



使用者指南

AWS 截止日期雲端



版本 latest

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 截止日期雲端: 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是截止日期雲端？	1
截止日期雲端的功能	1
概念和術語	2
陣列資源	2
任務執行資源	3
其他重要概念和術語	4
截止日期雲端入門	5
存取截止日期雲端	6
相關服務	6
截止日期雲端的運作方式	7
截止日期雲端中的許可	7
使用截止日期雲端的軟體支援	8
管道整合	8
什麼是管道整合？	8
具有陣列的內部部署 Studio 範例 AWS	9
開始使用	11
設定您的 AWS 帳戶	11
設定您的陣列基礎設施	12
建立您的監視器	12
定義陣列詳細資訊	14
定義佇列詳細資訊	15
定義機群詳細資訊	16
Review and create (檢閱和建立)	17
設定您的工作站	17
步驟 1：安裝截止日期雲端提交者	17
步驟 2：安裝和設定截止日期雲端監視器	21
步驟 3：啟動截止日期雲端提交者	25
使用監視器	27
共用截止日期雲端監視器 URL	27
開啟截止日期雲端監視器	28
變更您的語言設定	29
提交任務套件	30
檢視佇列和機群詳細資訊	30
管理任務、步驟和任務	31

檢視任務詳細資訊	32
封存任務	33
將任務排入佇列	33
重新提交任務	33
檢視步驟	34
檢視任務	34
檢視工作階段和工作者日誌	35
檢視工作者儀表板	36
使用案例	37
下載已完成的輸出	38
陣列	40
建立陣列	40
佇列	41
建立佇列	41
建立佇列環境	42
預設conda佇列環境	43
關聯佇列和機群	47
停止佇列機群關聯	47
重新啟用佇列機群關聯	48
機群	49
服務受管機群	49
建立 SMF	49
使用 GPU 加速器	51
軟體授權	52
VFX 平台	52
AMI 軟體內容	53
客戶管理的機群	56
管理使用者	58
了解您的身分來源	58
使用 建立使用者 IAM Identity Center 目錄	59
使用外部 IdP 管理使用者	60
了解存取層級	61
存取層級許可矩陣	61
成員繼承	62
指派許可	63
任務	66

使用提交者	66
共用任務設定索引標籤	68
任務特定設定索引標籤	70
任務附件索引標籤	71
主機需求索引標籤	72
處理任務	73
監控任務	73
支援的軟體	77
Adobe After Effects	77
支援概觀	77
After Effects 版本相容性	78
開始使用	78
使用 After Effects 提交者	79
進階組態。	80
截止日期雲端 Conda 頻道	80
開放原始碼資源	80
Autodesk 3ds Max	81
支援概觀	81
3ds Max 版本相容性	81
3ds 與其他數位內容建立工具的最大差異	82
開始使用	82
進階組態。	82
3ds Max 渲染器	83
開放原始碼資源	83
Autodesk Maya	83
支援概觀	84
Maya 版本相容性	84
開始使用	84
進階組態。	85
Maya 轉譯引擎	85
Maya 外掛程式	86
截止日期雲端 Conda 頻道	87
開放原始碼資源	88
Autodesk VRED	88
支援概觀	88
VRED 版本相容性	89

要求	89
開始使用	89
進階組態	90
截止日期雲端 Conda 頻道	90
開放原始碼資源	90
Blender	91
支援概觀	91
Blender 版本相容性	91
開始使用	92
使用 Blender 提交器	92
進階組態。	92
Blender 轉譯引擎	93
截止日期雲端 Conda 頻道	93
開放原始碼資源	94
Epic Unreal 引擎	94
支援概觀	94
Unreal Engine 版本相容性	95
開始使用	95
使用 Unreal Engine 提交者	96
進階組態。	96
Unreal Engine 轉譯功能	97
截止日期雲端 Conda 頻道	97
開放原始碼資源	97
Foundry Nuke	98
支援概觀	98
Nuke 版本相容性	98
開始使用	98
使用 Nuke 提交者	99
進階組態。	100
Nuke 合成功能	101
截止日期雲端 Conda 頻道	101
開放原始碼資源	101
KeyShot Studio	102
支援概觀	102
KeyShot 版本相容性	102
開始使用	102

使用 KeyShot 提交者	103
進階組態。	103
截止日期雲端 Conda 頻道	104
開放原始碼資源	104
Maxon Cinema 4D	104
支援概觀	104
電影 4D 版本相容性	105
開始使用	105
進階組態。	106
Cinema 4D 外掛程式	106
截止日期雲端 Conda 頻道	107
開放原始碼資源	108
SideFX Houdini	108
支援概觀	109
Houdini 版本相容性	109
開始使用	110
使用 Houdini 提交者	110
進階組態。	110
Houdini 轉譯引擎	111
截止日期雲端 Conda 頻道	111
開放原始碼資源	112
儲存	113
儲存設定檔	113
對於共用檔案系統	115
對於任務附件	116
任務附件	117
任務連接 S3 儲存貯體的加密	118
取代任務附件儲存貯體	119
管理 S3 儲存貯體中的任務附件	120
虛擬檔案系統	120
自動下載	122
追蹤支出和用量	140
成本假設	140
使用預算控制成本	141
先決條件	141
開啟截止日期雲端預算管理工具	142

建立預算	142
檢視預算	143
編輯預算	143
停用預算	144
使用 EventBridge 事件監控預算	144
追蹤用量和成本	145
先決條件	145
開啟用量總管	145
使用用量總管	145
成本管理	148
成本管理最佳實務	149
安全	151
資料保護	151
靜態加密	152
傳輸中加密	153
金鑰管理	153
網際網路流量隱私權	162
選擇退出	163
身分和存取權管理	163
目標對象	164
使用身分驗證	164
使用政策管理存取權	165
Deadline Cloud 如何與 IAM 搭配使用	167
身分型政策範例	171
AWS 受管政策	180
服務角色	184
疑難排解	196
法規遵循驗證	198
恢復能力	198
基礎設施安全性	198
組態與漏洞分析	199
預防跨服務混淆代理人	199
AWS PrivateLink	201
考量事項	201
Deadline Cloud 端點	201
建立端點	202

受限的網路環境	203
AWS 要允許清單的 API 端點	203
要允許清單的 Web 網域	203
要允許清單的環境特定端點	204
安全最佳實務	205
資料保護	205
IAM 許可	206
以使用者和群組身分執行任務	206
聯網	206
任務資料	206
陣列結構	207
任務連接佇列	207
自訂軟體儲存貯體	210
工作者主機	210
主機組態指令碼	211
工作站	212
驗證下載的軟體	212
監控	219
配額	221
AWS CloudFormation 資源	225
截止日期雲端和 CloudFormation 範本	225
進一步了解 CloudFormation	225
疑難排解	226
為什麼使用者看不到我的陣列、機群或佇列？	226
使用者存取	226
為什麼工作者沒有挑選我的任務？	227
機群角色組態	227
為什麼我的工作停滯在執行中？	227
工作者停滯退出 OpenJD 環境	227
對任務執行故障診斷	228
為什麼建立我的任務失敗？	228
為什麼我的任務不相容？	229
為什麼我的任務卡在 中？	229
為什麼我的任務失敗？	229
為什麼我的步驟待定？	230
其他資源	230

版本備註	231
AWS 詞彙表	239
.....	ccxi

什麼是AWS截止日期雲端？

Deadline Cloud 是 AWS 服務，可讓您直接從數位內容建立管道和工作站，在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上建立和管理轉譯專案和任務。

Deadline Cloud 提供主控台介面、本機應用程式、命令列工具和 API。使用截止日期雲端，您可以建立、管理和監控陣列、機群、任務、使用者群組和儲存。您也可以指定硬體功能、為特定工作負載建立環境，並將生產所需的內容建立工具整合到您的截止日期雲端管道。

Deadline Cloud 提供統一的界面，可在單一位置管理所有轉譯專案。您可以管理使用者、指派專案給他們，以及授予任務角色的許可。

主題

- [截止日期雲端的功能](#)
- [截止日期雲端的概念和術語](#)
- [截止日期雲端入門](#)
- [存取截止日期雲端](#)
- [相關服務](#)
- [截止日期雲端的運作方式](#)
- [將截止日期雲端整合到您的管道](#)

截止日期雲端的功能

以下是 Deadline Cloud 可協助您執行和管理視覺化運算工作負載的一些關鍵方式：

- 快速建立您的陣列、佇列和機群。監控其狀態，並深入了解陣列和任務的操作。
- 集中管理截止日期雲端使用者和群組，並指派許可。
- 使用 管理專案使用者和外部身分提供者的登入安全性AWS IAM Identity Center。
- 使用 AWS Identity and Access Management(IAM) 政策和角色安全地管理對專案資源的存取。
- 使用標籤來組織和快速尋找專案資源。
- 管理專案資源用量和預估的專案成本。
- 提供廣泛的運算管理選項，以支援雲端或現場渲染。

截止日期雲端的概念和術語

為了協助您開始使用 AWS 截止日期雲端，本主題說明其一些重要概念和術語。

陣列資源

此圖表顯示截止日期雲端陣列資源如何一起運作。

伺服器陣列

陣列包含與提交和執行任務相關的所有其他資源。陣列彼此獨立，因此有助於分隔生產環境。

佇列

佇列會保留在相關聯機群上排程的任務。使用者可以將任務提交至佇列，並在佇列中管理其優先順序和狀態。佇列必須與具有佇列機群關聯的機群相關聯，才能執行其任務，而且佇列可以與多個機群相關聯。

機群

機群包含執行中任務的運算容量。機群可以是服務受管或客戶受管。服務受管機群會在截止日期雲端中執行，並包含內建功能，例如自動擴展、授權和軟體存取。客戶受管機群會在您自己的運算資源上執行，例如 Amazon EC2 執行個體或內部部署伺服器。

Budget

預算會設定任務活動的花費閾值，並可讓您在達到閾值時採取動作，例如停止任務排程。

佇列環境

佇列環境會定義在每個工作者上執行的指令碼，以設定或銷毀工作負載環境。它們適用於設定環境變數、安裝軟體和設定資產儲存。

儲存設定檔

儲存設定檔是一組主機和工作站的組態，可告知資料位於檔案系統上的位置。截止日期雲端使用儲存描述檔，在不同設定的主機上執行任務時映射路徑，例如從提交 Windows 並在 Linux 上執行的任務。

限制

限制可讓您追蹤共用資源的使用情況，例如浮動授權，並控制任務之間的配置方式。限制與具有佇列限制關聯的佇列相關聯。

監控

監視器會設定截止日期雲端監視器 Web 應用程式的 URL，讓使用者能夠監控和管理任務。它可以在瀏覽器中或透過截止日期雲端監控桌面應用程式存取。

任務執行資源

此圖表顯示截止日期雲端任務資源如何一起運作。

任務

任務是一組工作，使用者提交至 Deadline Cloud 以排程並在可用的工作者上執行。任務可能會轉譯 3D 場景或執行模擬。任務是從可重複使用的任務範本建立的，這些範本會定義執行期環境和程序，以及任務特定的參數。任務包含定義要執行之工作的步驟和任務，而且可以設定優先順序、工作者計數上限和重試設定。

任務優先順序

任務優先順序是截止日期雲端在佇列中處理任務的大致順序。您可以設定 1 到 100 之間的任務優先順序，優先順序較高的任務通常會先處理。具有相同優先順序的任務會依收到的順序處理。

任務屬性

任務屬性是您在提交轉譯任務時定義的設定。一些範例包括影格範圍、輸出路徑、任務附件、可轉譯攝影機等。屬性會根據提交轉譯的 DCC 而有所不同。

步驟

步驟是任務的一部分，提供執行許多相同任務的範本，但任務參數值除外。步驟可以對其他步驟具有相依性，可讓您建立具有循序或平行執行路徑的複雜工作流程。在轉譯任務中，步驟通常會定義轉譯影格的命令，並使用影格編號做為任務參數。

任務

任務是截止日期雲端中最小的工作單位。任務是步驟的一部分，由工作者執行，代表需要在任務中執行的個別操作。任務可以使用特定參數設定，並根據其功能和可用性指派給工作者。在轉譯任務中，任務通常會轉譯單一影格。

工作程序

工作者是機群的一部分，並從任務執行任務。工作者可以設定特定功能，例如 GPU 加速器、CPU 架構和作業系統。在服務受管機群中，隨著機群向外和向內擴展，會自動建立工作者。

執行個體

機群使用 CPU 資源的執行個體。執行個體是 Amazon EC2 效能執行個體。Deadline Cloud 使用隨需執行個體和 Spot 執行個體。

隨需執行個體

隨需執行個體會以秒計價，沒有長期承諾，而且不會中斷。

Spot 執行個體

Spot 執行個體是以折扣價格使用的未預留容量，但可能會因為隨需請求而中斷。

等待並儲存

「等待和儲存」功能以較低的成本提供延遲的任務排程，並且可以被隨需和 Spot 請求中斷。Wait and Save 僅適用於截止日期雲端服務受管機群。

Wait and Save 是在 AWS 截止日期雲端中管理視覺運算工作負載的執行。如需詳細資訊，請參閱 [AWS 服務條款](#)。

Session (工作階段)

工作階段代表工作者在任務上的工作順序。在單一工作階段期間，工作者可能會被指派多個任務，其會逐一執行。工作階段通常具有設定動作，可在執行任務動作之前設定環境和載入資產。

工作階段動作

工作階段動作代表工作階段期間執行的特定操作，例如設定環境、執行任務和同步資產。

其他重要概念和術語

用量總管

用量總管是截止日期雲端監視器的一項功能。它提供成本和用量的預估值。

預算管理員

Budget Manager 是截止日期雲端監視器的一部分。使用預算管理員來建立和管理預算。您也可以使用它來限制活動以保持在預算內。

截止日期雲端用戶端程式庫

開放原始碼用戶端程式庫包含用於管理截止日期雲端的命令列界面和程式庫。功能包括根據開放任務描述規格將任務套件提交至截止日期雲端、下載任務連接輸出，以及使用命令列界面 (CLI) 監控您的陣列。

數位內容建立應用程式 (DCC)

數位內容建立應用程式 (DCCs) 是您建立數位內容的第三方產品。Deadline Cloud 內建與許多 DCCs 的整合，例如 Autodesk Maya、Blender 和 Maxon Cinema 4D，可讓您從 DCC 內提交任務，並在具有預先設定軟體和授權的服務受管機群上進行轉譯。

任務附件

任務連接是一種截止日期雲端功能，您可以在紋理、3D 模型和照明裝備等任務中上傳和下載資產。任務附件存放在 Amazon S3 中，並避免共用網路儲存的需求。

任務範本

任務範本會定義執行時間環境，以及做為截止日期雲端任務一部分執行的所有程序。

截止日期雲端提交者

截止日期雲端提交者是 DCC 的外掛程式，可讓使用者輕鬆地從 DCC 內提交任務。

授權端點

授權端點可讓 Deadline Cloud 在 VPC 內提供第三方產品的用量型授權。此模型會依您的進度付費，而且會向您收取使用時數和分鐘數的費用。授權端點未連線到陣列，可以獨立使用。

Tags (標籤)

標籤是您可以指派給 AWS 資源的標籤。每個標籤都包含您定義的索引鍵和選用值。您可以使用標籤，以不同的方式分類 AWS 資源，例如依用途、擁有者或環境。

以用量為基礎的授權 (UBL)

以用量為基礎的授權 (UBL) 是一種隨需授權模式，可供特定第三方產品使用。此模型是按您的用量付費，而且您需要支付使用時數和分鐘數的費用。

截止日期雲端入門

使用截止日期雲端快速建立具有預設設定和資源的轉譯陣列，例如 Amazon EC2 執行個體組態和 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

您也可以在建建立轉譯陣列時定義設定和資源。相較於使用預設設定和資源，此方法需要更多時間，但可讓您擁有更多控制權。

熟悉截止日期雲端 [概念和術語](#) 後，請參閱 [建立陣列、新增使用者和實用資訊連結的逐步說明入門](#)。step-by-step

存取截止日期雲端

您可以透過下列任何方式存取截止日期雲端：

- 截止日期雲端主控台 – 在瀏覽器中存取主控台以建立陣列及其資源，並管理使用者存取。如需詳細資訊，請參閱 [入門](#)。
- 截止日期雲端監控 – 管理您的轉譯任務，包括更新優先順序和任務狀態。監控您的陣列並檢視日誌和任務狀態。對於具有擁有者許可的使用者，截止日期雲端監視器也提供探索用量和建立預算的存取權。Deadline Cloud Monitor 可作為 Web 瀏覽器和桌面應用程式使用。
- AWSSDK 和AWS CLI – 使用 AWS Command Line Interface(AWS CLI) 從本機系統的命令列呼叫截止日期雲端 API 操作。如需詳細資訊，請參閱 [設定開發人員工作站](#)。

相關服務

Deadline Cloud 適用於下列項目AWS 服務：

- Amazon CloudWatch – 透過 CloudWatch，您可以監控專案和相關聯的AWS資源。如需詳細資訊，請參閱《截止日期雲端開發人員指南》中的 [使用 CloudWatch 進行監控](#)。
- Amazon EC2 – 這AWS 服務提供在雲端執行應用程式的虛擬伺服器。您可以設定專案為工作負載使用 Amazon EC2 執行個體。如需詳細資訊，請參閱 [Amazon EC2 執行個體](#)。
- Amazon EC2 Auto Scaling – 使用 Auto Scaling，您可以隨著對執行個體的需求變更，自動增加或減少執行個體的數量。Auto Scaling 有助於確保您執行所需的執行個體數量，即使執行個體失敗也一樣。如果您啟用 Auto Scaling with Deadline Cloud，Auto Scaling 啟動的執行個體會自動向工作負載註冊。同樣地，Auto Scaling 終止的執行個體會自動從工作負載取消註冊。如需詳細資訊，請參閱 [《Amazon EC2 Auto Scaling 使用者指南》](#)。
- AWS PrivateLink– AWS PrivateLink提供虛擬私有雲端 (VPCs) AWS 服務和內部部署網路之間的私有連線，而不會將您的流量暴露到公有網際網路。AWS PrivateLink可讓您輕鬆地跨不同帳戶和VPCs連接服務。如需詳細資訊，請參閱[AWS PrivateLink](#)。
- Amazon S3 – Amazon S3 是一種物件儲存服務。Deadline Cloud 使用 Amazon S3 儲存貯體來存放任務附件。如需詳細資訊，請參閱 [Amazon S3 使用者指南](#)。
- IAM Identity Center – IAM Identity Center 是 AWS 服務，可讓您從單一位置為使用者提供所有指派帳戶和應用程式的單一登入存取權。您也可以集中管理您 中所有帳戶的多帳戶存取和使用者許可 AWS Organizations。如需詳細資訊，請參閱 [AWS IAM Identity Center 常見問答集](#)。

截止日期雲端的運作方式

透過截止日期雲端，您可以直接從數位內容建立 (DCC) 管道和工作站建立和管理渲染專案和任務。

您可以使用 AWSSDK、AWS Command Line Interface(AWS CLI) 或 Deadline Cloud 任務提交者，將任務提交至 Deadline Cloud。Deadline Cloud 支援任務範本規格的 Open Job Description (OpenJD)。如需詳細資訊，請參閱 GitHub 網站上的[開啟任務描述](#)。

Deadline Cloud 提供任務提交者。任務提交者是一種 DCC 外掛程式，用於從第三方 DCC 介面提交轉譯任務，例如 Maya 或 Nuke。透過提交者，藝術家可以將渲染任務從第三方界面提交至 Deadline Cloud，其中會管理專案資源並監控任務，全部都在一個位置。

透過截止日期雲端陣列，您可以建立佇列和機群、管理使用者，以及管理專案資源用量和成本。陣列由佇列和機群組成。佇列是已提交任務所在的位置，並排定轉譯。機群是一組工作者節點，可執行任務以完成任務。佇列必須與機群相關聯，以便任務可以轉譯。單一機群可以支援多個佇列，而多個機群可以支援佇列。

任務由步驟組成，每個步驟由特定任務組成。使用截止日期雲端監視器，您可以存取任務、步驟和任務的狀態、日誌和其他故障診斷指標。

截止日期雲端中的許可

Deadline Cloud 支援下列項目：

- 使用 AWS Identity and Access Management(IAM) 管理對其 API 操作的存取
- 使用與整合來管理人力資源使用者的存取AWS IAM Identity Center

在任何人都可以處理專案之前，他們必須能夠存取該專案和相關聯的陣列。Deadline Cloud 已與 IAM Identity Center 整合，以管理人力資源身分驗證和授權。使用者可以直接新增至 IAM Identity Center，也可以將許可連線到現有的身分提供者 (IdP)，例如 Okta 或 Active Directory。IT 管理員可以將存取許可授予不同層級的使用者和群組。每個後續關卡都包含先前關卡的許可。下列清單說明從最低層級到最高層級的四個存取層級：

- 檢視器 – 檢視其可存取之陣列、佇列、機群和任務中資源的許可。檢視器無法提交或變更任務。
- 貢獻者 – 與檢視器相同，但具有將任務提交至佇列或陣列的許可。
- 管理員 – 與參與者相同，但有權編輯他們有權存取之佇列中的任務，並授予他們有權存取之資源的許可。
- 擁有者 – 與管理員相同，但可以檢視和建立預算並查看用量。

Note

這些許可不會讓使用者存取 AWS 管理主控台或 修改截止日期雲端基礎設施的許可。

使用者必須能夠存取陣列，才能存取相關聯的佇列和機群。使用者存取權會分別指派給陣列中的佇列和機群。

您可以將使用者新增為個人或群組的一部分。將群組新增至陣列、機群或佇列可讓您更輕鬆地管理大量人員的存取許可。例如，如果您有一個團隊正在處理特定專案，您可以將每個團隊成員新增至群組。然後，您可以將存取權授予對應陣列、機群或佇列的整個群組。

使用截止日期雲端的軟體支援

Deadline Cloud 適用於可從命令列界面執行並使用參數值控制的任何軟體應用程式。Deadline Cloud 支援將工作描述為任務的 OpenJD 規格，其軟體指令碼步驟會參數化（例如跨影格範圍）為任務。將 OpenJD 任務指示與 Deadline Cloud 工具和功能整合到任務套件中，以從第三方軟體應用程式建立、執行和授權步驟。

任務需要授權才能轉譯。Deadline Cloud 為一系列軟體應用程式授權提供以 usage-based-licensing (UBL)，這些授權會根據用量以小時為單位遞增計費。使用截止日期雲端，您也可以視需要使用自己的軟體授權。如果任務無法存取授權，則不會轉譯並產生在截止日期雲端監視器的任務日誌中顯示的錯誤。

將截止日期雲端整合到您的管道

您可以將現有的轉譯管道與 AWS 截止日期雲端整合，以簡化工作流程管理和任務提交程序。

什麼是管道整合？

Deadline Cloud 的管道整合是指 Deadline Cloud Farm 如何為您的互動式和自動化工作流程提供批次處理。此範例使用視覺化效果管道，您可以適應操作員在其工作流程中使用的應用程式和程序。

視覺效果管道包含後製階段，可處理輸入影像素材、3D 模型、動畫、紋理、照明、渲染影像等。它會指定不同部門如何交換資產來執行他們負責的任務。精心設計的管道有助於有效地為電視節目或類似節目建立最終影像。

透過將截止日期雲端陣列整合到您的管道中，您可以將長時間執行的任務卸載至佇列，並排定截止日期雲端在工作者主機機群上排程任務的優先順序。您可以使用由服務管理的機群，也可以在內部部署或上建立自己的機群 AWS。

若要建立管道整合，請考慮下列因素：

- 您的資產資料存放在何處，以及如何將它們提供給陣列中的工作者主機？
- 您的任務需要哪些應用程式和外掛程式，以及如何將它們佈建到陣列中的工作者主機？
- 當藝術家或其他運算子有任務要執行時，他們將如何將其提交到陣列？
- 誰將監控任務的進度和狀態，以及如何控制成本並最佳化工作者主機的使用率？

具有 陣列的內部部署 Studio 範例 AWS

此範例著重於一個管道，其中藝術家在現場部署一起工作，並將任務提交到 上的陣列 AWS 進行轉譯。此處提供的方法可快速加入截止日期雲端，並提供靈活的自訂起點。

以下是此範例 Studio 管道整合的因素：

- 資產資料存放在內部部署辦公室的 NAS 共用檔案系統上。
 - 在 Windows 上，專案會掛載至 P：磁碟機，而公用程式則會掛載至 X：。
 - 在 macOS 上，專案會掛載到 /Volumes/Projects 和公用程式會掛載到 /Volumes/Utilities。
- 它們使用 Maya 進行 3D 建模、使用 Arnold 進行轉譯，以及使用 Nuke 進行合成。這些應用程式中未安裝任何自訂外掛程式。
- 他們想要使用預設提交體驗。
- 藝術家將監控自己的任務，製作者將監控成本並視需要調整優先順序。

此 Studio 的管道整合使用任務附件，在 Studio 內部部署之間來回傳輸資料 AWS，因為使用很容易，並且可以擴展到大型機群。佇列上設定的任務會連接 S3 儲存貯體，做為內部部署 NAS 和工作者主機之間的快取層 AWS。

當藝術家從 Maya 或 Nuke 提交任務時，截止日期雲端整合提交者會掃描場景，以識別任務執行所需的檔案，然後將它們上傳到 S3 以連接到任務。高效能雜湊用於識別工作室中任何藝術家先前上傳的檔案。如此一來，當藝術家反覆提交相同鏡頭的新版本，或某個藝術家將鏡頭遞交給另一個藝術家時，只需要在提交任務的過程中上傳新的或修改的檔案。

Studio 同時使用 Windows 和 macOS 工作站，因此它們會針對其專案和公用程式磁碟機，使用本機類型的檔案系統位置來設定儲存設定檔。如需詳細資訊，請參閱[任務連接主題的儲存描述](#)檔，了解當任務在與提交任務不同的作業系統上執行時，如何支援必要的路徑映射。他們也會設定其網路上的 Linux 主機，以便在任務完成時自動下載佇列中所有任務的輸出。若要了解如何設定，請參閱[自動下載任務附件](#)。

陣列包含兩個Linux服務受管機群，其 vCPUs和 RAM 需求設定為從 Studio 工作所需的最低規格開始的範圍。其中一個機群設定為提供少量 Spot 執行個體，以在工作時間內提供一致的轉譯容量，另一個機群設定為等待並儲存，以在離峰時間以較低的成本轉譯更多任務。所有 Maya、Maya for Arnold 外掛程式和 Nuke 都適用於來自截止日期雲端 conda 頻道Linux的服務受管機群，以及以用量為基礎的授權。為了節省應用程式安裝的額外負荷，他們會將 Deadline Cloud 主控台中為佇列設定的預設 conda 環境取代為[具有改善快取的 github 範例 conda 佇列環境](#)。

為了支援任務提交，他們會在每個工作站上[設定截止日期雲端提交者](#)，選取 Maya 和 Nuke 整合。使用截止日期雲端監視器，他們可以登入陣列、監控任務進度，以及檢視日誌輸出以診斷問題。Maya 和 Nuke 提交者都具有整合對話方塊，可在應用程式界面內提交任務。

在陣列中[設定使用者存取層級](#)時，它們可讓 Contributor 存取藝術家，讓他們可以提交任務、檢視所有任務，以及修改自己的任務屬性。它們可讓管理員存取轉譯 Wrangler，以便修改所有任務的屬性。它們可讓擁有者存取生產者，以便透過建立預算[和探索用量成本來追蹤支出](#)和用量。

截止日期雲端入門

若要在 AWS 截止日期雲端中建立陣列，您可以使用[截止日期雲端主控台](#)或 AWS Command Line Interface (AWS CLI)。使用 主控台以取得建立陣列的引導式體驗，包括佇列和機群。使用 AWS CLI 直接使用 服務，或開發可搭配截止日期雲端使用的自有工具。

若要建立陣列並使用截止日期雲端監視器，請為截止日期雲端設定您的帳戶。您只需要為每個帳戶設定一次截止日期雲端監控基礎設施。您可以從您的陣列管理專案，包括使用者存取您的陣列及其資源。

若要建立資源最少的陣列以接受任務，請在主控台首頁中選取快速入門。會[設定截止日期雲端監視器](#)逐步引導您完成這些步驟。這些陣列從佇列和自動關聯的機群開始。這種方法是建立沙盒樣式陣列以供實驗的便利方法。

主題

- [設定您的 AWS 帳戶](#)
- [設定截止日期雲端監視器](#)
- [設定您的工作站](#)

設定您的 AWS 帳戶

設定您的 AWS 帳戶 以使用 AWS 截止日期雲端。

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

當您第一次建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。

Important

強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

設定截止日期雲端監視器

若要開始使用，您需要建立截止日期雲端陣列基礎設施，包括監視器、佇列和機群。您也可以執行其他選用步驟，包括新增群組和使用者、選擇服務角色，以及將標籤新增至資源。

步驟 1：建立監視器

Deadline Cloud Monitor 使用 AWS IAM Identity Center 授權使用者。根據預設，您用於 Deadline Cloud 的 IAM Identity Center 執行個體必須與 AWS 區域監視器位於相同的區域中。不過，如果您在 IAM Identity Center 中啟用了多區域支援，則可以在不同區域中建立監視器。如需詳細資訊，請參閱[什麼是 AWS IAM Identity Center](#)。如果您的主控台在建立監視器時使用不同的區域，您會收到變更為 IAM Identity Center 區域的提醒。

您的監視器基礎設施包含下列元件：

- **監視器名稱：**監視器名稱是識別監視器的方式，例如 AnyCompany 監視器。您的監視器名稱也會決定您的監視器 URL。
- **監控 URL：**您可以使用監控 URL 存取您的監控。URL 是以監控名稱為基礎，例如 `https://anycompanymonitor.awsapps.com`。
- **AWS 區域：**AWS 區域是 AWS 資料中心集合的實體位置。當您設定監視器時，區域預設為離您最近的位置。建議您變更區域，讓它最接近您的使用者。這可減少延遲並改善資料傳輸速度。根據預設，AWS IAM Identity Center 必須在與截止日期雲端 AWS 區域相同的區域中啟用，除非您已在 IAM Identity Center 中啟用多區域支援。如需詳細資訊，請參閱[什麼是 AWS IAM Identity Center](#)。

Important

在完成設定截止日期雲端之後，您無法變更您的區域。

完成本節中的任務，以設定監視器的基礎設施。

設定監視器的基礎設施

1. 登入 AWS 管理主控台以開始歡迎使用截止日期雲端設定，然後選擇下一步。
2. 輸入監控名稱 — 例如 **AnyCompany Monitor**。
3. (選用) 若要變更監控 URL，請選擇編輯 URL。
4. (選用) 若要變更，AWS 區域使其最接近您的使用者，請選擇變更區域。
 - a. 選取最接近您使用者的 區域。
 - b. 選擇套用區域。
5. (選用) 若要進一步自訂監視器設定，請選取 [其他設定](#)。
6. 如果您已準備好使用 [步驟 2：定義陣列詳細資訊](#)，請選擇下一步。

其他設定

截止日期雲端設定包含其他設定。透過這些設定，您可以檢視 Cloud 設定對所做的所有變更 AWS 帳戶、設定監視器使用者角色，以及變更加密金鑰類型。

AWS IAM Identity Center

AWS IAM Identity Center 是以雲端為基礎的單一登入服務，用於管理使用者和群組。IAM Identity Center 也可以與您的企業單一登入 (SSO) 提供者整合，讓使用者可以使用其公司帳戶登入。

Deadline Cloud 預設會啟用 IAM Identity Center，而且需要設定和使用 Deadline Cloud。根據預設，您用於 Deadline Cloud 的 IAM Identity Center 執行個體必須與 AWS 區域 監視器位於相同的 中。不過，如果您在 IAM Identity Center 中啟用了多區域支援，則可以在不同區域中建立監視器。如需詳細資訊，請參閱[什麼是 AWS IAM Identity Center](#)。

設定服務存取角色

AWS 服務可以擔任服務角色來代表您執行動作。Deadline Cloud 需要監視器使用者角色，才能讓使用者存取監視器中的資源。

您可以將 AWS Identity and Access Management (IAM) 受管政策連接至監控使用者角色。這些政策提供使用者執行特定動作的許可，例如在特定截止日期雲端應用程式中建立任務。由於應用程式取決於受管政策中的特定條件，因此如果您不使用受管政策，應用程式可能無法如預期般執行。

完成設定後，您可以隨時變更監控使用者角色。如需使用者角色的詳細資訊，請參閱 [IAM 角色](#)。

下列索引標籤包含兩個不同使用案例的說明。若要建立和使用新的服務角色，請選擇新增服務角色索引標籤。若要使用現有的服務角色，請選擇現有的服務角色索引標籤。

New service role

建立和使用新的服務角色

1. 選取建立並使用新的服務角色。
2. (選用) 輸入服務使用者角色名稱。
3. 如需角色的詳細資訊，請選擇檢視許可詳細資訊。

Existing service role

使用現有的服務角色

1. 選取使用現有的服務角色。
2. 開啟下拉式清單以選擇現有的服務角色。
3. (選用) 選擇在 IAM 主控台中檢視，以取得角色的詳細資訊。

步驟 2：定義陣列詳細資訊

返回截止日期雲端主控台，完成下列步驟以定義陣列詳細資訊。

1. 在陣列詳細資訊中，新增陣列的名稱。
2. 在描述中，輸入陣列描述。描述可協助您識別陣列的用途。
3. 建立群組並為您的陣列新增使用。設定陣列之後，您可以使用截止日期雲端管理主控台來新增或變更群組和使用者。
4. (選用) 選擇其他陣列設定。
 - a. (選用) 根據預設，您的資料會使用金鑰進行加密，該金鑰為安全性而 AWS 擁有和管理。您可以選擇自訂加密設定 (進階) 以使用現有金鑰，或建立您管理的新金鑰。

如果您選擇使用核取方塊自訂加密設定，請輸入 AWS KMS ARN，或 AWS KMS 選擇建立新的 KMS 金鑰來建立新的。

- b. (選用) 選擇新增標籤，將一或多個標籤新增至您的陣列。
5. 請選擇下列其中一個選項：

- 選取略過以檢閱和建立以[檢閱和建立您的陣列](#)。
- 選取下一步以繼續其他選用步驟。

(選用) 步驟 3：定義佇列詳細資訊

佇列負責追蹤任務的進度 and 排程工作。

1. 從佇列詳細資訊開始，提供佇列的名稱。
2. 針對描述，輸入佇列描述。明確的描述可協助您快速識別佇列的用途。
3. 對於任務連接，您可以建立新的 Amazon S3 儲存貯體或選擇現有的 Amazon S3 儲存貯體。如果您沒有現有的 Amazon S3 儲存貯體，則需要建立一個儲存貯體。
 - a. 若要建立新的 Amazon S3 儲存貯體，請選取建立新的任務儲存貯體。您可以在根字首欄位中定義任務儲存貯體的名稱。我們建議您呼叫儲存貯體 **deadlinecloud-job-attachments-[QUEUE_NAME]**。

您只能使用小寫字母和破折號。不可使用空格或特殊字元。
 - b. 若要搜尋並選取現有的 Amazon S3 儲存貯體，請選取從現有的 Amazon S3 儲存貯體中選擇。然後，選擇瀏覽 S3 來搜尋現有的儲存貯體。顯示可用的 Amazon S3 儲存貯體清單時，選取您要用於佇列的 Amazon S3 儲存貯體。
4. (選用) 選擇其他陣列設定。
 - a. 如果您使用的是客戶受管機群，請選取啟用與客戶受管機群的關聯。
 - i. 對於客戶管理的機群，新增佇列設定的使用者，然後設定 POSIX 和/或 Windows 登入資料。或者，您可以選取核取方塊來略過執行身分功能。
 - ii. 如果您想要設定佇列的預算，請選擇需要此佇列的預算。如果您需要預算，您必須使用截止日期雲端主控台來建立預算，以排程佇列中的任務。
 - b. 您的佇列需要代表您存取 Amazon S3 的許可。我們建議您為每個佇列建立新的服務角色。
 - i. 對於新角色，請完成下列步驟。
 - A. 選取建立並使用新的服務角色。
 - B. 輸入佇列角色的角色名稱，或使用提供的角色名稱。
 - C. (選用) 新增佇列角色描述。
 - D. 您可以選擇檢視許可詳細資訊，以檢視佇列角色的 IAM 許可。

- ii. 或者，您可以選取現有的服務角色。
- c. (選用) 使用名稱和值對為佇列環境新增環境變數。
- d. (選用) 使用金鑰和值對為佇列新增標籤。

請選擇下列其中一個選項：

- 選取略過以檢閱和建立以[檢閱和建立您的陣列](#)。
- 選取下一步以繼續其他選用步驟。

(選用) 步驟 4：定義機群詳細資訊

機群會配置工作者來執行轉譯任務。如果您需要用於轉譯任務的機群，請勾選建立機群的方塊。

1. 機群詳細資訊

- a. 為您的機群提供名稱和選用的描述。
- b. 檢閱機群類型和作業系統的意識。

- 2. 在執行個體市場類型區段中，選擇 Spot、隨需或等待並儲存執行個體。Amazon EC2 隨需執行個體提供更快的可用性，Amazon EC2 Spot 和 Wait and Save 執行個體更適合節省成本。
- 3. 對於自動擴展機群中的執行個體數量，請選擇執行個體數量下限和執行個體數量上限。

我們強烈建議一律將執行個體數量下限設定為 0，以避免產生額外費用。

- 4. 檢閱工作者的意識功能。

5. (選用) 選擇其他機群設定

- a. 您的機群需要代表您寫入 CloudWatch 的許可。我們建議您為每個機群建立新的服務角色。
 - i. 對於新角色，請完成下列步驟。
 - A. 選取建立並使用新的服務角色。
 - B. 輸入機群角色的角色名稱，或使用提供的角色名稱。
 - C. (選用) 新增機群角色描述。
 - D. 若要檢視機群角色的 IAM 許可，請選擇檢視許可詳細資訊。
 - ii. 或者，您可以使用現有的服務角色。
- b. (選用) 使用金鑰和值對為機群新增標籤。

輸入所有機群詳細資訊後，請選擇下一步。

步驟 4：檢閱和建立

檢閱輸入的資訊以建立您的陣列。當您準備好時，請選擇建立陣列。

您陣列建立的進度會顯示在陣列頁面上。當您的陣列可供使用時，會顯示成功訊息。

設定您的工作站

此程序適用於想要安裝、設定和啟動 AWS 截止日期雲端提交者的管理員和藝術家。截止日期雲端提交者是數位內容建立 (DCC) 外掛程式。藝術家使用它從他們熟悉的第三方 DCC 界面提交任務。

Note

此程序必須在藝術家將用於提交轉譯的所有工作站上完成。

每個工作站必須先安裝 DCC，才能安裝對應的提交者。例如，如果您想要下載的截止日期雲端提交者 Blender，您需要 Blender 已在工作站上安裝。

我們提供合理的預設值，以確保工作站的安全。如需保護工作站的詳細資訊，請參閱[安全最佳實務 - 工作站](#)。

主題

- [步驟 1：安裝截止日期雲端提交者](#)
- [步驟 2：安裝和設定截止日期雲端監視器](#)
- [步驟 3：啟動截止日期雲端提交者](#)

步驟 1：安裝截止日期雲端提交者

下列各節會引導您完成安裝截止日期雲端提交者的步驟。

Note

Unreal Engine：Unreal Engine 提交者不包含在標準安裝程式中，並且需要單獨的設定程序。如需安裝說明，請參閱 [Unreal Engine Submitter 設定指南](#)。

下載提交者安裝程式

您必須先下載提交者安裝程式，才能安裝截止日期雲端提交者。

- 為您的作業系統下載提交者安裝程式：

[適用於 Windows 的下載](#)

[下載 Linux 版本](#)

[下載適用於 MacOS \(arm64\)](#)

- (選用) [驗證下載軟體的真實性](#)。

安裝截止日期雲端提交者

使用安裝程式，您可以安裝下列提交者：

軟體	支援的版本	Windows 安裝程式	Linux 安裝程式	MacOS (arm64) 安裝程式
Adobe After Effects	2024 - 2025	包含	不包含	包含
Autodesk 3ds Max	2024 - 2026	包含	不包含	不包含
Autodesk Arnold for Cinema 4D	4.8.4.1	包含	不包含	包含
適用於 Maya 的 Autodesk Arnold	7.1 - 7.4	包含	包含	包含
Autodesk Maya	2023 - 2026	包含	包含	包含
Autodesk VRED	2025 - 2026	包含	不包含	不包含
Blender	3.6 - 5.0	包含	包含	包含
適用於 Maya 的 Chaos V-Ray	6 - 7	包含	包含	包含
Foundry Nuke	15 - 16	包含	包含	包含

軟體	支援的版本	Windows 安裝程式	Linux 安裝程式	MacOS (arm64) 安裝程式
KeyShot Studio	2023 - 2025	包含	不包含	包含
Maxon Cinema 4D	2024 - 2026	包含	不包含	包含
Maya 的 Maxon Redshift	2025-2026	包含	包含	包含
SideFX Houdini	19.5 - 21.0	包含	包含	包含

Note

Unreal Engine : Unreal Engine 提交者不包含在標準安裝程式中，並且需要單獨的設定程序。如需安裝說明，請參閱 [Unreal Engine Submitter 設定指南](#)。

Windows

- 在檔案瀏覽器中，導覽至安裝程式下載的資料夾，然後選取 `DeadlineCloudSubmitter-windows-x64-installer.exe`。
 - 如果 Windows 保護您的 PC 快顯視窗，請選擇更多資訊。
 - 無論如何，選擇執行。
- AWS 在截止日期雲端提交者設定精靈開啟後，選擇下一步。
- 完成下列其中一個步驟，以選擇安裝範圍：
 - 若要僅針對目前使用者安裝，請選擇使用者。
 - 若要為所有使用者安裝，請選擇系統。

如果您選擇系統，您必須結束安裝程式，並完成下列步驟，以管理員身分重新執行它：

- 在上按一下滑鼠右鍵 **DeadlineCloudSubmitter-windows-x64-installer.exe**，然後選擇以管理員身分執行。
- 輸入您的管理員登入資料，然後選擇是。
- 選擇安裝範圍的系統。

4. 選取安裝範圍後，選擇下一步。
5. 再次選擇下一步以接受安裝目錄。
6. 選取 的整合式提交者Nuke，或您要安裝的任何提交者。
7. 選擇下一步。
8. 檢閱安裝，然後選擇下一步。
9. 再次選擇下一步，然後選擇完成。

Linux

Note

適用於 的 Deadline Cloud 整合Nuke安裝程式Linux和 Deadline Cloud Monitor 只能安裝在至少具有 GLIBC 2.31 的Linux分發上。

1. 開啟終端機視窗。
2. 若要執行安裝程式的系統安裝，請輸入 命令 `sudo -i`，然後按 Enter 以成為根。
3. 導覽至您下載安裝程式的位置。

例如 `cd /home/USER/Downloads`。

4. 若要讓安裝程式可執行檔，請輸入 `chmod +x DeadlineCloudSubmitter-linux-x64-installer.run`。
5. 若要執行截止日期雲端提交者安裝程式，請輸入 `./DeadlineCloudSubmitter-linux-x64-installer.run`。
6. 安裝程式開啟時，請依照畫面上的提示完成設定精靈。

macOS (arm64)

1. 在檔案瀏覽器中，導覽至安裝程式下載的資料夾，然後選取檔案。
2. AWS 在截止日期雲端提交者設定精靈開啟後，選擇下一步。
3. 再次選擇下一步以接受安裝目錄。
4. 選取 的整合式提交者Maya，或您要安裝的任何提交者。
5. 選擇下一步。

6. 檢閱安裝，然後選擇下一步。
7. 再次選擇下一步，然後選擇完成。

步驟 2：安裝和設定截止日期雲端監視器

您可以使用 Windows、Linux 或 安裝截止日期雲端監控桌面應用程式 macOS。

Windows

1. 下載適用於 的截止日期雲端監視器安裝程式 Windows：

[下載適用於 Windows 的截止日期雲端監視器](#)

2. 執行下載的安裝程式，並依照提示完成安裝。

若要執行無提示安裝，請使用下列命令：

```
DeadlineCloudMonitor_x64-setup.exe /S
```

根據預設，監視器會安裝在 `C:\Users{username}\AppData\Local\DeadlineCloudMonitor`。若要變更安裝目錄，請改用此命令：

```
DeadlineCloudMonitor_x64-setup.exe /S /D={InstallDirectory}
```

Linux (Applmage)

在 Debian distros 上安裝 Deadline Cloud Monitor Applmage

1. 下載截止日期雲端監視器 Applmage：

[下載截止日期雲端監視器 \(Applmage\)](#)

- 2.

 Note

此步驟適用於 Ubuntu 22 及更高版本。對於其他版本的 Ubuntu，請略過此步驟。

若要安裝 `libfuse2`，請輸入：

```
sudo apt update
```

```
sudo apt install libfuse2
```

- 若要讓 AppImage 可執行檔成為可執行檔，請輸入：

```
chmod a+x deadline-cloud-monitor_amd64.AppImage
```

Linux (Debian)

在 Debian distros 上安裝 Debian 套件的截止日期雲端監視器

- 下載 Deadline Cloud Monitor Debian 套件：

[下載截止日期雲端監視器 \(.deb\)](#)

-

Note

此步驟適用於 Ubuntu 22 及更高版本。對於其他版本的 Ubuntu，請略過此步驟。

若要安裝 libssl1.1，請輸入：

```
wget https://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
```

- 若要安裝 Deadline Cloud Monitor Debian 套件，請輸入：

```
sudo apt update  
sudo apt install ./deadline-cloud-monitor_amd64.deb
```

- 如果在具有未滿足相依性的套件上安裝失敗，請修正中斷的套件，然後執行下列命令。

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

Linux (RPM)

在 Rocky Linux 9 或 上安裝截止日期雲端監視器 RPM Alma Linux 9

Note

Rocky Linux 9 根據預設，和 Alma Linux 9 會使用 OpenSSL 3.0，但不包含程式 `libssl.so.1.1` 庫。您必須安裝 `compat-openssl11` 套件，讓 Deadline Cloud Monitor 執行。

1. 下載截止日期雲端監視器 RPM：

[下載截止日期雲端監視器 \(.rpm\)](#)

2. 新增儲存 Enterprise Linux 9 庫的額外套件：

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

3. 安裝 `compat-openssl11` 做為 `libssl.so.1.1` 相依性：

```
sudo dnf install compat-openssl11 deadline-cloud-monitor.x86_64.rpm
```

在 上安裝截止日期雲端監視器 RPM Red Hat Linux 9

Note

Red Hat Linux 9 預設使用 OpenSSL 3.0，不包含程式 `libssl.so.1.1` 庫。您必須安裝 `compat-openssl11` 套件，讓 Deadline Cloud Monitor 執行。

1. 下載截止日期雲端監視器 RPM：

[下載截止日期雲端監視器 \(.rpm\)](#)

2. 啟用儲存 CodeReady Linux Builder 庫：

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

3. 安裝 的額外套件 Enterprise RPM：

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

4. 安裝 compat-openssl11 做為 libssl.so.1.1 相依性：

```
sudo dnf install compat-openssl11 deadline-cloud-monitor.x86_64.rpm
```

在 Rocky Linux 8、Alma Linux 8 或 上安裝截止日期雲端監視器 RPM Red Hat Linux 8

1. 下載截止日期雲端監視器 RPM：

[下載截止日期雲端監視器 \(.rpm\)](#)

2. 安裝截止日期雲端監視器：

```
sudo dnf install deadline-cloud-monitor.x86_64.rpm
```

macOS (arm64)

1. 下載適用於 的截止日期雲端監視器安裝程式 macOS：

[下載適用於 macOS 的截止日期雲端監視器 \(arm64\)](#)

2. 開啟下載的檔案。視窗顯示時，選取並拖曳截止日期雲端監視器圖示至應用程式資料夾。

完成下載後，您可以驗證下載軟體的真實性。您可能想要這樣做，以確保下載程序期間或之後沒有人竄改檔案。請參閱步驟 1 [驗證下載軟體的真實性](#) 中的。

下載截止日期雲端監視器並驗證真實性之後，請使用下列程序來設定截止日期雲端監視器。

設定截止日期雲端監視器

1. 開啟截止日期雲端監視器。
2. 出現建立新設定檔的提示時，請完成下列步驟。
 - a. 在 URL 輸入中輸入您的監視器 URL，看起來像 **https://MY-MONITOR.deadlinecloud.amazonaws.com/**
 - b. 輸入設定檔名稱。

c. 選擇建立設定檔。

您的設定檔已建立，您的登入資料現在會與使用您建立之設定檔名稱的任何軟體共用。

3. 建立截止日期雲端監視器設定檔後，您無法變更設定檔名稱或工作室 URL。如果您需要進行變更，請改為執行下列動作：
 - a. 刪除設定檔。在左側導覽窗格中，選擇截止日期雲端監視器 > 設定 > 刪除。
 - b. 使用您想要的變更建立新的設定檔。
4. 從左側導覽窗格中，使用 >截止日期雲端監控選項來執行下列動作：
 - 變更截止日期雲端監視器設定檔以登入不同的監視器。
 - 啟用自動登入，這樣您就不必在後續開啟截止日期雲端監視器時輸入您的監視器 URL。
5. 關閉截止日期雲端監控視窗。它會繼續在背景執行，並啟用其他截止日期雲端工具來存取您的轉譯陣列。
6. 對於您計劃用於轉譯專案的每個數位內容建立 (DCC) 應用程式，請完成以下步驟：
 - a. 從您的截止日期雲端提交者中，開啟截止日期雲端工作站組態。
 - b. 在工作站組態中，選取您在截止日期雲端監視器中建立的設定檔。您的截止日期雲端登入資料現在已與此 DCC 共用，您的工具應如預期般運作。

步驟 3：啟動截止日期雲端提交者

下列範例示範如何安裝 Blender 提交器。您可以使用類似的步驟安裝其他提交者。

在 中啟動截止日期雲端提交者 Blender

Note

支援Blender使用服務受管機群conda的環境提供。如需詳細資訊，請參閱[預設conda佇列環境](#)。

1. 打開 Blender。
2. 在轉譯功能表中，選擇提交至 AWS 截止日期雲端。
 - a. 如果系統提示您安裝 GUI 相依性，請選擇確定，然後截止日期雲端提交者對話方塊將很快出現。

- b. 如果您尚未在截止日期雲端提交者中驗證，登入資料狀態會顯示為 NEEDS_LOGIN。
 - c. 選擇 Login (登入)。系統會提示您在瀏覽器中使用使用者登入資料登入。
 - d. 您現在已登入，登入資料狀態顯示為 AUTHENTICATED。
3. 選擇提交。

現在您的任務已提交至截止日期雲端陣列，並由相容的機群處理。如需如何在監視器中檢視任務進度的資訊，請參閱[使用監視器](#)。

使用截止日期雲端監視器

AWS Deadline Cloud Monitor 為您提供視覺化運算任務的整體檢視。您可以使用它來監控和管理任務、檢視機群上的工作者活動、追蹤預算和用量，以及下載任務的結果。

每個佇列都有一個任務監控器，可顯示任務、步驟和任務的狀態。監視器提供直接從監視器管理任務的方法。您可以進行優先順序變更、取消任務、重新排入佇列任務，以及重新提交任務。

截止日期雲端監視器具有顯示任務摘要狀態的資料表，或者您可以選擇任務以查看詳細的任務日誌，以協助對任務的問題進行故障診斷。

您可以使用截止日期雲端監視器，將結果下載到建立任務時指定的工作站位置。

Deadline Cloud Monitor 也可協助您監控用量和管理成本。如需詳細資訊，請參閱[追蹤截止日期雲端陣列的支出和用量](#)。

主題

- [共用截止日期雲端監視器 URL](#)
- [開啟截止日期雲端監視器](#)
- [提交任務套件](#)
- [在截止日期雲端中檢視佇列和機群詳細資訊](#)
- [在截止日期雲端中管理任務、步驟和任務](#)
- [在截止日期雲端中檢視和管理任務詳細資訊](#)
- [在截止日期雲端中檢視步驟](#)
- [在截止日期雲端中檢視任務](#)
- [在截止日期雲端中檢視工作階段和工作員日誌](#)
- [在工作員儀表板中檢視工作員詳細資訊](#)
- [在截止日期雲端中下載完成的輸出](#)

共用截止日期雲端監視器 URL

當您設定截止日期雲端服務時，預設會建立 URL，以開啟您帳戶的截止日期雲端監視器。使用此 URL 在瀏覽器或桌面上開啟監視器。與其他使用者共用 URL，以便他們可以存取截止日期雲端監視器。

您必須先授予使用者存取權，使用者才能開啟截止日期雲端監視器。若要授予存取權，請將使用者新增至監視器的授權使用者清單，或將其新增至可存取監視器的群組。如需詳細資訊，請參閱[在截止日期雲端中管理使用者](#)。

共用監視器 URL

1. 開啟[截止日期雲端主控台](#)。
2. 從入門中，選擇前往截止日期雲端儀表板。
3. 在導覽窗格中，選擇 Dashboard (儀表板)。
4. 在帳戶概觀區段中，選擇帳戶詳細資訊。
5. 複製 URL，然後安全地將 URL 傳送給需要存取截止日期雲端監視器的任何人。

開啟截止日期雲端監視器

您可以透過下列任何方式開啟截止日期雲端監視器：

- 主控台 – 登入 AWS 管理主控台 並開啟截止日期雲端主控台。
- Web – 前往您在設定截止日期雲端時建立的監視器 URL。
- Monitor – 使用桌面截止日期雲端監視器。

當您使用 主控台時，您必須能夠 AWS 使用 AWS Identity and Access Management 身分登入，然後使用 AWS IAM Identity Center 憑證登入監視器。如果您只有 IAM Identity Center 登入資料，則必須使用監視器 URL 或桌面應用程式登入。

開啟截止日期雲端監視器 (Web)

1. 使用瀏覽器，開啟您在設定截止日期雲端時建立的監控 URL。
2. 使用您的 使用者登入資料登入。

開啟截止日期雲端監視器 (主控台)

1. 開啟[截止日期雲端主控台](#)。
2. 在導覽窗格中，選取陣列。
3. 選取陣列，然後選擇管理任務以開啟截止日期雲端監控頁面。
4. 使用您的 使用者登入資料登入。

開啟截止日期雲端監視器（桌面）

1. 開啟[截止日期雲端主控台](#)。

-或-

從監視器 URL 開啟截止日期雲端監視器 - Web。

2.
 - 在截止日期雲端主控台上，執行下列動作：
 1. 在監視器中，選擇前往截止日期雲端儀表板，然後從左側選單中選擇下載。
 2. 從截止日期雲端監視器中，選擇桌面的監視器版本。
 3. 選擇 Download (下載)。
 - 在截止日期雲端監視器 - Web 上，執行下列動作：
 - 從左側選單中，選擇工作站設定。如果看不到工作站設定項目，請使用箭頭開啟左側選單。
 - 選擇 Download (下載)。
 - 從選取作業系統中，選擇您的作業系統。
3. 下載截止日期雲端監視器 - 桌面。
4. 下載並安裝監視器後，請在電腦上開啟監視器。
 - 如果這是您第一次開啟截止日期雲端監視器，您必須提供監視器 URL 並建立設定檔名稱。接著，使用截止日期雲端登入資料登入監視器。
 - 建立設定檔之後，您可以透過選取設定檔來開啟監視器。您可能需要輸入您的截止日期雲端登入資料。

變更您的語言設定

建立並開啟截止日期雲端監視器後，您可以變更語言設定。根據預設，監控語言會設定為您系統的語言設定。

從截止日期雲端監視器（桌面）變更您的語言設定

1. 從使用者設定檔中，選取設定，然後選擇語言。
2. 從下拉式選單中選取其中一種可用的語言。
3. 確認您選擇的語言是列出的選項，然後選擇確認並套用以套用變更。

監視器重新整理後，會以選擇的語言顯示。

變更語言設定後，這是開啟時的預設值，並保持預設值，直到您再次變更或解除安裝桌面應用程式為止。

若要變更 Web 上的截止日期雲端監控語言，請在瀏覽器設定中變更偏好的語言。

Note

如果您的瀏覽器或作業系統設定為截止日期雲端不支援的語言，英文會成為截止日期雲端監視器的預設語言。

提交任務套件

您可以直接從 AWS 截止日期雲端監控桌面應用程式提交任務套件。任務套件是目錄，其中包含將任務提交至截止日期雲端所需的檔案和資訊。如需範例任務套件，請參閱 GitHub 上的 [deadline-cloud-samples](#) 儲存庫。

提交任務套件

- 在截止日期雲端監控桌面應用程式中，選擇檔案、提交任務套件。此功能不適用於 Linux Appliance 或 MacOS x64 組建。

在截止日期雲端中檢視佇列和機群詳細資訊

您可以使用截止日期雲端監視器來檢視陣列中佇列和機群的組態。您也可以使用監視器來查看佇列中的任務清單或機群中的工作者。

您必須具有檢視佇列和機群詳細資訊的VIEWING許可。如果詳細資訊未顯示，請聯絡您的管理員以取得正確的許可。

檢視佇列詳細資訊

- [開啟截止日期雲端監視器](#)。
- 從陣列清單中，選擇包含您感興趣的佇列的陣列。
- 在佇列清單中，選擇佇列以顯示其詳細資訊。若要比較兩個或多個佇列的組態，請選取多個核取方塊。

4. 若要查看佇列中的任務清單，請從佇列清單或詳細資訊面板中選擇佇列名稱。

如果監視器已開啟，您可以從左側導覽窗格中的佇列清單中選擇佇列。

檢視機群詳細資訊

1. [開啟截止日期雲端監視器](#)。
2. 從陣列清單中，選擇包含您感興趣的機群的陣列。
3. 在陣列資源中，選擇機群。
4. 在機群清單中，選擇要顯示其詳細資訊的機群。若要比較兩個或多個機群的組態，請選取多個核取方塊。
5. 若要查看機群中的工作者清單，請從機群清單或詳細資訊面板中選擇機群名稱。

如果監視器已開啟，您可以從左側導覽窗格中的機群清單中選擇機群。

在截止日期雲端中管理任務、步驟和任務

當您選取佇列時，截止日期雲端監視器的任務監控區段會顯示該佇列中的任務、任務中的步驟，以及每個步驟中的任務。選取任務、步驟或任務時，您可以使用動作功能表來管理每個任務。

若要開啟任務監視器，請依照步驟在 [中檢視佇列](#) [在截止日期雲端中檢視佇列和機群詳細資訊](#)，然後選取要使用的任務、步驟或任務。

對於任務、步驟和任務，您可以執行下列動作：

- 將狀態變更為已排入佇列、成功、失敗或取消。
- 從任務、步驟或任務下載已處理的輸出。
- 複製任務、步驟或任務的 ID。

對於選取的任務，您可以：

- 封存任務。
- 修改任務屬性，包括名稱、描述、優先順序或工作者計數上限。
- 檢視步驟 以步驟相依性。
- 使用任務的參數檢視其他詳細資訊。

- 重新提交任務。

如需詳細資訊，請參閱 [在截止日期雲端中檢視和管理任務詳細資訊](#)。

對於每個步驟，您可以：

- 檢視步驟的相依性。步驟的相依性必須在步驟執行之前完成。

如需詳細資訊，請參閱 [在截止日期雲端中檢視步驟](#)。

對於每個任務，您可以：

- 檢視任務的日誌。
- 檢視任務參數。

如需詳細資訊，請參閱 [在截止日期雲端中檢視任務](#)。

在截止日期雲端中檢視和管理任務詳細資訊

截止日期雲端監視器中的任務監控頁面為您提供下列項目：

- 任務進度的整體檢視。
- 組成任務的步驟和任務檢視。

從清單中選擇任務，以檢視任務的步驟清單，然後從步驟清單中選擇步驟，以檢視任務的任務。選擇項目之後，您可以使用該項目的動作功能表來檢視詳細資訊。

檢視任務詳細資訊

1. 依照步驟在 中檢視佇列 [在截止日期雲端中檢視佇列和機群詳細資訊](#)。
2. 在導覽窗格中，選取您提交任務的佇列。
3. 使用下列其中一種方法選取任務：
 - a. 從任務清單中，選取任務以檢視其詳細資訊。
 - b. 在搜尋欄位中，輸入與任務相關聯的任何文字，例如建立任務的任務名稱或使用者。從顯示的結果中，選取您要檢視的任務。

任務的詳細資訊包括任務中的步驟和每個步驟中的任務。您可以使用動作功能表來執行下列動作：

- 變更任務的狀態。
- 檢視和修改任務的屬性。
 - 您可以檢視任務中步驟之間的相依性。
 - 您可以變更佇列中任務的優先順序。優先順序較高的任務會在優先順序較低的任務之前處理。任務的優先順序可以介於 1 到 100 之間。當兩個任務具有相同的優先順序時，會先排程最舊的任務。
- 檢視提交任務時所設定任務的參數。
- 下載任務的輸出。當您下載任務的輸出時，它會包含任務中步驟和任務所產生的所有輸出。

封存任務

若要封存任務，其必須處於終端狀態、SUSPENDED、FAILED SUCCEEDED或 CANCELED。狀態為最終ARCHIVED狀態。任務封存後，就無法重新排入佇列或修改。

封存任務不會影響任務的資料。達到非作用中逾時時，或刪除包含任務的佇列時，就會刪除資料。

封存任務發生的其他情況：

- 封存的任務會在截止日期雲端監視器中隱藏。
- 在刪除之前，封存的任務會以唯讀狀態在截止日期雲端 CLI 中顯示 120 天。

將任務排入佇列

當您將任務排入佇列時，所有沒有步驟相依性的任務都會切換到 READY。具有相依性的步驟的狀態會在還原PENDING時切換到 READY或。

- 所有任務、步驟和任務都會切換到 PENDING。
- 如果步驟沒有相依性，則會切換到 READY。

重新提交任務

有時候，您可能想要再次執行任務，但使用不同的屬性和設定。例如，您可以提交任務以轉譯測試影格的子集、驗證輸出，然後使用完整的影格範圍再次執行任務。若要這樣做，請重新提交任務。

當您重新提交任務時，沒有相依性的新任務會變成 READY。具有相依性的新任務會變成 PENDING。

- 所有新任務、步驟和任務都會變成 PENDING。
- 如果新步驟沒有相依性，則會變成 READY。

當您重新提交任務時，您只能變更在第一次建立任務時定義為可設定的屬性。例如，如果任務名稱在第一次提交時未定義為任務的可設定屬性，則無法在重新提交時編輯名稱。

在截止日期雲端中檢視步驟

使用 AWS 截止日期雲端監視器來檢視處理任務中的步驟。在任務監控中，步驟清單會顯示組成所選任務的步驟清單。當您選取步驟時，任務清單會顯示步驟中的任務。

檢視步驟

1. 請依照 中的步驟 [在截止日期雲端中檢視和管理任務詳細資訊](#) 來檢視任務清單。
2. 從 Jobs (任務) 清單中選擇一項任務。
3. 從步驟清單中選取步驟。

您可以使用動作功能表來執行下列動作：

- 變更步驟的狀態。
- 下載 步驟的輸出。當您下載步驟的輸出時，它包含步驟中任務產生的所有輸出。
- 檢視步驟的相依性。相依性資料表顯示必須在所選步驟開始之前完成的步驟清單，以及等待此步驟完成的步驟清單。

在截止日期雲端中檢視任務

使用 AWS 截止日期雲端監視器來檢視處理任務中的任務。在任務監控中，任務清單會顯示組成步驟清單中所選步驟的任務。

檢視任務

1. 請依照 中的步驟 [在截止日期雲端中檢視和管理任務詳細資訊](#) 來檢視任務清單。
2. 從 Jobs (任務) 清單中選擇一項任務。
3. 從步驟清單中選取步驟。
4. 從任務清單中選取任務。

您可以使用動作功能表來執行下列動作：

- 變更任務的狀態。
- 檢視任務日誌。如需詳細資訊，請參閱[在截止日期雲端中檢視工作階段和工作者日誌](#)。
- 檢視建立任務時設定的參數。
- 下載任務的輸出。當您下載任務的輸出時，它只會包含所選任務所產生的輸出。

在截止日期雲端中檢視工作階段和工作者日誌

日誌為您提供有關任務狀態和處理的詳細資訊。在 AWS 截止日期雲端監視器中，您可以看到以下兩種類型的日誌：

- 工作階段日誌詳細說明動作的時間軸，包括：
 - 設定動作，例如附件同步和載入軟體環境
 - 執行任務或一組任務
 - 關閉動作，例如關閉工作者上的環境

工作階段包含至少一個任務的處理，並且可以包含多個任務。工作階段日誌也會顯示 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體類型、vCPU 和記憶體的相关資訊。工作階段日誌也包含工作階段中所用工作者的日誌連結。

- 工作者日誌提供工作者在其生命週期內處理之動作時間軸的詳細資訊。工作者日誌可以包含多個工作階段的相關資訊。

您可以下載工作階段和工作者日誌，以便離線檢查它們。

檢視工作階段日誌

1. 請依照 中的步驟[在截止日期雲端中檢視和管理任務詳細資訊](#)來檢視任務清單。
2. 從 Jobs (任務) 清單中選擇一項任務。
3. 從步驟清單中選取步驟。
4. 從任務清單中選取任務。
5. 從動作功能表中，選擇檢視日誌。

時間軸區段顯示任務的動作摘要。若要查看工作階段中執行的更多任務，以及查看工作階段的關閉動作，請選擇檢視所有任務的日誌。

從任務檢視工作者日誌

1. 請依照 中的步驟 [在截止日期雲端中檢視和管理任務詳細資訊](#) 來檢視任務清單。
2. 從 Jobs (任務) 清單中選擇一項任務。
3. 從步驟清單中選取步驟。
4. 從任務清單中選取任務。
5. 從動作功能表中，選擇檢視日誌。
6. 選擇工作階段資訊。
7. 選擇檢視工作者日誌。

從機群詳細資訊檢視工作者日誌

1. 依照中的步驟 [在截止日期雲端中檢視佇列和機群詳細資訊](#) 檢視機群。
2. 從工作者清單中選取工作者 ID。
3. 從動作功能表中，選擇檢視工作者日誌。

在工作者儀表板中檢視工作者詳細資訊

工作者儀表板會提供處理任務的工作者詳細資訊。您可以看到：

- 工作者的中繼資料，例如執行個體類型
- 工作者執行的工作階段動作
- 工作者效能，包括 CPU、記憶體和磁碟用量
- 一段時間內的 CPU、記憶體和磁碟用量圖表
- 一段時間內磁碟速度的圖表
- 任務的工作者日誌

從任務檢視工作者儀表板

1. 請依照 中的步驟 [在截止日期雲端中檢視和管理任務詳細資訊](#) 來檢視任務清單。
2. 從 Jobs (任務) 清單中選擇一項任務。
3. 從步驟清單中選取步驟。
4. 從任務清單中選取任務。

5. 在任務表格中，從動作功能表中，選擇檢視工作者儀表板。

從機群詳細資訊檢視工作者儀表板

1. 依照中的步驟[在截止日期雲端中檢視佇列和機群詳細資訊](#)檢視機群。
2. 從工作者清單中選取工作者。
3. 從動作功能表中，選擇檢視工作者儀表板。

使用案例

偵測佈建不足的執行個體

當轉譯時間超過預期時，工作者儀表板有助於判斷您的執行個體大小是否適合您的工作負載。雖然許多渲染器的 100% vCPU 使用率是正常的，但持續高記憶體使用率接近最大容量，且磁碟空間使用率增加可能表示您的執行個體佈建不足。在這種情況下，升級機群的執行個體組態可減少轉譯錯誤並大幅改善轉譯時間。不過，請務必在升級後繼續監控工作者效能，以確保您找到最佳平衡 - 升級過於積極可能會導致過度佈建產生不必要的成本。

偵測過度佈建的執行個體

即使任務成功完成，也可能有機會最佳化您的成本。工作者儀表板可以顯示您是否支付比工作負載所需的更多運算能力。如果您看到工作者的平均 vCPU 使用量低、記憶體使用率最低，以及未使用的磁碟空間過多，您可以縮減機群的執行個體組態。

故障診斷失敗的任務

調查失敗的任務時，工作者儀表板可做為寶貴的診斷工具。請特別注意尖峰記憶體用量和磁碟空間使用率 - 如果這些指標接近或達到 100%，它們可能是任務失敗的根本原因。這類資源耗盡表示您目前的執行個體缺乏有效處理工作負載的容量。在這些情況下，佈建記憶體或磁碟空間增加的執行個體將有助於確保任務成功完成。

最佳執行個體使用率

vCPU 使用率

目標範圍：70–90%

- 低於 70%：可能無法充分利用運算資源，這表示您支付比工作負載需求更多的 CPU

- 70–90%：最佳範圍，可讓您有效率地使用資源，而不會遇到瓶頸
- 持續達到 100%：可能表示 CPU 瓶頸，可能會減慢轉譯速度

請記住，某些轉譯任務自然會比其他轉譯任務更密集 CPU，100% vCPU 用量可能不是問題。即時視覺化任務可能會顯示更一致的 CPU 使用率，而運算需求不斷變化的任務可能會有不同的模式。

記憶體使用率

目標範圍：70–85%

- 低於 50%：工作負載可能過大的執行個體
- 70–85%：最佳使用率，具有足夠的空間來因應尖峰
- 高於 90%：效能降低或out-of-memory錯誤的風險

記憶體需求可能會因場景複雜性、紋理解析度和模擬資料而有很大差異。隨著時間的推移監控記憶體趨勢對於識別您的工作負載是否在記憶體需求中增長至關重要。

磁碟空間使用率

目標範圍：60–80%

- 低於 40%：可能過度佈建的儲存
- 60–85%：具有暫存檔案和快取空間的良好使用率
- 高於 85%：大型轉譯期間空間不足的風險

請記住，磁碟 I/O 效能與容量同樣重要，尤其是在轉譯期間讀取/寫入大型紋理或快取檔案的工作負載。

在截止日期雲端中下載完成的輸出

任務完成後，您可以使用 AWS 截止日期雲端監視器將結果下載到您的工作站。輸出檔案會以您在建立任務時指定的名稱和位置存放。

輸出檔案會無限期儲存。若要降低儲存成本，請考慮為佇列的 Amazon S3 儲存貯體建立 S3 生命週期組態。Amazon S3 如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[管理您的儲存生命週期](#)。

下載任務、步驟或任務的完成輸出

1. 請依照 中的步驟 [在截止日期雲端中檢視和管理任務詳細資訊](#) 來檢視任務清單。
2. 選取您要下載輸出的任務、步驟或任務。
 - 如果您選擇任務，您可以在該任務的所有步驟中下載所有任務的所有輸出。
 - 如果選取步驟，您可以下載該步驟中所有任務的所有輸出。
 - 如果您選擇任務，您可以下載該個別任務的輸出。
3. 從動作功能表中，選擇下載輸出。
4. 提交任務時，輸出將下載到位置集。

Note

目前僅支援 Windows 和 使用選單下載輸出Linux。如果您有 Mac 並選擇下載輸出選單項目，則視窗會顯示可用來下載轉譯輸出的 AWS CLI 命令。

截止日期 雲端陣列

使用截止日期雲端陣列，您可以管理使用者和專案資源。陣列是您專案資源所在的。您的陣列由佇列和機群組成。佇列是已提交任務所在的位置，並排定轉譯。機群是一組工作者節點，執行任務以完成任務。建立陣列之後，您可以建立佇列和機群，以滿足專案的需求。

建立陣列

1. 從[截止日期雲端主控台](#)中，選擇前往儀表板。
2. 在期限雲端儀表板的陣列區段中，選擇動作 → 建立陣列。
 - 或者，在左側面板中選擇陣列和其他資源，然後選擇建立陣列。
3. 為您的陣列新增名稱。
4. 針對描述，輸入陣列描述。明確的描述可協助您快速識別陣列的目的。
5. （選用）根據預設，您的資料會使用金鑰進行加密，該金鑰 AWS 會擁有並管理您的安全。您可以選擇自訂加密設定（進階）以使用現有金鑰，或建立您管理的新金鑰。

如果您選擇使用核取方塊自訂加密設定，請輸入 AWS KMS ARN，或 AWS KMS 選擇建立新的 KMS 金鑰來建立新的。

6. （選用）選擇新增標籤，將一或多個標籤新增至您的陣列。
7. 選擇建立陣列。建立後，會顯示您的陣列。

截止日期雲端佇列

佇列是管理和處理任務的陣列資源。

若要使用佇列，您應該已設定監視器和陣列。

主題

- [建立佇列](#)
- [建立佇列環境](#)
- [關聯佇列和機群](#)

建立佇列

1. 從[截止日期雲端主控台](#)儀表板中，選取您要為其建立佇列的陣列。
 - 或者，在左側面板中選擇陣列和其他資源，然後選取您要為其建立佇列的陣列。
2. 在佇列索引標籤中，選擇建立佇列。
3. 輸入佇列的名稱。
4. 針對描述，輸入佇列描述。描述可協助您識別佇列的用途。
5. 對於任務附件，您可以建立新的 Amazon S3 儲存貯體或選擇現有的 Amazon S3 儲存貯體。
 - a. 建立新的 Amazon S3 儲存貯體
 - i. 選取建立新任務儲存貯體。
 - ii. 輸入儲存貯體的名稱。建議您命名儲存貯體 `deadlinecloud-job-attachments-[MONITORNAME]`。
 - iii. 輸入根字首以定義或變更佇列的根位置。
 - b. 選擇現有的 Amazon S3 儲存貯體
 - i. 選取選擇現有的 S3 儲存貯體 > 瀏覽 S3。
 - ii. 從可用儲存貯體清單中選取佇列的 S3 儲存貯體。
6. (選用) 若要將佇列與客戶受管機群建立關聯，請選取啟用與客戶受管機群的關聯。
7. 如果您啟用與客戶受管機群的關聯，您必須完成以下步驟。

⚠ Important

我們強烈建議為執行身分功能指定使用者和群組。如果沒有，它會降低您陣列的安全狀態，因為任務可以執行工作者代理程式可以執行的所有操作。如需潛在安全風險的詳細資訊，請參閱以[使用者和群組身分執行任務](#)。

a. 對於以使用者身分執行：

若要提供佇列任務的登入資料，請選取佇列設定的使用者。

或者，若要選擇不設定您自己的登入資料並以工作者代理程式使用者身分執行任務，請選取工作者代理程式使用者。

b. (選用) 對於以使用者登入資料身分執行，輸入使用者名稱和群組名稱，以提供佇列任務的登入資料。

如果您使用的是機Windows群，則必須建立 AWS Secrets Manager 包含以使用者身分執行之密碼的秘密。如果您沒有具有密碼的現有秘密，請選擇建立秘密以開啟 Secrets Manager 主控台來建立秘密。如需詳細資訊，請參閱《截止日期雲端開發人員指南》中的[管理對 Windows 任務使用者秘密的存取](#)。

8. 需要預算有助於管理佇列的成本。選取不需要預算或需要預算。**9. 您的佇列需要代表您存取 Amazon S3 的許可。您可以建立新的服務角色或使用現有的服務角色。如果您沒有現有的服務角色，請建立並使用新的服務角色。**

a. 若要使用現有的服務角色，請選取選擇服務角色，然後從下拉式清單中選取角色。

b. 若要建立新的服務角色，請選取建立並使用新的服務角色，然後輸入角色名稱和描述。

10. (選用) 若要新增佇列環境的環境變數，請選擇新增環境變數，然後輸入您新增的每個變數的名稱和值。**11. (選用) 選擇新增標籤，將一或多個標籤新增至佇列。****12. 若要建立預設conda佇列環境，請保持選取核取方塊。若要進一步了解佇列環境，請參閱[建立佇列環境](#)。如果您要為客戶管理的機群建立佇列，請清除核取方塊。****13. 選擇建立佇列。**

建立佇列環境

佇列環境是一組設定機群工作者的環境變數和命令。您可以使用佇列環境為佇列中的任務提供軟體應用程式、環境變數和其他資源。

建立佇列時，您可以選擇建立預設conda佇列環境。此環境可讓服務受管機群存取合作夥伴 DCC 應用程式和轉譯器的套件。預設環境 如需詳細資訊，請參閱 [預設conda佇列環境](#)。

您可以使用 主控台新增佇列環境，或直接編輯 json 或 YAML 範本。此程序說明如何使用 主控台建立環境。

1. 若要將佇列環境新增至佇列，請導覽至佇列，然後選取佇列環境索引標籤。
2. 選擇動作，然後使用表單建立新的。
3. 輸入佇列環境的名稱和描述。
4. 選擇新增環境變數，然後為您新增的每個變數輸入名稱和值。
5. (選用) 輸入佇列環境的優先順序。優先順序表示此佇列環境在工作者上執行的順序。較高優先順序的佇列環境會先執行。
6. 選擇建立佇列環境。

預設conda佇列環境

當您建立與服務受管機群相關聯的佇列時，您可以選擇新增預設佇列環境，支援 [conda](#) 為您的任務在虛擬環境中下載和安裝套件。

如果您使用截止日期雲端 [主控台](#) 新增預設佇列環境，則會為您建立環境。如果您以其他方式新增佇列，例如 AWS CLI 或使用 CloudFormation，則需要自行建立佇列環境。為了確保您擁有環境的正確內容，您可以參考 GitHub 上的佇列環境範本 YAML 檔案。如需預設佇列環境的內容，請參閱 GitHub 上的 [預設佇列環境 YAML 檔案](#)。

GitHub 上還有其他 [佇列環境範本](#)，您可以用這些範本做為自己的需求的起點。

Conda 提供來自 頻道的套件。頻道是存放套件的位置。Deadline Cloud 提供頻道 `deadline-cloud`，可託管支援合作夥伴 DCC 應用程式和轉譯器的conda套件。選取以下每個索引標籤，以檢視 Linux 或 的可用套件Windows。

Linux

- Autodesk Arnold for Cinema 4D
 - `cinema4d-c4dtoa=2025`
- 適用於 Maya 的 Autodesk Arnold

- maya-mtoa=2024.5.3
- maya-mtoa=2025.5.4
- maya-mtoa=2026.5.5
- Autodesk Maya
 - maya=2024
 - maya=2025
 - maya=2026
 - maya-openjd
- Autodesk VRED
 - vredcore=2025
 - vredcore=2026
- Blender
 - blender=3.6
 - blender=4.2
 - blender=4.5
 - blender=5.0
 - blender-openjd
- Maya 專用 Chaos V-Ray
 - maya-vray=2025.7
 - maya-vray=2026.7
- Foundry Nuke
 - nuke=15
 - nuke=16
 - nuke-openjd
- Maxon 電影 4D
 - cinema4d=2025
 - cinema4d=2026
 - cinema4d-openjd
- Maya 的 Maxon Redshift

- maya-redshift=2026.2
- SideFX Houdini
 - houdini=19.5
 - houdini=20.0
 - houdini=20.5
 - houdini=21.0
 - houdini-openjd

Windows

- Adobe After Effects
 - aftereffects=24.6
 - aftereffects=25.1
 - aftereffects=25.2
- Autodesk Arnold for Cinema 4D
 - cinema4d-c4dtoa=2025
 - cinema4d-c4dtoa=2026
- KeyShot Studio
 - keyshot=2024
 - keyshot=2025
 - keyshot-openjd
- Maxon Cinema 4D
 - cinema4d=2024
 - cinema4d=2025
 - cinema4d=2026
 - cinema4d-openjd
- 虛擬引擎
 - unrealengine=5.4
 - unrealengine=5.5
 - unrealengine=5.6
 - unrealengine-openjd

Note

對於 Cinema 4D，Linuxconda 套件不支援物質 3D 材料。具有此材料的任務失敗，並發生下列其中一個錯誤：

```
Commandline: ./modules/io_substance/source/substance_framework/src/details/
detailsengine.cpp:794:
SubstanceAir::Details::Engine::Context::Context(SubstanceAir::Details::Engine&,
SubstanceAir::RenderCallbacks*): Assertion `res==0' failed.
```

```
/home/job-user/.conda/envs/<hash>/Lib/deadline/cinema4d_adaptor/Cinema4DAdaptor/
adaptor.sh: line 44: 10832 Segmentation fault      (core dumped) $C4DEXE
${ARGS[*]}
```

我們建議您Windows改為將含有物質材料的任務提交至。

在上的電影 4D 2025.3.3 中Linux，全域化資產路徑可能會導致分段故障。因此，Linuxconda 套件包含 Cinema 4D 2025.3.1 和 Redshift 2025.6.0。如果您需要來自 Cinema 4D 2025.3.3 的功能或錯誤修正，我們建議兩個選項：升級至 Cinema 4D 2026 或Windows改為將這些任務提交至。

對於 Cinema 4D OpenJD，為了防止任何逾時問題，我們建議您將任務執行逾時設定為預期轉譯時間的兩倍，而不是使用預設的 2 天逾時。

當您使用預設conda環境將任務提交至佇列時，環境會將兩個參數新增至任務。這些參數指定在處理任務之前，用來設定任務環境的conda套件和通道。參數為：

- CondaPackages – 以空格分隔的[套件比對規格](#)清單，例如 blender=3.6或 numpy>1.22。預設為空白，可略過建立虛擬環境。
- CondaChannels – 以空格分隔的[conda頻道](#)清單deadline-cloud，例如 conda-forge、或 s3://*amzn-s3-demo-bucket*/conda/channel。預設值為 deadline-cloud，這是可供服務受管機群使用的頻道，可提供合作夥伴 DCC 應用程式和渲染器。

當您使用整合式提交者從 DCC 將任務傳送至截止日期雲端時，提交者會根據 DCC 應用程式和提交者填入 CondaPackages 參數的值。例如，如果您使用的是 Blender，則 CondaPackage 參數會設為 blender=3.6.* blender-openjd=0.4.*。

我們建議您僅將任何提交項目鎖定在上表中列出的版本，例如 blender=3.6。建議釘選至 major.minor 版本，因為修補程式版本會影響可用的套件。例如，當我們發行 Blender 3.6.17 時，將不再分發 Blender 3.6.16。固定到混合器=3.6.16 的任何提交都會失敗。如果您鎖定混合器 = 3.6，則會取得最新的分散式修補程式版本，且任務不會受到影響。根據預設，DCC 提交者會釘選至上表中列出的目前版本，不包括修補程式編號，例如混合器=3.6。

關聯佇列和機群

若要處理任務，您必須將佇列與機群建立關聯。您可以將單一機群與多個佇列建立關聯，並將單一佇列與多個機群建立關聯。當您將機群與多個佇列建立關聯時，它會平均分配其工作者。同樣地，當您將佇列與多個機群建立關聯時，它會將任務平均分配到這些機群。

Note

若要使用等待和儲存，建議您只將佇列與使用等待和儲存執行個體類型的機群建立關聯。如果您將佇列與多個機群建立關聯，且其中任何機群使用 Spot 或隨需執行個體類型，則機群可能不會使用等待和儲存執行個體來處理任務。

若要將現有佇列與現有機群建立關聯，請完成下列步驟：

1. 從截止日期雲端陣列中，選取您要與機群建立關聯的佇列。佇列隨即顯示。
2. 若要選取要與佇列建立關聯的機群，請選擇關聯機群。
3. 選擇選取機群下拉式清單。可用的機群清單隨即顯示。
4. 從可用機群清單中，選取您要與佇列建立關聯的機群或機群旁的核取方塊。
5. 選擇關聯。機群關聯狀態現在應為作用中。

停止佇列機群關聯

若要停止佇列機群關聯，請完成下列步驟：

1. 從佇列中選取關聯的機群索引標籤。
2. 選取您要停止與佇列建立關聯之機群的核取方塊。
3. 從動作下拉式清單中，選取最終停止或立即停止。

若要在關聯停止之前完成處理任務，請選取最終停止。若要立即停止處理任務，請選取立即停止。

4. 在確認視窗中，輸入 **confirm**，然後選擇停止。
5. （選用）若要取消機群與佇列的關聯，請完成下列步驟：
 - a. 等待關聯狀態變更為已停止。
 - b. 關聯停止後，如果您尚未停止，請選取機群的核取方塊。
 - c. 從動作下拉式清單中，選取取消關聯機群。
 - d. 在確認視窗中，選擇取消關聯。

重新啟用佇列機群關聯

若要重新啟用佇列機群關聯，請完成下列步驟：

1. 從佇列中選取關聯的機群索引標籤。
2. 選取您要重新啟用佇列機群關聯的機群核取方塊。
3. 從動作下拉式清單中，選擇開始。關聯狀態會變更為作用中。

截止日期 雲端機群

本節說明如何管理 Deadline Cloud 的服務受管機群和客戶受管機群 (CMF)。

您可以設定兩種類型的截止日期雲端機群：

- 服務受管機群是具有截止日期雲端所提供預設設定的工作者機群。這些預設設定的設計既有效率又符合成本效益。
- 客戶受管機群 (CMFs) 可讓您完全控制處理管道。CMF 可以位於 AWS 基礎設施內、內部部署或位於共同位置的資料中心。CMFs 包括佈建、操作、管理和停用機群中的工作者。

當您將機群與多個佇列建立關聯時，它會將其工作者平均分配到這些佇列中。

主題

- [服務受管機群](#)
- [客戶管理的機群](#)

服務受管機群

服務受管機群 (SMF) 是具有截止日期雲端所提供預設設定的工作者機群。這些預設設定的設計既有效率又符合成本效益。

有些預設設定會限制工作者和任務可執行的時間量。工作者只能執行七天，而任務只能執行五天。達到限制時，任務或工作者會停止。如果發生這種情況，您可能會失去工作者或任務正在執行的工作。若要避免這種情況，請監控您的工作者和任務，以確保它們不超過最長持續時間限制。若要進一步了解如何監控您的工作者，請參閱 [使用截止日期雲端監視器](#)。

建立服務受管機群

您可以為服務受管機群選擇 3 種類型的執行個體選項；spot、隨需和 wait-and-save。Spot 執行個體是以折扣價格使用的未預留容量，但可能會因為隨需請求而中斷。隨需執行個體會以秒計價，沒有長期承諾，而且不會中斷。Wait-and-save 提供延遲的任務排程，可降低成本，並可因隨需和 Spot 請求而中斷。

1. 從[截止日期雲端主控台](#)，導覽至您要建立機群的陣列。
2. 選取機群索引標籤，然後選擇建立機群。

3. 輸入機群的名稱。
4. (選用) 輸入描述。明確的描述可協助您快速識別機群的用途。
5. 選取服務受管機群類型。
6. 選擇機群的 Spot、隨需或等待並儲存執行個體市場選項。根據預設，機群會使用 Spot 選項。
7. 如需機群的服務存取權，請選取現有角色或建立新的角色。服務角色會將登入資料提供給機群中的執行個體，授予他們處理任務的許可，以及授予監視器中的使用者，讓他們可以讀取日誌資訊。
8. 選擇下一步。
9. 選擇僅限 CPU 執行個體或 GPU 加速執行個體。GPU 加速的執行個體可以更快地處理您的任務，但成本可能更高。
10. 為您的工作者選取作業系統。您可以保留預設值，Linux或選擇 Windows。
11. (選用) 如果您選取 GPU 加速執行個體，請設定每個執行個體中的 GPUs 數量上限和下限。基於測試目的，您僅限於一個 GPU。若要為您的生產工作負載請求更多，請參閱《Service Quotas 使用者指南》中的[請求提高配額](#)。
12. 輸入機群所需的最小和最大 vCPUs。
13. 輸入您機群所需的記憶體數量下限和上限。
14. (選用) 您可以選擇允許或排除機群中的特定執行個體類型，以確保只有這些執行個體類型用於此機群。
15. (選用) 設定要擴展機群的執行個體數量上限，以便為佇列中的任務提供容量。建議您將執行個體數量下限保留在 0，以確保機群在沒有任務排入佇列時發行所有執行個體。
16. (選用) 您可以指定要連接到此機群中工作者的 Amazon Elastic Block Store (Amazon EBS) gp3 磁碟區大小。如需詳細資訊，請參閱[EBS 使用者指南](#)。
17. 選擇下一步。
18. (選用) 定義自訂工作者功能，定義此機群的功能，可與任務提交時指定的自訂主機功能結合。如果您打算將機群連接到自己的授權伺服器，其中一個範例是特定的授權類型。
19. 選擇下一步。
20. (選用) 若要將機群與佇列建立關聯，請從下拉式清單中選取佇列。如果佇列是使用預設conda 佇列環境設定，您的機群會自動獲得支援合作夥伴 DCC 應用程式和轉譯器的套件。如需提供的套件清單，請參閱[預設conda佇列環境](#)。
21. 選擇下一步。
22. (選用) 若要將標籤新增至機群，請選擇新增標籤，然後輸入該標籤的索引鍵和值。
23. 選擇下一步。

24. 檢閱您的機群設定，然後選擇建立機群。

使用 GPU 加速器

您可以在服務受管機群中設定工作者主機，以使用一或多個 GPU 來加速處理任務。使用 加速器可以縮短處理任務所需的時間，但可以增加每個工作者執行個體的成本。您應該測試工作負載，以了解使用 GPU 加速器的機群與不使用的機群之間的權衡。

GPUs 不適用於具有wait-and-save連線的機群。

Note

基於測試目的，您僅限於一個 GPU。若要為您的生產工作負載請求更多，請參閱《Service Quotas 使用者指南》中的[請求提高配額](#)。

當您指定工作者執行個體功能時，您可以決定機群是否會使用 GPU 加速器。如果您決定使用 GPUs，您可以指定每個執行個體的 GPUs 數量下限和上限、要使用的 GPU 晶片類型，以及 GPUs 的執行時間驅動程式。

可用的 GPU 加速器包括：

- T4 - NVIDIA T4 Tensor 核心 GPU
- A10G - NVIDIA A10G Tensor 核心 GPU
- L4 - NVIDIA L4 Tensor 核心 GPU
- L40s - NVIDIA L40S Tensor 核心 GPU

您可以從下列執行時間驅動程式中選擇：

- Latest - 使用晶片可用的最新執行時間。如果您指定 latest 並發行新版本的執行時間，則會使用新版本的執行時間。
- grid:r570 - [NVIDIA vGPU 軟體 18](#)
- grid:r550 (已棄用) - [NVIDIA vGPU 軟體 17](#)

如果您未指定執行時間，則 Deadline Cloud 會使用 latest 做為預設值。不過，如果您有多個加速器並為某些 加速器指定 latest，並將其他加速器保留空白，則 Deadline Cloud 會引發例外狀況。

服務受管機群的軟體授權

期限 雲端為常用的軟體套件提供以用量為基礎的授權 (UBL)。支援的軟體套件會在服務受管機群上執行時自動授權。您不需要設定或維護軟體授權伺服器。授權會擴展，因此您不會因為更大的任務而用盡。

您可以使用內建的截止日期雲端 conda 頻道安裝支援 UBL 的軟體套件，也可以使用自己的套件。如需 conda 頻道的詳細資訊，請參閱[建立佇列環境](#)。

如需支援的軟體套件清單和 UBL 定價的相關資訊，請參閱[AWS 截止日期雲端定價](#)。

使用服務受管機群取得自己的授權

使用期限 雲端用量型授權 (UBL)，您不需要管理與軟體供應商簽訂的個別授權協議。不過，如果您有現有的授權，或需要使用無法透過 UBL 取得的軟體，則可以將自己的軟體授權與期限雲端服務管理的機群搭配使用。您可以透過網際網路將 SMF 連線至軟體授權伺服器，以檢查機群中每個工作者的授權。

如需使用代理連線到授權伺服器的範例，請參閱 截止日期雲端開發人員指南中的[將服務受管機群連線到自訂授權伺服器](#)。

VFX Reference Platform 相容性

VFX Reference Platform 是 VFX 產業的常見目標平台。若要搭配支援的軟體使用執行 Amazon Linux 2023 的標準服務受管機群 Amazon EC2 執行個體 VFX Reference Platform，在使用服務受管機群時，請謹記下列考量。

VFX Reference Platform 會每年更新。這些使用 AL2023 的考量，包括截止日期雲端服務受管機群，是以 2022 年至 2024 年參考平台的日曆年 (CY) 為基礎。如需詳細資訊，請參閱[VFX Reference Platform](#)。

Note

如果您要為客戶管理的機群建立自訂 Amazon Machine Image(AMI)，您可以在準備 Amazon EC2 執行個體時新增這些需求。

若要在 AL2023 Amazon EC2 執行個體上使用 VFX Reference Platform 支援的軟體，請考慮下列事項：

- 與 AL2023 一起安裝的 glibc 版本相容於執行期使用，但不適用於建置與 CY2024 VFX Reference Platform 或更早版本相容的軟體。

- Python 3.9 和 3.11 隨附於服務受管機群，因此與 VFX Reference Platform CY2022 和 CY2024 相容。Python 3.7 和 3.10 未在服務受管機群中提供。需要它們的軟體必須在佇列或任務環境中提供 Python 安裝。
- 服務受管機群中提供的某些 Boost 程式庫元件是 1.75 版，與不相容。VFX Reference Platform 如果您的應用程式使用 Boost，您必須提供自己的程式庫版本才能相容。
- Intel TBB 更新 3 是在服務受管機群中提供。此版本與 VFX Reference Platform CY2022, CY2023 和 CY2024 相容。
- 服務受管機群 VFX Reference Platform 不提供具有指定版本的其他程式庫。您必須將服務受管機群上使用的任何應用程式提供給程式庫。如需程式庫的清單，請參閱[參考平台](#)。

工作者 AMI 軟體內容

本節提供在 AWS 截止日期雲端服務受管工作者 Amazon Machine Image (AMIs) 上安裝的軟體資訊。

AWS 期限雲端服務受管工作者 AMIs 是以 Windows Server 2022 和 Amazon Linux 2023 為基礎，並包含專門安裝以支援轉譯工作負載的額外軟體。這些 AMIs 會持續更新以維護功能。

這些 AMIs 上的軟體會組織成下列其中一個支援類別：

服務提供的軟體套件

專為轉譯工作負載而安裝和維護的軟體

其他系統軟體

所有其他可能變更的軟體，恕不另行通知

服務提供的軟體套件

安裝這些軟體套件是為了支援轉譯工作負載，並維護相容性。您可以安全地取得這些套件的相依性。

開發工具和語言

Linux (AL2023)：

- Python 3.11
- Git

Windows (伺服器 2022)：

- Python 3.11
- 的 Git Windows

AWS 工具

兩個平台：

- AWS 命令列界面 v2 (AWS CLI v2)

系統程式庫和公用程式

Linux:

- 檔案系統操作的 FUSE 和 FUSE3 程式庫
- 映像程式庫
 - libpng
 - libjpeg
 - libtiff
- OpenGL 程式庫
 - mesa-libGLU
 - mesa-libGL
 - mesa-libEGL
 - libglvnd-opengl
- 開發程式庫：
 - json-c (JSON 剖析)
 - libnsl (網路服務程式庫)
 - libxcrypt-compat (加密相容性)
- X 視窗程式庫
 - libXmu
 - libXpm
 - libXinerama
 - libXcomposite
 - libXrender

- libXrandr
- libXcursor
- libXi
- libxdamage
- libXtst
- libxkbcommon
- libSM
- 網路和系統公用程式
 - tcsh

GPU 加速機群

- Nvidia 網格驅動程式

套件管理工具

Linux:

- conda/Mamba 套件管理員 (安裝在 /opt/conda)
- DNF 套件管理員 (系統套件)
- pip (Python 套件安裝程式)

Windows:

- conda/Mamba 套件管理員 (安裝在 C:\ProgramData\conda)
- pip (Python 套件安裝程式)

其他系統軟體

AMI 上的所有其他軟體都可以更新、移除或變更，恕不另行通知。請勿對上面支援的軟體套件區段中未明確列出的任何軟體採取相依性。此限制包括但不限於：

- 作業系統套件和程式庫
- 服務管理元件
- Base AMI 軟體和驅動程式

- 軟體相依性和執行時間程式庫
- 系統組態工具和公用程式

其他系統軟體範例

Linux：系統套件，例如系統化、核心模組、硬體驅動程式、聯網元件，以及做為基本 AL2023 分佈的一部分安裝的支援程式庫。

Windows：Windows系統元件、Microsoft Edge、Amazon EC2 服務軟體、硬體驅動程式和Windows執行期元件。

最佳實務

相依性管理：僅對支援的軟體套件區段中列出的軟體取得相依性。

套件版本：對於特定軟體版本，請使用套件管理員（例如 pip、conda 等）安裝特定套件，而不是依賴 AMI 提供的版本。

環境隔離：使用虛擬環境（例如 Python venv 和 conda 環境）隔離您的特定相依性。

AMI 更新模型

請注意工作者 AMI 如何更新的相關資訊。

- 工作者 AMIs會在沒有版本控制系統的情況下持續更新。
- 更新會在服務操作中自動發生。
- AMI 更新不提供預先通知系統。

客戶管理的機群

當您想要使用您管理的工作者機群時，您可以建立客戶受管機群 (CMF)，讓 Deadline Cloud 用來處理您的任務。在下列情況下使用 CMF：

- 您現有的現場部署工作者要與截止日期雲端整合。
- 您在共置資料中心有工作者。
- 您想要直接控制 Amazon Elastic Compute Cloud (Amazon EC2) 工作者。

當您使用 CMF 時，您可以完全控制和負責機群。這包括佈建、操作、管理和停用機群中的工作者。

如需詳細資訊，請參閱 [《截止日期雲端開發人員指南》](#) 中的建立和使用截止日期雲端客戶受管機群。

在截止日期雲端中管理使用者

AWS Cloud 使用 AWS IAM Identity Center 來管理使用者和群組的截止日期。IAM Identity Center 是一種雲端型單一登入服務，可與企業單一登入 (SSO) 供應商整合。透過整合，使用者可以使用其公司帳戶登入。

截止日期雲端預設會啟用 IAM Identity Center，而且需要設定和使用截止日期雲端。您的組織擁有者 AWS Organizations 負責管理可存取您截止日期雲端監視器的使用者和群組。如需詳細資訊，請參閱[什麼是 AWS Organizations](#)。

如何管理使用者取決於您的 IAM Identity Center 身分來源組態。身分來源定義 IAM Identity Center 取得使用者資訊的位置。

主題

- [了解您的身分來源](#)
- [使用 建立和管理使用者 IAM Identity Center 目錄](#)
- [使用外部身分提供者管理使用者](#)
- [了解存取層級](#)

了解您的身分來源

IAM Identity Center 使用身分來源來定義使用者管理的位置。身分來源有兩種類型：

IAM Identity Center 目錄

這是預設身分來源。使用者會直接在 IAM Identity Center 中建立和管理。您可以透過截止日期雲端主控台或 IAM Identity Center 主控台建立使用者。使用者會收到加入組織的電子郵件邀請，而密碼是在 IAM Identity Center 中管理。

外部身分提供者 (IdP)

使用者來自外部系統，例如 Okta、Microsoft Entra ID 或其他 SAML 2.0 身分提供者。使用者必須先在外部系統中建立。設定外部 IdP 時，截止日期雲端主控台無法建立使用者，但您可以將許可指派給現有使用者。密碼由外部 IdP 管理。

若要檢查或變更您的身分來源組態，請參閱《IAM Identity Center 使用者指南》中的[管理您的身分來源](#)。

使用 建立和管理使用者 IAM Identity Center 目錄

如果您的身分來源設定為 IAM Identity Center 目錄，您可以透過截止日期雲端主控台直接建立和管理使用者和群組。在主控台中建立的使用者會收到來自 IAM Identity Center 的電子郵件邀請。接受邀請後，使用者可以存取截止日期雲端監視器。

Note

如果您的 IAM Identity Center 連接到外部身分提供者，則您無法透過截止日期雲端主控台建立使用者。[the section called “使用外部 IdP 管理使用者”](#) 如需使用外部 IdP 管理使用者的相關資訊，請參閱。

1. 登入 AWS 管理主控台 並開啟截止日期雲端[主控台](#)。在主頁面的入門區段中，選擇設定截止日期雲端或前往儀表板。
2. 在左側導覽窗格中，選擇使用者管理。根據預設，會選取群組索引標籤。

根據要採取的動作，選擇群組索引標籤或使用者索引標籤。

Groups

建立群組

1. 選擇建立群組。
2. 輸入群組名稱。名稱在 IAM Identity Center 組織中的群組之間必須是唯一的。

移除群組

1. 選取要移除的群組。
2. 選擇移除。
3. 在確認對話方塊中，選擇移除群組。

Note

您要從 IAM Identity Center 移除群組。群組成員無法再登入截止日期雲端或存取陣列資源。

Users

新增使用者

1. 選擇使用者索引標籤。
2. 選擇 Add users (新增使用者)。
3. 輸入新使用者的名稱、電子郵件地址和使用者名稱。
4. (選用) 選擇要將新使用者新增至其中的一或多個 IAM Identity Center 群組。
5. 選擇傳送邀請以傳送電子郵件給新使用者，其中包含加入 IAM Identity Center 組織的指示。

移除使用者

1. 選取要移除的使用者。
2. 選擇移除。
3. 在確認對話方塊中，選擇移除使用者。

Note

您要從 IAM Identity Center 移除使用者。使用者無法再登入截止日期雲端監視器或存取陣列資源。

使用外部身分提供者管理使用者

如果您的 IAM Identity Center 連接到外部身分提供者 (IdP)，例如 Okta 或 Microsoft Entra ID，則必須在該外部系統中建立和管理使用者。設定外部 IdP 時，截止日期雲端主控台無法建立新使用者。

在外部 IdP 中建立使用者並同步到 IAM Identity Center 之後，您可以將許可指派給截止日期雲端資源。[the section called “了解存取層級”](#) 如需在陣列、佇列和機群層級指派許可的相關資訊，請參閱。

如需有關管理外部身分提供者組態的資訊，請參閱《IAM Identity Center 使用者指南》中的[管理您的身分來源](#)。

了解存取層級

無論您的身分來源為何，您都可以透過截止日期雲端主控台，將許可指派給陣列、佇列和機群層級的使用者和群組。您可以授予不同層級的存取許可。每個後續關卡都包含先前關卡的許可。下列清單說明從最低層級到最高層級的四個存取層級：

- 檢視器 – 查看其可存取之陣列、佇列、機群和任務中資源的許可。檢視器無法提交或變更任務。
- 貢獻者 – 與檢視器相同，但具有將任務提交至佇列或陣列的許可。
- 管理員 – 與參與者相同，但有權編輯他們有權存取之佇列中的任務，並授予他們有權存取之資源的許可。
- 擁有者 – 與管理員相同，但可以檢視和建立預算並查看用量。

如需有關自訂這些存取層級的資訊，請參閱《截止日期雲端開發人員指南》中的[監控角色](#)。

主題

- [存取層級許可矩陣](#)
- [成員繼承](#)
- [將許可指派給使用者和群組](#)

存取層級許可矩陣

下表顯示使用預設 AWS 受管政策時，陣列、佇列和機群在每個存取層級可用的特定許可。管理使用者存取權目前只能透過截止日期雲端主控台使用，無法在截止日期雲端監視器中使用。如需有關自訂這些存取層級的資訊，請參閱《截止日期雲端開發人員指南》中的[監控角色](#)。

依存取層級的陣列許可

權限	觀眾	作者群	管理員	Owner
檢視陣列詳細資訊	是	是	是	是
檢視佇列和機群	是	是	是	是
提交任務	否	是	是	是
管理使用者存取	否	否	是	是

權限	觀眾	作者群	管理員	Owner
檢視和建立預算	否	否	否	是
檢視用量資料	否	否	否	是

依存取層級佇列許可

權限	觀眾	作者群	管理員	Owner
檢視佇列詳細資訊	是	是	是	是
檢視佇列中的任務	是	是	是	是
將任務提交至佇列	否	是	是	是
編輯和取消任務	否	否	是	是
管理佇列使用者存取權	否	否	是	是
檢視佇列預算分配	否	否	否	是

依存取層級的機群許可

權限	觀眾	作者群	管理員	Owner
檢視機群詳細資訊	是	是	是	是
檢視機群中的工作者	是	是	是	是
管理機群使用者存取	否	否	是	是
檢視機群成本資料	否	否	否	是

成員繼承

Deadline Cloud 使用階層成員模式，可在陣列、佇列或機群層級指派許可。了解成員資格繼承的運作方式可協助您有效地設定存取控制。

陣列層級成員資格

當您在陣列層級指派使用者或群組成員資格時，該成員資格會套用至陣列中的所有佇列和機群。陣列層級成員資格提供廣泛的存取，對於需要跨多個佇列或機群工作的使用者來說非常有用。

例如，如果您在陣列層級將使用者指派為貢獻者，則該使用者可以將任務提交到陣列中的任何佇列。

佇列和機群層級成員資格

您也可以在此層級指派成員資格，以獲得更精細的存取控制。佇列層級和機群層級成員資格僅適用於該特定資源。

例如，如果您將使用者指派為特定佇列的管理員，則該使用者只能編輯任務和管理該佇列的存取權，而不是陣列中的其他佇列。

使用者只能存取佇列或機群，無需擁有陣列層級成員資格。在此情況下，使用者無法在其陣列清單中看到陣列，但可以將任務提交至，並僅檢視其可存取的佇列或機群。

有效許可

當使用者在多個層級擁有成員資格時，截止日期雲端會使用最高的存取層級。例如：

- 在陣列層級具有檢視器存取權的使用者，以及在特定佇列具有管理員存取權的使用者，具有該佇列的管理員許可，以及所有其他佇列的檢視器許可。
- 在陣列層級具有貢獻者存取權的使用者，以及在特定機群上具有擁有者存取權的使用者，具有該機群的擁有者許可，以及在其他地方具有貢獻者許可。

Note

在陣列、佇列或機群層級沒有任何成員資格的使用者無法存取這些資源，即使他們是透過 IAM Identity Center 進行身分驗證。

如需將成員資格指派給使用者和群組的說明，請參閱 [the section called “指派許可”](#)。

將許可指派給使用者和群組

使用截止日期雲端主控台，將存取層級指派給陣列、佇列或機群層級的使用者和群組。

Note

存取許可的變更最多可能需要 10 分鐘才能反映在系統中。

導覽至存取管理

1. 登入 AWS 管理主控台 並開啟截止日期雲端[主控台](#)。
2. 在左側導覽窗格中，選擇陣列和其他資源。
3. 選取要管理的陣列。選擇陣列名稱以開啟詳細資訊頁面。您可以使用搜尋列來搜尋陣列。
4. (選用) 若要管理佇列或機群而非陣列，請選擇佇列或機群索引標籤，然後選擇要管理的佇列或機群。
5. 選擇存取管理索引標籤。

根據要採取的動作，選擇群組索引標籤或使用者索引標籤。

Groups

新增群組

1. 選取群組切換。
2. 選擇 Add group (新增群組)。
3. 從下拉式清單中，選取要新增的群組。
4. 針對群組存取層級，選擇下列其中一個選項：
 - Viewer (檢視者)
 - Contributor (作者群)
 - 管理員
 - 擁有者
5. 選擇新增。

移除群組

1. 選取要移除的群組。
2. 選擇移除。

3. 在確認對話方塊中，選擇移除群組。

Users

新增使用者

1. 若要新增使用者，請選擇新增使用者。
2. 從下拉式清單中，選取要新增的使用者。
3. 針對使用者存取層級，選擇下列其中一個選項：
 - Viewer (檢視者)
 - Contributor (作者群)
 - 管理員
 - 擁有者
4. 選擇新增。

移除使用者

1. 選取要移除的使用者。
2. 選擇移除。
3. 在確認對話方塊中，選擇移除使用者。

截止日期 雲端任務

任務是一組指示，AWS 讓 Deadline Cloud 用來排程和執行可用工作者的工作。建立任務時，您可以選擇要傳送任務的陣列和佇列。

提交者是數位內容建立 (DCC) 應用程式的外掛程式，可管理在 DCC 應用程式界面中建立任務。建立任務之後，您可以使用提交者將其傳送至截止日期雲端進行處理。

提交者會建立描述任務的 [Open Job Specification \(OpenJD\)](#) 範本。同時將資產檔案上傳至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。為了縮短上傳時間，提交者只會傳送自上次上傳至 Amazon S3 以來變更的檔案

您也可以使用下列方式建立任務。

- 從終端機 – 適用於提交使用命令列時感到放心之任務的使用者。
- 從指令碼 – 用於自訂和自動化工作負載。
- 從應用程式 – 適用於使用者的工作在應用程式中的時間，或應用程式的內容很重要的時間。

如需詳細資訊，請參閱 [《截止日期雲端開發人員指南》](#) 中的 [如何將任務提交至截止日期雲端](#)。

任務包含：

- 優先順序 – 截止日期雲端在佇列中處理任務的大致順序。您可以設定 0 到 100 之間的任務優先順序，通常會先處理具有較高優先順序的任務。具有相同優先順序的任務會依收到的順序處理。
- 步驟 – 定義要在工作者上執行的指令碼。步驟可能會有需求，例如最低工作者記憶體或其他需要先完成的步驟。每個步驟都有一或多個任務。
- 任務 – 傳送至工作者以執行的工作單位。任務是步驟的指令碼和參數的組合，例如用於指令碼的影格號碼。當所有步驟的所有任務都完成時，任務即完成。
- 環境 – 設定和銷毀多個步驟或任務共用的指示。

使用截止日期雲端提交者

提交者是與您的數位內容建立整合的工具，讓您可以將轉譯任務直接傳送到截止日期雲端。此整合可簡化您的工作流程，無需在應用程式之間切換或手動傳輸檔案。這可節省時間並降低發生錯誤的可能性。

提交者適用於許多熱門的 DCC 應用程式。安裝提交者，將截止日期雲端特定選項新增至應用程式的界面，通常在轉譯設定或匯出功能表中。

透過截止日期雲端提交者，您可以：

- 在您熟悉的 DCC 環境中設定轉譯任務參數
- 將任務提交至截止日期雲端，而不離開您的應用程式
- 降低與手動檔案傳輸相關的錯誤可能性
- 節省時間，因為您不需要在應用程式之間切換

若要尋找 DCC 應用程式的提交者，請查看 [設定您的工作站](#) 頁面。然後按照 中的指示 [設定您的工作站](#) 安裝提交者。

如果您的應用程式沒有支援的提交者，您仍然可以為您的應用程式執行任務。可能有可用的範例任務套件，或者您可以為應用程式的轉譯 CLI 命令建構簡單的提交者。如需詳細資訊，請參閱 [《截止日期雲端開發人員指南》](#) 中的 [截止日期雲端的開啟任務描述 \(OpenJD\) 範本](#)。

本主題中的範例使用Blender提交者，但使用其他提交者的步驟類似。

Note

若要使用提交者，您必須登入截止日期雲端監視器。

提交者有四個標籤：

主題

- [共用任務設定索引標籤](#)
- [任務特定設定索引標籤](#)
- [任務附件索引標籤](#)
- [主機需求索引標籤](#)

共用任務設定索引標籤

The screenshot shows the 'Submit to AWS Deadline Cloud' dialog box with the 'Shared job settings' tab selected. The dialog is organized into three main sections:

- Job Properties:** Contains fields for Name (testCube), Description, Priority (50), Initial state (READY), Maximum failed tasks count (20), Maximum retries per task (5), and Maximum worker count (No max worker count selected).
- Deadline Cloud settings:** Shows Farm (DocTestMonitor farm) and Queue (DocTestMonitor queue).
- Queue Environment: Conda:** Contains Conda Packages (blender=4.2.* blender-openjd=0.5.*) and Conda Channels (deadline-cloud).

At the bottom of the dialog, there are three status indicators: Credential source (DEADLINE_CLOUD_MONITOR_LOGIN), Authentication status (AUTHENTICATED), and AWS Deadline Cloud API (AUTHORIZED). Below these are buttons for Login, Logout, Settings..., Submit, and Export bundle.

共用任務設定索引標籤包含所有使用提交者傳送至截止日期雲端之任務常見的設定。這三個區段為：

- 任務屬性 – 設定任務的整體屬性。這些屬性存在於所有 DCC 應用程式的提交者中。

- 截止日期雲端設定 – 顯示任務傳送至的陣列和佇列。若要變更陣列和佇列，請使用提交者底部的設定...按鈕。
- 佇列環境 – 設定佇列環境中定義的參數值。Deadline Cloud 新增 DCC 應用程式的預設參數值，您可以視需要新增其他值。

任務特定設定索引標籤

The screenshot shows the 'Submit to AWS Deadline Cloud' dialog box with the 'Job-specific settings' tab selected. The settings are as follows:

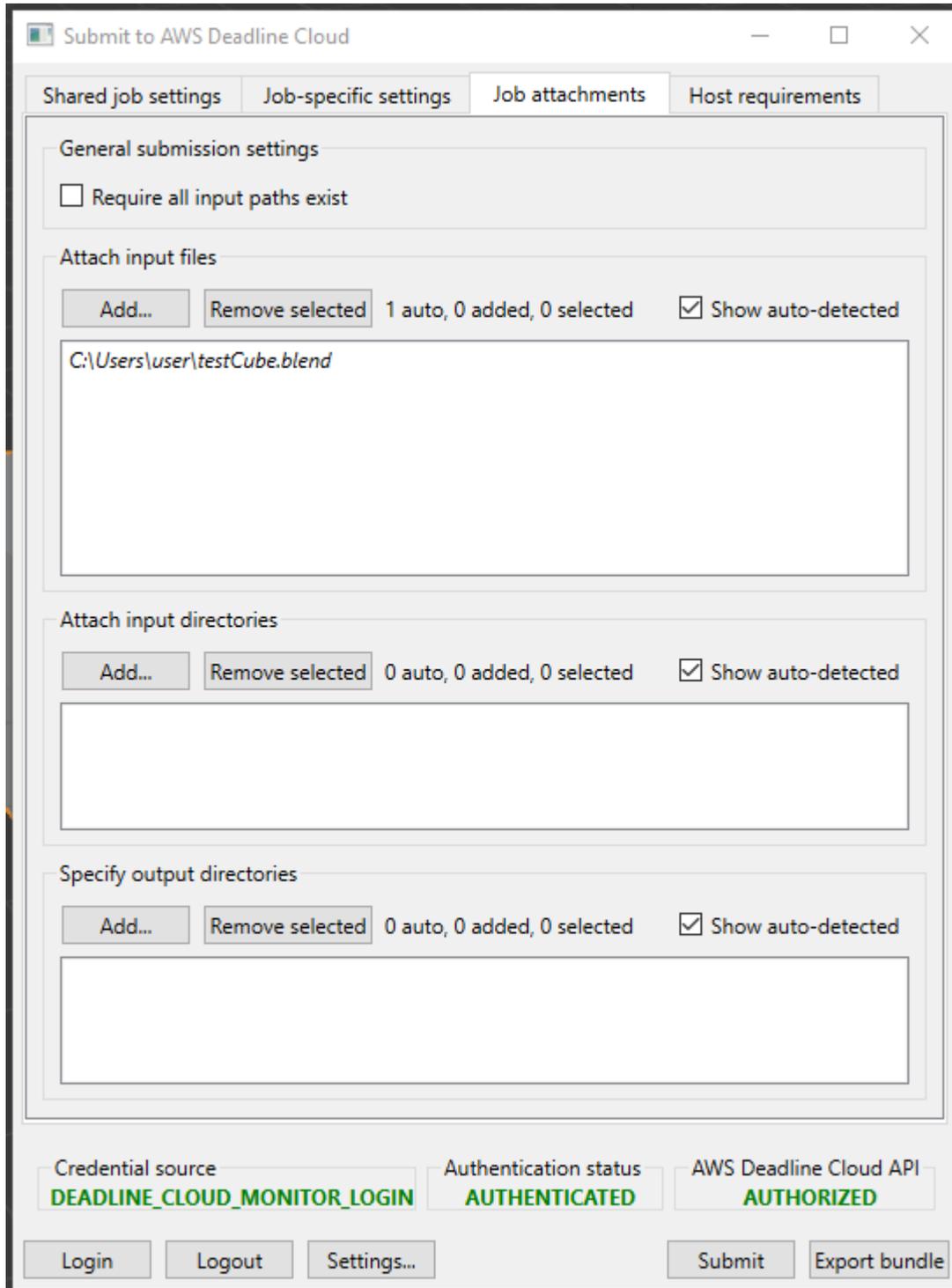
Setting	Value
Project Path	C:\Users\user\testCube.blend
Output Directory	C:\Users\user
Output File Prefix	output_####
Scene	Scene
Render Engine	cycles
View Layers	ViewLayer
Cameras	Camera
<input type="checkbox"/> Cycles GPU Rendering	CUDA
<input type="checkbox"/> Override Frame Range	1-250

At the bottom of the dialog, the following status indicators and buttons are visible:

- Credential source: DEADLINE_CLOUD_MONITOR_LOGIN
- Authentication status: AUTHENTICATED
- AWS Deadline Cloud API: AUTHORIZED
- Buttons: Login, Logout, Settings..., Submit, Export bundle

任務特定的設定索引標籤包含 DCC 應用程式特定的設定。根據應用程式中可用的選項指定這些設定。

任務附件索引標籤



任務附件索引標籤會顯示完成轉譯所需的所有檔案。提交者會嘗試尋找轉譯所需的所有檔案。其識別的檔案會以斜體顯示在清單中。

您可以新增其他輸入檔案和目錄，其中包含未自動偵測到的轉譯所需的其他資產。

如果您的任務將檔案寫入多個輸出目錄，您必須在此處指定目錄，讓 成為任務下載的一部分。

主機需求索引標籤

Submit to AWS Deadline Cloud

Shared job settings | Job-specific settings | Job attachments | **Host requirements**

Run on all available worker hosts

Run on worker hosts that meet the following requirements

All fields below are optional

Operating system -

CPU architecture -

Hardware requirements

vCPUs	Min	-	Max	-
Memory (GiB)	Min	-	Max	-
GPUs	Min	-	Max	-
GPU memory (GiB)	Min	-	Max	-
Scratch space	Min	-	Max	-

Custom host requirements

[More info](#)

Add amount Add attribute

Credential source: **DEADLINE_CLOUD_MONITOR_LOGIN** Authentication status: **AUTHENTICATED** AWS Deadline Cloud API: **AUTHORIZED**

Login Logout Settings... Submit Export bundle

主機需求索引標籤會設定處理任務所需的機群功能。功能是為整個機群指定，而不是機群中的個別工作者。

如果您的佇列有相關聯的資源限制，請使用新增數量按鈕來指定限制。如需詳細資訊，請參閱[建立任務的資源限制](#)

處理截止日期雲端任務

當任務進入佇列時，截止日期雲端會將其排程在與佇列相關聯的一或多個機群上。根據為機群設定的功能和特定步驟的主機需求來選擇機群。如果任務有任何與佇列相關聯的機群無法滿足的需求，任務的狀態會設為「不相容」，任務中的其餘步驟也會取消。

接下來，截止日期雲端會傳送指示給工作者，以設定步驟的工作階段。步驟所需的軟體必須在工作者執行個體上可用，才能執行任務。如果機群擴展設定允許，此服務會在多個工作者上開啟工作階段。

您可以在 Amazon Machine Image(AMI) 中設定軟體，或者您的工作者可以在執行時間從儲存庫或套件管理員載入軟體。您可以使用佇列、任務或步驟環境來部署您偏好的軟體。

Deadline Cloud 服務使用 OpenJD 範本來識別任務所需的步驟，以及每個步驟所需的任務。有些步驟與其他步驟有相依性，因此截止日期雲端會決定完成步驟的順序。然後，截止日期 Cloud 會將每個步驟的任務傳送給工作者來處理。當任務完成時，服務會在相同的工作階段中傳送另一個任務，或者工作者可以啟動新的工作階段。

在每個步驟中的所有任務完成後，任務即完成，且輸出已準備好下載到您的工作站。即使任務未完成，也可以下載完成的每個步驟和任務的輸出。

Note

Deadline Cloud 會在提交任務的 120 天後移除任務。移除任務時，也會移除與任務相關聯的所有步驟和任務。如果您需要重新執行任務，請再次提交任務的 OpenJD 範本。

監控截止日期雲端任務

AWS 截止日期雲端監視器可為您提供任務的整體檢視。使用它來：

- 監控和管理任務
- 檢視機群上的工作者活動
- 追蹤預算和用量
- 下載任務的結果。

若要監控特定任務，請選取包含任務的陣列和佇列，然後從清單中選取任務。您可以使用搜尋方塊來尋找佇列中的特定任務。

在任務、步驟或任務上按一下滑鼠右鍵，以查看項目的選項。您可以：

- 變更狀態
- 暫停和繼續項目
- 將項目排入佇列
- 下載輸出
- 對於任務：修改任務屬性，例如名稱、描述、優先順序或工作者計數上限。
- 對於任務：檢視任務和工作者日誌。

如需詳細資訊，請參閱[使用截止日期雲端監視器](#)。

任務或步驟中的每個任務都有一個狀態。任務或步驟的狀態取決於其任務的狀態。狀態由具有這些狀態的任務依序決定。步驟狀態的判斷方式與任務狀態相同。

The screenshot shows the AWS Job Monitor interface for the 'ProdRoseQueue' in the 'FuzzyPixelProdFarm' environment. The interface displays a list of 19 jobs with various statuses including Succeeded, Canceled, and Failed. Each job entry includes a progress bar, a status icon, and a status label.

Job name	User	Progress	Status	Duration	Priority	Current ...	Max wor...
sq0300_sh0060_noBrushstrokes_v27.mb		100% (162/162)	✓ Succeeded	98:14:19	50	0	-
sq0300_sh0060_noBrushstrokes_v27.mb		100% (162/162)	✓ Succeeded	01:03:56	50	0	-
sq0300_sh0060_noBrushstrokes_v25.mb		0% (0/162)	⊗ Canceled	-	50	0	-
sq0200_sh0072_light_v003.mb		0% (0/10)	⚠ Failed	00:03:02	50	0	-
sq0200_sh0072_light_v003.mb		100% (10/10)	✓ Succeeded	00:08:55	50	0	-
sq0200_sh0072_light_v003.mb		100% (10/10)	✓ Succeeded	00:06:45	50	0	-
sq0200_sh0072_light_v003.mb		40% (4/10)	⚠ Failed	165:36:35	50	0	-
sq0300_sh0050_lighting_v29_gtest.ma		0% (0/2)	⊗ Canceled	-	50	0	-
sq5000_sh0040_lightingHead_noBS_v02.mb		100% (1170/1170)	✓ Succeeded	02:26:29	50	0	-
sq5000_sh0040_lightingFull_greyScale_v02.mb		100% (1170/1170)	✓ Succeeded	01:37:54	50	0	-
sq5000_sh0040_lightingHead_v01.mb		0% (0/1170)	⊗ Canceled	-	50	0	-
sq5000_sh0040_lightingFull_noBS_v02.mb		100% (1170/1170)	✓ Succeeded	03:42:11	50	0	-
sq5000_sh0040_lightingHead_v04.mb		33% (1/3)	⊗ Canceled	00:38:38	50	0	-
sq5000_sh0040_lightingHead_v04.mb		33% (1/3)	⊗ Canceled	00:38:28	50	0	-
sq5000_sh0040_lightingHead_v04.mb		99% (1169/1170)	⚠ Failed	84:46:14	50	0	-
sq5000_sh0040_lightingFull_v02.mb		100% (1170/1170)	✓ Succeeded	06:04:12	50	0	-
sq5000_sh0040_lightingFull_v02.mb		0% (0/1170)	⚠ Failed	02:13:34	50	0	-
sq5000_sh0040_lightingHead_v04.mb		0% (0/1170)	⊗ Canceled	00:02:26	50	0	-
sq5000_sh0001_submitterTest_v03.mb		100% (1/1)	✓ Succeeded	840:08:16	50	0	-

下列清單說明狀態：

NOT_COMPATIBLE

任務與陣列不相容，因為沒有機群可以完成任務中的其中一個任務。

RUNNING

一或多個工作者正在從任務執行任務。只要至少有一個執行中的任務，任務就會標示為 RUNNING。

ASSIGNED

在任務中指派一或多個工作者做為其下一個動作。已設定環境，如果有的話。

STARTING

一或多個工作者正在設定環境以執行任務。

SCHEDULED

任務的任務會排程在一或多個工作者上，做為工作者的下一個動作。

READY

至少有一個任務已準備好進行處理。

INTERRUPTING

任務中至少有一個任務正在中斷。當您手動更新任務的狀態時，可能會發生中斷。也可能因為 Amazon Elastic Compute Cloud (Amazon EC2) Spot 價格變更而中斷而發生。

FAILED

任務中的一或多個任務未成功完成。

CANCELED

任務中的一或多個任務已取消。

SUSPENDED

任務中至少有一個任務已暫停。

PENDING

任務中的任務正在等待另一個資源的可用性。

SUCCEEDED

任務中的所有任務都已成功處理。

支援的軟體

Deadline Cloud 支援各種數位內容建立應用程式，用於 3D 轉譯、動畫、視覺效果和合成。支援的應用程式一律包含整合式提交者，但也可能支援 conda 套件、主機組態指令碼、以用量為基礎的授權等。下列應用程式會從截止日期雲端獲得官方支援。如需官方支援組態以外的自訂選項，請參閱《截止日期雲端開發人員指南》中的[為您的任務提供應用程式](#)和[為應用程式或外掛程式建立 conda 套件](#)。

截止日期雲端支援下列 DCC 應用程式：

主題

- [Adobe After Effects](#)
- [Autodesk 3ds Max](#)
- [Autodesk Maya](#)
- [Autodesk VRED](#)
- [Blender](#)
- [Epic Unreal 引擎](#)
- [Foundry Nuke](#)
- [KeyShot Studio](#)
- [Maxon Cinema 4D](#)
- [SideFX Houdini](#)

Adobe After Effects

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 After Effects 整合使用者指南](#)。

Adobe After Effects 是一種專業的數位視覺效果、動態圖形和合成應用程式。After Effects 受到 Deadline Cloud 的完全支援，具有全面的整合，包括提交者和 conda 套件，以提高渲染效能。

支援概觀

下列元件支援 After Effects：

- 提交者：整合提交者，用於透過自動場景和資產偵測從 After Effects 直接提交任務。
- Conda 套件：在服務受管機群上自動安裝的截止日期 Cloud。
- 跨平台相容性：使用 Windows 的工作者支援，提交 Windows 和 macOS 的支援。

After Effects 版本相容性

下表顯示 After Effects 版本的目前支援層級：

主要版本	提交者支援	Conda 支援
2024	Windows、macOS	Windows
2025	Windows、macOS	Windows

開始使用

完成下列步驟，以使用截止日期雲端設定事後效果。您將在工作站上安裝必要的提交者並監控，然後開始將轉譯任務提交到您的佇列。

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援截止日期雲端 conda 頻道的佇列環境進行設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端監視器安裝程式，在您的藝術家工作站上安裝截止日期雲端監視器。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用截止日期雲端提交者安裝程式，在您的藝術家工作站上安裝截止日期雲端效果後提交者。安裝提交者時，您可以選擇使用者安裝（不需要管理員）或系統安裝（僅限 Windows，需要管理員）。macOS 使用者必須使用使用者安裝。
 - 使用者安裝：在沒有管理員權限的情況下安裝至使用者目錄。提交者將是獨立的時段，而不是可停駐的面板。
 - Windows：C:\Users\\DeadlineCloudSubmitter\Submitters\AfterEffects\AE<version>
 - macOS：/Users/<user>/DeadlineCloudSubmitter/Submitters/AfterEffects/AE<version>
 - 系統安裝（僅限 Windows）：將安裝至 Adobe After Effects 安裝目錄做為可停駐面板。
 - Windows：C:\Program Files\Adobe\Adobe After Effects <version>\Support Files\Scripts\Script UI Panels

使用 After Effects 提交者

啟動提交者

啟動 After Effects 提交者

1. 啟動 Adobe After Effects。
2. 在 After Effects 中更新下列設定，以允許指令碼撰寫檔案並透過網路傳送通訊：
 - 針對 Windows，選擇編輯 > 偏好設定 > 指令碼和表達式，然後選擇允許指令碼寫入檔案和存取網路。
 - 針對 macOS，選擇效果後 > 設定 > 指令碼和表達式，然後選擇允許指令碼寫入檔案和存取網路。
3. 重新啟動 After Effects。
4. 根據您的安裝類型開啟截止日期雲端提交者：
 - 對於系統安裝，選取視窗，然後選擇 DeadlineCloudSubmitter.jsx。
 - 對於使用者安裝，選擇檔案 > 指令碼 > 執行指令碼檔案，然後尋找並選取 DeadlineCloudSubmitter.jsx。
5. (選用) 如果提交者已關閉且您使用使用者安裝，請選擇檔案 > 指令碼 > 最近指令碼檔案，然後選取 DeadlineCloudSubmitter.jsx 來重新開啟。

提交轉譯任務

從 After Effects 提交轉譯任務

1. 在提交者上選擇開啟轉譯佇列。
2. 將合成新增至轉譯佇列，並設定轉譯設定、輸出模組和輸出路徑。
3. 選擇提交者上的重新整理，在合成清單中查看您的合成。
4. 選取要轉譯的合成，然後選擇提交以提交轉譯任務。
5. 如果您看到有關執行指令碼檔案的警告，請遵循快顯中的指示來隱藏警告訊息。
6. 如果出現提示，請安裝任何 Python 程式庫。
7. 選擇提交以將您的任務傳送至截止日期雲端。
8. 監控任務，並使用截止日期雲端監視器下載輸出。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 After Effects 未出現在上面的版本表中，這將會失敗。

如果您需要不支援的 After Effects 版本，您有下列選項：

- 從 After Effects 提交任務時，您可以覆寫 CondaPackages 佇列參數，以指定要在工作者上使用的支援版本（例如 `aftereffects=2025`）。這可能會或可能不會運作，取決於場景使用的功能，以及 After Effects 如何搭配工作站版本中的場景運作。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列連結的支援版本使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

截止日期雲端 Conda 頻道

下表列出適用於截止日期雲端 conda 頻道中服務受管機群可用的 After Effects 的所有 conda 套件：

作業系統	套件	版本
Windows	事後效果	24.6
Windows	事後效果	25.1
Windows	事後效果	25.2

開放原始碼資源

提交者是開放原始碼，可在 GitHub 上取得：

- [After Effects 的截止日期雲端](#)
- [獨立 After Effects 任務套件](#)可在 GitHub 上取得。
- 提供[完整的使用者指南](#)。

Autodesk 3ds Max

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Autodesk 3ds Max 整合使用者指南](#)。

Note

將 Autodesk 3ds Max 與 AWS 截止日期雲端搭配使用時，您可以使用訂閱隨附的 Autodesk 雲端權利。如需有關雲端權利和訂閱利益的詳細資訊，請參閱 Autodesk 網站上的 [訂閱利益常見問答集：雲端權利](#)。

Autodesk 3ds Max 是一種專業 3D 電腦圖形程式，用於建立 3D 動畫、模型、遊戲和影像。Deadline Cloud 透過整合式提交者、主機組態指令碼、以用量為基礎的授權和轉接器，為 3ds Max 提供全面支援，以提高渲染效能。

支援概觀

下列元件支援 3ds Max：

- 提交者：從 3ds Max 直接提交任務的整合式提交者，具有自動場景和資產偵測。
- 主機組態指令碼：安裝 3ds Max 的主機組態指令碼範例。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：支援 Windows 的 Submitter，以及支援 Windows 的工作者和自動路徑映射。
- 以用量為基礎的授權：3ds Max 和 Corona Pay-as-you-go 授權。

3ds Max 版本相容性

下表顯示 3ds Max 版本的目前支援層級：

主要版本	提交者支援	主機組態支援
2024	Windows	Windows

主要版本	提交者支援	主機組態支援
2025	Windows	Windows
2026	Windows	Windows

3ds 與其他數位內容建立工具的最大差異

在截止日期雲端中，3ds Max 是使用主機組態指令碼而非 conda 套件進行安裝。由於 3ds Max 安裝程序的獨特需求，這與 Deadline Cloud 中的大多數其他 DCCs 不同，因為應用程式必須由系統管理員安裝。

開始使用

若要將 3ds Max 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。如果您想要使用 GPU 加速的轉譯功能，請使用 GPU 支援來設定機群。機群必須使用安裝 3ds Max 的主機組態指令碼進行設定。如需詳細資訊，請參閱 GitHub 上的 [3ds Max Host Configuration 指令碼設定](#) 和 3ds Max Host Config 範例。 [GitHub](#)
2. 使用截止日期雲端提交器在您的藝術家工作站上安裝截止日期雲端監視器和 3ds Max 提交器，並監控安裝程式。如需詳細資訊，請參閱 [設定您的工作站](#)。
3. 使用整合式提交者直接從 3ds Max 將您的任務提交到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

如需使用 3ds Max 整合提交器的詳細資訊，請參閱 [GitHub 上的 3ds Max 整合使用者指南](#)。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作軟體版本。您必須確保演出者使用的 3ds Max 版本與機群主機組態中設定的 3ds Max 版本相容。

可以透過主機組態指令碼支援較舊的 3ds Max 版本。不過，由於較舊的 Python 版本，整合式提交者可能無法運作。在這種情況下，自訂任務套件仍然可以做為截止日期雲端任務提交。

3ds Max 渲染器

使用包含它們的主機組態指令碼時，截止日期雲端支援使用下列轉譯器轉譯 3ds Max 任務：

轉譯器	轉譯器版本	提供的主機組態指令碼	以用量為基礎的授權支援
Autodesk Scanline	內建	N/A	N/A
Autodesk Raytracer (ART)	內建	N/A	N/A
Chaos V-Ray 6	6.x	是	是
Chaos V-Ray 7	7.x	是	是
Corona	最新	是	否

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得：

- [3ds Max Submitter 和轉接器](#)
- [截止日期雲端範例（適用於 3ds Max 工作流程範例）](#)
- [3ds Max 主機組態範例](#)

Autodesk Maya

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Maya 整合使用者指南](#)。

Autodesk Maya 是一種 3D 電腦動畫、建模、模擬和渲染軟體，用於建立互動式 3D 應用程式，包括視訊遊戲、動畫電影、電視影集和視覺效果。Maya 受到 Deadline Cloud 的全面整合支援，包括提交者、Conda 套件、以用量為基礎的授權和轉接器，以提高渲染效能。

支援概觀

下列元件支援 Maya：

- 提交者：從 Maya 直接提交任務的整合式外掛程式。
- Conda 套件：使用提交者時，在服務受管機群上自動安裝。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：支援 Windows、macOS 和 Linux 的 Submitter，以及支援 Windows 和 Linux 的工作者。
- 用量型授權：Maya 和轉譯器授權的 Pay-as-you-go。

Maya 版本相容性

下表顯示 Maya 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	轉譯引擎	以用量為基礎的授權
2024	Windows、macOS、Linux	Linux	Maya 軟體，Arnold (MtoA)	可用以用量為基礎的授權
2025	Windows、macOS、Linux	Linux	Maya 軟體、Arnold (MtoA)、V-Ray、Redshift	可用以用量為基礎的授權
2026	Windows、macOS、Linux	Linux	Maya 軟體、Arnold (MtoA)、V-Ray、Redshift	可用以用量為基礎的授權

開始使用

若要將 Maya 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援截止日期雲端 conda 頻道的佇列環境來設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端提交者在您的藝術家工作站上安裝截止日期雲端監視器和 Maya 提交者，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用整合式提交者直接從 Maya 提交您的任務到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 Maya 未出現在上述版本資料表中，這將會失敗。

如果您需要不支援的 Maya 版本，您有下列選項：

- 從 Maya 提交任務時，您可以覆寫 CondaPackages 佇列參數，以指定要在工作者上使用的支援版本（例如 maya=2026, maya-openjd=*）。這可能會或可能不會運作，取決於場景使用的功能，以及 Maya 如何搭配工作站版本中的場景運作。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對支援的版本使用 conda 配方做為起點：
 - [Maya conda 配方](#)
 - [Maya OpenJD 轉接器 conda 配方](#)

如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

Maya 轉譯引擎

Maya 支援多個與截止日期雲端完全相容的轉譯引擎：

轉譯引擎	Description	GPU 支援	備註	以用量為基礎的授權
Maya 軟體	內建 CPU 轉譯器	以 CPU 為基礎的	具有基本功能的舊版轉譯器	包含在 Maya 中

轉譯引擎	Description	GPU 支援	備註	以用量為基礎的授權
Arnold (MtoA)	Monte Carlo 射線追蹤器	GPU/CPU 混合	生產品質轉譯，需要 MtoA 5.3.5+	適用於 2024-2026
V-Ray	第三方擬真渲染器	GPU/CPU 混合	需要單獨的授權	適用於 2025-2026
Redshift	GPU 加速渲染器	GPU 最佳化	需要單獨的授權	適用於 2025-2026

Maya 整合提交者會自動偵測和設定所有轉譯引擎。提交者會維護適當的相依性處理和場景檔案管理。

Maya 外掛程式

外掛程式	外掛程式版本	提供的 Conda 配方	提供的 SMF Conda 套件	以用量為基礎的授權支援
Arnold (MtoA)	2024.5.3、2025.5.4、2026.5.5	是	是	是
V-Ray	2025.7、2026.7	是	是	是
Redshift	2025.4、2026.2.1	是	是	是

Arnold for Maya (MtoA)

支援使用 maya-mtoa conda 套件的 Arnold，並在使用 Maya 整合提交器時自動安裝。使用 Arnold 進行轉譯時，需支付額外的授權費用。

Conda 配方：[Maya-mtoa Conda 配方](#)

V-Ray 外掛程式

使用 maya-vray conda 套件支援 V-Ray，並在使用 Maya 整合提交器時自動安裝。使用 V-Ray 進行轉譯時，需支付額外的授權費用。

Conda 配方：[Maya-vray Conda 配方](#)

Redshift 外掛程式

使用 maya-redshift conda 套件支援 Redshift，並使用 Maya 整合提交程式自動安裝。使用 Redshift 進行轉譯時，需支付額外的授權費用。

Conda 配方：[Maya-redshift Conda 配方](#)

截止日期雲端 Conda 頻道

下表列出適用於 Maya 的所有 conda 套件，適用於截止日期雲端 conda 通道中的服務受管機群：

作業系統	套件	版本	備註
Linux	Maya	2024	包括 Maya 軟體轉譯器
Linux	Maya	2025	包括 Maya 軟體轉譯器
Linux	Maya	2026	包括 Maya 軟體轉譯器
Linux	maya-mtoa	2024.5.3	Arnold for Maya 2024
Linux	maya-mtoa	2025.5.4	Arnold for Maya 2025
Linux	maya-mtoa	2026.5.5	Arnold for Maya 2026
Linux	maya-openjd		包括 Maya 轉接器
Linux	maya-redshift	2025.4	Redshift for Maya 2025

作業系統	套件	版本	備註
Linux	maya-redshift	2026.2.1	Redshift for Maya 2026
Linux	maya-vray	2025.7	適用於 Maya 2025 的 V-Ray
Linux	maya-vray	2026.7	適用於 Maya 2026 的 V-Ray

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得：

- [Maya 提交者原始程式碼](#)
- [Maya conda 配方](#)

Autodesk VRED

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 VRED 整合使用者指南](#)。

Autodesk VRED 是一種專業的 3D 視覺化和虛擬原型軟體，可在逼真的虛擬環境中實現複雜的 3D 資料。設計人員和工程師廣泛使用此軟體來建立產品簡報、設計審查和虛擬原型，尤其是汽車產業。

支援概觀

Deadline Cloud 使用下列元件部分支援 VRED：

- 提交者：使用自動場景和資產偵測，從 VRED Pro 直接提交任務的整合式提交者。
- Conda 套件：使用 vredcore 套件，在 Linux 工作者的服務受管機群上自動安裝。
- 跨平台相容性：支援 Windows 和工作者支援 Linux 和自動路徑映射。(VRED Conda 套件僅適用於 Linux；Windows 工作者需要手動安裝。)

- BYOL 授權：VRED 需要自帶授權 (BYOL)。與 Deadline Cloud 中的一些其他 DCC 應用程式不同，以用量為基礎的授權不適用於 VRED。您必須擁有適用於轉譯陣列機群的有效 VRED 授權，並將授權伺服器設定為可從工作者存取。

VRED 版本相容性

下表顯示 VRED 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	以用量為基礎的授權
2026	Windows	Linux	需要 BYOL
2025	Windows	Linux	需要 BYOL

要求

若要將 VRED 與截止日期雲端搭配使用，您需要：

- 具備有效授權的 VRED Pro 或 VRED Core 2025/2026
- Python 3.11 或更新版本
- NVIDIA GPU 驅動程式 553.xx (建議獲得最佳效能)
- 可從轉譯陣列機群存取的有效 VRED 授權
- 選用：使用區域轉譯搭配射線追蹤時，適用於圖磚組件的 ImageMagick 靜態二進位檔

Important

VRED 整合需要自帶授權 (BYOL)。您必須擁有適用於轉譯陣列機群的有效 VRED 授權，並將授權伺服器設定為可從工作者節點存取。如需詳細資訊，請參閱[將服務受管機群連線至自訂授權伺服器](#)。

開始使用

若要將 VRED 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。確保您的機群可以存取您的 VRED 授權伺服器。

2. 使用截止日期雲端提交器在藝術家工作站上安裝截止日期雲端監控器和 VRED 提交器，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 開啟 VRED 並載入場景檔案。
4. 使用整合式提交者直接從 VRED 提交您的任務，方法是從功能表中選取截止日期雲端 > 提交至截止日期雲端。
5. 監控任務，並使用截止日期雲端監視器下載輸出。

進階組態

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 VRED 未出現在上述版本資料表中，則此操作將會失敗。

如果您需要不支援的 VRED 版本，您可以為要在工作者上安裝的所需版本建立自訂 Conda 配方和頻道。針對下列連結的支援版本使用 Conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 Conda 頻道的詳細資訊，請參閱[建立自訂 Conda 頻道](#)。

截止日期雲端 Conda 頻道

下表列出適用於 VRED 的所有 conda 套件，可供截止日期雲端 conda 通道中的服務受管機群使用：

作業系統	套件	版本	備註
Linux	vredcore	2025	適用於 Linux 的 VRED Core
Linux	vredcore	2026	適用於 Linux 的 VRED Core

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得：

- [VRED 提交者和轉接器](#)
- 支援的版本可在 GitHub 上使用 [VRED Conda 配方](#)。

Blender

Note

如需在您的工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Blender 整合使用者指南](#)。

Blender 是免費的開放原始碼 3D 電腦圖形軟體工具組，用於建立動畫電影、視覺效果、藝術、3D 列印模型、動態圖形、互動式 3D 應用程式、虛擬實境和電腦遊戲。Deadline Cloud 透過包括提交者、Conda 套件和轉接器在內的全面整合來支援 Blender，以提高渲染效能。

支援概觀

下列元件支援 Blender：

- 提交者：使用自動場景和資產偵測，從 Blender 直接提交任務的整合式提交者。
- Conda 套件：在服務受管機群上自動安裝的截止日期 Cloud。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：支援 Windows、macOS 和 Linux 的提交程式，以及支援 Windows 和 Linux 的工作者搭配自動路徑映射。

Blender 版本相容性

下表顯示 Blender 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	轉譯引擎
3.6	Windows、macOS、Linux	Linux	週期、Eevee、Workbench
4.2	Windows、macOS、Linux	Linux	週期、Eevee、Workbench
4.5	Windows、macOS、Linux	Linux	週期、Eevee、Workbench

開始使用

若要將 Blender 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援截止日期雲端 conda 頻道的佇列環境進行設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端監視器和提交器安裝程式，在您的藝術家工作站上安裝截止日期雲端監視器和 Blender 提交器。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用整合的提交者，直接從 Blender 提交您的任務到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

如需使用 Blender 整合提交者的詳細資訊，請參閱 [GitHub 上的 Blender 整合使用者指南](#)。

使用 Blender 提交器

若要從 Blender 提交轉譯任務：

1. 開啟 Blender 並載入場景檔案。
2. 設定您的轉譯設定，包括輸出路徑、影格範圍和轉譯引擎 (Cycles、Eevee 或 Workbench)。
3. 從頂端功能表中，選取轉譯 > 截止日期雲端。
4. 在截止日期雲端提交對話方塊中：
 - 輸入任務名稱和描述。
 - 選取您的目標陣列和佇列。
 - 設定任務附件以包含您的場景檔案和任何外部資產。
 - 檢閱轉譯設定和影格範圍。
5. 選擇提交，將您的任務傳送至佇列。

截止日期雲端提交會自動偵測您的場景相依性、設定適當的轉譯引擎，以及使用適用於 Blender 版本的正確 conda 套件提交任務。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 Blender 未出現在上述版本資料表中，則此操作將會失敗。

如果您需要不支援的 Blender 版本，您有下列選項：

- 從 Blender 提交任務時，您可以覆寫 CondaPackages 佇列參數，以指定要在工作者上使用的支援版本（例如 `blender=4.5, blender-openjd=*`）。這可能會或可能不會運作，取決於您的場景所使用的功能，以及 Blender 如何搭配工作站版本中的場景運作。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列連結的支援版本使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

Blender 轉譯引擎

Blender 包含數個支援的內建轉譯引擎：

轉譯引擎	Description	GPU 支援	備註
週期	以物理為基礎的路徑追蹤器	GPU/CPU 混合	GPU 加速的生產品質轉譯
逸出者	即時轉譯引擎	GPU 最佳化	快速檢視區和最終轉譯
Workbench	固體著色引擎	GPU 最佳化	用於建模和塑造工作流程

Blender 整合提交者會自動偵測和設定所有轉譯引擎。搭配啟用 GPU 的執行個體使用服務受管機群時，可使用 GPU 加速。

截止日期雲端 Conda 頻道

下表列出適用於 Blender 的所有 conda 套件，適用於截止日期雲端 conda 通道中的服務受管機群：

作業系統	套件	版本	備註
Linux	混合器	3.6	包含所有內建轉譯引擎

作業系統	套件	版本	備註
Linux	混合器	4.2	包含所有內建轉譯引擎
Linux	混合器	4.5	包含所有內建轉譯引擎
Linux	blender-openjd		包括 Blender 轉接器

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得：

- [Blender 的截止日期雲端](#)
- [Blender Conda 配方](#)可在 GitHub 上取得支援的版本。

Epic Unreal 引擎

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Unreal Engine 整合使用者指南](#)。

Unreal Engine 是一種即時 3D 建立工具，適用於擬真視覺效果和沉浸式體驗。Deadline Cloud 透過提交者、Conda 套件和轉接器支援 Unreal Engine，以提高渲染效能。

支援概觀

下列元件支援 Unreal Engine：

- 提交者：整合式提交者外掛程式，用於透過自動場景和資產偵測從 Unreal Engine 直接提交任務。
- Conda 套件：在服務受管機群上自動安裝的截止日期 Cloud。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：僅限 Windows 的 Submitter 和工作者支援。

- 電影渲染佇列整合：支援 Unreal 的電影渲染佇列系統。

Unreal Engine 版本相容性

下表顯示 Unreal Engine 版本的目前支援層級：

主要版本	提交者支援	Conda 支援
5.4	Windows	Windows
5.5	Windows	Windows
5.6	Windows	Windows

開始使用

先決條件

在安裝 Unreal Engine 提交者之前，請確定您有下列項目：

- Windows 工作站 (Windows 10 或更新版本)
- 支援的 Unreal Engine 版本已安裝
- 已安裝截止日期的雲端監視器 ([在此處下載](#))
- 使用具備 GPU 功能的 Windows 服務受管機群或具有 Unreal Engine、Unreal Engine 轉接器和授權設定的客戶受管機群存取截止日期雲端陣列

安裝 Unreal Engine Submitter

Unreal Engine 提交者會將 Deadline Cloud 功能新增為 Unreal Engine 的外掛程式，可讓您將 Movie Render 佇列任務直接提交至 Deadline Cloud 進行轉譯。

如需詳細安裝指示，請參閱 [Unreal Submitter 設定指南](#)。

更新提交者

重新整理您的 Git 儲存庫並重新執行安裝指令碼，如 [Unreal Submitter 設定指南](#) 中所述。

使用 Unreal Engine 提交者

若要使用 Unreal Engine 提交者：

1. 使用專案開啟 Unreal Engine。
2. 使用所需的鏡頭和渲染設定來設定您的電影渲染佇列。
3. 從 Unreal Engine 介面存取截止日期雲端提交者外掛程式。
4. 設定您的任務設定，包括：
 - 電影渲染佇列組態
 - 輸出路徑和格式
 - 轉譯參數
5. 選擇提交，將您的任務傳送至截止日期雲端。

提交者會自動偵測 Movie Render 佇列組態，並處理資產相依性，包括專案外掛程式和內容檔案。

進階組態。

服務受管機群與客戶受管機群

服務受管機群 (SMF)

在服務受管機群上，Unreal Engine 和轉接器會透過具有預設佇列環境的 `deadline-cloud` Conda 通道自動提供。這可提供最簡單的設定體驗。

客戶受管機群 (CMF)

對於客戶受管機群，必須在工作者主機上手動安裝 Unreal Engine 和轉接器。此設定提供更多控制，並支援其他功能，例如 Perforce 整合。

如需詳細說明，請參閱 [CMF 工作者設定指南](#)。

Perforce 整合

Unreal Engine 整合包含 Perforce 版本控制系統的支援。整合提供公用程式，可在轉譯期間同步相依檔案和管理 Perforce 工作區。

如需將 Perforce 整合任務提交至截止日期雲端的詳細資訊，請參閱 [Perforce 指南](#)。

Unreal Engine 轉譯功能

Unreal Engine 的轉譯系統可全面支援：

功能	Description	備註
電影渲染佇列	高品質離線轉譯	與任務提交整合
排序器	時間軸型動畫系統	自動拍攝偵測和處理
專案外掛程式	自訂外掛程式支援	自動偵測和包含
資產相依性	內容檔案管理	全方位資產追蹤
黏性轉譯	拍攝之間的應用程式持久性	改善多鏡頭序列的效能

Unreal Engine 整合提交者會自動偵測和設定所有轉譯功能。轉接器會維護適當的相依性處理，並支援高效的多鏡頭轉譯，而不會重新啟動 Unreal Engine。

截止日期雲端 Conda 頻道

下表列出適用於 Unreal Engine 的所有 deadline-cloud conda 套件，可供 Conda 頻道中的服務受管機群使用：

作業系統	套件	版本
Windows	unreal-engine	5.4
Windows	unreal-engine	5.5
Windows	unreal-engine	5.6
Windows	unreal-engine-openjd	

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上使用：

- [Unreal Engine 的截止日期雲端](#)

Foundry Nuke

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Nuke 整合使用者指南](#)。

Foundry Nuke 是一種節點型數位合成和視覺效果應用程式，用於電視和電影後製。使用提交者、Conda 套件和轉接器的 Deadline Cloud 支援 Nuke，以提高渲染效能。

支援概觀

下列元件支援 Nuke：

- 提交者：整合式提交者外掛程式，用於透過自動場景和資產偵測從 Nuke 直接提交任務。
- Conda 套件：安裝 nuke 版本 15 和 16 的套件可在服務受管機群的 Deadline Cloud Conda 頻道上取得。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：僅支援 Windows、macOS 和 Linux 的提交者，以及僅支援 Linux 的工作者與自動路徑映射。

Nuke 版本相容性

下表顯示 Nuke 版本的目前支援層級：

主要版本	提交者支援	Conda 支援
15	Windows、macOS、Linux	Linux
16	Windows、macOS、Linux	Linux

開始使用

若要將 Nuke 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援截止日期雲端 conda 頻道的佇列環境來設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端提交者在您的藝術家工作站上安裝截止日期雲端監視器和 Nuke 提交者，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用整合式提交者直接從 Nuke 提交您的任務到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

啟動提交者

在 Nuke 中啟動截止日期雲端提交者

Note

Nuke 的支援是使用服務受管機群的 Conda 環境提供。如需詳細資訊，請參閱[預設conda佇列環境](#)。

1. 使用截止日期雲端提交者在您的藝術家工作站上安裝截止日期雲端監視器和 Nuke 提交者，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
2. 開啟 Nuke。
3. 開啟資產根目錄中存在相依性的 Nuke 指令碼。
4. 選擇 AWS 截止日期，然後選擇提交至截止日期雲端以啟動提交者。
 - a. 如果您尚未在截止日期雲端提交者中驗證，登入資料狀態會顯示為 NEEDS_LOGIN。
 - b. 選擇 Login (登入)。
 - c. 在登入瀏覽器視窗中，使用您的使用者登入資料登入。
 - d. 選擇 Allow (允許)。您現在已登入，登入資料狀態會顯示為 AUTHENTICATED。
5. 選擇提交。

使用 Nuke 提交者

若要使用 Nuke 提交者：

1. 開啟 Nuke。
2. 載入已設定必要寫入節點的合成。

3. 從功能表中，選擇截止日期雲端以啟動提交者。
4. 如果您尚未進行身分驗證，請選擇登入並使用您的登入資料進行身分驗證。
5. 在提交者界面中設定您的任務設定，包括：
 - 影格範圍設定
 - 寫入節點選擇
 - 輸出路徑和格式
6. 選擇提交，將您的任務傳送至截止日期雲端。

提交者會自動偵測合成中的寫入節點，並允許您選取要轉譯的節點。它還處理自動輸入/輸出路徑偵測，並支援多個檢視轉譯。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站的 Nuke 版本未出現在上面的版本表中，這將會失敗。

如果您需要不支援的 Nuke 版本，您有下列選項：

- 從 Nuke 提交任務時，您可以覆寫 CondaPackages 佇列參數，以指定要在工作者上使用的支援版本（例如 `nuke=16`，`nuke-openjd=*`）。這可能會或可能不會運作，取決於您的合成所使用的功能，以及 Nuke 如何搭配工作站版本中的合成運作。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列連結的支援版本使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

自訂 Nuke 可執行檔

如果 PATH 上無法使用特定 Nuke 可執行檔，您可以將 `NUKE_EXECUTABLE` 環境變數設定為指向該可執行檔。

OpenColorIO 支援

Nuke 整合包含對 OpenColorIO (OCIO) 顏色管理工作流程的完整支援。色彩組態會自動偵測並包含在任務提交中，以確保整個轉譯陣列的顏色處理一致。

Nuke 合成功能

Nuke 的合成引擎為下列項目提供全面支援：

功能	Description	備註
寫入節點	多個輸出格式和轉碼器	提交者自動偵測
影格範圍	自訂影格範圍規格	支援覆寫和預設範圍
多個檢視	立體聲和多視角轉譯	正確處理檢視特定的輸出
顏色管理	OpenColorIO 整合	自動 OCIO 組態偵測
路徑映射	跨平台路徑轉譯	無縫 Windows/Linux 相容性

Nuke 整合提交者會自動偵測和設定合成功能。提交者會維護複雜組合的適當相依性處理和資產管理。

截止日期雲端 Conda 頻道

下表列出適用於 Nuke 的 conda 套件，適用於截止日期雲端 conda 通道中的服務受管機群：

作業系統	套件	版本	備註
Linux	nuke	15	包含內建合成引擎
Linux	nuke	16	包含內建合成引擎
Linux	nuke-openjd		包括 Nuke 轉接器

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上使用：

- [Nuke 的截止日期雲端](#)
- [Nuke Conda 配方](#)可在 GitHub 上取得支援的版本。

KeyShot Studio

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 KeyShot 整合使用者指南](#)。

KeyShot Studio 是由 Luxion 開發的即時光線追蹤和全域照明計畫，用於渲染 3D 模型和動畫。

支援概觀

下列元件支援 KeyShot Studio：

- 提交者：從 KeyShot 直接提交任務的整合式提交者延伸模組，具有自動場景和資產偵測。
- Conda 套件：預先封裝的軟體，可在服務受管機群上自動安裝。
- 跨平台相容性：支援 Windows 和 macOS 的 Submitter，以及支援 Windows 的工作者。
- 用量型授權：KeyShot 授權的 Pay-as-you-go。

KeyShot 版本相容性

下表顯示 Keyshot 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	轉譯引擎	以用量為基礎的授權
2024	Windows、macOS	Windows	內建射線追蹤器	可用以用量為基礎的授權
2025	Windows、macOS	Windows	內建射線追蹤器	可用以用量為基礎的授權

開始使用

將 KeyShot 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援 `deadline-cloud conda` 頻道的佇列環境來設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端提交器在藝術家工作站上安裝截止日期雲端監視器和 KeyShot 提交器，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。

使用 KeyShot 提交者

若要使用 KeyShot 提交者：

1. 開啟 KeyShot。
2. 選擇 Windows > 指令碼主控台 > 提交至截止日期雲端並執行。
3. 從顯示的對話方塊中選取您偏好的提交模式。
4. 在提交者界面中設定您的任務設定。
5. 選擇提交以將您的任務傳送至截止日期雲端。
6. 監控任務，並使用截止日期雲端監視器下載輸出。

如需使用適用於截止日期雲端的 KeyShot 提交器的詳細資訊，請參閱 [KeyShot 提交器指南](#)。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 KeyShot 未出現在上述版本資料表中，則此操作會失敗。

如果您需要不支援的 KeyShot 版本，您有下列選項：

- 從 KeyShot 提交任務時，您可以覆寫 `CondaPackages` 佇列參數，以指定要在工作者上使用的支援版本（例如 `keyshot=2024`）。任務可能會成功執行，具體取決於場景使用的功能，以及 KeyShot 如何與工作站版本中的場景搭配使用。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列連結的支援版本使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

截止日期雲端 Conda 頻道

下表列出適用於 Conda 頻道中服務受管機群之 Keyshot 的所有 deadline-cloud conda 套件：

作業系統	套件	版本	備註
Windows	keyhot	2024	包含內建的射線追蹤器
Windows	keyhot	2025	包含內建的射線追蹤器
Linux	keyhot-openjd		包含 KeyShot 轉接器

開放原始碼資源

提交者是開放原始碼，可在 GitHub 上取得：

- [KeyShot 的截止日期雲端](#)
- [獨立 KeyShot 任務套件](#)可在 GitHub 上取得。
- 提供[完整的使用者指南](#)。

Maxon Cinema 4D

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Cinema 4D 整合使用者指南](#)。

Cinema 4D 是 Maxon 的專業 3D 動畫、建模、模擬和渲染軟體解決方案。Deadline Cloud 支援電影 4D，包括提交者、Conda 套件、以用量為基礎的授權和轉接器，以提高效能。

支援概觀

下列元件支援電影 4D：

- 提交者：使用自動場景和資產偵測，從 Cinema 4D 直接提交任務的整合式提交者。
- Conda 套件：使用提交者時，在服務受管機群上自動安裝。
- 轉接器：中介軟體可更有效率地使用黏性工作階段和其他監控進行轉譯。
- 跨平台相容性：提交支援 Windows 和 macOS，以及工作者支援 Windows 和 Linux，以及自動路徑映射。
- 以用量為基礎的授權：電影 4D、Redshift 和 Red Giant 授權的隨 Pay-as-you-go 授權。

電影 4D 版本相容性

下表顯示 Cinema 4D 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	以用量為基礎的授權
2024	Windows、macOS	Windows	可用以用量為基礎的授權
2025	Windows、macOS	Windows , Linux	可用以用量為基礎的授權
2026	Windows、macOS	Windows , Linux	可用以用量為基礎的授權

開始使用

若要在截止日期雲端上使用 Cinema 4D 全受管：

1. 建立服務受管機群，並將其與佇列建立關聯。如果您想要使用需要 GPU 的 Redshift 或 Red Giant 功能，請使用 GPU 支援來設定機群。您的佇列應使用支援截止日期雲端 conda 頻道的佇列環境進行設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用截止日期雲端提交器在您的藝術家工作站上安裝截止日期雲端監視器和電影 4D 提交器，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用整合式提交器，直接從 Cinema 4D 提交您的任務到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

如需使用 Cinema 4D 整合提交者的詳細資訊，請參閱 [GitHub 上的 Cinema 4D 整合使用者指南](#)。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果上述版本資料表中未顯示 Cinema 4D 的工作站版本，則會失敗。

如果您需要不支援的 Cinema 4D 版本，您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列開放原始碼資源區段中連結的支援版本，使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

如果您為不同版本的 Cinema 4D 建立 conda 套件，則應確保它將正確取得授權。如果版本與上表中支援版本的授權相容，則以用量為基礎的授權將自動運作。您也可以將自己的授權帶到服務受管機群，方法是將 [Connect 服務受管機群追蹤到自訂授權伺服器](#)。

Cinema 4D 外掛程式

外掛程式	外掛程式版本	提供的 Conda 配方	提供的 SMF Conda 套件	以用量為基礎的授權支援
Redshift	2026.3.0	N/A	是	是
Redshift	2025.6.0	N/A	是	是
紅色巨型	2025.x	否	否	是
V-Ray	7.x	是	否	是
Insydium X-Particles	2024.x	是	否	N/A
C4DtoArnold	4.8.4.1	是	是	是

*包含在基本電影 4D 套件配方中

Maxon Redshift

Redshift 轉譯器包含在所有 Cinema 4D conda 套件中，並在適當時使用 Cinema 4D 整合提交器時自動使用。使用 Redshift 進行轉譯時，需支付額外的授權費用。如需截止日期雲端定價的詳細資訊，請參閱[截止日期雲端定價](#)。

Maxon Red Giant

Red Giant 是全方位的工具組，專為影片後製、動態圖形和視覺效果而設計。它提供豐富的顏色分級、平滑轉換、逼真的視覺效果、動作設計範本和工具，以建立和編輯視覺效果。如需詳細資訊，請參閱 [Red Giant](#)。

Red Giant 需要在服務受管機群上自訂設定。提供主機組態指令碼，您可以在截止日期雲端機群中使用。設定完成後，截止日期雲端用量型授權支援 Red Giant，且不需要進一步的組態即可操作。

V-Ray 外掛程式

V-Ray 是一種 3D 擬真射線追蹤渲染外掛程式。服務受管機群目前尚未完全支援適用於 Cinema 4D 的 V-Ray。提供 Conda 配方，您可以用來建立自己的 Conda 頻道，以便在截止日期雲端陣列中使用。如需建立自訂 conda 頻道的詳細資訊，請參閱 [建立自訂 conda 頻道](#)。安裝後，期限雲端用量型授權支援 V-Ray，且不需要進一步的組態即可操作。

C4DToArnold

Autodesk Arnold 軟體是進階的 Monte Carlo 射線追蹤渲染器。如需詳細資訊，請參閱 [Arnold](#)。服務受管機群完全支援 C4DToArnold。

Insydium X-Particles

X-Particles 是適用於 Maxon 電影 4D 的全功能進階粒子和 VFX 系統。如需詳細資訊，請參閱 [X-Particles](#)。服務受管機群目前尚未完全支援 Insydium X-Particles。提供 Conda 配方，您可以用來建立自己的 Conda 頻道，以便在截止日期雲端陣列中使用。如需建立自訂 conda 頻道的詳細資訊，請參閱 [建立自訂 conda 頻道](#)。當您從 X-Particles 套件建立 conda 套件時，它會包含您購買的授權。在服務受管機群上操作不需要額外的組態。

截止日期雲端 Conda 頻道

下表列出適用於 Cinema 4D 的所有 conda 套件，可供截止日期雲端 conda 頻道中的服務受管機群使用：

作業系統	套件	版本	備註
Windows	電影4d	2024	包括標準、實體和 Redshift 轉譯器

作業系統	套件	版本	備註
Windows , Linux	電影4d	2025	包括標準、實體和 Redshift 轉譯器
Windows , Linux	電影4d	2026	包括標準、實體和 Redshift 轉譯器
Windows , Linux	cinema4d-c4dtoa	2025	Cinema4D 到 Arnold
Windows	電影4d-c4dtoa	2026	Cinema4D 到 Arnold
Windows , Linux	cinema4d-openjd		包含電影 4D 轉接器

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得：

- [電影 4D 的截止日期雲端](#)
- [適用於 C4D 2024、C4D 2025、INSYDIUM X-PARTICLES 外掛程式、C4DtoA 外掛程式和 V-Ray 外掛程式的電影 4D Conda 配方](#)可在 GitHub 上取得。C4D C4DtoA
- 包含[主機組態指令碼](#)以支援 Red Giant 外掛程式。

SideFX Houdini

Note

如需在工作站上安裝、設定和使用此整合的詳細資訊，請參閱 [GitHub 上的 Houdini 整合使用者指南](#)。

SideFX Houdini 是一種 3D 程序軟體，用於在電影、電視、廣告和影片遊戲管道中建模、建構、動畫、VFX、注視開發、照明和渲染。Houdini 由 Deadline Cloud 提供完整整合的完全支援，包括提交者、Conda 套件和轉接器，以提高渲染效能。

支援概觀

下列元件支援 Houdini：

- 提交者：整合式轉譯輸出節點 (ROP)，用於從 Houdini 直接提交任務，具有自動場景和資產偵測。
- Conda 套件：在服務受管機群上自動安裝的截止日期 Cloud。
- 轉接器：中介軟體，可透過黏性工作階段和其他監控有效率地轉譯。
- 跨平台相容性：支援 Windows、macOS 和 Linux 的提交程式，以及支援 Windows 和 Linux 的工作者搭配自動路徑映射。

Houdini 版本相容性

下表顯示 Houdini 版本的目前支援層級：

主要版本	提交者支援	Conda 支援	轉譯引擎	以用量為基礎的授權
19.0	Windows、macOS、Linux	Linux	Mantra、Karma CPU、Karma XPU	可用以用量為基礎的授權
19.5	Windows、macOS、Linux	Linux	Mantra、Karma CPU、Karma XPU	可用以用量為基礎的授權
20.0	Windows、macOS、Linux	Linux	Mantra、Karma CPU、Karma XPU	可用以用量為基礎的授權
20.5	Windows、macOS、Linux	Linux	Mantra、Karma CPU、Karma XPU	可用以用量為基礎的授權
21.0	Windows、macOS、Linux	Linux	Mantra、Karma CPU、Karma XPU	可用以用量為基礎的授權

開始使用

若要將 Houdini 與截止日期雲端搭配使用：

1. 建立服務受管機群，並將其與佇列建立關聯。您的佇列必須使用支援截止日期雲端 conda 頻道的佇列環境來設定。如需詳細資訊，請參閱[建立佇列環境](#)。
2. 使用 Deadline Cloud Submitter 在藝術家工作站上安裝 Deadline Cloud Monitor 和 Houdini Submitter，並監控安裝程式。如需詳細資訊，請參閱[設定您的工作站](#)。
3. 使用整合的提交者，直接從 Houdini 提交您的任務到佇列。
4. 監控任務，並使用截止日期雲端監視器下載輸出。

使用 Houdini 提交者

若要使用 Houdini 提交者：

1. 開啟 Houdini。
2. 在網路編輯器中，通常在 Houdini 的右下角，選取/out網路。
3. 按 Tab，然後輸入 deadline。
4. 選取截止日期雲端選項，並將其放置在/out網路中以建立節點。
5. 將現有/out網路中最後一個轉譯輸出節點 (ROP) 的輸出（例如，Karma、Mantra 或合成）連接到截止日期雲端節點的輸入。
6. 選擇截止日期雲端節點。
7. 在節點編輯器中輸入任何任務設定，通常位於 Houdini 的右上角。
8. 在節點編輯器的右下角，選擇提交。

截止日期雲端提交會自動剖析連線/out的網路樹狀目錄，並提交每個節點做為維護相依性樹狀目錄中的步驟。/out 也支援使用以外的非預設轉譯網路。

進階組態。

使用不支援的版本

Deadline Cloud 僅支援和測試上表中的工作站和工作者軟體版本。使用提交者時，工作者會嘗試安裝與工作站相同的版本。如果工作站版本的 Houdini 未出現在上述版本表中，則可能會失敗。

如果您需要不支援的 Houdini 版本，您有下列選項：

- 從 Houdini 提交任務時，您可以覆寫 CondaPackages 佇列參數，以指定要在工作者上使用的支援版本（例如 houdini=21.0, houdini-openjd=*）。這可能會或可能不會運作，取決於場景使用的功能，以及 Houdini 如何搭配工作站版本中的場景運作。
- 您可以為要在工作者上安裝的所需版本建置自訂 conda 配方和頻道。針對下列連結的支援版本使用 conda 配方做為起點，並將您想要的版本封裝在自訂 conda 頻道中。如需建立自訂 conda 頻道的詳細資訊，請參閱[建立自訂 conda 頻道](#)。

Houdini 轉譯引擎

Houdini 支援多個與截止日期雲端相容的轉譯引擎：

轉譯引擎	Description	GPU 支援
Karma CPU	以 USD 為基礎的現代渲染器 (CPU 變體)	以 CPU 為基礎的
Karma XPU	現代 USD 型渲染器 (GPU 變體)	GPU 加速
曼特拉	傳統 Houdini 轉譯器	以 CPU 為基礎的
阿諾	第三方 Monte Carlo 射線追蹤器	GPU/CPU 混合
V-Ray	第三方擬真渲染器	GPU/CPU 混合
Redshift	GPU 加速渲染器	GPU 最佳化

Houdini 整合提交者會自動偵測和設定這些轉譯引擎，並自動授權用量。提交者會在連接的轉譯輸出節點 (ROPs) 之間維護相依性樹狀目錄。

截止日期雲端 Conda 頻道

下表列出適用於 Houdini 的所有 conda 套件，適用於截止日期雲端 conda 通道中的服務受管機群：

作業系統	套件	版本	備註
Linux	奧迪尼	19.0	包括 Mantra 和 Karma 轉譯器
Linux	奧迪尼	19.5	包括 Mantra 和 Karma 轉譯器
Linux	奧迪尼	20.0	包括 Mantra 和 Karma 轉譯器
Linux	奧迪尼	20.5	包括 Mantra 和 Karma 轉譯器
Linux	奧迪尼	21.0	包括 Mantra 和 Karma 轉譯器
Linux	houdini-openjd		包含 Houdini 轉接器

開放原始碼資源

提交者和轉接器是開放原始碼，可在 GitHub 上取得。Houdini Conda 配方可在 GitHub 上取得支援的版本。

- [GitHub 上的 Houdini 提交者原始程式碼](#)
- [GitHub 上的場景和工作流程範例](#)
- [GitHub 上支援版本的 Conda 配方](#)

截止日期雲端的檔案儲存

工作者必須能夠存取包含處理任務所需的輸入檔案的儲存位置，以及存放輸出的位置。AWS 截止日期雲端為儲存位置提供兩個選項：

- 透過任務附件，Deadline Cloud 會在工作站和 Deadline Cloud 工作者之間來回傳輸任務的輸入和輸出檔案。若要啟用檔案傳輸，Deadline Cloud 會在您的 中使用 Amazon Simple Storage Service (Amazon S3) 儲存貯體 AWS 帳戶。

當您使用任務附件搭配 Linux 服務受管機群時，您可以啟用虛擬檔案系統 (VFS) 來掛載任務附件檔案，並視需要存取它們，而不是在任務開始時將其同步到工作者。

- 透過共用儲存，您可以使用檔案與作業系統共用來提供檔案的存取權。

當您使用跨平台共用儲存時，您可以建立儲存設定檔，以便工作者可以將路徑映射到兩個不同作業系統之間的檔案。

您也可以整合第三方雲端儲存解決方案，例如 LucidLink，以及使用主機組態指令碼的服務受管機群。如需詳細資訊，請參閱適用於 M&E [的部落格上的使用適用於截止日期雲端的服務受管機群指令碼設定 LucidLink](#)。AWS

主題

- [截止日期雲端中的儲存設定檔](#)
- [截止日期雲端中的任務附件](#)

截止日期雲端中的儲存設定檔

當您使用來自多個作業系統或不同檔案系統掛載的工作站和機群工作者主機時，您可以在陣列中建立儲存設定檔，以指出相同檔案系統掛載在不同系統上的位置。當 Deadline Cloud 在與其提交的工作站不同的儲存設定檔上執行任務時，它會轉換儲存設定檔中設定的目錄中的檔案系統路徑。

在截止日期雲端陣列中使用儲存描述檔可啟用下列行為：

- 將任務提交至佇列時，任務參考的檔案會依工作站儲存描述檔進行分類：
 - 位於共用檔案系統位置下的檔案將單獨保留。
 - 位於本機檔案系統位置下的檔案，將上傳至任務附件 S3 儲存貯體，以連接至任務。先前上傳的檔案不會再次上傳。

- 不屬於任何檔案系統位置的檔案也會連接至任務。任務提交者將警告這些檔案路徑，除非它們位於本機截止日期雲端設定中的已知路徑。
- 當任務在具有與提交工作站不同作業系統或儲存描述檔的機群工作者主機上執行時，任務使用的檔案路徑將從提交儲存描述檔映射到機群儲存描述檔。
- 下載任務輸出時，針對不同作業系統或儲存描述檔提交的任務，其路徑將從提交儲存描述檔映射至本機工作站儲存描述檔。

如需詳細資訊，請參閱AWS 《截止日期雲端開發人員指南》中的[儲存設定檔和路徑映射](#)。

建立儲存設定檔

1. 開啟[截止日期雲端主控台](#)。
2. 從入門中，選擇前往截止日期雲端儀表板。
3. 選擇陣列，然後選擇儲存設定檔索引標籤。
4. 選擇建立儲存設定檔。
5. 從下拉式清單中選取作業系統。
6. 輸入儲存設定檔名稱。名稱是您為工作站選擇儲存設定檔的方式。例如，Windows-Workstation 或 Windows-OnPremFleet 等名稱可讓您在稍後輕鬆識別。
7. 為每個掛載在工作站和機群工作者主機上的共用檔案系統建立共用類型的檔案系統位置。
 1. 輸入可識別掛載的名稱，例如包含專案資料的共用檔案系統的專案，或具有要使用工具的共用檔案系統的工具。
 2. 在儲存設定檔的作業系統上，輸入所選共用檔案系統的掛載位置。
8. 為每個僅限工作站的共用檔案系統建立 Local 類型的檔案系統位置。例如，當您的機群已開啟，AWS 而且您希望任務附件處理資料傳輸時。您也可以為每個工作站本機目錄建立此類檔案系統位置，以便在不同的作業系統上指定同等路徑，即使它們不是掛載儲存。
 1. 輸入可識別掛載的名稱，例如包含專案資料的共用檔案系統的專案，或具有要使用工具的共用檔案系統的工具。
 2. 在儲存設定檔的作業系統上輸入選擇的檔案系統位置。
9. （選用）若要新增另一個檔案系統位置，請選擇新增所需的檔案系統位置，然後輸入所需的資料。
10. 新增所有必要的檔案系統位置之後，請選擇建立。

設定您的儲存設定檔以供使用

1. 導覽至您要使用此儲存設定檔的佇列，然後選取允許儲存設定檔索引標籤。
2. 選擇設定儲存設定檔。
3. 從下拉式清單中建立儲存設定檔的關聯，選取您建立的儲存設定檔。
4. 在必要檔案系統位置清單中，選取您要確保可在關聯機群的任何儲存設定檔上使用的檔案系統位置名稱。
5. (選用) 如果您為機群建立儲存設定檔，請導覽至機群，然後選取組態索引標籤。
 - a. 從儲存設定檔區段中，選擇設定儲存設定檔。
 - b. 選取儲存設定檔，然後選擇儲存變更。

在工作站上設定儲存設定檔

在將任務提交至佇列的每個工作站上，使用設定對話方塊來選取其預設儲存設定檔。

1. 若要開啟截止日期雲端設定對話方塊，請完成下列步驟之一：
 - a. 選取截止日期雲端提交者中的設定按鈕。或
 - b. 執行 `deadline config gui CLI` 命令。
2. 設定預設陣列和佇列之後，請從下拉式清單中選取預設儲存設定檔。

共用檔案系統的儲存設定檔

您可以透過在[服務受管機群上使用 VPC 資源端點](#)，或在 AWS 或內部部署上設定客戶受管機群的主機，將截止日期雲端機群設定為掛載共用檔案系統。當工作站與機群掛載相同的共用檔案系統時，您可以在儲存設定檔中建立共用類型的檔案系統位置，以設定每個共用檔案系統顯示為本機路徑的位置。

例如，假設您有一個用於專案的共用檔案系統，另一個用於工具。您的工作站和機群包含三個作業系統 Windows、macOS 和 Linux。您可以使用下列值為每個作業系統建立一個儲存設定檔：

- 儲存設定檔名稱：Linux-Host，作業系統系列：Linux。
 - 檔案系統位置名稱：專案、路徑：/mnt/專案、類型：共用。
 - 檔案系統位置名稱：工具、路徑：/mnt/projects、類型：共用。
- 儲存設定檔名稱：Windows-Host，作業系統系列：Windows。

- 檔案系統位置名稱：專案、路徑：X:\projects、類型：共用。
- 檔案系統位置名稱：工具、路徑：Z:、類型：共用。
- 儲存設定檔名稱：MacOS-Host，作業系統系列：MacOS。
 - 檔案系統位置名稱：專案、路徑：/磁碟區/專案、類型：共用。
 - 檔案系統位置名稱：工具、路徑：/Volumes/Tools、類型：共用。

當您從 提交Windows使用路徑 X:\Projects\ProjectA\Textures\texture.jpg 的任務時，Deadline Cloud 會將包含 Windows-Host 儲存描述檔 ID 的欄位新增至任務。

如果任務在Linux機群工作者主機上執行，截止日期雲端會根據對應的檔案系統位置名稱，為任務建立兩個路徑映射規則：X:\Projects -> /mnt/projects、Z: -> /mnt/tools。任務將套用這些規則，以解析Linux主機查看它們的原始路徑。

如果也為您的佇列設定任務連接，則任何不在共用類型檔案系統位置下的路徑都會連接到任務，並上傳到任務連接 S3 儲存貯體。這可讓您將資料檔案連接到任務，而不是要求一律將其複製到共用檔案系統。例如，提供您提交的任務套件所定義的輔助檔案。

任務附件的儲存設定檔

您可以設定截止日期雲端佇列，以使用任務附件將任務參考的資產資料來回傳輸 AWS。當工作站掛載相同的共用檔案系統，但您的機群未掛載時，您可以在儲存設定檔中建立本機類型的檔案系統位置。此組態可讓您設定從何處上傳和下載檔案，以及如何在作業系統之間對應路徑。

例如，假設您有一個用於專案的共用檔案系統，另一個用於工具。您的工作站和機群包含三個作業系統 Windows、macOS和 Linux。一切都與共用檔案系統主題的儲存設定檔相同，但檔案系統不會與陣列共用。它們適用於包含工作站的本機區域網路。您可以使用下列值為每個作業系統建立一個儲存設定檔：

- 儲存設定檔名稱：Linux-Host，作業系統系列：Linux。
 - 檔案系統位置名稱：專案、路徑：/mnt/專案、類型：本機。
 - 檔案系統位置名稱：工具、路徑：/mnt/projects、類型：本機。
- 儲存設定檔名稱：Windows-Host，作業系統系列：Windows。
 - 檔案系統位置名稱：專案、路徑：X:\projects、類型：本機。
 - 檔案系統位置名稱：工具、路徑：Z:、類型：本機。
- 儲存設定檔名稱：MacOS-Host，作業系統系列：MacOS。
 - 檔案系統位置名稱：專案、路徑：/磁碟區/專案、類型：本機。

- 檔案系統位置名稱：工具、路徑：/Volumes/Tools、類型：本機。

當您從 Windows 提交使用路徑 X:\Projects\ProjectA\Textures\texture.jpg 的任務時，Deadline Cloud 會將包含 Windows-Host 儲存設定檔 ID 的欄位新增至任務，如果尚未上傳，則將檔案上傳至任務附件 S3 儲存貯體。

如果任務在 Linux 機群工作者主機上執行，Deadline Cloud 會在本機暫時目錄中提供紋理檔案，然後從包含紋理的其中一個目錄建立路徑映射規則到暫時目錄。例如，X:\Projects\ProjectA -> /sessions/session-123/projects，以便 X:\Projects\ProjectA\Textures\texture.jpg 映射到 /sessions/session-123/projects/Textures/texture.jpg。當任務完成時，它會從任務指定的目錄收集輸出。假設 /sessions/session-123/projects/Output/frame0032.png 是輸出檔案。此輸出在任務上記錄為 X:\Projects\ProjectA\Output\frame0032.jpg，符合提交任務之工作站的儲存設定檔。

當您在 macOS 工作站下載任務輸出時，截止日期雲端會從 Windows 工作站建立路徑映射規則：X:\Projects -> /Volumes/Projects、Z:-> /Volumes/Tools。它會將規則套用至所有輸出路徑，將範例輸出檔案下載至 /Volumes/Projects/ProjectA/Output/frame0032.jpg。

如果任務的輸出檔案路徑不包含在任何儲存設定檔檔案系統位置下，當儲存設定檔與提交工作站不同時，Deadline Cloud 將無法判斷其下載路徑。根據您用於下載的命令，該檔案會被略過，或者您必須手動選取下載目錄。

截止日期雲端中的任務附件

使用任務附件，您可以在工作站和 AWS 截止日期雲端之間來回傳輸檔案。使用任務附件，您不需要手動設定檔案的 Amazon S3 儲存貯體。相反地，當您使用截止日期雲端主控台建立佇列時，您可以選擇任務附件的儲存貯體。

您第一次將任務提交至截止日期雲端時，任務的所有檔案都會傳輸到截止日期雲端。對於後續提交，只會傳輸已變更的檔案，同時節省時間和頻寬。

處理完成後，您可以從任務詳細資訊頁面或使用截止日期雲端 CLI `deadline job download-output` 命令下載結果。

您可以針對多個佇列使用相同的 S3 儲存貯體。為每個佇列設定不同的根字首，以組織儲存貯體中的附件。

當您使用主控台建立佇列時，您可以選擇現有的 AWS Identity and Access Management (IAM) 角色，也可以讓主控台建立新的角色。如果主控台建立角色，則會設定存取為佇列指定之儲存貯體的許可。如果您選擇現有的角色，您必須授予該角色存取 S3 儲存貯體的許可。

任務連接 S3 儲存貯體的加密

根據預設，任務連接檔案會在 S3 儲存貯體中加密。此加密有助於保護您的資訊免於未經授權的存取。您不需要採取任何動作，即可使用 Deadline Cloud 提供的金鑰加密檔案。如需詳細資訊，請參閱 [《Amazon S3 使用者指南》](#) 中的 [Amazon S3 現在會自動加密所有新物件](#)。Amazon S3

您可以使用自己的客戶受管 AWS Key Management Service 金鑰來加密包含任務附件的 S3 儲存貯體。若要這樣做，您必須修改與儲存貯體相關聯的佇列的 IAM 角色，以允許存取 AWS KMS key。

開啟佇列角色的 IAM 政策編輯器

1. 登入 AWS 管理主控台 並開啟截止日期雲端[主控台](#)。在主頁面的入門區段中，選擇檢視陣列。
2. 從陣列清單中，選擇包含要修改之佇列的陣列。
3. 從佇列清單中，選擇要修改的佇列。
4. 在佇列詳細資訊區段中，選擇服務角色以開啟服務角色的 IAM 主控台。

接著，完成下列程序。

使用的許可更新角色政策 AWS KMS

1. 從許可政策清單中，選擇角色的政策。
2. 在此政策定義的許可區段中，選擇編輯。
3. 選擇新增新陳述式。
4. 將下列政策複製並貼到編輯器中。將 *Region*、*accountID* 和 *keyID* 變更為您自己的值。

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:us-east-1:111122223333:key/keyID"
  ]
}
```

5. 選擇下一步。
6. 檢閱政策的變更，然後在滿意時選擇儲存變更。

取代任務附件儲存貯體

您可以將目前的任務附件儲存貯體取代為不同的任務附件儲存貯體。您可以在佇列詳細資訊的任務附件索引標籤下找到按鈕。您可以使用它來變更任務附件儲存貯體，或取代相同儲存貯體中的根資料夾，以上傳任務附件。

存取任務附件設定

1. 前往佇列詳細資訊，然後找到任務附件索引標籤。
2. 從任務附件索引標籤中，有 2 個選項：
 - a. 執行下列動作來變更任務附件儲存貯體：
 - i. 選取新的 S3 儲存貯體。
 - ii. 更新佇列的服務角色政策，以授予新儲存貯體的存取權。
 - 或
 - b. 執行下列動作，變更現有儲存貯體中的根資料夾：
 - i. 修改根資料夾名稱。
 - ii. 更新佇列服務角色中的資源 ARN。

更新服務角色

1. 導覽至您的陣列 > 佇列 > 佇列服務角色。
2. 選擇在 JSON 中編輯。
3. 尋找資源 ARN (預設根資料夾為 DeadlineCloud)：

```
"arn:aws:s3:::<your-job-attachments-bucket-name>/DeadlineCloud/*"  
]
```

4. 使用新的儲存貯體或資料夾更新 ARN：

```
"arn:aws:s3:::<your-job-attachments-NEW-bucket-name>/NEW-ROOT-FOLDER-NAME/*"  
]
```

5. 在進行這些變更後驗證許可，以確保適當的存取。

管理 S3 儲存貯體中的任務附件

Deadline Cloud 會將任務所需的任務附件檔案存放在 S3 儲存貯體中。這些檔案會隨著時間累積，導致 Amazon S3 成本增加。若要降低成本，您可以將 S3 生命週期組態套用至 S3 儲存貯體。此組態可以自動刪除儲存貯體中的檔案。由於 S3 儲存貯體位於您的帳戶中，因此您可以隨時選擇修改或移除 S3 生命週期組態。如需詳細資訊，請參閱《Amazon [S3 使用者指南](#)》中的 [S3 生命週期組態範例](#)。

Amazon S3

如需更精細的 S3 儲存貯體管理解決方案，您可以根據上次存取的物件 AWS 帳戶，將設定為使 S3 儲存貯體中的物件過期。如需詳細資訊，請參閱[架構部落格上的根據上次存取日期過期 Amazon S3 物件，以降低成本](#)。AWS

截止日期 雲端虛擬檔案系統

虛擬檔案系統支援 AWS Deadline Cloud 中的任務附件，可讓工作者上的用戶端軟體直接與 Amazon Simple Storage Service 通訊。工作者只能在需要時才載入檔案，而不是在處理之前下載所有檔案。檔案會儲存在本機。此方法可避免下載多次使用的資產。任務完成後，會移除所有檔案。

- 虛擬檔案系統為特定任務描述檔提供顯著的效能提升。一般而言，具有較大工作者機群之總檔案的較小子集會顯示最大效益。工作者較少的少量檔案具有大約相等的處理時間。
- 虛擬檔案系統支援僅適用於服務受管機群中的Linux工作者。
- Deadline Cloud 虛擬檔案系統支援下列操作，但不符合 POSIX：
 - 檔案
create、delete、open、close、read、write、append、truncaterename、move、copy、stat fsync和 falloc
 - 目錄 create、delete、rename、move、copy和 stat
- 當您的任務僅存取大型資料集的一部分時，虛擬檔案系統旨在減少資料傳輸並改善效能，而且並非所有工作負載都經過最佳化。您應該在執行生產任務之前測試工作負載。

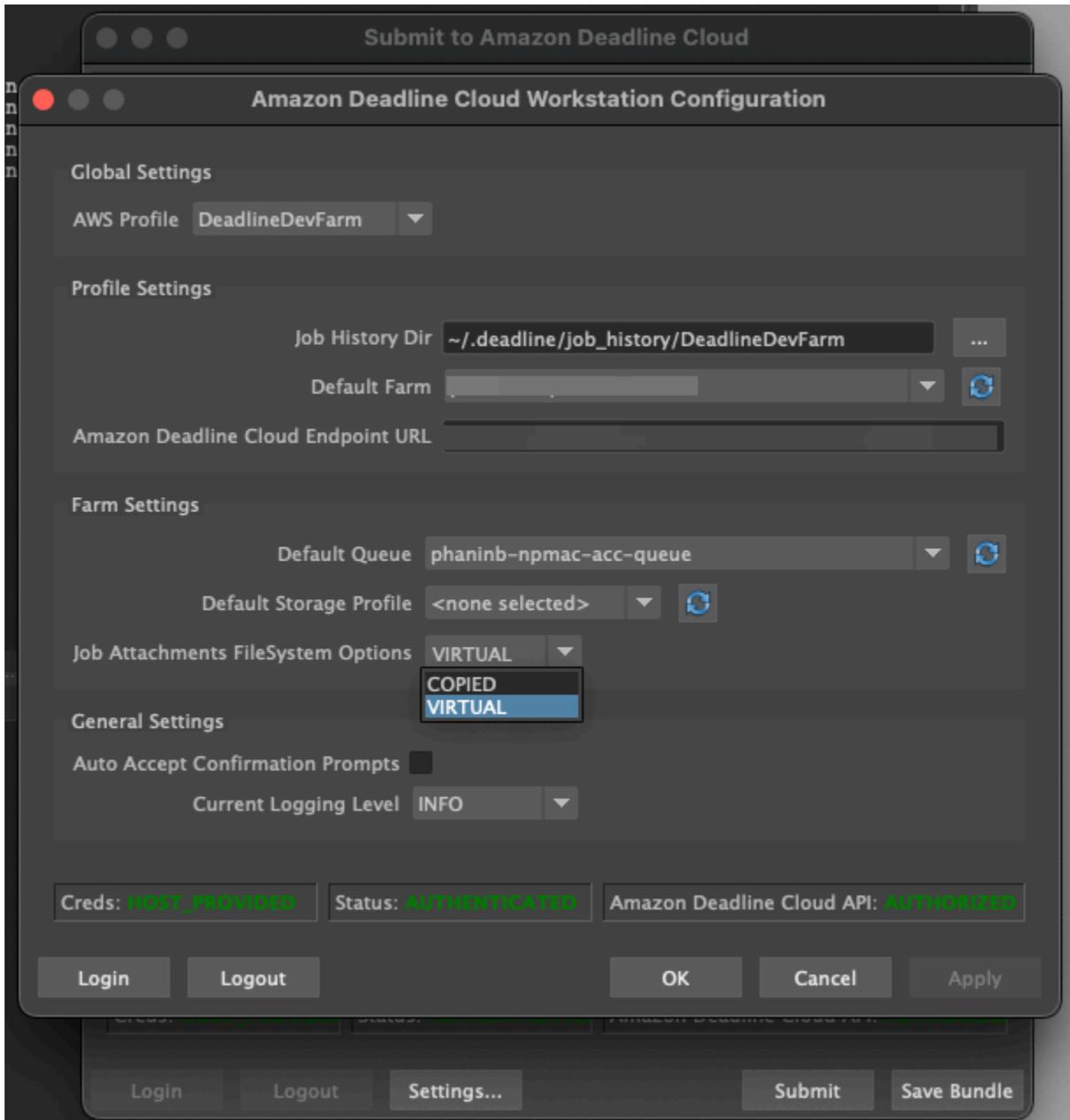
啟用 VFS 支援

為每個任務啟用虛擬檔案系統支援 (VFS)。在這些情況下，任務會回復為預設任務附件架構：

- 工作者執行個體描述檔不支援虛擬檔案系統。
- 無法啟動虛擬檔案系統程序的問題。
- 虛擬檔案系統無法掛載。

使用提交者啟用虛擬檔案系統支援

1. 提交任務時，請選擇設定按鈕以開啟AWS 截止日期雲端工作站組態面板。
2. 從任務連接檔案系統選項下拉式清單中，選擇 VIRTUAL。



3. 若要儲存變更，請選擇確定。

使用 啟用虛擬檔案系統支援 AWS CLI

- 當您提交儲存的任務時，請使用下列命令：

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

若要確認已針對特定任務成功啟動虛擬檔案系統，請在 Amazon CloudWatch Logs 中檢閱您的日誌。尋找下列訊息：

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

如果日誌包含下列訊息，則會停用虛擬檔案系統支援：

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

對虛擬檔案系統支援進行故障診斷

您可以使用截止日期雲端監視器檢視虛擬檔案系統の日誌。如需說明，請參閱[在截止日期雲端中檢視工作階段和工作者日誌](#)。

虛擬檔案系統日誌也會傳送至與與工作者代理程式輸出共用的佇列相關聯的 CloudWatch Logs 群組。

自動下載

截止日期 CLI 提供命令，以下載自上次執行相同命令後佇列中所有任務的輸出。您可以將此設定為 Cron 任務或排程任務，以重複執行。此組態會設定持續自動下載輸出。

在設定自動下載之前，請遵循[任務附件的儲存設定檔](#)中的步驟，設定資產資料的所有路徑以進行上傳和下載。如果任務使用不在其儲存設定檔中的輸出路徑，則自動下載會略過下載該輸出並列印警告訊息，以摘要其未下載的檔案。同樣地，如果提交的任務沒有儲存描述檔，則自動下載會略過該任務並列印警告訊息。根據預設，截止日期雲端提交者會顯示儲存設定檔以外路徑的警告訊息，以協助確保正確的組態。

設定 AWS 登入資料

自動下載使用截止日期 CLI 來持續下載任務輸出。若要驗證這些下載，您需要長期 IAM 登入資料。截止日期的雲端監視器登入資料會過期，因此您無法將其用於此目的。

請依照下列步驟設定長期登入資料。

⚠ Important

請注意下列警告：

- 請勿使用您帳戶的根登入資料來存取 AWS 資源。這些登入資料可讓未管制的帳戶存取和很難撤銷這些帳戶。
- 請勿在應用程式檔案中放置常值存取金鑰或憑證資訊。如果您不小心這麼做了，則會有暴露您登入資料的風險，例如，當您上傳專案到公有儲存庫時。
- 請勿在您的專案區域中放入包含憑證的檔案。
- 保護您的存取金鑰。請勿將您的存取金鑰提供給未經授權的當事方，即便是協助[尋找您的帳戶識別符](#)也不妥。如果這麼做，就可能讓他人能夠永久存取您的帳戶。
- 請注意，存放在共用 AWS 登入資料檔案中的任何登入資料都會以純文字形式儲存。

如需詳細資訊，請參閱《[AWS 一般參考](#)》中的[管理 AWS 存取金鑰的最佳實務](#)。

建立 IAM 使用者

1. 前往 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在導覽窗格中選取使用者，然後選取建立使用者。
3. 將使用者命名為 **deadline-output-downloader**。清除提供使用者存取權 AWS 管理主控台的核取方塊，然後選擇下一步。
4. 選擇直接連接政策。
5. 選擇建立政策以建立具有最低必要許可的自訂政策。
6. 在 JSON 編輯器中，指定下列許可：

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineCloudOutputDownload",
            "Effect": "Allow",
            "Action": [
                "deadline:AssumeQueueRoleForUser",
```

```

        "deadline:ListQueueEnvironments",
        "deadline:ListSessions",
        "deadline:ListSessionActions",
        "deadline:SearchJobs",
        "deadline:GetJob",
        "deadline:GetQueue",
        "deadline:GetStorageProfileForQueue"
    ],
    "Resource": "*"
}
]
}

```

7. 命名政策**DeadlineCloudOutputDownloadPolicy**，然後選擇建立政策。
8. 返回使用者建立頁面，重新整理政策清單，然後選取您剛建立的 **DeadlineCloudOutputDownloadPolicy**，然後選擇下一步。
9. 檢閱使用者詳細資訊，然後選擇建立使用者。

建立存取金鑰

1. 從使用者詳細資訊頁面，選取安全登入資料索引標籤。在存取金鑰區段中，選擇建立存取金鑰。
2. 表示您想要使用其他的金鑰，然後選擇下一步，然後選擇建立存取金鑰。
3. 在擷取存取金鑰頁面上，選擇顯示以顯示使用者私密存取金鑰的值。您可以複製憑證或下載 .csv 檔案。

存放使用者存取金鑰

- 將使用者存取金鑰存放在系統中的 AWS 登入資料檔案中：
 - 在上Linux，檔案位於 `~/.aws/credentials`
 - 在上Windows，檔案位於 `%USERPROFILE\.aws\credentials`

取代下列金鑰：

```

[deadline-downloader]
aws_access_key_id=ACCESS_KEY_ID
aws_secret_access_key=SECRET_ACCESS_KEY
region=YOUR_AWS_REGION

```

⚠ Important

當您不再需要此 IAM 使用者時，建議您將其移除，以符合 [AWS 安全最佳實務](#)。我們建議您要求人類使用者在存取 [AWS IAM Identity Center](#) 時透過 使用暫時登入資料 AWS。

先決條件

在建立 cron 任務或排程任務以進行自動下載之前，請完成下列步驟。

1. 如果您尚未安裝 [Python](#)，請安裝 Python。
2. 執行下列動作來安裝截止日期 CLI：

```
python -m pip install deadline
```

3. 使用以下命令確認截止日期 CLI 的版本為 0.52.1 或更新版本。

```
$ deadline --version  
deadline, version 0.52.1
```

測試輸出下載命令

驗證命令是否可在您的環境中運作

1. 取得截止日期的路徑

Linux and macOS

```
$ which deadline
```

Windows

```
C:\> where deadline
```

PowerShell

```
PS C:\> Get-Command deadline
```

2. 執行 sync-output 命令以引導。

```
/path/to/deadline queue sync-output \  
--profile deadline-downloader \  
--farm-id YOUR_FARM_ID \  
--queue-id YOUR_QUEUE_ID \  
--storage-profile-id YOUR_PROFILE_ID \  
--checkpoint-dir /path/to/checkpoint/directory \  

```

3. 只有在您的下載機器與提交機器相同時，才需要執行此步驟。將`--storage-profile-id YOUR_PROFILE_ID` \ 上述 取代為 `--ignore-storage-profiles`。

4. 提交測試任務。

a. 從 GitHub 下載 .zip 檔案。

- i. 開啟 [deadline-cloud-samples GitHub 儲存庫](#)。
- ii. 選擇程式碼，然後從下拉式功能表中選取下載 ZIP。
- iii. 將下載的封存解壓縮至本機目錄。

b. 執行

```
cd /path/to/unzipped/deadline-cloud-samples-mainline/job_bundles/  
job_attachments_devguide_output
```

c. 執行

```
deadline bundle submit .
```

- 如果您沒有預設的截止日期組態設定，您可能需要在命令列中提供下列項目。

```
--farm-id YOUR-FARM-ID --queue-id YOUR-QUEUE-ID
```

d. 等待任務完成，再前往下一個步驟。

5. 再次執行 `sync-output` 命令。

```
/path/to/deadline queue sync-output \  
--profile deadline-downloader \  
--farm-id YOUR_FARM_ID \  
--queue-id YOUR_QUEUE_ID \  
--storage-profile-id YOUR_PROFILE_ID \  
--checkpoint-dir /path/to/checkpoint/directory
```

6. 請確認下列內容：

- 您的測試任務輸出會出現在目的地目錄中。
- 檢查點檔案會在您指定的檢查點目錄中建立。

設定排定的下載

選取作業系統的索引標籤，了解如何設定每 5 分鐘自動下載一次。

Linux

1. 驗證截止日期 CLI 安裝

取得截止日期可執行檔的確切路徑：

```
$ which deadline
```

請注意此路徑（例如 `/opt/homebrew/bin/deadline`）可用於 plist 檔案。

2. 建立檢查點目錄

建立存放檢查點檔案的目錄。確保您的使用者執行 `命令` 的適當許可。

```
$ mkdir -p /path/to/checkpoint/directory
```

3. 建立日誌目錄

建立 cron 任務日誌的目錄：

```
$ mkdir -p /path/to/logs
```

考慮使用 <https://www.redhat.com/en/blog/setting-logrotate> 在日誌檔案上設定日誌輪換

4. 檢查目前的 Crontab

檢視您目前的 crontab 以查看現有的任務：

```
$ crontab -l
```

5. 編輯 Crontab

開啟您的 crontab 檔案以進行編輯：

```
$ crontab -e
```

如果這是您第一次使用，系統可能會提示您選擇編輯器 (nano、vim 等)。

6. 新增 Cron 任務項目

每 5 分鐘新增以下行來執行任務 (將路徑取代為步驟 1 和 2 的實際值)：

```
*/5 * * * * /path/to/deadline queue sync-output --profile deadline-downloader  
--farm-id YOUR_FARM_ID --queue-id YOUR_QUEUE_ID --storage-profile-id  
YOUR_PROFILE_ID --checkpoint-dir /path/to/checkpoint/directory >> /path/to/  
logs/deadline_sync.log 2>&1
```

7. 驗證 Cron 任務安裝

儲存並結束編輯器之後，請確認已新增 Cron 任務：

```
$ crontab -l
```

您應該會看到您的新任務已列出。

8. 檢查 Cron Service 狀態

確保 cron 服務正在執行：

```
# For systemd systems (most modern Linux distributions)  
$ sudo systemctl status cron  
# or  
$ sudo systemctl status crond  
  
# For older systems  
$ sudo service cron status
```

如果未執行，請啟動它：

```
$ sudo systemctl start cron  
$ sudo systemctl enable cron # Enable auto-start on boot
```

macOS

1. 驗證截止日期 CLI 安裝

取得截止日期可執行檔的確切路徑：

```
$ which deadline
```

請注意此路徑（例如 `/opt/homebrew/bin/deadline`）可用於 plist 檔案。

2. 建立檢查點目錄和日誌目錄

建立存放檢查點檔案的目錄：

```
$ mkdir -p /path/to/checkpoint/directory  
$ mkdir -p /path/to/logs
```

考慮使用 <https://formulae.brew.sh/formula/logrotate> 在日誌檔案上設定日誌輪換

3. 建立 Plist 檔案

使用 `~/Library/LaunchAgents/com.user.deadlinesync.plist` 下列內容在 建立組態檔案 (`/path/to/deadline` 以步驟 1 的實際路徑取代)：

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/  
PropertyList-1.0.dtd">  
<plist version="1.0">  
<dict>  
  <key>Label</key>  
  <string>com.user.deadlinesync</string>  
  <key>ProgramArguments</key>  
  <array>  
    <string>/path/to/deadline</string>  
    <string>queue</string>  
    <string>sync-output</string>  
    <string>--profile</string>  
    <string>deadline-downloader</string>  
    <string>--farm-id</string>  
    <string>YOUR_FARM_ID</string>  
    <string>--queue-id</string>  
    <string>YOUR_QUEUE_ID</string>  
    <string>--storage-profile-id</string>
```

```
<string>YOUR STORAGE PROFILE ID</string>
<string>--checkpoint-dir</string>
<string>/path/to/checkpoint/dir</string>
</array>
<key>RunAtLoad</key>
<true/>
<key>UserName</key>
<string>YOUR_USER_NAME</string>
<key>StandardOutPath</key>
<string>/path/to/logs/deadline_sync.log</string>
<key>StartInterval</key>
<integer>300</integer>
</dict>
</plist>
```

`--ignore-storage-profiles` 如果您的下載機器與提交機器相同，請將 `--storage-profile-id` *YOUR_PROFILE_ID* 上述 取代為。

4. 驗證清單檔案

驗證 plist 檔案的 XML 語法：

```
$ plutil -lint ~/Library/LaunchAgents/com.user.deadlinesync.plist
```

如果檔案有效，這應該會傳回 "OK"。

5. 檢查現有的啟動代理程式或啟動協助程式

檢查啟動代理程式是否已載入：

```
$ launchctl list | grep deadlinesync
OR
$ sudo launchctl list | grep deadlinesync
```

如果存在，請先卸載：

```
$ launchctl bootout gui/$(id -u)/com.user.deadlinesync
OR
$ sudo launchctl bootout system/com.user.deadlinesync
```

6. 建立和引導

若要在使用者登入時執行此任務，請以 LaunchAgent 身分執行。若要執行此任務，而不讓使用者在每次執行機器時登入，請以 LaunchDaemon 執行它。

- a. 若要以 LaunchAgent 身分執行：
 - i. 使用在下建立的組態 `~/Library/LaunchAgents/com.user.deadlinesync.plist`
 - ii. 然後使用引導命令載入組態：

```
$ launchctl bootstrap gui/$(id -u) ~/Library/LaunchAgents/  
com.user.deadlinesync.plist
```

- b. 若要以 LaunchDaemon 執行：
 - i. 執行下列動作以移動 Plist 檔案並變更許可：

```
$ sudo mv ~/Library/LaunchAgents/com.user.deadlinesync.plist /Library/  
LaunchDaemons/  
$ sudo chown root:wheel /Library/LaunchDaemons/  
com.user.deadlinesync.plist  
$ sudo chmod 644 /Library/LaunchDaemons/com.user.deadlinesync.plist
```

- ii. 使用現代引導命令載入啟動代理程式：

```
$ sudo launchctl bootstrap system /Library/LaunchDaemons/  
com.user.deadlinesync.plist
```

7. 驗證狀態

如果您啟動 LaunchAgent，請執行下列動作以確認已載入：

```
$ launchctl list | grep deadlinesync
```

如果您啟動 LaunchDaemon，請執行下列動作來確認已載入：

```
$ sudo launchctl list | grep deadlinesync
```

輸出看起來應該像

```
SOME_PID_NUMBER 0 com.user.deadlinesync
```

如需詳細狀態資訊：

```
$ launchctl print gui/$(id -u)/com.user.deadlinesync
```

這會顯示目前狀態、程式引數、環境變數、執行間隔和執行歷史記錄。

Windows

Note

使用這些指示建立的排程任務只有在使用者登入時才有效。

若要在系統啟動時設定它，而不需要使用者登入，請參閱官方[Windows文件](#)。

對於以下所有步驟，請使用命令提示 - 以管理員身分執行：

1. 驗證截止日期 CLI 安裝

尋找截止日期可執行檔：

```
C:\> where deadline
```

記下用於任務的完整路徑（例如 C:\Program Files\Amazon\DeadlineCloud\deadline.exe）。

2. 建立檢查點目錄

建立存放檢查點檔案的目錄：

```
C:\> mkdir "path\to\checkpoint\directory"
```

3. 建立日誌目錄

建立任務日誌的目錄：

```
C:\> mkdir "path\to\logs"
```

4. 建立批次檔案包裝函式

使用下列內容建立批次檔案：

```
C:\> notepad C:\path\to\deadline_sync.bat
```

```
YOUR_PATH_TO_DEADLINE.EXE queue sync-output --profile deadline-downloader  
--farm-id YOUR_FARM_ID --queue-id YOUR_QUEUE_ID --storage-profile-  
id YOUR_PROFILE_ID --checkpoint-dir path\to\checkpoint\checkpoints > path\to  
\logs\deadline.log 2>&1
```

5. 測試批次檔案

手動測試批次檔案：

```
C:\> .\path\to\deadline_sync.bat
```

檢查日誌檔案是否已建立：

```
C:\> notepad path\to\logs\deadline_sync.log
```

6. 檢查任務排程器服務

確保任務排程器服務正在執行：

```
C:\> sc query "Schedule"
```

如果服務不存在，請嘗試其他名稱：

```
C:\> sc query "TaskScheduler"  
C:\> sc query "Task Scheduler"
```

如果未執行，請啟動它：

```
C:\> sc start "Schedule"
```

7. 建立排程任務

建立任務以每 5 分鐘執行一次。

```
C:\> schtasks /create /tn "DeadlineOutputSync" /tr "C:\path\to\n\deadline_sync.bat" /sc minute /mo 5
```

命令明細：

- /tn - 任務名稱
- /tr - 要執行的任務（您的批次檔案）
- /sc minute /mo 5 - 排程：每 5 分鐘

8. 驗證任務建立

檢查任務是否已成功建立：

```
schtasks /query /tn "DeadlineOutputSync" /v /fo LIST
```

尋找：

- 要執行的任務：應該顯示您的批次檔案路徑
- 下次執行時間：應該會在 5 分鐘內顯示時間

9. 測試任務執行

手動執行任務以測試：

```
schtasks /run /tn "DeadlineOutputSync"
```

檢查任務狀態：

```
schtasks /query /tn "DeadlineOutputSync"
```

驗證設定

若要驗證自動下載設定是否成功，請完成下列步驟。

1. 提交新的測試任務。
2. 等待一個排程器間隔完成，在此情況下為 5 分鐘。
3. 確認已自動下載新的輸出。

如果輸出未下載，請檢查程序日誌的故障診斷區段。

對自動下載進行故障診斷

如果您遇到自動下載的問題，請檢查下列項目：

儲存設定檔問題

- 日誌檔案中類似 [Errno 2] No such file or directory 或 [Errno 13] Permission denied 的錯誤可能與遺失或設定錯誤的儲存設定檔有關。
- 如需下載機器與提交機器不同時如何設定儲存設定檔 <https://docs.aws.amazon.com/deadline-cloud/latest/userguide/storage-profile-job-attachments.html> 的相關資訊，請參閱儲存設定檔。
- 對於相同的機器下載，請嘗試 `--ignore-storage-profiles` 旗標。

目錄許可

- 確保排程器服務使用者具有：
 - 對檢查點目錄的讀取/寫入存取權
 - 輸出目的地目錄的寫入存取權
- 對於 Linux 和 macOS，使用 `ls -la` 檢查許可。
- 對於 Windows，請檢閱 屬性資料夾中的安全性設定。

檢查排程器日誌

Linux

1. 檢查 cron 服務是否正在執行：

```
# For systemd systems
$ sudo systemctl status cron
# or
$ sudo systemctl status crond

# Check if your user has cron job correctly configured
$ crontab -l
```

2. 檢視 Cron 執行日誌：

```
# Check system logs for cron activity (most common locations)
$ sudo tail -f /var/log/syslog | grep CRON
$ sudo tail -f /var/log/cron.log | grep deadline

# View recent cron logs
$ sudo journalctl -u cron -f
$ sudo journalctl -u crond -f # On some systems
```

3. 檢查您的特定 Cron 任務日誌：

```
# View the log file specified in your cron job
$ tail -100f /path/to/logs/deadline_sync.log
```

4. 在系統日誌中搜尋 Cron 任務執行：

```
# Look for your specific cron job executions
$ sudo grep "deadline.*incremental-output-download" /var/log/syslog

# Check for cron job starts and completions
$ sudo grep "$(whoami).*CMD.*deadline" /var/log/syslog
```

5. 檢查檢查點檔案更新：

```
# List checkpoint files with timestamps
$ ls -la /path/to/checkpoint/directory/

# Check when checkpoint was last modified
$ stat /path/to/checkpoint/directory/queue-*_download_checkpoint.json
```

6. 檢查日誌檔案：

```
$ ls -la /path/to/log/deadline_sync.log
```

macOS

檢視啟動代理程式執行日誌：

1. 檢查啟動代理程式是否正在執行：

```
$ sudo launchctl list | grep deadlinesync
```

輸出顯示：PID Status Label(PID 將在目前未執行-時，這是間隔任務的正常情況)

2. 檢視詳細的啟動代理程式狀態：

```
$ sudo launchctl print system/com.user.deadlinesync
```

這會顯示執行歷史記錄、上次結束程式碼、執行次數和目前狀態。

3. 檢視啟動代理程式執行日誌：

```
# View recent logs (last hour)
log show --predicate 'subsystem contains "com.user.deadlinesync"' --last 1h

# View logs from a specific time period
log show --predicate 'subsystem contains "com.user.deadlinesync"' --start
'2024-08-27 09:00:00'
```

4. 強制執行啟動代理程式以進行立即測試：

```
$ sudo launchctl kickstart gui/${id -u}/com.user.deadlinesync
```

無論排程為何，這都會立即觸發任務，這對於測試很有用。

5. 檢查檢查點檔案更新：

```
# List checkpoint files with timestamps
$ ls -la /path/to/checkpoint/directory/
```

6. 檢查日誌檔案：

```
$ ls -la /path/to/log/deadline_sync.log
```

Windows

1. 檢查任務排程器服務是否正在執行：

```
C:\> sc query "Schedule"
```

如果服務不存在，請嘗試其他名稱：

```
C:\> sc query "TaskScheduler"
C:\> sc query "Task Scheduler"
```

2. 檢視您的排程任務：

```
C:> schtasks /query /tn "DeadlineOutputSync"
```

3. 檢查任務的日誌檔案：

```
# View the log file created by your batch script
C:> notepad C:\path\to\logs\deadline_sync.log
```

4. 檢查檢查點檔案更新：

```
# List checkpoint files with timestamps
```

```
C:> dir "C:\path\to\checkpoint\directory" /od
```

追蹤截止日期雲端陣列的支出和用量

AWS Deadline Cloud 預算管理器和用量總管是成本管理工具，可根據成本變數的可用資訊提供使用 Deadline Cloud 的近似成本。成本管理工具不保證您實際使用截止日期雲端和其他 AWS 服務所欠的金額。

為了協助您管理截止日期雲端的成本，您可以使用下列功能：

- 預算經理 – 透過截止日期雲端預算經理，您可以建立和編輯預算，以協助管理專案成本。
- 用量總管 – 透過截止日期雲端用量總管，您可以檢視使用多少 AWS 資源以及這些資源的預估成本。
- AWS 成本分配標籤 – 透過成本分配標籤，您可以追蹤所有 AWS 服務的詳細成本。如需詳細資訊，請參閱[使用成本分配標籤組織和追蹤 AWS 成本](#)。

成本假設

截止日期雲端成本管理工具使用的基本計算為：

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

- 執行時間是任務中所有任務的總和，從開始時間到結束時間。
- 運算速率取決於服務受管機群的[AWS 截止日期雲端定價](#)。對於客戶管理的機群，運算速率估計為每個工作者小時 1 美元。
- 授權率取決於截止日期雲端基本授權價格，且僅適用於服務受管機群。不包含其他方案。如需授權定價的詳細資訊，請參閱[AWS 截止日期雲端定價](#)。

截止日期雲端成本管理工具的成本估算可能會與您的實際成本不同，原因有很多。常見原因包括：

- 客戶擁有的資源及其定價。您可以選擇從內部部署或其他雲端提供者或從 AWS 外部使用您自己的資源。這些資源的實際成本不會計算。
- 閒置工作者成本。當工作者狀態為 IDLE 時，不包含閒置工作者成本。對於執行個體計數下限大於零的機群，或當工作者在任務之間轉換時，可能會發生這種情況。閒置工作者成本不包含在計算中。
- 工作者停止和開始時間。工作者完成工作後，從 IDLE 移至 STOPPING 以及從 STOPPING 移至 STOPPED 的成本不會包含在截止日期雲端成本估算中。

- 促銷點數、折扣和自訂定價協議。成本管理工具不會計入促銷點數、私有定價協議或其他折扣。您可能符合其他不屬於預估的折扣資格。
- 資產儲存。資產儲存不包含在成本和用量預估中。
- price.offers 的變更為大多數服務 AWS 提供隨需付費定價。pay-as-you-go 價格可能會隨著時間而變更。成本管理工具使用可公開取得up-to-date價格，但變更後可能會有延遲。
- 稅金。成本管理工具不包含適用於我們購買服務的稅金。
- 四捨五入。成本管理工具會執行數學四捨五入定價資料。
- 貨幣。成本估算是以美元為單位。全球匯率會隨著時間而變化。如果您根據目前的匯率將預估值轉換為不同的貨幣，則匯率的變更會影響預估值。
- 外部授權。如果您選擇使用預先購買的授權 ([服務受管機群的軟體授權](#))，截止日期雲端成本管理工具無法計入此成本。

使用預算控制成本

截止日期雲端預算管理工具可協助您控制特定資源的花費，例如佇列、機群或陣列。您可以建立預算金額和限制，並設定自動化動作，以協助減少或停止預算的額外支出。

下列各節提供使用截止日期雲端預算管理器的步驟。

主題

- [先決條件](#)
- [開啟截止日期雲端預算管理工具](#)
- [建立截止日期雲端佇列的預算](#)
- [檢視截止日期雲端佇列預算](#)
- [編輯截止日期雲端佇列的預算](#)
- [停用截止日期雲端佇列的預算](#)
- [使用 EventBridge 事件監控預算](#)

先決條件

若要使用截止日期雲端預算管理器，您必須擁有OWNER存取層級。若要授予OWNER許可，請遵循中的步驟在[截止日期雲端中管理使用者](#)。

開啟截止日期雲端預算管理工具

若要開啟截止日期雲端預算管理器，請使用下列程序。

1. 登入 AWS 管理主控台 並開啟截止日期雲端[主控台](#)。
2. 選擇檢視陣列。
3. 找到您要取得相關資訊的陣列，然後選擇管理任務。
4. 在截止日期雲端監視器的左側導覽窗格中，選擇預算。

預算管理員摘要頁面會顯示作用中和非作用中預算的清單：

- 作用中預算會根據選取的資源（佇列）進行追蹤。
- 非作用中預算已過期或遭使用者取消，且不再根據此預算的限制追蹤成本。

選擇預算後，預算摘要頁面會包含預算的基本資訊。提供的資訊包括預算名稱、狀態、資源、剩餘百分比、剩餘金額、總預算、開始日期和結束日期。

建立截止日期雲端佇列的預算

若要建立預算，請使用下列程序。

1. 如果您尚未登入，請 AWS 管理主控台開啟截止日期雲端[主控台](#)，選擇陣列，然後選擇管理任務。
2. 在預算管理員頁面中，選擇建立預算。
3. 在詳細資訊區段中，輸入預算的預算名稱。
4. （選用）在描述欄位中，輸入預算的簡短描述。
5. 從資源中，使用佇列下拉式清單選取要為其建立預算的佇列。
6. 針對期間，請完成下列步驟來設定預算的開始和結束日期：
 - a. 對於開始日期，以 YYYY/MM/DD 格式輸入預算追蹤的第一個日期，或選擇行事曆圖示並選取日期。

預設開始日期是建立預算的日期。
 - b. 對於結束日期，以 YYYY/MM/DD 格式輸入預算追蹤的最後一個日期，或選擇行事曆圖示並選取日期。

預設結束日期是從開始日期起算 120 天。

7. 針對預算金額，輸入預算的美元金額。
8. (選用) 建議您建立限制提醒。在限制動作區段中，您可以實作特定金額保留在預算中時發生的自動化動作。若要執行此動作，請執行下列步驟。
 - a. 選擇新增動作。
 - b. 針對剩餘金額，輸入您要啟動動作的美元金額。
 - c. 在動作下拉式清單中，選擇您想要的動作。動作包括：
 - 完成目前的工作後停止 – 當達到閾值時，目前執行的所有工作都會繼續執行（並產生成本），直到完成為止。
 - 立即停止工作 – 達到閾值時，會立即取消所有工作。
 - d. 若要建立其他限制提醒，請選擇新增動作並重複上述步驟。
9. 選擇建立預算。

檢視截止日期雲端佇列預算

建立預算後，您可以在 Budget Manager 頁面上檢視預算。從那裡，您可以檢視預算的總金額和分配給特定預算的整體成本。

若要檢視預算，請使用下列程序。

1. 如果您尚未登入 AWS 管理主控台，請開啟截止日期雲端[主控台](#)，選擇陣列，然後選擇管理任務。
2. 從左側導覽窗格中選擇預算。預算管理員頁面隨即出現。
3. 若要檢視作用中預算，請選擇作用中預算索引標籤，然後選擇您要檢視的預算名稱。預算詳細資訊頁面隨即出現。
4. 若要檢視過期預算的預算詳細資訊，請選擇非作用中預算索引標籤。然後，選擇您要檢視的預算名稱。預算詳細資訊頁面隨即出現。

編輯截止日期雲端佇列的預算

您可以編輯任何作用中的預算。若要編輯作用中預算，請使用下列程序。

1. 如果您尚未登入，請 AWS 管理主控台開啟截止日期雲端[主控台](#)，選擇陣列，然後選擇管理任務。
2. 在預算管理員頁面的作用中預算索引標籤中，選擇您要編輯之預算旁的按鈕。
3. 從動作下拉式功能表中，選取編輯預算。

4. 進行您想要的變更，然後選擇更新預算。

停用截止日期雲端佇列的預算

您可以停用任何作用中的預算。停用預算會將其狀態從作用中變更為非作用中。當預算停用時，它不會再追蹤該預算金額的資源。

若要停用預算，請使用下列程序。

1. 如果您尚未登入，請 AWS 管理主控台開啟截止日期雲端[主控台](#)，選擇陣列，然後選擇管理任務。
2. 在預算管理員頁面的作用中預算索引標籤中，選擇您要停用之預算旁的按鈕。
3. 從動作下拉式功能表中，選取停用預算。稍後，選取的預算將從作用中變更為非作用中，並將從作用中預算索引標籤移至非作用中預算索引標籤。

使用 EventBridge 事件監控預算

Deadline Cloud 會使用 Amazon EventBridge 將預算相關事件傳送至您的預設 EventBridge 事件匯流排。您可以建立自訂函數來接收事件，並對其採取行動來傳送通知，以在預算達到預先定義的層級時透過電子郵件、Slack 或其他管道自動通知使用者。例如，您可以在預算達到特定閾值時傳送簡訊。這些通知可協助您掌握支出，並在預算用盡之前做出明智的決策。

Deadline Cloud 會定期彙總每個轉譯陣列的用量和成本資料。然後，它會檢查是否已超過任何預算閾值。如果超過閾值，截止日期雲端會觸發事件來提醒您，以便您可以採取適當的動作。每當預算超過其中一個閾值時，就會觸發事件，以使用的預算百分比指定：

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

隨著預算接近 100% 用量，預算用量閾值會越來越接近。此頻率可協助您在預算達到其限制時密切監控用量。您也可以設定自己的預算閾值。當用量超過您的自訂閾值時，截止日期 Cloud 會傳送事件。預算達到 100% 之後，截止日期 Cloud 會停止傳送事件。如果您調整預算，截止日期雲端會根據新的預算金額傳送閾值的事件。

您可以使用 EventBridge 主控台 (<https://console.aws.amazon.com/events/> : //) 建立規則，將截止日期雲端事件傳送至事件的適當目標。例如，您可以將事件傳送至 Amazon Simple Queue Service 佇列，然後從該佇列傳送至多個目標，例如 AWS 最終使用者傳訊簡訊或用於記錄的 Amazon Relational Database Service 資料庫。

如需 EventBridge 規則的範例，請參閱下列主題：

- [使用 Amazon EventBridge 在事件發生時傳送電子郵件。](#)
- [建立在聊天應用程式中傳送通知給 Amazon Q Developer 的 Amazon EventBridge 規則。](#)
- [Amazon EventBridge 入門。](#)

如需預算事件的詳細資訊，請參閱《截止日期雲端開發人員指南》中的[預算閾值達到事件](#)。

使用截止日期雲端用量總管追蹤用量和成本

使用截止日期雲端用量總管，您可以查看每個陣列上發生的活動的即時指標。您可以依不同的變數查看陣列的成本，例如佇列、任務、授權產品或執行個體類型。選取各種時間範圍以查看特定時段內的用量，並查看一段時間內的用量趨勢。您也可以查看所選資料點的詳細明細，以便更深入地查看指標。用量可以按時間（分鐘和小時）或成本（\$USD）顯示。

下列各節說明存取和使用截止日期雲端用量總管的步驟。

主題

- [先決條件](#)
- [開啟用量總管](#)
- [使用用量總管](#)

先決條件

若要使用截止日期雲端用量總管，您必須擁有 MANAGER 或 OWNER 陣列許可。如需詳細資訊，請參閱[了解存取層級](#)。

Note

如果您的時區不符合完整小時，例如印度標準時間 (UTC+5 : 30)，則用量總管不會顯示用量指標。若要查看指標，請將您的時區設定為符合完整小時的區域。

開啟用量總管

若要開啟截止日期雲端用量總管，請使用下列程序。

1. 登入 AWS 管理主控台 並開啟截止日期雲端[主控台](#)。
2. 若要查看所有可用的陣列，請選擇檢視陣列。
3. 找到您要取得相關資訊的陣列，然後選擇管理任務。截止日期雲端監視器會在新索引標籤中開啟。
4. 在截止日期雲端監視器的左側選單中，選取用量總管。

使用用量總管

從用量總管頁面，您可以選擇可以顯示資料的特定參數。根據預設，您會看到過去 7 天內的時間（小時和分鐘）總用量。您可以變更這些參數，而顯示的資訊會根據參數設定動態變更。

您可以根據佇列、任務、使用者、運算用量、執行個體類型或授權產品來分組結果。如果您選擇授權產品，則會針對特定授權計算成本。對於所有其他群組，時間的計算方式是將每個任務執行所需的時間相加。

用量總管只會根據您設定的篩選條件傳回 100 個結果。結果會依建立時間戳記的日期以遞減順序列出。如果結果超過 100 個，您會收到錯誤訊息。您可以精簡查詢，以減少結果的數量：

- 選取較小的時間範圍
- 選取較少的佇列
- 選取不同的分組，例如依佇列分組而非任務

主題

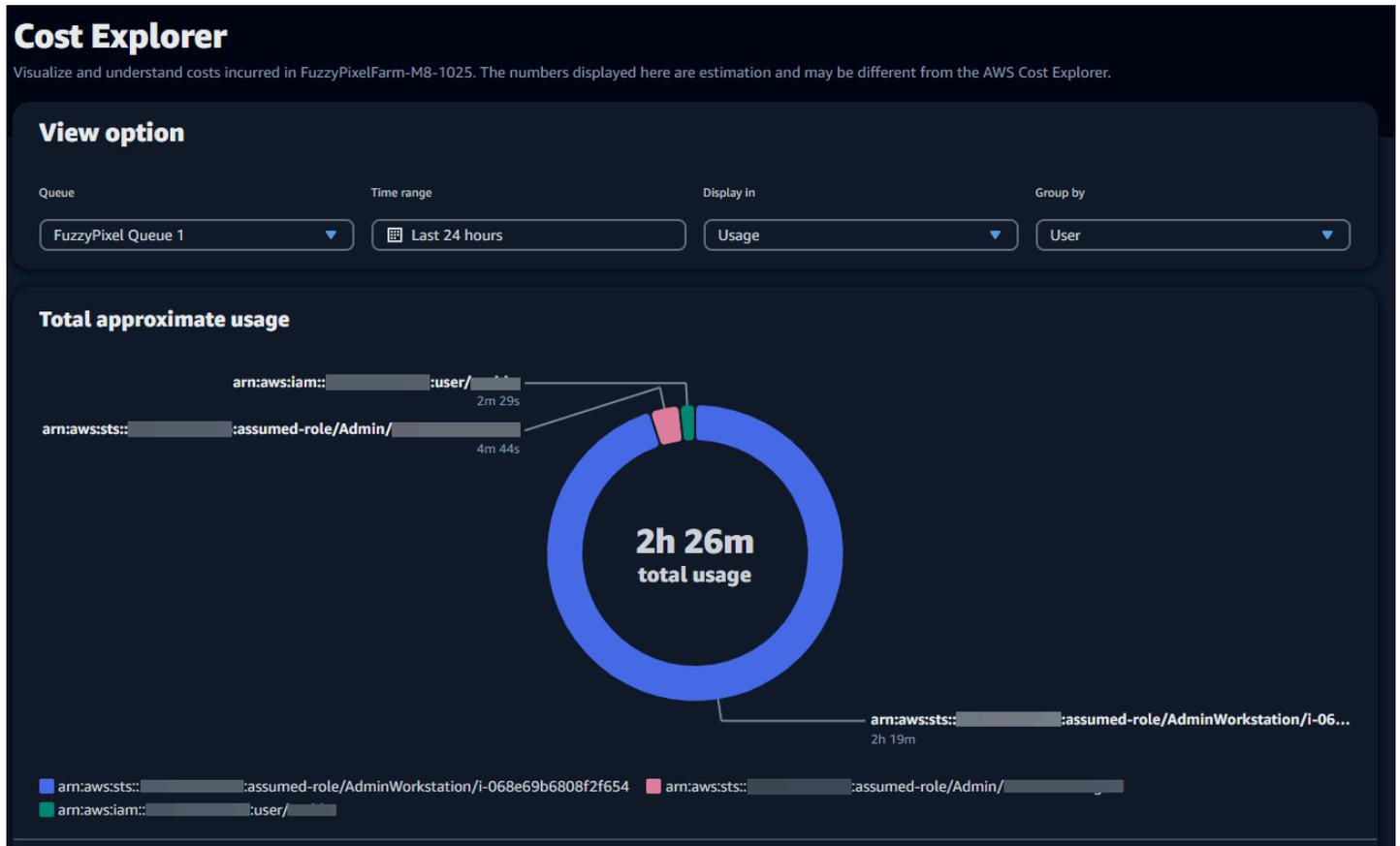
- [使用視覺化圖形來檢閱資料](#)
- [檢視指標明細](#)
- [檢視佇列的大約執行時間](#)

使用視覺化圖形來檢閱資料

您可以檢閱視覺化格式的資料，以識別可能需要更多分析或關注的趨勢和潛在領域。用量總管提供圓餅圖，顯示整體用量和成本，並可選擇將總計分組為較小的小計。

Note

圖表只會顯示前五個結果，並在「其他」區段中結合其他結果。您可以在圖表下方的明細區段中檢視所有結果。



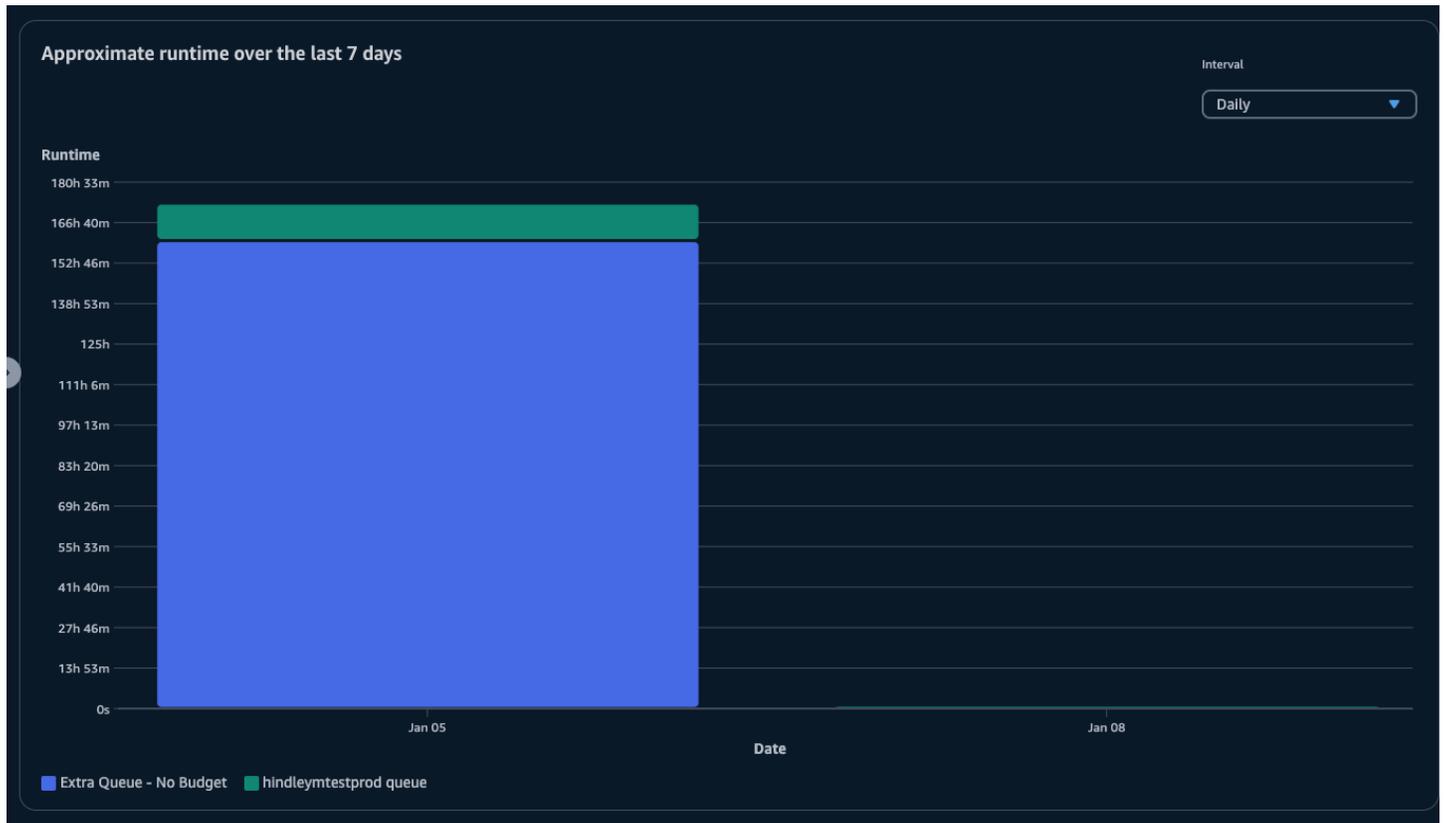
檢視指標明細

在圓餅圖下，用量總管提供更詳細的特定指標明細，這會隨著參數變更而變更。根據預設，用量總管中會顯示五個結果。您可以使用明細區段中的分頁箭頭來捲動結果。

預設會將明細降至最低。若要展開並顯示結果，請選取檢視所有明細箭頭。若要下載明細，請選擇下載資料。

檢視佇列的大約執行時間

您也可以根據您指定的不同間隔，檢視佇列的大約執行時間。間隔選項為每小時、每日、每週和每月。選取間隔後，圖形會顯示佇列的大約執行時間。



成本管理

AWS Deadline Cloud 提供預算和用量總管，協助您控制和視覺化任務的成本。不過，截止日期雲端會使用其他 AWS 服務，例如 Amazon S3。這些服務的成本不會反映在截止日期雲端預算或用量總管中，並根據用量單獨收費。視您設定截止日期雲端的方式而定，您可以使用下列 AWS 服務以及其他服務：

服務	定價頁面
Amazon CloudWatch Logs	Amazon CloudWatch Logs 定價
Amazon Elastic Compute Cloud	Amazon Elastic Compute Cloud 定價
AWS Key Management Service	AWS Key Management Service 定價
AWS PrivateLink	AWS PrivateLink 定價
Amazon Simple Storage Service	Amazon Simple Storage Service 定價

服務	定價頁面
Amazon Virtual Private Cloud	Amazon Virtual Private Cloud 定價

成本管理最佳實務

使用下列最佳實務可協助您了解和控制使用截止日期雲端時的成本，以及您可以在成本和效率之間做出的權衡。

Note

使用截止日期雲端的最終成本取決於多種 AWS 服務的互動、您處理的工作量，以及您執行工作 AWS 區域 所在的。下列最佳實務是指導方針，可能不會大幅降低成本。

CloudWatch Logs 的最佳實務

截止日期 雲端會將工作者和任務日誌傳送至 CloudWatch Logs。您需要支付收集、存放和分析這些日誌的費用。您可以只記錄監控任務所需的最低資料量，以降低成本。

當您建立佇列或機群時，Deadline Cloud 會使用下列名稱建立 CloudWatch Logs 日誌群組：

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

根據預設，這些日誌永遠不會過期。您可以調整日誌群組的保留政策，以移除舊日誌並協助降低儲存成本。您也可以將日誌匯出至 Amazon S3。Amazon S3 儲存成本低於 CloudWatch 的成本。如需詳細資訊，請參閱[將日誌資料匯出到 Amazon S3](#)。

Amazon EC2 的最佳實務

您可以針對服務受管和客戶受管機群使用 Amazon EC2 執行個體。有三個考量：

- 對於服務受管機群，您可以透過設定機群的最小工作者計數，選擇隨時有一或多個執行個體可用。當您將最小工作者計數設定為 0 以上時，機群一律會執行此數量的工作者。此設定可以減少截止日期雲端開始處理任務所需的時間，但您需要支付執行個體閒置時間的費用。
- 針對服務受管機群，設定機群的大小上限。此設定會限制機群可自動擴展的執行個體數量。即使有更多任務等待處理，機群也不會超過此大小。

- 對於服務受管和客戶受管機群，您可以在機群中指定 Amazon EC2 執行個體類型。使用較小的執行個體每分鐘成本較低，但可能需要更長的時間才能完成任務。相反地，較大的執行個體每分鐘成本較高，但可以縮短完成任務的時間。了解任務在執行個體上放置的需求，有助於降低成本。
- 可能的話，為您的機群選擇 Amazon EC2 Spot 執行個體。Spot 執行個體價格較低，但可能會因為隨需請求而中斷。隨需執行個體按秒計費，不會中斷。

的最佳實務 AWS KMS

根據預設，Deadline Cloud 會使用 AWS 擁有的金鑰來加密您的資料。您不需要為此金鑰付費。

您可以選擇使用客戶受管金鑰來加密您的資料。當您使用自己的金鑰時，會根據金鑰的使用方式向您收費。如果您使用現有的金鑰，這將是額外使用的增量成本。

的最佳實務 AWS PrivateLink

您可以使用 AWS PrivateLink 來使用介面端點在 VPC 與截止日期雲端之間建立連線。建立連線時，您可以呼叫所有截止日期雲端 API 動作。系統會針對您建立的每個端點按小時收費。如果您使用 PrivateLink，則必須建立至少三個端點，而且視您的組態而定，您可能需要最多五個端點。

Amazon S3 的最佳實務

Deadline Cloud 使用 Amazon S3 存放資產以進行處理、任務連接、輸出和日誌。若要降低與 Amazon S3 相關的成本，請減少您存放的資料量。一些建議：

- 僅存放目前正在使用或即將使用的資產。
- 使用 [S3 生命週期組態](#)，自動從 S3 儲存貯體刪除未使用的檔案。

Amazon VPC 的最佳實務

當您使用客戶受管機群的用量型授權時，您可以建立截止日期雲端授權端點，這是在您的帳戶中建立的 Amazon VPC 端點。此端點會以每小時費率計費。若要降低成本，請在不使用用量型授權時移除端點。

中的安全性 Deadline Cloud

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模式](#)將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。作為[AWS 合規計劃](#)的一部分，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計劃 AWS Deadline Cloud，請參閱[AWS 服務 合規計劃範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 服務 的。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 時套用共同責任模型 Deadline Cloud。下列主題說明如何設定 Deadline Cloud 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務 來協助您監控和保護 Deadline Cloud 資源。

主題

- [中的資料保護 Deadline Cloud](#)
- [截止日期雲端中的身分和存取管理](#)
- [的合規驗證 Deadline Cloud](#)
- [中的彈性 Deadline Cloud](#)
- [截止日期雲端中的基礎設施安全性](#)
- [截止日期雲端中的組態和漏洞分析](#)
- [預防跨服務混淆代理人](#)
- [AWS Deadline Cloud 使用界面端點存取 \(AWS PrivateLink\)](#)
- [受限的網路環境](#)
- [截止日期雲端的安全最佳實務](#)

中的資料保護 Deadline Cloud

AWS [共同責任模型](#)適用於 中的資料保護 AWS Deadline Cloud。如此模型所述，AWS 負責保護執行所有的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答](#)

[集](#)。如需有關歐洲資料保護的相關資訊，請參閱AWS 安全性部落格上的[AWS 共同責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Deadline Cloud 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

輸入 Deadline Cloud 任務範本中名稱欄位的資料也可能包含在帳單或診斷日誌中，且不應包含機密或敏感資訊。

主題

- [靜態加密](#)
- [傳輸中加密](#)
- [金鑰管理](#)
- [網際網路流量隱私權](#)
- [選擇退出](#)

靜態加密

AWS Deadline Cloud 使用存放在 [AWS Key Management Service \(AWS KMS\)](#) 中的加密金鑰加密靜態資料，以保護敏感資料。所有 都可以使用靜態加密 AWS 區域 Deadline Cloud 。

加密資料表示沒有有效金鑰的使用者或應用程式無法讀取儲存在磁碟上的敏感資料。只有具有有效受管金鑰的一方才能解密資料。

Deadline Cloud 當服務受管機群工作者執行個體終止時，會刪除 Amazon Elastic Block Store 磁碟區。

如需 Deadline Cloud 如何使用 AWS KMS 加密靜態資料的資訊，請參閱 [金鑰管理](#)。

傳輸中加密

對於傳輸中的資料，AWS Deadline Cloud 會使用 Transport Layer Security (TLS) 1.2 或 1.3 來加密服務與工作者之間傳送的資料。我們需要 TLS 1.2 並建議使用 TLS 1.3。此外，如果您使用虛擬私有雲端 (VPC)，您可以使用在 VPC 與之間 AWS PrivateLink 建立私有連線 Deadline Cloud。

金鑰管理

建立新的陣列時，您可以選擇下列其中一個金鑰來加密您的陣列資料：

- AWS 擁有的 KMS 金鑰 – 如果您在建立陣列時未指定金鑰，則預設加密類型。KMS 金鑰由擁有 AWS Deadline Cloud。您無法檢視、管理或使用 AWS 擁有的金鑰。不過，您不需要採取任何動作來保護加密資料的金鑰。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 [AWS 擁有的金鑰](#)。
- 客戶受管 KMS 金鑰 – 您在建立陣列時指定客戶受管金鑰。陣列中的所有內容都會使用 KMS 金鑰加密。金鑰會存放在您的帳戶中，並由您建立、擁有和管理，並 AWS KMS 收取費用。您可以完全控制 KMS 金鑰。您可以執行下列任務：
 - 建立和維護金鑰政策
 - 建立和維護 IAM 政策和授予操作
 - 啟用和停用金鑰政策
 - 新增 標籤
 - 建立金鑰別名

您無法手動輪換與 Deadline Cloud 陣列搭配使用的客戶擁有金鑰。支援自動輪換金鑰。

如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [客戶擁有的金鑰](#)。

若要建立客戶受管金鑰，請遵循《AWS Key Management Service 開發人員指南》中的 [建立對稱客戶受管金鑰](#) 的步驟。

Deadline Cloud 如何使用 AWS KMS 授予

Deadline Cloud 需要[授予](#)才能使用您的客戶受管金鑰。當您建立使用客戶受管金鑰加密的陣列時，會透過傳送[CreateGrant](#)請求至 AWS KMS 來代表您 Deadline Cloud 建立授予，以存取您指定的 KMS 金鑰。

Deadline Cloud 使用多個授予。每個授權都會由 Deadline Cloud 需要加密或解密資料的不同部分使用。Deadline Cloud 也會使用授權來允許存取 AWS 其他用來代表您存放資料的服務，例如 Amazon Simple Storage Service、Amazon Elastic Block Store 或 OpenSearch。

可讓 Deadline Cloud 管理服務受管機群中機器的授予包括 Deadline Cloud 中的帳號和角色，`GranteePrincipal`而不是服務主體。雖然不是典型的，但這對於使用為陣列指定的客戶受管 KMS 金鑰來加密服務受管機群中工作者的 Amazon EBS 磁碟區是必要的。

客戶受管金鑰政策

金鑰政策會控制客戶受管金鑰的存取權限。每個金鑰都必須只有一個金鑰政策，其中包含可決定誰可以使用金鑰及其使用方式的陳述式。當您建立客戶受管金鑰時，您可以指定金鑰政策。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[管理客戶受管金鑰的存取](#)。

CreateFarm 的最低 IAM 政策

若要使用客戶受管金鑰來使用主控台或 [CreateFarm](#) API 操作建立陣列，必須允許下列 AWS KMS API 操作：

- [kms:CreateGrant](#)：新增客戶受管金鑰的授權。授予主控台對指定 AWS KMS 金鑰的存取權。如需詳細資訊，請參閱AWS Key Management Service 《開發人員指南》中的[使用授權](#)。
- [kms:Decrypt](#) – 允許 Deadline Cloud 解密陣列中的資料。
- [kms:DescribeKey](#) – 提供客戶受管金鑰詳細資訊，Deadline Cloud 以允許 驗證金鑰。
- [kms:GenerateDataKey](#) – 允許 Deadline Cloud 使用唯一的資料金鑰加密資料。

下列政策陳述式會授予 CreateFarm操作的必要許可。

JSON

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

唯讀操作的最低 IAM 政策

若要將客戶受管金鑰用於唯讀 Deadline Cloud 操作，例如取得有關陣列、佇列和機群的資訊。必須允許下列 AWS KMS API 操作：

- [kms:Decrypt](#) – 允許 Deadline Cloud 解密陣列中的資料。
- [kms:DescribeKey](#) – 提供客戶受管金鑰詳細資訊，Deadline Cloud 以允許 驗證金鑰。

下列政策陳述式會授予唯讀操作的必要許可。

JSON

```
{
  "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"
        }
      }
    }
  ]
}

```

讀取寫入操作的最低 IAM 政策

若要將客戶受管金鑰用於讀寫 Deadline Cloud 操作，例如建立和更新陣列、佇列和機群。必須允許下列 AWS KMS API 操作：

- [kms:Decrypt](#) – 允許 Deadline Cloud 解密陣列中的資料。
- [kms:DescribeKey](#) – 提供客戶受管金鑰詳細資訊，Deadline Cloud 以允許 驗證金鑰。
- [kms:GenerateDataKey](#) – 允許 Deadline Cloud 使用唯一的資料金鑰加密資料。

下列政策陳述式會授予 CreateFarm操作的必要許可。

JSON

```

{
  "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"
        }
    }
}

```

監控加密金鑰

當您搭配 Deadline Cloud 陣列使用 AWS KMS 客戶受管金鑰時，您可以使用 [AWS CloudTrail](#) 或 [Amazon CloudWatch Logs](#) 來追蹤 Deadline Cloud 傳送至 的請求 AWS KMS。

授予的 CloudTrail 事件

建立授予時，通常會在呼叫 CreateFarm、CreateMonitor 或 CreateFleet 操作時發生下列 CloudTrail 事件範例。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "arn": "arn:aws::iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-04-23T02:05:26Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "invokedBy": "deadline.amazonaws.com"
},

```

```
"eventTime": "2024-04-23T02:05:35Z",
"eventSource": "kms.amazonaws.com",
"eventName": "CreateGrant",
"awsRegion": "us-west-2",
"sourceIPAddress": "deadline.amazonaws.com",
"userAgent": "deadline.amazonaws.com",
"requestParameters": {
  "operations": [
    "CreateGrant",
    "Decrypt",
    "DescribeKey",
    "Encrypt",
    "GenerateDataKey"
  ],
  "constraints": {
    "encryptionContextSubset": {
      "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
      "aws:deadline:accountId": "111122223333"
    }
  },
  "granteePrincipal": "deadline.amazonaws.com",
  "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "retiringPrincipal": "deadline.amazonaws.com"
},
"responseElements": {
  "grantId": "6bbe819394822a400fe5e3a75d0e9ef16c1733143fff0c1fc00dc7ac282a18a0",
  "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
"eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
"readOnly": false,
"resources": [
  {
    "accountId": "AWS Internal",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE44444"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
```

```
"eventCategory": "Management"
}
```

用於解密的 CloudTrail 事件

使用客戶受管 KMS 金鑰解密值時，會發生下列 CloudTrail 事件範例。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "arn": "arn:aws::iam::111122223333:role/SampleRole",
        "accountId": "111122223333",
        "userName": "SampleRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-04-23T18:46:51Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "deadline.amazonaws.com"
  },
  "eventTime": "2024-04-23T18:51:44Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "deadline.amazonaws.com",
  "userAgent": "deadline.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
      "aws:deadline:accountId": "111122223333",
      "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLERealAGTESTONLY+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-eeeeefffffff",
  "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"
}

```

用於加密的 CloudTrail 事件

使用客戶受管 KMS 金鑰加密值時，會發生下列 CloudTrail 事件範例。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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-abcdef12345678900987654321fedcba",
        "aws:deadline:accountId": "111122223333",
        "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEEaaqNOTREALaGTESTONLY
+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"
}
```

刪除客戶受管 KMS 金鑰

在 AWS Key Management Service (AWS KMS) 中刪除客戶受管 KMS 金鑰具有破壞性和潛在危險性。它會不可復原地刪除金鑰材料以及與金鑰相關聯的所有中繼資料。刪除客戶受管 KMS 金鑰後，您無法再解密該金鑰加密的資料。刪除金鑰表示資料無法復原。

這就是為什麼在刪除 KMS 金鑰之前，AWS KMS 會給予客戶最多 30 天的等待期。預設等待期間為 30 天。

關於等待期

由於刪除客戶受管 KMS 金鑰具有破壞性和潛在危險性，因此我們要求您設定 7–30 天的等待期間。預設等待期間為 30 天。

不過，實際等待期間可能比您排定的期間長最多 24 小時。若要取得要刪除金鑰的實際日期和時間，請使用 [DescribeKey](#) 操作。您也可以在金鑰的詳細資訊頁面的一般組態區段中，在 [AWS KMS 主控台](#) 中查看金鑰的排程刪除日期。請注意時區。

在等待期間，客戶受管金鑰的狀態和金鑰狀態為待刪除。

- 待刪除的客戶受管 KMS 金鑰無法用於任何 [密碼編譯操作](#)。
- AWS KMS 不會 [輪換待刪除之客戶受管 KMS 金鑰的備份](#) 金鑰。

如需刪除客戶受管 KMS 金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [刪除客戶主金鑰](#)。

網際網路流量隱私權

AWS Deadline Cloud 支援 Amazon Virtual Private Cloud (Amazon VPC) 保護連線。Amazon VPC 提供您可以用來提高和監控虛擬私有雲端 (VPC) 安全性的功能。

您可以使用在 VPC 內執行的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體來設定客戶受管機群 (CMF)。透過部署要使用的 Amazon VPC 端點 AWS PrivateLink，CMF 中的工作者與 Deadline Cloud 端點之間的流量會保留在您的 VPC 內。此外，您可以設定 VPC 以限制執行個體的網際網路存取。

在服務受管機群中，工作者無法從網際網路連線，但他們確實可以存取網際網路並透過網際網路連線至 Deadline Cloud 服務。每個服務受管機群都會在自己的隔離網路中執行，而工作者執行個體仍專屬於個別客戶。

選擇退出

AWS Deadline Cloud 會收集特定操作資訊，以協助我們開發和改善 Deadline Cloud。收集的資料包含 AWS 您的帳戶 ID 和使用者 ID 等物件，因此如果您對 有問題，我們可以正確識別您的身分 Deadline Cloud。我們也會收集 Deadline Cloud 特定資訊，例如資源 IDs (適用時為 FarmID 或 QueueID)、產品名稱 (例如 JobAttachments、WorkerAgent 等) 和產品版本。

您可以選擇使用應用程式組態選擇退出此資料收集。與用戶端工作站和機群工作者 Deadline Cloud 互動的每個電腦都需要分別選擇退出。

Deadline Cloud Monitor - 桌面

Deadline Cloud 監控 - 桌面會收集操作資訊，例如當當機和開啟應用程式時，以協助我們了解應用程式何時發生問題。若要選擇退出收集此操作資訊，請前往設定頁面並清除開啟資料收集，以測量截止日期雲端監視器的效能。

選擇不接收後，桌面監視器不會再傳送操作資料。任何先前收集的資料都會保留，但仍可用於改善服務。如需更多資訊，請參閱 [資料隱私權常見問答集](#)。

AWS Deadline Cloud CLI 和工具

AWS Deadline Cloud CLI、提交者和工作者代理程式都會收集操作資訊，例如何時發生當機，以及何時提交任務，以協助我們了解您何時遇到這些應用程式的問題。若要選擇退出收集此操作資訊，請使用下列任一方法：

- 在終端機中，輸入 **deadline config set telemetry.opt_out true**。

以目前使用者身分執行時，這會選擇退出 CLI、提交者和工作者代理程式。

- 安裝 Deadline Cloud 工作者代理程式時，請新增 **--telemetry-opt-out** 命令列引數。例如 **./install.sh --farm-id \$FARM_ID --fleet-id \$FLEET_ID --telemetry-opt-out**。
- 在執行工作者代理程式、CLI 或提交者之前，請設定環境變數：

```
DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true
```

在您選擇退出後，Deadline Cloud 工具不會再傳送操作資料。任何先前收集的資料都會保留，但仍可用於改善服務。如需更多資訊，請參閱 [資料隱私權常見問答集](#)。

截止日期雲端中的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可），以使用截止日期雲端資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [Deadline Cloud 如何與 IAM 搭配使用](#)
- [截止日期雲端的身分型政策範例](#)
- [AWS 截止日期雲端的 受管政策](#)
- [服務角色](#)
- [對 AWS 截止日期雲端身分和存取進行故障診斷](#)

目標對象

您的使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [對 AWS 截止日期雲端身分和存取進行故障診斷](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [Deadline Cloud 如何與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [截止日期雲端的身分型政策範例](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的 [如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center？](#)。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者，以 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

Deadline Cloud 如何與 IAM 搭配使用

在您使用 IAM 管理對截止日期雲端的存取之前，請先了解哪些 IAM 功能可與截止日期雲端搭配使用。

您可以搭配截止日期雲端使用的 IAM AWS 功能

IAM 功能	截止日期雲端支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	否

若要全面了解 Deadline Cloud 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用，請參閱《IAM 使用者指南》中的與 [AWS IAM 搭配使用的 服務](#)。

截止日期雲端的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的 [透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素參考](#)。

截止日期雲端的身分型政策範例

若要檢視截止日期雲端身分型政策的範例，請參閱 [截止日期雲端的身分型政策範例](#)。

截止日期雲端中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

截止日期雲端的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看截止日期雲端動作的清單，請參閱服務授權參考中的 [AWS 截止日期雲端定義的動作](#)。

Deadline Cloud 中的政策動作在動作之前使用下列字首：

```
deadline
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
```

```
"deadline:action1",  
"deadline:action2"  
]
```

若要檢視截止日期雲端身分型政策的範例，請參閱 [截止日期雲端的身分型政策範例](#)。

截止日期雲端的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看截止日期雲端資源類型及其 ARNs 的清單，請參閱服務授權參考中的 [AWS 截止日期雲端定義的資源](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS 截止日期雲端定義的動作](#)。

若要檢視截止日期雲端身分型政策的範例，請參閱 [截止日期雲端的身分型政策範例](#)。

截止日期雲端的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

若要查看截止日期雲端條件索引鍵的清單，請參閱服務授權參考中的 [AWS 截止日期雲端的條件索引鍵](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [AWS 截止日期雲端定義的動作](#)。

若要檢視截止日期雲端身分型政策的範例，請參閱 [截止日期雲端的身分型政策範例](#)。

截止日期雲端中的 ACLs

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 與截止日期雲端

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的 [使用屬性型存取控制 \(ABAC\)](#)。

將臨時登入資料與截止日期雲端搭配使用

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務](#)。

轉送截止日期雲端的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱 [轉發存取工作階段](#)。

截止日期雲端的服務角色

支援服務角色：是

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可給 AWS 服務](#)。

Warning

變更服務角色的許可可能會中斷截止日期雲端功能。只有在截止日期雲端提供指引時，才能編輯服務角色。

截止日期雲端的服務連結角色

支援服務連結角色：否

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱[可搭配 IAM 運作的 AWS 服務](#)。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

截止日期雲端的身分型政策範例

根據預設，使用者和角色沒有建立或修改截止日期雲端資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

如需 Deadline Cloud 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的[AWS Deadline Cloud 的動作、資源和條件索引鍵](#)。

主題

- [政策最佳實務](#)
- [使用截止日期雲端主控台](#)
- [存取主控台的政策](#)
- [將任務提交至佇列的政策](#)
- [允許建立授權端點的政策](#)
- [允許監控特定陣列佇列的政策](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除截止日期雲端資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

使用截止日期雲端主控台

若要存取 AWS 截止日期雲端主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視您 中截止日期雲端資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用截止日期雲端主控台，也請將截止日期雲端 [ConsoleAccess](#) 或 [ReadOnly](#) AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可到使用者](#)。

存取主控台的政策

若要授予對 Deadline Cloud 主控台中所有功能的存取權，請將此身分政策連接至您想要擁有完整存取權的使用者或角色。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2InstanceTypeSelection",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "pricing:GetProducts"
      ],
      "Resource": ["*"]
    },
    {
      "Sid": "VPCResourceSelection",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": ["*"]
    },
    {
      "Sid": "ViewVpcLatticeResources",
      "Effect": "Allow",
      "Action": [
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource": ["*"]
    },
    {
      "Sid": "ManageVpcEndpointsViaDeadline",
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:CreateVpcEndpoint",
      "ec2:DescribeVpcEndpoints",
      "ec2>DeleteVpcEndpoints",
      "ec2:CreateTags"
    ],
    "Resource": ["*"],
    "Condition": {
      "StringEquals": { "aws:CalledViaFirst": "deadline.amazonaws.com" }
    }
  },
  {
    "Sid": "ChooseJobAttachmentsBucket",
    "Effect": "Allow",
    "Action": ["s3:GetBucketLocation", "s3:ListAllMyBuckets"],
    "Resource": "*"
  },
  {
    "Sid": "CreateDeadlineCloudLogGroups",
    "Effect": "Allow",
    "Action": ["logs:CreateLogGroup"],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/deadline/*",
    "Condition": {
      "StringLike": { "aws:CalledViaFirst": "deadline.amazonaws.com" }
    }
  },
  {
    "Sid": "ValidateDependencies",
    "Effect": "Allow",
    "Action": ["s3:ListBucket"],
    "Resource": "*",
    "Condition": {
      "StringLike": { "aws:CalledViaFirst": "deadline.amazonaws.com" }
    }
  },
  {
    "Sid": "RoleSelection",
    "Effect": "Allow",
    "Action": ["iam:GetRole", "iam:ListRoles"],
    "Resource": "*"
  },
  {
    "Sid": "PassRoleToDeadlineCloud",
    "Effect": "Allow",

```

```
    "Action": ["iam:PassRole"],
    "Condition": {
      "StringLike": { "iam:PassedToService": "deadline.amazonaws.com" }
    },
    "Resource": "*"
  },
  {
    "Sid": "KMSKeySelection",
    "Effect": "Allow",
    "Action": ["kms:ListKeys", "kms:ListAliases"],
    "Resource": "*"
  },
  {
    "Sid": "IdentityStoreReadOnly",
    "Effect": "Allow",
    "Action": [
      "identitystore:DescribeUser",
      "identitystore:DescribeGroup",
      "identitystore:ListGroups",
      "identitystore:ListUsers",
      "identitystore:IsMemberInGroups",
      "identitystore:ListGroupMemberships",
      "identitystore:ListGroupMembershipsForMember",
      "identitystore:GetGroupMembershipId"
    ],
    "Resource": "*"
  },
  {
    "Sid": "OrganizationAndIdentityCenterIdentification",
    "Effect": "Allow",
    "Action": [
      "sso:ListDirectoryAssociations",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "sso:DescribeRegisteredRegions",
      "sso:GetManagedApplicationInstance",
      "sso:GetSharedSsoConfiguration",
      "sso:ListInstances",
      "sso:GetApplicationAssignmentConfiguration",
      "sso:GetSSOStatus",
      "sso:ListRegions",
      "sso:DescribeRegion"
    ],
    "Resource": "*"
  }
}
```

```

    },
    {
      "Sid": "ManagedDeadlineCloudIDCAApplication",
      "Effect": "Allow",
      "Action": [
        "sso:CreateApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso>DeleteApplication",
        "sso:UpdateApplication"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": { "aws:CalledViaFirst": "deadline.amazonaws.com" }
      }
    },
    {
      "Sid": "ChooseSecret",
      "Effect": "Allow",
      "Action": ["secretsmanager:ListSecrets"],
      "Resource": "*"
    },
    {
      "Sid": "DeadlineMembershipActions",
      "Effect": "Allow",
      "Action": [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToQueue",
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListQueueMembers",
        "deadline:ListJobMembers"
      ],
      "Resource": ["*"]
    },
    {
      "Sid": "DeadlineControlPlaneActions",

```

```
"Effect": "Allow",
"Action": [
    "deadline:CreateMonitor",
    "deadline:GetMonitor",
    "deadline:UpdateMonitor",
    "deadline>DeleteMonitor",
    "deadline:ListMonitors",
    "deadline:CreateFarm",
    "deadline:GetFarm",
    "deadline:UpdateFarm",
    "deadline>DeleteFarm",
    "deadline:ListFarms",
    "deadline:CreateQueue",
    "deadline:GetQueue",
    "deadline:UpdateQueue",
    "deadline>DeleteQueue",
    "deadline:ListQueues",
    "deadline:CreateFleet",
    "deadline:GetFleet",
    "deadline:UpdateFleet",
    "deadline>DeleteFleet",
    "deadline:ListFleets",
    "deadline:ListWorkers",
    "deadline:CreateQueueFleetAssociation",
    "deadline:GetQueueFleetAssociation",
    "deadline:UpdateQueueFleetAssociation",
    "deadline>DeleteQueueFleetAssociation",
    "deadline:ListQueueFleetAssociations",
    "deadline:CreateQueueEnvironment",
    "deadline:GetQueueEnvironment",
    "deadline:UpdateQueueEnvironment",
    "deadline>DeleteQueueEnvironment",
    "deadline:ListQueueEnvironments",
    "deadline:CreateLimit",
    "deadline:GetLimit",
    "deadline:UpdateLimit",
    "deadline>DeleteLimit",
    "deadline:ListLimits",
    "deadline:CreateQueueLimitAssociation",
    "deadline:GetQueueLimitAssociation",
    "deadline>DeleteQueueLimitAssociation",
    "deadline:UpdateQueueLimitAssociation",
    "deadline:ListQueueLimitAssociations",
    "deadline:CreateStorageProfile",
```

```

        "deadline:GetStorageProfile",
        "deadline:UpdateStorageProfile",
        "deadline>DeleteStorageProfile",
        "deadline>ListStorageProfiles",
        "deadline>ListStorageProfilesForQueue",
        "deadline>ListBudgets",
        "deadline:TagResource",
        "deadline:UntagResource",
        "deadline>ListTagsForResource",
        "deadline>CreateLicenseEndpoint",
        "deadline:GetLicenseEndpoint",
        "deadline>DeleteLicenseEndpoint",
        "deadline>ListLicenseEndpoints",
        "deadline>ListAvailableMeteredProducts",
        "deadline>ListMeteredProducts",
        "deadline:PutMeteredProduct",
        "deadline>DeleteMeteredProduct"
    ],
    "Resource": ["*"]
  }]
}

```

將任務提交至佇列的政策

在此範例中，您會建立縮小範圍政策，授予在特定陣列中將任務提交至特定佇列的許可。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SubmitJobsFarmAndQueue",
      "Effect": "Allow",
      "Action": "deadline:CreateJob",
      "Resource": "arn:aws:deadline:us-east-1:111122223333:farm/FARM_A/queue/QUEUE_B/job/*"
    }
  ]
}

```

允許建立授權端點的政策

在此範例中，您會建立縮小範圍政策，授予建立和管理授權端點所需的許可。使用此政策為與陣列相關的 VPC 建立授權端點。

JSON

```
{
  "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": [
      "arn:aws:deadline:*:111122223333:*",
      "arn:aws:ec2:*:111122223333:vpc-endpoint/*"
    ]
  }]
}
```

允許監控特定陣列佇列的政策

在此範例中，您會建立縮小範圍政策，授予許可來監控特定陣列特定佇列中的任務。

JSON

```
{
  "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:us-east-1:123456789012:farm/FARM_A/queue/QUEUE_B",
    "arn:aws:deadline:us-east-1:123456789012:farm/FARM_A/queue/QUEUE_B/*"
  ]
}]
}
```

AWS 截止日期雲端的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 受管政策：AWSDeadlineCloud-FleetWorker

您可以將AWSDeadlineCloud-FleetWorker政策連接至 AWS Identity and Access Management (IAM) 身分。

此政策授予此機群中的工作者從服務連線和接收任務所需的許可。

許可詳細資訊

此政策包含以下許可：

- deadline – 允許主體管理機群中的工作者。

如需政策詳細資訊的 JSON 清單，請參閱 [《AWS 受管政策參考指南》中的 AWSDeadlineCloud-FleetWorker](#)。

AWS 受管政策：AWSDeadlineCloud-WorkerHost

您可將 AWSDeadlineCloud-WorkerHost 政策連接到 IAM 身分。

此政策會授予最初連線至 服務所需的許可。它可以用作 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體描述檔。

許可詳細資訊

此政策包含以下許可：

- deadline – 允許使用者建立工作者、擔任工作者的機群角色，以及將標籤套用至工作者

如需政策詳細資訊的 JSON 清單，請參閱 [AWS 受管政策參考指南中的 AWSDeadlineCloud-WorkerHost](#)。

AWS 受管政策：AWSDeadlineCloud-UserAccessFarms

您可將 AWSDeadlineCloud-UserAccessFarms 政策連接到 IAM 身分。

此政策可讓使用者根據他們所屬的陣列及其成員層級來存取陣列資料。

許可詳細資訊

此政策包含以下許可：

- `deadline` – 允許使用者存取陣列資料。
- `ec2` – 允許使用者查看 Amazon EC2 執行個體類型的詳細資訊。
- `identitystore` – 允許使用者查看使用者和群組名稱。
- `kms` – 允許使用者為其 AWS Key Management Service (IAM Identity Center AWS KMS) 執行個體設定 AWS IAM Identity Center () 客戶受管金鑰。

如需政策詳細資訊的 JSON 清單，請參閱 [《AWS 受管政策參考指南》中的 `AWSDeadlineCloud-UserAccessFarms`](#)。

AWS 受管政策：AWSDeadlineCloud-UserAccessFleets

您可將 AWSDeadlineCloud-UserAccessFleets 政策連接到 IAM 身分。

此政策可讓使用者根據他們所屬的陣列及其成員層級來存取機群資料。

許可詳細資訊

此政策包含以下許可：

- `deadline` – 允許使用者存取陣列資料。
- `ec2` – 允許使用者查看 Amazon EC2 執行個體類型的詳細資訊。
- `identitystore` – 允許使用者查看使用者和群組名稱。

如需政策詳細資訊的 JSON 清單，請參閱 [AWS 受管政策參考指南中的 `AWSDeadlineCloud-UserAccessFleets`](#)。

AWS 受管政策：AWSDeadlineCloud-UserAccessJobs

您可將 AWSDeadlineCloud-UserAccessJobs 政策連接到 IAM 身分。

此政策允許使用者根據他們所屬的陣列及其成員層級來存取任務資料。

許可詳細資訊

此政策包含以下許可：

- `deadline` – 允許使用者存取陣列資料。
- `ec2` – 允許使用者查看 Amazon EC2 執行個體類型的詳細資訊。
- `identitystore` – 允許使用者查看使用者和群組名稱。

如需政策詳細資訊的 JSON 清單，請參閱 [《AWS 受管政策參考指南》中的 `AWSDeadlineCloud-UserAccessJobs`](#)。

AWS 受管政策：AWSDeadlineCloud-UserAccessQueues

您可將 `AWSDeadlineCloud-UserAccessQueues` 政策連接到 IAM 身分。

此政策可讓使用者根據他們所屬的陣列及其成員層級來存取佇列資料。

許可詳細資訊

此政策包含以下許可：

- `deadline` – 允許使用者存取陣列資料。
- `ec2` – 允許使用者查看 Amazon EC2 執行個體類型的詳細資訊。
- `identitystore` – 允許使用者查看使用者和群組名稱。

如需政策詳細資訊的 JSON 清單，請參閱 [《AWS 受管政策參考指南》中的 `AWSDeadlineCloud-UserAccessQueues`](#)。

AWS 受管政策的雲端更新截止日期

檢視自此服務開始追蹤這些變更以來，對 Deadline Cloud AWS 受管政策進行更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱截止日期雲端文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AWSDeadlineCloud-UserAccessFarms – 變更	期限 雲端新增了新動作 <code>kms:Decrypt</code> ，讓您可以將 AWS KMS 客戶管理的金鑰	2025 年 12 月 22 日

變更	描述	Date
	與 IAM Identity Center 執行個體搭配使用。	
AWSDeadlineCloud-WorkerHost – 變更	截止日期 雲端新增了動作 <code>deadline:TagResource</code> <code>deadline:ListTagsForResource</code> ，並允許您新增和檢視與機群中的工作者相關聯的標籤。	2025 年 5 月 30 日
AWSDeadlineCloud-UserAccessFarms – 變更	截止日期 雲端新增了動作 <code>deadline:GetJobTemplate</code> <code>deadline:ListJobParameterDefinitions</code> ，並允許您重新提交任務。	2024 年 10 月 7 日
AWSDeadlineCloud-UserAccessJobs – 變更		
AWSDeadlineCloud-UserAccessQueues – 變更		
截止日期 雲端已開始追蹤變更	截止日期 雲端開始追蹤其 AWS 受管政策的變更。	2024 年 4 月 2 日

服務角色

Deadline Cloud 如何使用 IAM 服務角色

Deadline Cloud 會自動擔任 IAM 角色，並提供臨時登入資料給工作者、任務和 Deadline Cloud Monitor。此方法消除手動憑證管理，同時透過角色型存取控制來維護安全性。

當您建立監視器、機群和佇列時，您可以指定 Deadline Cloud 代表您擔任的 IAM 角色。然後，工作者和截止日期雲端監視器會從這些角色接收臨時登入資料以供存取 AWS 服務。

機群角色

設定機群角色，為截止日期雲端工作者提供接收工作所需的許可，並報告該工作的進度。

您通常不需要自行設定此角色。您可以在截止日期雲端主控台中為您建立此角色，以包含必要的許可。使用下列指南來了解此角色的故障診斷詳細資訊。

以程式設計方式建立或更新機群時，請使用 `CreateFleet` 或 `UpdateFleet` API 操作指定機群角色 ARN。

機群角色的功能

機群角色為工作者提供以下許可：

- 接收新工作並向截止日期雲端服務報告進行中工作的進度
- 管理工作者生命週期和狀態
- 將日誌事件記錄到工作者日誌的 Amazon CloudWatch Logs

設定機群角色信任政策

您的機群角色必須信任截止日期雲端服務，並限定您的特定陣列範圍。

最佳實務是，信任政策應包含混淆代理人保護的安全條件。若要進一步了解混淆代理人保護，請參閱截止日期雲端使用者指南中的[混淆代理人](#)。

- `aws:SourceAccount` 確保只有來自相同的資源 AWS 帳戶 才能擔任此角色。
- `aws:SourceArn` 將角色假設限制為特定的截止日期雲端陣列。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDeadlineCredentialsService",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "Service": "credentials.deadline.amazonaws.com"
      },
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "YOUR_ACCOUNT_ID"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:YOUR_ACCOUNT_ID:farm/YOUR_FARM_ID"
        }
      }
    }
  ]
}
```

```
]
}
```

連接機群角色許可

將下列 AWS 受管政策連接至您的機群角色：

[AWSDeadlineCloud-FleetWorker](#)

此受管政策提供以下項目的許可：

- `deadline:AssumeFleetRoleForWorker` - 允許工作者重新整理其登入資料。
- `deadline:UpdateWorker` - 允許工作者更新其狀態（例如，退出時已停止）。
- `deadline:UpdateWorkerSchedule` - 用於取得工作和報告進度。
- `deadline:BatchGetJobEntity` - 用於擷取任務資訊。
- `deadline:AssumeQueueRoleForWorker` - 用於在任務執行期間存取佇列角色登入資料。

新增加密陣列的 KMS 許可

如果您的陣列是使用 KMS 金鑰建立的，請將這些許可新增至您的機群角色，以確保工作者可以存取陣列中的加密資料。

只有在您的陣列具有相關聯的 KMS 金鑰時，才需要 KMS 許可。`kms:ViaService` 條件必須使用格式 `deadline.{region}.amazonaws.com`。

建立機群時，會為該機群建立 CloudWatch Logs 日誌群組。Deadline Cloud 服務會使用工作者的許可，專門為該特定工作者建立日誌串流。在工作者設定並執行之後，工作者將使用這些許可將日誌事件直接傳送到 CloudWatch Logs。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": "arn:aws:logs:REGION:YOUR_ACCOUNT_ID:log-group:/aws/
deadline/YOUR_FARM_ID/*",
```

```

    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": [
          "deadline.REGION.amazonaws.com"
        ]
      }
    },
    {
      "Sid": "ManageLogEvents",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:REGION:YOUR_ACCOUNT_ID:log-group:/aws/
deadline/YOUR_FARM_ID/*"
    },
    {
      "Sid": "ManageKmsKey",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource": "YOUR_FARM_KMS_KEY_ARN",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "deadline.REGION.amazonaws.com"
        }
      }
    }
  ]
}

```

修改機群角色

機群角色的許可無法自訂。描述的許可始終是必要的，新增額外的許可沒有效果。

客戶管理的機群主機角色

如果您在 Amazon EC2 執行個體或內部部署主機上使用客戶管理的機群，請設定 WorkerHost 角色。

WorkerHost 角色的功能

WorkerHost 角色會在客戶受管機群主機上引導工作者。它提供主機所需的最低許可，以便：

- 在截止日期雲端中建立工作者
- 擔任機群角色以擷取操作登入資料
- 使用機群標籤標記工作者（如果已啟用標籤傳播）

設定 WorkerHost 角色許可

將下列 AWS 受管政策連接至您的 WorkerHost 角色：

[AWSDeadlineCloud-WorkerHost](#)

此受管政策提供以下項目的許可：

- `deadline:CreateWorker` - 允許主機註冊新的工作者。
- `deadline:AssumeFleetRoleForWorker` - 允許主機擔任機群角色。
- `deadline:TagResource` - 允許在建立期間標記工作者（如果啟用）。
- `deadline:ListTagsForResource` - 允許讀取機群標籤以進行傳播。

了解引導程序

WorkerHost 角色僅在初始工作者啟動期間使用：

1. 工作者代理程式會使用 WorkerHost 登入資料在主機上啟動。
2. 它叫用 `deadline:CreateWorker` 向截止日期雲端註冊。
3. 然後，它會叫用 `deadline:AssumeFleetRoleForWorker` 來擷取機群角色登入資料。
4. 從現在開始，工作者只會對所有操作使用機群角色登入資料。

工作者開始執行後，不會使用 WorkerHost 角色。服務受管機群不需要此政策。在服務受管機群中，會自動執行引導。

佇列角色

處理任務時，工作者會擔任佇列角色。此角色提供完成任務所需的許可。

以程式設計方式建立或更新佇列時，請使用 `CreateQueue` 或 `UpdateQueue` API 操作指定佇列角色 ARN。

設定佇列角色信任政策

您的佇列角色必須信任截止日期雲端服務。

最佳實務是，信任政策應包含混淆代理人保護的安全條件。若要進一步了解混淆代理人保護，請參閱截止日期雲端使用者指南中的[混淆代理人](#)。

- `aws:SourceAccount` 確保只有來自相同的資源 AWS 帳戶 才能擔任此角色。
- `aws:SourceArn` 將角色假設限制為特定的截止日期雲端陣列。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "credentials.deadline.amazonaws.com",
          "deadline.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "YOUR_ACCOUNT_ID"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:us-west-2:123456789012:farm/{farm-id}"
        }
      }
    }
  ]
}
```

了解佇列角色許可

佇列角色不使用單一受管政策。相反地，當您在主控台中設定佇列時，Deadline Cloud 會根據您的組態為您的佇列建立自訂政策。

此自動建立的政策可讓您存取：

任務附件

用於任務輸入和輸出檔案的指定 Amazon S3 儲存貯體讀取和寫入存取權：

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource": [
    "arn:aws:s3:::YOUR_JOB_ATTACHMENTS_BUCKET",
    "arn:aws:s3:::YOUR_JOB_ATTACHMENTS_BUCKET/YOUR_PREFIX/*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "YOUR_ACCOUNT_ID"
    }
  }
}
```

任務日誌

此佇列中任務的 CloudWatch Logs 讀取存取權。每個佇列都有自己的日誌群組，每個工作階段都有自己的日誌串流：

```
{
  "Effect": "Allow",
  "Action": [
    "logs:GetLogEvents"
  ],
  "Resource": "arn:aws:logs:REGION:YOUR_ACCOUNT_ID:log-group:/aws/
deadline/YOUR_FARM_ID/*"
}
```

第三方軟體

存取以下載 Deadline Cloud 支援的第三方軟體（例如 Maya、Blender 等）：

```
{
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "s3:DataAccessPointArn": "arn:aws:s3:*:*:accesspoint/deadline-software-*"
    },
    "StringEquals": {
      "s3:AccessPointNetworkOrigin": "VPC"
    }
  }
}
```

新增任務的許可

為您的任務需要存取 AWS 服務的佇列角色新增許可。撰寫 OpenJobDescription 步驟指令碼時，AWS CLI 和 SDK 會自動使用佇列角色的登入資料。使用此項目來存取完成任務所需的其他服務。

範例使用案例包括：

- 用於擷取自訂資料
- 通道到自訂授權伺服器的 SSM 許可
- 用於發出自訂指標的 CloudWatch
- 為動態工作流程建立新任務的截止日期雲端許可

如何使用佇列角色登入資料

Deadline Cloud 提供佇列角色登入資料給：

- 任務執行期間的工作者
- 透過截止日期雲端 CLI 的使用者，並在與任務附件和日誌互動時監控

Deadline Cloud 會為每個佇列建立個別的 CloudWatch Logs 日誌群組。任務使用佇列角色登入資料將日誌寫入其佇列的日誌群組。截止日期雲端 CLI 和監視器使用佇列角色（透過

`deadline:AssumeQueueRoleForRead`) 從佇列的日誌群組讀取任務日誌。截止日期雲端 CLI 和監視器使用佇列角色 (透過 `deadline:AssumeQueueRoleForUser`) 上傳或下載任務附件資料。

監控角色

設定監控角色，讓截止日期雲端監控 Web 和桌面應用程式存取您的截止日期雲端資源。

以程式設計方式建立或更新監視器時，請使用 `CreateMonitor` 或 `UpdateMonitor` API 操作指定監視器角色 ARN。

監控角色的功能

監控角色可讓 Deadline Cloud Monitor 提供最終使用者存取：

- 截止日期雲端整合提交者、CLI 和監視器所需的基本功能
- 最終使用者的自訂功能

設定監控角色信任政策

您的監控角色必須信任截止日期雲端服務。

最佳實務是，信任政策應包含混淆代理人保護的安全條件。若要進一步了解混淆代理人保護，請參閱截止日期雲端使用者指南中的[混淆代理人](#)。

`aws:SourceAccount` 確保只有來自相同的資源 AWS 帳戶 才能擔任此角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "credentials.deadline.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "YOUR_ACCOUNT_ID"
        }
      }
    }
  ]
}
```

```
]
}
```

連接監視器角色許可

將下列所有 AWS 受管政策連接至監視器角色以進行基本操作：

- [AWSDeadlineCloud-UserAccessFarms](#)
- [AWSDeadlineCloud-UserAccessFleets](#)
- [AWSDeadlineCloud-UserAccessJobs](#)
- [AWSDeadlineCloud-UserAccessQueues](#)

監控角色的運作方式

使用截止日期雲端監視器時，服務使用者會使用 AWS IAM Identity Center (IAM Identity Center) 登入，並擔任監視器角色。監控應用程式會使用擔任的角色登入資料來顯示監控 UI，包括陣列、機群、佇列和其他資訊的清單。

使用 Deadline Cloud Monitor 桌面應用程式時，這些登入資料會使用與最終使用者提供的設定檔名稱對應的具名 AWS 登入資料設定檔，在工作站上另外提供。請參閱 [AWS SDK 和工具參考指南](#)，進一步了解具名設定檔。

此具名設定檔是截止日期 CLI 和提交者存取截止日期雲端資源的方式。

自訂進階使用案例的監控角色

您可以自訂監控角色，以修改使用者在每個存取層級（檢視程式、貢獻者、管理員、擁有者）可執行的操作，或新增進階工作流程的許可。

自訂存取層級許可

連接到監控角色的四個 AWS 受管政策控制每個存取層級可以執行的操作。您可以將自訂政策新增至監控角色，以使用 `deadline:MembershipLevel` 條件金鑰授予或限制特定存取層級的許可。

例如，若要允許貢獻者更新和取消任務（通常僅限於經理和擁有者），請新增如下所示的政策：

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

```
{
  "Effect": "Allow",
  "Action": "deadline:UpdateJob",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "deadline:MembershipLevel": "CONTRIBUTOR"
    }
  }
}
```

透過此政策，貢獻者除了提交任務之外，還可以更新和取消任務。

新增進階工作流程的許可

您可以將自訂 IAM 政策新增至監控角色，以授予其他許可給所有監控使用者。這適用於進階指令碼工作流程，其中使用者需要存取標準截止日期雲端功能 AWS 服務 以外的。

修改您的監控角色時，請遵循下列準則：

- 請勿移除任何 受管政策。移除這些政策會中斷監視器功能。

Deadline Cloud Monitor 如何使用監控角色登入資料

期限 雲端監控會在您驗證時自動取得監控角色登入資料。此功能可讓桌面應用程式提供標準 Web 瀏覽器中可用功能以外的增強型監控功能。

當您使用截止日期雲端監視器登入時，它會自動建立您可以與 AWS CLI 或任何其他 AWS 工具搭配使用的設定檔。此設定檔使用監控角色登入資料，AWS 服務 可讓您根據監控角色中的許可，以程式設計方式存取。

截止日期雲端提交者的運作方式相同 - 他們使用截止日期雲端監視器建立的設定檔，以 AWS 服務 適當的角色許可存取。

期限雲端角色的進階自訂

您可以使用其他許可擴展截止日期雲端角色，以啟用基本轉譯工作流程以外的進階使用案例。此方法利用 Deadline Cloud 的存取管理系統，AWS 服務 根據佇列成員資格控制對其他的存取。

與的團隊協作 AWS CodeCommit

將 AWS CodeCommit 許可新增至佇列角色，以在專案儲存庫上啟用團隊協作。此方法將 Deadline Cloud 的存取管理系統用於其他使用案例 - 只有具有特定佇列存取權的使用者才會收到這些 AWS CodeCommit 許可，允許您透過 Deadline Cloud 佇列成員資格管理每個專案儲存庫的存取權。

這對於藝術家在轉譯工作流程中需要存取儲存在 AWS CodeCommit 儲存庫中的專案特定資產、指令碼或組態檔案的情況非常有用。

將 AWS CodeCommit 許可新增至佇列角色

將下列許可新增至佇列角色以啟用 AWS CodeCommit 存取：

```
{
  "Effect": "Allow",
  "Action": [
    "codecommit:GitPull",
    "codecommit:GitPush",
    "codecommit:GetRepository",
    "codecommit:ListRepositories"
  ],
  "Resource": "arn:aws:codecommit:REGION:YOUR_ACCOUNT_ID:PROJECT_REPOSITORY"
}
```

在藝術家工作站上設定登入資料提供者

將每個藝術家工作站設定為使用截止日期雲端佇列登入資料進行 AWS CodeCommit 存取。此設定會在每個工作站完成一次。

設定登入資料提供者

1. 將登入資料提供者設定檔新增至您的組態檔案 AWS (~/.aws/config)：

```
[profile queue-codecommit]
credential_process = deadline queue export-credentials --farm-id farm-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX --queue-id queue-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

2. 設定 Git 以將此設定檔用於 AWS CodeCommit 儲存庫：

```
git config --global credential.https://git-codecommit.REGION.amazonaws.com.helper '!aws codecommit credential-helper --profile queue-codecommit $@'
```

```
git config --global credential.https://git-  
codecommit.REGION.amazonaws.com.UseHttpPath true
```

將 *farm-XXXXXXXXXXXXXXXXXXXXXXXXXXXX* 和 *queue-XXXXXXXXXXXXXXXXXXXXXXXXXXXX* 取
代為您實際的陣列和佇列 IDs。將 *REGION* 取代為您的 AWS 區域 (例如 us-west-2)。

使用 AWS CodeCommit 搭配佇列登入資料

設定完成後，Git 操作會在存取 AWS CodeCommit 儲存庫時自動使用佇列角色登入資料。deadline
queue export-credentials 命令會傳回如下所示的臨時登入資料：

```
{  
  "Version": 1,  
  "AccessKeyId": "ASIA...",  
  "SecretAccessKey": "...",  
  "SessionToken": "...",  
  "Expiration": "2025-11-10T23:02:23+00:00"  
}
```

這些登入資料會視需要自動重新整理，Git 操作將順暢運作：

```
git clone https://git-codecommit.REGION.amazonaws.com/v1/repos/PROJECT_REPOSITORY  
git pull  
git push
```

藝術家現在可以使用其佇列許可存取專案儲存庫，而不需要個別的 AWS CodeCommit 登入資料。只有
具有特定佇列存取權的使用者才能存取相關聯的儲存庫，透過截止日期雲端的佇列成員資格系統啟用精
細存取控制。

對 AWS 截止日期雲端身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用截止日期雲端和 IAM 時可能遇到的常見問題。

主題

- [我無權在截止日期雲端中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要允許以外的人員 AWS 帳戶 存取我的截止日期雲端資源](#)

我無權在截止日期雲端中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 deadline:*GetWidget* 許可時發生。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 deadline:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole 動作，您的政策必須更新，以允許您將角色傳遞至截止日期雲端。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM marymajor 使用者嘗試使用主控台在截止日期雲端中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許以外的人員 AWS 帳戶 存取我的截止日期雲端資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解截止日期雲端是否支援這些功能，請參閱 [Deadline Cloud 如何與 IAM 搭配使用](#)。

- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 [《IAM 使用者指南》中的在您的 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 [《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 [《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

的合規驗證 Deadline Cloud

若要了解 是否 AWS 服務 在特定合規計劃範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

中的彈性 Deadline Cloud

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。AWS 區域 提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

AWS Deadline Cloud 不會備份存放在任務附件 S3 儲存貯體中的資料。您可以使用任何標準 Amazon S3 備份機制來啟用任務附件資料的備份，例如 [S3 版本控制](#)或 [AWS Backup](#)。

截止日期雲端中的基礎設施安全性

做為受管服務，AWS 截止日期雲端受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取截止日期雲端。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

截止日期雲端不支援使用 AWS PrivateLink 虛擬私有雲端 (VPC) 端點政策。它使用 AWS PrivateLink 預設政策，授予端點的完整存取權。如需詳細資訊，請參閱AWS PrivateLink 《使用者指南》中的[預設端點政策](#)。

截止日期雲端中的組態和漏洞分析

AWS 處理基本安全任務，例如訪客作業系統 (OS) 和資料庫修補、防火牆組態和災難復原。這些程序已由適當的第三方進行檢閱並認證。如需詳細資訊，請參閱以下資源：

- [共同的責任模型](#)
- [Amazon Web Services : 安全程序概觀](#) (白皮書)

AWS Deadline Cloud 會管理服務受管或客戶受管機群上的任務：

- 對於服務受管機群，Deadline Cloud 會管理訪客作業系統。
- 對於客戶受管機群，您需負責管理作業系統。

如需 Deadline Cloud AWS 組態和漏洞分析的其他資訊，請參閱

- [截止日期雲端的安全最佳實務](#)

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況，AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源政策中使用 [aws:SourceArn](#) 和 [aws:SourceAccount](#) 全域條件內容索引鍵，以限制將另一個服務 AWS Deadline Cloud 提供給資源的許可。如果您想要僅允許一個資源與跨服務存取相關

聯，則請使用 `aws:SourceArn`。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 `aws:SourceAccount`。

防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，其中包含資源的完整 Amazon Resource Name (ARN)。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 `arn:aws:deadline:*:123456789012:*`。

如果 `aws:SourceArn` 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

下列範例示範如何在 中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵 `Deadline Cloud`，以防止混淆代理人問題。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "deadline.amazonaws.com"
      },
      "Action": "deadline:CreateFarm",
      "Resource": [
        "*"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:deadline:*:111122223333:*"
        },
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

AWS Deadline Cloud 使用界面端點存取 (AWS PrivateLink)

您可以使用在 VPC 與之間 AWS PrivateLink 建立私有連線 AWS Deadline Cloud。您可以 Deadline Cloud 像在 VPC 中一樣存取，無需使用網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 Deadline Cloud。

您可以建立由 AWS PrivateLink 提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可作為目的地為 Deadline Cloud 之流量的進入點。

Deadline Cloud 也提供雙堆疊端點。雙堆疊端點支援透過 IPv6 和 IPv4 的請求。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「[透過 AWS PrivateLink 存取 AWS 服務](#)」。

的考量事項 Deadline Cloud

設定介面端點之前 Deadline Cloud，請參閱《AWS PrivateLink 指南》中的[使用介面 VPC 端點存取 AWS 服務](#)。

Deadline Cloud 支援透過介面端點呼叫其所有 API 動作。

根據預設，Deadline Cloud 允許透過介面端點完整存取。或者，您可以將安全群組與端點網路介面建立關聯，以控制 Deadline Cloud 透過介面端點傳入的流量。

Deadline Cloud 也支援 VPC 端點政策。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[使用端點政策控制 VPC 端點的存取](#)。

Deadline Cloud 端點

Deadline Cloud 使用四個端點來存取服務 AWS PrivateLink - 兩個用於 IPv4，兩個用於 IPv6。

工作者使用 `scheduling.deadline.region.amazonaws.com` 端點從佇列取得任務、向回報進度 Deadline Cloud，以及將任務輸出傳回。如果您使用客戶受管機群，除非您使用管理操作，否則排程端點是唯一需要建立的端點。例如，如果任務建立更多任務，您需要啟用管理端點以呼叫 `CreateJob` 操作。

Deadline Cloud 監視器會使用 `management.deadline.region.amazonaws.com` 來管理陣列中的資源，例如建立和修改佇列和機群，或取得任務、步驟和任務的清單。

AWS SDKs 和 CLI 會自動將 `management` 和 `scheduling` 首新增至端點。如果您想要停用此行為，請參閱 AWS SDKs 和工具參考指南中的[主機字首注入](#)一節。

Deadline Cloud 也需要下列 AWS 服務端點的端點：

- Deadline Cloud 使用 AWS STS 來驗證工作者，以便他們可以存取任務資產。如需詳細資訊 AWS STS，請參閱AWS Identity and Access Management 《使用者指南》中的 [IAM 中的暫時安全登入資料](#)。
- 如果您在沒有網際網路連線的子網路中設定客戶受管機群，則必須為 Amazon CloudWatch Logs 建立 VPC 端點，以便工作者可以寫入日誌。如需詳細資訊，請參閱[使用 CloudWatch 監控](#)。
- 如果您使用任務附件，則必須為 Amazon Simple Storage Service (Amazon S3) 建立 VPC 端點，以便工作者可以存取附件。如需詳細資訊，請參閱 [中的任務附件 Deadline Cloud](#)。

建立的端點 Deadline Cloud

您可以使用 Amazon VPC Deadline Cloud 主控台或 AWS Command Line Interface () 建立的介面端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「[建立介面端點](#)」。

Deadline Cloud 使用下列服務名稱建立的 管理和排程端點。將##取代為您已部署 AWS 區域的 Deadline Cloud。

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

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

Deadline Cloud 支援雙堆疊端點。

如果您為介面端點啟用私有 DNS，您可以使用 Deadline Cloud 其預設的區域 DNS 名稱向 提出 API 請求。例如，`scheduling.deadline.us-east-1.amazonaws.com`用於工作者操作，或`management.deadline.us-east-1.amazonaws.com`用於所有其他操作。

您還必須使用 AWS STS 下列服務名稱建立的端點：

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

如果您的客戶受管機群位於沒有網際網路連線的子網路上，您必須使用下列服務名稱建立 CloudWatch Logs 端點：

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

如果您使用任務附件傳輸檔案，則必須使用以下服務名稱建立 Amazon S3 端點：

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

受限的網路環境

Deadline Cloud 提供藝術家或其他使用者在其本機工作站上使用的工具。這些工具需要存取 AWS API 和 Web 端點才能執行其功能。如果您使用 Web 內容篩選解決方案篩選特定 AWS 網域或 URL 端點的存取權，例如新一代防火牆 (NGFW) 或安全 Web Gateway (SWG)，則必須將下列網域或 URL 端點新增至 Web 內容篩選解決方案允許清單。

AWS 要允許清單的 API 端點

截止日期雲端用戶端工具，例如 AWS 管理主控台、監視器、CLI 和整合式提交者，除了截止日期雲端之外，還需要存取 AWS APIs。這些端點僅支援 IPv4。

- `scheduling.deadline.[Region].amazonaws.com`
- `management.deadline.[Region].amazonaws.com`
- `logs.[Region].amazonaws.com`
- `ec2.[Region].amazonaws.com`
- `s3.[Region].amazonaws.com`
- `sts.[Region].amazonaws.com`
- `identitystore.[Region].amazonaws.com`

要允許清單的 Web 網域

Deadline Cloud Monitor 需要存取下列網域才能操作。

如需允許列出 AWS 登入網域的詳細資訊，請參閱 AWS 《登入使用者指南》中的[要新增至允許清單的網域](#)。

- `downloads.deadlinecloud.amazonaws.com`
- `d2ev1rdnjzhmnr.cloudfront.net`
- `prod.log.shortbread.aws.dev`

- prod.tools.shortbread.aws.dev
- prod.log.shortbread.analytics.console.aws.a2z.com
- prod.tools.shortbread.analytics.console.aws.a2z.com
- global.help-panel.docs.aws.a2z.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- sso.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.amazonaws.com
- oidc.*[Region]*.amazonaws.com
- assets.sso-portal.*[Region]*.amazonaws.com

截止日期雲端提交者需要存取下列網域，才能下載 GUI 相依性。

- pypi.python.org
- pypi.org
- pythonhosted.org
- files.pythonhosted.org

要允許清單的環境特定端點

這些網域會根據截止日期雲端的特定組態而有所不同。如果建立其他截止日期雲端監視器或佇列，則需要允許列出其他網域。

- *[Directory ID or alias]*.awsapps.com

此網域繫結至 IAM Identity Center 設定，且此中的所有設定應使用相同的 IAM Identity Center 執行個體。您可以在設定 → AWS 存取入口網站 URL 下的 IAM Identity Center 主控台中找到確切的值。

- *[Monitor alias]*.*[Region]*.deadlinecloud.amazonaws.com

此網域適用於截止日期雲端中的監控設定。藝術家在其瀏覽器或截止日期雲端監控應用程式中輸入此連結。如果未來在其他帳戶或區域中設定截止日期雲端，此網域將會變更。您可以在儀表板 → 監控概觀 → 監控詳細資訊 → URL 的截止日期雲端主控台中找到此值。

- *[Bucket name]*.*[Region]*.s3.amazonaws.com

這是截止日期雲端佇列所使用的任務附件儲存貯體網域。每個佇列都可以設定自己的任務附件儲存貯體。您可以在 佇列 → 佇列詳細資訊 → 任務附件下的截止日期雲端主控台中找到確切的儲存貯體名稱。如需任務附件的詳細資訊，請參閱佇列文件。

截止日期雲端的安全最佳實務

AWS Deadline Cloud (Deadline Cloud) 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

Note

如需許多安全主題重要性的詳細資訊，請參閱[共同責任模型](#)。

資料保護

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS Identity and Access Management (IAM) 設定個別帳戶。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制 AWS 服務。
- 使用進階受管安全服務，例如 Amazon Macie，可協助探索和保護存放在 Amazon Simple Storage Service (Amazon S3) 中的個人資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需 FIPS 和 FIPS 端點的詳細資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

我們強烈建議您絕對不要將客戶帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如名稱欄位。此建議包括當您使用 AWS Deadline Cloud 或使用主控台、API AWS CLI 或其他 AWS 服務 時 AWS SDKs。您在截止日期雲端或其他服務中輸入的任何資料都可能被挑選納入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含登入資料資訊。

AWS Identity and Access Management 許可

使用使用者、AWS Identity and Access Management (IAM) 角色，以及將最低權限授予使用者，來管理對 AWS 資源的存取。建立憑證管理政策和程序，以建立、分發、輪換和撤銷 AWS 存取憑證。如需詳細資訊，請參 [《IAM 使用者指南》](#) 中的 IAM 最佳實務。

以使用者和群組身分執行任務

在截止日期雲端中使用佇列功能時，最佳實務是指定作業系統 (OS) 使用者及其主要群組，以便作業系統使用者具有佇列任務的最低權限許可。

當您指定「以使用者身分執行」（和群組）時，提交至佇列之任務的任何程序都會使用該作業系統使用者執行，並繼承該使用者的相關聯作業系統許可。

機群和佇列組態結合以建立安全狀態。在佇列端，「以使用者身分執行任務」和 IAM 角色可指定為使用佇列任務的作業系統和 AWS 許可。機群定義基礎設施（工作者主機、網路、掛載的共用儲存體），當與特定佇列相關聯時，會在佇列中執行任務。工作者主機上可用的資料需要由一或多個相關聯佇列中的任務存取。指定使用者或群組有助於保護任務中的資料不受其他佇列、其他已安裝的軟體或其他可存取工作者主機的使用者影響。當佇列沒有使用者時，它會以代理程式使用者身分執行，其可以模擬 (sudo) 任何佇列使用者。如此一來，沒有使用者的佇列就可以將權限提升到另一個佇列。

聯網

為了防止流量遭到攔截或重新導向，請務必保護網路流量的路由方式和位置。

建議您以下列方式保護您的聯網環境：

- 保護 Amazon Virtual Private Cloud (Amazon VPC) 子網路路由表，以控制 IP 層流量的路由方式。
- 如果您在陣列或工作站設定中使用 Amazon Route 53 (Route 53) 做為 DNS 供應商，請安全存取 Route 53 API。
- 如果您使用內部部署工作站或其他資料中心連線到 AWS 以外的 Deadline Cloud，請保護任何內部部署聯網基礎設施。這包括路由器、交換器和其他聯網裝置上的 DNS 伺服器路由表。

任務和任務資料

截止日期 雲端任務會在工作者主機的工作階段中執行。每個工作階段都會在工作者主機上執行一或多個程序，這通常會要求您輸入資料才能產生輸出。

若要保護此資料，您可以使用佇列設定作業系統使用者。工作者代理程式會使用佇列作業系統使用者來執行工作階段子程序。這些子程序會繼承佇列作業系統使用者的許可。

我們建議您遵循最佳實務，以安全存取這些子程序存取的資料。如需詳細資訊，請參閱[共同責任模式](#)。

陣列結構

您可以透過多種方式安排截止日期雲端機群和佇列。不過，某些安排會帶來安全性影響。

一個陣列具有最安全的界限之一，因為它無法與其他陣列共用截止日期雲端資源，包括機群、佇列和儲存設定檔。不過，您可以在陣列中共用外部 AWS 資源，這會危及安全界限。

您也可以使用適當的組態，在相同陣列內的佇列之間建立安全界限。

請遵循下列最佳實務，在相同的陣列中建立安全佇列：

- 僅將機群與相同安全界限內的佇列建立關聯。注意下列事項：
 - 在工作者主機上執行任務後，資料可能會保留在後面，例如暫存目錄或佇列使用者的主目錄中。
 - 無論您提交任務的目標佇列為何，相同的作業系統使用者都會在服務擁有的機群工作者主機上執行所有任務。
 - 任務可能會讓程序在工作者主機上執行，讓來自其他佇列的任務能夠觀察其他執行中的程序。
- 確保只有相同安全界限內的佇列才能共用任務附件的 Amazon S3 儲存貯體。
- 確保只有相同安全界限內的佇列才能共用作業系統使用者。
- 將任何其他整合到陣列 AWS 的資源保護到邊界。

任務連接佇列

任務附件與使用 Amazon S3 儲存貯體的佇列相關聯。

- 寫入 Amazon S3 儲存貯體中根字首並從中讀取的任務附件。您可以在 `CreateQueue` API 呼叫中指定此根字首。
- 儲存貯體具有對應的 `Queue Role`，指定授予佇列使用者存取儲存貯體和根字首的角色。建立佇列時，您可以指定 `Queue Role Amazon Resource Name (ARN)` 以及任務附件儲存貯體和根字首。
- 對 `AssumeQueueRoleForRead`、`AssumeQueueRoleForUser` 和 `AssumeQueueRoleForWorker` API 操作的授權呼叫會傳回一組的臨時安全登入資料 `Queue Role`。

如果您建立佇列並重複使用 Amazon S3 儲存貯體和根字首，則會有向未經授權方公開資訊的風險。例如，QueueA 和 QueueB 共用相同的儲存貯體和根字首。在安全工作流程中，ArtistA 可以存取 QueueA，但無法存取 QueueB。不過，當多個佇列共用儲存貯體時，ArtistA 可以存取 QueueB 資料中的資料，因為它使用與 QueueA 相同的儲存貯體和根字首。

主控台預設會設定安全的佇列。確保佇列具有 Amazon S3 儲存貯體和根字首的不同組合，除非它們是常見安全界限的一部分。

若要隔離佇列，您必須 Queue Role 將設定為僅允許佇列存取儲存貯體和根字首。在下列範例中，將每個####取代為您的資源特定資訊。

JSON

```
{
  "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": "111122223333"
        }
      }
    },
    {
      "Action": [
        "logs:GetLogEvents"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/
deadline/FARM_ID/*"
    }
  ]
}
```

```
    }  
  ]  
}
```

您也必須在角色上設定信任政策。在下列範例中，將####文字取代為您的資源特定資訊。

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": [  
        "sts:AssumeRole"  
      ],  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "deadline.amazonaws.com"  
      },  
      "Condition": {  
        "StringEquals": {  
          "aws:SourceAccount": "111122223333"  
        },  
        "ArnEquals": {  
          "aws:SourceArn": "arn:aws:deadline:us-  
east-1:111122223333:farm/FARM_ID"  
        }  
      }  
    },  
    {  
      "Action": [  
        "sts:AssumeRole"  
      ],  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "credentials.deadline.amazonaws.com"  
      },  
      "Condition": {  
        "StringEquals": {  
          "aws:SourceAccount": "111122223333"  
        },  
        "ArnEquals": {
```

```

        "aws:SourceArn": "arn:aws:deadline:us-
east-1:111122223333:farm/FARM_ID"
    }
}
]
}

```

自訂軟體 Amazon S3 儲存貯體

您可以將下列陳述式新增至 `Queue Role` 以存取 Amazon S3 儲存貯體中的自訂軟體。在下列範例中，將 `Software_BUCKET_NAME` 取代為 S3 儲存貯體的名稱，並將 `BUCKET_ACCOUNT_OWNER` 取代為擁有儲存貯體的 AWS 帳戶 ID。

```

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

```

如需 Amazon S3 安全最佳實務的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》](#) 中的 [Amazon S3 安全最佳實務](#)。

工作者主機

保護工作者主機，以協助確保每個使用者只能對其指派的角色執行操作。

我們建議採用下列最佳實務來保護工作者主機：

- 使用主機組態指令碼可以變更工作者的安全性和操作。不正確的組態可能會導致工作者不穩定或停止運作。您需負責偵錯此類失敗。
- 除非提交到這些佇列的任務位於相同的安全界限內，否則請勿對多個佇列使用相同的 `jobRunAsUser` 值。
- 請勿將佇列設定為工作者代理程式執行時所使用的 `jobRunAsUser` 作業系統使用者名稱。
- 授予佇列使用者預期佇列工作負載所需的最低權限作業系統許可。確保他們沒有工作代理程式檔案或其他共用軟體的檔案系統寫入許可。
- 確保只有 上的根使用者 Linux 和 Administrator 擁有 Windows 自己的帳戶，並且可以修改工作者代理程式檔案。
- 在 Linux 工作者主機上，請考慮在 中設定 `umask` 覆寫 `/etc/sudoers`，以允許工作者代理程式使用者以佇列使用者身分啟動程序。此組態有助於確保其他使用者無法存取寫入佇列的檔案。
- 授予受信任的個人對工作者主機的最低權限存取權。
- 將許可限制為本機 DNS 覆寫組態檔案 (`/etc/hosts` 上的 Linux 和 `C:\Windows\system32\etc\hosts` 上的 Windows)，以及在工作站和工作者主機作業系統上路由資料表。
- 限制對工作站和工作者主機作業系統上 DNS 組態的許可。
- 定期修補作業系統和所有已安裝的軟體。此方法包括專門與截止日期雲端搭配使用的軟體，例如提交者、轉接器、工作者代理程式、OpenJD 套件等。
- 針對 Windows 佇列 使用強式密碼 `jobRunAsUser`。
- 定期輪換佇列 的密碼 `jobRunAsUser`。
- 確保最低權限存取 Windows 密碼秘密，並刪除未使用的秘密。
- 請勿給予佇列未來執行的排程命令 `jobRunAsUser` 許可：
 - 在 上 Linux，拒絕這些帳戶存取 `cron` 和 `at`。
 - 在 上 Windows，拒絕這些帳戶存取 Windows 任務排程器。

Note

如需定期修補作業系統和已安裝軟體之重要性的詳細資訊，請參閱 [共同責任模型](#)。

主機組態指令碼

- 使用主機組態指令碼可以變更工作者的安全性和操作。不正確的組態可能會導致工作者不穩定或停止運作。您需負責偵錯此類失敗。

工作站

請務必保護可存取截止日期雲端的工作站。此方法有助於確保您提交至 Deadline Cloud 的任何任務都無法執行向您的計費的任意工作負載 AWS 帳戶。

我們建議採用下列最佳實務來保護藝術家工作站。如需詳細資訊，請參閱 [共同責任模型](#)。

- 保護任何提供存取權的持久憑證 AWS，包括截止日期雲端。如需詳細資訊，請參閱《IAM 使用者指南》中的[管理 IAM 使用者的存取金鑰](#)。
- 僅安裝受信任且安全的軟體。
- 要求使用者與身分提供者聯合，以 AWS 使用臨時憑證存取。
- 在截止日期雲端提交者程式檔案上使用安全許可，以防止竄改。
- 授予受信任的個人對藝術家工作站的最低權限存取權。
- 僅使用您透過截止日期雲端監視器取得的提交者和轉接器。
- 限制本機 DNS 覆寫組態檔案的許可 (/etc/hosts Linux 和 上的 macOS，以及 C:\Windows\system32\etc\hosts 上的 Windows)，以及在工作站和工作者主機作業系統上路由資料表。
- 限制對工作站和工作者主機作業系統/etc/resolve.conf 的許可。
- 定期修補作業系統和所有已安裝的軟體。此方法包括專門與截止日期雲端搭配使用的軟體，例如提交者、轉接器、工作者代理程式、OpenJD 套件等。

驗證下載軟體的真實性

在下載安裝程式後驗證軟體的真實性，以防止檔案遭到竄改。此程序適用於 Windows 和 Linux 系統。

Windows

若要驗證下載檔案的真實性，請完成下列步驟。

1. 在下列命令中，將 *file* 取代為您要驗證的檔案。例如 **C:\PATH\TO\MY \DeadlineCloudSubmitter-windows-x64-installer.exe**。此外，請將取代 *signtool-sdk-version* 為已安裝的 SignTool SDK 版本。例如 **10.0.22000.0**。

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

2. 例如，您可以執行下列命令來驗證截止日期雲端提交者安裝程式檔案：

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

Linux

若要驗證下載檔案的真實性，請使用gpg命令列工具。

1. 執行下列命令來匯入OpenPGP金鑰：

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

mQINBG1ANDUBEACg6zffjN43gqe5ryPhk+wQM10rEdvmItw4WPWaVsN+/at/OIJw
MGCagSYXcgR+jKbsHQ0QoEQdo5SrxHjpkTEs3KQhGvf+ehrU1Ac7koXKIBWtes+
BI9F0s1RECz0nXT0y/cd/90RXjpF07mreTLIKNIbybULfad82nYykpITjFr5XRGj
/shYkucxRQZdwkgkIYyV25pPICPd2RsX+Zua85jV8mCqVffDFRXvgcPe3+ofClj/
2CE8UfUIq08Csu4YEKsqR3aeoT0EFT4kuQR5nFXVzor0EkQt03gB35KNWKM1IOU
2vA+wyoL7nWSii4yfYtW3EZ+3gq6HxvnT9Zs8MC53uT0i0damASXecYREwGmY/io
6n5XTEA/35LNb14A756vSTZ7h4VFJAN5BpuqxstI1D7ou94skoSmcPoC/iniTvY9
kZy1U50CH/nifMAHM2a5jrQe180cW4oko9eyc8ENQpSy15JE1F0Kff7D/4tcZJLF
F0VBTXbhfvq3dPfoq94Iwt7p540vwj0S//CEu3jZYbN12QC/3YiHE2H2XyGCQbq6
2MjcuxLnEapoRIqfbi8GPtCWVPzm28WGyKIDofWICczzeJFFJnvzrY3wRG64ibKJ
bR/uedwua1UuiC482V1FD5ffmzSSs8ktTp9hgj7RGDX1c9NTcF1jHxG9hwARAQAB
tCxBV1MgRGVhZGxpbnUgQ2xvdWQgPGF3cy1kZWFKbGluZUBhbWF6b24uY29tPokC
VwQTAQgAQRyhbBmXj7So2csyehiIYsg71N18bhtjBQJpQDQ1AhsVBQkDwmcABQsJ
CAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAOJEMg71N18bhtjk2UP/3h4K1EzZ0/7
BxRmkbixuo1Quq0GvA6tXbSWaM8QH5jglcvL12PZLALk1LT4v82uCsLR11F8/Tch
cC10SZE0FIS+XxAaw1Xfai6jlyLhab0wKF2ylq5eJ1Lcw11h2nAArDRb4fLD0m1g
Dfquetq/XEpyXp0SkWxGRV4R1UdjQfytxrncUnsT5/fk5f9VDdblu6K/1EmwfyYjB
lXv0uUCkqPot0Smbv0h3PY3Hi3n54ncy8NfTeV+TUvSe3C1s1zN18aqHoTxJB/eU
kp+LFZ9m+igpSYnKeg1KnytylH3KGCjThglT/QXnI1wNTqmj1kFBVwtt/y1mtnA+
CPIUHP1CtbKsHaLtp411Bm5TVtPN/Wqqicn5QL14khg7R4K+V2aaA4ubY6p1tG9
0fFhN5tTnHDSKWMfmb83wfh5Zkcg85c3egjoit+wgQRAQVqbznx7NqAHs9VoDIu
SPcAr+C329A0Bzod4gyNGH7Ah5DkMITo404+axnAU9yhFOHcMjMtiask/fNg1Aum
OqYPMUwcv1GZjLaTJyfGGC1xALsYR0KHnwIehD06MHR/Z98bGkcV8+Y0q8UPsd1
VN1fc1rjCJh/AT3w6owvG4DaEwspseSjzHv16mW4e2N6Uu23SPzgQsJ5qYN2g8D+
P7N9LGDfP8DaYc5JM9mlyFmYI2Q94ufl
=rY5l
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

2. 決定是否信任OpenPGP金鑰。決定是否信任上述金鑰時需要考慮的一些因素包括：
 - 您用來從此網站取得 GPG 金鑰的網際網路連線是安全的。
 - 您在上存取此網站的裝置是安全的。
 - AWS 已採取措施來保護此網站上的OpenPGP公有金鑰託管。
3. 如果您決定信任OpenPGP金鑰，請編輯金鑰以信任，gpg類似下列範例：

```
$ 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. 驗證截止日期雲端提交者安裝程式

若要驗證截止日期雲端提交者安裝程式，請完成下列步驟：

- a. 下載截止日期雲端提交者安裝程式的簽章檔案。

[下載簽章檔案 \(.sig\)](#)

- b. 執行下列動作來驗證截止日期雲端提交者安裝程式的簽章：

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

5. 驗證截止日期雲端監視器

Note

您可以使用簽章檔案或平台特定方法，驗證截止日期雲端監視器下載。如需平台特定的方法，請參閱 [Linux \(Debian\) 標籤](#)、[Linux\(RPM\) 標籤](#)，或根據您下載的檔案類型的 [Linux \(ApplImage\) 標籤](#)。

若要使用簽章檔案驗證截止日期雲端監控桌面應用程式，請完成下列步驟：

- a. 為您的截止日期雲端監視器安裝程式下載對應的簽章檔案：

- [下載 .deb 簽章檔案](#)
- [下載 .rpm 簽章檔案](#)
- [下載 .ApplImage 簽章檔案](#)

- b. 驗證簽章：

對於 .deb：

```
gpg --verify ./deadline-cloud-monitor_amd64.deb.sig ./deadline-cloud-
monitor_amd64.deb
```

對於 .rpm：

```
gpg --verify ./deadline-cloud-monitor.x86_64.rpm.sig ./deadline-cloud-monitor.x86_64.rpm
```

對於 .AppImage :

```
gpg --verify ./deadline-cloud-monitor_amd64.AppImage.sig ./deadline-cloud-monitor_amd64.AppImage
```

c. 確認輸出看起來類似以下內容：

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

```
gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

如果輸出包含片語 Good signature from "AWS Deadline Cloud"，表示簽章已成功驗證，您可以執行截止日期雲端監視器安裝指令碼。

歷史金鑰

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQINBGX6GQsBEADduUtJgqSXI+q7606fsFwEYKmbnlyL0xKv1q32EZuyv0otZo5L  
le4m5Gg52AzrvPvDiUTLooAlvYeozaYyirIGsK08Ydz0Ftdjroiuh/mw9JSJDJRI  
rnRn5yKet1JFzjkjopA3pjsTBP6lW/mb1bDBDEwwwtH0x91V7A03FJ9T7Uzu/qSh  
q0/UYdkafro3cPASvkkqgDt2tCvURfBcUCAjZVFcLZcVD5iwXacxvKsxxS/e7kuVV  
I1+VGT8Hj8XzWYhjCZx0LZk/fvpYPMYEEujN0fYUp6RtMIXve0C9awwMCy5nBG2J  
eE2015DsCpTaBd4Fdr3LWcSs8JFA/YfP9auL3Ncz0ozPoVJt+fw8CB1VIX00J715  
hvHDjcC+5v0wxqA1MG6+f/SX7CT8FXK+L3i0J5gBYUNXqHSxUdv8kt76/KVmQa1B  
Ak1+MPKpMq+1hw++S3G/1XqwWaDNQbRRw7dSZHymQVXvPp1nscq3hV7K10M+6s6g  
1g4mvFY41f6DhptwZLWYQXU8rBQpojvQfiSmDFrFPWF15BexesuVnkGIo1Qok1Kx  
AVUSdJPVEJCteyy7td4FPhBaSqT5vW3+ANbr9b/uoRYWJvn17dN0cc9HuRh/Ai+I  
nkfECo2WUDLZ0fEKGjGyFX+todWvJXjvc5kmE9Ty5vJp+M9Vvb8jd6t+mwARAQAB  
tCxBV1MgRGVhZGxpbnUgQ2xvdWQgPGF3cy1kZWFKbGluZUBhbWF6b24uY29tPokC  
VwQTAQgAQRyhbLhAwIwpqQeWoHH6pfbNP0a3bzzvBQJ1+hkLAXsvBAUJA8JnAAUL  
CQgHAgIiAgYVCgkICwIDFgIBAh4HAheAAAoJEPbNP0a3bzzvKswQAJXzKSAY8sY8  
F6Eas2oYwIDDDuirs8FiEnFghjUE06MTt9AykF/jw+CQg2UzFtEy0bHBymhgmhXE  
3buVeom96tgM3ZDfZu+sxi5pGX6oAQnZ6riztN+VpkipQmLgwtMGpSML13KLwnv2k  
WK8mrR/fPMkfaewB7A6RIUYiW33GAL4KfMIIs8/vIwIJw99NxHpZQVoU6dFpuDtE  
10uxGcCqGJ7mAmo6H/YawSNp2Ns80gyqIKYo7o3LJ+WRroIR1Qyctq8gnR9JvYXX  
42ASqLq5+0XKo4qh81b1XKYqtc176BbbSNFjWnzIQgKDgNiHFZCdc0VgqDhw015r
```

```
NICbqqwNLj/Fr2kecYx180Ktp10j00w5I0yh3bf3MVGWnYRdjvA1v+/CO+55N4g
z0kf50Lcdu5RtqV10XBCifn28pecqPaSdYcssYSR15DLiFktGbNzTGcZZwITTKQc
af8PPdTGtnnb6P+cdbW3bt9MVtN5/dgSHLThnS8MPEuNCtkTnpXshuVuBGgwBMdb
qUC+HjqvhZzbwns8dr5WI+6HWNBFgGANn6ageY158vVp0UkuNP8wcWjRARciHXZx
ku6W2jPTHDWGNrBQ02Fx7fd2QYJheIPPAShHcfJ0+xgWCof45D0vAxAJ8gGg9Eq+
gFWhsx4NSHn2gh1gDZ410u/4exJ1lwPM
=uVaX
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

Linux (AppImage)

若要驗證使用 Linux .AppImage 二進位檔的套件，請先完成Linux索引標籤中的步驟 1-3，然後完成下列步驟。

1. 從 GitHub 的 AppImageUpdate [頁面](#)，下載 validate-x86_64.AppImage 檔案。
2. 下載檔案後，若要新增執行許可，請執行下列命令。

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

3. 若要新增執行許可，請執行下列命令。

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

4. 若要驗證截止日期雲端監視器簽章，請執行下列命令。

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

如果輸出包含片語 Validation successful，表示簽章已成功驗證，而且您可以安全地執行截止日期雲端監視器安裝指令碼。

Linux (Debian)

若要驗證使用 Linux .deb 二進位檔的套件，請先完成 Linux 標籤中的步驟 1-3。

dpkg 是大多數debian以為基礎的Linux分佈中的核心套件管理工具。您可以使用 工具驗證 .deb 檔案。

1. 下載截止日期雲端監視器 .deb 檔案：

[下載截止日期雲端監視器 \(.deb\)](#)

2. 驗證 .deb 檔案：

```
dpkg-sig --verify deadline-cloud-monitor_amd64.deb
```

3. 輸出將類似於：

```
Processing deadline-cloud-monitor_amd64.deb...  
GOODSIG _gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
```

4. 若要驗證 .deb 檔案，請確認 GOODSIG 存在於輸出中。

Linux (RPM)

若要驗證使用 Linux .rpm 二進位檔的套件，請先完成Linux標籤中的步驟 1-3。

1. 下載截止日期雲端監視器 .rpm 檔案：

[下載截止日期雲端監視器 \(.rpm\)](#)

2. 驗證 .rpm 檔案：

```
gpg --export --armor "Deadline Cloud" > key.pub  
sudo rpm --import key.pub  
rpm -K deadline-cloud-monitor.x86_64.rpm
```

3. 輸出將類似於：

```
deadline-cloud-monitor.x86_64.rpm: digests signatures OK
```

4. 若要驗證 .rpm 檔案，請確認 digests signatures OK 位於輸出中。

監控 AWS 截止日期雲端

監控是維護截止日期雲端（截止日期雲端）AWS 和您 AWS 解決方案的可靠性、可用性和效能的重要部分。從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。開始監控截止日期雲端之前，您應該建立監控計畫，其中包含下列問題的答案：

- 監控目標是什麼？
- 監控哪些資源？
- 監控這些資源的頻率為何？
- 將使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

AWS 和 截止日期雲端提供工具，可讓您用來監控資源並回應潛在事件。其中一些工具會為您執行監控，有些工具需要手動介入。您應該盡可能自動化監控任務。

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

期限雲端有三個 CloudWatch 指標。

- Amazon CloudWatch Logs 可讓您監控、存放和存取來自 Amazon EC2 執行個體、CloudTrail 及其他來源的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 [Amazon CloudWatch Logs 使用者指南](#)。
- Amazon EventBridge 可用來自動化您的 AWS 服務，並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時的方式交付至 EventBridge。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 [Amazon EventBridge 使用者指南](#)。
- AWS CloudTrail 會擷取由您的帳戶或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/>。

如需詳細資訊，請參閱截止日期雲端開發人員指南中的下列主題：

- [CloudTrail日誌](#)
- [使用 EventBridge 管理事件](#)
- [使用 CloudWatch 進行監控](#)

的配額 Deadline Cloud

AWS Deadline Cloud 提供可用於處理任務的資源，例如陣列、機群和佇列。當您建立時 AWS 帳戶，我們會為每個資源設定這些資源的預設配額 AWS 區域。

Service Quotas 是一個集中位置，您可以在其中檢視和管理 的配額 AWS 服務。您也可以請求提高使用許多資源的配額。

若要檢視 的配額 Deadline Cloud，請開啟 [Service Quotas 主控台](#)。在導覽窗格中，選擇 AWS 服務並選取 Deadline Cloud。

若要請求提高配額，請參閱 [《Service Quotas 使用者指南》](#) 中的請求提高配額。如果 Service Quotas 中尚未提供配額，請使用 [服務配額增加表單](#)。

AWS 您的帳戶具有下列與 相關的配額 Deadline Cloud。

名稱	預設	可調整	Description
每個陣列的關聯成員	每個支援的區域： 75	否	可與目前 AWS 區域中的每個陣列相關聯的成員數目上限。
每個機群的關聯成員	每個支援的區域： 75	否	可與目前 AWS 區域中的每個機群相關聯的成員數量上限。
每個任務的關聯成員	每個支援的區域： 75	否	可與目前 AWS 區域中的每個任務相關聯的成員數目上限。
每個佇列的關聯成員	每個支援的區域： 75	否	可與目前 AWS 區域中的每個佇列相關聯的成員數目上限。
每個陣列的預算	每個受支援的區域： 20	<u>是</u>	目前 AWS 區域中每個陣列的預算數量上限

名稱	預設	可調整	Description
每個區域的陣列數	每個受支援的區域：2	是	可在目前 AWS 區域中建立的陣列數目上限。
每個陣列的機群數	每個受支援的區域：5	是	目前 AWS 區域中每個陣列可建立的機群數量上限。
每個陣列的任務	每個受支援的區域：100,000	是	目前 AWS 區域中每個陣列的任務數量上限。
每個區域的授權端點	每個受支援的區域：5	是	目前 AWS 區域中的授權端點數量上限。
每個授權端點的授權工作階段	每個受支援的區域：500	是	目前 AWS 區域中每個授權端點的授權工作階段數量上限。
每個陣列的限制	每個受支援的區域：50	是	目前 AWS 區域中每個陣列可建立的限制數目上限。
每個區域的監視器	每個受支援的區域：1	否	目前區域中的監視器數量上限 AWS 。
每個區域的 OnDemand G 執行個體 GPUs	每個受支援的區域：1	是	可在目前 AWS 區域中所有服務受管機群之間佈建的隨需 G 執行個體 GPUs 數量上限。
每個區域的 OnDemand vCPUs	每個受支援的區域：50	是	可在目前 AWS 區域中所有服務受管機群之間佈建的隨需 vCPUs 數量上限。

名稱	預設	可調整	Description
每個佇列的佇列環境	每個受支援的區域：10	否	目前 AWS 區域中每個佇列可建立的佇列環境數目上限。
每個陣列的佇列機群關聯	每個受支援的區域：100	<u>是</u>	目前 AWS 區域中每個陣列的佇列機群關聯數目上限
每個佇列的佇列限制關聯	每個受支援的區域：10	<u>是</u>	可與目前 AWS 區域中的每個佇列相關聯的限制數目上限。
每個陣列的佇列數	每個受支援的區域：20	<u>是</u>	目前 AWS 區域中每個陣列可建立的佇列數量上限。
每個機群的資源組態	每個受支援的區域：1	<u>是</u>	可新增至每個機群的 VPC Lattice 資源組態數目上限。
每個區域的 Spot G 執行個體 GPUs	每個受支援的區域：1	<u>是</u>	目前 AWS 區域中可跨所有服務受管機群佈建的 Spot G 執行個體 GPUs 數量上限。
每個區域的 Spot vCPUs	每個受支援的區域：500	<u>是</u>	目前 AWS 區域中可跨所有服務受管機群佈建的 Spot vCPUs 數量上限。
每個任務的步驟	每個受支援的區域：200	<u>是</u>	目前 AWS 區域中每個任務的步驟數目上限。

名稱	預設	可調整	Description
一般用途 SSD (gp3) 磁碟區的儲存體，以 TiB 為單位	每個受支援的區域：50	是	EBS 儲存體的彙總數量上限，以 TiB 為單位，可用於目前 AWS 區域中的所有機群。
每個陣列的儲存設定檔	每個受支援的區域：50	否	目前 AWS 區域中每個陣列可建立的儲存設定檔數目上限。
每個區塊的任務	每個受支援的區域：150	否	提交任務時可合併為單一區塊的任務數量上限。
每個任務的任務	每個受支援的區域：10,000	是	目前 AWS 區域中每個任務的任務數量上限。
每個步驟的任務	每個受支援的區域：10,000	是	目前 AWS 區域中每個步驟的任務數量上限。
每個區域的Wait-and-save vCPUs	每個受支援的區域：50	是	可在目前 AWS 區域中所有服務受管機群之間佈建的wait-and-save vCPUs 數量上限。
每個陣列的工作者數	每個支援的區域：7,500	是	目前 AWS 區域中每個陣列的工作者數量上限。

使用 AWS 建立截止日期雲端資源 AWS CloudFormation

AWS Deadline Cloud 已與 整合 AWS CloudFormation，這項服務可協助您模型化和設定 AWS 資源，以減少建立和管理資源和基礎設施的時間。您可以建立範本來描述您想要的所有 AWS 資源（例如陣列、佇列和機群），並為您 CloudFormation 佈建和設定這些資源。

使用時 CloudFormation，您可以重複使用範本，以一致且重複地設定截止日期雲端資源。描述您的資源一次，然後在多個 AWS 帳戶和區域中逐一佈建相同的資源。

截止日期雲端和 CloudFormation 範本

若要佈建和設定截止日期雲端和相關服務的資源，您必須了解 [CloudFormation 範本](#)。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您要在 CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 CloudFormation 設計工具來協助您開始使用 CloudFormation 範本。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的 [什麼是 CloudFormation 設計器？](#)。

Deadline Cloud 支援在其中建立陣列、佇列和機群 CloudFormation。如需詳細資訊，包括陣列、佇列和機群的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation 《使用者指南》中的 [AWS 截止日期雲端](#)。

進一步了解 CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- [AWS CloudFormation](#)
- [AWS CloudFormation 使用者指南](#)
- [CloudFormation API 參考](#)
- [AWS CloudFormation 命令列界面使用者指南](#)

疑難排解

下列程序與秘訣可協助您針對 AWS 截止日期雲端陣列和資源的問題進行疑難排解。

主題

- [為什麼使用者看不到我的陣列、機群或佇列？](#)
- [為什麼工作者沒有挑選我的任務？](#)
- [為什麼我的工作停滯在執行中？](#)
- [對截止日期雲端任務進行故障診斷](#)
- [其他資源](#)

為什麼使用者看不到我的陣列、機群或佇列？

使用者存取

當您的使用者在截止日期雲端監視器中看不到您的陣列、機群或佇列時，他們存取您的陣列和資源可能會發生問題。

無法存取任何陣列的使用者會在截止日期雲端監視器中收到「沒有可用的陣列」訊息。

若要確認您已將正確的使用者或群組指派給您的陣列、機群或佇列

1. 在 AWS 截止日期雲端主控台中，尋找您的陣列、機群或佇列，然後選擇存取管理。
2. 預設會選取群組索引標籤。如果您依建議群組指派許可，您的群組應該會顯示在清單中，並具有指派的存取層級。

如果群組不在清單中，請選擇新增群組以指派群組的許可。

3. 如果您要依使用者指派許可，請選取使用者索引標籤。您的使用者應該會顯示在清單中，並具有指派的存取層級。

如果您的使用者不在清單中，請選擇新增使用者以為使用者指派許可。

若要確認您已將使用者指派給您的 群組

1. 在 AWS 截止日期雲端主控台中，尋找您的陣列、機群或佇列，然後選擇存取管理。
2. 預設會選取群組索引標籤。選取群組名稱以檢視其成員。

3. 如果使用者未列在群組中，則必須新增使用者。

如果您使用的是預設身分設定，則可以直接將使用者新增至 Identity Center 主控台群組。如果您連線到外部身分提供者，例如 Okta 或 Google Workspace，您可以將使用者新增至身分提供者中的群組。

Note

有些外部身分提供者會將使用者而非群組同步至 Identity Center。在這種情況下，請考慮直接將許可指派給使用者，而不是依群組指派許可。

如需管理使用者存取截止日期雲端的詳細資訊，請參閱 [在截止日期雲端中管理使用者](#)。

為什麼工作者沒有挑選我的任務？

機群角色組態

有時，當工作者建立但未完成初始化且未開始處理任務時，這是因為機群角色未正確設定。

若要驗證是否發生這種情況，請檢查您的 CloudTrail 日誌是否有任何存取遭拒的錯誤。確認存取遭拒問題後，請前往您的機群，並將角色組態更新為正確的許可。如需詳細資訊，請參閱 Deadline Cloud 開發人員指南中的 [CloudTrail 日誌](#)。

為什麼我的工作停滯在執行中？

工作者停滯退出 OpenJD 環境

工作者可能會卡在長時間執行的 envExit 工作階段動作中。如果您使用覆寫 OpenJD 範本並設定環境結束動作逾時超過 5 分鐘的任務範本，可能會發生這種情況。Deadline Cloud Monitor 提供一些可見性，了解在這種情況下停滯的工作者，但需要針對關聯佇列中的可用工作交叉參考 RUNNING 工作者。

若要尋找停滯的工作者，請前往截止日期雲端監視器中的所有機群，並完成下列步驟：

1. 在工作者狀態欄中，尋找 RUNNING 工作者。
2. 從機群詳細資訊區段中，導覽至每個相關聯的佇列。
3. 在每個相關聯的佇列中，搜尋 RUNNING、READY 或 的任務 PENDING。如果所有關聯的佇列在這些狀態下沒有任何任務，則工作者正在執行環境結束。

若要停止工作者停滯在此狀態，請使用下列 AWS CLI 命令：

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

執行命令後，工作者代理程式會在程式結束時重新啟動。然後，工作者會回到線上，並從相關聯的佇列執行更多任務。如果佇列包含更多具有環境結束動作逾時超過 5 分鐘的任務，工作者將會再次停滯。如果發生這種情況，您將需要重複此程序，直到不再有工作者停滯離開為止。

若要避免此問題，請在使用任務範本時，將逾時選項設定為不超過 5 分鐘。

對截止日期雲端任務進行故障診斷

如需 AWS 在截止日期雲端中任務常見問題的相關資訊，請參閱下列主題。

為什麼建立我的任務失敗？

配額驗證

任務無法通過驗證檢查的一些可能原因包括：

- 任務範本未遵循 OpenJD 規格。
- 任務包含太多步驟。
- 任務包含太多任務總數。
- 發生內部服務錯誤，導致無法建立任務。

若要查看任務中步驟和任務數量上限的配額，請使用 Service Quotas 主控台。如需詳細資訊，請參閱的配額 [Deadline Cloud](#)。

CHUNK【INT】 任務參數錯誤

如果任務建立失敗並顯示下列錯誤訊息，您需要將TASK_CHUNKING延伸模組新增至任務範本。

```
The CHUNK[INT] task parameter requires the TASK_CHUNKING extension.
```

若要解決此問題，請將下列內容新增至您的任務範本：

```
extensions:  
  - TASK_CHUNKING
```

為什麼我的任務不相容？

任務與佇列不相容的常見原因包括：

- 沒有機群與提交任務的佇列相關聯。開啟截止日期雲端監視器，並檢查佇列是否有相關聯的機群。如需如何檢視佇列的詳細資訊，請參閱 [在截止日期雲端中檢視佇列和機群詳細資訊](#)。
- 任務的主機需求不符合任何與佇列相關聯的機群。若要檢查，請將任務範本中的 `hostRequirements` 項目與陣列中機群的組態進行比較。請確定其中一個機群符合主機需求。如需機群相容性的詳細資訊，請參閱 [判斷機群相容性](#)。若要檢視機群組態，請參閱 [在截止日期雲端中檢視佇列和機群詳細資訊](#)。

為什麼我的任務卡在 中？

您的任務似乎卡在 READY 狀態的可能原因包括：

- 與佇列相關聯的機群最大工作者計數設定為零。若要檢查，請參閱 [在截止日期雲端中檢視佇列和機群詳細資訊](#)。
- 佇列中有較高的優先順序任務。若要檢查，請參閱 [在截止日期雲端中檢視佇列和機群詳細資訊](#)。
- 對於客戶管理的機群，請檢查自動擴展組態。如需詳細資訊，請參閱《截止日期雲端開發人員指南》中的 [使用 Amazon EC2 Auto Scaling 群組建立機群基礎設施](#)。

為什麼我的任務失敗？

任務可能會因為許多原因而失敗。若要搜尋問題，請開啟截止日期雲端監視器，然後選擇失敗的任務。選擇失敗的任務，然後檢視任務的日誌。如需說明，請參閱 [在截止日期雲端中檢視工作階段和工作者日誌](#)。

- 如果您看到授權錯誤，或是因為軟體沒有有效的授權而取得浮水印，請確定工作者可以連線到所需的授權伺服器。如需詳細資訊，請參閱《截止日期雲端開發人員指南》中的 [將客戶受管機群連接至授權端點](#)。
- 最後一個工作階段動作訊息或程序結束碼可能會提供工作失敗原因的相關資訊。如果您使用的是 Windows 且您的結束代碼為負數，請嘗試搜尋未簽署版本的結束代碼：

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

為什麼我的步驟待定？

當一或多個相依性未完成時，步驟可能會保持在 PENDING 狀態。您可以使用截止日期雲端監視器檢查相依性的狀態。如需說明，請參閱[在截止日期雲端中檢視步驟](#)。

其他資源

您可以在 [GitHub](#) 上找到其他資訊和資源。

截止日期雲端版本備註

此頁面包含有關 AWS 截止日期雲端的最新版本和更新的資訊。

Date	Title	Description
2026-02-24	截止日期雲端文件現在包含支援的軟體使用者指南	截止日期雲端使用者指南現在包含每個支援應用程式的專用子頁面，提供有關版本相容性和功能支援的深入詳細資訊。
2026-02-24	截止日期 雲端監控用量總管現在支援依使用者分組用量	使用用量總管分析您團隊中每個使用者的用量模式和屬性成本。
2026-02-24	Deadline Cloud 現在支援任務區塊，以提高轉譯效率	AWS Deadline Cloud 現在支援任務區塊，可將多個影格分組為單一任務執行。此功能透過為每個區塊載入應用程式和場景一次，而不是每個影格一次，來減少額外負荷。您可以指定預設區塊大小，或讓 Deadline Cloud 根據目標執行時間動態調整區塊大小。
2026-02-19	Submitter Installer v2026-02-19 已發行	已發行新的提交者安裝程式，將 Autodesk Maya 提交者從 0.15.12 更新至 0.15.13 。
2026-02-13	OpenJD 規格現在包含用於 RFC 檢閱的 Claude 和 Kiro 技能	開放任務描述規格儲存庫現在包含一項 Kiro 技能，用於 AI 輔助檢閱 RFC 提案、檢查完整性、清晰度、原則一致性，以及與現有規格的相容性。
2026-02-13	3ds Max 的截止日期雲端為 AI 輔助開發新增了 Kiro 功能	Deadline Cloud for 3ds Max 儲存庫現在包含 Kiro 功能，可提供內建護欄和最佳實務的 AI

Date	Title	Description
		輔助設定、設計和開發工作流程。
2026-02-06	Deadline Cloud 新增用於存取控制的任務標記	任務資源現在支援標記和屬性型存取控制 (ABAC)。IAM 政策可以使用條件索引鍵參考任務標籤，啟用標籤型授權模式，例如限制對具有特定團隊標籤之任務的 GetJob API 呼叫。
2026-02-05	Deadline Cloud 現在支援 IAM Identity Center 多區域複寫	AWS Deadline Cloud 現在支援 IAM Identity Center 的多區域複寫功能，讓工作室更靈活地設定相對於 Identity Center 執行個體的 Deadline Cloud。Studio 可以在符合其轉譯需求的區域中建立截止日期雲端陣列，同時管理員繼續從主要區域管理 Identity Center。
2026-02-04	FLUX.2 Klein LoRA 訓練的範例任務套件現已推出	現已提供範例任務套件，示範如何使用 20-50 個映像，在 FLUX.2 Klein 模型上訓練自訂 LoRA 轉接器。這可讓您為產品、角色或品牌資產建立個人化的映像產生器，而不需要深度學習專業知識。LoRA 微調方法可建立小型的可攜式模型轉接器，可有效率地訓練並輕鬆地與團隊共用。

Date	Title	Description
2026-01-29	V-Ray 獨立並排轉譯任務套件 現已推出	匯出的 V-Ray 場景的並排轉譯的新任務套件現已可用。此任務套件可將高解析度影像分割為可跨轉譯陣列平行處理的圖磚，以有效率地轉譯高解析度影像。使用 3ds Max 和 V-Ray 的客戶可以在本機匯出 V-Ray 場景，並使用此套件將其提交給 Linux 工作者，而不需要使用 Windows。
2026-01-27	Deadline Cloud 現在支援編輯任務名稱和描述	AWS Deadline Cloud 現在支援在提交後編輯任務名稱和描述。這項新功能可透過更新名稱或在描述欄位中新增有用的追蹤詳細資訊，在提交後更輕鬆地組織和識別任務。
2026-01-22	Maya 的截止日期雲端上的 Redshift 2026 支援	Linux 服務受管機群現在支援 Redshift 2026 搭配 Maya 的截止日期雲端。
2026-01-22	Deadline Cloud 現在支援使用 Foundry Nuke CopyCat 進行機器學習訓練	Deadline Cloud 現在與 Foundry Nuke CopyCat 整合，讓您能夠在雲端中執行 ML 訓練任務，以獲得視覺化效果。CopyCat 會從範例影格學習調整，並將其套用至整個序列。將訓練任務提交至您的 Deadline Cloud 轉譯陣列、平行擴展工作負載，並釋放您的藝術家工作站。

Date	Title	Description
2026-01-15	截止日期SDKs現在包含任務完成的等待程式	AWS Deadline Cloud SDKs 現在包含 JobComplete 和 JobSucceeded 等待程式，可簡化任務狀態的輪詢。JobComplete 等待程式輪詢直到任務達到任何終止狀態 (SUCCEEDED、FAILED 或 CANCELED)，而 JobSucceeded 等待程式輪詢直到任務成功。這些等待者不需要撰寫自訂輪詢邏輯，因此更容易建置依賴於任務完成的自動化工作流程。
2026-01-15	Deadline Cloud 現在支援標記預算	AWS Deadline Cloud 客戶現在可以將標籤套用至 Budget 資源，並使用屬性型存取控制 (ABAC) 進行精細的許可管理。這項新功能可讓客戶使用標籤來組織、管理和控制對期限雲端預算的存取，從而在其 AWS 資源之間實現一致的授權模式。客戶現在可以在建立期間標記預算，並在 IAM 政策中使用這些標籤來控制誰可以根據標籤值存取特定預算。

Date	Title	Description
2026-01-15	截止日期雲端監視器搜尋現在支援多選篩選	使用截止日期雲端監視器時，您現在可以為任何搜尋篩選條件選取最多 16 個值，包括使用者名稱和任務狀態。這可讓您快速尋找多個使用者的任務，或一次篩選多個狀態。此功能也可透過適用於任務、步驟、任務和工作者的新 StringListFilterExpression，在截止日期雲端 API 中使用。
2026-01-07	截止日期雲端文件現在包含直接截止日期雲端監控和提交者安裝程式下載連結	使用者現在可以直接從截止日期雲端文件下載截止日期雲端監視器桌面應用程式和提交者安裝程式。這可讓沒有 AWS 主控台存取權的使用者下載開始使用截止日期雲端所需的軟體。
2025-12-19	Submitter Installer v2025-12-19 已發行	已發行新的提交者安裝程式，以更新下列元件： <ul style="list-style-type: none">• cinema-4d : 0.9.0 → 0.9.2 (版本備註)• deadline-cloud : 0.53.3 → 0.54.0 (版本備註)• nuke : 0.18.13 → 0.18.14 (版本備註)

Date	Title	Description
2025-12-17	截止日期雲端監視器 1.1.7 - 整合任務提交	<p>最新的截止日期 Cloud Monitor 桌面應用程式版本包括：</p> <ul style="list-style-type: none"> • 支援直接從截止日期雲端監視器桌面應用程式提交任務。 • 簡化工作站設定。 • 改善代理支援。 • 讀取和寫入截止日期雲端設定檔組態檔案時，邊緣案例的錯誤修正。
2025-12-11	截止日期雲端開發人員指南現在包含使用 AI 代理器的指引	<p>Deadline Cloud 開發人員指南現在包含將 AI 代理器與 AWS Deadline Cloud 搭配使用的最佳實務，以便更有效率地撰寫任務套件、開發 conda 套件和疑難排解任務。</p>
2025-12-10	Autodesk VRED 提交者現可使用使用者指南	<p>適用於 Autodesk VRED 的 AWS 截止日期雲端提交者文件現已提供。本指南說明如何安裝提交者並將轉譯任務提交至截止日期雲端。這有助於 VRED 使用者快速開始使用雲端轉譯。</p>
2025-12-10	截止日期雲端文件現在包含 LicensesInUse 指標	<p>截止日期雲端文件現在包含 LicensesInUse 指標的相關資訊。此指標可協助您監控任務目前在機群中耗用的授權數量。您可以使用此資訊來最佳化授權用量，並避免在擴展工作負載時耗盡授權。</p>

Date	Title	Description
2025-12-10	對服務受管機群的電影 4D 2026.1 支援	Linux 和 Windows 服務受管機群現在支援 Maxon Cinema 4D 2026.1。此版本包含 Redshift 2026.2.0。所有版本的 Cinema 4D 也已新增跨平台字型轉譯支援。此版本可讓客戶使用最新的電影 4D 功能。它還允許客戶在跨平台設定上使用自訂字型，例如在從 Windows 提交任務時，同時使用更快的啟動時間和更低的 Linux 工作者成本。
2025-12-09	增強型 Autodesk Maya 提交者設定和使用文件	針對適用於 Autodesk Maya 的 AWS 截止日期雲端提交者新增了新的設定和使用文件。
2025-12-09	After Effects 提交器 0.4.4 改善了 macOS 安裝和字型支援	After Effects 提交者現在會自動安裝到 macOS 上的使用者偏好設定目錄，無需手動安裝。此版本也新增對大多數 TrueType Collection (TTC) 字型檔案的支援，可讓您提交和轉譯使用這些字型的任務。這些改善可簡化設定並擴展 After Effects 使用者的字型相容性。

Date	Title	Description
2025-12-08	截止日期雲端版本備註	<p>截止日期雲端功能、應用程式、整合、範例和文件的所有主要變更現在都會列在後續使用者指南的版本備註頁面上。您可以在 Deadline Cloud github 組織的儲存庫中，在 AWS What's New 和 CLI/Worker/integration-specific Release Notes 中找到先前的主要截止日期雲端版本 https://github.com/aws-deadline</p>

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的[AWS 詞彙表](#)。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。