使用者指南

AWS 截止日期 雲端

版本 latest

AWS 截止日期 雲端: 使用者指南

Table of Contents

什麼是 AWS 截止日期雲端？

Deadline Cloud 是 AWS 服務 ，您可以直接使用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渲染專案和任務。

Deadline Cloud 提供主控台介面、本機應用程式、命令列工具和 API。透過截止日期雲端，您可以建立、管理和監控陣列、機群、任務、使用者群組和儲存體。您也可以指定硬體功能、為特定工作負載建立環境，以及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渲染專案。您可以管理使用者、將專案指派給他們，以及授予任務角色的許可。

主題

截止日期雲端的功能

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 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。
- 使用標籤來整理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，以支援雲端或當面渲染。

期限雲端的概念和術語

為了協助您開始使用 AWS 截止日期雲端，本主題會說明其一些關鍵概念和術語。

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範圍內。

截止日期雲端用戶端程式庫

Client Library 包含命令列界面和程式庫，用於管理截止日期雲端。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。DCCs 的範例為 Maya、 Nuke和 Houdini。截止日期 雲端為特定 DCCs 提供任務提交者整合外掛程式。

伺服器陣列

陣列是您專案資源所在的 。它由佇列和機群組成。

機群

機群是一組執行轉譯的工作者節點。工作者節點會處理任務。機群可以與多個佇列相關聯，而佇列可以與多個機群相關聯。

任務

任務是轉譯請求。使用者提交任務。任務包含概述為步驟和任務的特定任務屬性。

任務附件

任務連接是一種截止日期雲端功能，可用來管理任務的輸入和輸出。任務檔案會在轉譯過程中上傳為任務附件。這些檔案可以是紋理、3D 模型、照明設備和其他類似的項目。

任務優先順序

任務優先順序是截止日期 Cloud 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，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。

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。

任務範本

任務範本會定義執行期環境，以及做為截止日期雲端任務一部分執行的所有程序。

佇列

佇列是已提交任務所在的位置，並排定轉譯。佇列必須與機群相關聯，才能建立成功的轉譯。佇列可以與多個機群建立關聯。

佇列機群關聯

當佇列與機群相關聯時，會有佇列機群關聯。使用 關聯將工作者從機群排程到該佇列中的任務。您可以啟動和停止關聯，以控制工作排程。

步驟

步驟是在任務中執行的一個特定程序。

截止日期 雲端提交者

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。

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金鑰和選用值。

使用標籤，您可以用不同的方式分類 AWS 資源。例如，您可以為帳戶的 Amazon EC2 執行個體定義一組標籤，協助您追蹤每個執行個體的擁有者和堆疊層級。

您也可以依用途、擁有者或環境來分類 AWS 資源。當您有許多相同類型的資源時，此方法很有用。您可以根據您指派給該資源的標籤快速識別特定資源。

任務

任務是轉譯步驟的單一元件。

以用量為基礎的授權 (UBL)

以用量為基礎的授權 (UBL) 是一種隨需授權模型，可供特定第三方產品使用。此模型是按您的付費，而且會向您收取您使用的小時和分鐘數。

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。

工作程序

工作者屬於機群，並執行截止日期雲端指派的任務以完成步驟和任務。工作者會將任務操作的日誌存放在 Amazon CloudWatch Logs 中。工作者也可以使用任務附件功能，將輸入和輸出同步至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

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。

您也可以在建立轉譯陣列時定義設定和資源。此方法比使用預設設定和資源需要更多的時間，但可讓您有更多的控制權。

熟悉截止期限雲端概念和術語後，請參閱建立陣列、新增使用者和實用資訊連結step-by-step說明入門。

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：

- 期限雲端主控台 – 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。
- 期限雲端監控 – 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。截止日期雲端監視器可做為 Web 瀏覽器和桌面應用程式使用。
- AWS SDK 和 AWS CLI – 使用 AWS Command Line Interface (AWS CLI) 從本機系統的命令列呼叫截止期限雲端 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

截止日期 雲端適用於下列項目 AWS 服務：

- Amazon CloudWatch – 使用 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 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，以將 Amazon EC2 執行個體用於工作負載。如需詳細資訊，請參閱 Amazon EC2 執行個體。

- Amazon EC2 Auto Scaling – 使用 Auto Scaling，您可以隨著執行個體需求的變化，自動增加或減少執行個體數量。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。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。截止日期 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 ，可讓您從單一位置提供使用者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 AWS SDK、 AWS Command Line Interface (AWS CLI) 或截止日期雲端任務提交者，將任務提交至截止日期雲端。截止日期 雲端支援任務範本規格的開放任務描述 (OpenJD)。如需詳細資訊，請參閱 GitHub 網站上的開啟任務描述。

截止日期 雲端提供任務提交者。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。使用提交者，藝術家可以從第三方界面將渲染任務提交至期限雲端，其中管理專案資源並監控任務，所有這些任務都集中在一個位置。

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，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、日誌和其他疑難排解指標。

截止日期雲端中的許可

截止日期 雲端支援下列項目：

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

在任何人可以處理專案之前，他們必須能夠存取該專案和相關聯的陣列。截止日期雲端已與 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。每個後續層級都包含先前層級的許可。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 – 有權查看其可存取的陣列、佇列、機群和任務中的資源。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 Management Console 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，可以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，您可以為對應陣列、機群或佇列將存取許可授予整個群組。

使用截止日期雲端的軟體支援

期限 雲端適用於可以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 支援描述任務的OpenJD規格，其軟體指令碼步驟會參數化（例如跨影格範圍）至任務。將OpenJD任務說明與 Deadline Cloud 工具和功能整合到任務套件中，以建立、執行和授權第三方軟體應用程式的步驟。

任務需要授權才能轉譯。Deadline Cloud 提供以usage-based-licensing(UBL)，以根據用量以小時為單位遞增計費的多種軟體應用程式授權。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。

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，獲得建立陣列的引導式體驗，包括佇列和機群。使用 AWS CLI 來直接使用 服務，或開發使用截止期限雲端的自有工具。

若要建立陣列並使用截止日期雲端監視器，請將您的帳戶設定為截止日期雲端。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。

若要在不設定截止日期雲端監視器基礎設施的情況下建立陣列，請為截止日期雲端設定開發人員工作站。

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 Quickstart。 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。這種方法是一種方便的方法，可建立沙盒樣式的陣列進行實驗。

主題

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。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   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監控基礎設施並定義您的陣列。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

期限 雲端監視器使用 AWS IAM Identity Center 授權使用者。您用於截止日期雲端的 IAM Identity Center 執行個體必須與 AWS 區域 監視器位於相同的 中。如果您的主控台在建立監視器時使用不同的區域，則會收到變更為 IAM Identity Center 區域的提醒。

您的監視器基礎設施包含下列元件：

- 監控顯示名稱：監控顯示名稱是識別監控的方式，例如 AnyCompany 監控。您的監視器名稱也會決定您的監視器 URL。

  > **Important**
  >
  > 在完成設定後，您無法變更監視器顯示名稱。

- 監控 URL：您可以使用監控 URL 存取您的監控。URL 是以監控顯示名稱為基礎，例如 https://anycompanymonitor.awsapps.com。

  > **Important**
  >
  > 在完成設定後，您無法變更監視器 URL。

- 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。這可降低延遲並改善資料傳輸速度。 AWS IAM Identity Center 必須在與截止日期雲端 AWS 區域 相同的 中啟用。

> **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 Management Console以開始歡迎使用截止日期雲端設定，然後選擇下一步。
2. 輸入監視器顯示名稱 — 例如 **`AnyCompany Monitor`**。
3. （選用）若要變更監視器名稱，請選擇編輯 URL。
4. （選用）若要變更AWS 區域最接近您使用者的 ，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。

   - （選用）若要新增群組和使用者，請選取 （選用）新增群組和使用者。
   - （選用）若要進一步自訂您的監視器設定，請選取 其他設定。
5. 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。

（選用）新增群組和使用者

在完成截止日期雲端監視器設定之前，您可以新增監視器使用者，並將其新增至群組。

設定完成後，您可以建立新的使用者和群組，並管理 等使用者，以為其指派群組、許可和應用程式，或從監視器中刪除使用者。

其他設定

期限 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、設定您的監控使用者角色，以及變更加密金鑰類型。

AWS IAM Identity Center

AWS IAM Identity Center 是一種雲端型單一登入服務，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。

截止日期雲端預設會啟用 IAM Identity Center，而且必須設定和使用截止日期雲端。您用於截止日期雲端的 IAM Identity Center 執行個體必須與 AWS 區域 監視器位於相同的 中。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。期限 雲端需要監控使用者角色，才能讓使用者存取您監控中的資源。

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，例如在特定期限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。若要使用現有服務角色，請選擇現有服務角色索引標籤。

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. 選擇檢視許可詳細資訊以取得角色的詳細資訊。

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 IAM 主控台中的檢視，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. 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。
3. （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 。
4. （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和排程工作。

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目的。
3. 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。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-[MONITORNAME]`**。

      您只能使用小寫字母和破折號。沒有空格或特殊字元。

   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. 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。

- 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。

5. 您的佇列需要代表您存取 Amazon S3 的許可。建議您為每個佇列建立新的服務角色。

   a. 對於新角色，請完成下列步驟。

      i. 選取建立並使用新的服務角色。

      ii. 輸入佇列角色的角色名稱，或使用提供的角色名稱。

      iii. （選用）新增佇列角色描述。

      iv. 您可以選擇檢視許可詳細資訊，以檢視佇列角色的 IAM 許可。

   b. 或者，您可以選取現有的服務角色。

6. （選用）使用名稱和值對為佇列環境新增環境變數。

7. （選用）使用金鑰和值對為佇列新增標籤。

輸入所有佇列詳細資訊後，請選擇下一步。

（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描述。

   b. 選取運算資源應擴展的方式。服務受管選項可讓 Deadline Cloud 自動擴展您的運算資源。客戶受管選項可讓您控制自己的運算擴展。

2. 在執行個體選項區段中，選擇 Spot 或隨需。Amazon EC2 隨需執行個體提供更快的可用性，Amazon EC2 Spot 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目下限設為 **0**，以避免產生額外費用。

4. 您的機群需要代表您寫入 CloudWatch 的許可。建議您為每個機群建立新的服務角色。

   a. 對於新角色，請完成下列步驟。

      i. 選取建立並使用新的服務角色。

      ii. 輸入機群角色的角色名稱，或使用提供的角色名稱。

iii. （選用）新增機群角色描述。

iv. 若要檢視機群角色的 IAM 許可，請選擇檢視許可詳細資訊。

b. 或者，您可以使用現有的服務角色。

5. （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。

（選用）步驟 5：設定工作者功能

定義工作者執行個體的功能。

1. 選擇機群中工作者的作業系統。在本教學課程中，請保留預設值 Linux。
2. 檢閱 CPU 架構設定是否有意識。
3. 更新硬體功能的 vCPUs數量下限和上限。
4. 更新硬體功能的記憶體數量下限和上限 (GiB)。
5. 您可以允許或排除工作者執行個體的類型來篩選執行個體類型。在這兩種篩選選項中，您最多可以篩選 10 個 Amazon EC2 執行個體類型。
6. 在其他功能（選用）下，您可以依大小 (GiB)、IOPS 和輸送量 (MiB/s) 定義根 EBS 磁碟區。
7. 設定所有工作者功能後，請選擇下一步來定義群組的存取層級。

（選用）步驟 6：定義存取層級

如果您有群組連接到監視器，您可以定義其存取層級。使用截止期限雲端功能的許可由存取層級管理。您可以將不同的存取層級指派給使用者群組。

1. 使用截止日期雲端陣列存取層級選單，為群組選取許可層級。
2. 選擇下一步以繼續並檢閱輸入的所有陣列詳細資訊。

步驟 7：檢閱和建立

檢閱輸入的所有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。當您的陣列準備好使用時，會顯示成功訊息。

設定截止日期雲端提交者

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用於提交渲染的所有工作站上完成。

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

主題

步驟 1：安裝截止日期雲端提交者

以下各節會引導您完成安裝截止日期雲端提交者的步驟。

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。目前，截止日期雲端提交者安裝程式僅支援 Windows和 Linux。

1. 登入 AWS Management Console 並開啟截止日期雲端主控台。
2. 從側邊導覽窗格中，選擇下載。
3. 找到截止日期雲端提交者安裝程式區段。
4. 選取您電腦作業系統的安裝程式，然後選擇下載。

（選用）驗證下載軟體的真實性

若要確認您下載的軟體是真實的，請針對 Windows或 使用下列程序Linux。您可能想要這麼做，以確保下載程序期間或之後沒有人竄改檔案。

您可以使用這些指示來先驗證安裝程式，然後在 中下載後驗證截止日期雲端監視器 步驟 2：安裝和設定截止日期雲端監視器。

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，*file*將 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-----

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

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

2. 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. 返回截止日期雲端主控台下載頁面，並下載截止日期雲端提交者安裝程式的簽章檔案。

   b. 執行下列動作，以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。如需平台特定方法，請參閱 Linux (Debian)索引標籤、 Linux(RPM) 索引標籤，或根據您下載的檔案類型的Linux (AppImage)索引標籤。

   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. 返回截止日期雲端主控台下載頁面並下載對應的 .sig 檔案，然後執行

對於 .deb：

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

對於 .rpm：

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

對於 .AppImage：

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

b. 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。

Linux (AppImage)

若要驗證使用 Linux .AppImage 二進位檔的套件，請先在 Linux索引標籤中完成步驟 1-3，然後完成下列步驟。

1. 從 GitHub 中的 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，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 型Linux分佈的核心套件管理工具。您可以使用 工具驗證 .deb 檔案。

1. 從截止日期雲端主控台下載頁面，下載截止日期雲端監視器 .deb 檔案。
2. 將 *<APP_VERSION>* 取代為您要驗證的 .deb 檔案版本。

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

3. 輸出將類似於：

```
ProcessingLinux deadline-cloud-monitor_<APP_VERSION>_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. 從截止日期雲端主控台下載頁面，下載截止日期雲端監視器 .rpm 檔案。
2. 將 *<APP_VERSION>* 取代為要驗證的 .rpm 檔案版本。

```
gpg --export --armor "Deadline Cloud" > key.pub
sudo rpm --import key.pub
rpm -K deadline-cloud-monitor-<APP_VERSION>-1.x86_64.rpm
```

3. 輸出將類似於：

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

安裝截止日期雲端提交者

您可以使用 Windows或 安裝截止日期雲端提交者Linux。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
Adobe After Effects	2024 年、2025 年	包含	不包含
適用於 Maya 的 Autodesk Arnold	7.1、7.2	包含	包含
Autodesk Maya	2023、2024、2025	已包含	已包含
混合器	3.6、4.2	已包含	已包含
KeyShot Studio	2023 年、2024 年	已包含	不包含
Maxon Cinema 4D	2024 年、2025 年	已包含	不包含
Nuke	15	已包含	已包含
SideFX Houdini	19.5、20、20.5	已包含	已包含
虛擬引擎	5.2、5.3、5.4	已包含	不包含

您可以安裝此處未列出的其他提交者。我們使用截止日期雲端程式庫來建置提交者。有些提交者包括 3ds Max 和 Rhino。您可以在 aws-deadline GitHub 組織中找到這些程式庫和提交者的原始碼。

Windows

1. 在檔案瀏覽器中，導覽至安裝程式下載所在的資料夾，然後選取 `DeadlineCloudSubmitter-windows-x64-installer.exe`。

   a. 如果 Windows 保護您的 PC 快顯視窗，請選擇更多資訊。

b. 無論如何，選擇執行。

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. 完成下列其中一個步驟，以選擇安裝範圍：
   - 若要僅為目前使用者安裝 ，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：

     a. 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。

     b. 輸入您的管理員登入資料，然後選擇是。

     c. 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，或您要安裝的提交者。
7. 選擇 Next (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分佈上。

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 鍵成為根。
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，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。

步驟 2：安裝和設定截止日期雲端監視器

您可以使用 Windows或 安裝截止日期雲端監控桌面應用程式Linux。

Windows

1. 如果您尚未登入，請登入 AWS Management Console 並開啟截止日期雲端主控台。
2. 從左側導覽窗格中，選擇監視器下載。
3. 在截止日期雲端監控區段中，選取您電腦作業系統的檔案。
4. 若要下載截止日期雲端監視器，請選擇下載。

若要執行無訊息安裝，請使用下列命令：

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

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

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

Linux (AppImage)

在 Debian distros 上安裝 Deadline Cloud Monitor AppImage

1. 下載最新的截止日期雲端監視器 AppImage。
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 udpate
```

```
sudo apt install libfuse2
```

3. 若要讓 AppImage 可執行檔，請輸入：

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

Linux (Debian)

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

1. 下載最新的 Deadline Cloud Monitor Debian 套件。
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 libssl1.1，請輸入：

```
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/
libssl1.1_1.1.1f-1ubuntu2_amd64.deb
sudo apt install ./libssl1.1_1.1.1f-1ubuntu2_amd64.deb
```

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

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

4. 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

1. 下載最新的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. 針對 libssl.so.1.1 相依性安裝 compat-openssl11：

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

在 上安裝截止日期雲端監視器 RPM Red Hat Linux 9

1. 下載最新的截止日期雲端監視器 RPM。
2. 啟用CodeReady Linux Builder儲存庫：

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

3. 安裝適用於 的額外套件Enterprise RPM：

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

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

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

完成下載後，您可以驗證下載軟體的真實性。您可能想要這麼做，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 中的驗證下載軟體的真實性。

下載截止日期雲端監控並確認真實性後，請使用下列程序來設定截止日期雲端監控。

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，並每 15 分鐘同步您的登入資料。
6. 對於您計劃用於渲染專案的每個數位內容建立 (DCC) 應用程式，請完成下列步驟：

   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。您的截止期限雲端憑證現在會與此 DCC 共用，且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提交者。您可以使用 中的指示來安裝其他提交者支援的提交者。

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. 選擇編輯，然後選擇偏好設定。在檔案路徑下選擇指令碼目錄，然後選擇新增。為安裝Blender提交者所在的 python 資料夾新增指令碼目錄：

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

3. 重新啟動 Blender。
4. 選擇編輯，然後選擇偏好設定。接著，選擇附加元件，然後搜尋 的截止日期雲端Blender。選取核取方塊以啟用附加元件。
5. 開啟資產根目錄中存在相依性的Blender場景。
6. 在轉譯功能表中，選取截止日期雲端對話方塊。
   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. 登入瀏覽器視窗隨即顯示。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，登入資料狀態顯示為 AUTHENTICATED。
7. 選擇提交。

支援的提交者

下列各節會引導您完成啟動可用截止日期雲端提交者外掛程式的步驟。

您可以安裝此處未列出的其他提交者。我們使用截止日期雲端程式庫來建置提交者。有些提交者包括 3ds Max 和 Rhino。您可以在 aws-deadline GitHub 組織中找到這些程式庫和提交者的原始碼。

軟體	支援的版本	Windows 安裝程式	Linux 安裝程式
Adobe After Effects	2024 年、2025 年	包含	不包含
Autodesk Arnold for Maya	7.1、7.2	包含	包含
Autodesk Maya	2023、2024、2025	已包含	已包含
混合器	3.6、4.2	已包含	已包含
KeyShot Studio	2023 年、2024 年	已包含	不包含
Maxon Cinema 4D	2024 年、2025 年	已包含	不包含
Nuke	15	已包含	已包含
SideFX Houdini	19.5、20、20.5	已包含	已包含
虛擬引擎	5.2、5.3、5.4	已包含	不包含

After Effects

在 中啟動截止日期雲端提交者 After Effects

1. 打開 After Effects.
2. 選擇編輯，然後選擇偏好設定，然後選擇指令碼和表達式。
3. 選擇允許指令碼寫入檔案和存取網路。
4. 重新啟動效果後
5. 選取視窗，然後選擇 DeadlineCloudSubmitter.jsx。

使用 After Effects 提交者

1. 在提交者面板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. 選擇提交者面板上的重新整理。

4. 從清單中選擇您的構圖，然後選擇提交。當您從轉譯佇列新增或移除構圖時，可以選擇再次重新整理。

您可以透過選擇提交者右上角並將其放入 中任何反白區段，將提交者停駐到側邊面板After Effects。

Blender

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. 選擇編輯，然後選擇偏好設定。在檔案路徑下選擇指令碼目錄，然後選擇新增。為安裝Blender提交者所在的 python 資料夾新增指令碼目錄：

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

3. 重新啟動 Blender。
4. 選擇編輯，然後選擇偏好設定。接著，選擇附加元件，然後搜尋 的截止日期雲端Blender。選取核取方塊以啟用附加元件。
5. 開啟資產根目錄中存在相依性的Blender場景。
6. 在轉譯功能表中，選取截止日期雲端對話方塊。
   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. 登入瀏覽器視窗隨即顯示。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，登入資料狀態顯示為 AUTHENTICATED。
7. 選擇提交。

Cinema 4D

在 中啟動截止日期雲端提交者 Cinema 4D

> **Note**
>
> 支援Cinema 4D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. 開啟電影 4D。
2. 如果系統提示您安裝 AWS 截止日期雲端的 GUI 元件，請完成下列步驟：
   a. 當提示顯示時，選擇是，並等待相依性安裝。
   b. 重新啟動Cinema 4D以確保套用變更。
3. 選擇延伸 > AWS 截止日期雲端提交者。

Houdini

在 中啟動截止日期雲端提交者 Houdini

> **Note**
>
> 支援Houdini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 Houdini.
2. 在網路編輯器中，選取 /out 網路。
3. 按 索引標籤，然後輸入 **`deadline`**。
4. 選取截止日期雲端選項，並將其連接到現有的網路。
5. 按兩下截止日期雲端節點。

KeyShot

在 中啟動截止日期雲端提交者 KeyShot

1. 打開 KeyShot.
2. 選擇 Windows > 指令碼主控台 > 提交至 AWS 截止日期雲端並執行。

KeyShot 提交者有兩種提交模式。選取提交模式以開啟提交者。

- 連接場景 BIP 檔案和所有外部檔案參考 – 開啟的場景檔案和 BIP 中參考的所有外部檔案都包含在任務附件中。
- 僅連接場景 BIP 檔案 – 只有開啟的場景檔案會連接至提交。場景中參考的任何外部檔案必須透過網路儲存或其他方法提供給工作者。

Maya and Arnold for Maya

在 中啟動截止日期雲端提交者 Maya

> **Note**
>
> 支援 Maya和 Arnold for Maya (MtoA) 是使用服務受管機群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 Maya.
2. 設定您的專案，並開啟資產根目錄中存在的檔案。
3. 選擇 Windows → 設定/偏好設定 → 外掛程式管理員。
4. 搜尋 DeadlineCloudSubmitter。
5. 若要載入截止日期雲端提交者外掛程式，請選取已載入。
    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. 登入瀏覽器視窗隨即顯示。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，登入資料狀態顯示為 AUTHENTICATED。
6. （選用）若要在每次開啟 時載入截止日期雲端提交者外掛程式Maya，請選擇自動載入。
7. 選取截止日期雲端架，然後選取綠色按鈕以啟動提交者。

Nuke

在 中啟動截止日期雲端提交者 Nuke

> **Note**
>
> 支援Nuke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 Nuke.
2. 開啟具有存在於資產根目錄中之相依性的Nuke指令碼。
3. 選擇 AWS Deadline，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，登入資料狀態顯示為 AUTHENTICATED。
4. 選擇提交。

Unreal Engine

在 中啟動截止日期雲端提交者 Unreal Engine

1. 建立或開啟您用於Unreal Engine專案的資料夾。
2. 開啟命令列並執行下列命令：
   - **`git clone https://github.com/aws-deadline/deadline-cloud-for-unreal-engine`**
   - **`cd deadline-cloud-for-unreal/test_projects`**
   - **`git lfs fetch -all`**
3. 若要下載 的外掛程式Unreal Engine，請開啟Unreal Engine專案資料夾，然後啟動 deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat。

   這會將外掛程式檔案放入 C：/LocalProjects/UnrealDeadlineCloudTest/Plugins/UnrealDeadlineCloudService。

4. 若要下載提交者，請開啟 UnrealDeadlineCloudService 資料夾，然後執行 **deadline-cloud-forunreal/ test_projects/Plugins/UnrealDeadlineCloudService/ install_unreal_submitter.bat**。
5. 若要從 啟動提交者Unreal Engine，請完成下列步驟：

   a. 選擇**編輯 > 專案設定**。
   b. 在搜尋列中，輸入 **movie render pipeline**。
   c. 調整下列電影渲染管道設定：

      i. 對於預設遠端執行器，輸入 **MoviePipelineDeadlineCloudRemote Executor**。
      ii. 針對預設執行器任務，輸入 **MoviePipelineDeadlineCloudExecutorJob**。
      iii. 針對預設任務設定類別，選擇加號，然後輸入 **DeadlineCloudRenderStepSetting**。

      使用這些設定，您可以從 選擇截止日期雲端外掛程式Unreal Engine。

使用截止日期雲端監視器

AWS 截止日期雲端監視器可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視器，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，或者您可以選取任務以查看詳細的任務日誌，以協助對任務的問題進行疑難排解。

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。

期限雲端監控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

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，讓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，或將使用者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 傳送給任何需要存取截止日期雲端監視器的人。

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 Management Console 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 登入資料登入監視器。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視器 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，則必須提供監視器 URL 並建立設定檔名稱。接下來，您可以使用截止日期雲端憑證登入監視器。
   • 建立設定檔之後，您可以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憑證。

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

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佇列的陣列。
3. 在佇列清單中，選擇要顯示其詳細資訊的佇列。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，例如將優先順序變更或檢視步驟變更為步驟相依性。
- 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提供您下列項目：

- 任務進度的整體檢視。
- 構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，選取要檢視其詳細資訊的任務。
    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。具有較高數量優先順序的任務會在具有較低數量優先順序的任務之前處理。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，其必須處於終端機狀態、FAILED、SUSPENDED、 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顯示在截止日期雲端 CLI 中 120 天。

將任務排入佇列

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

- 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，然後再次以完整的影格範圍執行任務。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，任務清單會顯示構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日誌

日誌提供您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表，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，例如關閉工作者的環境

  工作階段包含至少處理一個任務，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 和記憶體的相關資訊。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所處理動作的時間軸詳細資訊。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. 請依照 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。輸出檔案會與您建立任務時指定的名稱和位置一起存放。

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。
   - 如果您選擇步驟，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，輸出會下載到設定的位置。

> **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。

截止期限雲端佇列

佇列是一種陣列資源，可管理和處理任務。

若要使用佇列，您應該已設定監視器和陣列。

主題

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，在左側面板選擇陣列和其他資源，然後選擇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目的。
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，您必須完成下列步驟。

> **Important**
>
> 我們強烈建議為執行身分功能指定使用者和群組。如果不這樣做，它會降低您陣列的安全狀態，因為任務接著可以執行工作者代理程式可以執行的所有工作。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Windows機群，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。

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）若要為佇列環境新增環境變數，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 應用程式和渲染器的套件。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，或直接編輯 json 或 YAML 範本來新增佇列環境。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，然後輸入您新增的每個變數的名稱和值。
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，Conda支援在虛擬環境中下載和安裝任務的套件。

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 AWS 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 上還有其他可用的佇列環境範本，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`，該頻道託管支援合作夥伴 DCC 應用程式和渲染器的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

- 混合器
  - `blender=3.6`

    - blender=4.2
    - blender-openjd
- 奧迪尼
    - houdini=19.5
    - houdini=20.0
    - houdini=20.5
    - houdini-openjd
- Maya
    - maya=2024

      maya=2025
    - maya-mtoa=2024.5.3

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

Windows

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

當您將任務提交至具有預設Conda環境的佇列時，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套件和頻道。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，此頻道可供服務受管機群使用，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將任務從 DCC 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， CondaPackage 參數會設為 blender=3.6.* blender-openjd=0.4.*。

關聯佇列和機群

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。若要將現有佇列與現有機群建立關聯，請完成下列程序。

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。顯示可用的機群清單。
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該已關聯。

截止日期 雲端機群

本節說明如何管理服務受管機群和客戶受管機群 (CMF) 的截止日期雲端。

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此服務 Deadline Cloud 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。這包括佈建、操作、管理和停用機群中的工作者。

主題

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以執行的時間量。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，您可能會失去正在執行工作者或任務的工作。若要避免這種情況，請監控您的工作者和任務，以確保它們不會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

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目的。
5. 選取服務受管機群類型。
6. 選擇機群的 Spot 或隨需執行個體市場選項。Spot 執行個體是無保留的容量，您可以折扣價使用，但可能會受到隨需請求的干擾。隨需執行個體會依第二個定價，但沒有長期承諾，而且不會中斷。根據預設，機群會使用 Spot 執行個體。

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。服務角色會提供登入資料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 Next (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. 輸入您機群所需的最小和最大 vCPU。
13. 輸入您機群所需的最小和最大記憶體。
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，以確保此機群只會使用這些執行個體類型。
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。我們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 Next (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，其中一個範例就是特定的授權類型。
19. 選擇 Next (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。如果使用預設Conda佇列環境設定佇列，您的機群會自動獲得支援合作夥伴 DCC 應用程式和渲染器的套件。如需提供的套件清單，請參閱 預設Conda佇列環境。
21. 選擇 Next (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 Next (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 GPUs 來加速處理任務。使用 加速器可以減少處理任務所需的時間，但可以提高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 加速器與不使用的機群之間的權衡。

> **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將使用 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 的執行期驅動程式。

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

您可以從下列執行期驅動程式中選擇：

- `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:R550` - NVIDIA vGPU 軟體 17
- `GRID:R535` - NVIDIA vGPU 軟體 16

如果您未指定執行時間，Deadline Cloud 會使用 `latest`做為預設值。不過，如果您有多個加速器，並`latest`針對某些加速器指定 ，並保留其他加速器空白，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。使用 AL2023 的這些考量，包括期限雲端服務受管機群，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，使其與 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。這與 VFX Reference Platform CY2022, CY2023和 CY2024 相容。
- 服務受管機群VFX Reference Platform不提供其他具有 指定版本的程式庫。您必須向程式庫提供用於服務受管機群的任何應用程式。如需程式庫清單，請參閱參考平台。

客戶管理的機群

當您想要使用您管理的工作者機群時，您可以建立客戶管理的機群 (CMF)，讓截止日期 Cloud 用來處理您的任務。在下列情況下使用 CMF：

- 您有現有的現場部署工作者可與截止日期雲端整合。
- 您在位於共同位置的資料中心有工作者。
- 您想要直接控制 Amazon Elastic Compute Cloud (Amazon EC2) 工作者。

當您使用 CMF 時，您可以完全控制機群並負責。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管理的機群。

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 是以雲端為基礎的單一登入服務，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。如需詳細資訊，請參閱管理您的身分來源。

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。您可以使用 IAM Identity Center 或 Deadline Cloud 主控台建立和管理這些使用者和群組。如需詳細資訊，請參閱什麼是 AWS Organizations。

您可以使用截止日期雲端主控台建立和移除可管理陣列、佇列和機群的使用者和群組。當您將使用者新增至截止日期雲端時，他們必須先使用 IAM Identity Center 重設密碼，才能取得存取權。

主題

管理監視器的使用者和群組

Organizations 擁有者可以使用 Deadline Cloud 主控台來管理可存取 Deadline Cloud 監視器的使用者和群組。您可以從現有的 IAM Identity Center 使用者和群組中選擇，也可以從主控台新增新的使用者和群組。

1. 登入 AWS Management Console 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）選擇一或多個 IAM Identity Center 群組以新增使用者。
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。

管理陣列、佇列和機群的使用者和群組

在管理使用者和群組的過程中，您可以授予不同層級的存取許可。每個後續層級都包含先前層級的許可。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 – 有權查看其可存取的陣列、佇列、機群和任務中的資源。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，但具有許可，可編輯他們有權存取的佇列中的任務，並授予他們有權存取的資源許可。
- 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**
>
> 存取許可的變更最多可能需要 10 分鐘才能反映在系統中。

1. 如果您尚未登入，請登入 AWS Management Console 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. 若要管理佇列或機群，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。根據預設，會選取群組索引標籤。若要管理使用者，請選擇使用者。

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 用來排程和對可用工作者執行工作。當您建立任務時，您可以選擇要傳送任務的陣列和佇列。您也可以提供 JSON 或 YAML 檔案，提供工作者處理的指示。期限 雲端接受遵循開放任務描述 (OpenJD) 規格來描述任務的任務範本。如需詳細資訊，請參閱 GitHub 網站上的開放任務描述文件。

任務包含：

- 優先順序 – 截止日期 Cloud 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，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。步驟可能有最低工作者記憶體等需求，或是需要先完成的其他步驟。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，例如指令碼中使用的影格編號。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。

您可以透過下列任何方式建立任務：

- 使用截止日期雲端提交者。
- 建立任務套件並使用截止日期雲端命令列界面 （ 截止日期雲端 CLI)。
- 使用 AWS SDK。
- 使用 AWS Command Line Interface (AWS CLI)。

提交者是數位內容建立 (DCC) 軟體的外掛程式，可管理在 DCC 軟體的界面中建立任務。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。在幕後，提交者會建立描述任務的 OpenJD 任務範本。同時，它會將您的資產檔案上傳至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。為了減少傳送檔案所需的時間，只會將自上次上傳檔案以來變更的檔案傳送至 Amazon S3。

您可以建立限制來管理任務如何使用限制的資源，例如軟體授權。使用限制的任務只會使用限制下允許的資源數量。如需詳細資訊，請參閱建立任務的資源限制。

若要建立自己的指令碼和管道以將任務提交至截止日期雲端，您可以使用截止日期雲端 CLI、 AWS 軟體開發套件或 AWS CLI 呼叫操作來建立、取得、檢視和列出任務。下列主題說明如何使用截止日期雲端 CLI。

截止日期雲端 CLI 會與截止日期雲端提交者一起安裝。如需詳細資訊，請參閱設定截止日期雲端提交者。

主題

- 使用截止日期雲端 CLI 提交任務
- 在截止日期雲端中排程任務
- 截止日期雲端中的任務狀態
- 在截止日期雲端中修改任務
- 期限 雲端如何處理任務
- 建立任務的資源限制

使用截止日期雲端 CLI 提交任務

若要使用截止日期雲端命令列界面 （ 截止日期雲端 CLI) 提交任務，請使用 `deadline bundle submit`命令。

任務會提交至佇列。如果您尚未設定陣列和佇列，請使用截止日期雲端主控台來設定陣列和佇列，並查看陣列和佇列 ID。如需詳細資訊，請參閱定義陣列詳細資訊和定義佇列詳細資訊。

若要設定截止日期雲端 CLI 的預設陣列和佇列，請使用下列命令。當您設定預設值時，您可以使用截止日期雲端 CLI 命令，而無需指定陣列或佇列。在下列範例中，將 *farmId*和 取代*queueId*為您自己的資訊：

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

若要指定任務中的步驟和任務，請建立 OpenJD 任務範本。如需詳細資訊，請參閱 Open Job Description 規格 GitHub 儲存庫中的範本結構描述 【版本：2023-09】。

下列範例是 YAML 任務範本。它定義了一個任務，每個步驟有兩個步驟和五個任務。

```
name: Sample Job
specificationVersion: jobtemplate-2023-09
steps:
- name: Sample Step 1
  parameterSpace:
    taskParameterDefinitions:
    - name: var
```

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

若要建立任務，請建立一個名為 的新資料夾sample_job，然後將範本檔案儲存在新資料夾中，做為 template.yaml。您可以使用下列截止日期雲端 CLI 命令提交任務：

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

來自 命令的回應包含任務的識別符。請記住 ID，以便稍後檢查任務的狀態。

```
Submitting to Queue: test-queue
Waiting for Job to be created...
Submitted job bundle:
   sample_job
Job creation completed successfully
jobId
```

提交任務時，您可以使用其他選項。如需詳細資訊，請參閱使用截止日期雲端 CLI 提交任務的更多選項。

使用截止日期雲端 CLI 提交任務的更多選項

deadline bundle submit Deadline Cloud CLI 命令提供選項，可讓您用來指定任務的其他資訊。下列範例向您示範如何：

- 指定處理任務範本時使用的參數。
- 將共用環境中的檔案和資料夾連接到任務。
- 設定可處理任務的工作者數量上限。
- 設定任務取消之前的任務失敗次數上限。
- 設定任務的重試次數上限。

任務參數

當您建立任務時， parameters選項會設定任務參數的值。任務範本會定義 欄位，而 parameters選項會設定 值。參數可以有預設值。如果為 參數指定值，則指定的值會覆寫預設值。

下列任務範本定義 TestParameter 欄位：

```
name: Sample Job With Job Parameter
parameterDefinitions:
- default: test
  name: TestParameter
  type: STRING
specificationVersion: jobtemplate-2023-09
steps:
- description: step description
  name: MyStep
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
```

下列命令會將 的值TestParameter設定為「Hello AWS」：

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

儲存設定檔

儲存設定檔可協助在不同作業系統的工作者之間共用檔案。使用截止日期雲端主控台建立儲存設定檔。然後，使用 storage-profile-id 參數來使用儲存設定檔。如需詳細資訊，請參閱 截止日期雲端開發人員指南中的儲存設定檔和路徑映射。

若要設定任務提交的儲存設定檔，請使用截止日期雲端 CLI，使用以下命令來設定storage-profile-id組態參數：

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

任務的工作者上限

max-worker-count 選項會設定可指派給任務的工作者數量上限。當達到上限時，即使機群中有更多工作者可用，也不會再將工作者指派給任務。

```
deadline bundle submit sample_job --max-worker-count 10
```

失敗任務上限

max-failed-tasks-count 選項會設定在整個任務失敗之前可失敗的任務數目上限，且所有剩餘的任務都會標示為 CANCELED。預設值為 100.

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

失敗的任務重試次數上限

max-retries-per-task 選項會設定任務失敗前重試的次數上限。重試任務時，任務會進入 READY 狀態。預設值為 5。

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

在截止日期雲端中排程任務

建立任務後， AWS 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進行處理。根據為機群設定的功能和特定步驟的主機需求，選擇處理特定任務的機群。

佇列中的任務會以最盡力的優先順序排定，從最高到最低。當兩個任務具有相同的優先順序時，會先排程最舊的任務。

下列各節提供排程任務程序的詳細資訊。

判斷機群相容性

建立任務後，截止日期 Cloud 會根據與提交任務的佇列相關聯的機群功能，檢查任務中每個步驟的主機需求。如果機群符合主機需求，任務會進入 READY 狀態。

如果任務中的任何步驟具有與佇列相關聯的機群無法滿足的要求，則該步驟的狀態會設為 NOT_COMPATIBLE。此外，任務中的其餘步驟也會取消。

機群的功能是在機群層級設定。即使機群中的工作者符合任務的要求，如果其機群不符合任務的要求，則不會從任務中指派任務。

下列任務範本有一個步驟，指定步驟的主機需求：

```
name: Sample Job With Host Requirements
specificationVersion: jobtemplate-2023-09
steps:
- name: Step 1
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
  hostRequirements:
    amounts:
    # Capabilities starting with "amount." are amount capabilities. If they start with
 "amount.worker.",
    # they are defined by the OpenJD specification. Other names are free for custom
 usage.
    - name: amount.worker.vcpu
      min: 4
      max: 8
    attributes:
    - name: attr.worker.os.family
      anyOf:
      - linux
```

此任務可以排程到具有下列功能的機群：

```
{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
```

此任務無法排程到具有下列任何功能的機群：

```
{
    "vCpuCount": {"min": 4},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no maximum, so it exceeds the maximum vCPU host requirement.

{
    "vCpuCount": {"max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no minimum, so it doesn't satisfy the minimum vCPU host
 requirement.

{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "windows",
    "cpuArchitectureType": "x86_64"
}
    The osFamily doesn't match.
```

機群擴展

當任務指派給相容的服務受管機群時，機群會自動擴展。機群中的工作者數量會根據機群可執行的任務數量而變更。

當任務指派給客戶管理的機群時，工作者可能已存在，也可以使用事件型自動擴展來建立。如需詳細資訊，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的使用 EventBridge 來處理自動擴展事件。Amazon EC2 Auto Scaling

工作階段

任務中的任務分為一或多個工作階段。工作者會執行工作階段來設定環境、執行任務，然後清除環境。每個工作階段都由工作者必須採取的一或多個動作組成。

當工作者完成區段動作時，可以將其他工作階段動作傳送給工作者。工作者會重複使用工作階段中的現有環境和任務附件，以更有效率地完成任務。

任務附件是由您做為截止日期雲端 CLI 任務套件一部分的提交者建立。您也可以使用 create-job AWS CLI 命令--attachments的選項來建立任務附件。環境定義有兩個位置：連接到特定佇列的佇列環境，以及任務範本中定義的任務和步驟環境。

有四種工作階段動作類型：

- syncInputJobAttachments – 將輸入任務附件下載至工作者。
- envEnter – 執行環境onEnter的動作。
- taskRun – 執行任務onRun的動作。
- envExit – 執行環境onExit的動作。

下列任務範本具有步驟環境。它具有設定步驟環境onEnter的定義、定義要執行之任務onRun的定義，以及淘汰步驟環境onExit的定義。為此任務建立的工作階段將包含 envEnter動作、一或多個taskRun動作，然後包含 envExit動作。

```
name: Sample Job with Maya Environment
specificationVersion: jobtemplate-2023-09
steps:
- name: Maya Step
  stepEnvironments:
  - name: Maya
    description: Runs Maya in the background.
    script:
      embeddedFiles:
      - name: initData
        filename: init-data.yaml
        type: TEXT
        data: |
          scene_file: MyAwesomeSceneFile
          renderer: arnold
          camera: persp
```

```
      actions:
        onEnter:
          command: MayaAdaptor
          args:
          - daemon
          - start
          - --init-data
          - file://{{Env.File.initData}}
        onExit:
          command: MayaAdaptor
          args:
          - daemon
          - stop
  parameterSpace:
    taskParameterDefinitions:
    - name: Frame
      range: 1-5
      type: INT
  script:
    embeddedFiles:
    - name: runData
      filename: run-data.yaml
      type: TEXT
      data: |
        frame: {{Task.Param.Frame}}
    actions:
      onRun:
        command: MayaAdaptor
        args:
        - daemon
        - run
        - --run-data
        - file://{{ Task.File.runData }}
```

步驟相依性

期限 雲端支援在步驟之間定義相依性，讓一個步驟等待另一個步驟完成再開始。您可以為步驟定義多個相依性。在所有相依性完成之前，不會排程具有相依性的步驟。

如果任務範本定義循環相依性，則會拒絕任務，並將任務狀態設定為 CREATE_FAILED。

下列任務範本會建立具有兩個步驟的任務。 StepB 取決於 StepA。 StepB只會在 StepA 成功完成之後執行。

建立任務後， StepA 處於 READY 狀態，且 StepB 處於 PENDING 狀態。StepA 完成後， StepB會移至 READY 狀態。如果StepA失敗，或StepA如果 已取消， StepB會移至 CANCELED 狀態。

您可以設定多個步驟的相依性。例如，如果 同時StepC取決於 StepA和 StepB，則在其他兩個步驟完成之前， StepC不會開始。

```
name: Step-Step Dependency Test
specificationVersion: 'jobtemplate-2023-09'
steps:
- name: A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail

          sleep 1
          echo Task A Done!
- name: B
  dependencies:
  - dependsOn: A # This means Step B depends on Step A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail

          sleep 1
          echo Task B Done!
```

截止日期雲端中的任務狀態

本主題說明如何使用 AWS 截止日期雲端命令列界面 （ 截止日期雲端 CLI) 來檢視任務或步驟的狀態。若要使用截止日期雲端監視器來檢視任務或步驟的狀態，請參閱 在截止日期雲端中管理任務、步驟和任務。

您也可以為預設 Amazon EventBridge 事件匯流排建立規則，將事件傳送至目標，例如 Amazon Simple Notification Service，以在任務、步驟或任務變更狀態時傳送簡訊或電子郵件。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 EventBridge 管理截止日期雲端事件。

您可以使用`deadline job get --job-id`截止日期雲端 CLI 命令查看任務的狀態。對命令的回應包括任務或步驟的狀態，以及每個處理狀態中的任務數量。

當您第一次提交任務時，狀態為 `CREATE_IN_PROGRESS`。如果任務通過驗證檢查，其狀態會變更為 `CREATE_COMPLETE`。如果沒有，狀態會變更為 `CREATE_FAILED`。

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。

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。

也可能發生內部服務錯誤，導致無法建立任務。如果發生這種情況，任務的狀態碼為 `INTERNAL_ERROR`，狀態訊息欄位會提供更詳細的說明。

使用下列截止日期雲端 CLI 命令來檢視任務的詳細資訊。在下列範例中，將 取代*jobID*為您自己的資訊：

```
deadline job get --job-id jobId
```

來自 `deadline job get`命令的回應如下所示：

```
jobId: jobId
name: Sample Job
lifecycleStatus: CREATE_COMPLETE
```

```
lifecycleStatusMessage: Job creation completed successfully
priority: 50
createdAt: 2024-03-26 18:11:19.065000+00:00
createdBy: Test User
startedAt: 2024-03-26 18:12:50.710000+00:00
taskRunStatus: STARTING
taskRunStatusCounts:
  PENDING: 0
  READY: 5
  RUNNING: 0
  ASSIGNED: 0
  STARTING: 0
  SCHEDULED: 0
  INTERRUPTING: 0
  SUSPENDED: 0
  CANCELED: 0
  FAILED: 0
  SUCCEEDED: 0
  NOT_COMPATIBLE: 0
maxFailedTasksCount: 100
maxRetriesPerTask: 5
```

任務或步驟中的每個任務都有一個狀態。任務狀態會合併，以提供任務和步驟的整體狀態。每個狀態中的任務數量都會在回應的 taskRunStatusCounts 欄位中報告。

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。

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。環境，如果有的話，已設定。

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其他資源的可用性。

SUCCEEDED

任務中的所有任務都已成功處理。

在截止日期雲端中修改任務

您可以使用下列 AWS Command Line Interface (AWS CLI) update命令來修改任務組態，或設定任務、步驟或任務的目標狀態：

- aws deadline update-job
- aws deadline update-step
- aws deadline update-task

在下列 update命令範例中，將每個 取代*user input placeholder*為您自己的資訊。

您也可以使用截止日期雲端監視器來修改任務的組態。如需詳細資訊，請參閱在截止日期雲端中管理任務、步驟和任務。

Example – 將任務排入佇列

除非有步驟相依性，否則任務中的所有任務都會切換到 READY 狀態。具有相依性的步驟會在還原PENDING時切換到 READY或 。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status PENDING
```

Example – 取消任務

任務中沒有 狀態SUCCEEDED或FAILED標記為 的所有任務CANCELED。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status CANCELED
```

Example – 標記任務失敗

任務中狀態為 的所有任務SUCCEEDED保持不變。所有其他任務都會標示為 FAILED。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status FAILED
```

Example – 成功標記任務

任務中的所有任務都會移至 SUCCEEDED 狀態。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
```

```
--job-id jobID \
--target-task-run-status SUCCEEDED
```

Example – 暫停任務

SUCCEEDED、 CANCELED或 FAILED 狀態的任務不會變更。所有其他任務都會標示為 SUSPENDED。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status SUSPENDED
```

Example – 變更任務的優先順序

更新佇列中任務的優先順序，以變更排程任務的順序。較高優先順序的任務通常會先排程。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--priority 100
```

Example – 變更允許的失敗任務數量

在取消其餘任務之前，更新任務可以擁有的失敗任務數量上限。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-failed-tasks-count 200
```

Example – 變更允許的任務重試次數

在任務失敗之前，更新任務的重試次數上限。在增加此值之前，無法重新排入佇列已達重試次數上限的任務。

```
aws deadline update-job \
--farm-id farmID \
```

```
--queue-id queueID \
--job-id jobID \
--max-retries-per-task 10
```

Example – 封存任務

將任務的生命週期狀態更新為 ARCHIVED。封存的任務無法排程或修改。您只能封存處於 FAILED、SUCCEEDED、 CANCELED或 SUSPENDED 狀態的任務。

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--lifecycle-status ARCHIVED
```

Example – 將步驟排入佇列

除非有步驟相依性，否則步驟中的所有任務都會切換到 READY 狀態。具有相依性的步驟中的任務會切換到 READY或 PENDING，並還原任務。

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status PENDING
```

Example – 取消步驟

步驟中沒有 狀態SUCCEEDED或FAILED標記為 的所有任務CANCELED。

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status CANCELED
```

Example – 標記步驟失敗

具有 狀態的步驟中的所有任務SUCCEEDED保持不變。所有其他任務都會標示為 FAILED。

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status FAILED
```

Example – 成功標記步驟

步驟中的所有任務都會標示為 SUCCEEDED。

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUCCEEDED
```

Example – 暫停步驟

SUCCEEDED、 CANCELED或 FAILED 狀態中步驟中的任務不會變更。所有其他任務都會標示為 SUSPENDED。

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUSPENDED
```

Example – 變更任務的狀態

當您使用update-task截止日期雲端 CLI 命令時，任務會切換到指定的狀態。

```
aws deadline update-task \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--task-id taskID \
```

```
--target-task-run-status SUCCEEDED | SUSPENDED | CANCELED | FAILED | PENDING
```

期限 雲端如何處理任務

為了處理任務， AWS 截止日期 Cloud 使用開放任務描述 (OpenJD) 任務範本來判斷所需的資源。期限雲端會從與您的佇列相關聯的機群中，為步驟選取合適的工作者。選取的工作者符合步驟所需的所有功能屬性。

接下來，截止日期 Cloud 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。如果機群的擴展設定具有容量，則服務可以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 範本來判斷任務所需的步驟，以及每個步驟所需的任務。某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進行處理。當任務完成時，服務會在相同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。

您可以在截止日期雲端監視器、截止日期雲端命令列界面 （ 截止日期雲端 CLI) 或 中追蹤任務進度 AWS CLI。如需使用監視器的詳細資訊，請參閱 使用截止日期雲端監視器。如需使用截止日期雲端 CLI 的詳細資訊，請參閱截止日期雲端中的任務狀態。

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，完成的每個步驟和任務的輸出仍可下載。

截止日期 雲端會在提交任務的 120 天後移除任務。移除任務時，與任務相關聯的所有步驟和任務也會一併移除。如果您需要重新執行任務，請再次提交任務的 OpenJD 範本。

建立任務的資源限制

提交至截止期限雲端的任務可能取決於多個任務之間共用的資源。例如，相較於針對特定資源的浮動授權，一個陣列可能有更多工作者。或者，共用檔案伺服器可能只能同時將資料提供給數量有限的工作者。在某些情況下，一或多個任務可以申請所有這些資源，導致新工作者啟動時資源無法使用而造成錯誤。

為了協助解決此問題，您可以使用這些受限資源的限制。期限 雲端會考慮限制資源的可用性，並使用該資訊來確保資源在新工作者啟動時可用，因此任務因資源無法使用而失敗的可能性較低。

限制會針對整個陣列建立。提交至佇列的任務只能取得與佇列相關聯的限制。如果您為未與佇列相關聯的任務指定限制，則該任務不相容且無法執行。

若要使用限制，您可以

- 建立限制
- 關聯限制和佇列
- 提交需要限制的任務

> **Note**
>
> 如果您執行的任務在佇列中具有與限制無關的資源限制，則該任務可能會消耗所有資源。如果您有限制的資源，請確定佇列中使用該資源的任務中的所有步驟都與限制相關聯。

對於在陣列中定義、與佇列相關聯，以及在任務中指定的限制，可能會發生以下四種情況之一：

- 如果您建立限制，將其與佇列建立關聯，並在任務的範本中指定限制，任務會執行並僅使用限制中定義的資源。
- 如果您建立限制，請在任務範本中指定該限制，但不要將限制與佇列建立關聯，任務會標記為不相容，且不會執行。
- 如果您建立限制，請勿將其與佇列建立關聯，也不要在任務的範本中指定限制，任務會執行，但不會使用限制。
- 如果您完全不使用限制，任務會執行。

如果您將限制與多個佇列建立關聯，佇列會共用限制限制的資源。例如，如果您建立 100 個限制，且一個佇列使用 60 個資源，則其他佇列只能使用 40 個資源。釋出資源時，任務可以從任何佇列取得。

期限雲端提供兩個 AWS CloudFormation 指標，協助您監控限制提供的資源。您可以監控目前使用中的資源數量，以及限制中可用的資源數量上限。如需詳細資訊，請參閱 截止日期雲端開發人員指南中的資源限制指標。

您可以將限制套用至任務範本中的任務步驟。當您在`hostRequirements`步驟 的 `amounts`區段中指定限制的數量需求名稱，且具有相同限制的限制與任務的佇列`amountRequirementName`相關聯時，為此步驟排程的任務會受到資源限制的限制。

如果步驟需要限制達到限制的資源，則該步驟中的任務將不會由其他工作者取得。

您可以將多個限制套用至任務步驟。例如，如果步驟使用兩個不同的軟體授權，您可以為每個授權套用個別的限制。如果步驟需要兩個限制，且其中一個資源達到限制，則在該步驟中的任務將不會被其他工作者提取，直到資源可用為止。

停止和刪除限制

當您停止或刪除佇列與限制之間的關聯時，使用限制的任務會從需要此限制的步驟停止排程任務，並封鎖為步驟建立新工作階段。

處於就緒狀態的任務會保持就緒狀態，且任務會自動繼續與佇列和限制之間的關聯，再次變為作用中。您不需要重新排入任何任務的佇列。

當您停止或刪除佇列與限制之間的關聯時，有兩種選擇可讓您停止執行中的任務：

- 停止和取消任務 – 具有取得限制的工作階段的工作者會取消所有任務。
- 停止並完成執行中的任務 – 具有取得限制之工作階段的工作者完成其任務。

當您使用主控台刪除限制時，工作者會先停止執行任務，或在任務完成時最終停止執行。刪除關聯時，會發生以下情況：

- 需要限制的步驟標示為不相容。
- 包含這些步驟的整個任務都會取消，包括不需要限制的步驟。
- 任務標示為不相容。

如果與限制相關聯的佇列具有與限制數量需求名稱相符的機群功能，該機群將繼續處理具有指定限制的任務。

建立限制

您可以使用截止日期雲端主控台或截止日期雲端 API 中的 CreateLimit 操作來建立限制。限制是為陣列定義，但與佇列相關聯。建立限制之後，您可以將其與一或多個佇列建立關聯。

建立限制

1. 從截止日期雲端主控台 (https://console.aws.amazon.com/deadlinecloud/home) 儀表板中，選取您要為其建立佇列的陣列。
2. 選擇要新增限制的陣列，選擇限制索引標籤，然後選擇建立限制。

3. 提供限制的詳細資訊。金額需求名稱是任務範本中用來識別限制的名稱。它必須以字首開頭，**amount.**後面接著金額名稱。在與限制相關聯的佇列中，數量需求名稱必須是唯一的。
4. 如果您選擇設定最大數量，即此限制允許的資源總數。如果您選擇無最大數量，則資源用量不受限制。即使資源用量不受限制，也會發出 `CurrentCount` Amazon CloudWatch 指標，以便您可以追蹤用量。如需詳細資訊，請參閱 截止日期雲端開發人員指南中的 CloudWatch CloudWatch 指標。
5. 如果您已經知道應使用限制的佇列，現在可以選擇它們。您不需要建立佇列的關聯，即可建立限制。
6. 選擇建立限制。

關聯限制和佇列

建立限制之後，您可以將一或多個佇列與限制建立關聯。只有與限制相關聯的佇列才會使用限制中指定的值。

您可以使用截止日期雲端主控台或截止日期雲端 API 中的 CreateQueueLimitAssociation 操作建立與佇列的關聯。

將佇列與限制建立關聯

1. 從截止日期雲端主控台 (https://console.aws.amazon.com/deadlinecloud/home) 儀表板中，選取您要將限制與佇列建立關聯的陣列。
2. 選擇限制索引標籤，選擇要與佇列建立關聯的限制，然後選擇編輯限制。
3. 在關聯佇列區段中，選擇要與限制建立關聯的佇列。
4. 選擇 Save changes (儲存變更)。

提交需要限制的任務

您可以將限制指定為任務或任務步驟的主機需求，以套用限制。如果您未在步驟中指定限制，且該步驟使用相關聯的資源，則在排程任務時，該步驟的用量不會計入限制。

有些截止日期雲端提交者可讓您設定主機需求。您可以在提交者中指定限制的金額需求名稱，以套用限制。

如果您的提交者不支援新增主機需求，您也可以編輯任務的任務範本來套用限制。

將限制套用至任務套件中的任務步驟

1. 使用文字編輯器開啟任務的任務範本。任務範本位於任務的任務套件目錄中。如需詳細資訊，請參閱 截止日期雲端開發人員指南中的任務套件。
2. 尋找要套用限制之步驟的步驟定義。
3. 將下列項目新增至步驟定義。將 *amount.name* 取代為您限制的金額需求名稱。對於一般用途，您應該將min值設定為 1。

   YAML

   ```
   hostRequirements:
     amounts:
     - name: amount.name
       min: 1
   ```

   JSON

   ```
   "hostRequirements": {
       "amounts": [
           {
               "name": "amount.name",
               "min": "1"
           }
       ]
   }
   ```

   您可以在任務步驟中新增多個限制，如下所示。將 *amount.name_1* 和 *amount.name_2* 取代為您限制的數量需求名稱。

   YAML

   ```
   hostRequirements:
     amounts:
     - name: amount.name_1
       min: 1
     - name: amount.name_2
       min: 1
   ```

JSON

```
"hostRequirements": {
    "amounts": [
        {
            "name": "amount.name_1",
            "min": "1"
        },
        {
            "name": "amount.name_2",
            "min": "1"
        }
    }
}
```

4. 將變更儲存至任務範本。

期限雲端的檔案儲存

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 期限 雲端提供儲存位置的兩個選項：

- 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。

  當您搭配服務受管機群使用任務附件時，您可以在虛擬私有網路 (VPN) 中設定虛擬檔案系統 (VFS)。然後，工作者只能在需要時載入檔案。
- 透過共用儲存，您可以使用與作業系統共用的檔案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。

主題

截止日期雲端中的任務附件

任務附件可讓您在工作站和 AWS 截止日期雲端之間來回傳輸檔案。透過任務附件，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至截止日期雲端。對於後續提交，只會傳輸已變更的檔案，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 儲存貯體加密

根據預設，任務連接檔案會在 S3 儲存貯體中加密。這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，即可使用截止日期雲端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 Management Console 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，選擇要修改之佇列所在的陣列。
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:Region:accountID:key/keyID"
   ]
}
```

5. 選擇 Next (下一步)。

6. 檢閱政策的變更，然後在您滿意時，選擇儲存變更。

管理 S3 儲存貯體中的任務附件

期限 雲端會將任務所需的任務連接檔案存放在 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 S3 儲存貯體中的物件過期。如需詳細資訊，請參閱根據上次存取日期過期的 Amazon S3 物件，以降低架構部落格的成本 AWS 。

期限 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。檔案存放在本機。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可顯示最大利益。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`、`appendtruncate`、`rename`、、`move`、`copy`、、
    `stat` `fsync`和 `falloc`
  - 目錄 `create`、`delete`、`rename`、`move`、 `copy`和 `stat`
- 虛擬檔案系統旨在減少資料傳輸並改善當您的任務僅存取部分大型資料集時的效能，而且並非所有工作負載都最佳化。您應該在執行生產任務之前測試工作負載。

啟用 VFS 支援

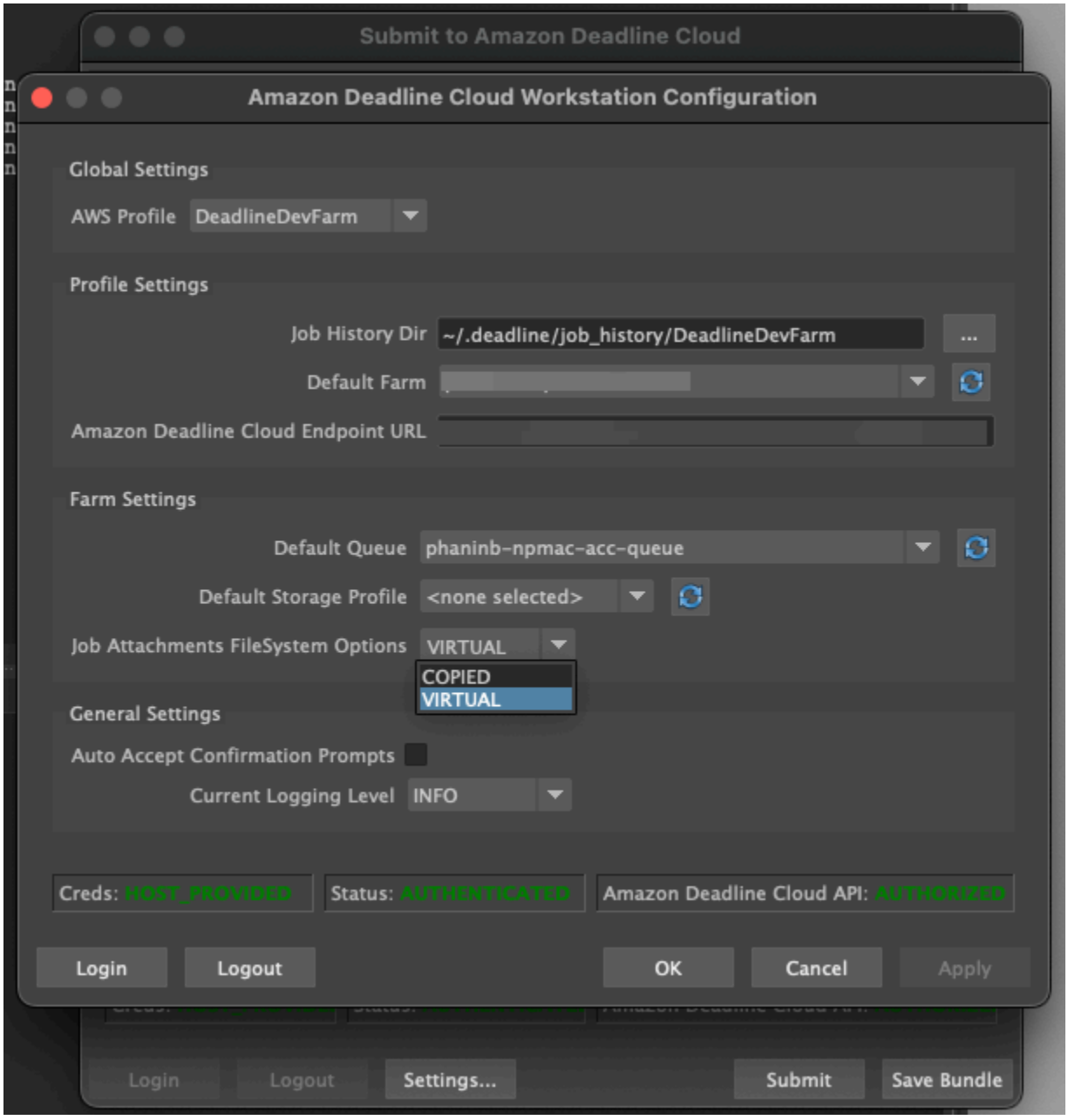
為每個任務啟用虛擬檔案系統支援 (VFS)。在這些情況下，任務會回復為預設任務附件架構：

- 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. 從任務附件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
```

若要驗證虛擬檔案系統是否針對特定任務成功啟動，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的日誌。如需說明，請參閱 在截止日期雲端中檢視日誌。

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。

追蹤截止日期雲端陣列的支出和用量

AWS Deadline Cloud 預算管理員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 服務時所欠的金額。

為了協助您管理期限雲端的成本，您可以使用下列功能：

- 預算管理工具 – 使用截止日期雲端預算管理工具，您可以建立和編輯預算，以協助管理專案成本。
- 用量總管：使用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。

成本假設

期限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)
```

- 執行時間是任務中從開始時間到結束時間的所有任務的總和。
- 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。

截止期限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 AWS 或其他雲端供應商，或從外部攜帶您自己的資源。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。您可能有資格獲得估算值以外的其他折扣。
- 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員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員的步驟。

主題

先決條件

若要使用截止日期雲端預算管理員，您必須具有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員

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 Management Console 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 Management Console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您要為其建立預算的佇列。
6. 針對期間，請完成下列步驟，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. 針對結束日期，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，然後選取日期。

    預設結束日期為開始日期後 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，您可以實作當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：

      - 完成目前工作後停止 – 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。您可以在該處檢視預算的總金額，以及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 Management Console，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。隨即出現 Budget Manager 頁面。
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 Management Console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 Budget Manager 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 Management Console開啟截止日期雲端主控台，選擇陣列，然後選擇管理任務。
2. 在預算管理工具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

截止日期 雲端會使用 Amazon EventBridge 將預算相關事件傳送到您的預設 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，以便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。這可協助您掌握支出，並在預算用盡之前做出明智的決策。

截止日期 雲端會定期彙總每個轉譯陣列的使用和成本資料。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緊密。這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，Cloud 會傳送事件。預算達到 100% 後，截止日期 Cloud 會停止傳送事件。如果您調整預算，截止期限 Cloud 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 Amazon Relational Database Service 資料庫以供記錄。

如需 EventBridge 規則的範例，請參閱下列主題：

- 使用 Amazon EventBridge 發生事件時傳送電子郵件。
- 建立 Amazon EventBridge 規則，在聊天應用程式中將通知傳送給 Amazon Q 開發人員。
- 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已到達事件。

使用截止日期雲端用量瀏覽器追蹤用量和成本

使用截止期限雲端用量總管，您可以查看每個陣列上發生之活動的即時指標。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期間的用量，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。

下列各節會為您說明存取和使用截止日期雲端用量瀏覽器的步驟。

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，您必須具有 MANAGER或 OWNER 陣列許可。如需詳細資訊，請參閱管理陣列、佇列和機群的使用者和群組。

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 Management Console 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

在用量總管頁面中，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、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。您可以縮小查詢範圍，以減少結果數量：

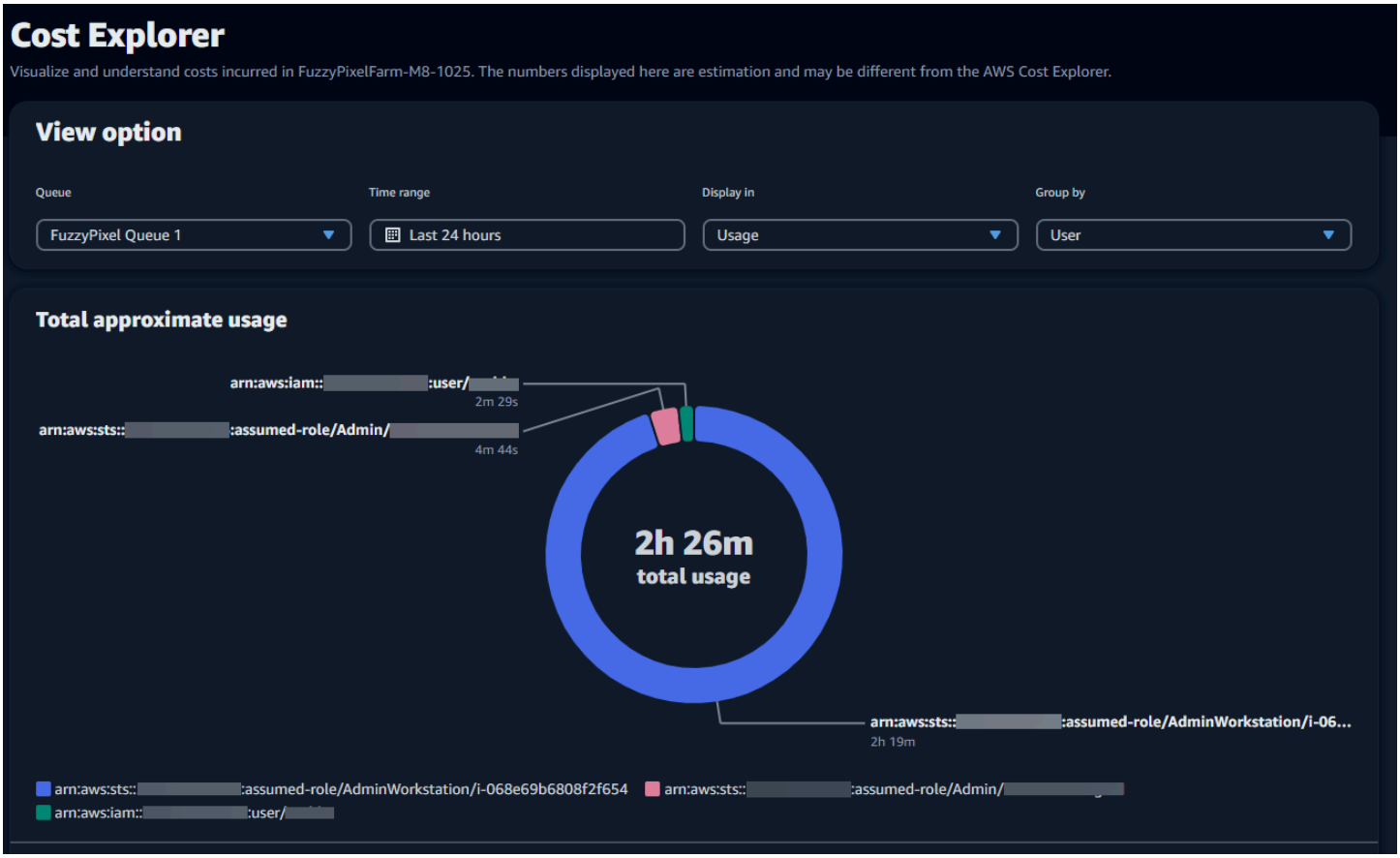
- 選取較小的時間範圍
- 選取較少佇列
- 選取不同的分組，例如依佇列分組而非任務

主題

使用視覺化圖形來檢閱資料

您可以檢視視覺化格式的資料，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，並可選擇將總數分組為較小的小計。

> **Note**
>
> 圖表只會顯示前五個結果，並在「其他」區段中合併其他結果。您可以在圖表下方的明細區段中檢視所有結果。



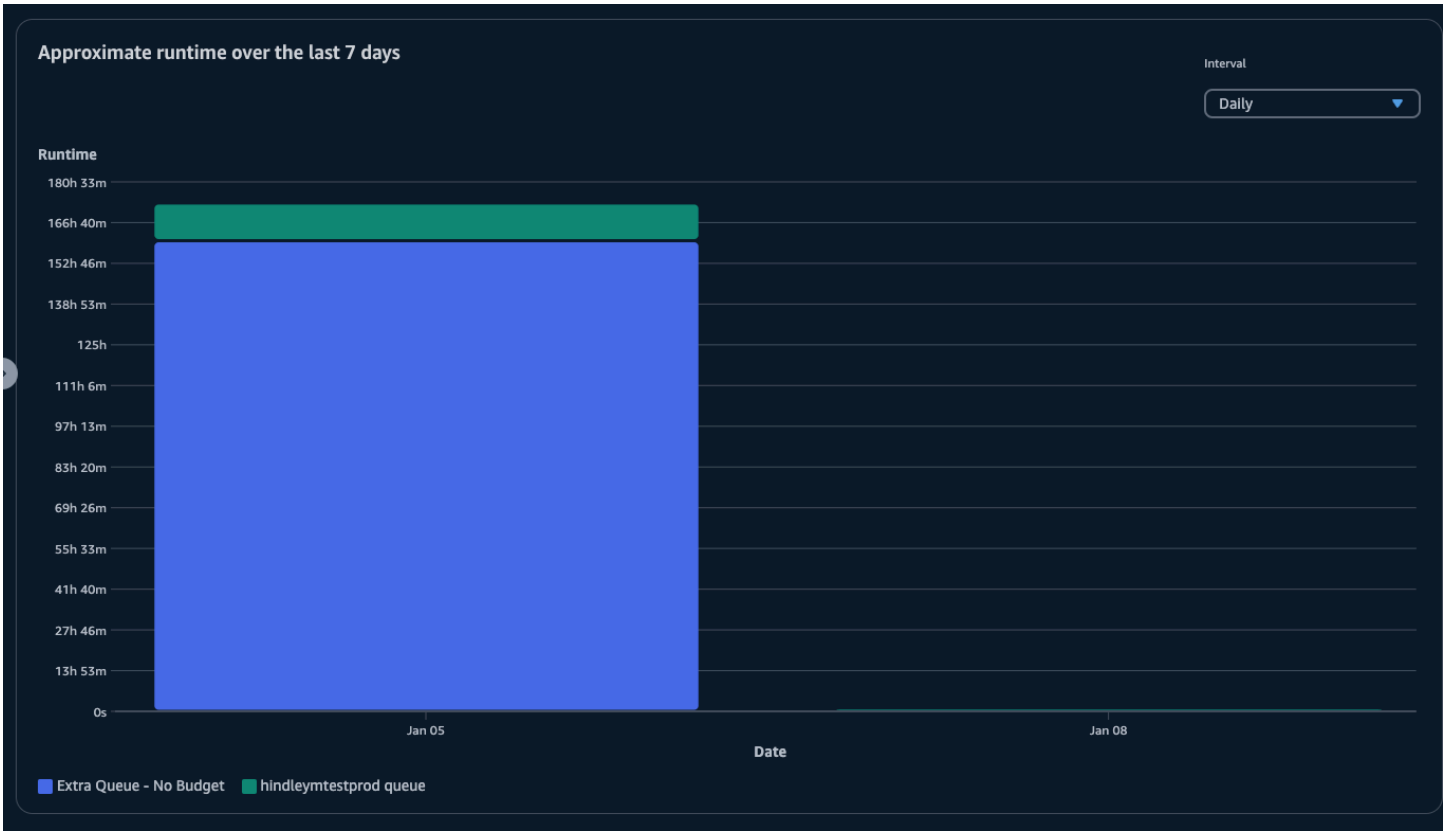
檢視指標的明細

在圓餅圖下方，用量總管提供特定指標的更詳細明細，這將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。

依預設，將細項降至最低。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 期限 雲端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 Cloud 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
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期限雲端時的成本，以及您可以在成本和效率之間取得的權衡。

> **Note**
>
> 使用截止日期雲端的最終成本取決於多項 AWS 服務之間的互動、您處理的工作量，以及您執行任務 AWS 區域 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。這可以減少期限雲端開始處理任務所需的時間量，但您需要支付執行個體閒置時間的費用。
- 對於服務受管機群，設定機群的大小上限。這限制了機群可以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，但可以縮短完成工作的時間。了解任務在執行個體上放置的需求，有助於降低成本。

- 如果可能，為您的機群選擇 Amazon EC2 Spot 執行個體。Spot 執行個體以較低的價格提供，但可能會因為隨需請求而中斷。隨需執行個體會依秒計費，不會中斷。

的最佳實務 AWS KMS

根據預設，截止日期雲端會使用 AWS 擁有的金鑰來加密您的資料。您不需要支付此金鑰的費用。

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，系統會根據金鑰的使用方式向您收取費用。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 和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。您建立的每個端點每小時都會收費。如果您使用 PrivateLink，則必須至少建立三個端點，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

期限 雲端使用 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，這是在帳戶中建立的 Amazon VPC 端點。此端點以小時費率計費。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 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。

安全是 AWS 和 之間的共同責任。共同責任模型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。第三方稽核人員會定期測試和驗證我們安全的有效性，做為AWS 合規計畫的一部分。若要了解適用的合規計劃 AWS Deadline Cloud，請參閱AWS 服務 合規計劃範圍內的
- 雲端安全性 – 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 時套用共同的責任模型 Deadline Cloud。下列主題說明如何設定 Deadline Cloud 以符合您的安全和合規目標。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 使用介面端點 (AWS PrivateLink) 存取
- 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 的全域基礎設施 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 共同的責任模型和 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 或其他 AWS 服務 使用主控台、API AWS CLI或 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

AWS Deadline Cloud 使用存放在 AWS Key Management Service (AWS KMS) 中的加密金鑰，透過靜態加密來保護敏感資料。靜態加密可在所有 Deadline Cloud 可用 AWS 區域 的地方使用。

加密資料表示使用者或應用程式如果沒有有效的金鑰，就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。

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 擁有金鑰。
- 客戶受管 KMS 金鑰 – 您可以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，由您建立、擁有和管理，並收取 AWS KMS 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 來代表您 Deadline Cloud 建立授予 AWS KMS ，以存取您指定的 KMS 金鑰。

Deadline Cloud 使用多個授與。每個授權都會由 Deadline Cloud 需要加密或解密您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。

准許 Deadline Cloud 管理服務受管機群中的機器， Deadline Cloud 包括 中的帳戶號碼和角色，GranteePrincipal而不是服務主體。雖然不是典型的，但這是使用陣列指定的客戶受管 KMS 金鑰加密服務受管機群中工作者的 Amazon EBS 磁碟區所必需。

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。每個金鑰必須只有一個金鑰政策，其中包含可決定誰可以使用金鑰的陳述式，以及他們可以如何使用它。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，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予。
- 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。

```
{
    "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。

```
{
    "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

使用客戶受管金鑰進行讀寫 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。

```
{
    "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，通常會在您呼叫 CreateFarm、 CreateMonitor或 CreateFleet操作時，發生下列 CloudTrail 事件範例。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T02:05:26Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T02:05:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "operations": [
            "CreateGrant",
            "Decrypt",
            "DescribeKey",
            "Encrypt",
            "GenerateDataKey"
        ],
        "constraints": {
```

```
            "encryptionContextSubset": {
                "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
                "aws:deadline:accountId": "111122223333"
            }
        },
        "granteePrincipal": "deadline.amazonaws.com",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "retiringPrincipal": "deadline.amazonaws.com"
    },
    "responseElements": {
        "grantId": "6bbe819394822a400fe5e3a75d0e9ef16c1733143fff0c1fc00dc7ac282a18a0",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE44444"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

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": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:51:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeffffff",
    "eventID": "ffffffff-eeee-dddd-cccc-bbbbbbaaaaaa",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

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": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "encryptionContext": {
```

```
            "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "keyId": "arn:aws::kms:us-
west-2:111122223333:key/abcdef12-3456-7890-0987-654321fedcba"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


刪除客戶受管 KMS 金鑰

在 AWS Key Management Service (AWS KMS) 中刪除客戶受管的 KMS 金鑰具有破壞性且可能危險。它會不可逆地刪除與金鑰相關聯的金鑰材料和所有中繼資料。刪除客戶受管 KMS 金鑰後，您無法再解密該金鑰加密的資料。這表示資料無法復原。

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，因此我們會要求您設定 7–30 天的等待期。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 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 AWS KMS 主控台中，於一般組態區段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 金鑰的後端金鑰。

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 提供功能，可讓您用來提高和監控虛擬私有雲端 (VPC) 的安全性。

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 來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。

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。我們也收集 Deadline Cloud 特定資訊，例如資源 IDs(FarmID 或 QueueID，如適用）、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。 Deadline Cloud與用戶端工作站和機群工作者互動的每個電腦都需要分別選擇退出。

Deadline Cloud Monitor - 桌面

Deadline Cloud monitor - 桌面會收集操作資訊，例如當當當機時和應用程式開啟時，以協助我們了解應用程式何時發生問題。若要選擇退出此操作資訊的收集，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。

在您選擇退出後，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，例如當當當機時，以及當任務提交時，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，這將選擇退出 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 AWS 服務 您可以免費使用的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在截止日期雲端中所做的工作。

服務使用者 – 如果您使用截止日期雲端服務來執行您的任務，則您的管理員會為您提供所需的登入資料和許可。當您使用更多截止日期雲端功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取截止日期雲端中的功能，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 – 如果您在公司負責期限雲端資源，您可能可以完整存取期限雲端。您的任務是判斷您的服務使用者應存取哪些最終雲端功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與截止日期雲端搭配使用，請參閱截止日期雲端如何與 IAM 搭配使用。

IAM 管理員 - 如果您是 IAM 管理員，建議您了解撰寫政策以管理截止日期雲端存取的詳細資訊。若要檢視您可以在 IAM 中使用的以雲端身分為基礎的政策範例，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 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

視您身分的使用者類型而定，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

AWS 帳戶 根使用者

當您建立 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。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。

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務 來使用與身分提供者的聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或 AWS 服務 是透過身分來源提供的登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色 （主控台）。

您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。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。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。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權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是一種連結至 的服務角色。 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的

程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到 AWS 身分或資源 AWS 來控制 中的存取。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）提出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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。

預設情況下，使用者和角色沒有許可。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 API AWS 取得角色資訊。

身分型政策

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。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 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。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是用於分組和集中管理您企業擁有 AWS 帳戶 之多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，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) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。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

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種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。

截止日期雲端如何與 IAM 搭配使用

在您使用 IAM 管理截止日期雲端的存取權之前，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
暫時性憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	否

若要取得 Deadline Cloud 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用的高階檢視，請參閱《IAM 使用者指南》中的AWS 與 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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。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，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。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。

期限雲端的政策動作

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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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。

截止日期雲端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。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。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。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定的條件金鑰。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，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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)。

使用臨時登入資料搭配截止日期雲端

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的 使用 IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的從使用者切換至 IAM 角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 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 中的暫時性安全憑證。

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

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷期限雲端功能。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 的服務角色類型 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。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，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。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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)。

如需截止期限雲端定義之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 截止期限雲端的動作、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
- 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

以身分為基礎的政策會判斷是否有人可以建立、存取或刪除您帳戶中的截止日期雲端資源。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 AWS 受管政策來授予許多常見使用案例的許可。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 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS 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 以增加安全性。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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html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期限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。

對於僅對 AWS CLI 或 AWS API 進行呼叫的使用者，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。

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，授予將任務提交至特定陣列中特定佇列的許可。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SubmitJobsFarmAndQueue",
            "Effect": "Allow",
            "Action": "deadline:CreateJob",
            "Resource": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_A/queue/QUEUE_B/
job/*"
        }
    ]
}
```

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。使用此政策來建立與陣列相關聯的 VPC 的授權端點。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "SID": "CreateLicenseEndpoint",
        "Effect": "Allow",
        "Action": [
            "deadline:CreateLicenseEndpoint",
            "deadline:DeleteLicenseEndpoint",
            "deadline:GetLicenseEndpoint",
            "deadline:UpdateLicenseEndpoint",
            "deadline:ListLicenseEndpoints",
            "deadline:PutMeteredProduct",
            "deadline:DeleteMeteredProduct",
            "deadline:ListMeteredProducts",
            "deadline:ListAvailableMeteredProducts",
            "ec2:CreateVpcEndpoint",
            "ec2:DescribeVpcEndpoints",
            "ec2:DeleteVpcEndpoints"
        ],
        "Resource": "*"
    }]
}
```

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。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "MonitorJobsFarmAndQueue",
        "Effect": "Allow",
        "Action": [
            "deadline:SearchJobs",
            "deadline:ListJobs",
            "deadline:GetJob",
            "deadline:SearchSteps",
            "deadline:ListSteps",
            "deadline:ListStepConsumers",
            "deadline:ListStepDependencies",
            "deadline:GetStep",
            "deadline:SearchTasks",
            "deadline:ListTasks",
            "deadline:GetTask",
            "deadline:ListSessions",
            "deadline:GetSession",
            "deadline:ListSessionActions",
            "deadline:GetSessionAction"
        ],
        "Resource": [
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B",
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B/*"
        ]
    }]
}
```

AWS 截止日期雲端的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，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。我們建議您定義使用案例專屬的客戶管理政策，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 受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（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政策連接至您的 AWS Identity and Access Management (IAM) 身分。

此政策會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 – 允許主體建立工作者。

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。

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。

此政策可讓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，針對截止日期雲端的 AWS 受管政策更新的詳細資訊。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	日期
AWSDeadlineCloud-UserAccessFarms – 變更 AWSDeadlineCloud-UserAccessJobs – 變更 AWSDeadlineCloud-UserAccessQueues – 變更	截止日期 雲端新增了 動作deadline:GetJobTemplate deadline:ListJobParameterDefinitions ，並允許您重新提交任務。	2024 年 10 月 7 日

變更	描述	日期
Cloud 開始追蹤變更的截止日期	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

對 AWS 截止日期雲端身分和存取進行故障診斷

使用下列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，表示您無權執行iam:PassRole動作，則必須更新您的政策，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 沒有將角色傳遞至該服務的許可。

```
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 截止日期雲端如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個資源中提供存取權給 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》中的提供存取權給第三方 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 在特定合規計劃的範圍內，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 Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。

- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明保護 的最佳實務，AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

中的彈性 Deadline Cloud

AWS 全域基礎設施是以 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 期限雲端受到 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的最佳實務設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的 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。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

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 期限 雲端管理服務受管或客戶受管機群的任務：

- 對於服務受管機群，Deadline Cloud 會管理訪客作業系統。
- 對於客戶管理的機群，您需負責管理作業系統。

如需 AWS 截止期限雲端組態和漏洞分析的詳細資訊，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。

下列範例示範如何使用 中的 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。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "deadline.amazonaws.com"
    },
    "Action": "deadline:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:deadline:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

AWS Deadline Cloud 使用介面端點 (AWS PrivateLink) 存取

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 連線或 AWS 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。

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 Deadline Cloud 透過介面端點控制流量至 。

Deadline Cloud 不支援 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對 VPC 端點的存取。

Deadline Cloud 端點

Deadline Cloud 使用兩個端點來存取使用 的服務 AWS PrivateLink。

工作者使用 `com.amazonaws.region.deadline.scheduling`端點從佇列取得任務、向 報告進度 Deadline Cloud，以及向後傳送任務輸出。如果您使用的是客戶受管機群，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來呼叫 `CreateJob`操作。

Deadline Cloud 監視器使用 `com.amazonaws.region.deadline.management`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。

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 中的臨時安全登入資料。
- 如果您在沒有網際網路連線的子網路中設定客戶管理的機群，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##取代為您部署 AWS 區域 的 Deadline Cloud。

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

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

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，`worker.deadline.us-east-1.amazonaws.com`對於工作者操作，或`management.deadline.us-east-1.amazonaws.com`對於所有其他操作。

您還必須使用 AWS STS 下列服務名稱建立 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，您必須使用以下服務名稱建立 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
```

截止日期雲端的安全最佳實務

AWS 期限雲端 （期限雲端） 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。這包括當您使用 AWS 截止日期雲端，或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務時。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擁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。機群會定義基礎設施（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

佇列的任務存取。指定使用者或群組有助於保護任務中的資料免受其他佇列、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，該使用者可模擬 (sudo) 任何佇列使用者。如此一來，沒有使用者的佇列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路由的方式和位置。

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，請安全地存取 Route 53 API。
- 如果您使用內部部署工作站或其他資料中心，在 AWS 之外連線到截止日期雲端，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 伺服器和路由表。

任務和任務資料

截止日期 雲端任務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期限雲資源，包括機群、佇列和儲存設定檔。不過，您可以在陣列內共用外部 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。

  - 無論提交任務的佇列為何，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 中的資源保護到邊界。

任務連接佇列

任務附件與佇列相關聯，佇列使用 Amazon S3 儲存貯體。

- 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 可以使用與 QueueA 相同的儲存貯體和根字首來存取 QueueB 資料。

主控台會設定預設安全的佇列。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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
```

```
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME",
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME/JOB_ATTACHMENTS_ROOT_PREFIX/*"
      ],
      "Condition": {
        "StringEquals": { "aws:ResourceAccount": "ACCOUNT_ID" }
      }
    },
    {
      "Action": ["logs:GetLogEvents"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:REGION:ACCOUNT_ID:log-group:/aws/deadline/FARM_ID/*"
    }
  ]
}
```

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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    },
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "credentials.deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
```

```
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    }
  ]
}
```

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。

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

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 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：

- 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。確保他們沒有檔案系統寫入許可來處理代理程式檔案或其他共用軟體。

- 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 Linux和 C:\Windows\system32\etc\hosts上的 Windows)，以及將資料表路由至工作站和工作者主機作業系統。
- 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。
- 不要將排程命令提供給佇列jobRunAsUser許可，以在未來執行：
  - 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。

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使用 AWS 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 macOS上的 ，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。
- 在工作站和工作者主機作業系統`/etc/resolve.conf`上限制 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。

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 提供資源，例如陣列、機群和佇列，可用於處理任務。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。您也可以請求增加您所使用的許多資源配額。

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。

使用 AWS 建立截止日期雲端資源 AWS CloudFormation

AWS Deadline Cloud 已與 整合 AWS CloudFormation，此服務可協助您建立和設定 AWS 資源的模型，以便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 AWS CloudFormation 佈建和設定這些資源。

使用 時 AWS 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。

期限 雲端和 AWS 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AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您想要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation 設計工具來協助您開始使用 AWS CloudFormation 範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南 中的 什麼是 AWS CloudFormation 設計器？。

截止日期 雲端支援在其中建立陣列、佇列和機群 AWS 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 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS 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？

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時可能會發生問題。

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。

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. 群組索引標籤預設為選取。如果您依群組指派許可，建議您使用，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，請選擇新增使用者來為使用者指派許可。

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. 群組索引標籤預設為選取。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 主控台中的群組。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。

為什麼工作者沒有接我的任務？

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，是因為機群角色未正確設定。

若要確認這是正在發生的情況，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 截止日期雲端開發人員指南中的 CloudTrail 日誌。

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？

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，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。

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與佇列相關聯的任何機群。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工作者計數上限設定為零。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日誌。

- 如果您看到授權錯誤，或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》中的將客戶管理的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有關任務失敗原因的資訊。如果您使用的是 ，Windows且您的結束碼為負數，請嘗試搜尋未簽署的結束碼版本：

```
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來檢查相依性的狀態。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。

截止日期雲端使用者指南的文件歷史記錄

下表說明AWS 每個期限雲端使用者指南版本的重要變更。

變更	描述	日期
Adobe After Effects 提交者安裝程式	新增將 Adobe After Effects 提交者安裝程式新增至數位內容建立軟體的指示。如需詳細資訊，請參閱 Adobe After Effects。	2025 年 2 月 13 日
疑難排解	新增了有關故障診斷截止日期雲端問題的資訊。如需詳細資訊，請參閱疑難排解。	2025 年 2 月 7 日
任務資源限制	新增了新任務資源限制和工作者主機數量上限的文件。如需詳細資訊，請參閱建立任務的資源限制。	2025 年 1 月 30 日
Adobe After Effects UBL	新增有關截止日期雲端的 Adobe After Effects 用量型授權 (UBL) 的資訊。如需詳細資訊，請參閱連線至授權端點。	2025 年 1 月 30 日
使用者指南中的重組內容	將開發人員聚焦內容從使用者指南移至開發人員指南： • 已將建立客戶受管機群的說明移至開發人員指南中的新客戶受管機群章節。 • 將有關使用自有授權的資訊移至開發人員指南中的使用軟體授權章節。 • 將有關使用 CloudTrai l、CloudWatch 和 EventBrid	2025 年 1 月 6 日

	ge 監控的詳細資訊移至開發人員指南中的監控章節。	
預算閾值事件	新增預算閾值 EventBridge 事件。如需詳細資訊，請參閱截止日期雲端事件詳細資訊參考。	2024 年 10 月 30 日
任務狀態事件	新增了任務和任務狀態 EventBridge 事件。如需詳細資訊，請參閱截止日期雲端事件詳細資訊參考。	2024 年 10 月 24 日
重新提交任務	新增如何重新提交任務的相關資訊。如需詳細資訊，請參閱重新提交任務。	2024 年 10 月 7 日
AWS 受管政策更新	更新現有的 AWS 受管政策。如需詳細資訊，請參閱AWS 截止日期雲端的 受管政策。	2024 年 10 月 7 日
攜帶您自己的授權	已新增有關如何使用自己的授權伺服器或授權代理執行個體搭配截止日期雲端的相關資訊。如需詳細資訊，請參閱服務受管機群。	2024 年 7 月 26 日
Autodesk 3ds Max UBL	新增了有關 Autodesk 3ds Max 使用型授權 (UBL) 的截止日期雲端相關資訊。如需詳細資訊，請參閱連線至授權端點。	2024 年 6 月 18 日

監控和成本管理功能	您可以使用 EventBridge 來支援在截止日期雲端中監控。如需詳細資訊，請參閱在 EventBridge 事件上執行動作。期限 雲端提供預算和用量總管，協助您控制和視覺化任務的成本。了解一些協助管理這些成本的最佳實務。如需詳細資訊，請參閱成本管理。	2024 年 5 月 23 日
初始版本	這是截止日期雲端使用者指南的初始版本。	2024 年 4 月 2 日

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。