니다. 기본 환경 자세한 내용은 섹션을 참조하세요기본 Conda 대기열 환경.

콘솔을 사용하거나 json 또는 YAML 템플릿을 직접 편집하여 대기열 환경을 추가할 수 있습니다. 이 절차에서는 콘솔을 사용하여 환경을 생성하는 방법을 설명합니다.

1. 대기열에 대기열 환경을 추가하려면 대기열로 이동하여 대기열 환경 탭을 선택합니다.
2. 작업을 선택한 다음 양식으로 새로 생성을 선택합니다.
3. 대기열 환경의 이름과 설명을 입력합니다.
4. 새 환경 변수 추가를 선택한 다음 추가하는 각 변수의 이름과 값을 입력합니다.
5. (선택 사항) 대기열 환경의 우선 순위를 입력합니다. 우선 순위는이 대기열 환경이 작업자에서 실행되는 순서를 나타냅니다. 우선 순위가 높은 대기열 환경이 먼저 실행됩니다.
6. 대기열 환경 생성을 선택합니다.

기본 Conda 대기열 환경

서비스 관리형 플릿과 연결된 대기열을 생성할 때가 작업을 위한 가상 환경에서 패키지를 다운로드하고 설치Conda하도록 지원하는 기본 대기열 환경을 추가할 수 있습니다.

Deadline Cloud 콘솔을 사용하여 기본 대기열 환경을 추가하면 환경이 자동으로 생성됩니다. AWS CLI 또는와 같은 다른 방법으로 대기열을 추가하는 경우 대기열 환경을 직접 생성 AWS CloudFormation해야 합니다. 환경에 대한 올바른 콘텐츠가 있는지 확인하려면 GitHub에서 대기열 환경 템플릿 YAML 파일을 참조할 수 있습니다. 기본 대기열 환경의 내용은 GitHub의 기본 대기열 환경 YAML 파일을 참조하세요.

GitHub에서 필요에 따라 시작점으로 사용할 수 있는 다른 대기열 환경 템플릿이 있습니다.

Conda는 채널의 패키지를 제공합니다. 채널은 패키지가 저장되는 위치입니다. Deadline Cloud는 파트너 DCC 애플리케이션 및 렌더러를 지원하는 Conda 패키지를 호스팅`deadline-cloud`하는 채널을 제공합니다. 아래의 각 탭을 선택하여 Linux 또는에 사용할 수 있는 패키지를 확인합니다Windows.

Linux

- 블렌더
  - `blender=3.6`
  - `blender=4.2`
  - `blender-openjd`
- 하우디니
  - `houdini=19.5`
  - `houdini=20.0`
  - `houdini=20.5`
  - `houdini-openjd`
- Maya
  - `maya=2024`

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

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

Windows

- After Effects
  - `aftereffects=24.6`
  - `aftereffects=25.1`
- Cinema 4D

    - `cinema4d=2024`
    - `cinema4d=2025`
    - `cinema4d-openjd`
  - KeyShot
    - `keyshot=2024`
    - `keyshot-openjd`

기본 Conda 환경이 있는 대기열에 작업을 제출하면 환경이 작업에 두 개의 파라미터를 추가합니다. 이러한 파라미터는 작업이 처리되기 전에 작업 환경을 구성하는 데 사용할 Conda 패키지와 채널을 지정합니다. 파라미터는 다음과 같습니다.

- `CondaPackages` - `blender=3.6` 또는와 같은 패키지 일치 사양의 공백으로 구분된 목록입니다`numpy>1.22`. 가상 환경 생성을 건너뛰려면 기본값이 비어 있습니다.
- `CondaChannels` - `deadline-cloud`, `conda-forge`또는와 같이 공백으로 구분된 Conda 채널 목록입니다`s3://amzn-s3-demo-bucket/conda/channel`. 기본값은 파트너 DCC 애플리케이션 및 렌더러`deadline-cloud`를 제공하는 서비스 관리형 플릿에서 사용할 수 있는 채널인 입니다.

통합 제출자를 사용하여 DCC에서 Deadline Cloud로 작업을 전송하는 경우 제출자는 DCC 애플리케이션 및 제출자를 기반으로 `CondaPackages` 파라미터 값을 채웁니다. 예를 들어 Blender를 사용하는 경우 `CondaPackage` 파라미터는 로 설정됩니다`blender=3.6.* blender-openjd=0.4.*`.

블렌더=3.6과 같이 위 표에 나열된 버전에만 제출을 고정시키는 것이 좋습니다. 이는 패치 릴리스가 사용 가능한 패키지에 영향을 미치기 때문입니다. 예를 들어 Blender 3.6.17을 릴리스하면 더 이상 Blender 3.6.16을 배포하지 않습니다. blender=3.6.16에 고정된 모든 제출은 실패합니다. blender=3.6에 고정하면 최신 분산 패치 버전을 받게 되며 작업은 영향을 받지 않습니다. 기본적으로 DCC 제출자는 블렌더=3.6과 같은 패치 번호를 제외하고 위 표에 나열된 현재 버전에 고정됩니다.

대기열과 플릿 연결

작업을 처리하려면 대기열을 플릿과 연결해야 합니다. 단일 플릿을 여러 대기열에 연결하고 단일 대기열을 여러 플릿에 연결할 수 있습니다. 플릿을 여러 대기열과 연결하면 해당 대기열 간에 작업자를 균등하게 나눕니다. 마찬가지로 대기열을 여러 플릿과 연결하면 해당 플릿에 작업이 균등하게 분산됩니다. 다음 단계에 따라 기존 대기열을 기존 플릿과 연결합니다.

1. Deadline Cloud 팜에서 플릿과 연결할 대기열을 선택합니다. 대기열이 표시됩니다.

2. 대기열과 연결할 플릿을 선택하려면 플릿 연결을 선택합니다.
3. 플릿 선택 드롭다운을 선택합니다. 사용 가능한 플릿 목록이 표시됩니다.
4. 사용 가능한 플릿 목록에서 대기열과 연결할 플릿 또는 플릿 옆에 있는 확인란을 선택합니다.
5. 연결을 선택합니다. 이제 플릿 연결 상태가 연결됨이어야 합니다.

Deadline Cloud 플릿

이 섹션에서는 Deadline Cloud에 대한 서비스 관리형 플릿 및 고객 관리형 플릿(CMF)을 관리하는 방법을 설명합니다.

두 가지 유형의 Deadline Cloud 플릿을 설정할 수 있습니다.

- 서비스 관리형 플릿은 Deadline Cloud에서 제공하는 기본 설정이 있는 작업자 플릿입니다. 이러한 기본 설정은 효율적이고 비용 효율적으로 설계되었습니다.
- 고객 관리형 플릿(CMFs)을 사용하면 처리 파이프라인을 완벽하게 제어할 수 있습니다. CMF는 AWS 인프라, 온프레미스 또는 공동 위치 데이터 센터에 상주할 수 있습니다. 여기에는 플릿의 작업자 프로비저닝, 운영, 관리 및 폐기가 포함됩니다.

플릿을 여러 대기열과 연결하면 해당 대기열 간에 작업자를 균등하게 나눕니다.

주제

- 서비스 관리형 플릿
- 고객 관리형 플릿

서비스 관리형 플릿

서비스 관리형 플릿(SMF)은 Deadline Cloud에서 제공하는 기본 설정이 있는 작업자 플릿입니다. 이러한 기본 설정은 효율적이고 비용 효율적으로 설계되었습니다.

일부 기본 설정은 작업자와 작업을 실행할 수 있는 시간을 제한합니다. 작업자는 7일 동안만 실행할 수 있으며 작업은 5일 동안만 실행할 수 있습니다. 한도에 도달하면 작업 또는 작업자가 중지됩니다. 이 경우 작업자 또는 작업이 실행 중인 작업이 손실될 수 있습니다. 이를 방지하려면 작업자와 작업을 모니터링하여 최대 기간 제한을 초과하지 않는지 확인합니다. 작업자 모니터링에 대한 자세한 내용은 섹션을 참조하세요Deadline Cloud 모니터 사용.

서비스 관리형 플릿 생성

1. Deadline Cloud 콘솔에서 플릿을 생성할 팜으로 이동합니다.
2. 플릿 탭을 선택한 다음 플릿 생성을 선택합니다.
3. 플릿의 이름을 입력합니다.

4. (선택 사항) 설명을 입력합니다. 명확한 설명은 플릿의 목적을 빠르게 식별하는 데 도움이 될 수 있습니다.
5. 서비스 관리형 플릿 유형을 선택합니다.
6. 플릿의 스팟 또는 온디맨드 인스턴스 시장 옵션을 선택합니다. 스팟 인스턴스는 예약되지 않은 용량으로, 할인된 가격으로 사용할 수 있지만 온디맨드 요청에 의해 중단될 수 있습니다. 온디맨드 인스턴스는 초 단위로 요금이 책정되지만 장기 약정은 없으며 중단되지 않습니다. 기본적으로 플릿은 스팟 인스턴스를 사용합니다.
7. 플릿에 대한 서비스 액세스에서 기존 역할을 선택하거나 새 역할을 생성합니다. 서비스 역할은 플릿의 인스턴스에 자격 증명을 제공하여 작업을 처리할 수 있는 권한을 부여하고, 사용자가 로그 정보를 읽을 수 있도록 모니터의 사용자에게 자격 증명을 제공합니다.
8. 다음을 선택합니다.
9. CPU 전용 인스턴스 또는 GPU 가속 인스턴스 중에서 선택합니다. GPU 가속 인스턴스는 작업을 더 빠르게 처리할 수 있지만 비용이 더 많이 들 수 있습니다.
10. 작업자의 운영 체제를 선택합니다. 기본값인 Linux를 그대로 두거나를 선택할 수 있습니다Windows.
11. (선택 사항) GPU 가속 인스턴스를 선택한 경우 각 인스턴스의 최대 및 최소 GPUs 설정합니다. 테스트 목적으로 GPU는 1개로 제한됩니다. 프로덕션 워크로드에 대해 더 많은 것을 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.
12. 플릿에 필요한 최소 및 최대 vCPU를 입력합니다.
13. 플릿에 필요한 최소 및 최대 메모리를 입력합니다.
14. (선택 사항) 특정 인스턴스 유형만이 플릿에 사용되도록 플릿에서 특정 인스턴스 유형을 허용하거나 제외하도록 선택할 수 있습니다.
15. (선택 사항) 대기열의 작업에 용량을 사용할 수 있도록 플릿을 확장할 최대 인스턴스 수를 설정합니다. 대기열에 작업이 없을 때 플릿이 모든 인스턴스를 해제0하도록 최소 인스턴스 수를에 두는 것이 좋습니다.
16. (선택 사항)이 플릿의 작업자에 연결할 Amazon Elastic Block Store(Amazon EBS) gp3 볼륨의 크기를 지정할 수 있습니다. 자세한 내용은 EBS 사용 설명서를 참조하세요.
17. 다음을 선택합니다.
18. (선택 사항) 작업 제출 시 지정된 사용자 지정 호스트 기능과 결합할 수 있는이 플릿의 기능을 정의하는 사용자 지정 작업자 기능을 정의합니다. 한 가지 예는 플릿을 자체 라이선스 서버에 연결하려는 경우의 특정 라이선스 유형입니다.
19. 다음을 선택합니다.

20. (선택 사항) 플릿을 대기열과 연결하려면 드롭다운에서 대기열을 선택합니다. 대기열이 기본 Conda 대기열 환경으로 설정된 경우 플릿에 파트너 DCC 애플리케이션 및 렌더러를 지원하는 패키지가 자동으로 제공됩니다. 제공된 패키지 목록은 섹션을 참조하세요기본 Conda 대기열 환경.
21. 다음을 선택합니다.
22. (선택 사항) 플릿에 태그를 추가하려면 새 태그 추가를 선택한 다음 해당 태그의 키와 값을 입력합니다.
23. 다음을 선택합니다.
24. 플릿 설정을 검토한 다음 플릿 생성을 선택합니다.

GPU 액셀러레이터 사용

하나 이상의 GPUs를 구성할 수 있습니다. 액셀러레이터를 사용하면 작업을 처리하는 데 걸리는 시간을 줄일 수 있지만 각 작업자 인스턴스의 비용이 증가할 수 있습니다. GPU 액셀러레이터를 사용하는 플릿과 그렇지 않은 플릿 간의 장단점을 이해하려면 워크로드를 테스트해야 합니다.

> **Note**
> 테스트 목적으로 GPU는 1개로 제한됩니다. 프로덕션 워크로드에 대해 더 많은 것을 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

작업자 인스턴스 기능을 지정할 때 플릿이 GPU 액셀러레이터를 사용할지 여부를 결정합니다. GPUs를 사용하기로 결정한 경우 각 인스턴스의 최소 및 최대 GPUs 수, 사용할 GPU 칩 유형, GPU의 런타임 드라이버를 GPUs.

사용 가능한 GPU 액셀러레이터는 다음과 같습니다.

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

다음 런타임 드라이버 중에서 선택할 수 있습니다.

- `Latest` - 칩에 사용할 수 있는 최신 런타임을 사용합니다. 를 지정`latest`하고 새 버전의 런타임이 릴리스되면 새 버전의 런타임이 사용됩니다.

- `grid:r570` - NVIDIA vGPU 소프트웨어 18
- `grid:r550` - NVIDIA vGPU 소프트웨어 17
- `grid:r535` - NVIDIA vGPU 소프트웨어 16

런타임을 지정하지 않으면 Deadline Cloud는를 기본값`latest`으로 사용합니다. 그러나 액셀러레이터가 여러 개 있고 일부에 `latest` 대해를 지정하고 다른는 비워 두면 Deadline Cloud에서 예외가 발생합니다.

서비스 관리형 플릿에 대한 소프트웨어 라이선스

Deadline Cloud는 일반적으로 사용되는 소프트웨어 패키지에 대해 사용량 기반 라이선스(UBL)를 제공합니다. 지원되는 소프트웨어 패키지는 서비스 관리형 플릿에서 실행될 때 자동으로 라이선스가 부여됩니다. 소프트웨어 라이선스 서버를 구성하거나 유지 관리할 필요가 없습니다. 라이선스는 대규모 작업에서 부족하지 않도록 확장됩니다.

기본 제공 Deadline Cloud conda 채널을 사용하여 UBL을 지원하는 소프트웨어 패키지를 설치하거나 자체 패키지를 사용할 수 있습니다. conda 채널에 대한 자세한 내용은 섹션을 참조하세요대기열 환경 생성.

지원되는 소프트웨어 패키지 목록과 UBL 요금에 대한 자세한 내용은 AWS Deadline Cloud 요금을 참조하세요.

서비스 관리형 플릿으로 자체 라이선스 사용

Deadline Cloud UBL(사용 기반 라이선스)을 사용하면 소프트웨어 공급업체와 별도의 라이선스 계약을 관리할 필요가 없습니다. 그러나 기존 라이선스가 있거나 UBL을 통해 사용할 수 없는 소프트웨어를 사용해야 하는 경우 Deadline Cloud 서비스 관리형 플릿에서 자체 소프트웨어 라이선스를 사용할 수 있습니다. 인터넷을 통해 SMF를 소프트웨어 라이선스 서버에 연결하여 플릿의 각 작업자에 대한 라이선스를 확인합니다.

프록시를 사용하여 라이선스 서버에 연결하는 예제는 Deadline Cloud 개발자 안내서의 서비스 관리형 플릿을 사용자 지정 라이선스 서버에 연결을 참조하세요.

VFX Reference Platform 호환성

VFX Reference Platform는 VFX 산업의 공통 대상 플랫폼입니다. Amazon Linux 2023을 실행하는 표준 서비스 관리형 플릿 Amazon EC2 인스턴스를를 지원하는 소프트웨어와 함께 사용하려면 서비스 관리형 플릿을 사용할 때 다음 사항을 고려해야 VFX Reference Platform합니다.

VFX Reference Platform는 매년 업데이트됩니다. Deadline Cloud 서비스 관리형 플릿을 포함한 AL2023 사용에 대한 이러한 고려 사항은 2022년부터 2024년까지의 역년(CY) 참조 플랫폼을 기반으로 합니다. 자세한 내용은 VFX Reference Platform 단원을 참조하십시오.

> **Note**
>
> 고객 관리형 플릿에 대한 사용자 지정Amazon Machine Image(AMI)을 생성하는 경우 Amazon EC2 인스턴스를 준비할 때 이러한 요구 사항을 추가할 수 있습니다.

AL2023 Amazon EC2 인스턴스에서 VFX Reference Platform 지원되는 소프트웨어를 사용하려면 다음을 고려하세요.

- AL2023과 함께 설치된 glibc 버전은 런타임 사용에 호환되지만 VFX Reference PlatformCY2024 이하와 호환되는 소프트웨어를 빌드하는 데는 호환되지 않습니다.
- Python 3.9 및 3.11은 서비스 관리형 플릿과 함께 제공되므로 VFX Reference Platform CY2022 및 CY2024와 호환됩니다. Python 3.7 및 3.10은 서비스 관리형 플릿에서 제공되지 않습니다. 필요한 소프트웨어는 대기열 또는 작업 환경에 Python 설치를 제공해야 합니다.
- 서비스 관리형 플릿에 제공된 일부 Boost 라이브러리 구성 요소는 버전 1.75이며와 호환되지 않습니다VFX Reference Platform. 애플리케이션에서 Boost를 사용하는 경우 호환성을 위해 자체 버전의 라이브러리를 제공해야 합니다.
- Intel TBB 업데이트 3은 서비스 관리형 플릿에서 제공됩니다. 이는 VFX Reference Platform CY2022, CY2023 및 CY2024와 호환됩니다.
- 에서 지정한 버전이 있는 다른 라이브러리VFX Reference Platform는 서비스 관리형 플릿에서 제공하지 않습니다. 서비스 관리형 플릿에서 사용되는 모든 애플리케이션을 라이브러리에 제공해야 합니다. 라이브러리 목록은 참조 플랫폼을 참조하세요.

고객 관리형 플릿

관리하는 작업자 플릿을 사용하려는 경우 Deadline Cloud가 작업을 처리하는 데 사용하는 고객 관리형 플릿(CMF)을 생성할 수 있습니다. 다음과 같은 경우 CMF를 사용합니다.

- Deadline Cloud와 통합할 기존 온프레미스 작업자가 있습니다.
- 공동 위치 데이터 센터에 작업자가 있습니다.
- Amazon Elastic Compute Cloud(Amazon EC2) 작업자를 직접 제어해야 합니다.

CMF를 사용하는 경우 플릿을 완전히 제어하고 책임을 집니다. 여기에는 플릿의 작업자 프로비저닝, 운영, 관리 및 폐기가 포함됩니다.

자세한 내용은 Deadline Cloud 개발자 안내서의 Deadline Cloud 고객 관리형 플릿 생성 및 사용을 참조하세요.

Deadline Cloud에서 사용자 관리

AWS Deadline Cloud는 AWS IAM Identity Center 를 사용하여 사용자 및 그룹을 관리합니다. IAM Identity Center는 엔터프라이즈 SSO(Single Sign On) 공급자와 통합할 수 있는 클라우드 기반 Single Sign-On 서비스입니다. 통합을 통해 사용자는 회사 계정으로 로그인할 수 있습니다.

Deadline Cloud는 기본적으로 IAM Identity Center를 활성화하며 Deadline Cloud를 설정하고 사용해야 합니다. 자세한 내용은 자격 증명 소스 관리를 참조하세요.

의 조직 소유자 AWS Organizations 는 Deadline Cloud 모니터에 액세스할 수 있는 사용자 및 그룹을 관리할 책임이 있습니다. IAM Identity Center 또는 Deadline Cloud 콘솔을 사용하여 이러한 사용자 및 그룹을 생성하고 관리할 수 있습니다. 자세한 내용은 AWS Organizations란 무엇인가요?를 참조하세요.

Deadline Cloud 콘솔을 사용하여 팜, 대기열 및 플릿을 관리할 수 있는 사용자 및 그룹을 생성하고 제거합니다. Deadline Cloud에 사용자를 추가할 때 액세스하기 전에 IAM Identity Center를 사용하여 암호를 재설정해야 합니다.

주제

- 모니터의 사용자 및 그룹 관리
- 팜, 대기열 및 플릿에 대한 사용자 및 그룹 관리

모니터의 사용자 및 그룹 관리

Organizations 소유자는 Deadline Cloud 콘솔을 사용하여 Deadline Cloud 모니터에 액세스할 수 있는 사용자 및 그룹을 관리할 수 있습니다. 기존 IAM Identity Center 사용자 및 그룹 중에서 선택하거나 콘솔에서 새 사용자 및 그룹을 추가할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다. 기본 페이지의 시작하기 섹션에서 기한 클라우드 설정 또는 대시보드로 이동을 선택합니다.
2. 왼쪽 탐색 창에서 사용자 관리를 선택합니다. 기본적으로 그룹 탭이 선택됩니다.

수행할 작업에 따라 그룹 탭 또는 사용자 탭을 선택합니다.

Groups

그룹 생성

1. 그룹 생성을 선택합니다.
2. 그룹 이름을 입력합니다. 이름은 IAM Identity Center 조직의 그룹 간에 고유해야 합니다.

그룹을 제거하려면

1. 제거할 그룹을 선택합니다.
2. 제거를 선택합니다.
3. 확인 대화 상자에서 그룹 제거를 선택합니다.

> **Note**
>
> IAM Identity Center에서 그룹을 제거하는 중입니다. 그룹 멤버는 더 이상 Deadline Cloud에 로그인하거나 팜 리소스에 액세스할 수 없습니다.

Users

사용자를 추가하려면

1. 사용자 탭을 선택합니다.
2. 사용자 추가를 선택합니다.
3. 새 사용자의 이름, 이메일 주소 및 사용자 이름을 입력합니다.
4. (선택 사항) 새 사용자를 추가할 IAM Identity Center 그룹을 하나 이상 선택합니다.
5. 초대 전송을 선택하여 새 사용자에게 IAM Identity Center 조직에 가입하기 위한 지침이 포함된 이메일을 보냅니다.

사용자를 제거하려면

1. 제거할 사용자를 선택합니다.
2. 제거를 선택합니다.
3. 확인 대화 상자에서 사용자 제거를 선택합니다.

> **Note**
> IAM Identity Center에서 사용자를 제거 중입니다. 사용자는 더 이상 Deadline Cloud 모니터에 로그인하거나 팜 리소스에 액세스할 수 없습니다.

팜, 대기열 및 플릿에 대한 사용자 및 그룹 관리

사용자 및 그룹 관리의 일환으로 다양한 수준에서 액세스 권한을 부여할 수 있습니다. 각 후속 수준에는 이전 수준에 대한 권한이 포함됩니다. 다음 목록은 가장 낮은 수준에서 가장 높은 수준까지 네 가지 액세스 수준을 설명합니다.

- 뷰어 - 액세스할 수 있는 팜, 대기열, 플릿 및 작업의 리소스를 볼 수 있는 권한입니다. 최종 사용자는 작업을 제출하거나 변경할 수 없습니다.
- 기여자 - 최종 사용자와 동일하지만 대기열 또는 팜에 작업을 제출할 수 있는 권한이 있습니다.
- 관리자 - 기고자와 동일하지만 액세스 권한이 있는 대기열에서 작업을 편집하고 액세스 권한이 있는 리소스에 대한 권한을 부여합니다.
- 소유자 - 관리자와 동일하지만 예산을 보고 생성하고 사용량을 확인할 수 있습니다.

> **Note**
> 액세스 권한 변경은 시스템에 반영되는 데 최대 10분이 걸릴 수 있습니다.

1. 아직 로그인하지 않았다면에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 팜 및 기타 리소스를 선택합니다.
3. 관리할 팜을 선택합니다. 팜 이름을 선택하여 세부 정보 페이지를 엽니다. 검색 창을 사용하여 팜을 검색할 수 있습니다.
4. 대기열 또는 플릿을 관리하려면 대기열 또는 플릿 탭을 선택한 다음 관리할 대기열 또는 플릿을 선택합니다.
5. 액세스 관리 탭을 선택합니다. 기본적으로 그룹 탭이 선택됩니다. 사용자를 관리하려면 사용자를 선택합니다.

수행할 작업에 따라 그룹 탭 또는 사용자 탭을 선택합니다.

Groups

그룹을 추가하려면

1. 그룹 토글을 선택합니다.
2. 그룹 추가를 선택합니다.
3. 드롭다운에서 추가할 그룹을 선택합니다.
4. 그룹 액세스 수준에서 다음 옵션 중 하나를 선택합니다.
   - 최종 사용자
   - 기고자
   - Manager
   - 소유자
5. 추가를 선택합니다.

그룹을 제거하려면

1. 제거할 그룹을 선택합니다.
2. 제거를 선택합니다.
3. 확인 대화 상자에서 그룹 제거를 선택합니다.

Users

사용자를 추가하려면

1. 사용자를 추가하려면 사용자 추가를 선택합니다.
2. 드롭다운에서 추가할 사용자를 선택합니다.
3. 사용자 액세스 수준에서 다음 옵션 중 하나를 선택합니다.
   - 최종 사용자
   - 기고자
   - Manager
   - 소유자

4. 추가를 선택합니다.

사용자를 제거하려면

1. 제거할 사용자를 선택합니다.
2. 제거를 선택합니다.
3. 확인 대화 상자에서 사용자 제거를 선택합니다.

Deadline Cloud 작업

작업은 AWS Deadline Cloud가 사용 가능한 작업자에 대한 작업을 예약하고 실행하는 데 사용하는 일련의 지침입니다. 작업을 생성할 때 작업을 보낼 팜과 대기열을 선택합니다.

제출자는 DCC 애플리케이션의 인터페이스에서 작업 생성을 관리하는 디지털 콘텐츠 생성(DCC) 애플리케이션을 위한 플러그인입니다. 작업을 생성한 후 제출자를 사용하여 처리를 위해 Deadline Cloud로 전송합니다.

제출자는 작업을 설명하는 Open Job Specification(OpenJD) 템플릿을 생성합니다. 동시에 Amazon Simple Storage Service(Amazon S3) 버킷에 자산 파일을 업로드합니다. 업로드 시간을 줄이기 위해 제출자는 Amazon S3에 마지막으로 업로드한 이후 변경된 파일만 전송합니다.

다음과 같은 방법으로 작업을 생성할 수도 있습니다.

- 터미널에서 - 명령줄을 사용하여 편안하게 작업을 제출하는 사용자의 경우.
- 스크립트에서 - 워크로드를 사용자 지정하고 자동화합니다.
- 애플리케이션에서 - 사용자의 작업이 애플리케이션에 있는 경우 또는 애플리케이션의 컨텍스트가 중요한 경우.

자세한 내용은 Deadline Cloud 개발자 안내서의 Deadline Cloud에 작업을 제출하는 방법을 참조하세요.

작업은 다음으로 구성됩니다.

- 우선순위 - Deadline Cloud가 대기열에서 작업을 처리하는 대략적인 순서입니다. 작업 우선 순위를 0에서 100 사이로 설정할 수 있으며, 일반적으로 우선 순위가 높은 작업이 먼저 처리됩니다. 우선 순위가 동일한 작업은 수신된 순서대로 처리됩니다.
- 단계 - 작업자에 대해 실행할 스크립트를 정의합니다. 단계에는 최소 작업자 메모리 또는 먼저 완료해야 하는 기타 단계와 같은 요구 사항이 있을 수 있습니다. 각 단계에는 하나 이상의 작업이 있습니다.
- 작업 - 작업자가 수행할 작업 단위입니다. 작업은 스크립트에 사용되는 프레임 번호와 같은 단계의 스크립트와 파라미터의 조합입니다. 모든 단계에 대해 모든 작업이 완료되면 작업이 완료됩니다.
- 환경 - 여러 단계 또는 작업에서 공유하는 지침을 설정하고 해제합니다.

Deadline Cloud 제출자 사용

제출자는 렌더 작업을 Deadline Cloud로 직접 보낼 수 있도록 디지털 콘텐츠 생성과 통합되는 도구입니다. 이 통합을 통해 애플리케이션 간에 전환하거나 파일을 수동으로 전송할 필요가 없으므로 워크플로가 간소화됩니다. 이렇게 하면 시간을 절약하고 오류 가능성을 줄일 수 있습니다.

제출자는 널리 사용되는 많은 DCC 애플리케이션에서 사용할 수 있습니다. 제출자를 설치하면는 일반적으로 렌더링 설정 또는 내보내기 메뉴에서 애플리케이션의 인터페이스에 Deadline Cloud 관련 옵션을 추가합니다.

Deadline Cloud 제출자를 사용하면 다음을 수행할 수 있습니다.

- 익숙한 DCC 환경에서 렌더링 작업 파라미터 구성
- 애플리케이션을 떠나지 않고 Deadline Cloud에 작업 제출
- 수동 파일 전송과 관련된 오류 가능성 감소
- 애플리케이션 간에 전환할 필요가 없으므로 시간 절약

DCC 애플리케이션의 제출자를 찾으려면 지원되는 제출자 목록을 확인하세요. 그런 다음의 지침에 따라 제출자를 Deadline Cloud 제출자 설정 설치합니다.

애플리케이션에 지원되는 제출자가 없는 경우에도 애플리케이션에 대한 작업을 실행할 수 있습니다. 샘플 작업 번들을 사용할 수 있거나 애플리케이션의 렌더링 CLI 명령에 대한 간단한 제출자를 구성할 수 있습니다. 자세한 내용은 Deadline Cloud 개발자 안내서의 Deadline Cloud에 대한 Open Job Description(OpenJD) 템플릿을 참조하세요.

이 주제의 예제에서는 Blender 제출자를 사용하지만 다른 제출자를 사용하는 단계는 비슷합니다.

> **Note**
> 제출자를 사용하려면 Deadline Cloud 모니터에 로그인해야 합니다.

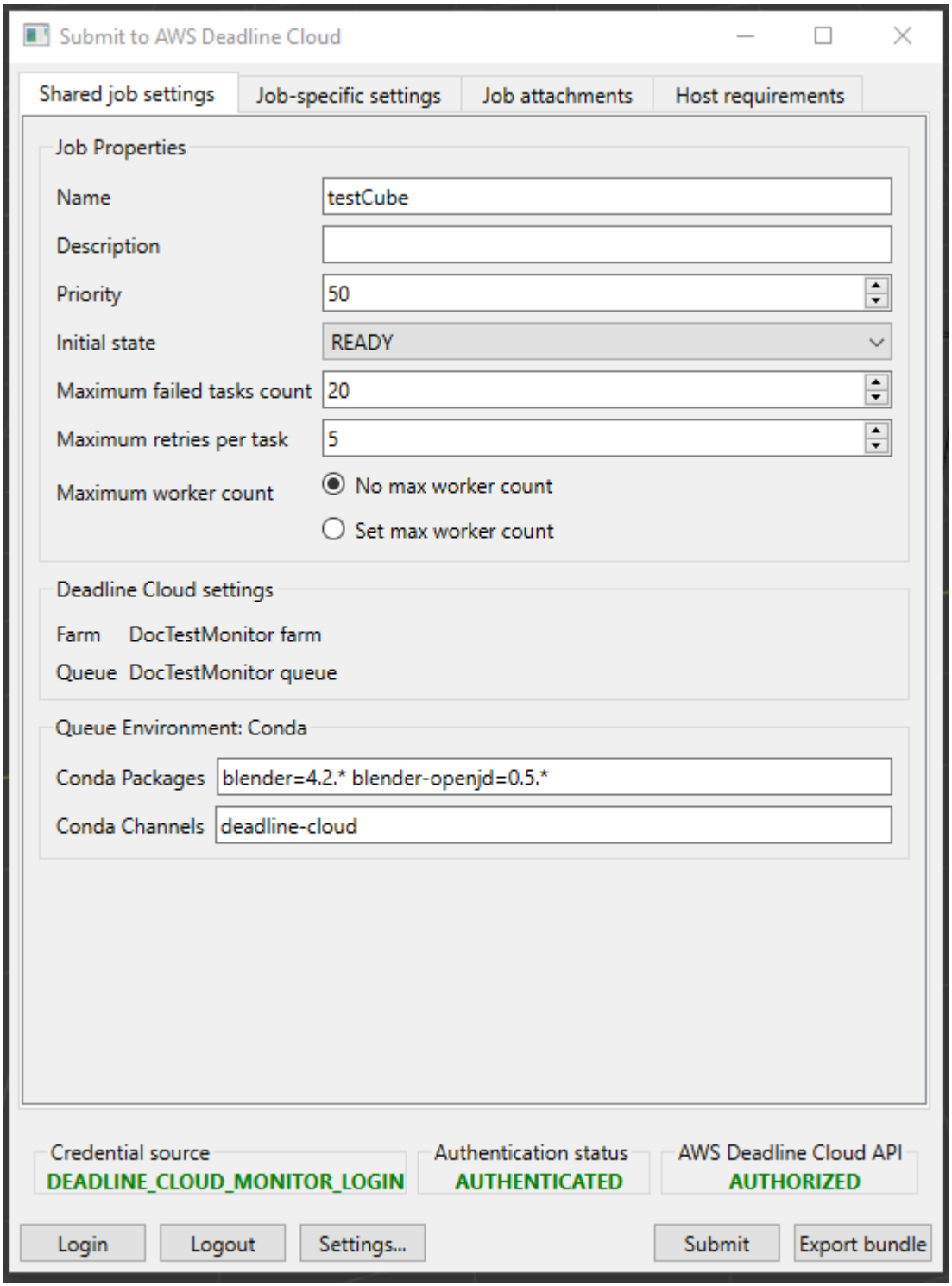
제출자에는 4개의 탭이 있습니다.

주제

- 공유 작업 설정 탭
- 작업별 설정 탭

- 작업 첨부 파일 탭
- 호스트 요구 사항 탭

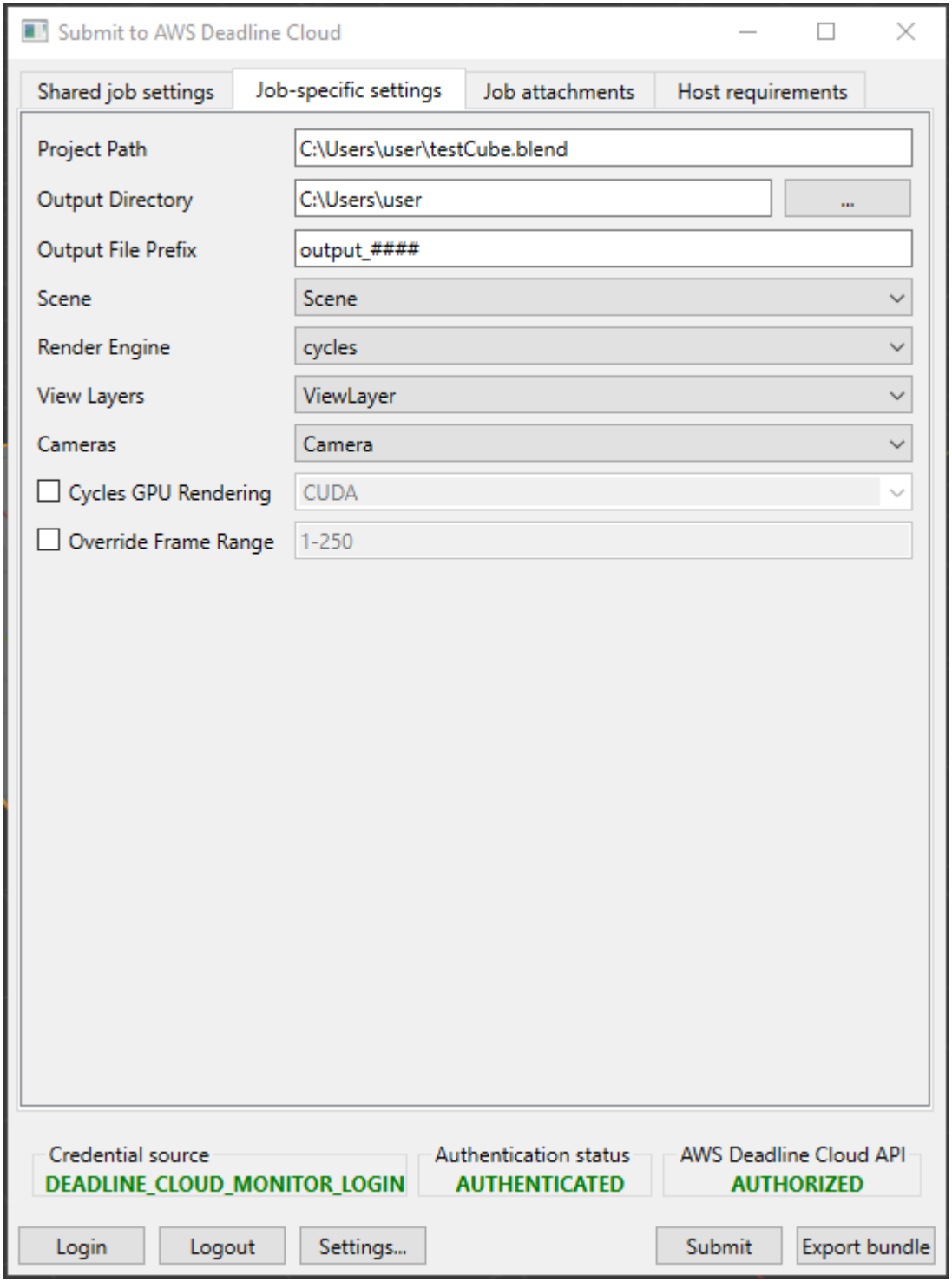
공유 작업 설정 탭



공유 작업 설정 탭에는 제출자를 사용하여 Deadline Cloud로 전송된 모든 작업에 공통적인 설정이 포함되어 있습니다. 세 섹션은 다음과 같습니다.

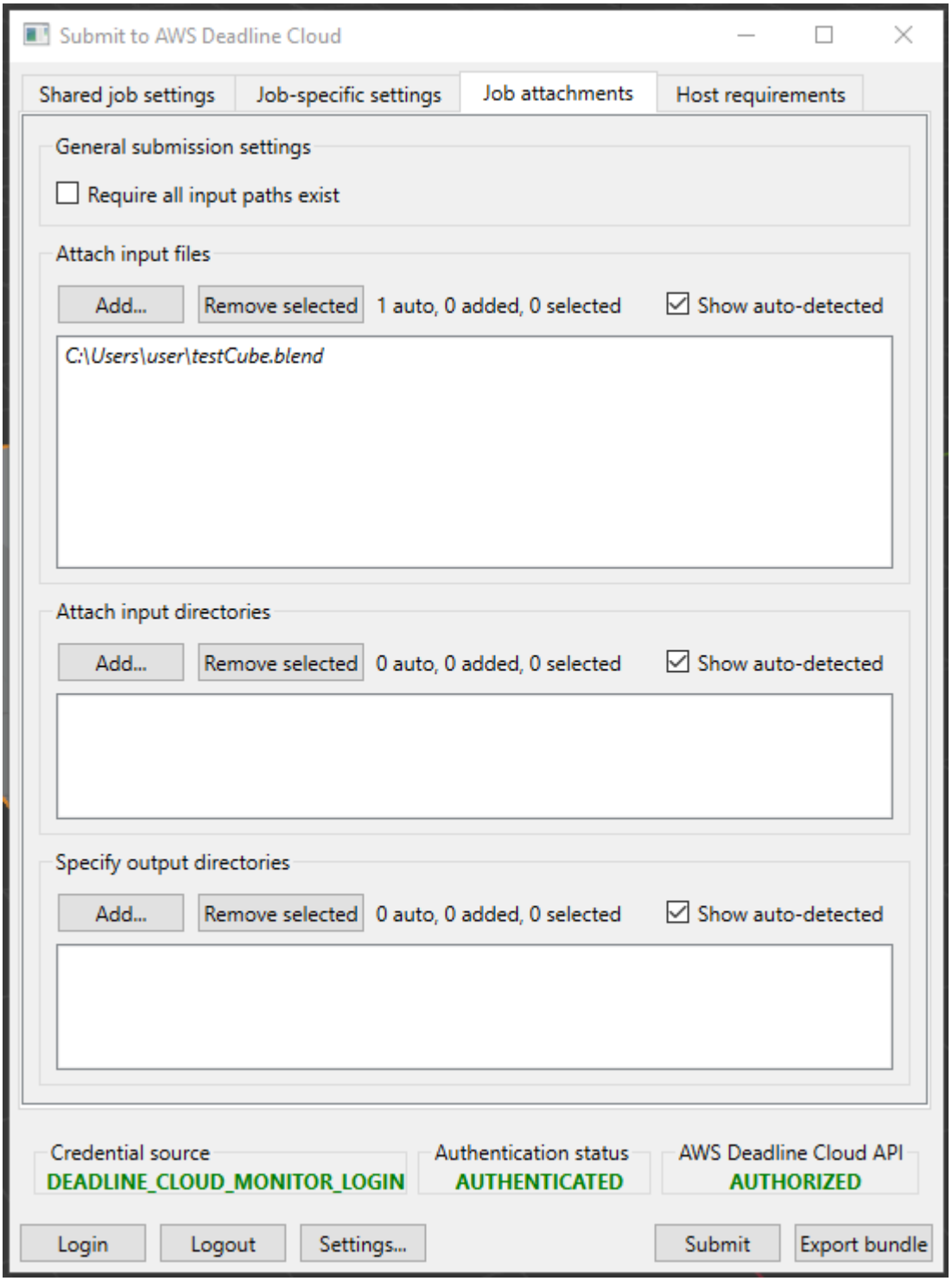
- 작업 속성 - 작업의 전체 속성을 설정합니다. 이러한 속성은 모든 DCC 애플리케이션의 제출자에 있습니다.
- 기한 클라우드 설정 - 작업이 전송되는 팜과 대기열을 표시합니다. 팜과 대기열을 변경하려면 제출자 하단에 있는 설정... 버튼을 사용합니다.
- 대기열 환경 - 대기열 환경에 정의된 파라미터 값을 설정합니다. Deadline Cloud는 DCC 애플리케이션의 기본 파라미터 값을 추가하며, 필요한 경우 값을 추가할 수 있습니다.

작업별 설정 탭



작업별 설정 탭에는 DCC 애플리케이션별 설정이 포함되어 있습니다. 애플리케이션에서 사용할 수 있는 옵션을 기반으로 이러한 설정을 지정합니다.

작업 첨부 파일 탭

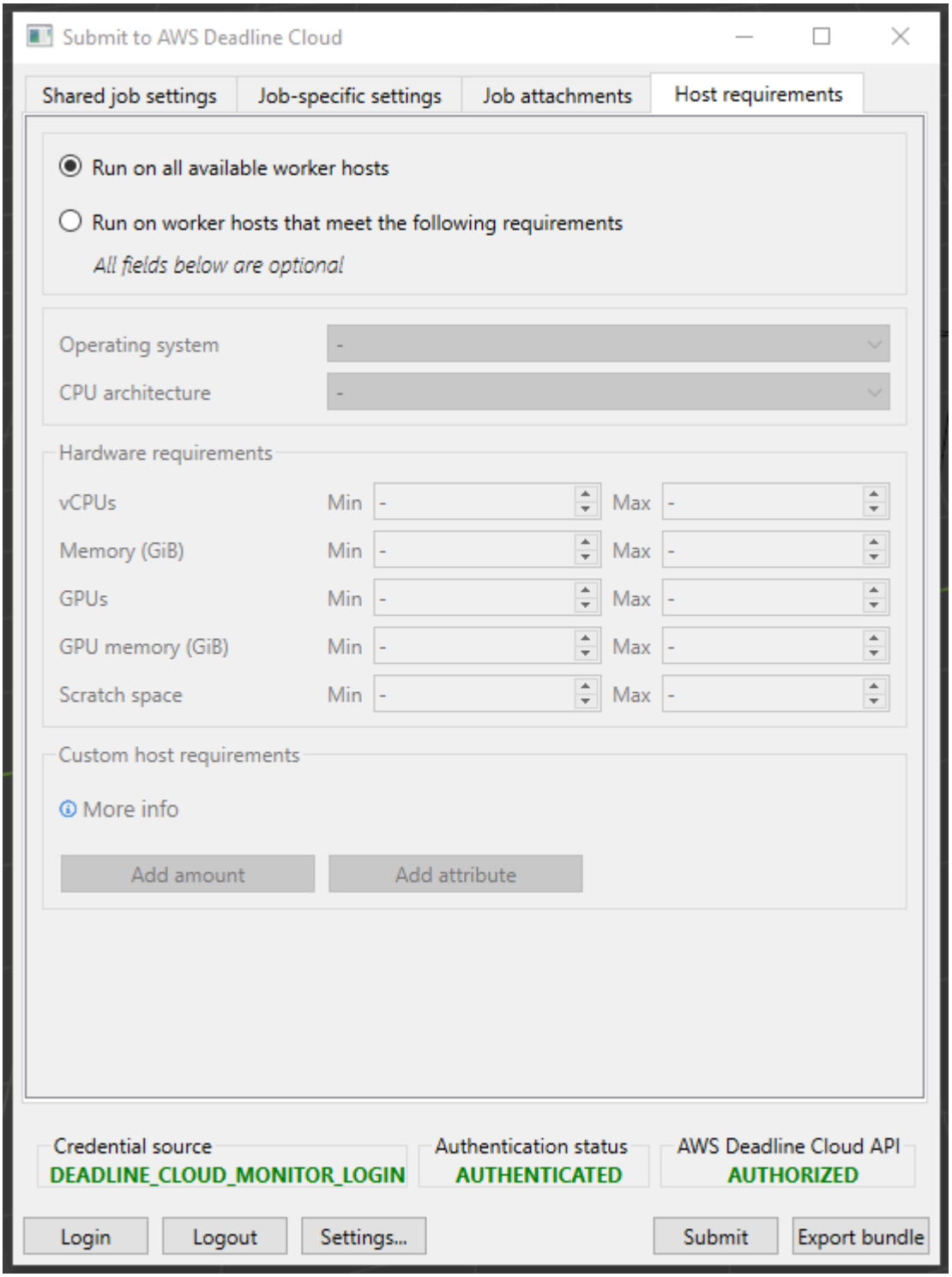


작업 첨부 파일 탭에는 렌더링을 완료하는 데 필요한 모든 파일이 표시됩니다. 제출자는 렌더링에 필요한 모든 파일을 찾으려고 합니다. 식별되는 파일은 목록에 기울임꼴로 표시됩니다.

자동으로 감지되지 않은 렌더링에 필요한 다른 자산이 포함된 추가 입력 파일 및 디렉터리를 추가할 수 있습니다.

작업이 여러 출력 디렉터리에 파일을 쓰는 경우가 작업 다운로드의 일부가 되도록 여기에 디렉터리를 지정해야 합니다.

호스트 요구 사항 탭



호스트 요구 사항 탭은 작업을 처리하는 데 필요한 플릿 기능을 설정합니다. 기능은 플릿의 개별 작업자가 아닌 전체 플릿에 대해 지정됩니다.

대기열에 연결된 리소스 제한이 있는 경우 금액 추가 버튼을 사용하여 제한을 지정합니다. 자세한 내용은 작업에 대한 리소스 제한 생성을 참조하세요.

Deadline Cloud 작업 처리

작업이 대기열에 들어가면 Deadline Cloud는 대기열과 연결된 하나 이상의 플릿에서 작업을 예약합니다. 플릿은 플릿에 대해 구성된 기능과 특정 단계의 호스트 요구 사항에 따라 선택됩니다. 작업에 대기열과 연결된 플릿이 충족할 수 없는 요구 사항이 있는 경우 작업의 상태는 "호환되지 않음"으로 설정되고 작업의 나머지 단계는 취소됩니다.

다음으로 Deadline Cloud는 작업자에게 단계에 대한 세션을 설정하라는 지침을 보냅니다. 작업을 실행하려면 작업자 인스턴스에서 단계에 필요한 소프트웨어를 사용할 수 있어야 합니다. 플릿 조정 설정이 허용하는 경우 서비스는 여러 작업자에 대한 세션을 엽니다.

Amazon Machine Image (AMI)에서 소프트웨어를 설정하거나 작업자가 런타임에 리포지토리 또는 패키지 관리자에서 소프트웨어를 로드할 수 있습니다. 대기열, 작업 또는 단계 환경을 사용하여 원하는 소프트웨어를 배포할 수 있습니다.

Deadline Cloud 서비스는 OpenJD 템플릿을 사용하여 작업에 필요한 단계와 각 단계에 필요한 작업을 식별합니다. 일부 단계는 다른 단계에 종속되므로 Deadline Cloud는 단계를 완료하는 순서를 결정합니다. 그런 다음 Deadline Cloud는 각 단계의 작업을 작업자에게 전송하여 처리합니다. 작업이 완료되면 서비스가 동일한 세션에서 다른 작업을 보내거나 작업자가 새 세션을 시작할 수 있습니다.

각 단계의 모든 작업이 완료되면 작업이 완료되고 출력을 워크스테이션에 다운로드할 준비가 된 것입니다. 작업이 완료되지 않았더라도 완료된 각 단계 및 작업의 출력을 다운로드할 수 있습니다.

> **Note**
>
> Deadline Cloud는 작업이 제출된 후 120일이 지나면 제거합니다. 작업이 제거되면 작업과 연결된 모든 단계와 작업도 제거됩니다. 작업을 다시 실행해야 하는 경우 작업에 대한 OpenJD 템플릿을 다시 제출합니다.

Deadline Cloud 작업 모니터링

AWS Deadline Cloud 모니터는 작업에 대한 전체 보기를 제공합니다. 이를 사용하여 다음을 수행할 수 있습니다.

- 작업 모니터링 및 관리

- 플릿에서 작업자 활동 보기
- 예산 및 사용량 추적
- 작업 결과를 다운로드합니다.

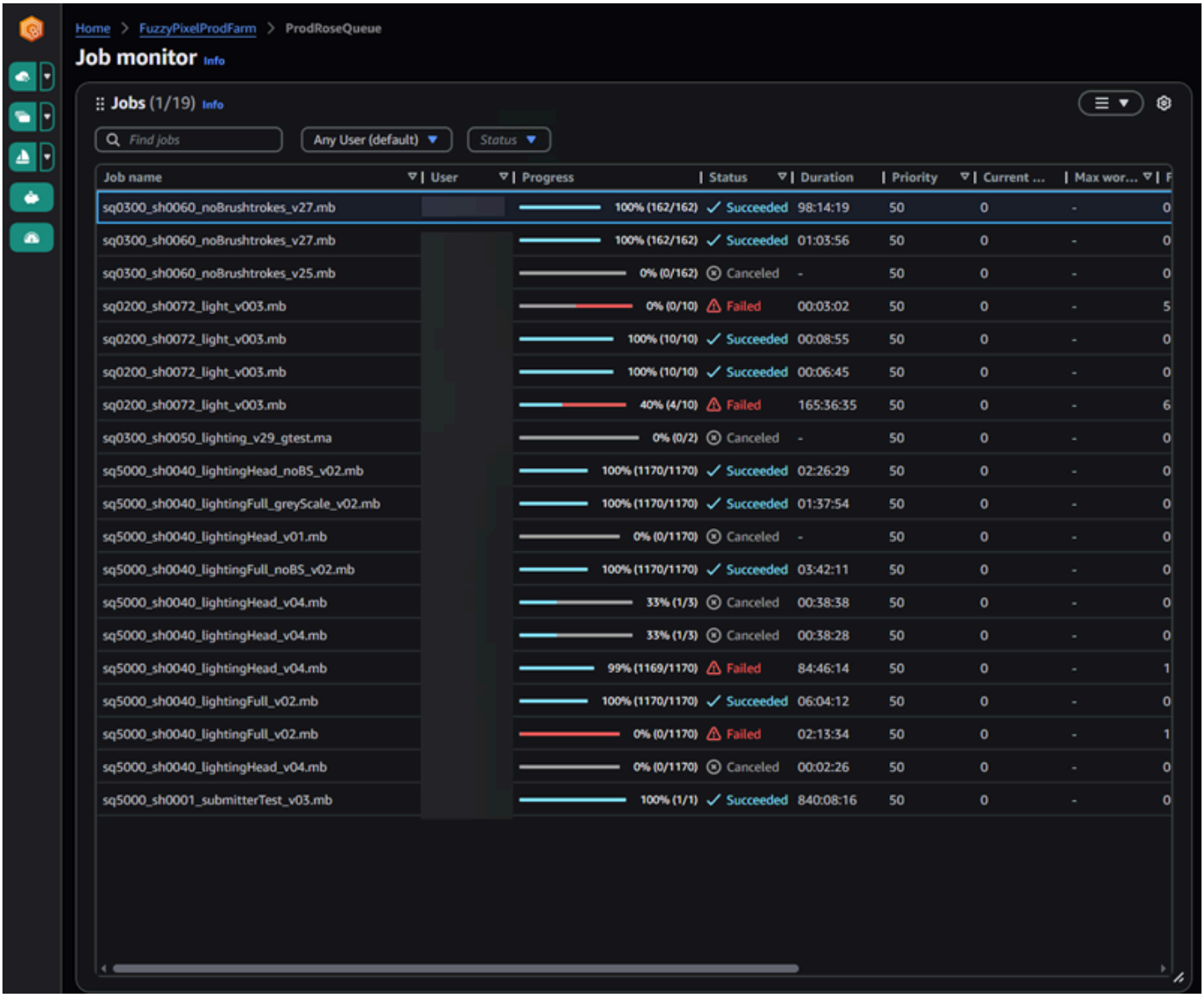
특정 작업을 모니터링하려면 작업이 포함된 팜과 대기열을 선택한 다음 목록에서 작업을 선택합니다. 검색 상자를 사용하여 대기열에서 특정 작업을 찾을 수 있습니다.

작업, 단계 또는 작업을 마우스 오른쪽 버튼으로 클릭하여 항목에 대한 옵션을 확인합니다. 다음을 할 수 있습니다.

- 상태 변경
- 항목 일시 중지 및 재개
- 항목 대기열 재지정
- 출력 다운로드
- 작업의 경우: 작업 및 작업자 로그를 봅니다.

자세한 내용은 Deadline Cloud 모니터 사용 단원을 참조하십시오.

작업 또는 단계의 각 작업에는 상태가 있습니다. 작업 또는 단계의 상태는 해당 작업의 상태에 따라 달라집니다. 상태는 이러한 상태가 있는 태스크에 따라 순서대로 결정됩니다. 단계 상태는 작업 상태와 동일하게 결정됩니다.



다음 목록은 상태를 설명합니다.

`NOT_COMPATIBLE`

작업의 작업 중 하나를 완료할 수 있는 플릿이 없으므로 작업이 팜과 호환되지 않습니다.

`RUNNING`

하나 이상의 작업자가 작업에서 작업을 실행하고 있습니다. 실행 중인 작업이 하나 이상 있는 한 작업은 로 표시됩니다`RUNNING`.

`ASSIGNED`

한 명 이상의 작업자에게 다음 작업으로 작업의 작업이 할당됩니다. 환경이 설정된 경우

`STARTING`

하나 이상의 작업자가 작업 실행을 위한 환경을 설정하고 있습니다.

`SCHEDULED`

작업에 대한 작업은 한 명 이상의 작업자에 대해 작업자의 다음 작업으로 예약됩니다.

`READY`

작업에 대해 하나 이상의 작업을 처리할 준비가 되었습니다.

`INTERRUPTING`

작업에서 하나 이상의 작업이 중단되고 있습니다. 작업 상태를 수동으로 업데이트할 때 중단이 발생할 수 있습니다. Amazon Elastic Compute Cloud(Amazon EC2) 스팟 가격 변경으로 인한 중단에 대한 응답으로 발생할 수도 있습니다.

`FAILED`

작업에서 하나 이상의 작업이 성공적으로 완료되지 않았습니다.

`CANCELED`

작업에서 하나 이상의 작업이 취소되었습니다.

`SUSPENDED`

작업에서 하나 이상의 작업이 일시 중지되었습니다.

`PENDING`

작업의 작업이 다른 리소스의 가용성을 기다리고 있습니다.

`SUCCEEDED`

작업의 모든 작업이 성공적으로 처리되었습니다.

Deadline Cloud용 파일 스토리지

작업자는 작업을 처리하는 데 필요한 입력 파일이 포함된 스토리지 위치와 출력을 저장하는 위치에 액세스할 수 있어야 합니다. AWS Deadline Cloud는 스토리지 위치에 대한 두 가지 옵션을 제공합니다.

- Deadline Cloud는 작업 연결을 통해 워크스테이션과 Deadline Cloud 작업자 간에 작업에 대한 입력 및 출력 파일을 주고받습니다. 파일 전송을 활성화하기 위해 Deadline Cloud는에서 Amazon Simple Storage Service(Amazon S3) 버킷을 사용합니다 AWS 계정.

  서비스 관리형 플릿과 함께 작업 연결을 사용하는 경우 가상 프라이빗 네트워크(VPN)에서 가상 파일 시스템(VFS)을 설정할 수 있습니다. 그런 다음 작업자는 필요한 경우에만 파일을 로드할 수 있습니다.
- 공유 스토리지에서는 운영 체제와의 파일 공유를 사용하여 파일에 대한 액세스를 제공합니다.

  교차 플랫폼 공유 스토리지를 사용하는 경우 작업자가 두 운영 체제 간의 파일에 경로를 매핑할 수 있도록 스토리지 프로파일을 생성할 수 있습니다.

주제

- Deadline Cloud의 작업 첨부 파일

Deadline Cloud의 작업 첨부 파일

작업 연결을 사용하면 워크스테이션과 AWS Deadline Cloud 간에 파일을 주고받을 수 있습니다. 작업 첨부 파일을 사용하면 파일에 대해 Amazon S3 버킷을 수동으로 설정할 필요가 없습니다. 대신 Deadline Cloud 콘솔을 사용하여 대기열을 생성할 때 작업 첨부 파일의 버킷을 선택합니다.

Deadline Cloud에 작업을 처음 제출하면 작업에 대한 모든 파일이 Deadline Cloud로 전송됩니다. 후속 제출의 경우 변경된 파일만 전송되어 시간과 대역폭이 모두 절약됩니다.

처리가 완료되면 작업 세부 정보 페이지에서 또는 Deadline Cloud CLI `deadline job download-output` 명령을 사용하여 결과를 다운로드할 수 있습니다.

여러 대기열에 동일한 S3 버킷을 사용할 수 있습니다. 각 대기열에 대해 다른 루트 접두사를 설정하여 버킷에 첨부 파일을 구성합니다.

콘솔을 사용하여 대기열을 생성할 때 기존 AWS Identity and Access Management (IAM) 역할을 선택하거나 콘솔에서 새 역할을 생성하도록 할 수 있습니다. 콘솔이 역할을 생성하면 대기열에 지정된 버킷

에 액세스할 수 있는 권한을 설정합니다. 기존 역할을 선택하는 경우 역할에게 S3 버킷에 액세스할 수 있는 권한을 부여해야 합니다.

작업 연결 S3 버킷에 대한 암호화

작업 연결 파일은 기본적으로 S3 버킷에서 암호화됩니다. 이렇게 하면 무단 액세스로부터 정보를 보호할 수 있습니다. Deadline Cloud에서 제공하는 키로 파일을 암호화하기 위해 아무 작업도 수행할 필요가 없습니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3, 이제 모든 새 객체 자동 암호화를 참조하세요.

자체 고객 관리형 AWS Key Management Service 키를 사용하여 작업 첨부 파일이 포함된 S3 버킷을 암호화할 수 있습니다. 이렇게 하려면 버킷과 연결된 대기열의 IAM 역할을 수정하여에 대한 액세스를 허용해야 합니다 AWS KMS key.

대기열 역할에 대한 IAM 정책 편집기를 열려면

1. 에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다. 기본 페이지의 시작하기 섹션에서 팜 보기를 선택합니다.
2. 팜 목록에서 수정할 대기열이 포함된 팜을 선택합니다.
3. 대기열 목록에서 수정할 대기열을 선택합니다.
4. 대기열 세부 정보 섹션에서 서비스 역할을 선택하여 서비스 역할에 대한 IAM 콘솔을 엽니다.

그런 다음 다음 절차를 완료합니다.

에 대한 권한으로 역할 정책을 업데이트하려면 AWS KMS

1. 권한 정책 목록에서 역할에 대한 정책을 선택합니다.
2. 이 정책에 정의된 권한 섹션에서 편집을 선택합니다.
3. 새 문 추가를 선택합니다.
4. 다음 정책을 복사하여 편집기에 붙여 넣습니다. *Region*, *accountID*및를 *keyID* 자체 값으로 변경합니다.

```
{
   "Effect": "Allow",
   "Action": [
       "kms:Decrypt",
       "kms:DescribeKey",
       "kms:GenerateDataKey"
```

```
    ],
    "Resource": [
        "arn:aws:kms:Region:accountID:key/keyID"
    ]
}
```

5. Next(다음)를 선택합니다.
6. 정책의 변경 사항을 검토한 다음 만족하면 변경 사항 저장을 선택합니다.

S3 버킷에서 작업 연결 관리

Deadline Cloud는 작업에 필요한 작업 연결 파일을 S3 버킷에 저장합니다. 이러한 파일은 시간이 지남에 따라 누적되어 Amazon S3 비용이 증가합니다. 비용을 절감하기 위해 S3 버킷에 S3 수명 주기 구성을 적용할 수 있습니다. 이 구성은 버킷의 파일을 자동으로 삭제할 수 있습니다. S3 버킷은 계정에 있으므로 언제든지 S3 수명 주기 구성을 수정하거나 제거할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 S3 수명 주기 구성 예제를 참조하세요. Amazon S3

보다 세분화된 S3 버킷 관리 솔루션을 위해 마지막으로 액세스한 시간을 기준으로 S3 버킷의 객체를 만료 AWS 계정 하도록를 설정할 수 있습니다. 자세한 내용은 아키텍처 블로그에서 마지막으로 액세스한 날짜를 기준으로 Amazon S3 객체 만료를 참조하여 비용을 절감하세요 AWS .

Deadline Cloud 가상 파일 시스템

AWS Deadline Cloud에서 작업 연결에 대한 가상 파일 시스템을 지원하면 작업자의 클라이언트 소프트웨어가 Amazon Simple Storage Service와 직접 통신할 수 있습니다. 작업자는 처리 전에 모든 파일을 다운로드하는 대신 필요한 경우에만 파일을 로드할 수 있습니다. 파일은 로컬에 저장됩니다. 이 접근 방식은 두 번 이상 사용된 자산을 다운로드하지 않도록 합니다. 작업이 완료되면 모든 파일이 제거됩니다.

- 가상 파일 시스템은 특정 작업 프로필에 대해 상당한 성능 향상을 제공합니다. 일반적으로 작업자 플릿이 더 많은 총 파일의 하위 집합이 더 작을수록 가장 큰 이점이 있습니다. 작업자 수가 적은 파일 수는 처리 시간이 거의 동일합니다.
- 가상 파일 시스템 지원은 서비스 관리형 플릿의 Linux 작업자만 사용할 수 있습니다.
- Deadline Cloud 가상 파일 시스템은 다음 작업을 지원하지만 POSIX를 준수하지 않습니다.
  - 파일 `create`, `delete`, `open`, `close`, `read`, `write`, `append`, `truncate`, `rename`, `copy`, `movefsync`, `stat`, 및 `falloc`
  - 디렉터리 `create`, `delete`, `rename`, `copy`, `move`및 `stat`

- 가상 파일 시스템은 작업이 대규모 데이터 세트의 일부에만 액세스할 때 데이터 전송을 줄이고 성능을 개선하도록 설계되었으며 모든 워크로드에 최적화되지 않았습니다. 프로덕션 작업을 실행하기 전에 워크로드를 테스트해야 합니다.

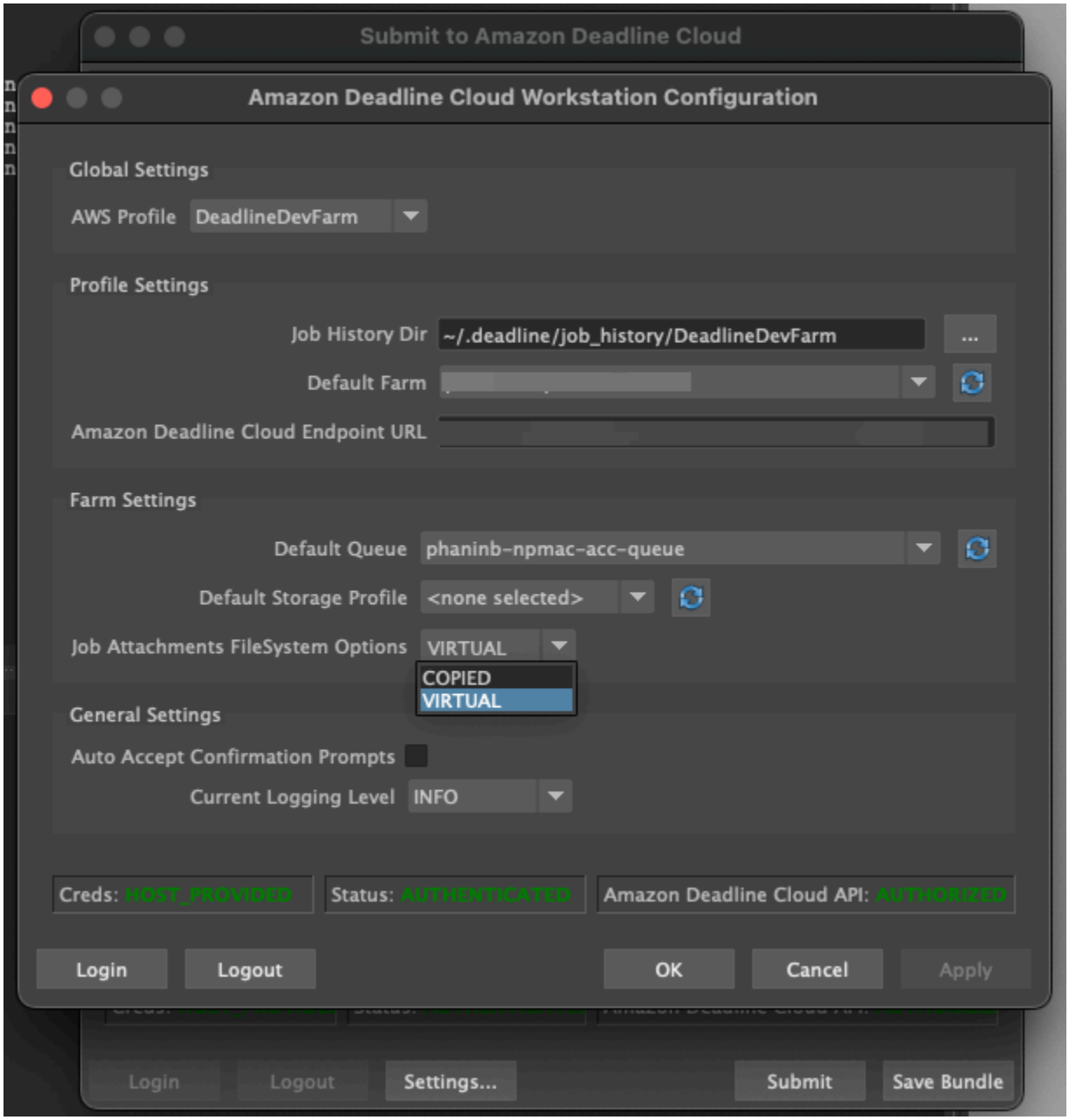
VFS 지원 활성화

각 작업에 대해 가상 파일 시스템 지원(VFS)이 활성화됩니다. 다음과 같은 경우 작업은 기본 작업 연결 프레임워크로 돌아갑니다.

- 작업자 인스턴스 프로필은 가상 파일 시스템을 지원하지 않습니다.
- 문제가 발생하여 가상 파일 시스템 프로세스가 시작되지 않습니다.
- 가상 파일 시스템은 탑재할 수 없습니다.

제출자를 사용하여 가상 파일 시스템 지원을 활성화하려면

1. 작업을 제출할 때 설정 버튼을 선택하여 AWS Deadline Cloud 워크스테이션 구성 패널을 엽니다.
2. 작업 첨부 파일 시스템 옵션 드롭다운에서 가상을 선택합니다.



3. 변경 사항을 저장하려면 확인을 선택합니다.

를 사용하여 가상 파일 시스템 지원을 활성화하려면 AWS CLI

- 저장된 작업을 제출할 때 다음 명령을 사용합니다.

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

가상 파일 시스템이 특정 작업에 대해 성공적으로 시작되었는지 확인하려면 Amazon CloudWatch Logs에서 로그를 검토합니다. 다음 메시지를 찾습니다.

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

로그에 다음 메시지가 포함된 경우 가상 파일 시스템 지원이 비활성화됩니다.

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

가상 파일 시스템 지원 문제 해결

Deadline Cloud 모니터를 사용하여 가상 파일 시스템의 로그를 볼 수 있습니다. 지침은 Deadline Cloud에서 세션 및 작업자 로그 보기 단원을 참조하십시오.

가상 파일 시스템 로그는 작업자 에이전트 출력과 공유된 대기열과 연결된 CloudWatch Logs 그룹으로도 전송됩니다.

Deadline Cloud 팜의 지출 및 사용량 추적

AWS Deadline Cloud 예산 관리자 및 사용량 탐색기는 비용 변수에 대해 사용 가능한 정보를 기반으로 Deadline Cloud 사용의 대략적인 비용을 제공하는 비용 관리 도구입니다. 비용 관리 도구는 Deadline Cloud 및 기타 AWS 서비스의 실제 사용에 대해 지불해야 하는 금액을 보장하지 않습니다.

Deadline Cloud의 비용을 관리하는 데 도움이 되도록 다음 기능을 사용할 수 있습니다.

- 예산 관리자 - Deadline Cloud 예산 관리자를 사용하면 프로젝트 비용을 관리하는 데 도움이 되는 예산을 생성하고 편집할 수 있습니다.
- 사용량 탐색기 - Deadline Cloud 사용량 탐색기를 사용하면 사용된 AWS 리소스 수와 해당 리소스의 예상 비용을 볼 수 있습니다.
- AWS 비용 할당 태그 - 비용 할당 태그를 사용하면 모든 AWS 서비스에 대한 세부 비용을 추적할 수 있습니다. 자세한 내용은 비용 할당 태그를 사용하여 AWS 비용 구성 및 추적을 참조하세요.

비용 가정

Deadline Cloud 비용 관리 도구에서 사용하는 기본 계산은 다음과 같습니다.

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

- 런타임은 시작 시간부터 종료 시간까지의 작업 내 모든 작업의 합계입니다.
- 컴퓨팅 속도는 서비스 관리형 플릿의 AWS Deadline Cloud 요금에 따라 결정됩니다. 고객 관리형 플릿의 경우 컴퓨팅 속도는 작업자 시간당 1 USD로 추정됩니다.
- 라이선스 요금은 Deadline Cloud 기본 라이선스 가격에 따라 결정되며 서비스 관리형 플릿에만 사용할 수 있습니다. 추가 계층은 포함되지 않습니다. 라이선스 요금에 대한 자세한 내용은 AWS Deadline Cloud 요금을 참조하세요.

Deadline Cloud 비용 관리 도구의 예상 비용은 여러 가지 이유로 실제 비용과 다를 수 있습니다. 일반적인 이유는 다음과 같습니다.

- 고객 소유 리소스 및 요금. 온프레미스 AWS 또는 기타 클라우드 공급자로부터 또는 외부로 자체 리소스를 가져오도록 선택할 수 있습니다. 이러한 리소스의 실제 비용은 계산되지 않습니다.

- 유휴 작업자 비용. 유휴 작업자 비용은 작업자 상태가 IDLE인 경우 포함되지 않습니다. 이는 최소 인스턴스 수가 0보다 큰 플릿 또는 작업자가 작업 간에 전환할 때 발생할 수 있습니다. 유휴 작업자 비용은 계산에 포함되지 않습니다.
- 작업자 중지 및 시작 시간입니다. 작업자가 작업을 완료한 후 IDLE에서 STOPPING으로, STOPPING에서 STOPPED로 이동하는 비용은 Deadline Cloud 비용 추정치에 포함되지 않습니다.
- 프로모션 크레딧, 할인 및 사용자 지정 요금 계약. 비용 관리 도구는 프로모션 크레딧, 비공개 요금 계약 또는 기타 할인을 고려하지 않습니다. 견적에 포함되지 않은 다른 할인을 받을 수 있습니다.
- 자산 스토리지. 자산 스토리지는 비용 및 사용량 추정치에 포함되지 않습니다.
- price.offs의 변경 사항은 대부분의 서비스에 대해 pay-as-you-go제 요금을 제공합니다. AWS 요금은 시간이 지남에 따라 변경될 수 있습니다. 비용 관리 도구는 공개적으로 사용 가능한 up-to-date 가격을 사용하지만 변경 후 지연이 발생할 수 있습니다.
- 세금. 비용 관리 도구에는 서비스 구매에 적용되는 세금이 포함되지 않습니다.
- 반올림. 비용 관리 도구는 요금 데이터의 수학적 반올림을 수행합니다.
- 통화. 예상 비용은 미국 달러로 계산됩니다. 글로벌 환율은 시간이 지남에 따라 달라집니다. 견적을 현재 환율을 기반으로 다른 통화로 변환하면 환율의 변화가 견적에 영향을 미칩니다.
- 외부 라이선스. 사전 구매한 라이선스(서비스 관리형 플릿에 대한 소프트웨어 라이선스)를 사용하기로 선택한 경우 Deadline Cloud 비용 관리 도구는이 비용을 처리할 수 없습니다.

예산으로 비용 제어

Deadline Cloud 예산 관리자는 대기열, 플릿 또는 팜과 같은 지정된 리소스에 대한 지출을 제어하는 데 도움이 됩니다. 예산 금액 및 한도를 생성하고 자동 작업을 설정하여 예산에 대한 추가 지출을 줄이거나 중지할 수 있습니다.

다음 섹션에서는 Deadline Cloud 예산 관리자를 사용하는 단계를 제공합니다.

주제

- 전제 조건
- Deadline Cloud 예산 관리자 열기
- Deadline Cloud 대기열에 대한 예산 생성
- Deadline Cloud 대기열 예산 보기
- Deadline Cloud 대기열에 대한 예산 편집
- Deadline Cloud 대기열에 대한 예산 비활성화

- EventBridge 이벤트를 사용하여 예산 모니터링

전제 조건

Deadline Cloud 예산 관리자를 사용하려면 OWNER 액세스 수준이 있어야 합니다. OWNER 권한을 부여하려면의 단계를 따릅니다Deadline Cloud에서 사용자 관리.

Deadline Cloud 예산 관리자 열기

Deadline Cloud 예산 관리자를 열려면 다음 절차를 사용합니다.

1. 에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 팜 보기를 선택합니다.
3. 정보를 가져오려는 팜을 찾은 다음 작업 관리를 선택합니다.
4. 기한 클라우드 모니터의 왼쪽 탐색 창에서 예산을 선택합니다.

예산 관리자 요약 페이지에는 활성 예산과 비활성 예산의 목록이 모두 표시됩니다.

- 활성 예산은 선택한 리소스(대기열)를 기준으로 추적됩니다.
- 비활성 예산이 만료되었거나 사용자가 취소했으며,이 예산의 한도에 대한 비용을 더 이상 추적하지 않습니다.

예산을 선택하면 예산 요약 페이지에 예산에 대한 기본 정보가 포함됩니다. 제공된 정보에는 예산 이름, 상태, 리소스, 남은 비율, 남은 금액, 총 예산, 시작 날짜 및 종료 날짜가 포함됩니다.

Deadline Cloud 대기열에 대한 예산 생성

예산을 생성하려면 다음 절차를 사용합니다.

1. 아직 로그인하지 않은 경우에 로그인하고, Deadline Cloud 콘솔을 AWS Management Console열고, 팜을 선택한 다음 작업 관리를 선택합니다.
2. 예산 관리자 페이지에서 예산 생성을 선택합니다.
3. 세부 정보 섹션에 예산의 예산 이름을 입력합니다.
4. (선택 사항) 설명 필드에 예산에 대한 간략한 설명을 입력합니다.
5. 리소스에서 대기열 드롭다운을 사용하여 예산을 생성할 대기열을 선택합니다.
6. 기간의 경우 다음 단계를 완료하여 예산의 시작 및 종료 날짜를 설정합니다.

a. 시작 날짜에 예산 추적의 첫 번째 날짜를 YYYY/MM/DD 형식으로 입력하거나 달력 아이콘을 선택하고 날짜를 선택합니다.

   기본 시작 날짜는 예산이 생성된 날짜입니다.

b. 종료 날짜에 예산 추적의 마지막 날짜를 YYYY/MM/DD 형식으로 입력하거나 달력 아이콘을 선택하고 날짜를 선택합니다.

   기본 종료일은 시작 날짜로부터 120일입니다.

7. 예산 금액에 예산의 달러 금액을 입력합니다.
8. (선택 사항) 제한 알림을 생성하는 것이 좋습니다. 작업 제한 섹션에서 특정 금액이 예산에 남아 있을 때 발생하는 자동화된 작업을 구현할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

   a. 새 작업 추가를 선택합니다.
   b. 남은 금액에 작업을 시작하려는 달러 금액을 입력합니다.
   c. 작업 드롭다운에서 원하는 작업을 선택합니다. 작업은 다음과 같습니다.

      - 현재 작업 완료 후 중지 - 임계값 양이 충족될 때 현재 실행 중인 모든 작업은 완료될 때까지 계속 실행됩니다(비용 발생).
      - 즉시 작업 중지 - 임계값 양이 충족되면 모든 작업이 즉시 취소됩니다.

   d. 추가 제한 알림을 생성하려면 새 작업 추가를 선택하고 이전 단계를 반복합니다.
9. 예산 생성을 선택합니다.

Deadline Cloud 대기열 예산 보기

예산을 생성한 후 예산 관리자 페이지에서 예산을 볼 수 있습니다. 여기에서 예산의 총 금액과 특정 예산에 할당된 전체 비용을 볼 수 있습니다.

예산을 보려면 다음 절차를 사용합니다.

1. 아직 로그인하지 않은 경우에 로그인하고, Deadline Cloud 콘솔을 AWS Management Console열고, 팜을 선택한 다음 작업 관리를 선택합니다.
2. 왼쪽 탐색 창에서 예산을 선택합니다. Budget Manager 페이지가 나타납니다.
3. 활성 예산을 보려면 활성 예산 탭을 선택하고 보려는 예산의 이름을 선택합니다. 예산 세부 정보 페이지가 나타납니다.
4. 만료된 예산에 대한 예산 세부 정보를 보려면 비활성 예산 탭을 선택합니다. 그런 다음 보려는 예산의 이름을 선택합니다. 예산 세부 정보 페이지가 나타납니다.

Deadline Cloud 대기열에 대한 예산 편집

활성 예산을 편집할 수 있습니다. 활성 예산을 편집하려면 다음 절차를 사용합니다.

1. 아직 로그인하지 않은 경우에 로그인하고, Deadline Cloud 콘솔을 AWS Management Console열고, 팜을 선택한 다음 작업 관리를 선택합니다.
2. 예산 관리자 페이지의 활성 예산 탭에서 편집하려는 예산 옆의 버튼을 선택합니다.
3. 작업 드롭다운 메뉴에서 예산 편집을 선택합니다.
4. 원하는 대로 변경한 다음 예산 업데이트를 선택합니다.

Deadline Cloud 대기열에 대한 예산 비활성화

활성 예산을 비활성화할 수 있습니다. 예산을 비활성화하면 상태가 활성에서 비활성으로 변경됩니다. 예산이 비활성화되면 더 이상 해당 예산 금액에 대한 리소스를 추적하지 않습니다.

예산을 비활성화하려면 다음 절차를 사용합니다.

1. 아직 로그인하지 않은 경우에 로그인하고, Deadline Cloud 콘솔을 AWS Management Console열고, 팜을 선택한 다음 작업 관리를 선택합니다.
2. 예산 관리자 페이지의 활성 예산 탭에서 비활성화하려는 예산 옆의 버튼을 선택합니다.
3. 작업 드롭다운 메뉴에서 예산 비활성화를 선택합니다. 잠시 후 선택한 예산이 활성에서 비활성으로 변경되고 활성 예산 탭에서 비활성 예산 탭으로 이동합니다.

EventBridge 이벤트를 사용하여 예산 모니터링

Deadline Cloud는 Amazon EventBridge를 사용하여 예산 관련 이벤트를 기본 EventBridge 이벤트 버스로 전송합니다. 예산이 사전 정의된 수준에 도달하면 이벤트를 수신하고 이벤트를 기반으로 알림을 전송하여 이메일, Slack 또는 기타 채널을 통해 사용자에게 자동으로 알리는 사용자 지정 함수를 생성할 수 있습니다. 예를 들어 예산이 특정 임계값에 도달하면 SMS 메시지를 보낼 수 있습니다. 이렇게 하면 예산이 소진되기 전에 지출을 파악하고 정보에 입각한 결정을 내릴 수 있습니다.

Deadline Cloud는 각 렌더 팜의 사용량 및 비용 데이터를 주기적으로 집계합니다. 그런 다음 예산 임계값을 초과했는지 확인합니다. 임계값을 초과하면 Deadline Cloud는 적절한 조치를 취할 수 있도록 사용자에게 알리는 이벤트를 트리거합니다. 예산이 사용된 예산의 백분율로 지정된 이러한 임계값 중 하나를 초과할 때마다 이벤트가 트리거됩니다.

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

예산 사용량 임계값이 100% 사용량에 가까워지면 예산 사용량 임계값이 더 가까워집니다. 이렇게 하면 예산이 한도에 도달하면 사용량을 면밀히 모니터링할 수 있습니다. 자체 예산 임계값을 설정할 수도 있습니다. Deadline Cloud는 사용량이 사용자 지정 임계값을 통과하면 이벤트를 전송합니다. 예산이 100%에 도달하면 Deadline Cloud는 이벤트 전송을 중지합니다. 예산을 조정하면 Deadline Cloud는 새 예산 금액에 따라 임계값에 대한 이벤트를 전송합니다.

EventBridge 콘솔(https://console.aws.amazon.com/events/)을 사용하여 데드라인 클라우드 이벤트를 이벤트의 적절한 대상으로 전송하는 규칙을 생성할 수 있습니다. 예를 들어 이벤트를 Amazon Simple Queue Service 대기열로 보내고 거기에서 로깅을 위해 AWS End User Messaging SMS 또는 Amazon Relational Database Service 데이터베이스와 같은 여러 대상으로 보낼 수 있습니다.

EventBridge 규칙의 예는 다음 주제를 참조하세요.

- Amazon EventBridge를 사용하여 이벤트가 발생하면 이메일을 보냅니다.
- 채팅 애플리케이션에서 Amazon Q Developer에 알림을 보내는 Amazon EventBridge 규칙 생성.
- Amazon EventBridge 시작하기.

예산 이벤트에 대한 자세한 내용은 Deadline Cloud 개발자 안내서의 Budget Threshold Reached 이벤트를 참조하세요.

Deadline Cloud 사용량 탐색기를 사용하여 사용량 및 비용 추적

Deadline Cloud 사용량 탐색기를 사용하면 각 팜에서 발생하는 활동에 대한 실시간 지표를 볼 수 있습니다. 대기열, 작업, 라이선스 제품 또는 인스턴스 유형과 같은 다양한 변수별로 팜 비용을 볼 수 있습니다. 다양한 기간을 선택하여 특정 기간 동안의 사용량을 확인하고 일정 기간 동안의 사용량 추세를 확인합니다. 또한 선택한 데이터 포인트의 세부 분석을 확인하여 지표를 자세히 살펴볼 수 있습니다. 사용량은 시간(분 및 시간) 또는 비용(USD)별로 표시할 수 있습니다.

다음 섹션에서는 Deadline Cloud 사용량 탐색기에 액세스하고 사용하는 단계를 보여줍니다.

주제

- 전제 조건
- 사용량 탐색기 열기
- 사용량 탐색기 사용

전제 조건

Deadline Cloud 사용량 탐색기를 사용하려면 MANAGER 또는 OWNER팜 권한이 있어야 합니다. 자세한 내용은 팜, 대기열 및 플릿에 대한 사용자 및 그룹 관리 단원을 참조하십시오.

> **Note**
> 시간대가 인도 표준시(UTC+5:30)와 같은 전체 시간에 맞지 않는 경우 사용량 탐색기는 사용량 지표를 표시하지 않습니다. 지표를 보려면 시간대를 1시간에 맞춰 조정된 영역으로 설정합니다.

사용량 탐색기 열기

Deadline Cloud 사용량 탐색기를 열려면 다음 절차를 사용합니다.

1. 에 로그인 AWS Management Console 하고 Deadline Cloud 콘솔을 엽니다.
2. 사용 가능한 모든 팜을 보려면 팜 보기를 선택합니다.
3. 정보를 가져오려는 팜을 찾은 다음 작업 관리를 선택합니다. Deadline Cloud 모니터가 새 탭에서 열립니다.
4. Deadline Cloud Monitor의 왼쪽 메뉴에서 Usage Explorer를 선택합니다.

사용량 탐색기 사용

사용량 탐색기 페이지에서 데이터를 표시할 수 있는 특정 파라미터를 선택할 수 있습니다. 기본적으로 지난 7일 동안의 총 시간(시간 및 분)이 표시됩니다. 이러한 파라미터를 변경할 수 있으며 표시된 정보는 파라미터 설정에 따라 동적으로 변경됩니다.

대기열, 작업, 컴퓨팅 사용량, 인스턴스 유형 또는 라이선스 제품을 기준으로 결과를 그룹화할 수 있습니다. 라이선스 제품을 선택하면 특정 라이선스에 대한 비용이 계산됩니다. 다른 모든 그룹의 경우 각 작업을 실행하는 데 걸리는 시간을 합산하여 시간을 계산합니다.

사용량 탐색기는 설정한 필터 기준에 따라 100개의 결과만 반환합니다. 결과는 생성된 타임스탬프를 기준으로 내림차순으로 나열됩니다. 결과가 100개 이상인 경우 오류 메시지가 표시됩니다. 쿼리를 구체화하여 결과 수를 줄일 수 있습니다.

- 더 작은 시간 범위 선택

- 더 적은 대기열 선택
- 작업 대신 대기열별로 그룹화하는 등 다른 그룹화 선택

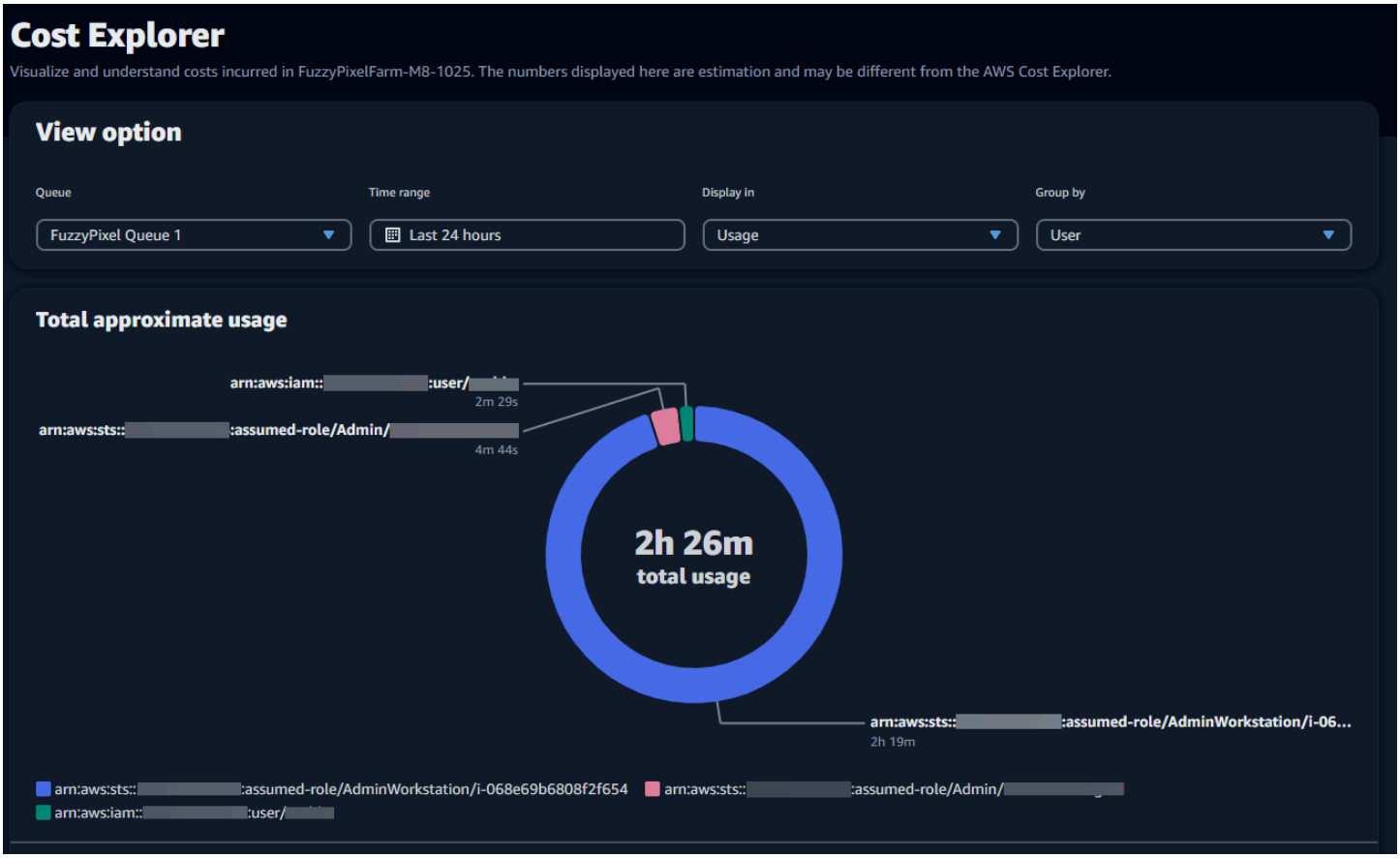
주제

- 시각적 그래프를 사용하여 데이터 검토
- 지표 분석 보기
- 대기열의 대략적인 런타임 보기

시각적 그래프를 사용하여 데이터 검토

시각적 형식으로 데이터를 검토하여 더 많은 분석이나 주의가 필요할 수 있는 추세와 잠재적 영역을 식별할 수 있습니다. 사용량 탐색기는 합계를 더 작은 소계로 그룹화하는 옵션과 함께 전체 사용량 및 비용을 표시하는 파이형 차트를 제공합니다.

> **Note**
>
> 차트에는 상위 5개 결과만 표시되고 다른 결과는 "기타" 섹션에 결합됩니다. 차트 아래의 분석 섹션에서 모든 결과를 볼 수 있습니다.



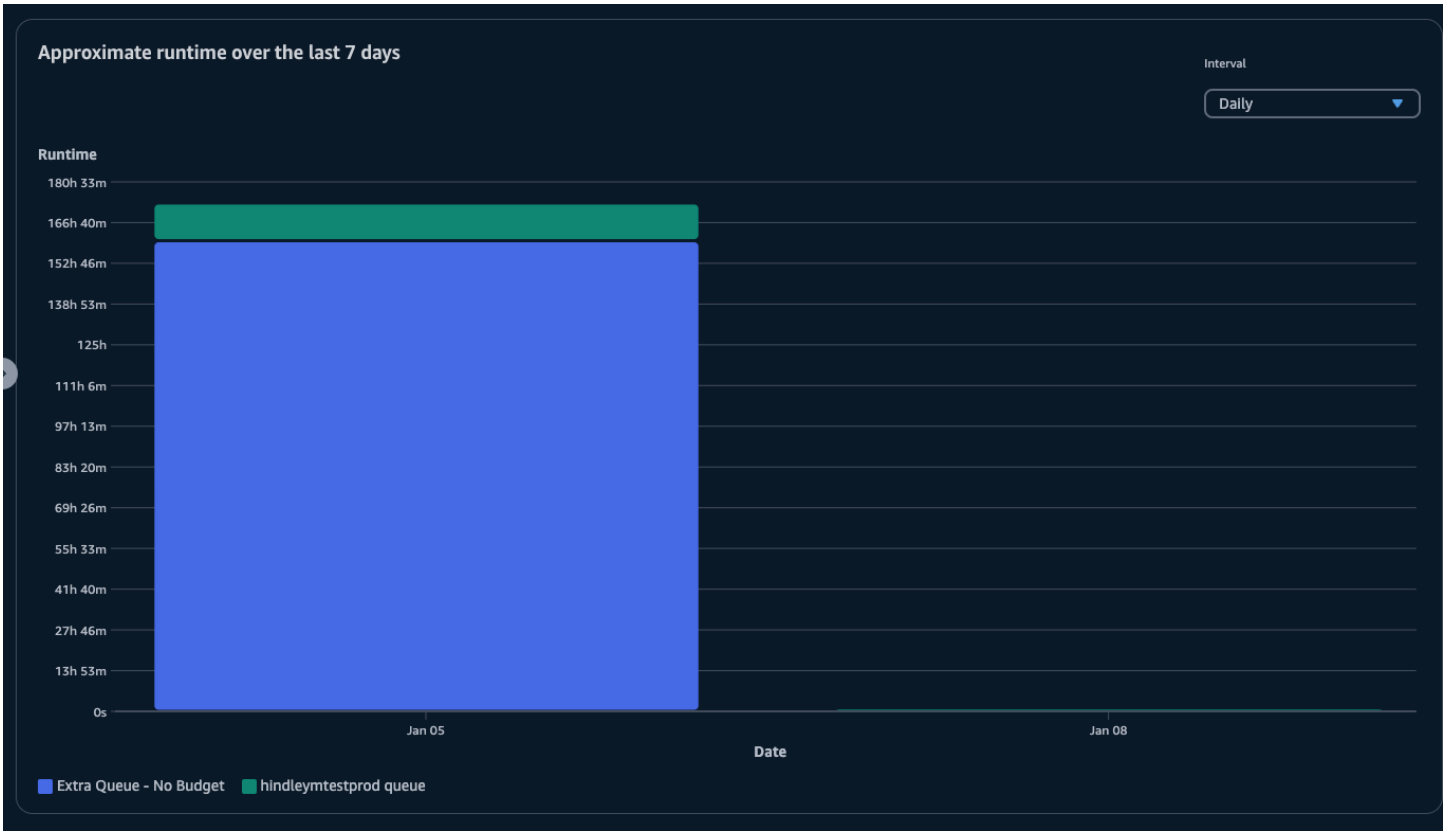
지표 분석 보기

파이형 차트 아래에 있는 사용량 탐색기는 파라미터가 변경될 때 변경되는 특정 지표에 대한 보다 자세한 분석을 제공합니다. 기본적으로 사용량 탐색기에 5개의 결과가 표시됩니다. 분석 섹션의 페이지 매김 화살표를 사용하여 결과를 스크롤할 수 있습니다.

기본적으로 분류가 최소화됩니다. 결과를 확장하고 표시하려면 모든 분석 보기 화살표를 선택합니다. 분석을 다운로드하려면 데이터 다운로드를 선택합니다.

대기열의 대략적인 런타임 보기

지정한 다양한 간격에 따라 대기열의 대략적인 런타임을 볼 수도 있습니다. 간격 옵션은 시간별, 일별, 주별 및 월별입니다. 간격을 선택하면 그래프에 대기열의 대략적인 런타임이 표시됩니다.



비용 관리

AWS Deadline Cloud는 작업 비용을 제어하고 시각화하는 데 도움이 되는 예산과 사용량 탐색기를 제공합니다. 그러나 Deadline Cloud는 Amazon S3와 같은 다른 AWS 서비스를 사용합니다. 이러한 서비스에 대한 비용은 Deadline Cloud 예산 또는 사용량 탐색기에 반영되지 않으며 사용량에 따라 별도로 청구됩니다. Deadline Cloud를 구성하는 방법에 따라 다음 서비스뿐만 아니라 다른 서비스도 사용할 AWS 수 있습니다.

Service	요금 페이지
Amazon CloudWatch Logs	Amazon CloudWatch Logs 요금
Amazon Elastic Compute Cloud	Amazon Elastic Compute Cloud 요금
AWS Key Management Service	AWS Key Management Service 요금
AWS PrivateLink	AWS PrivateLink 요금
Amazon Simple Storage Service(S3)	Amazon Simple Storage Service 요금

Service	요금 페이지
Amazon Virtual Private Cloud	Amazon Virtual Private Cloud 요금

비용 관리 모범 사례

다음 모범 사례를 사용하면 Deadline Cloud를 사용할 때 발생하는 비용과 비용과 효율성 간의 장단점을 이해하고 제어하는 데 도움이 될 수 있습니다.

> **Note**
>
> Deadline Cloud 사용의 최종 비용은 여러 AWS 서비스 간의 상호 작용, 처리하는 작업량 및 작업을 실행하는 AWS 리전 에 따라 달라집니다. 다음 모범 사례는 지침이며 비용을 크게 절감하지 못할 수 있습니다.

CloudWatch Logs 모범 사례

Deadline Cloud는 작업자 및 작업 로그를 CloudWatch Logs로 전송합니다. 이러한 로그를 수집, 저장 및 분석하는 데는 요금이 부과됩니다. 작업을 모니터링하는 데 필요한 최소 데이터 양만 로깅하여 비용을 절감할 수 있습니다.

대기열 또는 플릿을 생성할 때 Deadline Cloud는 다음 이름으로 CloudWatch Logs 로그 그룹을 생성합니다.

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

기본적으로 이러한 로그는 만료되지 않습니다. 로그 그룹의 보존 정책을 조정하여 이전 로그를 제거하고 스토리지 비용을 줄일 수 있습니다. 또한 로그를 Amazon S3로 내보낼 수 있습니다. Amazon S3 스토리지 비용은 CloudWatch보다 저렴합니다. 자세한 내용은 Amazon S3에 로그 데이터 내보내기를 참조하세요.

Amazon EC2 모범 사례

서비스 관리형 플릿과 고객 관리형 플릿 모두에 Amazon EC2 인스턴스를 사용할 수 있습니다. 세 가지 고려 사항이 있습니다.

- 서비스 관리형 플릿의 경우 플릿의 최소 작업자 수를 설정하여 항상 하나 이상의 인스턴스를 사용할 수 있도록 선택할 수 있습니다. 최소 작업자 수를 0보다 높게 설정하면 플릿에는 항상이 많은 작업자가 실행됩니다. 이렇게 하면 Deadline Cloud가 처리 작업을 시작하는 데 걸리는 시간을 줄일 수 있지만 인스턴스의 유휴 시간에 대한 요금이 청구됩니다.
- 서비스 관리형 플릿의 경우 플릿의 최대 크기를 설정합니다. 이렇게 하면 플릿이 자동으로 확장할 수 있는 인스턴스 수가 제한됩니다. 처리 대기 중인 작업이 더 많더라도 플릿은이 크기를 초과하여 증가하지 않습니다.
- 서비스 관리형 플릿과 고객 관리형 플릿 모두에 대해 플릿에서 Amazon EC2 인스턴스 유형을 지정할 수 있습니다. 더 작은 인스턴스를 사용하면 분당 비용이 저렴하지만 작업을 완료하는 데 더 오래 걸릴 수 있습니다. 반대로 인스턴스가 클수록 분당 비용이 더 많이 들지만 작업을 완료하는 데 걸리는 시간을 줄일 수 있습니다. 인스턴스에 대한 작업 요구 사항을 이해하면 비용을 절감하는 데 도움이 될 수 있습니다.
- 가능하면 플릿에 대해 Amazon EC2 스팟 인스턴스를 선택합니다. 스팟 인스턴스는 저렴한 가격으로 사용할 수 있지만 온디맨드 요청에 의해 중단될 수 있습니다. 온디맨드 인스턴스는 초 단위로 요금이 부과되며 중단되지 않습니다.

모범 사례 AWS KMS

기본적으로 Deadline Cloud는 AWS 소유 키로 데이터를 암호화합니다. 이 키에 대해서는 요금이 부과되지 않습니다.

고객 관리형 키를 사용하여 데이터를 암호화하도록 선택할 수 있습니다. 자체 키를 사용하는 경우 키 사용 방식에 따라 요금이 부과됩니다. 기존 키를 사용하는 경우 추가 사용에 대한 증분 비용이 발생합니다.

모범 사례 AWS PrivateLink

AWS PrivateLink 를 사용하여 인터페이스 엔드포인트를 사용하여 VPC와 Deadline Cloud 간에 연결을 생성할 수 있습니다. 연결을 생성할 때 모든 Deadline Cloud API 작업을 호출할 수 있습니다. 생성한 각 엔드포인트에 대해 시간당 요금이 부과됩니다. PrivateLink를 사용하는 경우 엔드포인트를 3개 이상 생성해야 하며 구성에 따라 최대 5개가 필요할 수 있습니다.

Amazon S3 모범 사례

Deadline Cloud는 Amazon S3를 사용하여 처리, 작업 연결, 출력 및 로그에 대한 자산을 저장합니다. Amazon S3와 관련된 비용을 줄이려면 저장하는 데이터의 양을 줄이세요. 몇 가지 제안 사항은 다음과 같습니다.

- 현재 사용 중이거나 곧 사용될 자산만 저장합니다.
- S3 수명 주기 구성을 사용하여 S3 버킷에서 미사용 파일을 자동으로 삭제합니다.

Amazon VPC 모범 사례

고객 관리형 플릿에 사용량 기반 라이선스를 사용하는 경우 계정에서 생성된 Amazon VPC 엔드포인트인 Deadline Cloud 라이선스 엔드포인트를 생성합니다. 이 엔드포인트에는 시간당 요금이 부과됩니다. 비용을 줄이려면 사용량 기반 라이선스를 사용하지 않을 때 엔드포인트를 제거합니다.

의 보안 Deadline Cloud

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 서비스 프로그램 제공 범위 내 규정 준수 AWS Deadline Cloud참조하세요.
- 클라우드의 보안 - 사용자의 책임은 AWS 서비스 사용하는에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 Deadline Cloud. 다음 주제에서는 보안 및 규정 준수 목표를 충족 Deadline Cloud 하도록를 구성하는 방법을 보여줍니다. 또한 Deadline Cloud 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 다른를 사용하는 방법을 알아봅니다.

주제

- 의 데이터 보호 Deadline Cloud
- Deadline Cloud의 Identity and Access Management
- 에 대한 규정 준수 검증 Deadline Cloud
- 의 복원력 Deadline Cloud
- Deadline Cloud의 인프라 보안
- Deadline Cloud의 구성 및 취약성 분석
- 교차 서비스 혼동된 대리인 방지
- 인터페이스 엔드포인트를 AWS Deadline Cloud 사용한 액세스(AWS PrivateLink)
- Deadline Cloud의 보안 모범 사례

의 데이터 보호 Deadline Cloud

AWS 공동 책임 모델의 데이터 보호에 적용됩니다 AWS Deadline Cloud. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Deadline Cloud 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

Deadline Cloud 작업 템플릿의 이름 필드에 입력된 데이터는 결제 또는 진단 로그에도 포함될 수 있으며 기밀 또는 민감한 정보를 포함해서는 안 됩니다.

주제

- 저장 시 암호화

- 전송 중 암호화
- 키 관리
- 인터네트워크 트래픽 개인 정보 보호
- 옵트아웃

저장 시 암호화

AWS Deadline Cloud 는 AWS Key Management Service (AWS KMS)에 저장된 암호화 키를 사용하여 저장 데이터를 암호화하여 민감한 데이터를 보호합니다. 유휴 시 암호화는를 사용할 수 AWS 리전 있는 모든에서 사용할 수 Deadline Cloud 있습니다.

데이터를 암호화하면 유효한 키가 없는 사용자 또는 애플리케이션에서 디스크에 저장된 민감한 데이터를 읽을 수 없습니다. 유효한 관리형 키가 있는 당사자만 데이터를 해독할 수 있습니다.

가 저장 데이터 암호화를 위해 Deadline Cloud 를 사용하는 방법에 AWS KMS 대한 자세한 내용은 섹션을 참조하세요키 관리.

전송 중 암호화

전송 중인 데이터의 경우 TLS(전송 계층 보안) 1.2 또는 1.3을 AWS Deadline Cloud 사용하여 서비스와 작업자 간에 전송된 데이터를 암호화합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다. 또한 Virtual Private Cloud(VPC)를 사용하는 경우 AWS PrivateLink 를 사용하여 VPC와 간에 프라이빗 연결을 설정할 수 있습니다 Deadline Cloud.

키 관리

새 팜을 생성할 때 다음 키 중 하나를 선택하여 팜 데이터를 암호화할 수 있습니다.

- AWS 소유 KMS 키 - 팜을 생성할 때 키를 지정하지 않으면 기본 암호화 유형입니다. KMS 키는에서 소유합니다 AWS Deadline Cloud. AWS 소유 키는 보거나 관리하거나 사용할 수 없습니다. 그러나 데이터를 암호화하는 키를 보호하기 위해 조치를 취할 필요는 없습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS 소유 키를 참조하세요.
- 고객 관리형 KMS 키 - 팜을 생성할 때 고객 관리형 키를 지정합니다. 팜 내의 모든 콘텐츠는 KMS 키로 암호화됩니다. 키는 계정에 저장되며 사용자가 생성, 소유 및 관리하며 AWS KMS 요금이 적용됩니다. KMS 키를 완전히 제어할 수 있습니다. 다음과 같은 작업을 수행할 수 있습니다.
  - 키 정책 수립 및 유지 관리
  - IAM 정책 및 권한 부여 수립 및 유지

- 키 정책 활성화 및 비활성화
- 태그 추가
- 키 별칭 만들기

Deadline Cloud 팜에 사용되는 고객 소유 키는 수동으로 교체할 수 없습니다. 키의 자동 교체가 지원됩니다.

자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 소유 키를 참조하세요.

고객 관리형 키를 생성하려면 AWS Key Management Service 개발자 안내서의 대칭 고객 관리형 키 생성 단계를 따르세요.

AWS KMS 권한 부여 Deadline Cloud 사용 방법

Deadline Cloud 고객 관리형 키를 사용하려면에 권한 부여가 필요합니다. 고객 관리형 키로 암호화된 팜을 생성하면는 지정한 KMS 키에 대한 액세스 권한을 `CreateGrant` AWS KMS 에 요청하여 사용자를 대신하여 권한 부여를 Deadline Cloud 생성합니다.

Deadline Cloud 는 여러 권한 부여를 사용합니다. 각 권한 부여는 데이터를 암호화하거나 해독해야 Deadline Cloud 하는의 다른 부분에서 사용됩니다. Deadline Cloud 또한 권한 부여를 사용하여 Amazon Simple Storage Service, Amazon Elastic Block Store 또는 OpenSearch와 같이 사용자를 대신하여 데이터를 저장하는 데 사용되는 다른 AWS 서비스에 대한 액세스를 허용합니다.

가 서비스 관리형 플릿에서 시스템을 관리할 Deadline Cloud 수 있는 권한 부여에는 서비스 보안 주체 `GranteePrincipal` 대신의 계정 번호와 역할이 포함됩니다 Deadline Cloud . 일반적으로는 아니지만 팜에 지정된 고객 관리형 KMS 키를 사용하여 서비스 관리형 플릿의 작업자에 대한 Amazon EBS 볼륨을 암호화하는 데 필요합니다.

고객 관리형 키 정책

키 정책에서는 고객 관리형 키에 대한 액세스를 제어합니다. 각 키에는 키를 사용할 수 있는 사용자와 키 사용 방법을 결정하는 문이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리형 키에 대한 액세스 관리를 참조하세요.

CreateFarm에 대한 최소 IAM 정책

고객 관리형 키를 사용하여 콘솔 또는 `CreateFarm` API 작업을 사용하여 팜을 생성하려면 다음 AWS KMS API 작업을 허용해야 합니다.

- `kms:CreateGrant` - 고객 관리형 키에 권한 부여를 추가합니다. 콘솔에 지정된 AWS KMS 키에 대한 액세스 권한을 부여합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 권한 부여 사용을 참조하세요.
- `kms:Decrypt` -가 팜의 데이터를 복호화 Deadline Cloud 할 수 있습니다.
- `kms:DescribeKey` -가 키를 Deadline Cloud 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.
- `kms:GenerateDataKey` -가 고유한 데이터 키를 사용하여 데이터를 암호화 Deadline Cloud 하도록 허용합니다.

다음 정책 설명은 `CreateFarm` 작업에 필요한 권한을 부여합니다.

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

읽기 전용 작업에 대한 최소 IAM 정책

팜, 대기열 및 플릿에 대한 정보 가져오기와 같은 읽기 전용 Deadline Cloud 작업에 고객 관리형 키를 사용합니다. 다음 AWS KMS API 작업을 허용해야 합니다.

- `kms:Decrypt` -가 팜의 데이터를 복호화 Deadline Cloud 할 수 있습니다.

- kms:DescribeKey -가 키를 Deadline Cloud 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.

다음 정책 설명은 읽기 전용 작업에 필요한 권한을 부여합니다.

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

읽기-쓰기 작업에 대한 최소 IAM 정책

팜, 대기열 및 플릿 생성 및 업데이트와 같은 읽기-쓰기 Deadline Cloud 작업에 고객 관리형 키를 사용합니다. 다음 AWS KMS API 작업을 허용해야 합니다.

- kms:Decrypt -가 팜의 데이터를 복호화 Deadline Cloud 할 수 있습니다.
- kms:DescribeKey -가 키를 Deadline Cloud 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.
- kms:GenerateDataKey -가 고유한 데이터 키를 사용하여 데이터를 암호화 Deadline Cloud 하도록 허용합니다.

다음 정책 설명은 `CreateFarm` 작업에 필요한 권한을 부여합니다.

```
{
```

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

암호화 키 모니터링

Deadline Cloud 팜에 AWS KMS 고객 관리형 키를 사용하는 경우 AWS CloudTrail 또는 Amazon CloudWatch Logs를 사용하여가 로 Deadline Cloud 보내는 요청을 추적할 수 있습니다 AWS KMS.

권한 부여에 대한 CloudTrail 이벤트

다음 예제 CloudTrail 이벤트는 권한 부여가 생성될 때, 일반적으로 `CreateFarm`, `CreateMonitor`또는 `CreateFleet` 작업을 호출할 때 발생합니다.

```
{
    "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"
}
```

복호화를 위한 CloudTrail 이벤트

다음 예제 CloudTrail 이벤트는 고객 관리형 KMS 키를 사용하여 값을 해독할 때 발생합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:51:44Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeffffff",
    "eventID": "ffffffff-eeee-dddd-cccc-bbbbbbaaaaaa",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

암호화를 위한 CloudTrail 이벤트

다음 예제 CloudTrail 이벤트는 고객 관리형 KMS 키를 사용하여 값을 암호화할 때 발생합니다.

```
{
    "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"
}
```

고객 관리형 KMS 키 삭제

AWS Key Management Service (AWS KMS)에서 고객 관리형 KMS 키를 삭제하면 파괴적이고 위험할 수 있습니다. 이렇게 하면 키와 연결된 키 구성 요소와 모든 메타데이터가 되돌릴 수 없는 방식으로 삭제됩니다. 고객 관리형 KMS 키가 삭제된 후에는 해당 키로 암호화된 데이터를 더 이상 복호화할 수 없습니다. 즉, 데이터를 복구할 수 없게 됩니다.

따라서는 KMS 키를 삭제하기 전에 고객에게 최대 30일의 대기 기간을 AWS KMS 제공합니다. 기본 대기 기간은 30일입니다.

대기 기간에 대해

고객 관리형 KMS 키를 삭제하는 것은 파괴적이고 잠재적으로 위험하기 때문에 대기 기간을 7~30일로 설정해야 합니다. 기본 대기 기간은 30일입니다.

그러나 실제 대기 기간은 예약한 기간보다 최대 24시간 더 길 수 있습니다. 키가 삭제될 실제 날짜와 시간을 가져오려면 DescribeKey 작업을 사용합니다. AWS KMS 콘솔의 키 세부 정보 페이지에 있는 일반 구성 섹션에서 예약된 삭제 날짜를 확인할 수도 있습니다. 시간대를 확인하세요.

대기 기간 동안 고객 관리형 키의 상태 및 키 상태는 삭제 대기 중입니다.

- 삭제 대기 중인 고객 관리형 KMS 키는 어떠한 암호화 작업에도 사용할 수 없습니다.
- AWS KMS 는 삭제 보류 중인 고객 관리형 KMS 키의 백업 키를 교체하지 않습니다.

고객 관리형 KMS 키 삭제에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 마스터 키 삭제를 참조하세요.

인터네트워크 트래픽 개인 정보 보호

AWS Deadline Cloud 는 연결을 보호하기 위해 Amazon Virtual Private Cloud(VPC)를 지원합니다. Amazon VPC는 Virtual Private Cloud(VPC)의 보안을 강화하고 모니터링하기 위해 사용할 수 있는 여러 가지 기능을 제공합니다.

VPC 내에서 실행되는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 사용하여 고객 관리형 플릿(CMF)을 설정할 수 있습니다. 사용할 Amazon VPC 엔드포인트를 배포하면 CMF의 작업자와 Deadline Cloud 엔드포인트 간의 AWS PrivateLink트래픽이 VPC 내에 유지됩니다. 또한 인스턴스에 대한 인터넷 액세스를 제한하도록 VPC를 구성할 수 있습니다.

서비스 관리형 플릿에서는 작업자가 인터넷에서 연결할 수 없지만 인터넷에 액세스할 수 있고 인터넷을 통해 Deadline Cloud 서비스에 연결됩니다.

옵트아웃

AWS Deadline Cloud 는 개발 및 개선에 도움이 되는 특정 운영 정보를 수집합니다 Deadline Cloud. 수집된 데이터에는 AWS 계정 ID 및 사용자 ID와 같은 항목이 포함되어 있으므로에 문제가 있는 경우 사용자를 올바르게 식별할 수 있습니다 Deadline Cloud. 또한 리소스 IDs(해당하는 경우 FarmID 또는 QueueID), 제품 이름(예: JobAttachments, WorkerAgent 등), 제품 버전과 같은 Deadline Cloud 특정 정보를 수집합니다.

애플리케이션 구성을 사용하여이 데이터 수집을 옵트아웃하도록 선택할 수 있습니다. 클라이언트 워크스테이션과 플릿 작업자 Deadline Cloud모두와 상호 작용하는 각 컴퓨터는 별도로 옵트아웃해야 합니다.

Deadline Cloud 모니터 - 데스크톱

Deadline Cloud 모니터 - 데스크톱은 충돌 발생 시점 및 애플리케이션 열기 시점과 같은 운영 정보를 수집하여 애플리케이션에 문제가 있는 시점을 파악하는 데 도움이 됩니다. 이 운영 정보 수집을 옵트아웃하려면 설정 페이지로 이동하여 데이터 수집 켜기를 선택 취소하여 Deadline Cloud Monitor의 성능을 측정합니다.

옵트아웃한 후에는 데스크톱 모니터가 더 이상 운영 데이터를 전송하지 않습니다. 이전에 수집된 모든 데이터는 유지되며 서비스를 개선하는 데 계속 사용될 수 있습니다. 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

AWS Deadline Cloud CLI 및 도구

AWS Deadline Cloud CLI, 제출자 및 작업자 에이전트는 모두 충돌이 발생하는 시기 및 작업이 제출되는 시기와 같은 운영 정보를 수집하여 이러한 애플리케이션에 문제가 있는 시기를 파악하는 데 도움이 됩니다. 이 운영 정보 수집을 옵트아웃하려면 다음 방법 중 하나를 사용합니다.

- 터미널에를 입력합니다**`deadline config set telemetry.opt_out true`**.

  이렇게 하면 현재 사용자로 실행될 때 CLI, 제출자 및 작업자 에이전트가 옵트아웃됩니다.
- Deadline Cloud 작업자 에이전트를 설치할 때 **`--telemetry-opt-out`** 명령줄 인수를 추가합니다. 예를 들어 **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**입니다.
- 작업자 에이전트, CLI 또는 제출자를 실행하기 전에 환경 변수를 설정합니다. **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

옵트아웃한 후에는 Deadline Cloud 도구가 더 이상 운영 데이터를 전송하지 않습니다. 이전에 수집된 모든 데이터는 유지되며 서비스를 개선하는 데 계속 사용될 수 있습니다. 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

Deadline Cloud의 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 Deadline Cloud 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- Deadline Cloud와 IAM의 작동 방식
- Deadline Cloud의 자격 증명 기반 정책 예제
- AWS Deadline Cloud에 대한 관리형 정책
- AWS Deadline Cloud 자격 증명 및 액세스 문제 해결

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 Deadline Cloud에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Deadline Cloud 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Deadline Cloud 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Deadline Cloud의 기능에 액세스할 수 없는 경우 섹션을 참조하세요AWS Deadline Cloud 자격 증명 및 액세스 문제 해결.

서비스 관리자 - 회사에서 Deadline Cloud 리소스를 책임지고 있는 경우 Deadline Cloud에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Deadline Cloud 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Deadline Cloud에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Deadline Cloud와 IAM의 작동 방식.

IAM 관리자 - IAM 관리자인 경우 Deadline Cloud에 대한 액세스를 관리하는 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. IAM에서 사용할 수 있는 Deadline Cloud 자격 증명 기반 정책 예제를 보려면 섹션을 참조하세요Deadline Cloud의 자격 증명 기반 정책 예제.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를

사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용

자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.

- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 기업이 소유한 여러을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Deadline Cloud와 IAM의 작동 방식

IAM을 사용하여 Deadline Cloud에 대한 액세스를 관리하기 전에 Deadline Cloud에서 사용할 수 있는 IAM 기능을 알아봅니다.

AWS Deadline Cloud와 함께 사용할 수 있는 IAM 기능

IAM 기능	Deadline Cloud 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	아니요

Deadline Cloud 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Deadline Cloud에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지

를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Deadline Cloud에 대한 자격 증명 기반 정책 예제

Deadline Cloud 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Deadline Cloud의 자격 증명 기반 정책 예제.

Deadline Cloud 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Deadline Cloud에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없

는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Deadline Cloud 작업 목록을 보려면 서비스 승인 참조의 AWS Deadline Cloud에서 정의한 작업을 참조하세요.

Deadline Cloud의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
awsdeadlinecloud
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

Deadline Cloud 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Deadline Cloud의 자격 증명 기반 정책 예제.

Deadline Cloud에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Deadline Cloud 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 AWS Deadline Cloud에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Deadline Cloud에서 정의한 작업을 참조하세요.

Deadline Cloud 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Deadline Cloud의 자격 증명 기반 정책 예제.

Deadline Cloud에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Deadline Cloud 조건 키 목록을 보려면 서비스 승인 참조의 AWS Deadline Cloud에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS Deadline Cloud에서 정의한 작업을 참조하세요.

Deadline Cloud 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Deadline Cloud의 자격 증명 기반 정책 예제.

Deadline CloudACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC와 Deadline Cloud

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Deadline Cloud에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 포함한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는

access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Deadline Cloud에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Deadline Cloud의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 Deadline Cloud 기능이 중단될 수 있습니다. Deadline Cloud가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Deadline Cloud의 서비스 연결 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Deadline Cloud의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 Deadline Cloud 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 Deadline Cloud에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 AWS Deadline Cloud에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Deadline Cloud 콘솔 사용
- 대기열에 작업을 제출하는 정책
- 라이선스 엔드포인트 생성을 허용하는 정책
- 특정 팜 대기열 모니터링을 허용하는 정책

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Deadline Cloud 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Deadline Cloud 콘솔 사용

AWS Deadline Cloud 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Deadline Cloud 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Deadline Cloud 콘솔을 계속 사용할 수 있도록 하려면 Deadline Cloud `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책을 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

대기열에 작업을 제출하는 정책

이 예제에서는 특정 팜의 특정 대기열에 작업을 제출할 수 있는 권한을 부여하는 범위 축소 정책을 생성합니다.

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

라이선스 엔드포인트 생성을 허용하는 정책

이 예제에서는 라이선스 엔드포인트를 생성하고 관리하는 데 필요한 권한을 부여하는 범위 축소 정책을 생성합니다. 이 정책을 사용하여 팜과 연결된 VPC에 대한 라이선스 엔드포인트를 생성합니다.

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

특정 팜 대기열 모니터링을 허용하는 정책

이 예제에서는 특정 팜의 특정 대기열에서 작업을 모니터링할 수 있는 권한을 부여하는 범위 축소 정책을 생성합니다.

```
{
```

```
    "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 Deadline Cloud에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-FleetWorker

`AWSDeadlineCloud-FleetWorker` 정책을 (IAM) 자격 증명에 연결할 수 있습니다 AWS Identity and Access Management .

이 정책은이 플릿의 작업자에게 서비스에 연결하고 서비스에서 작업을 수신하는 데 필요한 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 보안 주체가 플릿에서 작업자를 관리할 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-FleetWorker를 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-WorkerHost

`AWSDeadlineCloud-WorkerHost` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 서비스에 처음 연결하는 데 필요한 권한을 부여합니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 프로파일로 사용할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 사용자가 작업자를 생성하고, 작업자의 플릿 역할을 수임하고, 작업자에 태그를 적용할 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-WorkerHost를 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-UserAccessFarms

`AWSDeadlineCloud-UserAccessFarms` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 사용자는 자신이 속한 팜과 멤버십 수준에 따라 팜 데이터에 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 사용자가 팜 데이터에 액세스할 수 있도록 허용합니다.
- `ec2` - 사용자가 Amazon EC2 인스턴스 유형에 대한 세부 정보를 볼 수 있도록 허용합니다.
- `identitystore` - 사용자가 사용자 및 그룹 이름을 볼 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-UserAccessFarms를 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-UserAccessFleets

`AWSDeadlineCloud-UserAccessFleets` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 사용자는 자신이 속한 팜과 멤버십 수준에 따라 플릿 데이터에 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 사용자가 팜 데이터에 액세스할 수 있도록 허용합니다.
- `ec2` - 사용자가 Amazon EC2 인스턴스 유형에 대한 세부 정보를 볼 수 있도록 허용합니다.
- `identitystore` - 사용자가 사용자 및 그룹 이름을 볼 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-UserAccessFleets를 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-UserAccessJobs

`AWSDeadlineCloud-UserAccessJobs` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 사용자는 자신이 속한 팜과 멤버십 수준에 따라 작업 데이터에 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 사용자가 팜 데이터에 액세스할 수 있도록 허용합니다.
- `ec2` - 사용자가 Amazon EC2 인스턴스 유형에 대한 세부 정보를 볼 수 있도록 허용합니다.
- `identitystore` - 사용자가 사용자 및 그룹 이름을 볼 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-UserAccessJobs를 참조하세요.

AWS 관리형 정책: AWSDeadlineCloud-UserAccessQueues

`AWSDeadlineCloud-UserAccessQueues` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 사용자는 자신이 속한 팜과 멤버십 수준에 따라 대기열 데이터에 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `deadline` - 사용자가 팜 데이터에 액세스할 수 있도록 허용합니다.
- `ec2` - 사용자가 Amazon EC2 인스턴스 유형에 대한 세부 정보를 볼 수 있도록 허용합니다.
- `identitystore` - 사용자가 사용자 및 그룹 이름을 볼 수 있도록 허용합니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 AWSDeadlineCloud-UserAccessQueues를 참조하세요.

AWS 관리형 정책에 대한 기한 클라우드 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Deadline Cloud의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 기한 클라우드 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSDeadlineCloud-WorkerHost – 변경	Deadline Cloud는 플릿의 작업자`deadline:TagResour`	2025년 5월 30일

변경 사항	설명	날짜
	`ce` 와 연결된 태그를 추가하고 볼 수 `deadline:ListTagsForResource` 있도록 새로운 작업 및를 추가했습니다.	
AWSDeadlineCloud-UserAccessFarms – 변경 AWSDeadlineCloud-UserAccessJobs – 변경 AWSDeadlineCloud-UserAccessQueues – 변경	Deadline Cloud는 작업을 다시 제출할 수 `deadline:ListJobParameterDefinitions` 있도록 새 작업 `deadline:GetJobTemplate` 및를 추가했습니다.	2024년 10월 7일
Deadline Cloud에서 변경 사항 추적 시작	Deadline Cloud가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2024년 4월 2일

AWS Deadline Cloud 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Deadline Cloud 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Deadline Cloud에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 Deadline Cloud 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Deadline Cloud에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `awsdeadlinecloud:`*`GetWidget`* 권한이 없을 때 발생합니다.

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

이 경우, `awsdeadlinecloud:GetWidget` 작업을 사용하여 `my-example-widget` 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 권한이 없다는 오류가 수신되면 Deadline Cloud에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 Deadline Cloud에서 작업을 수행하려고 `marymajor` 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Deadline Cloud 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Deadline Cloud가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요Deadline Cloud와 IAM의 작동 방식.

- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

에 대한 규정 준수 검증 Deadline Cloud

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 내 보안 상태에 대한 포괄적인 보기를 AWS 서비스 제공합니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.

- Amazon GuardDuty - 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

의 복원력 Deadline Cloud

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS Deadline Cloud 는 작업 연결 S3 버킷에 저장된 데이터를 백업하지 않습니다. S3 버전 관리 또는 와 같은 표준 Amazon S3 백업 메커니즘을 사용하여 작업 연결 데이터의 백업을 활성화할 수 있습니다AWS Backup. S3

Deadline Cloud의 인프라 보안

관리형 서비스인 AWS Deadline Cloud는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Deadline Cloud에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Deadline Cloud는 AWS PrivateLink Virtual Private Cloud(VPC) 엔드포인트 정책 사용을 지원하지 않습니다. 엔드포인트에 대한 전체 액세스 권한을 부여하는 AWS PrivateLink 기본 정책을 사용합니다. 자세한 내용은 AWS PrivateLink 사용 설명서의 기본 엔드포인트 정책을 참조하세요.

Deadline Cloud의 구성 및 취약성 분석

AWS 는 게스트 운영 체제(OS) 및 데이터베이스 패치, 방화벽 구성, 재해 복구와 같은 기본 보안 작업을 처리합니다. 적합한 제3자가 이 절차를 검토하고 인증하였습니다. 자세한 내용은 다음 리소스를 참조하세요.

- 공동 책임 모델
- Amazon Web Services: 보안 프로세스의 개요(백서)

AWS Deadline Cloud는 서비스 관리형 또는 고객 관리형 플릿에서 작업을 관리합니다.

- 서비스 관리형 플릿의 경우 Deadline Cloud는 게스트 운영 체제를 관리합니다.
- 고객 관리형 플릿의 경우 운영 체제를 관리할 책임은 사용자에게 있습니다.

AWS Deadline Cloud의 구성 및 취약성 분석에 대한 자세한 내용은 섹션을 참조하세요.

- Deadline Cloud의 보안 모범 사례

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 가장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 aws:SourceArn 및 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스를 AWS Deadline Cloud 제공하는 권한을 제한하는 것이 좋습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 `aws:SourceArn`를 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 `aws:SourceAccount`를 사용하세요.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 Amazon 리소스 이름(ARN)이 포함된 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드 문자(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어 `arn:aws:awsdeadlinecloud:*:123456789012:*`입니다.

만약 `aws:SourceArn` 값에 Amazon S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우, 권한을 제한하려면 두 글로벌 조건 컨텍스트 키를 모두 사용해야 합니다.

다음 예제에서는에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 Deadline Cloud 방지하는 방법을 보여줍니다.

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

인터페이스 엔드포인트를 AWS Deadline Cloud 사용한 액세스 (AWS PrivateLink)

AWS PrivateLink 를 사용하여 VPC와 간에 프라이빗 연결을 생성할 수 있습니다 AWS Deadline Cloud. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결을 사용하지 않고 VPC에 있는 Deadline Cloud 것처럼에 액세스할 수 있습니다. VPC의 인스턴스에서 Deadline Cloud API에 액세스하는 데는 퍼블릭 IP 주소가 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 Deadline Cloud로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

Deadline Cloud 에는 듀얼 스택 엔드포인트도 있습니다. 듀얼 스택 엔드포인트는 IPv6 및 IPv4를 통한 요청을 지원합니다.

자세한 내용은AWS PrivateLink 가이드의 AWS PrivateLink를 통해 AWS 서비스 에 액세스를 참조하세요.

에 대한 고려 사항 Deadline Cloud

에 대한 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스 액세스를 Deadline Cloud참조하세요.

Deadline Cloud 는 인터페이스 엔드포인트를 통해 모든 API 작업을 호출할 수 있도록 지원합니다.

기본적으로 인터페이스 엔드포인트를 통해에 대한 전체 액세스 Deadline Cloud 가 허용됩니다. 또는 보안 그룹을 엔드포인트 네트워크 인터페이스와 연결하여 인터페이스 엔드포인트를 Deadline Cloud 통해에 대한 트래픽을 제어할 수 있습니다.

Deadline Cloud 는 VPC 엔드포인트 정책도 지원합니다. 자세한 정보는 AWS PrivateLink 가이드의 엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어를 참조하세요.

Deadline Cloud 엔드포인트

Deadline Cloud 는를 사용하여 서비스에 액세스하는 데 4개의 엔드포인트를 사용합니다. AWS PrivateLink 하나는 IPv4용이고 다른 하나는 IPv6용입니다.

작업자는 `scheduling.deadline.`*`region`*`.amazonaws.com` 엔드포인트를 사용하여 대기열에서 작업을 가져오고, 진행 상황을 보고하고 Deadline Cloud, 작업 출력을 다시 보냅니다. 고객 관리형 플릿

을 사용하는 경우 관리 작업을 사용하지 않는 한 생성해야 하는 유일한 엔드포인트는 예약 엔드포인트입니다. 예를 들어 작업이 더 많은 작업을 생성하는 경우 관리 엔드포인트가 `CreateJob` 작업을 호출하도록 활성화해야 합니다.

Deadline Cloud 모니터는 `management.deadline.`*`region`*`.amazonaws.com`를 사용하여 대기열 및 플릿을 생성 및 수정하거나 작업, 단계 및 작업 목록을 가져오는 등 팜의 리소스를 관리합니다.

Deadline Cloud 에는 다음 AWS 서비스 엔드포인트에 대한 엔드포인트도 필요합니다.

- Deadline Cloud 는 AWS STS 를 사용하여 작업 자산에 액세스할 수 있도록 작업자를 인증합니다. 에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM의 임시 보안 자격 증명을 AWS STS참조하세요.
- 인터넷 연결이 없는 서브넷에서 고객 관리형 플릿을 설정하는 경우 작업자가 로그를 작성할 수 있도록 Amazon CloudWatch Logs에 대한 VPC 엔드포인트를 생성해야 합니다. 자세한 내용은 CloudWatch를 사용한 모니터링을 참조하세요.
- 작업 첨부 파일을 사용하는 경우 작업자가 첨부 파일에 액세스할 수 있도록 Amazon Simple Storage Service(Amazon S3)에 대한 VPC 엔드포인트를 생성해야 합니다. 자세한 내용은 의 작업 첨부 Deadline Cloud 파일을 참조하세요.

에 대한 엔드포인트 생성 Deadline Cloud

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 Deadline Cloud 사용하여 용 인터페이스 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 Deadline Cloud 사용하여에 대한 관리 및 예약 엔드포인트를 생성합니다. *`region`*을 배포한 AWS 리전 로 바꿉니다 Deadline Cloud.

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

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

Deadline Cloud 는 듀얼 스택 엔드포인트를 지원합니다.

인터페이스 엔드포인트에 대해 프라이빗 DNS를 활성화하면 기본 리전 DNS 이름을 Deadline Cloud 사용하여에 API 요청을 할 수 있습니다. 예를 들어 작업자 작업의 `scheduling.deadline.us-east-1.amazonaws.com` 경우 , 다른 모든 작업`management.deadline.us-east-1.amazonaws.com`의 경우 입니다.

또한 다음 서비스 이름을 AWS STS 사용하여에 대한 엔드포인트를 생성해야 합니다.

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

고객 관리형 플릿이 인터넷 연결 없이 서브넷에 있는 경우 다음 서비스 이름을 사용하여 CloudWatch Logs 엔드포인트를 생성해야 합니다.

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

작업 첨부 파일을 사용하여 파일을 전송하는 경우 다음 서비스 이름을 사용하여 Amazon S3 엔드포인트를 생성해야 합니다.

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

Deadline Cloud의 보안 모범 사례

AWS Deadline Cloud(Deadline Cloud)는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

> **Note**
>
> 여러 보안 주제의 중요성에 대한 자세한 내용은 공동 책임 모델을 참조하세요.

데이터 보호

데이터 보호를 위해 자격 AWS 계정 증명을 보호하고 AWS Identity and Access Management (IAM)을 사용하여 개별 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon Simple Storage Service(S3)에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.

- 명령행 인터페이스 또는 API를 통해 AWS 에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2 섹션을 참조하세요.

명칭 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마세요. 여기에는 AWS Deadline Cloud 또는 기타에서 콘솔 AWS CLI, API 또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. Deadline Cloud 또는 기타 서비스에 입력하는 모든 데이터가 진단 로그에 포함되도록 선택될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함하지 마십시오.

AWS Identity and Access Management 권한

사용자, AWS Identity and Access Management (IAM) 역할을 사용하고 사용자에게 최소 권한을 부여하여 AWS 리소스에 대한 액세스를 관리합니다. AWS 액세스 자격 증명을 생성, 배포, 교체 및 취소하기 위한 자격 증명 관리 정책 및 절차를 수립합니다. 자세한 설명은 IAM 사용자 가이드의 IAM 모범 사례 섹션을 참조하세요.

사용자 및 그룹으로 작업 실행

Deadline Cloud에서 대기열 기능을 사용하는 경우 OS 사용자에게 대기열 작업에 대한 최소 권한 권한이 있도록 운영 체제(OS) 사용자와 기본 그룹을 지정하는 것이 가장 좋습니다.

“사용자로 실행”(및 그룹)을 지정하면 대기열에 제출된 작업에 대한 모든 프로세스가 해당 OS 사용자를 사용하여 실행되고 해당 사용자의 연결된 OS 권한을 상속합니다.

플릿 및 대기열 구성이 결합되어 보안 태세를 설정합니다. 대기열 측에서 대기열 작업에 OS 및 권한을 사용하도록 '사용자로 작업 실행' 및 AWS IAM 역할을 지정할 수 있습니다. 플릿은 특정 대기열에 연결된 경우 대기열 내에서 작업을 실행하는 인프라(작업자 호스트, 네트워크, 탑재된 공유 스토리지)를 정의합니다. 작업자 호스트에서 사용할 수 있는 데이터는 하나 이상의 연결된 대기열의 작업에서 액세스해야 합니다. 사용자 또는 그룹을 지정하면 다른 대기열, 설치된 다른 소프트웨어 또는 작업자 호스트에 액세스할 수 있는 다른 사용자로부터 작업의 데이터를 보호하는 데 도움이 됩니다. 대기열에 사용자가 없는 경우 모든 대기열 사용자를 가장(sudo)할 수 있는 에이전트 사용자로 실행됩니다. 이러한 방식으로 사용자가 없는 대기열은 권한을 다른 대기열로 에스컬레이션할 수 있습니다.

네트워킹

트래픽이 가로채거나 리디렉션되지 않도록 하려면 네트워크 트래픽이 라우팅되는 방식과 위치를 보호하는 것이 중요합니다.

다음과 같은 방법으로 네트워킹 환경을 보호하는 것이 좋습니다.

- Amazon Virtual Private Cloud(Amazon VPC) 서브넷 라우팅 테이블을 보호하여 IP 계층 트래픽이 라우팅되는 방식을 제어합니다.
- Amazon Route 53(Route 53)을 팜 또는 워크스테이션 설정에서 DNS 공급자로 사용하는 경우 Route 53 API에 대한 액세스를 보호하세요.
- 온프레미스 워크스테이션 또는 기타 데이터 센터를 사용하는 AWS 등 외부에서 Deadline Cloud에 연결하는 경우 온프레미스 네트워킹 인프라를 보호합니다. 여기에는 라우터, 스위치 및 기타 네트워킹 디바이스의 DNS 서버 및 라우팅 테이블이 포함됩니다.

작업 및 작업 데이터

Deadline Cloud 작업은 작업자 호스트의 세션 내에서 실행됩니다. 각 세션은 작업자 호스트에서 하나 이상의 프로세스를 실행하므로 일반적으로 출력을 생성하려면 데이터를 입력해야 합니다.

이 데이터를 보호하기 위해 대기열을 사용하여 운영 체제 사용자를 구성할 수 있습니다. 작업자 에이전트는 대기열 OS 사용자를 사용하여 세션 하위 프로세스를 실행합니다. 이러한 하위 프로세스는 대기열 OS 사용자의 권한을 상속합니다.

이러한 하위 프로세스가 액세스를 처리하는 데이터에 대한 액세스를 보호하려면 모범 사례를 따르는 것이 좋습니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

팜 구조

다양한 방법으로 Deadline Cloud 플릿 및 대기열을 정렬할 수 있습니다. 그러나 특정 배열에는 보안에 영향을 미칩니다.

팜은 Deadline Cloud 리소스를 플릿, 대기열 및 스토리지 프로파일을 포함한 다른 팜과 공유할 수 없으므로 가장 안전한 경계 중 하나가 있습니다. 그러나 팜 내에서 외부 AWS 리소스를 공유할 수 있으므로 보안 경계가 손상됩니다.

적절한 구성을 사용하여 동일한 팜 내의 대기열 간에 보안 경계를 설정할 수도 있습니다.

다음 모범 사례에 따라 동일한 팜에 보안 대기열을 생성합니다.

- 동일한 보안 경계 내의 대기열에만 플릿을 연결합니다. 다음 사항에 유의하세요.
  - 작업자 호스트에서 작업이 실행된 후 임시 디렉터리 또는 대기열 사용자의 홈 디렉터리와 같은 데이터가 뒤쳐질 수 있습니다.

  - 작업을 제출하는 대기열에 관계없이 동일한 OS 사용자가 서비스 소유 플릿 작업자 호스트에서 모든 작업을 실행합니다.
  - 작업은 작업자 호스트에서 실행 중인 프로세스를 그대로 둘 수 있으므로 다른 대기열의 작업이 실행 중인 다른 프로세스를 관찰할 수 있습니다.
- 동일한 보안 경계 내의 대기열만 작업 연결을 위해 Amazon S3 버킷을 공유하는지 확인합니다.
- 동일한 보안 경계 내의 대기열만 OS 사용자를 공유하는지 확인합니다.
- 팜에 통합된 다른 모든 AWS 리소스를 경계에 보호합니다.

작업 연결 대기열

작업 연결은 Amazon S3 버킷을 사용하는 대기열과 연결됩니다.

- 작업 연결은 Amazon S3 버킷의 루트 접두사에 쓰고 읽습니다. `CreateQueue` API 호출에서이 루트 접두사를 지정합니다.
- 버킷에는 대기열 사용자에게 버킷 및 루트 접두사에 대한 액세스 권한을 부여하는 역할을 `Queue Role`지정하는 해당이 있습니다. 대기열을 생성할 때 작업 연결 버킷 및 루트 접두사와 함께 `Queue Role` Amazon 리소스 이름(ARN)을 지정합니다.
- `AssumeQueueRoleForRead`, `AssumeQueueRoleForUser`및 `AssumeQueueRoleForWorker` API 작업에 대한 승인된 호출은에 대한 임시 보안 자격 증명 세트를 반환합니다`Queue Role`.

대기열을 생성하고 Amazon S3 버킷과 루트 접두사를 재사용하면 권한이 없는 당사자에게 정보가 공개될 위험이 있습니다. 예를 들어 QueueA와 QueueB는 동일한 버킷과 루트 접두사를 공유합니다. 보안 워크플로에서 ArtistA는 QueueA에 액세스할 수 있지만 QueueB에는 액세스할 수 없습니다. 그러나 여러 대기열이 버킷을 공유하는 경우 ArtistA는 QueueA와 동일한 버킷 및 루트 접두사를 사용하기 때문에 QueueB 데이터의 데이터에 액세스할 수 있습니다. QueueA

콘솔은 기본적으로 안전한 대기열을 설정합니다. 대기열이 공통 보안 경계에 속하지 않는 한 대기열에 Amazon S3 버킷과 루트 접두사의 고유한 조합이 있는지 확인합니다.

대기열을 격리하려면 버킷 및 루트 접두사에 대한 대기열 액세스만 허용`Queue Role`하도록를 구성해야 합니다. 다음 예제에서는 각 `## ####` 리소스별 정보로 바꿉니다.

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

또한 역할에 대한 신뢰 정책을 설정해야 합니다. 다음 예제에서는 *## ###* 텍스트를 리소스별 정보로 바꿉니다.

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

사용자 지정 소프트웨어 Amazon S3 버킷

에 다음 문`Queue Role`을 추가하여 Amazon S3 버킷의 사용자 지정 소프트웨어에 액세스할 수 있습니다. 다음 예제에서는 *SOFTWARE_BUCKET_NAME*을 S3 버킷의 이름으로 바꿉니다.

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

Amazon S3 보안 모범 사례에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon Amazon S3 보안 모범 사례를 참조하세요.

작업자 호스트

각 사용자가 할당된 역할에 대해서만 작업을 수행할 수 있도록 작업자 호스트를 보호합니다.

작업자 호스트를 보호하려면 다음 모범 사례를 따르는 것이 좋습니다.

- 호스트 구성 스크립트를 사용하면 작업자의 보안 및 작업이 변경될 수 있습니다. 구성이 올바르지 않으면 작업자가 불안정해지거나 작동이 중지될 수 있습니다. 이러한 실패를 디버깅하는 것은 사용자의 책임입니다.

- 대기열에 제출된 작업이 동일한 보안 경계 내에 있지 않는 한 여러 대기열에 동일한 `jobRunAsUser` 값을 사용하지 마세요.
- 작업자 에이전트가 실행되는 OS 사용자의 `jobRunAsUser` 이름으로 대기열을 설정하지 마십시오.
- 대기열 사용자에게 의도한 대기열 워크로드에 필요한 최소 권한 OS 권한을 부여합니다. 에이전트 프로그램 파일 또는 기타 공유 소프트웨어를 작업할 수 있는 파일 시스템 쓰기 권한이 없는지 확인합니다.
- 의 루트 사용자Linux와의 `Administrator` 소유 계정만 Windows 소유하며 작업자 에이전트 프로그램 파일을 수정할 수 있는지 확인합니다.
- Linux 작업자 호스트에서는 작업자 에이전트 사용자가 대기열 사용자로 프로세스를 시작할 수 `/etc/sudoers` 있도록에서 `umask` 재정의를 구성하는 것이 좋습니다. 이 구성은 다른 사용자가 대기열에 기록된 파일에 액세스할 수 없도록 하는 데 도움이 됩니다.
- 신뢰할 수 있는 개인에게 작업자 호스트에 대한 최소 권한 액세스 권한을 부여합니다.
- 로컬 DNS 재정의 구성 파일(`/etc/hosts` Linux 및 Windows) 및 워크스테이션 및 작업자 호스트 운영 체제에서 테이블을 라우팅할 수 `C:\Windows\system32\etc\hosts` 있는 권한을 제한합니다.
- 워크스테이션 및 작업자 호스트 운영 체제의 DNS 구성에 대한 권한을 제한합니다.
- 운영 체제와 설치된 모든 소프트웨어를 정기적으로 패치합니다. 이 접근 방식에는 제출자, 어댑터, 작업자 에이전트, OpenJD 패키지 등과 같이 Deadline Cloud와 함께 특별히 사용되는 소프트웨어가 포함됩니다.
- Windows 대기열에 강력한 암호를 사용합니다`jobRunAsUser`.
- 대기열의 암호를 정기적으로 교체합니다`jobRunAsUser`.
- Windows 암호 보안 암호에 대한 최소 권한 액세스를 보장하고 사용하지 않는 보안 암호를 삭제합니다.
- 대기열에 향후 실행할 `jobRunAsUser` 일정 명령을 부여하지 마십시오.
  - 에서 `cron` 및에 대한 이러한 계정 액세스를 Linux거부합니다`at`.
  - 에서 Windows 작업 스케줄러에 대한 이러한 계정 액세스를 Windows거부합니다.

> **Note**
>
> 운영 체제 및 설치된 소프트웨어를 정기적으로 패치하는 것의 중요성에 대한 자세한 내용은 공동 책임 모델을 참조하세요.

호스트 구성 스크립트

- 호스트 구성 스크립트를 사용하면 작업자의 보안 및 작업이 변경될 수 있습니다. 구성이 올바르지 않으면 작업자가 불안정해지거나 작동이 중지될 수 있습니다. 이러한 실패를 디버깅하는 것은 사용자의 책임입니다.

워크스테이션

Deadline Cloud에 액세스할 수 있는 워크스테이션을 보호하는 것이 중요합니다. 이 접근 방식은 Deadline Cloud에 제출하는 모든 작업이에 청구되는 임의 워크로드를 실행할 수 없도록 하는 데 도움이 됩니다 AWS 계정.

아티스트 워크스테이션을 보호하려면 다음 모범 사례를 따르는 것이 좋습니다. 자세한 내용은 공동 책임 모델을 참조하세요.

- Deadline Cloud를 AWS포함하여 액세스를 제공하는 지속적인 자격 증명을 보호합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요.
- 신뢰할 수 있는 보안 소프트웨어만 설치합니다.
- 사용자가 자격 증명 공급자와 페더레이션하여 임시 자격 증명 AWS 으로에 액세스하도록 요구합니다.
- Deadline Cloud 제출자 프로그램 파일에 대한 보안 권한을 사용하여 변조를 방지합니다.
- 신뢰할 수 있는 개인에게 아티스트 워크스테이션에 대한 최소 권한을 부여합니다.
- Deadline Cloud Monitor를 통해 얻은 제출자 및 어댑터만 사용합니다.
- 로컬 DNS 재정의 구성 파일(`/etc/hosts` Linux 및 macOS, Windows) 및 워크스테이션 및 작업자 호스트 운영 체제에서 테이블을 라우팅할 수 `C:\Windows\system32\etc\hosts` 있는 권한을 제한합니다.
- 워크스테이션 및 작업자 호스트 운영 체제`/etc/resolve.conf`에 대한 권한을 로 제한합니다.
- 운영 체제와 설치된 모든 소프트웨어를 정기적으로 패치합니다. 이 접근 방식에는 제출자, 어댑터, 작업자 에이전트, OpenJD 패키지 등과 같이 Deadline Cloud와 함께 특별히 사용되는 소프트웨어가 포함됩니다.

다운로드한 소프트웨어의 신뢰성 확인

설치 관리자를 다운로드한 후 소프트웨어의 신뢰성을 확인하여 파일 변조를 방지합니다. 이 절차는 Windows 및 Linux 시스템 모두에서 작동합니다.

Windows

다운로드한 파일의 신뢰성을 확인하려면 다음 단계를 완료하세요.

1. 다음 명령에서를 확인하려는 파일로 *file* 바꿉니다. 예를 들어 ***C:\PATH\TO\MY\DeadlineCloudSubmitter-windows-x64-installer.exe*** 입니다. 또한 *signtool-sdk-version*를 설치된 SignTool SDK 버전으로 바꿉니다. 예를 들어 **10.0.22000.0**입니다.

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

2. 예를 들어 다음 명령을 실행하여 Deadline Cloud 제출자 설치 관리자 파일을 확인할 수 있습니다.

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

Linux

다운로드한 파일의 신뢰성을 확인하려면 gpg 명령줄 도구를 사용합니다.

1. 다음 명령을 실행하여 OpenPGP 키를 가져옵니다.

   ```
    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. OpenPGP 키를 신뢰할지 여부를 결정합니다. 위 키를 신뢰할지 여부를 결정할 때 고려해야 할 몇 가지 요소는 다음과 같습니다.

   - 이 웹 사이트에서 GPG 키를 가져오는 데 사용한 인터넷 연결은 안전합니다.
   - 이 웹 사이트에 액세스하는 디바이스는 안전합니다.
   - AWS 는이 웹 사이트에서 OpenPGP 퍼블릭 키의 호스팅을 보호하기 위한 조치를 취했습니다.

3. OpenPGP 키를 신뢰하기로 결정한 경우 다음 예와 gpg 마찬가지로에서 신뢰하도록 키를 편집합니다.

```
$ 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. Deadline Cloud 제출자 설치 프로그램 확인

   Deadline Cloud 제출자 설치 프로그램을 확인하려면 다음 단계를 완료하세요.

   a. Deadline Cloud 콘솔 다운로드 페이지로 돌아가서 Deadline Cloud 제출자 설치 프로그램의 서명 파일을 다운로드합니다.

   b. 다음을 실행하여 Deadline Cloud 제출자 설치 프로그램의 서명을 확인합니다.

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

5. Deadline Cloud 모니터 확인

> **Note**
>
> 서명 파일 또는 플랫폼별 방법을 사용하여 Deadline Cloud 모니터 다운로드를 확인할 수 있습니다. 플랫폼별 방법은 다운로드한 파일 유형에 따라 Linux (Debian) 탭, Linux (RPM) 탭 또는 Linux (AppImage) 탭을 참조하세요.

서명 파일을 사용하여 Deadline Cloud Monitor 데스크톱 애플리케이션을 확인하려면 다음 단계를 완료하세요.

a. Deadline Cloud 콘솔 다운로드 페이지로 돌아가서 해당 .sig 파일을 다운로드한 다음를 실행합니다.

.deb의 경우:

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

.rpm의 경우:

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

.AppImage의 경우:

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

b. 출력이 다음과 비슷한지 확인합니다.

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

gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

출력에 문구가 포함된 경우 서명이 성공적으로 확인되었으며 Deadline Cloud Monitor 설치 스크립트를 실행할 수 있음을 `Good signature from "AWS Deadline Cloud"`의 미합니다.

Linux (AppImage)

Linux .AppImage 바이너리를 사용하는 패키지를 확인하려면 먼저 Linux 탭에서 1~3단계를 완료한 다음 다음 단계를 완료합니다.

1. GitHub의 AppImageUpdate 페이지에서 validate-x86_64.AppImage 파일을 다운로드합니다.
2. 파일을 다운로드한 후 실행 권한을 추가하려면 다음 명령을 실행합니다.

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

3. 실행 권한을 추가하려면 다음 명령을 실행합니다.

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

4. Deadline Cloud Monitor 서명을 확인하려면 다음 명령을 실행합니다.

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

출력에 문구가 포함된 경우 서명이 성공적으로 확인되었으며 Deadline Cloud 모니터 설치 스크립트를 안전하게 실행할 수 있음을 `Validation successful`의미합니다.

Linux (Debian)

Linux .deb 바이너리를 사용하는 패키지를 확인하려면 먼저 Linux 탭에서 1~3단계를 완료합니다.

dpkg은 대부분의 debian 기반 Linux 배포에서 핵심 패키지 관리 도구입니다. 도구를 사용하여 .deb 파일을 확인할 수 있습니다.

1. Deadline Cloud 콘솔 다운로드 페이지에서 Deadline Cloud monitor .deb 파일을 다운로드합니다.
2. *<APP_VERSION>*을 확인하려는 .deb 파일의 버전으로 바꿉니다.

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

3. 출력은 다음과 유사합니다.

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

4. .deb 파일을 확인하려면 `GOODSIG`가 출력에 있는지 확인합니다.

Linux (RPM)

Linux .rpm 바이너리를 사용하는 패키지를 확인하려면 먼저 Linux 탭에서 1~3단계를 완료합니다.

1. Deadline Cloud 콘솔 다운로드 페이지에서 Deadline Cloud monitor .rpm 파일을 다운로드합니다.

2. *<APP_VERSION>*을 확인할 .rpm 파일의 버전으로 바꿉니다.

```
gpg --export --armor "Deadline Cloud" > key.pub
sudo rpm --import key.pub
rpm -K deadline-cloud-monitor-<APP_VERSION>-1.x86_64.rpm
```

3. 출력은 다음과 유사합니다.

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

4. .rpm 파일을 확인하려면 `digests signatures OK`가 출력에 있는지 확인합니다.

AWS 기한 클라우드 모니터링

모니터링은 AWS Deadline Cloud(Deadline Cloud) 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집하여 다중 지점 장애가 발생할 경우 더 쉽게 디버깅할 수 있습니다. Deadline Cloud 모니터링을 시작하기 전에 다음 질문에 대한 답변을 포함하는 모니터링 계획을 생성해야 합니다.

- 모니터링의 목표
- 모니터링할 리소스
- 이러한 리소스를 모니터링하는 빈도
- 사용할 모니터링 도구
- 모니터링 작업을 수행할 사람
- 문제 발생 시 알려야 할 대상

AWS 및 Deadline Cloud는 리소스를 모니터링하고 잠재적 인시던트에 대응하는 데 사용할 수 있는 도구를 제공합니다. 이러한 도구 중 일부는 모니터링을 자동으로 수행하며, 일부 도구는 수동 개입이 필요합니다. 모니터링 작업을 최대한 자동화해야 합니다.

- Amazon CloudWatch는 AWS 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임곗값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

  Deadline Cloud에는 세 가지 CloudWatch 지표가 있습니다.
- Amazon CloudWatch Logs로 Amazon EC2 인스턴스, CloudTrail, 기타 소스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임곗값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.
- Amazon EventBridge를 사용하여 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

- AWS CloudTrail는 AWS 계정에서 또는 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

자세한 내용은 Deadline Cloud 개발자 안내서의 다음 주제를 참조하세요.

- CloudTrail 로그
- EventBridge를 사용하여 이벤트 관리
- CloudWatch를 사용한 모니터링

에 대한 할당량 Deadline Cloud

AWS Deadline Cloud 는 작업을 처리하는 데 사용할 수 있는 팜, 플릿 및 대기열과 같은 리소스를 제공합니다. 를 생성하면 각 리소스에 대해 이러한 리소스에 대한 기본 할당량이 AWS 계정설정됩니다 AWS 리전.

Service Quotas는에 대한 할당량을 보고 관리할 수 있는 중앙 위치입니다 AWS 서비스. 사용하는 많은 리소스에 대한 할당량 증가를 요청할 수도 있습니다.

할당량을 보려면 Service Quotas 콘솔을 Deadline Cloud엽니다. 탐색 창에서 AWS 서비스을(를) 선택한 다음 Deadline Cloud을(를) 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 서비스 할당량 증가 양식을 사용합니다.

AWS 계정에는 다음과 관련된 할당량이 있습니다 Deadline Cloud.

명칭	기본값	조정 가능	설명
팜당 연결된 멤버	지원되는 각 리전: 75	아니요	현재 AWS 리전의 각 팜에 연결할 수 있는 최대 멤버 수입니다.
플릿당 연결된 멤버	지원되는 각 리전: 75	아니요	현재 AWS 리전의 각 플릿에 연결할 수 있는 최대 멤버 수입니다.
작업당 연결된 멤버	지원되는 각 리전: 75	아니요	현재 AWS 리전의 각 작업에 연결할 수 있는 최대 멤버 수입니다.
대기열당 연결된 멤버	지원되는 각 리전: 75	아니요	현재 AWS 리전의 각 대기열에 연결할 수 있는 최대 멤버 수입니다.

명칭	기본값	조정 가능	설명
팜당 예산	지원되는 각 리전: 20개	예	현재 AWS 리전의 팜당 최대 예산 수
리전당 팜	지원되는 각 지역: 2	예	현재 AWS 리전에서 생성할 수 있는 최대 팜 수입니다.
팜당 플릿	지원되는 각 리전: 5	예	현재 AWS 리전의 각 팜에 대해 생성할 수 있는 최대 플릿 수입니다.
팜당 작업	지원되는 각 리전: 100,000	예	현재 AWS 리전의 팜당 최대 작업 수입니다.
리전별 라이선스 엔드포인트	지원되는 각 리전: 5	예	현재 AWS 리전의 최대 라이선스 엔드포인트 수입니다.
라이선스 엔드포인트당 라이선스 세션	지원되는 각 리전: 500	예	현재 AWS 리전의 라이선스 엔드포인트당 최대 라이선스 세션 수입니다.
팜당 한도	지원되는 각 지역: 50	예	현재 AWS 리전의 각 팜에 대해 생성할 수 있는 최대 제한 수입니다.
리전당 모니터 수	지원되는 각 리전: 1	아니요	현재 AWS 리전의 최대 모니터 수입니다.

명칭	기본값	조정 가능	설명
리전당 OnDemand G 인스턴스 GPUs	각 지원되는 지역: 1	예	현재 AWS 리전의 모든 서비스 관리형 플릿에 프로비저닝할 수 있는 온디맨드 G 인스턴스 GPUs의 최대 수입니다.
리전당 OnDemand vCPUs	지원되는 각 지역: 50	예	현재 AWS 리전의 모든 서비스 관리형 플릿에 프로비저닝할 수 있는 온디맨드 vCPUs의 최대 수입니다.
대기열당 대기열 환경	지원되는 각 지역: 10개	아니요	현재 AWS 리전의 각 대기열에 대해 생성할 수 있는 최대 대기열 환경 수입니다.
팜당 대기열 플릿 연결	지원되는 각 리전: 100	예	현재 AWS 리전의 팜당 최대 대기열 플릿 연결 수
대기열당 대기열 제한 연결	지원되는 각 리전: 10	예	현재 AWS 리전의 각 대기열과 연결할 수 있는 최대 제한 수입니다.
팜당 대기열	지원되는 각 리전: 20개	예	현재 AWS 리전의 각 팜에 대해 생성할 수 있는 최대 대기열 수입니다.
리전당 스팟 G 인스턴스 GPUs	각 지원되는 지역: 1	예	현재 AWS 리전의 모든 서비스 관리형 플릿에 프로비저닝할 수 있는 스팟 G 인스턴스 GPUs의 최대 수입니다.

명칭	기본값	조정 가능	설명
리전당 스팟 vCPUs	지원되는 각 리전: 500	예	현재 AWS 리전의 모든 서비스 관리형 플릿에 프로비저닝할 수 있는 스팟 vCPUs의 최대 수입니다.
작업당 단계	지원되는 각 리전: 200	예	현재 AWS 리전의 작업당 최대 단계 수입니다.
범용 SSD(gp3) 볼륨을 위한 스토리지(TiB)	지원되는 각 지역: 50	예	현재 AWS 리전의 모든 플릿에서 사용할 수 있는 TiB로 측정된 EBS 스토리지의 최대 집계량입니다.
팜당 스토리지 프로필	지원되는 각 리전: 50	아니요	현재 AWS 리전의 각 팜에 대해 생성할 수 있는 스토리지 프로파일의 최대 수입니다.
작업당 작업 수	지원되는 각 리전: 10,000	예	현재 AWS 리전의 작업당 최대 작업 수입니다.
단계당 작업	지원되는 각 리전: 10,000	예	현재 AWS 리전의 단계당 최대 작업 수입니다.
팜당 작업자 수	지원되는 각 리전: 7,500	아니요	현재 AWS 리전의 팜당 최대 작업자 수입니다.

를 사용하여 AWS Deadline Cloud 리소스 생성 AWS CloudFormation

AWS Deadline Cloud는 AWS 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 리소스를 모델링하고 설정하는 데 도움이 되는 AWS CloudFormation서비스와 통합됩니다. 원하는 모든 AWS 리소스(예: 팜, 대기열, 플릿)를 설명하는 템플릿을 생성하고 해당 리소스를 AWS CloudFormation 프로비저닝하고 구성합니다.

를 사용하면 템플릿을 재사용하여 Deadline Cloud 리소스를 일관되고 반복적으로 설정할 AWS CloudFormation수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝합니다.

기한 클라우드 및 AWS CloudFormation 템플릿

Deadline Cloud 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이러한 템플릿은 AWS CloudFormation 스택에서 프로비저닝하려는 리소스를 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 Designer를 사용하여 AWS CloudFormation AWS CloudFormation 템플릿을 시작할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

Deadline Cloud는에서 팜, 대기열 및 플릿 생성을 지원합니다 AWS CloudFormation. 팜, 대기열 및 플릿에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS Deadline Cloud를 참조하세요.

에 대해 자세히 알아보기 AWS CloudFormation

에 대해 자세히 알아보려면 다음 리소스를 AWS CloudFormation참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API Reference
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

문제 해결

다음 절차와 팁은 AWS Deadline Cloud 팜 및 리소스 관련 문제를 해결하는 데 도움이 될 수 있습니다.

주제

- 사용자가 내 팜, 플릿 또는 대기열을 볼 수 없는 이유는 무엇입니까?
- 작업자가 내 작업을 선택하지 않는 이유는 무엇입니까?
- 작업자의 실행이 멈춘 이유는 무엇입니까?
- Deadline Cloud 작업 문제 해결
- 추가 리소스

사용자가 내 팜, 플릿 또는 대기열을 볼 수 없는 이유는 무엇입니까?

사용자 액세스

사용자가 Deadline Cloud 모니터에서 팜, 플릿 또는 대기열을 볼 수 없는 경우 팜 및 리소스에 대한 액세스에 문제가 있을 수 있습니다.

팜에 액세스할 수 없는 사용자는 Deadline Cloud 모니터에서 "No farms available"라는 메시지를 받습니다.

팜, 플릿 또는 대기열에 올바른 사용자 또는 그룹이 할당되었는지 확인하려면

1. AWS Deadline Cloud 콘솔에서 팜, 플릿 또는 대기열을 찾은 다음 액세스 관리를 선택합니다.
2. 그룹 탭은 기본적으로 선택됩니다. 그룹별로 권한을 할당하는 경우 그룹에 목록에 표시되고 액세스 수준이 할당되어야 합니다.

   그룹이 목록에 없는 경우 그룹 추가를 선택하여 그룹에 대한 권한을 할당합니다.
3. 사용자별로 권한을 할당하는 경우 사용자 탭을 선택합니다. 사용자에게 목록에가 표시되고 액세스 수준이 할당되어야 합니다.

   사용자가 목록에 없는 경우 사용자 추가를 선택하여 사용자에게 권한을 할당합니다.

그룹에 사용자가 할당되었는지 확인하려면

1. AWS Deadline Cloud 콘솔에서 팜, 플릿 또는 대기열을 찾은 다음 액세스 관리를 선택합니다.

2. 그룹 탭은 기본적으로 선택됩니다. 그룹 이름을 선택하여 멤버를 확인합니다.
3. 사용자가 그룹에 나열되지 않은 경우 사용자를 추가해야 합니다.

   기본 자격 증명 설정을 사용하는 경우 Identity Center 콘솔에서 그룹에 사용자를 직접 추가할 수 있습니다. Okta 또는와 같은 외부 자격 증명 공급자에 연결된 경우 자격 증명 공급자의 그룹에 사용자를 추가할 Google Workspace수 있습니다.

   > **Note**
   > 일부 외부 자격 증명 공급자는 그룹을 제외한 사용자를 Identity Center에 동기화합니다. 이 경우 그룹별로 할당하는 대신 사용자에게 직접 권한을 할당하는 것이 좋습니다.

Deadline Cloud에 대한 사용자 액세스 관리에 대한 자세한 내용은 섹션을 참조하세요Deadline Cloud에서 사용자 관리.

작업자가 내 작업을 선택하지 않는 이유는 무엇입니까?

플릿 역할 구성

작업자가 생성되었지만 초기화를 완료하지 않고 작업 작업을 시작하지 않는 경우가 있습니다. 플릿 역할이 올바르게 구성되지 않았기 때문입니다.

이 문제가 발생하고 있는지 확인하려면 CloudTrail 로그에서 액세스 거부 오류가 있는지 확인하세요. 액세스 거부 문제를 확인한 후 플릿으로 이동하여 역할 구성을 올바른 권한으로 업데이트합니다. 자세한 내용은 Deadline Cloud 개발자 안내서의 CloudTrail 로그를 참조하세요.

작업자의 실행이 멈춘 이유는 무엇입니까?

작업자가 OpenJD 환경에서 나가지 못함

작업자는 장기 실행 `envExit` 세션 작업에 멈출 수 있습니다. 이는 OpenJD 템플릿을 재정의하고 환경 종료 작업 제한 시간을 5분 이상으로 설정하는 작업 템플릿을 사용하는 경우 발생할 수 있습니다. Deadline Cloud 모니터는이 상황에서 멈춘 작업자에게 약간의 가시성을 제공하지만 연결된 대기열에서 사용 가능한 작업에 대해 `RUNNING` 작업자를 상호 참조해야 합니다.

멈춘 작업자를 찾으려면 Deadline Cloud 모니터의 모든 플릿을 살펴보고 다음 단계를 완료하세요.

1. 작업자 상태 열에서 `RUNNING` 작업자를 찾습니다.

2. 플릿 세부 정보 섹션에서 연결된 각 대기열로 이동합니다.
3. 연결된 각 대기열에서 , `READY`또는 `RUNNING`인 작업을 검색합니다`PENDING`. 연결된 모든 대기열에 해당 상태의 작업이 없는 경우 작업자는 환경 종료를 실행하고 있습니다.

이 상태에서 멈춘 작업자를 중지하려면 다음 AWS CLI 명령을 사용합니다.

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

명령을 실행한 후 프로그램이 종료되면 작업자 에이전트가 다시 시작됩니다. 그런 다음 작업자는 온라인 상태로 돌아와서 연결된 대기열에서 더 많은 작업을 실행합니다. 대기열에 5분보다 긴 환경 종료 작업 제한 시간이 있는 작업이 더 많은 경우 작업자는 다시 멈춥니다. 이 경우 더 이상 작업자가 나가지 않을 때까지이 프로세스를 반복해야 합니다.

이 문제를 방지하려면 작업 템플릿을 사용할 때 제한 시간 옵션을 5분 이하로 설정합니다.

Deadline Cloud 작업 문제 해결

AWS Deadline Cloud의 일반적인 작업 문제에 대한 자세한 내용은 다음 주제를 참조하세요.

작업 생성이 실패한 이유는 무엇입니까?

작업이 검증 검사에 실패할 수 있는 몇 가지 가능한 이유는 다음과 같습니다.

- 작업 템플릿은 OpenJD 사양을 따르지 않습니다.
- 작업에 너무 많은 단계가 포함되어 있습니다.
- 작업에 총 작업이 너무 많습니다.
- 작업을 생성할 수 없는 내부 서비스 오류가 발생했습니다.

작업의 최대 단계 및 작업 수에 대한 할당량을 보려면 Service Quotas 콘솔을 사용합니다. 자세한 내용은 에 대한 할당량 Deadline Cloud 단원을 참조하십시오.

내 작업이 호환되지 않는 이유는 무엇입니까?

작업이 대기열과 호환되지 않는 일반적인 이유는 다음과 같습니다.

- 작업이 제출된 대기열과 연결된 플릿이 없습니다. Deadline Cloud 모니터를 열고 대기열에 연결된 플릿이 있는지 확인합니다. 대기열을 보는 방법에 대한 자세한 내용은 섹션을 참조하세요Deadline Cloud에서 대기열 및 플릿 세부 정보 보기.
- 작업에 대기열과 연결된 플릿이 충족하지 않는 호스트 요구 사항이 있습니다. 확인하려면 작업 템플릿의 `hostRequirements` 항목을 팜의 플릿 구성과 비교합니다. 플릿 중 하나가 호스트 요구 사항을 충족하는지 확인합니다. 플릿 호환성에 대한 자세한 내용은 플릿 호환성 확인을 참조하세요. 플릿 구성을 보려면 섹션을 참조하세요Deadline Cloud에서 대기열 및 플릿 세부 정보 보기.

내 작업이 준비된 이유는 무엇입니까?

작업이 `READY` 상태에서 멈춘 것처럼 보이는 가능한 이유는 다음과 같습니다.

- 대기열과 연결된 플릿의 최대 작업자 수는 0으로 설정됩니다. 확인하려면 섹션을 참조하세요Deadline Cloud에서 대기열 및 플릿 세부 정보 보기.
- 대기열에 우선 순위가 더 높은 작업이 있습니다. 확인하려면 섹션을 참조하세요Deadline Cloud에서 대기열 및 플릿 세부 정보 보기.
- 고객 관리형 플릿의 경우 Auto Scaling 구성을 확인합니다. 자세한 내용은 Deadline Cloud 개발자 안내서의 Amazon EC2 Auto Scaling 그룹을 사용하여 플릿 인프라 생성을 참조하세요.

내 작업이 실패한 이유는 무엇입니까?

여러 가지 이유로 작업이 실패할 수 있습니다. 문제를 검색하려면 Deadline Cloud 모니터를 열고 실패한 작업을 선택합니다. 실패한 작업을 선택한 다음 해당 작업에 대한 로그를 확인합니다. 지침은 Deadline Cloud에서 세션 및 작업자 로그 보기 섹션을 참조하세요.

- 소프트웨어에 유효한 라이선스가 없어서 라이선스 오류가 발생하거나 워터마크가 발생하는 경우 작업자가 필요한 라이선스 서버에 연결할 수 있는지 확인합니다. 자세한 내용은 Deadline Cloud 개발자 안내서의 고객 관리형 플릿을 라이선스 엔드포인트에 연결을 참조하세요.
- 마지막 세션 작업 메시지 또는 프로세스 종료 코드는 작업이 실패한 이유에 대한 정보를 제공할 수 있습니다. 를 사용 중Windows이고 종료 코드가 음수인 경우 종료 코드의 서명되지 않은 버전을 검색해 보십시오.

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

내 단계가 보류 중인 이유는 무엇입니까?

하나 이상의 종속성이 완료되지 않은 경우 단계가 `PENDING` 상태로 유지될 수 있습니다. Deadline Cloud 모니터를 사용하여 종속성의 상태를 확인할 수 있습니다. 지침은 Deadline Cloud에서 단계 보기 섹션을 참조하세요.

추가 리소스

GitHub에서 추가 정보와 리소스를 찾을 수 있습니다.

Deadline Cloud 사용 설명서의 문서 기록

다음 표에서는 AWS Deadline Cloud 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	날짜
AWS 관리형 정책 업데이트	기존 AWS AWSDeadlineCloud-WorkerHost 관리형 정책을 업데이트했습니다. 자세한 내용은 AWS Deadline Cloud에 대한 관리형 정책을 참조하세요.	2025년 5월 30일
Adobe After Effects 제출자 설치 프로그램	디지털 콘텐츠 생성 소프트웨어에 Adobe After Effects 제출자 설치 프로그램을 추가하기 위한 지침이 추가되었습니다. 자세한 내용은 Adobe After Effects를 참조하세요.	2025년 2월 13일
문제 해결	Deadline Cloud 문제 해결에 대한 정보가 추가되었습니다. 자세한 설명은 문제 해결을 참조하십시오.	2025년 2월 7일
작업 리소스 제한	새 작업 리소스 제한 및 최대 작업자 호스트 수에 대한 설명서가 추가되었습니다. 자세한 내용은 작업에 대한 리소스 제한 생성을 참조하세요.	2025년 1월 30일
Adobe After Effects UBL	Deadline Cloud용 Adobe After Effects 사용 기반 라이선스(UBL)에 대한 정보가 추가되었습니다. 자세한 내용은 라이선	2025년 1월 30일

	스 엔드포인트에 연결을 참조하세요.	
사용 설명서의 재구성된 콘텐츠	개발자 중심 콘텐츠를 사용 설명서에서 개발자 안내서로 이동했습니다. • 개발자 안내서의 고객 관리형 플릿 생성 지침을 새로운 고객 관리형 플릿 장으로 이동했습니다. • 자체 라이선스 사용에 대한 정보를 개발자 안내서의 새로운 소프트웨어 라이선스 사용 장으로 이동했습니다. • CloudTrail, CloudWatch CloudWatch 및 EventBridge를 사용한 모니터링에 대한 세부 정보를 개발자 안내서의 모니터링 장으로 이동했습니다.	2025년 1월 6일
예산 임계값 이벤트	새 예산 임계값 EventBridge 이벤트가 추가되었습니다. 자세한 내용은 Deadline Cloud 이벤트 세부 정보 참조를 참조하세요.	2024년 10월 30일
작업 상태 이벤트	새 작업 및 작업 상태 EventBridge 이벤트를 추가했습니다. 자세한 내용은 Deadline Cloud 이벤트 세부 정보 참조를 참조하세요.	2024년 10월 24일

작업 다시 제출	작업을 다시 제출하는 방법에 대한 정보가 추가되었습니다. 자세한 내용은 작업 다시 제출을 참조하세요.	2024년 10월 7일
AWS 관리형 정책 업데이트	기존 AWS 관리형 정책을 업데이트했습니다. 자세한 내용은 AWS Deadline Cloud에 대한 관리형 정책을 참조하세요.	2024년 10월 7일
자체 라이선스 사용	Deadline Cloud에서 자체 라이선스 서버 또는 라이선스 프록시 인스턴스를 사용하는 방법에 대한 정보가 추가되었습니다. 자세한 내용은 서비스 관리형 플릿을 참조하세요.	2024년 7월 26일
Autodesk 3ds Max UBL	Deadline Cloud의 Autodesk 3ds Max 사용량 기반 라이선스(UBL)에 대한 정보가 추가되었습니다. 자세한 내용은 라이선스 엔드포인트에 연결을 참조하세요.	2024년 6월 18일
모니터링 및 비용 관리 기능	EventBridge를 사용하여 Deadline Cloud에서 모니터링을 지원할 수 있습니다. 자세한 내용은 EventBridge 이벤트에 대한 작업을 참조하세요. Deadline Cloud는 작업 비용을 제어하고 시각화하는 데 도움이 되는 예산과 사용량 탐색기를 제공합니다. 이러한 비용을 관리하는 데 도움이 되는 몇 가지 모범 사례에 대해 알아봅니다. 자세한 내용은 비용 관리를 참조하세요.	2024년 5월 23일

최초 릴리스	Deadline Cloud 사용 설명서의 최초 릴리스입니다.	2024년 4월 2일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.