
Amazon EMR

管理指南



Amazon EMR: 管理指南

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

什麼是 Amazon EMR ?	1
概觀	1
了解叢集和節點	1
將工作提交到叢集	2
處理資料	2
了解叢集生命週期	3
優勢	4
節省成本	4
AWS 整合	4
部署	5
可擴展性與彈性	5
可靠性	5
安全性	5
監控	6
管理界面	6
架構	7
儲存	7
叢集資源管理	8
資料處理架構	8
應用程式與程式	8
開始使用	9
步驟 1 : 設定先決條件	9
註冊 AWS 帳號 :	9
建立 Amazon S3 儲存貯體	9
建立 Amazon EC2 金鑰對	10
步驟 2 : 啟動叢集	10
啟動範例叢集	10
快速選項的摘要	11
步驟 3 : 允許 SSH 存取	13
步驟 4 : 執行 Hive 指令碼來處理資料	14
了解資料和指令碼	14
提交 Hive 指令碼做為步驟	15
檢視結果	16
步驟 5 : 清除資源	17
使用 EMR 筆記本	18
考量	18
建立筆記本	19
為筆記本建立叢集	19
每個叢集的筆記本限制	20
在建立筆記本時建立叢集	20
使用現有的 Amazon EMR 叢集	20
使用筆記本	21
了解筆記本的狀態	21
使用筆記本編輯器	21
變更叢集	22
刪除筆記本和筆記本檔案	23
共用筆記本檔案	23
監控	24
設定 Spark 使用者模擬	24
使用 Spark 任務監控小工具	24
安全性	25
使用筆記本範圍程式庫	25
考量事項與限制	26
使用筆記本範圍程式庫	26

建立 Git 儲存庫與 Amazon EMR 筆記本的關聯性	27
將 Git 儲存庫新增至 Amazon EMR	27
更新或刪除 Git 儲存庫	28
連結或解除連結 Git 儲存庫	28
使用關聯的 Git 儲存庫建立新筆記本	30
在筆記本中使用 Git 儲存庫	30
規劃和設定叢集	31
設定叢集位置和資料儲存體	31
選擇一個 AWS 區域	31
使用儲存和檔案系統	32
準備輸入資料	34
設定輸出位置	41
規劃和設定主節點	46
支援的應用程式和功能	46
啟動具多個主節點的 EMR 叢集	50
考量事項和最佳實務	52
使用 EMR 檔案系統 (EMRFS)	52
一致性檢視	53
授權存取在 Amazon S3 中的 EMRFS 資料	66
使用 EMRFS 屬性來指定 Amazon S3 加密	67
控制叢集終止	73
設定叢集自動終止或繼續	74
使用終止保護	75
使用 AMI	78
使用預設 AMI	79
使用自訂 AMI	79
指定 Amazon EBS 根設備磁碟區大小	84
設定叢集軟體	85
建立引導操作來安裝其他軟體	86
設定叢集硬體和聯網	89
了解節點類型	89
設定 EC2 執行個體	90
設定網路	95
設定執行個體機群或執行個體群組	104
準則和最佳實務	114
設定叢集記錄和除錯	118
預設日誌檔案	118
封存日誌檔到 Amazon S3	119
啟用除錯工具	120
除錯選項資訊	121
標籤叢集	122
標籤限制	122
帳單的標籤資源	123
將標籤新增到新叢集	123
將標籤新增到現有的叢集	124
查看叢集上的標籤	124
從叢集移除標籤	125
驅動程式和第三方應用程式整合	125
使用商業智慧工具搭配 Amazon EMR	125
安全性	127
安全組態	127
資料保護	127
AWS Identity and Access Management 取代為 Amazon EMR	127
Kerberos	128
Lake Formation	128
安全通訊殼層 (SSH)	128
Amazon EC2 安全群組	128

預設 Amazon Linux AMI 更新	128
使用安全組態設定叢集安全性	128
建立安全組態	129
指定適用於叢集的安全組態	142
資料保護	143
加密靜態和傳輸中的資料	144
IAM 取代為 Amazon EMR	151
對象	152
使用身分來驗證	152
使用政策管理存取權	153
Amazon EMR 如何搭配 IAM 運作	154
設定 Amazon EMR 的服務角色	156
身分類型政策範例	179
對叢集節點進行驗證	190
使用 SSH 登入資料的 Amazon EC2 金鑰對	190
使用 Kerberos 身份驗證	190
Amazon EMR 與 AWS Lake Formation 整合 (Beta 版)	214
Amazon EMR 與 Lake Formation 整合的概念性概觀	214
支援的應用程式和功能	218
開始之前	219
使用 Lake Formation 啟動 Amazon EMR 叢集	225
使用安全群組控制網路流量	230
使用 Amazon EMR 受管安全群組	231
使用額外的安全群組	235
指定安全群組	235
EMR 筆記本 的安全群組	236
使用封鎖公開存取	238
合規驗證	239
彈性	239
基礎設施安全	240
管理叢集	241
查看和監控叢集	241
查看叢集狀態和詳細資訊	241
增強型步驟偵錯	246
查看應用程式歷史記錄	247
檢視日誌檔	250
檢視 Amazon EC2 中的叢集執行個體	254
CloudWatch 事件與指標	254
使用 Ganglia 檢視叢集應用程式指標	274
在 AWS CloudTrail 中記錄 Amazon EMR API 呼叫	274
連接叢集	276
使用 SSH 連接至主節點	277
檢視 Amazon EMR 叢集上託管的 Web 界面	281
終止叢集	288
使用主控台終止叢集	288
使用 AWS CLI 終止叢集	289
使用 API 終止叢集	290
調整叢集資源規模	290
於 Amazon EMR 使用自動調整規模	291
手動調整執行中的叢集規模	298
縮小叢集	303
使用主控台複製叢集	304
將工作提交到叢集	305
使用 CLI 和主控台來使用步驟	305
以互動方式提交 Hadoop 任務	307
在叢集中新增 256 個以上的步驟	309
使用 AWS Data Pipeline 自動化再次出現的叢集	309

故障診斷叢集	310
哪些工具適用於故障診斷？	310
顯示叢集詳細資訊的工具	310
檢視日誌檔的工具	311
監控叢集效能的工具	311
檢視和重新啟動 Amazon EMR 和應用程式程序 (常駐程式)	311
檢視執行中的程序	311
重新啟動程序	312
對失敗的叢集進行故障排除	313
步驟 1：收集有關問題的資料	313
步驟 2：檢查環境	313
步驟 3：查看最後狀態變更	314
步驟 4：檢查日誌檔	315
步驟 5：逐步測試叢集	315
故障診斷執行緩慢的叢集	316
步驟 1：收集有關問題的資料	316
步驟 2：檢查環境	317
步驟 3：檢查日誌檔	317
步驟 4：檢查叢集和執行個體運作狀態	318
步驟 5：檢查遭阻擋的群組	319
步驟 6：檢閱組態設定	320
步驟 7：檢查輸入資料	321
Amazon EMR 中的常見錯誤	321
輸入和輸出錯誤	321
許可錯誤	323
資源錯誤	324
串流叢集錯誤	330
自訂 JAR 叢集錯誤	331
Hive 叢集錯誤	331
VPC 錯誤	332
AWS GovCloud (US-West) 錯誤	335
其他問題	335
故障診斷 Lake Formation 叢集 (Beta 版)	335
工作階段過期	335
請求的資料表上沒有使用者的許可	335
插入、建立和更改資料表：Beta 版中不支援	336
撰寫啟動和管理叢集的應用程式	337
端對端 Amazon EMR Java 原始程式碼範例	337
API 呼叫的常見概念	339
Amazon EMR 的端點	340
在 Amazon EMR 指定叢集參數	340
Amazon EMR 中的可用區域	340
如何在 Amazon EMR 叢集使用其他檔案和程式庫	340
使用軟體開發套件呼叫 Amazon EMR API	341
使用適用於 Java 的 AWS 開發套件來建立 Amazon EMR 叢集	341
AWS Glossary	343

什麼是 Amazon EMR？

Amazon EMR 是一項受管的叢集平台，可簡化在 AWS 上執行大數據架構（例如 Apache Hadoop 與 Apache Spark），以便處理和分析大量資料。透過使用這些架構和相關的開放原始碼專案（例如 Apache Hive 和 Apache Pig），您可以處理資料以供分析用途和商業智慧工作負載。此外，您可以使用 Amazon EMR，來將大量資料進行轉換，和傳入及傳出其他 AWS 資料存放區與資料庫（例如 Amazon Simple Storage Service (Amazon S3) 與 Amazon DynamoDB）。

如果您是第一次使用 Amazon EMR，我們建議您在開始前除了此章節以外，先閱讀以下章節：

- [Amazon EMR – 此服務頁面提供 Amazon EMR 重點介紹、產品詳細資訊和定價資訊。](#)
- [入門：使用 Amazon EMR 來分析大數據 \(p. 9\)](#) – 這些教學課程可協助您快速地開始使用 Amazon EMR。

本節內容

- [Amazon EMR 概觀 \(p. 1\)](#)
- [使用 Amazon EMR 的優勢？\(p. 4\)](#)
- [Amazon EMR 架構概觀 \(p. 7\)](#)

Amazon EMR 概觀

本主題提供 Amazon EMR 叢集的概觀，包括如何將工作提交到叢集，該資料的處理方式，以及該叢集在處理期間經歷的各種狀態。

在這個主題中

- [了解叢集和節點 \(p. 1\)](#)
- [將工作提交到叢集 \(p. 2\)](#)
- [處理資料 \(p. 2\)](#)
- [了解叢集生命週期 \(p. 3\)](#)

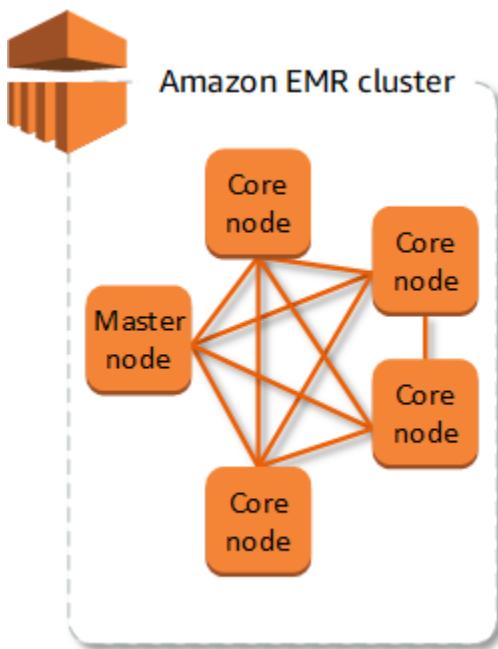
了解叢集和節點

Amazon EMR 的中心元件是叢集。叢集是 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的集合。叢集中的每個執行個體稱為節點。每個節點在叢集中具有角色（稱為節點類型）。Amazon EMR 也會針對每個節點類型安裝不同的軟體元件，讓 Apache Hadoop 等分散式應用程式中的節點，都具有角色。

在 Amazon EMR 中的節點類型如下：

- 主節點：此種節點會執行軟體元件，統籌其他節點之間的資料與任務分發以進行處理，藉此管理叢集。主節點會追蹤任務的狀態，並監控叢集運作狀況。每個叢集都會有主節點，因此您可以建立只有主節點的單一節點叢集。
- 核心節點：一種節點，內含軟體元件，這些元件可在叢集上的 Hadoop 分散式檔案系統 (HDFS) 中，執行任務和儲存資料。多節點叢集至少會有一個核心節點。
- 任務節點：一種節點，內含軟體元件，這些元件只會執行任務，而不會在 HDFS 中儲存資料。任務節點是選用的。

下圖顯示叢集，此叢集包含一個主節點和四個核心節點。



將工作提交到叢集

在 Amazon EMR 上執行叢集時，有幾個選項可讓您指定需要完成之工作的方式。

- 提供要透過函式完成的完整工作定義，而該函式已在叢集建立時指定為步驟。此定義通常會用於處理一組資料量的叢集，然後在處理完成時終止。
- 建立長時間執行的叢集，並使用 Amazon EMR 主控台、Amazon EMR API 或 AWS CLI 來提交步驟，這些步驟中可能會包含一個或多個任務。如需更多詳細資訊，請參閱 [將工作提交到叢集 \(p. 305\)](#)。
- 建立叢集，並依需要使用 SSH 來連線到主節點和其他節點，並使用已安裝應用程式提供的界面來執行任務、提交查詢，不論是以指令碼撰寫或是以互動的方式進行。如需詳細資訊，請參閱 [Amazon EMR Release Guide](#).

處理資料

啟動您的叢集時，您可以選擇要安裝的架構和應用程式來處理您的資料處理需求。若要在 Amazon EMR 叢集中處理資料，您可以將任務或查詢直接提交給已安裝的應用程式，或是在叢集中執行步驟。

將任務直接提交到應用程式

您可以提交任務並與在 Amazon EMR 叢集中安裝的軟體直接互動。若要這樣做，您通常會透過安全連線連接到主節點並存取可用於在叢集上直接執行之軟體的界面和工具。如需更多詳細資訊，請參閱 [連接叢集 \(p. 276\)](#)。

執行步驟來處理資料

您可以將一或多個排定順序的步驟提交到 Amazon EMR 叢集。每個步驟是工作的單位，其中包含透過叢集上安裝的軟體來操作資料進行處理的指示。

下面是使用四個步驟的程序：

1. 提交輸入資料集以進行處理。

2. 使用 Pig 程式以處理第一步的輸出。
3. 使用 Hive 程式以處理第二個輸入資料集。
4. 寫入輸出資料集。

一般而言，在 Amazon EMR 中處理資料時，輸入即為資料，這些資料是在您所選擇的底層檔案系統（例如 Amazon S3 或 HDFS）中，以檔案形式所儲存的。此資料會在處理序列中從一個步驟傳遞到下一個步驟。最後步驟會將輸出資料寫入到指定的位置（如 Amazon S3 儲存貯體）。

在下列序列中執行步驟：

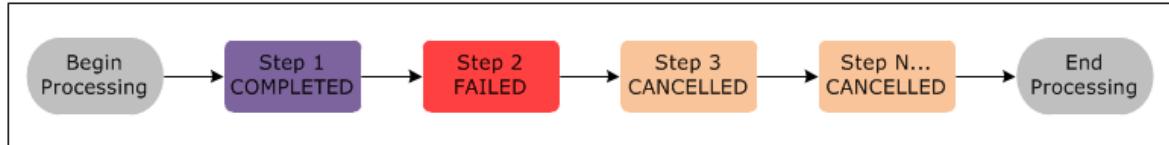
1. 提交請求以開始處理步驟。
2. 所有步驟的狀態會設定為 PENDING (待定)。
3. 序列中的第一個步驟開始時，其狀態會變更為 RUNNING (執行中)。其他步驟的狀態則會保持為 PENDING (待定)。
4. 第一個步驟完成之後，其狀態會變更為 COMPLETED (已完成)。
5. 序列中的下一個步驟開始時，其狀態會變更為 RUNNING (執行中)。該步驟完成時，其狀態會變更為 COMPLETED (已完成)。
6. 每個步驟會重複此模式，直到所有步驟都完成和結束處理。

下圖代表步驟處理時的步驟序列和步驟的狀態變更。



如果步驟在處理時失敗，其狀態會變更為 TERMINATED_WITH_ERRORS (已錯誤終止)。您可以決定每個步驟之後會發生什麼事情。根據預設，此序列中剩下的任何步驟都會設定成 CANCELLED (已取消)，因此不會執行。您也可以選擇忽略失敗，允許剩下的步驟繼續執行，或者立刻終止叢集運作。

下圖代表步驟在處理期間故障時的步驟序列和狀態的預設變更。



了解叢集生命週期

成功 Amazon EMR 叢集會遵循此程序：

1. Amazon EMR 會先根據您的規格，為每個執行個體叢集內的 EC2 執行個體進行佈建。如需更多詳細資訊，請參閱 [設定叢集硬體和聯網 \(p. 89\)](#)。針對所有的執行個體，Amazon EMR 會使用 Amazon EMR 的預設 AMI，或是您所指定的自訂 Amazon Linux AMI。如需更多詳細資訊，請參閱 [使用自訂 AMI \(p. 79\)](#)。在此階段，叢集狀態為 STARTING。
2. Amazon EMR 會在每個執行個體上執行您所指定的引導操作。您可以使用引導操作來安裝自訂的應用程式，並執行您需要的自訂操作。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#)。在此階段，叢集狀態為 BOOTSTRAPPING。
3. Amazon EMR 會安裝您在建立叢集時所指定的原生應用程式，例如，Hive、Hadoop、Spark 和其他應用程式。
4. 引導操作成功完成、且原生應用程式安裝完成之後，叢集狀態會變成 RUNNING。此時，您可以連線到叢集執行個體，而叢集會循序執行您在叢集建立時所指定的任何步驟。您可以提交其他額外步驟，

該步驟將在任何先前步驟完成之後開始執行。如需更多詳細資訊，請參閱 [使用 CLI 和主控台來使用步驟 \(p. 305\)](#)。

5. 在步驟執行成功之後，叢集就會進入 WAITING 狀態。如果叢集已設定成在最後步驟完成後自動終止，則叢集會進入 SHUTTING_DOWN 狀態。
6. 在所有執行個體均已終止後，叢集會進入 COMPLETED 狀態。

叢集生命週期期間的故障會造成 Amazon EMR 終止該叢集及其所有執行個體，除非您啟用終止保護。如果因失敗而終止叢集，則叢集上的任何儲存資料都將遭到刪除，而且叢集將設為 FAILED 狀態。如果已啟用終止保護，則您可以從叢集上擷取資料，並且移除終止保護，並接著終止叢集。如需更多詳細資訊，請參閱 [使用終止保護 \(p. 75\)](#)。

使用 Amazon EMR 的優勢？

使用 Amazon EMR 有許多好處。此章節會提供其他好處的概觀和其他資訊的連結，這些資訊可協助您深入探索。

主題

- [節省成本 \(p. 4\)](#)
- [AWS 整合 \(p. 4\)](#)
- [部署 \(p. 5\)](#)
- [可擴展性與彈性 \(p. 5\)](#)
- [可靠性 \(p. 5\)](#)
- [安全性 \(p. 5\)](#)
- [監控 \(p. 6\)](#)
- [管理界面 \(p. 6\)](#)

節省成本

Amazon EMR 定價取決於執行個體類型和您部署的 EC2 執行個體數量以及啟動叢集所在的區域。隨需定價提供低費率，但您可以透過購買預留執行個體或 Spot 執行個體來進一步降低成本。Spot 執行個體可以讓您省下大幅的成本 — 在某些情況下價格可低至隨需定價的十分之一。

Note

如果您使用 Amazon S3、Amazon Kinesis 或 DynamoDB 搭配 EMR 叢集，這些服務將產生額外的費用，會與您的 Amazon EMR 用量分開計費。

如需更多關於定價選項的資訊和詳細資訊，請參閱 [Amazon EMR 定價](#)。

AWS 整合

Amazon EMR 會與其他 AWS 服務整合，為您的叢集提供和聯網、儲存與安全等相關的功能。以下清單提供此整合的多個範例：

- 包含叢集中節點之執行個體的 Amazon EC2
- Amazon Virtual Private Cloud (Amazon VPC) 會設定啟動執行個體所在的虛擬網路
- Amazon S3 會存放輸入和輸出資料
- Amazon CloudWatch 會監控叢集效能和設定警報
- AWS Identity and Access Management (IAM) 會設定許可
- AWS CloudTrail 會針對向服務發出的請求進行稽核

- AWS Data Pipeline 會排定和啟動您的叢集

部署

EMR 叢集包含 EC2 執行個體，其會執行您提交到叢集的工作。啟動叢集時，Amazon EMR 會使用您選擇的應用程式（例如 Apache Hadoop 或 Spark）設定執行個體。選擇執行個體大小和最適合處理叢集需求的類型：批次處理、低延遲查詢、串流資料或大型資料儲存體。關於 Amazon EMR 可用的執行個體類型，詳細資訊請參閱 [設定叢集硬體和聯網 \(p. 89\)](#)。

Amazon EMR 在叢集上提供設定軟體的多種方法。例如，您可以安裝 Amazon EMR 版本，內含可包括多樣化架構（例如 Hadoop）和應用程式（如 Hive、Pig、或 Spark）的所選應用程式組。您也可以安裝多個 MapR 發行版本的其中一個。Amazon EMR 使用 Amazon Linux，因此您也可以用手動方式，使用 yum 軟體管理工具或是透過來源，在叢集上安裝軟體。如需更多詳細資訊，請參閱 [設定叢集軟體 \(p. 85\)](#)。

可擴展性與彈性

Amazon EMR 可隨著運算需求變更而提供彈性來擴展或縮減叢集。您可以重新調整叢集來為尖峰工作負載新增執行個體並在尖峰工作負載需求趨於平緩時移除執行個體來控制成本。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#)。

Amazon EMR 也提供執行多個執行個體群組的選項，讓您可以在一個群組中使用隨需執行個體以保證處理能力，並在另一個群組中使用 Spot 執行個體讓任務完成速度更快並降低成本。您也可以結合不同的執行個體類型，以針對不同 Spot 執行個體類型使用更佳的定價。如需更多詳細資訊，請參閱 [我應何時使用 Spot 執行個體？\(p. 115\)](#)。

此外，Amazon EMR 讓您可以靈活地將多個檔案系統用於輸入、輸出和中繼資料。例如，您可以選擇 Hadoop 分散式檔案系統 (HDFS)，其會在主要和核心節點上執行叢集來處理您無需存放超過叢集生命週期的資料。您可以為叢集上執行的應用程式，選擇使用 Amazon S3 的 EMR 檔案系統 (EMRFS) 做為資料層，讓您可以將運算和儲存資源，以及叢集生命週期以外的持久儲存資料做分隔。EMRFS 提供額外好處，可讓您單獨擴展或縮減來符合您的運算和儲存需求。您可以透過調整叢集來擴展運算需求，而您可以透過使用 Amazon S3 來擴展儲存需求。如需更多詳細資訊，請參閱 [使用儲存和檔案系統 \(p. 32\)](#)。

可靠性

Amazon EMR 在叢集中會監控節點，並在故障時自動終止和更換執行個體。

Amazon EMR 提供組態選項，這些選項會控制您的叢集終止的方式 - 自動或手動。如果您將叢集設定為自動終止，叢集會在所有步驟完成後即終止。這稱為暫時性叢集。不過，您可以設定叢集，以在處理完成後繼續執行，因此您可以在不再需要該叢集時手動選擇將其終止。或者，您可以建立一個叢集，直接與已安裝的應用程式互動，然後在您不再需要它時手動終止叢集。這些範例中的叢集稱為長時間執行的叢集。

此外，您可以設定終止保護，以避免叢集中的執行個體因為處理時的錯誤或問題而終止。終止保護已啟用時，您可以在終止恢復來自執行個體的資料。這些選項的預設設定會因您是使用主控台、CLI 或 API 來啟動叢集而有所不同。如需更多詳細資訊，請參閱 [使用終止保護 \(p. 75\)](#)。

安全性

Amazon EMR 會運用其他的 AWS 服務（例如 IAM 和 Amazon VPC），以及 Amazon EC2 金鑰對等功能，來協助您保護叢集和資料。

IAM

Amazon EMR 會與 IAM 整合以管理許可。您會使用連接到 IAM 使用者或 IAM 群組的 IAM 政策，來定義許可。您在政策定義的許可會決定那些使用者或群組成員可以執行的動作和他們可以存取的資源。如需詳細資訊，請參閱 [Amazon EMR 如何搭配 IAM 運作 \(p. 154\)](#)。

此外，Amazon EMR 會使用 Amazon EMR 服務本身的 IAM 角色，和執行個體的 EC2 執行個體描述檔。這些角色授與服務和執行個體許可，讓他們可以代表您存取其他 AWS 服務。這是一個 Amazon EMR 服務的預設角色和 EC2 執行個體描述檔的預設角色。預設角色使用 AWS 受管政策，系統會在您第一次從主控台啟動 EMR 叢集時自動為您建立該政策，然後選擇預設的許可。您也可以透過 AWS CLI 來建立預設的 IAM 角色。如果您要管理許可（而不是 AWS），您可以選擇服務和執行個體描述檔的自訂角色。如需更多詳細資訊，請參閱 [將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。

安全群組

Amazon EMR 使用安全群組來控制對 EC2 執行個體的傳入和傳出流量。啟動叢集時，Amazon EMR 會使用主執行個體的安全群組，以及要由核心/任務執行個體共用的安全群組。Amazon EMR 會設定安全群組規則，來確保叢集中執行個體之間的通訊。或者，您可以設定其他安全群組，並將它們指派給您的主要和核心/任務執行個體和以進行更進階的規則。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

加密

Amazon EMR 支援選用的 Amazon S3 伺服器端和用戶端加密搭配 EMRFS，有助於保護您存放於 Amazon S3 中的資料。使用伺服器端加密時，在上傳後 Amazon S3 會加密您的資料。

使用用戶端加密，加密及解密程序會在您 EMR 叢集上的 EMRFS 用戶端進行。您會使用 AWS Key Management Service (AWS KMS) 或自己的金鑰管理系統，來管理用戶端加密的主金鑰。

如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [以 EMRFS 進行 Amazon S3 資料加密](#)。

Amazon VPC

Amazon EMR 支援在 Amazon VPC 的虛擬私有雲端 (VPC) 中啟動叢集。VPC 是 AWS 中的隔離、虛擬網路，能夠讓您控制進階層面的網路設定和存取。如需更多詳細資訊，請參閱 [設定網路 \(p. 95\)](#)。

AWS CloudTrail

Amazon EMR 會與 CloudTrail 整合，針對由 AWS 帳戶或代表該帳戶所發出的請求，來記錄其相關資訊。您可以利用此資訊，追蹤哪些使用者正在存取您的叢集，以及進行請求所使用的 IP 地址。如需更多詳細資訊，請參閱 [在 AWS CloudTrail 中記錄 Amazon EMR API 呼叫 \(p. 274\)](#)。

Amazon EC2 金鑰對

您可以監控和與您的叢集互動，方法是在遠端電腦和主節點形成安全的連接。您可以使用 Secure Shell (SSH) 網路通訊協定來進行連接，或使用 Kerberos 進行身份驗證。如果您使用的是 SSH，則需要 Amazon EC2 金鑰對。如需更多詳細資訊，請參閱 [使用 SSH 登入資料的 Amazon EC2 金鑰對 \(p. 190\)](#)。

監控

您可以利用 Amazon EMR 管理界面和日誌檔來排除叢集問題，例如故障或錯誤。Amazon EMR 提供在 Amazon S3 中封存日誌檔案的功能，因此即使叢集終止，您也可以儲存日誌和進行疑難排解。Amazon EMR 也在 Amazon EMR 主控台中，提供了選用的偵錯工具，以瀏覽日誌檔案，這些檔案會記錄步驟、工作和任務的資訊。如需更多詳細資訊，請參閱 [設定叢集記錄和除錯 \(p. 118\)](#)。

Amazon EMR 會與 CloudWatch 互動，以針對叢集和叢集內的任務，追蹤其效能指標。您可以根據各種指標設定警報，例如叢集是否閒置或所用儲存體的百分比。如需更多詳細資訊，請參閱 [使用 CloudWatch 監控指標 \(p. 262\)](#)。

管理界面

您有多種方式可以與 Amazon EMR 互動：

- 主控台 — 一種圖形化使用者界面，可用來啟動和管理叢集。有了它，您填寫 Web 表單，以指定要啟動叢集的詳細資訊、檢視現有叢集的詳細資訊、偵錯和終止叢集。使用主控台是 Amazon EMR 入門的最簡單方式；不需任何程式設計知識。您可在 <https://console.aws.amazon.com//elasticmapreduce/home> 中線上使用主控台。
- AWS Command Line Interface (AWS CLI) — 一種用戶端應用程式，您可以在本機電腦上執行該程式，來連線到 Amazon EMR，並建立和管理叢集。AWS CLI 包含 Amazon EMR 特定的一組功能豐富的指令。您可以使用它來撰寫指令碼，該指令碼會將啟動和管理叢集的程序自動化。如果您偏好透過命令列來工作，使用 AWS CLI 是最好的選項。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [Amazon EMR](#)。
- 軟體開發套件 (SDK) — 軟體開發套件所提供的功能，可用來呼叫 Amazon EMR，以建立和管理叢集。您可以使用他們來撰寫應用程式，該應用程式會將建立和管理叢集的程序自動化。若要擴展或自訂 Amazon EMR 的功能，使用軟體開發套件是最好的選項。Amazon EMR 目前可在下列的軟體開發套件中使用：Go、Java、.NET (C# 和 VB.NET)、Node.js、PHP、Python 和 Ruby。如需關於這些軟體開發套件的詳細資訊，請參閱 [適用於 AWS 的工具](#) 和 [Amazon EMR 範本程式碼與程式庫](#)。
- Web Service API (Web 服務 API) — 一種低層級的界面，您可以來透過 JSON 直接呼叫 Web 服務。使用 API 是建立呼叫 Amazon EMR 之自訂軟體開發套件的最佳選項。如需詳細資訊，請參閱 [Amazon EMR API Reference](#)。

Amazon EMR 架構概觀

Amazon EMR 服務架構包含多個層，這些層會分別將特定的功能提供給叢集。此章節概略說明各個層級和元件。

在這個主題中

- [儲存 \(p. 7\)](#)
- [叢集資源管理 \(p. 8\)](#)
- [資料處理架構 \(p. 8\)](#)
- [應用程式與程式 \(p. 8\)](#)

儲存

儲存層包含與您叢集搭配使用的不同檔案系統。有多種不同類型的儲存選項，如下所示。

Hadoop 分散式檔案系統 (HDFS)

Hadoop 分散式檔案系統 (HDFS) 是一種適用於 Hadoop 的分散式、可擴展的檔案系統。HDFS 會分配在叢集中執行個體之間存放的資料，以便將多個資料的複本存放在不同的執行個體，以確保個別執行個體故障時資料不會遺失。HDFS 是暫時性儲存，其會在您終止叢集時遭到回收。HDFS 可用於在 MapReduce 處理期間快取中繼結果或用於有明顯隨機 I/O 的工作負載。

如需詳細資訊，請參閱 Apache Hadoop 網站上的 [HDFS 使用者指南](#)。

EMR 檔案系統 (EMRFS)

使用 EMR 檔案系統 (EMRFS)，Amazon EMR 會擴展 Hadoop，來讓您能夠直接存取 Amazon S3 中所儲存的資料，就如同這是 HDFS 之類的檔案系統。您可以將 HDFS 或 Amazon S3 用做為叢集中的檔案系統。大多數情況下，會使用 Amazon S3 來存放輸入和輸出資料，且中繼結果會存放在 HDFS 中。

本機檔案系統

本機檔案系統是指與本機連接的磁碟。當您建立 Hadoop 叢集時，每個節點都會從稱為執行個體存放區的預先連接磁碟儲存體中，預先設定區塊隨附的 Amazon EC2 執行個體建立。執行個體存放區磁碟區上的資料，只會保存在 Amazon EC2 執行個體的生命週期內。

叢集資源管理

資源管理層負責管理叢集資源，並排定處理資料任務的時程。

在預設情況下，Amazon EMR 使用 YARN (Yet Another Resource Negotiator)，這是在 Apache Hadoop 2.0 中引進的一種元件，能夠集中管理多個資料處理架構的叢集資源。不過，在 Amazon EMR 中也有其他的架構和應用程式，並未使用 YARN 做為資源管理程式。Amazon EMR 在每個節點上也具有代理程式，功能是管理 YARN 元件、維持叢集的健全運作，以及和 Amazon EMR 進行通訊。

因為 Spot 執行個體經常用來執行任務節點，Amazon EMR 具有用於排定 YARN 工作的預設功能，使得當 Spot 執行個體上執行的任務節點終止時，執行中的工作不會失敗。Amazon EMR 透過允許應用程式主控程序只在核心節點上執行來達成此目的。應用程式主控程序會控制執行中工作，並且需要在工作的生命週期中保持作用中。

Amazon EMR 發行版本 5.19.0 和更新版本使用內建的 [YARN 節點標籤](#) 功能來達成此目的。(較早版本使用的是程式碼修補程式。) `yarn-site` 和 `capacity-scheduler` 組態分類中的屬性會依設設定，使得 YARN 功能排程器和公平排程器會利用節點標籤。Amazon EMR 會自動將核心節點標記 CORE 標籤，並且設定屬性，使得應用程式主控只會排程在具有 CORE 標籤的節點上執行。在 `yarn-site` 和 `capacity-scheduler` 組態分類中手動修改相關屬性，或是直接在相關聯的 XML 檔案中修改，可能會破壞此特性或修改此功能。

資料處理架構

資料處理架構層是用於處理和分析資料的引擎。有許多架構可在 YARN 上執行或者有自己的資源管理。不同架構適用於不同類型的處理需求(例如批次、互動式、記憶體內、串流等等)。您選擇的架構取決於您的使用案例。這會影響應用程式層提供使用的語言和界面，應用程式層與您想處理的資料互動。適用於 Amazon EMR 的主要處理架構是 Hadoop MapReduce 和 Spark。

Hadoop MapReduce

Hadoop MapReduce 是一種開放原始碼的分散式運算程式設計模型。它可簡化撰寫平行分散式應用程式的程序，方法是處理所有邏輯，同時提供 Map 和 Reduce 函數。Map 函數會將資料映射為名為中繼結果的金鑰值對集。Reduce 函數會結合中繼結果、套用額外的演算法，並產生最終輸出。適用於 MapReduce 的架構有很多(如 Hive)，其會自動產生 Map 和 Reduce 程式。

如需詳細資訊，請參閱 Apache Hadoop Wiki 網站上的 [Map 和 Reduce 操作實際上的執行方式](#)。

Apache Spark

Spark 是一個叢集架構和程式設計模型，可處理大數據工作負載。與 Hadoop MapReduce 類似，Spark 是一種開放原始碼、分散式處理系統，但使用有向無環圖來執行資料集的計畫和記憶體內快取。在 Amazon EMR 上執行 Spark 時，您可以使用 EMRFS 來直接存取 Amazon S3 中的資料。Spark 支援多種互動式查詢模組(例如 SparkSQL)。

如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [Amazon EMR 叢集上的 Apache Spark](#)。

應用程式與程式

Amazon EMR 支援許多應用程式(例如 Hive、Pig 和 Spark Streaming 程式庫)，以提供使用更高層級語言之類的功能，來建立處理工作負載、運用機器學習演算法，製作串流處理應用程式和建置資料倉儲。此外，Amazon EMR 還支援開放原始碼專案，該專案有他們自己的叢集管理功能(而不使用 YARN)。

您可以使用各種程式庫和語言來與在 Amazon EMR 中執行的應用程式互動。例如，您可以使用、Hive 或 Pig 搭配 MapReduce，或使用 Spark Streaming、Spark SQL、MLlib 和 GraphX 搭配 Spark。

如需詳細資訊，請參閱 [Amazon EMR Release Guide](#)。

入門：使用 Amazon EMR 來分析大數據

本教學課程會逐步說明程序，教您如何使用 AWS Management Console 中的 Quick Create (快速建立) 選項，來建立 Amazon EMR 叢集範例。在建立叢集之後，您會將 Hive 指令碼以步驟提交，來處理 Amazon Simple Storage Service (Amazon S3) 中所儲存的範例資料。

本教學課程不適用於生產環境，而且不涵蓋深入的組態選項。此教學課程旨在協助您快速設置叢集，以進行評估。如果您有任何問題或進度停滯不前，可以在我們的[開發論壇](#)上張貼文章，來聯繫 Amazon EMR 團隊。

您所建立的範例叢集，會在實際環境中執行。叢集執行個體的費用會依 Amazon EMR 價格的每秒費率計費。如需詳細資訊，請參閱 [Amazon EMR 定價](#)。這些費用會隨區域而有不同。其成本應該是最低的，因為在叢集佈建之後，叢集執行的時間應該不到一個小時。

進行本教學課程時，您如果在 Amazon S3 中存放查詢輸出檔案，也可能會產生費用。這些檔案很小，因此費用應該不多。此外，如果您還在第一年使用 AWS 的期間內，而且用量未超過 AWS 免費方案的上限，則可以免除 Amazon S3 的部分或全部費用。如需詳細資訊，請參閱 [Amazon S3 定價](#) 和 [AWS 免費方案](#)。

如果您考慮在產能中納入 Amazon EMR，請利用 [AWS 每月成本簡易計算機](#)來預估您的成本。

在此教學課程中的步驟：

- [步驟 1：設定您範例叢集的先決條件 \(p. 9\)](#)
- [步驟 2：啟動範例 Amazon EMR 叢集 \(p. 10\)](#)
- [步驟 3：允許從用戶端到叢集的 SSH 連線 \(p. 13\)](#)
- [步驟 4：將 Hive 指令碼做為步驟執行以處理資料 \(p. 14\)](#)
- [步驟 5：終止叢集和刪除儲存貯體 \(p. 17\)](#)

步驟 1：設定您範例叢集的先決條件

在開始設置 Amazon EMR 叢集之前，請務必先完成此主題中的先決條件。

註冊 AWS 帳號：

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

建立 Amazon S3 儲存貯體

在本教學課程中，您會指定 Amazon S3 儲存貯體和資料夾，來儲存 Hive 查詢的輸出資料。本教學課程會使用預設的日誌儲存位置，但您也可以根據自己的喜好，指定自訂的位置。由於 Hadoop 的要求，您用於 Amazon EMR 的儲存貯體和資料夾名稱，必須符合下列的限制：

- 必須只包含字母、數字、英文句點(.) 和英文連字號(-)。
- 結尾不能是數字。

如果您已可存取符合這些要求的資料夾，可以將該資料夾用於此教學課程。該輸出資料夾應為空。另一個要記得的要求，就是涵跨所有 AWS 帳戶的儲存貯體名稱必須是唯一的。

如需關於建立儲存貯體的詳細資訊，請參閱 Amazon Simple Storage Service Getting Started Guide中的[建立儲存貯體](#)。在建立儲存貯體之後，請從清單中選擇該儲存貯體，然後選擇 Create folder (建立資料夾)、使用符合要求的名稱來取代 New folder (新資料夾)，然後選擇 Save (儲存)。

本教學後續內容中所使用的儲存貯體和資料夾名稱是 `s3://mybucket/MyHiveQueryResults`。

建立 Amazon EC2 金鑰對

您必須擁有 Amazon Elastic Compute Cloud (Amazon EC2) 金鑰對，才能使用 Secure Shell (SSH) 通訊協定，透過安全通道連線到您叢集中的節點。如果您已擁有想要使用的金鑰對，則可略過此步驟。如果您不需要金鑰對，請遵循以下其中一個程序 (視您的作業系統而定)。

- Amazon EC2 User Guide for Windows Instances中的[使用 Amazon EC2 來建立金鑰對](#)。
- Amazon EC2 User Guide for Linux Instances中的[使用 Amazon EC2 來建立金鑰對](#)。也請針對 Mac OS 使用這套程序。

步驟 2：啟動範例 Amazon EMR 叢集

在此步驟中，您會使用 Amazon EMR 主控台中的 Quick Options (快速選項)，來啟動範例叢集，並且讓大多數的選項保持其預設值。若要進一步了解這些選項，請參閱步驟之後的[快速選項的摘要 \(p. 11\)](#)。您也可以選擇 Go to advanced options (前往進階選項)，來了解叢集可使用的其他組態選項。在建立本教學課程要使用的叢集之前，請先確定已完成[步驟 1：設定您範例叢集的先決條件 \(p. 9\)](#) 中的要求。

啟動範例叢集

啟動範例 Amazon EMR 叢集

- Sign in to the AWS Management Console and open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
- 選擇 Create cluster (建立叢集)。
- 在 Create Cluster - Quick Options (建立叢集 - 快速選項) 頁面上接受預設值 (但不包括下列欄位)：
 - 輸入 Cluster name (叢集名稱) 來協助您識別叢集，例如，`#####_EMR##`。
 - 在 Security and access (安全性與存取) 中，選擇您在[建立 Amazon EC2 金鑰對 \(p. 10\)](#) 中所建立的 EC2 key pair (EC2 金鑰對)。
- 選擇 Create cluster (建立叢集)。

隨即會顯示叢集狀態頁面，內含叢集 Summary (摘要)。您可以利用此頁面，來監控叢集建立的進度，和檢視叢集狀態的相關詳細資訊。當建立叢集的任務完成時，狀態頁面上的項目會更新。您可能會需要選擇右側的重新整理圖示，或是重新整理您的瀏覽器，以接收更新。

在 Network and hardware (網路和硬體) 中，找出 Master (主要) 和 Core (核心) 執行個體狀態。在叢集建立的過程中，狀態會依序從 Provisioning (佈建中)、Bootstrapping (啟動中) 變成 Waiting (等待中)。如需更多詳細資訊，請參閱[了解叢集生命週期 \(p. 3\)](#)。

一旦出現 Security groups for Master (主叢集的安全群組) 和 Security Groups for Core & Task (核心與任務叢集的安全群組) 的連結，您就可以進入下一個步驟，但最好先等到叢集順利啟動，並且變成 Waiting (等待中) 的狀態。

如需關於閱讀叢集摘要的詳細資訊，請參閱 [查看叢集狀態和詳細資訊 \(p. 241\)](#)。

快速選項的摘要

下表說明當您在 Amazon EMR 主控台中使用 Quick cluster configuration (快速叢集組態) 頁面來啟動叢集時，相關的欄位和預設值。

主控台欄位	預設值	描述
叢集名稱	My cluster (我的叢集)	叢集名稱是選用的，叢集的描述名稱不需要是唯一的。
日誌	啟用	啟用記錄功能之後，Amazon EMR 會將詳細的日誌資料，寫入指定的 Amazon S3 資料夾。記錄功能只能在建立叢集時啟用，而且此項設定之後就無法再變更。會指定預設的 Amazon S3 儲存貯體。您可以選擇性地指定自己的儲存貯體。如需更多詳細資訊，請參閱 檢視封存到 Amazon S3 的日誌檔 (p. 252) 。
S3 folder (S3 資料夾)	s3://aws-logs- account_number-region/elasticmapreduce/	此選項會指定到 Amazon S3 儲存貯體中某個資料夾的路徑，您希望 Amazon EMR 將日誌資料寫入該資料夾。如果指定路徑中的預設資料夾，不存在於儲存貯體中，會自動為您建立。您可以輸入或瀏覽至 Amazon S3 資料夾，來指定不同的資料夾。
Launch mode (啟動模式)	叢集	此選項指定是否啟動長時間執行的叢集，或是否啟動在執行完您指定的任何步驟之後，就會終止的叢集。 如果使用 Cluster (叢集) 選項，叢集會持續執行，直到您將其終止，這稱為長時間執行的叢集。如果您選擇 Step execution (步驟執行)，Amazon EMR 會提示您新增和設定步驟。您可以利用這些步驟，來將工作提交給叢集。在您指定的步驟執行完成之後，叢集會自動終止。如需更多詳細資訊，請參閱 設定叢集自動終止或繼續 (p. 74) 。
發行版本	emr-5.28.0	此選項會指定建立叢集時所要使用的 Amazon EMR 發行版本。Amazon EMR 版本會決定 Amazon EMR 所安裝開放原始碼應用程式（例如 Hadoop 和 Hive）的版本。預設會選擇最新發行版本的標籤。如果您需要不同的開放原始碼應用程式版本，來與您

主控台欄位	預設值	描述
		的解決方案相容，可以選擇舊的 Amazon EMR 版本。在使用舊的 Amazon EMR 發行版本時，可能會無法使用某些 Amazon EMR 功能和應用程式，所以建議您在可取得時使用最新的版本。如需關於每個 Amazon EMR 發行版本的詳細資訊，請參閱 Amazon EMR Release Guide 。
應用程式	Core Hadoop (核心 Hadoop)	<p>此選項會決定要在您的叢集上，從大數據生態系統安裝哪些開放原始碼應用程式。透過快速入門，可使用最常見的應用程式組合。若要選擇自己的應用程式組合，包括未列在快速入門中的其他應用程式，請選擇 Go to advanced options (前往進階選項)。關於每個 Amazon EMR 發行版本可使用的應用程式和版本，詳細資訊請參閱 Amazon EMR Release Guide。</p> <p>此外，如果 Amazon EMR 無法安裝某個應用程式，或是您要在所有的叢集執行個體上，安裝自訂應用程式，可以使用引導操作。如需更多詳細資訊，請參閱 建立引導操作來安裝其他軟體 (p. 86)。如果選擇 Step execution (步驟執行)，Amazon EMR 會根據您步驟的需要，來選擇要安裝的應用程式。</p>
執行個體類型	m5.xlarge	此選項會決定 Amazon EC2 執行個體類型 (Amazon EMR 針對您叢集中執行的執行個體，進行初始化的執行個體類型)。預設的執行個體選擇，會隨區域而有不同，而且在某些區域中，可能會無法使用某些執行個體類型。如需更多詳細資訊，請參閱 設定叢集硬體和聯網 (p. 89) 。
執行個體的數目	3	此選項會決定要初始化的 Amazon EC2 執行個體數目。每個執行個體會對應到 Amazon EMR 叢集中的節點。您必須擁有一個節點，也就是主節點。如需選擇執行個體類型和數量的指引，請參閱 叢集組態指南和最佳實務 (p. 114) 。

主控台欄位	預設值	描述
EC2 金鑰對	Choose an option (選擇選項)	這會指定在透過 Secure Shell (SSH) 來連線到叢集中的節點時，所要使用的 Amazon EC2 金鑰對。我們強力建議您建立和指定 Amazon EC2 金鑰對。如果未選擇金鑰對，您會無法連線到叢集，以提交步驟，或是與應用程式進行互動。如需更多詳細資訊，請參閱 連接叢集 (p. 276) 。若要連線，您還需要在安全群組中建立傳入規則，來允許 SSH 連線。
權限	預設	利用此選項來指定叢集使用的 AWS Identity and Access Management 角色。這些角色會決定 Amazon EMR 和叢集執行個體上執行的應用程式，能夠擁有哪些許可來和其他的 AWS 服務進行互動。您可以選擇 Custom (自訂)，來指定自己的角色。我們建議剛開始先使用預設的角色。如需更多詳細資訊，請參閱 將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 (p. 156) 。

步驟 3：允許從用戶端到叢集的 SSH 連線

安全群組就像是虛擬防火牆，可控管傳入和傳出叢集的流量。建立您的第一個叢集時，Amazon EMR 會建立與主執行個體關聯的預設 Amazon EMR 受管安全群組 ElasticMapReduce-master 和與核心和任務節點關聯的安全群組 ElasticMapReduce-slave。

Warning

系統會使用可允許在連接埠 22 上來自所有來源 (IPv4 0.0.0.0/0) 之傳入流量的規則，來預先設定適用於公有子網路中主執行個體的預設 EMR 受管安全群組 ElasticMapReduce-master。這麼做可簡化 SSH 用戶端到主節點的初始連接。我們強烈建議您編輯此傳入規則，來限制只接收來自信任來源的流量或指定會限制存取的自訂安全群組。

不需修改安全群組就能完成此教學，但我們建議您不要允許來自所有來源的傳入流量。此外，如果其他使用者根據此建議，編輯 ElasticMapReduce-master 安全群組來消除這個規則，您就無法使用 SSH 存取後續步驟所用的叢集。如需關於安全群組的詳細資訊，請參閱 Amazon VPC User Guide 中的 [使用安全群組控制網路流量 \(p. 230\)](#) 和 [適用於 VPC 的安全群組](#)。

針對 ElasticMapReduce-master 安全群組來移除可允許使用 SSH 進行公用存取的傳入規則

下列程序假設 ElasticMapReduce-master 安全群組先前未曾經過編輯。此外，若要編輯安全群組，您還必須以根使用者身分或可讓您管理叢集所在 VPC 之安全群組的 IAM 委託人身分，來登入 AWS。如需詳細資訊，請參閱 IAM User Guide 中的 [變更 IAM 使用者的許可](#) 和允許管理 EC2 安全群組的 [範例政策](#)。

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Clusters (叢集)。
3. 選擇叢集的 Name (名稱)。

4. 在 Security and access (安全性與存取) 中，選擇 Security groups for Master (主叢集的安全群組) 連結。
5. 從清單中選擇 ElasticMapReduce-master (ElasticMapReduce-master)。
6. 選擇 Inbound (傳入)、Edit (編輯)。
7. 尋找具有下列設定的規則，然後選擇 x 圖示來刪除該規則：
 - 類型
 - SSH
 - 連接埠
 - 22
 - 來源
 - 自訂 0.0.0.0/0
8. 向下捲動到規則清單底部，然後選擇 Add Rule (新增規則)。
9. 針對 Type (類型)，選擇 SSH (SSH)。

這會自動輸入 TCP 作為 Protocol (通訊協定)，並輸入 22 作為 Port Range (連接埠範圍)。
10. 針對來源，選擇 My IP (我的 IP)。

這會自動將您用戶端電腦的 IP 地址，新增為來源地址。或者，您可以新增各種 Custom (自訂) 的受信任用戶端 IP 地址，然後選擇 Add rule (新增規則)，來為其他的用戶端建立額外的規則。在許多的網路環境中，IP 地址是動態分配的，因此您可能會需要定期編輯安全群組規則，來更新受信任用戶端的 IP 地址。
11. 選擇 Save (儲存)。
12. (選擇性) 從清單中選擇 ElasticMapReduce-slave (ElasticMapReduce-slave)，並重複上述的步驟，以允許 SSH 用戶端從受信任的用戶端存取核心節點和任務節點。

步驟 4：將 Hive 指令碼做為步驟執行以處理資料

在您的叢集啟動和執行之後，就可以提交 Hive 指令碼。在本教學課程中，您會使用 Amazon EMR 主控台，來將 Hive 指令碼做為步驟提交。在 Amazon EMR 中，步驟是包含一個以上任務的工作單位。如步驟 2：啟動範例 Amazon EMR 叢集 (p. 10) 中的教學，您可以將步驟提交到長時間執行的叢集，我們將在本項步驟中完成這個動作。您也可以在建立叢集時指定步驟，或者您可以連線到主節點、在本機檔案系統中建立指令碼，然後使用命令列來執行這些指令碼，例如 `hive -f Hive_CloudFront.q`。

了解資料和指令碼

在您可以存取的 Amazon S3 位置中，已經提供您於本教學課程中所使用的範例資料和指令碼。

範例資料是一系列的 Amazon CloudFront 存取日誌檔。如需關於 CloudFront 和日誌檔案格式的詳細資訊，請參閱 [Amazon CloudFront Developer Guide](#)。資料儲存於 Amazon S3 中 (`s3://region.elasticmapreduce.samples/cloudfront/data`)，其中 `region (##)` 是您的區域，例如 `us-west-2`。當您提交步驟時，如果輸入位置，會略過 `cloudfront/data` 的部分，因為指令碼自己會將這部分加上去。

CloudFront 日誌檔中的每個項目會以下列格式提供單一使用者請求的相關詳細資訊：

```
2014-07-05 20:00:00 LHR3 4260 10.0.0.15 GET eabcd12345678.cloudfront.net /test-image-1.jpeg 200 - Mozilla/5.0%20(MacOS;%20U;%20Windows%20NT%205.1;%20en-US;%20rv:1.9.0.9)%20Gecko/2009040821%20IE/3.0.9
```

範例指令碼會計算在指定的時間範圍內，每個作業系統的請求總數。使用 HiveQL 的指令碼，這是一種類似 SQL 指令碼語言，可用於資料倉儲和分析。指令碼儲存於 Amazon S3 中 (`s3://region.elasticmapreduce.samples/cloudfront/code/Hive_CloudFront.q`)，其中 `region` (##) 是您的區域。

範例 Hive 指令碼看起來會像下面這樣：

- 建立名為 `cloudfront_logs` 的 Hive 資料表結構描述。如需關於 Hive 資料表的詳細資訊，請參閱 Hive wiki 上的 [Hive 教學](#)。
 - 使用內建的一般表達式序列化程式/去序列化程式 (RegEx SerDe)，來剖析輸入的資料和套用資料表結構描述。如需詳細資訊，請參閱 Hive wiki 上的 [SerDe](#)。
 - 對 `cloudfront_logs` 資料表執行 HiveQL 查詢，並將查詢的結果寫入您指定的 Amazon S3 輸出位置。

下列顯示 `Hive_CloudFront.q` 指令碼的內容。 `${INPUT}` 和 `${OUTPUT}` 變數，會換成您在將指令碼做為步驟提交時，所指定的 Amazon S3 位置。當您如同下列指令碼參考 Amazon S3 中的資料時，Amazon EMR 會使用 EMR 檔案系統 (EMRFS) 來讀取輸入資料和寫入輸出資料。

提交 Hive 指令碼做為步驟

利用 Add Step (新增步驟) 選項，透過主控台來將 Hive 指令碼提交到叢集。Hive 指令碼和範例資料已上傳到 Amazon S3，而且您會將輸出的位置，指定為先前在[建立 Amazon S3 儲存貯體 \(p. 9\)](#)中所建立的資料夾。

將 Hive 指令碼當做步驟提交以執行

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
 2. 在 Cluster List (叢集清單) 中，選擇叢集的名稱。請確定叢集處於 Waiting (等待中) 狀態。
 3. 選擇 Steps (步驟)，然後選擇 Add step (新增步驟)。
 4. 根據下列的準則來設定步驟：

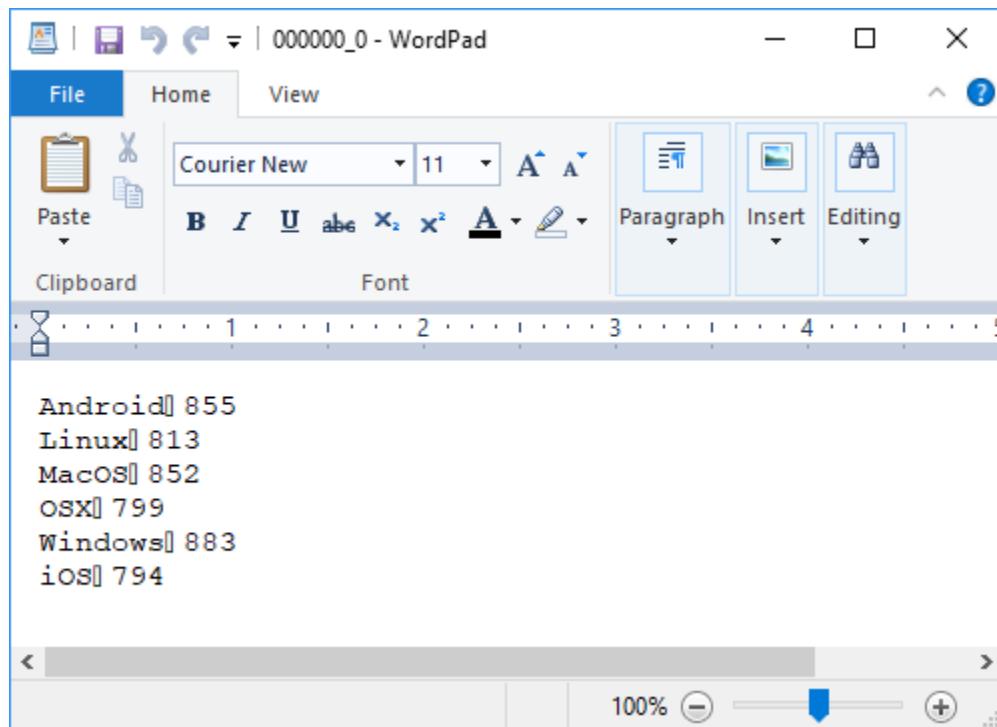
- 針對 Step type (步驟類型) , 選擇 Hive program (Hive 程式)。
 - 針對 Name (名稱) , 您可以保留預設值或輸入新的名稱。如果您的叢集中有許多步驟，名稱可幫助您追蹤這些步驟。
 - 針對 Script S3 location (指令碼 S3 位置) , 輸入 `s3://region.elasticmapreduce.samples/cloudfront/code/Hive_CloudFront.q`。將 `region (##)` 換成您的區域識別符。例如，如果您是在 Oregon (奧勒岡) 區域中使用，請輸入 `s3://us-west-2.elasticmapreduce.samples/cloudfront/code/Hive_CloudFront.q`。如需區域的清單和對應的區域識別符，詳細資訊請參閱 AWS General Reference 中的 [Amazon EMR 的 AWS 區域和端點](#)。
 - 針對 Input S3 location (輸入 S3 位置) , 輸入 `s3://region.elasticmapreduce.samples` 將 `region (##)` 換成您的區域識別符。
 - 針對 Output S3 location (輸出 S3 位置) , 輸入或瀏覽至您在 [建立 Amazon S3 儲存貯體 \(p. 9\)](#) 中所建立的 output 儲存貯體。
 - 針對 Action on failure (失敗時執行的動作) , 接受預設選項 Continue (繼續)。這會指定在步驟失敗時，叢集持續執行和處理後續的步驟。Cancel and wait (取消和等待) 選項指定應該取消失敗的步驟、後續的步驟不應執行，但叢集應繼續執行。Terminate cluster (終止叢集) 選項指定叢集應在步驟失敗時終止。
- 選擇 Add (新增)。該步驟會出現於主控台中，而且狀態為 Pending (待定)。
 - 隨著步驟的執行，步驟的狀態會依序從 Pending (待定)、Running (執行中) 變成 Completed (完成)。若要更新狀態，請選擇 Filter (篩選條件) 右方的重新整理圖示。指令碼的執行約需花費一分鐘的時間。

檢視結果

步驟順利完成之後，會將 Hive 查詢輸出以文字檔的格式，儲存到您在提交步驟時所指定的 Amazon S3 輸出資料夾中。

要查看 Hive 指令碼的輸出

- Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
- 先選擇 Bucket name (儲存貯體名稱)，然後再選擇您先前設定的資料夾。例如，先選擇 `mybucket`，然後再選擇 `MyHiveQueryResults`。
- 查詢會將結果寫入您輸出資料夾中名為 `os_requests` 的資料夾。選擇該資料夾。資料夾中應該存在一個名為 `000000_0` 的檔案。這是一個文字檔案，其中包含您的 Hive 查詢結果。
- 選取該檔案，然後選擇 Download (下載)，將該檔案儲存到本機上。
- 使用您偏好的文字編輯器來開啟該檔案。在輸出檔中，會顯示作業系統所提出存取要求的數量。下列範例顯示 WordPad 中的輸出：



步驟 5：終止叢集和刪除儲存貯體

在完成教學課程後，您最好終止叢集，並刪除 Amazon S3 儲存貯體，以避免產生額外的費用。

終止您的叢集時，會終止相關的 Amazon EC2 執行個體，並停止 Amazon EMR 費用的計費。Amazon EMR 會免費保留關於已完成叢集的中繼資料，為期兩個月，以供您參考。主控台並未提供方法來刪除已終止的叢集，因此在主控台中無法檢視這些叢集。當中繼資料移除時，已終止的叢集會從叢集中移除。

終止叢集

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Clusters (叢集)、選擇您的叢集，然後選擇 Terminate (終止)。

通常會在終止保護開啟的情況下建立叢集，有助於避免意外關機。如果您確實遵循教學課程的指示操作，終止保護功能應為關閉。如果終止保護功能開啟，在終止叢集之前，系統會提示您變更設定 (做為預防措施)。選擇 Change (變更)、Off (關閉)。

刪除輸出儲存貯體

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. 從清單中選擇儲存貯體，以選取整個儲存貯體資料列。
3. 選擇刪除儲存貯體、輸入儲存貯體的名稱，然後按一下 Confirm (確認)。

如需關於刪除資料夾和儲存貯體的詳細資訊，請參閱 Amazon Simple Storage Service Getting Started Guide中的[我要如何刪除 S3 儲存貯體](#)。

使用 Amazon EMR 筆記本

使用 Amazon EMR 筆記本，透過 Amazon EMR 主控台來建立和開啟 Jupyter 筆記本。您可以使用 EMR 筆記本 搭配執行 Apache Spark 的 Amazon EMR 叢集，來執行查詢和程式碼。EMR 筆記本 是「無伺服器」Jupyter 筆記本。與傳統的筆記本不同，— 本身的 EMR 筆記本 內容 (等式、視覺化項目、查詢、模型、程式碼和描述文字 —)，會另外儲存於 Amazon S3 中，和執行程式碼的叢集分開。這為 EMR 筆記本 提供了持久的儲存、具效率的存取和靈活性。

若要在 EMR 筆記本 內執行程式碼和查詢，需使用 Amazon EMR 叢集，但筆記本未鎖定至叢集。這可讓支援暫時性叢集變得更有效率。您可以啟動叢集、將 EMR 筆記本 連接到該叢集，和終止叢集。筆記本仍會持續存在，因此下次想要分析資料或建立資料的模型時，您可以建立另一個叢集，然後將同一個筆記本連接到該叢集。

您也可以停止已經連接到執行中叢集的 EMR 筆記本，然後變更叢集。您可以連接到另一個執行中的叢集，或是建立新的叢集，而不需重新設定筆記本或終止叢集。這些功能可讓您隨需執行叢集，以節省成本。此外，如果想要針對不同的叢集或資料集使用同一個筆記本，您也可以省下重新設定筆記本的時間。

Amazon S3 儲存和 Amazon EMR 叢集的使用，將會產生費用。

主題

- [使用 EMR 筆記本 的考量 \(p. 18\)](#)
- [建立筆記本 \(p. 19\)](#)
- [為筆記本建立 Amazon EMR 叢集 \(p. 19\)](#)
- [使用筆記本 \(p. 21\)](#)
- [監控 Spark 使用者與任務活動 \(p. 24\)](#)
- [EMR 筆記本安全性與存取控制 \(p. 25\)](#)
- [使用筆記本範圍程式庫 \(p. 25\)](#)
- [建立 Git 儲存庫與 Amazon EMR 筆記本的關聯性 \(p. 27\)](#)

使用 EMR 筆記本 的考量

EMR 筆記本 會執行 Jupyter Notebook 5.7.0 版和 Python 3.6.5。

EMR 筆記本 預先設定了下列的核心，並且已安裝程式庫套件。

核心

- PySpark
- PySpark3
- Python3
- Spark
- SparkR

程式庫套件

- [64 位元 Linux 搭配 Python 3.6 的套件](#)

如果您需要其他的程式庫供所有使用者存取，請利用引導操作，或是在建立叢集時，為 Amazon EMR 指定自訂的 Amazon Linux AMI，來安裝這些項目。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#) 及 [使用自訂 AMI \(p. 79\)](#)。

使用 Amazon EMR 5.26.0 和更新版本，您可以從筆記本編輯器中安裝其他的程式庫套件。這些程式庫是 筆記本範圍 的程式庫。它們僅適用於目前的筆記本工作階段。它們不會干擾整個叢集範圍的程式庫或其他筆記本中安裝的程式庫。如需詳細資訊，請參閱 [使用筆記本範圍程式庫 \(p. 25\)](#)。

您搭配 EMR 筆記本 使用的叢集，須符合某些要求。您可以搭配叢集使用的筆記本數量，會受到主節點組態的限制。如需更多詳細資訊，請參閱 [為筆記本建立 Amazon EMR 叢集 \(p. 19\)](#)。

建立筆記本

您可以使用 Amazon EMR 主控台來建立 EMR 筆記本。不支援使用 AWS CLI 或 Amazon EMR API 來建立筆記本。

建立 EMR 筆記本

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Notebooks (筆記本)、Create notebook (建立筆記本)。
3. 輸入 Notebook name (筆記本名稱) 和選填的 Notebook description (筆記本說明)。
4. 如果您擁有作用中的叢集 (執行 Hadoop、Spark 和 Livy)，而您想要將其連接到筆記本，請保留預設值、選擇 Choose (選取)、從清單中選擇叢集，然後選擇 Choose cluster (選取叢集)。只有符合要求的叢集才會列出。

—或—

選擇 Create a cluster (建立叢集)、輸入 Cluster name (叢集名稱)，然後為叢集選擇 EC2 執行個體的數量和類型。一個執行個體用來託管主節點，其他的執行個體則都是用於核心節點。如有必要，您也可以選擇自訂服務角色和 EC2 執行個體描述檔。如需更多詳細資訊，請參閱 [在建立筆記本時建立叢集 \(p. 20\)](#)。

5. 對於 Security groups (安全群組)，選擇 Use default security groups (使用預設的安全群組)。或者，請選擇 Choose security groups (選擇安全群組)，然後選擇自訂安全群組。您會分別針對主執行個體和筆記本服務，各為其選擇一個安全群組。如需更多詳細資訊，請參閱 [the section called “EMR 筆記本的安全群組” \(p. 236\)](#)。
6. 對於 AWS Service Role (AWS 服務角色)，請保留預設值，或從清單中選擇自訂角色。如需更多詳細資訊，請參閱 [EMR 筆記本的服務角色 \(p. 165\)](#)。
7. 對於 Notebook location (筆記本位置)，選擇 Amazon S3 中儲存筆記本檔案的位置，或是指定您自己的位置。如果儲存貯體和資料夾不存在，Amazon EMR 會建立這些項目。

Amazon EMR 會建立資料夾，並使用 Notebook ID (筆記本 ID) 來做為資料夾的名稱，然後將筆記本儲存到名為 `NotebookName.ipynb` 的檔案。例如，如果為名為 MyFirstEMRManagedNotebook 的筆記本，指定了 Amazon S3 位置 `s3://MyBucket/MyNotebooks`，則筆記本檔案會儲存到 `s3://MyBucket/MyNotebooks/NotebookID/MyFirstEMRManagedNotebook.ipynb`。

8. 或者，您可以選擇 Tags (標籤)，然後為筆記本新增任何額外的索引鍵/值標籤。

Important

為了進行存取，會使用預設的標籤，此標籤的 Key (索引鍵) 字串設定為 `creatorUserID`，其值設定為您的 IAM 使用者 ID。我們建議您不要變更或移除此標籤，因為該標籤可用來控制存取。如需詳細資訊，請參閱 [使用叢集和筆記本標籤搭配 IAM 政策來進行存取控制 \(p. 155\)](#)。

為筆記本建立 Amazon EMR 叢集

在建立筆記本或變更叢集時，您可以讓 Amazon EMR 建立新的叢集和筆記本，也可以選擇先前已經建立的叢集。建立新的叢集加上筆記本，可讓您快速開始使用。如果需要安裝額外的應用程式、使用 SSH 來連線到

叢集，或是在建立叢集時需要 Amazon EMR 提供的其他自訂項目（例如使用者模擬），則事先建立叢集會非常有幫助。

每個叢集的筆記本限制

在建立支援筆記本的叢集時，請考慮叢集主節點的 EC2 執行個體類型。這個 EC2 執行個體的記憶體限制，會決定筆記本的數量（這些是已經準備就緒的筆記本，可在叢集上同時執行程式碼和查詢）。

主節點 EC2 執行個體類型	筆記本的數量
*.medium	2
*.large	4
*.xlarge	8
*.2xlarge	16
*.4xlarge	24
*.8xlarge	24
*.16xlarge	24

在建立筆記本時建立叢集

如果在您建立 EMR 筆記本時，是由 Amazon EMR 建立叢集，則叢集會具有下列的特性和限制：

- 叢集會使用最新的 Amazon EMR 發行版本，以及該發行版本中隨附的 Hadoop、Spark 與 Livy 版本。如需詳細資訊，請參閱 [Amazon EMR Release Guide](#)。
- 叢集建立時沒有 EC2 金鑰對，因此您無法使用 SSH 來連線到叢集的 EC2 執行個體。如果需要 SSH 連線，請先建立叢集，然後在建立 EMR 筆記本時指定該叢集。
- 叢集使用隨需執行個體，以及適用於所有執行個體的同一種執行個體類型。一個執行個體用來託管主節點，其他的執行個體則都是用於核心節點。
- 叢集使用統一執行個體群組態。如需詳細資訊，請參閱 [Amazon EMR Management Guide](#) 中的 [建立使用執行個體機群或統一執行個體群組的叢集](#)。
- 這會在 AWS 帳戶的預設 VPC 中啟動。

如有需要，您可以指定自訂的 AWS 服務角色和安全群組。如需更多詳細資訊，請參閱 [EMR 筆記本的服務角色 \(p. 165\)](#) 及 [為 EMR 筆記本指定 EC2 安全群組 \(p. 236\)](#)。如果您需要其他的自訂項目或不同的設定，請事先使用 Amazon EMR 來建立叢集，然後在您建立筆記本時指定該叢集。

使用現有的 Amazon EMR 叢集

EMR 筆記本只支援使用 Amazon EMR 所建立的叢集。如果您需要更多的處理能力、儲存，或是 Amazon EMR 所提供任何廣泛的叢集自訂功能，可以使用 Amazon EMR 來建立叢集。如需關於建立叢集的詳細資訊，請參閱 [Amazon EMR Management Guide](#) 中的 [規劃和設定叢集](#)。

叢集必須符合下列的要求，才能搭配 EMR 筆記本使用：

- 叢集必須在 EC2-VPC 中啟動。可支援公有和私有子網路。未支援 EC2-Classic 平台。
- 建立叢集必須使用 Amazon EMR 發行版本 5.18.0 或更新的版本。

- 叢集啟動時必須已安裝 Hadoop、Spark 和 Livy。可以安裝其他的應用程式，但 EMR 筆記本 目前只支援 Spark 叢集。
- 不支援使用 Kerberos 身份驗證的叢集。

使用筆記本

在建立 EMR 筆記本 之後，筆記本在短時間內就會啟動。Notebooks (筆記本) 清單中的 Status (狀態) 會顯示 Starting (啟動中)。當筆記本的狀態為 Ready (就緒) 時，您可以開啟該筆記本。如果建立了叢集和筆記本，則筆記本可能要花費較長的時間才會 Ready (就緒)。

Tip

重新整理您的瀏覽器，或選取筆記本清單上方的重新整理圖示，來重新整理筆記本的狀態。

了解筆記本的狀態

在 Notebooks (筆記本) 清單中，EMR 筆記本 可以具有下列的 Status (狀態)。

Status	意義
備妥	您可以使用筆記本編輯器來開啟筆記本。當筆記本處於 Ready (就緒) 狀態時，您可以加以停止或刪除。若要變更叢集，您必須先停止筆記本。如果處於 Ready (就緒) 狀態的筆記本長時間閒置，將會自動停止。
啟動	正在建立筆記本，並將其連接到叢集。筆記本正在啟動時，您無法開啟筆記本編輯器、停止或刪除筆記本，也無法變更叢集。
待定	筆記本已建立，並且正在等待與叢集整合，以完成這項動作。叢集可能仍在佈建資源或回應其他請求。當筆記本處於本機模式時，您可以開啟筆記本編輯器。依附叢集程序的任何程式碼，皆不會執行，而且會失效。
停止中	筆記本正在關閉中，或是正在終止筆記本所連接的叢集。筆記本正在停止時，您無法開啟筆記本編輯器、停止或刪除筆記本，也無法變更叢集。
已停止	筆記本已關閉。只要叢集仍在執行中，您就可以在同一個叢集上啟動筆記本。您可以變更叢集和刪除叢集。
正在刪除	正在從可用叢集的清單中刪除叢集。筆記本檔案 NotebookName.ipynb 仍會保留於 Amazon S3 中，並且繼續產生適用的儲存費用。

使用筆記本編輯器

使用 EMR 筆記本 的好處是，您可以直接從主控台，在 Jupyter 或 JupyterLab 中啟動筆記本。

使用 EMR 筆記本 時，您可以從 Amazon EMR 主控台存取您熟悉的開放原始碼 Jupyter 筆記本編輯器或 JupyterLab。由於筆記本編輯器是在 Amazon EMR 主控台中啟動，因此相較於 Amazon EMR 叢集上所託管

的筆記本，前者可更有效率地設定存取。您不需要設定使用者的用戶端，才能透過 SSH 進行 Web 存取、使用安全群組規則和代理組態。如果使用者擁有足夠的許可，只要在 Amazon EMR 主控台中開啟筆記本編輯器即可。

在 Amazon EMR 中，一次只有一個使用者能夠開啟 EMR 筆記本。如果有另一個使用者嘗試開啟已經開啟的 EMR 筆記本，就會發生錯誤。

Important

Amazon EMR 會為每個筆記本編輯器工作階段建立一個唯一的預先簽章 URL，該 URL 僅在短時間內有效。我們建議您不要共用筆記本編輯器 URL。這樣做會產生安全性風險，因為 URL 的收件人會使用您的許可來編輯筆記本，並在 URL 的生命週期內執行筆記本程式碼。如果其他人需要存取筆記本，可透過許可政策提供許可給他們的 IAM 使用者。如需更多詳細資訊，請參閱 [the section called “安全性” \(p. 25\)](#)。

開啟 EMR 筆記本 的筆記本編輯器

1. 從 Notebooks (筆記本) 清單中，選擇 Status (狀態) 為 Ready (就緒) 或 Pending (待定) 的筆記本。
2. 選擇 Open in JupyterLab (在 JupyterLab 中開啟) 或 Open in Jupyter (在 Jupyter 中開啟)。

新的瀏覽器分頁會開啟 JupyterLab 或 Jupyter 筆記本編輯器。

3. 從 Kernel (核心) 選單中選擇 Change kernel (變更核心)，然後選擇適用於您程式設計語言的核心。

現在已就緒，可以從筆記本編輯器寫入和執行程式碼。

儲存筆記本的內容

當您 在筆記本編輯器中進行作業時，筆記本區塊和輸出的內容，會自動定期儲存到 Amazon S3 中的筆記本檔案。自上次編輯區塊以來沒有變更的筆記本，會在編輯器的筆記本名稱旁，顯示 (autosaved) (已自動儲存)。如果變更尚未儲存，會顯示 unsaved changes (未儲存的變更)。

您可以手動儲存筆記本。從 File (檔案) 選單選擇 Save and Checkpoint (儲存和檢查點)，或是按下 CTRL+S。這會在 Amazon S3 內筆記本資料夾的 checkpoints (檢查點) 資料夾中，建立名為 *NotebookName.ipynb* 的檔案。例如，`s3://MyBucket/MyNotebookFolder/NotebookID/checkpoints/NotebookName.ipynb`。只有最新的檢查點檔案，才會儲存於此位置。

變更叢集

您可以變更的 EMR 筆記本 連接的叢集，而不需變更筆記本自身的內容。您只能針對狀態為 Stopped (已停止) 的筆記本，來變更叢集。

變更 EMR 筆記本 的叢集

1. 如果您想要變更的筆記本正在執行中，請從 Notebooks (筆記本) 清單中選擇該筆記本，然後選擇 Stop (停止)。
2. 當筆記本的狀態為 Stopped (已停止) 時，請從 Notebooks (筆記本) 清單中選擇筆記本，然後選擇 View details (檢視詳細資訊)。
3. 選擇 Change cluster (變更叢集)。
4. 如果您擁有作用中的叢集 (執行 Hadoop、Spark 和 Livy)，而您想要將其連接到筆記本，請保留預設值，然後從清單中選擇該叢集。只有符合要求的叢集才會列出。

—或—

選擇 Create a cluster (建立叢集)，然後選擇叢集選項。如需更多詳細資訊，請參閱 [在建立筆記本時建立叢集 \(p. 20\)](#)。

- 針對 Security groups (安全群組) 選擇選項，然後選擇 Change cluster and start notebook (變更叢集並啟動筆記本)。

刪除筆記本和筆記本檔案

當您使用 Amazon EMR 主控台來刪除 EMR 筆記本時，會從可用筆記本的清單中刪除筆記本。不過，筆記本檔案仍會保留於 Amazon S3 中，並且繼續產生儲存費用。

刪除筆記本並移除相關檔案

- Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
- 選擇 Notebooks (筆記本)、從清單中選擇筆記本，然後選擇 View details (檢視詳細資訊)。
- 選取 Notebook location (筆記本位置) 旁的資料夾圖示，然後複製 URL (URL) (格式為 s3://*MyNotebookLocationPath/NotebookID*)。
- 選擇 Delete (刪除)。

會從清單中移除該筆記本，而且無法再檢視其詳細資訊。

- 請遵循 Amazon Simple Storage Service Console User Guide 中 [如何從 S3 儲存貯體刪除資料夾](#) 的說明。從步驟 3 瀏覽到儲存貯體和資料夾。

—或—

如果您已安裝 AWS CLI，請開啟命令提示字元，然後輸入本段結尾的指令。將 Amazon S3 位置換成您在前面內容中所複製的位置。請確定 AWS CLI 已設定使用者的存取金鑰 (該使用者具有刪除 Amazon S3 位置的許可)。如需詳細資訊，請參閱 AWS Command Line Interface User Guide 中的 [設定 AWS CLI](#)。

```
aws s3 rm s3://MyNotebookLocationPath/NotebookID
```

共用筆記本檔案

每個 EMR 筆記本 會儲存到 Amazon S3 (成為名稱是 *NotebookName.ipynb* 的檔案)。只要筆記本檔案和 EMR 筆記本 所採用的同一個 Jupyter Notebook 版本相容，您就可以將筆記本開啟為 EMR 筆記本。您可以將 EMR 筆記本 的檔案，換成名稱相同的不同筆記本檔案。

您可以利用這項程序，來使用別人分享的 EMR 筆記本、Jupyter 社群中所分享的筆記本，或是在筆記本檔案仍存在時，回復已經從主控台刪除的筆記本。

使用不同的筆記本檔案做為 EMR 筆記本的根據

- 在繼續進行之前，請針對您將會使用的任何筆記本，關閉其筆記本編輯器，接著，如果筆記本是 EMR 筆記本，請加以停止。
- 建立 EMR 筆記本，並且輸入其名稱。您為筆記本所輸入的名稱，將會成為需替換檔案的名稱。新的檔案名稱必須和這個檔案名稱完全符合。
- 請記下您為筆記本選擇的 Amazon S3 位置。您替換的檔案位於資料夾中，具有如同下列格式的路徑和檔案名稱：s3://*MyNotebookLocation/NotebookID/MyNotebookName.ipynb*。
- 停止筆記本。
- 將 Amazon S3 位置中的舊筆記本檔案換成新的 (使用完全的相同名稱)。

適用於 Amazon S3 的下列 AWS CLI 指令，會將已儲存至本機、名為 SharedNotebook.ipynb 的檔案，換成 EMR 筆記本 (名稱為 MyNotebook (我的筆記本))、ID 為 e-12A3BCDEFJHIJKLMNOP45PQRST，而且建立時使用 Amazon S3 中指定的 MyBucket/

MyNotebooksFolder。關於使用 Amazon S3 主控台來複製和取代檔案，請參閱 Amazon Simple Storage Service Console User Guide中的[上傳、下載和管理物件](#)。

```
aws s3 cp SharedNotebook.ipynb s3://MyBucket/  
MyNotebooksFolder/-12A3BCDEFJHIJKLMNOP45PQRST/MyNotebook.ipynb
```

監控 Spark 使用者與任務活動

EMR 筆記本 可讓您在 Spark叢集上設定使用者模擬。此功能可協助您追蹤從筆記本編輯器起始的任務活動。此外，EMR 筆記本 具有內建的 Jupyter 筆記本小工具，可讓您在筆記本檢視器中，檢視 Spark 任務詳細資訊和查詢輸出。這項小工具為預設提供，不需要進行特別的設定。不過，若要檢視歷程記錄伺服器，必須設定您的用戶端，以檢視主節點上所託管的 Amazon EMR Web 界面。

設定 Spark 使用者模擬

根據預設，使用者透過筆記本編輯器所提交的 Spark 任務，似乎源自於模糊的 livy 使用者身分。您可以為該叢集設計使用者模擬，如此這些任務就會改為和執行程式碼的 IAM 使用者身分具有關聯。會針對在筆記本中執行程式碼的每個使用者身分，在主節點上建立 HDFS 使用者目錄。例如，如果使用者 NbUser1 從筆記本編輯器執行程式碼，您可以連線到主節點，然後檢視 hadoop fs -ls /user 顯示的目錄 /user/_NbUser1。

若要啟用這項功能，您可以在 core-site 和 livy-conf 組態分類中設定屬性。當您讓 Amazon EMR 同時建立叢集和筆記本時，這項功能預設不能使用。關於使用組態分類來自訂應用程式，詳細資訊請參閱 Amazon EMR Release Guide 中的 [設定應用程式](#)。

使用下列的組態分類和值，來啟用 EMR 筆記本 的使用者模擬功能：

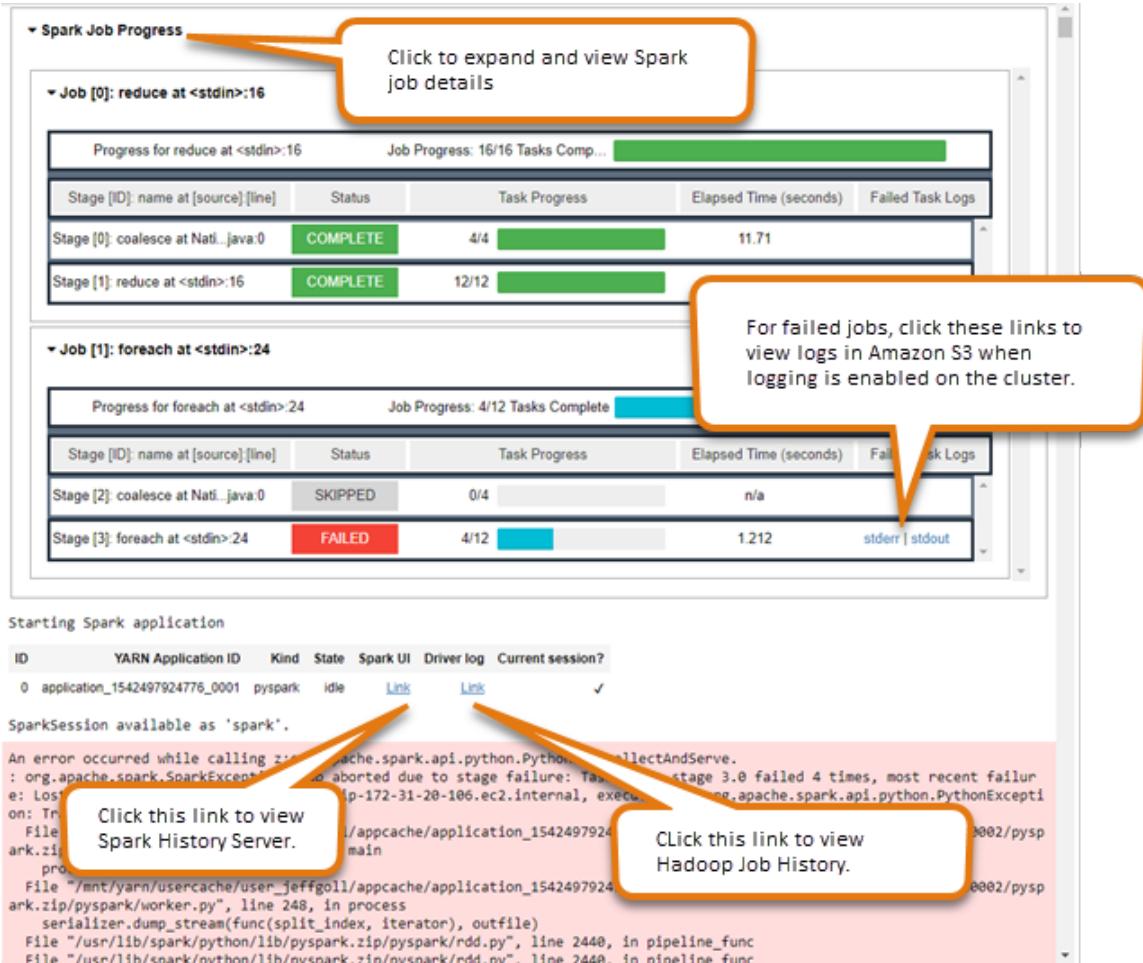
```
[  
  {  
    "Classification": "core-site",  
    "Properties": {  
      "hadoop.proxyuser.livy.groups": "*",  
      "hadoop.proxyuser.livy.hosts": "*"  
    }  
  },  
  {  
    "Classification": "livy-conf",  
    "Properties": {  
      "livy.impersonation.enabled": "true"  
    }  
  }  
]
```

使用 Spark 任務監控小工具

當您在筆記本編輯器中執行程式碼，來執行 EMR 叢集上的 Spark 任務時，輸入會包括用來監控 Spark 任務的 Jupyter 筆記本小工具。這項小工具會提供任務詳細資訊和實用的連結(連結到 Spark 歷程記錄伺服器頁面與 Hadoop 任務歷程記錄頁面)，以及便利的連結，可針對任何失敗的任務，連結到 Amazon S3 中的任務日誌。

若要檢視叢集主節點上的歷程記錄伺服器頁面，您必須適當地設置 SSH 用戶端與代理。如需更多詳細資訊，請參閱 [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。若要檢視 Amazon S3 中的日誌，必須啟用叢集日誌記錄，這是新叢集的預設功能。如需更多詳細資訊，請參閱 [檢視封存到 Amazon S3 的日誌檔 \(p. 252\)](#)。

下列是 Spark 任務監控小工具的範例。



EMR 筆記本安全性與存取控制

有幾個功能可協助您量身打造 EMR 筆記本的安全狀態。這有助於確保只有授權使用者才能存取 EMR 筆記本、使用筆記本，以及使用筆記本編輯器來在叢集上執行程式碼。這些功能可和 Amazon EMR 與 Amazon EMR 叢集的安全功能一起運作。如需詳細資訊，請參閱 [Amazon EMR 中的安全性 \(p. 127\)](#)。

- 您可以使用 AWS Identity and Access Management 政策陳述式搭配筆記本標籤，來限制存取。如需更多詳細資訊，請參閱 [條件金鑰 \(p. 155\)](#) 及 [EMR 筆記本的身分類型政策陳述式範例 \(p. 186\)](#)。
- EC2 安全群組可做為虛擬防火牆，控管叢集的主執行個體和筆記本編輯器之間的網路流量。您可以使用預設值或自訂這些安全群組。如需更多詳細資訊，請參閱 [為 EMR 筆記本指定 EC2 安全群組 \(p. 236\)](#)。
- 您可以指定 AWS 服務角色，來決定 EMR 筆記本在和其他的 AWS 服務進行互動時，擁有哪些許可。如需更多詳細資訊，請參閱 [EMR 筆記本的服務角色 \(p. 165\)](#)。

使用筆記本範圍程式庫

如果叢集上的提供適用於 EMR 筆記本的預設程式庫無法滿足您的應用程式，使用 Amazon EMR 5.26.0 和更新版本，您可以從公有或私有 Python Package Index (PyPI) 儲存庫的筆記本編輯器中安裝 筆記本範圍的 Python 程式庫。筆記本範圍程式庫是在 Python 虛擬環境中安裝至目前的筆記本工作階段。它們僅適用於筆記本工作階段期間可用。工作階段結束後，程式庫將被刪除。後續工作階段將無法使用程式庫。若要在

EMR 筆記本工作階段之間提供程式庫，請利用引導操作或適用於 EMR 的自訂 Amazon Linux AMI，在叢集執行個體上安裝程式庫。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#) 及 [使用自訂 AMI \(p. 79\)](#)。

筆記本範圍的程式庫提供下列優點：

- 您可以在 EMR 筆記本 中使用程式庫且無需重新建立叢集或將筆記本重新連接至叢集。
- 您可以隔離 EMR 筆記本 的程式庫相依性與個別筆記本工作階段。從筆記本內安裝的程式庫無法干擾叢集上的其他程式庫，或是在其他筆記本工作階段中安裝的程式庫。

考量事項與限制

使用筆記本範圍的程式庫時，請考慮以下事項：

- 您只能解除安裝使用 `install_pypi_package` API 安裝的程式庫。您無法解除安裝叢集上安裝的任何程式庫。
- 如果叢集上安裝不同版本的相同程式庫，並做為筆記本範圍的程式庫，則筆記本範圍的程式庫版本會覆寫叢集程式庫版本。

使用筆記本範圍程式庫

若要安裝程式庫，您的 Amazon EMR 叢集必須能夠存取程式庫所在的 PyPI 儲存庫。例如，對於私有子網路中的叢集，您可能需要設定網路位址轉譯 (NAT) 並提供路徑，讓叢集存取位於叢集 VPC 外部的儲存庫。如需有關為不同網路組態設定外部存取的詳細資訊，請參閱 Amazon VPC User Guide 中的 [案例和範例](#)。

根據預設，Python 2 是用來建立環境。若要使用 Python 3，您可以在筆記本儲存格中執行下列指令來設定 PySpark 屬性，以重新設定筆記本工作階段。

```
%%configure -f
{ "conf": {
  "spark.pyspark.python": "python3",
  "spark.pyspark.virtualenv.enabled": "true",
  "spark.pyspark.virtualenv.type": "native",
  "spark.pyspark.virtualenv.bin.path": "/usr/bin/virtualenv"
}}
```

以下範例示範使用 PySpark API 從筆記本儲存格內列出、安裝和解除安裝程式庫的指令。

Example – 列出目前的程式庫

以下指令列出可用於目前 Spark 筆記本工作階段的 Python 套件。這會列出安裝在叢集上和筆記本範圍的程式庫。

```
sc.list_packages()
```

Example – 安裝 Celery 程式庫

下列指令會將 [Celery](#) 程式庫安裝為筆記本範圍的程式庫。

```
sc.install_pypi_package("celery")
```

安裝程式庫之後，下列指令會確認可在 Spark 驅動程式和執行器上使用該程式庫。

```
import celery
sc.range(1,10000,1,100).map(lambda x: celery.__version__).collect()
```

Example – 安裝 Arrow 程式庫，指定版本和儲存庫

以下指令會將 Arrow 程式庫安裝為筆記本範圍的程式庫，並指定程式庫版本和儲存庫 URL。

```
sc.install_pypi_package("arrow==0.14.0", "https://pypi.org/simple")
```

Example – 解除安裝程式庫

下列指令會解除安裝 Arrow 程式庫，並將其做為筆記本範圍的程式庫從目前工作階段中移除。

```
sc.uninstall_package("arrow")
```

建立 Git 儲存庫與 Amazon EMR 筆記本的關聯性

您可以建立 Git 儲存庫與 Amazon EMR 筆記本的關聯性，將筆記本儲存在版本受控的環境中。您可以將多達三個儲存庫與筆記本建立關聯。Git 儲存庫必須透過下列以 Web 為基礎的 Git 託管服務進行託管：GitHub 或 Bitbucket。建立 Git 儲存庫與您筆記本的關聯性有利於：

- 版本控制 – 將筆記本存放在 Git 儲存庫，您便可在版本控制系統中記錄程式碼變更，進而檢閱變更的歷程記錄，以及選擇性地反轉某些變更。
- 協同合作 – 將筆記本存放在 Git 儲存庫中，可讓使用不同筆記本的同事透過遠端 Git 儲存庫共享程式碼。筆記本可以從遠端 Git 儲存庫複製或合併程式碼，然後將變更推回至這些遠端儲存庫。
- 程式碼重複使用 – 許多示範資料分析或機器學習技巧的 Jupyter 筆記本，可於 GitHub 等公開託管的 Git 儲存庫中取得。您可以建立筆記本與儲存庫的關聯性，重複使用該儲存庫所包含的 Jupyter 筆記本。

建立 Git 儲存庫與筆記本的關聯性前，您必須確認您的叢集、IAM 角色和安全群組具備正確的設定與權限。

- 筆記本連接的叢集必須位於具有網路位址轉譯 (NAT) 閘道的私有子網路中，或必須能夠透過虛擬私有閘道存取網際網路。如需詳細資訊，請參閱 [Amazon VPC 選項](#)。
- 如果您需要儲存庫的私密金鑰，EMR Notebooks 的服務角色在其 IAM 政策中必須具備 `secretsmanager:GetSecretValue` 權限。如需詳細資訊，請參閱 [EMR Notebooks 的服務角色](#)。
- 筆記本的安全群組必須包含傳出規則，讓筆記本能夠透過叢集將流量路由傳送到網際網路。建議您建立自己的安全群組。如需詳細資訊，請參閱 [為 EMR Notebook 指定 EC2 安全群組](#)。

若要管理 Git 儲存庫，請將儲存庫新增為 Amazon EMR 主控台的資源、建立與需要身份驗證之儲存庫登入資料的關聯性，並將這些儲存庫與您的筆記本連結。您可以檢視存放在您帳戶中的儲存庫清單，以及 Amazon EMR 主控台中每個儲存庫的詳細資訊。您也可以透過現有的 Git 儲存庫建立筆記本。

主題

- [將 Git 儲存庫新增至 Amazon EMR \(p. 27\)](#)
- [更新或刪除 Git 儲存庫 \(p. 28\)](#)
- [連結或解除連結 Git 儲存庫 \(p. 28\)](#)
- [使用關聯的 Git 儲存庫建立新筆記本 \(p. 30\)](#)
- [在筆記本中使用 Git 儲存庫 \(p. 30\)](#)

將 Git 儲存庫新增至 Amazon EMR

將 Git 儲存庫新增為您 Amazon EMR 帳戶的資源

1. 開啟位於 <https://console.aws.amazon.com/elasticmapreduce/> 的 Amazon EMR 主控台。

2. 選擇 Git repositories (Git 儲存器) , 然後選擇 Add repository (新增儲存器)。
3. 針對 Repository name (儲存庫名稱) , 在 Amazon EMR 中輸入用於儲存庫的名稱。

名稱僅可含有英數字元、連字號 (-) 或底線 (_)。

4. 針對 Git repository URL (Git 儲存庫 URL) , 輸入儲存庫的 URL。
5. 針對 Branch (分支) , 輸入分支名稱。
6. 針對 Git credentials (Git 登入資料) , 選擇用來向儲存器驗證身分的登入資料。

- 選擇 Use an existing AWS secret (使用現有的 AWS 私密金鑰) , 然後從清單選取私密金鑰。

現有私密金鑰必須使用下列格式 : {"gitUsername": UserName, "gitPassword": Password}。

- 選擇 Create a new secret (建立新的私密金鑰)。
 - 如果您使用 Username and password (使用者名稱和密碼) , 請輸入私密金鑰的名稱 , 然後輸入使用者名稱和密碼。
 - 如果您為 Git 儲存庫啟用了雙重身份驗證 , 請選擇 Personal access token (PAT) (個人存取字符 (PAT))。建議您使用 Git 服務供應商產生的個人存取字符 , 不要使用您的帳戶密碼。如需詳細資訊 , 請參閱[建立 GitHub 命令列的個人存取字符](#)和[Bitbucket 的個人存取字符](#)。
 - 如果 Git 儲存庫是公有儲存庫 , 請選擇 Use a public repository without credentials (使用不需要登入資料的公有儲存庫)。
- 7. 選擇 Add repository (新增儲存器)。

更新或刪除 Git 儲存庫

更新 Git 儲存庫

1. 在 Git repositories (Git 儲存庫) 頁面上 , 選擇您要更新的儲存庫。
2. 在儲存庫頁面上 , 選擇 Edit repository (編輯儲存庫)。
3. 更新儲存庫頁面上的 Git credentials (Git 登入資料)。

刪除 Git 儲存庫

1. 在 Git repositories (Git 儲存庫) 頁面上 , 選擇您要刪除的儲存庫。
2. 在儲存庫頁面上 , 選擇目前已連結到儲存庫的所有筆記本。選擇 Unlink notebook (解除連結筆記本)。
3. 在儲存庫頁面上 , 選擇 Delete (刪除)。

Note

若要從 Amazon EMR 刪除本機 Git 儲存庫 , 您必須先從此儲存庫解除連結所有筆記本。如需詳細資訊 , 請參閱[連結或解除連結 Git 儲存庫 \(p. 28\)](#)。刪除 Git 儲存庫不會刪除為該儲存庫建立的任何私密金鑰。您可以在 AWS Secrets Manager 中刪除私密金鑰。

連結或解除連結 Git 儲存庫

將 Git 儲存庫連結至 EMR 筆記本

當筆記本就緒後 , 即可將儲存庫連結到筆記本。

1. 從 Notebooks (筆記本) 清單中選擇您要更新的筆記本。
2. 在 Notebook (筆記本) 頁面的 Git repositories (Git 儲存庫) 區段中 , 選擇 Link new repository (連結新的儲存庫)。

- 在 Link Git repository to notebook (將 Git 儲存庫連結到筆記本) 視窗的儲存庫清單中，選取您要連結到筆記本的一或多個儲存庫，然後選擇 Link repository (連結儲存庫)。

或

- 在 Git repositories (Git 儲存庫) 頁面上，選擇您要連結到筆記本的儲存庫。
- 在 EMR Notebooks 清單中，選擇 Link new notebook (連結新的筆記本) 以將此儲存庫連結到現有的筆記本。

從 EMR 筆記本解除連結 Git 儲存庫

- 從 Notebooks (筆記本) 清單中選擇您要更新的筆記本。
- 在 Git repositories (Git 儲存庫) 清單中，選取您要從筆記本解除連結的儲存庫，然後選擇 Unlink repository (解除連結儲存庫)。

或

- 在 Git repositories (Git 儲存庫) 頁面上，選擇您要更新的儲存庫。
- 在 EMR Notebooks 清單中，選取您要從儲存庫解除連結的筆記本，然後選擇 Unlink notebook (解除連結筆記本)。

Note

將 Git 儲存庫連結到筆記本時，遠端儲存庫就會複製到本機 Jupyter 筆記本。從筆記本取消連結 Git 儲存庫時，將只有筆記本與遠端儲存庫的連線會中斷，但本機 Git 儲存庫不會刪除。

了解儲存庫狀態

Git 儲存庫的狀態可能是以下任何一種。

Status	意義
正在連結	Git 儲存庫正在連結到筆記本。儲存庫的狀態為正在連結時，您無法停止筆記本。
已連結	Git 儲存庫已連結到筆記本。儲存庫的狀態為已連結時，表示已連線到遠端儲存庫。
連結失敗	Git 儲存庫無法連結到筆記本。您可以再次嘗試將其連結。
正在解除連結	Git 儲存庫正在解除與筆記本的連結。儲存庫的狀態為正在解除連結時，您無法停止筆記本。解除 Git 儲存庫與筆記本的連結只會中斷其與遠端儲存庫的連線，但不會從筆記本刪除任何程式碼。
解除連結失敗	Git 儲存庫無法解除與筆記本的連結。您可以再次嘗試將其解除連結。

使用關聯的 Git 儲存庫建立新筆記本

在 AWS Management Console 中建立筆記本以及建立與 Git 儲存庫的關聯性

1. 按照 [建立筆記本 \(p. 19\)](#) 中的指示進行。
2. 針對 Security group (安全群組) , 選擇 Use your own security group (使用您自己的安全群組)。

Note

筆記本的安全群組必須包含傳出規則，讓筆記本能夠透過叢集將流量路由傳送到網際網路。建議您建立自己的安全群組。如需詳細資訊，請參閱[為 EMR Notebook 指定 EC2 安全群組](#)。

3. 針對 Git repositories (Git 儲存庫) , 選擇儲存庫以建立與筆記本的關聯性。
 1. 選擇存放為帳戶資源的儲存庫，然後選擇 Save (儲存)。
 2. 若要將新的儲存庫新增為帳戶資源，請選擇 add a new repository (新增儲存庫)。在新視窗中完成 Add repository (新增儲存庫) 工作流程。

在筆記本中使用 Git 儲存庫

當您開啟筆記本時，您可以選擇 Open in JupyterLab (在 JupyterLab 中開啟) 或 Open in Jupyter (在 Jupyter 中開啟)。

如果您選擇在 Jupyter 中開啟筆記本，則會顯示筆記本內可展開的檔案和資料夾清單。您可以在筆記本儲存格中，手動執行如下 Git 命令。

```
!git pull origin master
```

若要開啟任何其他儲存庫，請導覽至其他資料夾。

如果您選擇使用 JupyterLab 界面開啟筆記本，jupyter-git 延伸隨即完成安裝，並可供您使用。如需 JupyterLab 之 jupyter-git 延伸的資訊，請參閱[jupyterlab-git](#)。

規劃和設定叢集

本節會介紹各種組態選項，並說明如何使用 Amazon EMR 來規劃、設定、啟動叢集。在啟動叢集之前，請視所要處理的資料，還有您在成本、速度、容量、可用性、安全性、易管理性方面的需求，據此選擇系統的各種選項。選項包含：

- 叢集執行的區域、資料儲存的位置和方式、輸出結果的方式。請參閱「[設定叢集位置和資料儲存體 \(p. 31\)](#)」。
- 叢集要長時間執行，抑或只是暫時性的叢集，以及所要執行的軟體。請參閱[設定叢集自動終止或繼續 \(p. 74\)](#)和[設定叢集軟體 \(p. 85\)](#)。
- 叢集要包含一個主節點或三個主節點。請參閱[規劃和設定主節點 \(p. 46\)](#)。
- 能夠最佳化應用程式成本、效能與可用性的硬體和聯網選項。請參閱[設定叢集硬體和聯網 \(p. 89\)](#)。
- 如何設定叢集，讓您可以更輕鬆地管理和監控活動、效能及運作狀態。請參閱[設定叢集記錄和除錯 \(p. 118\)](#)和[標籤叢集 \(p. 122\)](#)。
- 如何驗證和授權叢集資源存取權限，以及加密資料的方式。請參閱「[Amazon EMR 中的安全性 \(p. 127\)](#)」。
- 與其他軟體和服務整合的方式。請參閱「[驅動程式和第三方應用程式整合 \(p. 125\)](#)」。

設定叢集位置和資料儲存體

本節會說明如何設定叢集的區域以及在使用 Amazon EMR 時所提供的不同檔案系統，還有這些系統的使用方式。也會介紹在有需要時如何準備資料或將資料上傳到 Amazon EMR，以及如何備妥輸出位置給日誌檔和您所設定的輸出資料檔案使用。

主題

- [選擇一個 AWS 區域 \(p. 31\)](#)
- [使用儲存和檔案系統 \(p. 32\)](#)
- [準備輸入資料 \(p. 34\)](#)
- [設定輸出位置 \(p. 41\)](#)

選擇一個 AWS 區域

在全世界資料中心裡伺服器上執行的 Amazon Web Services。資料中心是依地理區域進行組織。在您啟動 Amazon EMR 叢集時，您必須指定區域。您可以選擇區域以減少延遲、降低成本或因應法規需求。如需 Amazon EMR 所支援的區域與端點清單，請參閱 Amazon Web Services General Reference 中的[區域與端點](#)。

為獲得最佳效能，您應該啟動與資料相同區域中的叢集。例如，若 Amazon S3 儲存貯體將您的輸入資料存放在 US West (Oregon) 區域，您應該在 US West (Oregon) 區域中啟動您的叢集，以避免跨區域資料傳輸費用。若您使用一個 Amazon S3 儲存貯體來接收叢集的輸出，您也會想在 US West (Oregon) 區域中建立一個 &S3; 儲存貯體。

若您打算將一個 Amazon EC2 金鑰對關聯至叢集（必須使用 SSH 以登入至主節點），金鑰對必須建立在與叢集相同的區域。同樣地，Amazon EMR 建立用來管理該叢集的安全群組，也是建立在與叢集相同的區域中。

If you signed up for an AWS account on or after May 17, 2017, the default region when you access a resource from the AWS Management Console is US East (Ohio) (us-east-2); for older accounts, the default region is either US West (Oregon) (us-west-2) or US East (N. Virginia) (us-east-1). For more information, see [Regions and Endpoints](#).

某些 AWS 功能僅在限制區域提供。例如，叢集運算執行個體僅在 US East (N. Virginia) 區域、Asia Pacific (Sydney) 區域中提供，並僅支援 1.0.3 與以上版本的 Hadoop。當選擇一個區域時，請檢查該區域支援您想使用的功能。

為獲得最佳效能，請為您所有將與叢集一起使用的 AWS 資源使用相同區域。下表映射了服務間的區域名稱。如需 Amazon EMR 區域的清單，請參閱《Amazon Web Services General Reference》中的 [AWS 區域與終端節點](#)。

使用主控台選擇一個區域

您的預設區域會自動顯示。

使用主控台變更區域

- 若要切換區域，在導覽列上的您的帳戶資訊右方選擇區域清單。

使用 AWS CLI 指定一個區域

使用 aws configure 命令或 AWS_DEFAULT_REGION 環境變數以在 AWS CLI 中指定一個預設區域。如需詳細資訊，請參閱 AWS Command Line Interface User Guide 中的 [設定 AWS 區域](#)。

使用軟體開發套件或 API 選擇一個區域

若要使用軟體開發套件選擇一個區域，請設定您的應用程式以使用該區域的端點。若您正在使用 AWS 開發套件建立一個用戶端應用程式，您可以透過呼叫 setEndpoint 以變更用戶端端點，如下範例所示：

```
client.setEndpoint("elasticmapreduce.us-west-2.amazonaws.com");
```

在透過設定端點讓您的應用程式指定區域後，您可以為叢集的 EC2 執行個體設定可用區域。可用區域是多個不同地理的位置，其在工程設計上是為了與其他可用區域的故障隔離，並能夠以低成本、低延遲的方式，透過網路連線至相同區域中的其他可用區域。一個區域包含一個或更多的可用區域。若要最佳化效能並降低延遲，所有資源都應該位於與使用它們的叢集相同的可用區域。

使用儲存和檔案系統

Amazon EMR 和 Hadoop 提供各式各樣的檔案系統，讓您在處理叢集步驟時使用。您可藉由用來存取資料的 URI 字首指定要使用的檔案系統。例如，`s3://aws-s3-bucket1/path` 會使用 EMRFS 參考 Amazon S3 儲存貯體。下表列出可用的檔案系統，並提供各檔案系統的最佳使用時機建議。

Amazon EMR 和 Hadoop 在處理叢集時，通常會使用下列檔案系統當中的兩種或多種。HDFS 和 EMRFS 是搭配 Amazon EMR 使用的兩種主要檔案系統。

Important

從 Amazon EMR 發行版本 5.22.0 開始，Amazon EMR 只會使用 AWS Signature 第 4 版來驗證對於 Amazon S3 的要求。較早的 Amazon EMR 發行版本會在某些情況下使用 AWS Signature 第 2 版，除非版本備註指出只會使用 Signature 第 4 版。如需詳細資訊，請參閱「Amazon Simple Storage Service 開發人員指南」中的 [驗證要求 \(AWS Signature 第 4 版\)](#) 和 [驗證要求 \(AWS Signature 第 2 版\)](#)。

檔案系統	字首	敘述
HDFS	<code>hdfs://</code> (或不含字首)	HDFS 是一種分散式且具可擴展性的可攜式檔案系統，適用於 Hadoop。HDFS 的優勢在於能夠感知管理叢集的

檔案系統	字首	敘述
		<p>Hadoop 叢集節點與管理個別步驟的 Hadoop 叢集節點之間的資料。如需詳細資訊，請參閱 Hadoop 文件。</p> <p>HDFS 是由主節點和核心節點所使用。其中一個優點是速度快；缺點在於它是暫時性儲存，會在叢集結束時回收。最適合用於快取中繼任務流程步驟所產生的結果。</p>
EMRFS	s3://	<p>EMRFS 是 Hadoop 檔案系統的實作，用途是從 Amazon EMR 直接將一般檔案讀取和寫入至 Amazon S3。EMRFS 提供將持久性資料存放在 Amazon S3 的方便性，可讓您與 Hadoop 搭配使用，同時提供 Amazon S3 伺服器端加密、先寫後讀一致性及清單一致性這類功能。</p> <p>Note</p> <p>以往 Amazon EMR 是使用 S3 原生 FileSystem 搭配 URI 機制 s3n。雖然此方式仍然有效，但我們建議您使用 s3 URI 機制以獲得最佳效能、安全性和可靠性。</p>
本機檔案系統		<p>本機檔案系統是指與本機連接的磁碟。當 Hadoop 叢集建立時，每個節點都會從稱為執行個體存放區的預先連接磁碟儲存體中，預先設定區塊隨附的 EC2 執行個體建立。執行個體存放區磁碟區上的資料只會在 EC2 執行個體的週期內保存。執行個體存放區磁碟區非常適合存放不斷變動的暫存資料，例如緩衝區、快取、臨時資料及其他暫存的內容。如需詳細資訊，請參閱 Amazon EC2 執行個體儲存體。</p>
(舊式) Amazon S3 區塊檔案系統	s3bfs://	<p>Amazon S3 區塊檔案系統是舊式檔案儲存系統。我們非常不建議使用此系統。</p> <p>Important</p> <p>我們建議您不要使用此檔案系統，因為它可能觸發競爭條件，而造成您的叢集失敗。不過，舊版應用程式可能會需要此系統。</p>

Note

不支援 s3a 協定。我們建議您使用 s3 代替 s3a。

存取檔案系統

您可藉由用來存取資料的統一資源識別符 (URI) 字首指定要使用的檔案系統。以下程序說明如何參考數種不同類型的檔案系統。

存取本機 HDFS

- 在 URI 中指定 hdfs:/// 字首。Amazon EMR 會將未在 URI 中指定字首的路徑解析成本機 HDFS。例如，下面兩個 URI 都會解析成 HDFS 中相同的位置。

```
hdfs:///path-to-data
/path-to-data
```

存取遠端 HDFS

- 包含 URI 中主節點的 IP 地址，如以下範例所示。

```
hdfs://master-ip-address/path-to-data  
master-ip-address/path-to-data
```

存取 Amazon S3

- 使用 s3:// 字首。

```
s3://bucket-name/path-to-file-in-bucket
```

存取 Amazon S3 區塊檔案系統

- 僅適用於需要 Amazon S3 區塊檔案系統的舊型應用程式。若要使用此檔案系統存取或存放資料，請在 URI 中使用 s3bfs:// 字首。

Amazon S3 區塊檔案系統是舊式檔案系統，以往用來支援將超過 5 GB 的項目上傳至 Amazon S3。使用 Amazon EMR 透過 AWS Java 軟體開發套件提供的分段上傳功能，就可以將最大 5 TB 的檔案上傳至 Amazon S3 原生檔案系統，而且 Amazon S3 區塊檔案系統已棄用。

Warning

由於此舊式檔案系統可能產生競爭條件，造成檔案系統損毀，因此您應該避免此格式並改用 EMRFS。

```
s3bfs://bucket-name/path-to-file-in-bucket
```

準備輸入資料

大多數叢集會載入輸入資料，然後處理該資料。為了載入資料，其必須處於該叢集可存取的位置並使用該叢集可處理的格式。最常用案例是將輸入資料上傳到 Amazon S3。Amazon EMR 提供您的叢集對於 Amazon S3 匯入或讀取資料的工具。

在 Hadoop 中的預設輸入格式為文字檔案，但您可以自訂 Hadoop 和使用工具以匯入以其他格式存放的資料。

主題

- [Amazon EMR 可接受的輸入類型 \(p. 34\)](#)
- [如何將資料取至 Amazon EMR 中 \(p. 35\)](#)

Amazon EMR 可接受的輸入類型

叢集的預設輸入格式為文字檔，其中每列以換行 (\n) 字元分隔，這是最常用的輸入格式。

如果您的輸入資料是使用預設文字檔案以外的格式，您可以使用 Hadoop 界面 `InputFormat` 來指定其他輸入類型。您甚至可以建立 `FileInputFormat` 的子類別，以處理自訂資料類型。如需詳細資訊，請參閱 <http://hadoop.apache.org/docs/current/api/org/apache/hadoop/mapred/InputFormat.html>。

如果您使用的是 Hive，您可以使用串聯器/解串器 (SerDe) 來將指定格式的資料讀取至 HDFS 中。如需詳細資訊，請參閱 <https://cwiki.apache.org/confluence/display/Hive/SerDe>。

如何將資料取至 Amazon EMR 中

Amazon EMR 提供多種將資料載入到叢集的方式。最常見的方法是將資料上傳至 Amazon S3，並使用 Amazon EMR 內建功能，以將資料載入到您的叢集。您也可以使用 Hadoop 分散式快取功能，將檔案從分散式檔案系統傳輸到本機檔案系統。此 Amazon EMR 提供的 Hive 實作 (Hive 版本 0.7.1.1 和更高版本) 包含可用於匯入和匯出 DynamoDB 和 Amazon EMR 叢集間資料的功能。如果您有要處理的大量現場部署資料，您會發現 AWS Direct Connect 服務很有用。

主題

- [將資料上傳至 Amazon S3 \(p. 35\)](#)
- [使用分散式快取匯入檔案 \(p. 38\)](#)
- [如何處理壓縮檔案 \(p. 41\)](#)
- [將 DynamoDB 資料匯入到 Hive \(p. 41\)](#)
- [使用 AWS DirectConnect 連接資料 \(p. 41\)](#)
- [使用 AWS Import/Export 上傳大量資料 \(p. 41\)](#)

將資料上傳至 Amazon S3

有關如何將物件上傳至 Amazon S3 的詳細資訊，請參閱Amazon Simple Storage Service Getting Started Guide中的[將物件新增到您的儲存貯體](#)。如需有關使用 Amazon S3 搭配 Hadoop 的詳細資訊，請參閱 <http://wiki.apache.org/hadoop/AmazonS3>。

主題

- [建立並設定 Amazon S3 儲存貯體 \(p. 35\)](#)
- [設定適用於 Amazon S3 的分段上傳 \(p. 36\)](#)
- [最佳實務 \(p. 37\)](#)

建立並設定 Amazon S3 儲存貯體

Amazon EMR 使用 AWS SDK for Java 搭配 Amazon S3 存放輸入資料、日誌檔和輸出資料。Amazon S3 將這些儲存位置視為儲存貯體。為了符合 Amazon S3 和 DNS 需求，儲存貯體有特定的限制。如需詳細資訊，請參閱《Amazon Simple Storage Service Developer Guide》中的[儲存貯體限制](#)。

本節說明如何使用 Amazon S3AWS Management Console 建立 Amazon S3 儲存貯體並為其設定許可。您也可以使用 Amazon S3 API 或 AWS CLI 為 Amazon S3 儲存貯體建立並設定許可。您也可以搭配修改來使用 Curl，將適合的身份驗證參數傳遞到 Amazon S3。

請參閱下列資源：

- 若要使用主控台來建立儲存貯體，請參閱 Amazon Simple Storage Service Console User Guide中的[建立儲存貯體](#)。
- 若要使用 AWS CLI 建立和使用儲存貯體，請參閱 Amazon Simple Storage Service Console User Guide中的[使用高階 S3 命令搭配 AWS Command Line Interface](#)。
- 若要使用 SDK 建立儲存貯體，請參閱 Amazon Simple Storage Service Developer Guide中的[建立儲存貯體的範例](#)。
- 若要使用 Curl 搭配儲存貯體，請參閱 [Curl 的 Amazon S3 身份驗證工具](#)。

- 如需指定特定區域儲存貯體的詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide中的[存取儲存貯體](#)。

Note

如果您為儲存貯體啟用登入，這只會啟用儲存貯體存取日誌而非 Amazon EMR cluster 日誌。

在儲存貯體建立期間或之後，您可以根據您的應用程式來設定存取儲存貯體的適當權限。通常，您會授予讀取、寫入權限給您自己(擁有者)，而將讀取權限授予給已驗證的使用者。

所需的 Amazon S3 儲存貯體必須先存在，您才能夠建立 cluster。您必須將所需指令碼和 cluster 參考的資料上傳至 Amazon S3。下表說明了資料、指令碼和日誌檔案位置的範例。

設定適用於 Amazon S3 的分段上傳

Amazon EMR 支援透過適用於 Java 的 AWS 開發套件進行 Amazon S3 分段上傳。分段上傳可讓您將單一物件以一組組件進行上傳。您可依任何順序分別上傳這些物件組件。若任何組件的傳輸失敗，您可再次傳輸該組件，而不會影響其他組件。當物件的所有組件都全部上傳完後，Amazon S3 會將組件組合起來建立該物件。

如需詳細資訊，請參閱《Amazon Simple Storage Service Developer Guide》中的[分段上傳概觀](#)。

此外，Amazon EMR 提供的屬性可讓您更精確控制對於失敗的分段上傳部分進行的清除。

下表說明分段上傳的 Amazon EMR 組態屬性。您可以使用 core-site 組態分類來設定這些屬性。如需詳細資訊，請參閱《Amazon EMR Release Guide》中的[設定應用程式](#)。

組態參數名稱	預設值	描述
<code>fs.s3n.multipart.uploads.enabled</code>		布林值類型，用以指示是否啟用分段上傳。EMRFS 一致性檢視 (p. 53) 啟用時，分段上傳預設會啟用，而且會忽略對於 <code>false</code> 設定這個值。
<code>fs.s3n.multipart.uploads.splitSize</code>		啟用分段上傳時，指定部分的大小上限 (位元組數)，EMRFS 才會開始新的部分上傳。最小值為 5242880 (5 MB)。如果已指定較小的值，會使用 5242880。上限為 5368709120 (5 GB)。如果已指定較大的值，會使用 5368709120。 如果 EMRFS 用戶端加密已停用，而且 Amazon S3 Optimized Committer 也已停用，這個值也會控制資料檔案直到 EMRFS 使用分段上傳 (而非 <code>PutObject</code> 請求上傳檔案) 之前可增加的大小上限。如需詳細資訊，請參閱
<code>fs.s3n.ssl.enabled</code>	<code>true</code>	布林值類型，用以指示使用 http 或 https。
<code>fs.s3.buckets.create.enabled</code>	<code>false</code>	布林值類型，用以指示是否要在儲存貯體不存在的情況下建立儲存貯體。設定為 <code>false</code> 會導致 <code>CreateBucket</code> 操作發生例外狀況。
<code>fs.s3.multipart.clean.enabled</code>	<code>false</code>	指示對於不完整的分段上傳是否啟用背景定期清除的布林值類型。
<code>fs.s3.multipart.clean.age.threshold</code>		指定考慮清除之前分段上傳存留期下限 (秒數) 的長類型。預設為一週。

組態參數名稱	預設值	描述
fs.s3.multipart.clean.jitterTime	10000	指定在排定的下次清除之前將隨機抖動延遲上限(秒數)新增到 15 分鐘固定延遲的整數類型。

使用 Amazon EMR 主控台來停用分段上傳

此程序說明您建立叢集時如何使用 Amazon EMR 主控台停用分段上傳。

若要停用分段上傳

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集) , Go to advanced options (前往進階選項)。
3. 在 Edit Software Settings (編輯軟體設定) 下，輸入以下設定 : classification=core-site, properties=[fs.s3.multipart.uploads.enabled=false]
4. 繼續建立叢集。

使用 AWS CLI 停用分段上傳

此程序說明如何使用 AWS CLI 停用分段上傳。若要停用分段上傳，請輸入含 create-cluster 參數的 --bootstrap-actions 命令。

使用 AWS CLI 停用分段上傳

1. 建立有下列內容的檔案 myConfig.json，並將該檔案儲存在您執行命令的同一個目錄中：

```
[  
  {  
    "Classification": "core-site",  
    "Properties": {  
      "fs.s3n.multipart.uploads.enabled": "false"  
    }  
  }  
]
```

2. 輸入下列命令，然後使用 EC2 金鑰對的名稱來取代 myKey。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "Test cluster" \  
--release-label emr-5.28.0 --applications Name=Hive Name=Pig \  
--use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge \  
--instance-count 3 --configurations file://myConfig.json
```

使用 API 來停用分段上傳

如需有關以程式設計的方式使用 Amazon S3 分段上傳的資訊，請參閱《Amazon Simple Storage Service Developer Guide》中的為分段上傳使用適用於 Java 的 AWS 開發套件。

關於適用於 Java 的 AWS 開發套件的詳細資訊，請參閱適用於 Java 的 AWS 開發套件。

最佳實務

以下是使用 Amazon S3 儲存貯體搭配 EMR 叢集的建議。

啟用版本控制

版本控制是適用於您 Amazon S3 儲存貯體的建議組態。您可透過啟用版本控制，確保資料不小心刪除或覆寫時，仍可復原。如需詳細資訊，請參閱《Amazon Simple Storage Service Developer Guide》中的[使用版本控制](#)。

清理失敗的分段上傳

EMR 叢集元件透過適用於 Java 的 AWS 開發套件與 Amazon S3 API 來使用分段上傳，以依預設寫入日誌檔和輸出資料到 Amazon S3。如需使用 Amazon EMR 變更此組態相關屬性的資訊，請參閱[設定適用於 Amazon S3 的分段上傳 \(p. 36\)](#)。上傳大型檔案有時會導致 Amazon S3 分段上傳不完整。當分段上傳無法成功完成時，進行中的分段上傳會持續佔用您的儲存貯體，並會產生儲存費用。建議採取下列選項避免過多檔案儲存：

- 針對與 Amazon EMR 搭配使用的儲存貯體，在 Amazon S3 中使用生命週期規則，在上傳起始日後三天移除不完整的分段上傳。生命週期組態規則可讓您控制物件的儲存類別和生命週期。如需詳細資訊，請參閱[物件生命週期管理](#)和[使用儲存貯體生命週期政策以中止不完整的分段上傳](#)。
- 透過將 `fs.s3.multipart.clean.enabled` 設定為 TRUE 並調校其他清除參數啟用 Amazon EMR 的分段清除功能。對於大量、大規模，以及運作時間有限的叢集。此功能相當實用。在這種情況下，生命週期組態規則的 `DaysAfterInitiation` 參數可能過長，即使設定為最低，仍會導致 Amazon S3 儲存中出現峰值。Amazon EMR 的分段清除可以達到更精確的控制。如需更多詳細資訊，請參閱[設定適用於 Amazon S3 的分段上傳 \(p. 36\)](#)。

管理版本標記

針對與 Amazon EMR 搭配使用的版本控制儲存貯體，我們建議在 Amazon S3 中啟用生命週期組態規則，以移除過期的物件刪除標記。在版本控制的儲存貯體中刪除物件時，即會建立一個刪除標記。如果物件的舊版本於後續過期，則會留下儲存貯體中的過期物件刪除標記。雖然不會針對刪除標記收費，移除過期的標記可以提升 LIST 請求的效能。如需詳細資訊，請參閱《Amazon Simple Storage Service Console User Guide》中的[具有版本控制之儲存貯體的生命週期組態](#)。

效能最佳實務

根據您的工作負載而定，對這些叢集的特定類型使用 EMR 叢集和應用程式會導致對儲存貯體的請求數量過高。如需詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的[請求率和效能考量](#)。

使用分散式快取匯入檔案

主題

- [支援的檔案類型 \(p. 39\)](#)
- [快取檔案的位置 \(p. 39\)](#)
- [從串流應用程式存取快取檔案 \(p. 39\)](#)
- [使用 Amazon EMR 主控台從串流應用程式存取快取檔案 \(p. 39\)](#)
- [使用 AWS CLI 從串流應用程式存取快取檔案 \(p. 40\)](#)

分散式快取是 Hadoop 功能，其可在對應或降低任務需要存取共用資料時提升效率。如果您的叢集是根據現有的應用程式或是在建立叢集時未安裝的二進位，您可以使用分散式快取來匯入這些檔案。此功能可讓叢集節點從其本機檔案系統讀取匯入的檔案，而不是從其他叢集節點擷取檔案。

如需詳細資訊，請前往 <http://hadoop.apache.org/docs/stable/api/org/apache/hadoop/filecache/DistributedCache.html>。

建立叢集時，您會叫用分散式快取。Hadoop 任務開始之前會將檔案快取，並在任務期間保持快取。您可以快取存放在任何 Hadoop 相容的檔案系統的檔案（例如，HDFS 或 Amazon S3）。檔案快取的預設大小為 10 GB。若要變更快取大小，請使用引導操作重新設定 Hadoop 參數 `local.cache.size`。如需更多詳細資訊，請參閱[建立引導操作來安裝其他軟體 \(p. 86\)](#)。

支援的檔案類型

分散式快取可允許單一檔案和封存。個別檔案會快取成唯讀檔案。可執行檔和二進位檔有執行權限設定。

封存是使用公用程式 (例如，gzip) 來封裝一或多個檔案。分散式快取會在快取過程中，將壓縮檔案傳遞給每個核心節點，並解壓縮封存。分散式快取支援以下壓縮格式：

- zip
- tgz
- tar.gz
- tar
- jar

快取檔案的位置

分散式快取只會將檔案複製到核心節點。如果叢集中沒有核心節點，則分散式快取會將檔案複製到主節點。

分散式快取會使用 symlinks 將快取檔案對應到映射器和縮減器的目前工作目錄。符號連結是檔案位置的別名，而非實際的檔案位置。`yarn-site.xml` 中的 `yarn.nodemanager.local-dirs` 參數值會指定暫存檔的位置。Amazon EMR 會將此參數設定為 `/mnt/mapred`，或依據執行個體類型和 EMR 版本設定為一些類似的值。例如，設定可能會有 `/mnt/mapred` 和 `/mnt1/mapred`，因為執行個體類型有兩個暫時性磁碟區。快取檔案位於 `/mnt/mapred/taskTracker/archive` 中的臨時檔案位置的子目錄。

如果您快取單一檔案，分散式快取會將檔案放在 `archive` 目錄。如果您快取存檔，分散式快取會解壓縮檔案，在 `/archive` 中建立子目錄，其名稱與封存檔案名稱相同。個別檔案位於新的子目錄。

您僅可在使用串流時使用分散式快取。

從串流應用程式存取快取檔案

若要從您的映射器或縮減器應用程式存取快取的檔案，務必將目前的工作目錄 (`./`) 新增到您的應用程式，並且如同目前工作目錄中的檔案一般參考快取的檔案。

使用 Amazon EMR 主控台從串流應用程式存取快取檔案

您可以使用 Amazon EMR 主控台來建立使用分散式快取的叢集。

使用主控台來指定分散式快取檔案

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Step execution (步驟執行) 做為啟動模式。
4. 在 Steps (步驟) 部分，於 Add step (新增步驟) 欄位中，從清單中選擇 Streaming program (串流程式)，然後按一下 Configure and add (設定和新增)。
5. 在 Arguments (引數) 欄位中，納入檔案和封存以儲存到快取，然後按一下 Add (新增)。

檔案大小 (或在封存檔案中的檔案大小總和) 必須少於分配的快取大小。

如果您想要...	動作	範例
將個別檔案新增到分散式快取	如果檔案是放置在本機快取，則在檔案的名稱和位置、井字號 (#)，以及您想要提供給檔案	<code>-cacheFile \s3://bucket_name/file_name#cache_file_name</code>

如果您想 要...	動作	範例	
	的名稱後面接著指定 -cacheFile。		
將封存檔案新增到分散式快取	在 Amazon S3 中的檔案的位置、井字號 (#) , 以及您想要提供給本機快取中檔案集合的名稱後面接著輸入 -cacheArchive。	<pre>-cacheArchive \ s3://bucket_name/ archive_name#cache_archive_name</pre>	

6. 繼續設定和啟動您的叢集。您的叢集在處理任何叢集步驟前，會將檔案複製到快取位置。

使用 AWS CLI 從串流應用程式存取快取檔案

您可以使用 CLI 來建立使用分散式快取的叢集。

使用 AWS CLI 來指定分散式快取檔案

- 若要在叢集建立時提交串流步驟，輸入含 `create-cluster` 參數的 `--steps` 命令。若要使用 AWS CLI 指定分散式快取檔案，請在提交串流步驟時指定適當的引數。

如果您想要...	將以下參數新增至叢集...
將個別檔案新增到分散式快取	如果檔案是放置在本機快取，則在檔案的名稱和位置、井字號 (#) , 以及您想要提供給檔案的名稱後面接著指定 -cacheFile。
將封存檔案新增到分散式快取	在 Amazon S3 中的檔案的位置、井字號 (#) , 以及您想要提供給本機快取中檔案集合的名稱後面接著輸入 -cacheArchive。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

Example 1

輸入以下命令來啟動叢集並提交使用 `-cacheFile` 的串流步驟，將一個檔案 `sample_dataset_cached.dat` 新增至快取。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 --applications Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge --instance-count 3 --steps Type=STREAMING,Name="Streaming program",ActionOnFailure=CONTINUE,Args=[>--files", "s3://my_bucket/my_mapper.py s3://my_bucket/my_reducer.py", "-mapper", "my_mapper.py", "-reducer", "my_reducer.py", "-input", "s3://my_bucket/my_input", "-output", "s3://my_bucket/my_output", "-cacheFile", "s3://my_bucket/sample_dataset.dat#sample_dataset_cached.dat"]]
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

Example 2

以下命令會顯示串流叢集的建立，並使用 `-cacheArchive` 將封存檔案新增到快取。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 --  
applications Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey  
--instance-type m5.xlarge --instance-count 3 --steps Type=STREAMING,Name="Streaming  
program",ActionOnFailure=CONTINUE,Args=["--files","s3://my_bucket/my_mapper.py s3://  
my_bucket/my_reducer.py","-mapper","my_mapper.py","-reducer","my_reducer.py","-input","s3://  
my_bucket/my_input","-output","s3://my_bucket/my_output", "-cacheArchive","s3://my_bucket/  
sample_dataset.tgz#sample_dataset_cached"]
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如何處理壓縮檔案

Hadoop 會檢查副檔名以偵測壓縮檔案。Hadoop 支援的壓縮類型為：gzip、bzip2 和 LZO。您不需要採取任何額外的動作來擷取使用這些壓縮類型的檔案；Hadoop 會為您處理。

若要為 LZO 檔案建立索引，您可以使用 `hadoop-lzo` 資料庫，您可從 <https://github.com/kevinweil/hadoop-lzo> 下載。請注意，因為這是第三方程式庫，Amazon EMR 不提供如何使用此工具的開發人員支援。如需使用資訊，請參閱 [hadoop-lzo 讀我檔](#)。

將 DynamoDB 資料匯入到 Hive

Amazon EMR 提供的 Hive 實作包含您可在 DynamoDB 和 Amazon EMR 叢集間匯入和匯出資料的功能。如果您的輸入資料存放在 DynamoDB 時，此功能會很有幫助。

使用 AWS DirectConnect 連接資料

您可以使用 AWS Direct Connect 服務，建立從資料中心、辦公室或主機託管環境連接到 AWS 的私有專用網路連線。如果您有大量的輸入資料，則使用 AWS Direct Connect 可以降低您的網路成本，提高頻寬傳輸速率，並提供比一般網際網路連線更為一致的網路體驗。如需更多詳細資訊，請參閱 [AWS Direct Connect User Guide](#)。

使用 AWS Import/Export 上傳大量資料

AWS Import/Export 是一項服務，可將大量資料從實體儲存裝置傳輸到 AWS。您可將可攜式儲存裝置寄送至 AWS，AWS Import/Export 會使用 Amazon 的高速內部網路以從您的儲存裝置中直接傳出資料。資料載入通常會在儲存裝置抵達 AWS 後的下一個工作日開始。在資料匯出或匯入完成後，我們會傳回您的儲存裝置。對大型資料集而言，AWS 資料傳輸比網際網路傳輸快速許多，且比升級網路連線更加划算。如需詳細資訊，請參閱 [AWS Import/Export Developer Guide](#)。

設定輸出位置

最常見的 Amazon EMR 叢集輸出格式為文字檔案（壓縮或未壓縮）。一般而言，這些是寫入至 Amazon S3 儲存貯體的。此儲存貯體必須在叢集啟動前建立。當您啟動叢集時，指定 S3 儲存貯體做為輸出位置。

如需詳細資訊，請參閱下列主題：

主題

- [建立並設定 Amazon S3 儲存貯體 \(p. 42\)](#)
- [Amazon EMR 可以傳回什麼格式？\(p. 43\)](#)
- [如何將資料寫入至您並未擁有的 Amazon S3 儲存貯體 \(p. 43\)](#)
- [壓縮叢集的輸出 \(p. 45\)](#)

建立並設定 Amazon S3 儲存貯體

Amazon EMR (Amazon EMR) 使用 Amazon S3 存放輸入資料、日誌檔案和輸出資料。Amazon S3 將這些存放位置視為儲存貯體。為了符合 Amazon S3 和 DNS 需求，儲存貯體有特定的限制。如需詳細資訊，請參閱 Amazon Simple Storage Service 開發人員指南中的 [儲存貯體限制](#)。

本節說明如何使用 Amazon S3 AWS Management Console 建立 Amazon S3 儲存貯體並為其設定許可。然而，您也可以使用 Amazon S3 API 或第三方的 Curl 命令列工具來建立 Amazon S3 儲存貯體並設定許可。如需 Curl 的詳細資訊，請前往 [Amazon S3 對 Curl 的驗證工具](#)。如需使用 Amazon S3 API 建立並設定 Amazon S3 儲存貯體的詳細資訊，請前往 [Amazon Simple Storage Service API Reference](#)。

使用主控台建立 Amazon S3 儲存貯體

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. 選擇 Create Bucket (建立儲存貯體)。

Create a Bucket (建立儲存貯體) 對話方塊會出現。

3. 輸入儲存貯體名稱，例如 **aws-s3-bucket1**。

此名稱應為全域唯一，且不可與另一個儲存貯體使用的名稱相同。

4. 選擇儲存貯體的 Region (區域)。為了避免支付跨域頻寬費用，請在與叢集相同的區域中建立 Amazon S3 儲存貯體。

請參閱 [選擇一個 AWS 區域 \(p. 31\)](#) 了解選擇區域的操作指示。

5. 選擇 Create (建立)。

您建立了儲存貯體和 URI **s3n://aws-s3-bucket1/**。

Note

如果您啟用登入 Create a Bucket (建立儲存貯體) 精靈，只會啟用儲存貯體存取日誌而非叢集日誌。

Note

如需指定區域特定儲存貯體的詳細資訊，請參閱 Amazon Simple Storage Service 開發人員指南和 [AWS 開發套件可用區域端點](#) 中的 [儲存貯體與區域](#)。

建立儲存貯體之後，您就可以為其設定適當的許可。通常，您會讓自己 (擁有者) 能夠讀寫存取，讓已驗證使用者能夠讀取存取。

使用主控台設定 Amazon S3 儲存貯體的許可

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. 在 Buckets (儲存貯體) 窗格中，開啟 (按一下右鍵) 您剛建立的儲存貯體。
3. 選擇 Properties (屬性)。
4. 在 Properties (屬性) 窗格中選擇 Permissions (許可) 標籤。
5. 選擇 Add more permissions (新增其他許可)。
6. 在 Grantee (被授與者) 欄位中選擇 Authenticated Users (已驗證使用者)。
7. 在 Grantee (被授與者) 的下拉式選單右方，選擇 List (清單)。
8. 選擇 Save (儲存)。

您已經建立儲存貯體以及對已驗證使用者的限制許可。

所需的 Amazon S3 儲存貯體必須先存在，您才能夠建立叢集。您必須將所需指令碼和叢集參考的資料上傳至 Amazon S3。下表說明了資料、指令碼和日誌檔案位置的範例。

資訊	Amazon S3 位置範例
指令碼或程式	s3://aws-s3-bucket1/script/MapperScript.py
日誌檔案	s3://aws-s3-bucket1/logs
輸入資料	s3://aws-s3-bucket1/input
輸出資料	s3://aws-s3-bucket1/output

Amazon EMR 可以傳回什麼格式？

叢集的預設輸出格式是帶有金鑰的文字、寫入至文字檔案個別行的值對。這是最常用的輸出格式。

如果您的輸出資料必須以預設文字檔案以外的格式來寫入，您可以使用 Hadoop 界面 `OutputFormat` 來指定其他輸出類型。您甚至可以建立 `FileOutputFormat` 的子類別，以處理自訂資料類型。如需詳細資訊，請參閱 <http://hadoop.apache.org/docs/current/api/org/apache/hadoop/mapred/OutputFormat.html>。

如果您正在啟動 Hive 叢集，您可以使用串聯器/解串器 (SerDe) 以從 HDFS 輸出指定格式的資料。如需詳細資訊，請參閱 <https://cwiki.apache.org/confluence/display/Hive/SerDe>。

如何將資料寫入至您並未擁有的 Amazon S3 儲存貯體

當您將檔案寫入至 Amazon Simple Storage Service (Amazon S3) 儲存貯體時，依預設，您是唯一一個能讀取該檔案的人。假設您將檔案寫入自己的儲存貯體，且此預設設定可保護檔案的隱私。

但是，如果您正在執行叢集，並希望該輸出寫入至另一個 AWS 使用者的 Amazon S3 儲存貯體，且您希望其他 AWS 使用者能夠讀取該輸出，則必須執行兩項操作：

- 讓其他 AWS 使用者授予您他們 Amazon S3 儲存貯體的寫入權限。您啟動的叢集在您的 AWS 登入資料下執行，因此您啟動的任何叢集都將能夠寫入其他 AWS 使用者的儲存貯體。
- 為您或叢集寫入 Amazon S3 儲存貯體的檔案設定其他 AWS 使用者的讀取權限。設定這些讀取權限最簡單的方法，是使用預設的存取控制清單 (ACL)，這是由 Amazon S3 定義的一組預先定義的存取政策。

關於其他 AWS 使用者如何授予您寫入檔案至其他使用者 Amazon S3 儲存貯體許可的詳細資訊，請參閱 Amazon Simple Storage Service Console User Guide 中的 [編輯儲存貯體許可](#)。

為了讓叢集在將檔案寫入至 Amazon S3 時使用固定 ACL，請將 `fs.s3.canned.acl` 叢集組態選項設定為要使用的固定 ACL。下表列出目前定義的固定 ACL。

固定的 ACL	描述
AuthenticatedRead	指定擁有者已授予 <code>Permission.FullControl</code> 且 <code>GroupGrantee.AuthenticatedUsers</code> 群組承授者被授予 <code>Permission.Read</code> 存取權限。
BucketOwnerFullControl	指定儲存貯體擁有者已授予 <code>Permission.FullControl</code> 。儲存貯體的擁有者不一定與物件的擁有者相同。
BucketOwnerRead	指定儲存貯體擁有者已授予 <code>Permission.Read</code> 。儲存貯體的擁有者不一定與物件的擁有者相同。

固定的 ACL	描述
LogDeliveryWrite	指定擁有者已授予 <code>Permission.FullControl</code> 且 <code>GroupGrantee.LogDelivery</code> 群組承授者被授予 <code>Permission.Write</code> 存取權限，故可提供該存取日誌。
Private	指定擁有者已授予 <code>Permission.FullControl</code> 。
PublicRead	指定擁有者已授予 <code>Permission.FullControl</code> 且 <code>GroupGrantee.AllUsers</code> 群組承授者被授予 <code>Permission.Read</code> 存取權限。
PublicReadWrite	指定擁有者已授予 <code>Permission.FullControl</code> 且 <code>GroupGrantee.AllUsers</code> 群組承授者被授予 <code>Permission.Read</code> 與 <code>Permission.Write</code> 存取權限。

根據您正在執行的叢集類型，有許多方法可以設定叢集組態選項。下列程序說明如何為一般情況設定選項。

在 Hive 中使用固定 ACL 寫入檔案

- 從 Hive 命令提示字元處，將 `fs.s3.canned.acl` 組態選項設定為您想在寫入至 Amazon S3 的檔案上設定叢集的固定 ACL。若要存取使用 SSH 連接到主節點的 Hive 命令提示字元，然後在 Hadoop 命令提示字元處鍵入 Hive。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

下列範例將 `fs.s3.canned.acl` 組態選項設為 `BucketOwnerFullControl`，以給予 Amazon S3 儲存貯體擁有者完整的檔案控制能力。請注意，設定命令區分大小寫，且不包含引號或空格。

```
hive> set fs.s3.canned.acl=BucketOwnerFullControl;
create table acl (n int) location 's3://acltestbucket/acl/';
insert overwrite table acl select count(n) from acl;
```

範例的最後兩行會建立一個存放於 Amazon S3 中的表格，並將資料寫入表格中。

在 Pig 中使用固定 ACL 寫入檔案

- 從 Pig 命令提示字元處，將 `fs.s3.canned.acl` 組態選項設定為您想在寫入至 Amazon S3 的檔案上設定叢集的固定 ACL。若要存取使用 SSH 連接到主節點的 Pig 命令提示字元，然後在 Hadoop 命令提示字元處鍵入 Pig。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

下列範例將 `fs.s3.canned.acl` 組態選項設為 `BucketOwnerFullControl`，以給予 Amazon S3 儲存貯體擁有者完整的檔案控制能力。請注意，設定命令在固定 ACL 名稱前包含一個空格，並且不包含引號。

```
pig> set fs.s3.canned.acl BucketOwnerFullControl;
store some data into 's3://acltestbucket/pig/acl';
```

在自訂 JAR 中使用固定 ACL 寫入檔案

- 透過 Hadoop 與 -D 旗標設定 `fs.s3.canned.acl` 組態選項。這顯示於下列範例中：

```
hadoop jar hadoop-examples.jar wordcount
-Dfs.s3.canned.acl=BucketOwnerFullControl s3://mybucket/input s3://mybucket/output
```

壓縮叢集的輸出

主題

- [輸出資料壓縮 \(p. 45\)](#)
- [中繼資料壓縮 \(p. 45\)](#)
- [搭配使用 Snappy 程式庫與 Amazon EMR \(p. 45\)](#)

輸出資料壓縮

此會壓縮 Hadoop 任務的輸出。若您使用的是 `TextOutputFormat`，輸出成果便是 gzip 壓縮的文字檔。若正在寫入 `SequenceFiles`，壓縮成果會是內部壓縮的 `SequenceFile`。將 `mapred.output.compress` 設定為 `true`，即可透過設定組態來達成。

若您執行的是串流任務，將以下三個引入傳遞給串流任務即可達成。

```
-jobconf mapred.output.compress=true
```

也可以使用引導操作來自動壓縮所有任務輸出。以下是使用 Ruby 用戶端的方式。

```
--bootstrap-actions s3://elasticmapreduce/bootstrap-actions/configure-hadoop \
--args "-s,mapred.output.compress=true"
```

最後一項，若寫入的是自訂的 Jar，則可以在建立任務時，以下列這行啟用輸出壓縮。

```
FileOutputFormat.setCompressOutput(conf, true);
```

中繼資料壓縮

若您的任務會從映射器將大量資料隨機播放到縮減器，啟用中繼資料壓縮可大幅改善效能。可壓縮映射輸出，在資料抵達核心節點時再解壓縮。組態設定為 `mapred.compress.map.output`。啟用方式與輸出壓縮類似。

若寫入的是自訂的 Jar，請使用以下命令：

```
conf.setCompressMapOutput(true);
```

搭配使用 Snappy 程式庫與 Amazon EMR

Snappy 是針對速度最佳化處理的壓縮與解壓縮程式庫。Amazon EMR AMI 2.0 版及更新版本均有提供，且是中繼壓縮的預設方式。如需 Snappy 的詳細資訊，請至 <http://code.google.com/p/snappy/>。

規劃和設定主節點

當您啟動 EMR 叢集時，可以選擇要在叢集中包含一個或三個主節點。唯有 Amazon EMR 5.23.0 版和更新版本支援啟動含有三個主節點的叢集。

具有多個主節點的 EMR 叢集具有以下主要優點：

- 主節點不會再出現單一故障點問題。如果其中一個主節點故障，叢集會使用另外兩個主節點，讓執行不會遭到中斷。同時，Amazon EMR 會自動使用佈建了相同組態和引導操作的新主節點來替換故障的主節點。
- EMR 可讓使用者體驗 Hadoop 的 HDFS NameNode 和 YARN ResourceManager 高可用性功能，亦可支援其他幾個開放原始碼應用程式的高可用性。

如需具有多個主節點的 EMR 叢集如何支援開放原始碼應用程式和其他 EMR 功能的詳細資訊，請參閱[支援的應用程式和功能 \(p. 46\)](#)。

Note

叢集只可位在一個可用區域或子網路中。

本節提供的資訊包含具有多個主節點的 EMR 叢集支援的應用程式和功能，以及啟動叢集時的組態詳細資訊、最佳實務和考量事項。

主題

- [支援的應用程式和功能 \(p. 46\)](#)
- [啟動具多個主節點的 EMR 叢集 \(p. 50\)](#)
- [考量事項和最佳實務 \(p. 52\)](#)

支援的應用程式和功能

本主題會提供 EMR 叢集中 Hadoop 的 HDFS NameNode 和 YARN ResourceManager 高可用性功能相關資訊，以及如何搭配這些高可用性功能使用開放原始碼應用程式和其他 EMR 功能。

HDFS 高可用性

具有多個主節點的 EMR 叢集可讓使用者運用 Hadoop 中的 HDFS NameNode 高可用性功能。如需詳細資訊，請參閱[HDFS High Availability \(HDFS 高可用性\)](#)。

在 EMR 叢集中，NameNode 只可在三個主節點中的其中兩個節點上運作。其中一個 NameNode 會處於 active 狀態，而另一個則會處於 standby 狀態。如果含有 active NameNode 的主節點故障，EMR 就會開始執行 HDFS 自動容錯移轉程序。如此一來，standby NameNode 主節點的狀態就會變成 active，然後接管叢集中所有用戶端操作。接著，EMR 會用新主節點來替換故障的主節點，而這個重新加入的主節點狀態將是 standby。

若要找出處於 active 狀態的 NameNode，可以透過 SSH 連接至叢集中的任一主節點，並執行以下命令：

```
hdfs haadmin -getAllServiceState
```

輸出結果會列出安裝 NameNode 的兩個節點及其狀態。例如：

```
ip-##-##-##-##1.ec2.internal:8020 active
ip-##-##-##-##2.ec2.internal:8020 standby
```

YARN ResourceManager 高可用性

具有多個主節點的 EMR 叢集可讓使用者運用 Hadoop 中的 YARN ResourceManager 高可用性功能。如需詳細資訊，請參閱 [ResourceManager High Availability](#) (ResourceManager 高可用性)。

在具有多個主節點的 EMR 叢集中，YARN ResourceManager 可在所有三個主節點上運作。其中一個 ResourceManager 會處於 active 狀態，而另外兩個則會處於 standby 狀態。如果含有 active ResourceManager 的主節點故障，EMR 就會自動開始容錯移轉程序，讓處於 standby 狀態的 ResourceManager 主節點接管所有操作。然後，EMR 會用新主節點來替換故障的主節點，而這個新的主節點會以 standby 狀態重新加入 ResourceManager 仲裁中。

您可以連接至任何主節點的「`http://master-public-dns-name:8088/cluster`」，其會自動將您導向狀態為 active 的資源管理員。若要找出處於 active 狀態的資源管理員，則可透過 SSH 連接至叢集中的任一主節點，並執行以下命令，即可取得三個主節點的清單及其狀態：

```
yarn rmadmin -getAllServiceState
```

具多個主節點 EMR 叢集中支援的應用程式

您可以在 具有多個主節點的 EMR 叢集 上安裝和執行下列應用程式。每個應用程式的主節點容錯移轉程序各有不同。

應用程式	主節點容錯移轉期間的可用性	備註
Flink	可用性不會受到主節點容錯移轉程序影響	<p>Amazon EMR 上的 Flink 任務以 YARN 應用程式執行。Flink 的 JobManagers 在核心節點上以 YARN 的 ApplicationMasters 執行。JobManager 不會受到主節點容錯移轉程序的影響。</p> <p>如果您使用 5.27.0 或更早的 Amazon EMR 版本，JobManager 是單一故障點。JobManager 故障時會失去所有任務狀態，而且執行中的任務將不再繼續。您可以設定應用程式嘗試計數、檢查點作業，並啟用 ZooKeeper 做為 Flink 的狀態儲存，以啟用 JobManager 高可用性。如需詳細資訊，請參閱 在具有多個主節點的 EMR 叢集上設定 Flink。</p> <p>從 Amazon EMR 5.28.0 版開始，無需手動設定即可啟用 JobManager 高可用性。</p>
Ganglia	可用性不會受到主節點容錯移轉程序影響	Ganglia 可在所有主節點上使用，因此 Ganglia 在主節點容錯移轉程序期間仍可繼續執行。
Hadoop	高可用性	作用中的主節點故障時，HDFS NameNode 和 YARN ResourceManager 會自動容錯移轉至備用節點。
HBase	高可用性	<p>作用中的主節點故障時，HBase 會自動容錯移轉至備用節點。</p> <p>如果您要透過 REST 或 Thrift 伺服器連接至 HBase，請務必在作用中主節點故障時切換到另一個主節點。</p>
HCatalog	可用性不會受到主節點容錯移轉程序影響	HCatalog 是以叢集外部的 Hive 中繼存放區為基礎建置而成，因此主節點容錯移轉程序期間仍可繼續使用 HCatalog。

應用程式	主節點容錯移轉期間的可用性	備註
JupyterHub	高可用性	JupyterHub 安裝在所有三個主執行個體上。強烈建議您設定筆記本持久性，以防止筆記本在主節點故障時遺失。如需詳細資訊，請參閱 在 Amazon S3 中設定筆記本的持久性 。
Livy	高可用性	所有三個主節點上均已安裝 Livy。作用中的主節點故障時，您就無法存取目前的 Livy 工作階段，且必須在不同的主節點或新的替換節點上建立新的 Livy 工作節點。
Mahout	可用性不會受到主節點容錯移轉程序影響	由於 Mahout 沒有協助程式，其不會受到主節點容錯移轉程序影響。
MXNet	可用性不會受到主節點容錯移轉程序影響	由於 MXNet 沒有協助程式，因此不會受到主節點容錯移轉程序的影響。
Phoenix	高可用性	Phoenix 的 QueryServer 只能在三個主節點之一上執行。Phoenix 在所有三個主節點皆已設定為連接 Phoenix QueryServer。您可以使用 /etc/phoenix/conf/phoenix-env.sh 文件找到 Phoenix 的 Query Server 的私有 IP
Pig	可用性不會受到主節點容錯移轉程序影響	由於 Pig 沒有協助程式，其不會受到主節點容錯移轉程序影響。
Spark	高可用性	所有 Spark 應用程式都會在 YARN 容器中運作，且可依照與 YARN 高可用性功能相同的方式來回應主節點容錯移轉作業。
Sqoop	高可用性	依據預設，sqoop-job 和 sqoop-metastore 將資料(任務描述)存放在執行命令的主節點的本機磁碟上，如果你要將中繼存放區資料存放在外部資料庫，請參閱 apache Sqoop 文件
Tez	高可用性	Tez 容器會在 YARN 上執行，因此 Tez 在主節點容錯移轉程序期間的行為方式與 YARN 相同。
TensorFlow	可用性不會受到主節點容錯移轉程序影響	由於 TensorFlow 沒有協助程式，因此不會受到主節點容錯移轉程序的影響。
Zeppelin	高可用性	所有三個主節點上均已安裝 Zeppelin。依據預設，Zeppelin 會將筆記和解譯器組態存放於 HDFS 以防止資料遺失。解譯器工作階段會在所有三個主執行個體中完全隔離。主節點故障時，工作階段資料將會遺失。建議不要在不同的主執行個體上同時修改相同的筆記。
ZooKeeper	高可用性	ZooKeeper 是 HDFS 自動容錯移轉功能的基礎。ZooKeeper 提供具高度可用性的服務，不僅能用來維護協調資料，還能在該資料變更時通知用戶端，並監控用戶端的故障情形。如需詳細資訊，請參閱 HDFS Automatic Failover (HDFS 自動容錯移轉) 。

若要在具有多個主節點的 EMR 叢集上執行下列應用程式，您必須設定外部資料庫。外部資料庫位於叢集之外，因此資料在主節點容錯移轉程序期間不會變動。針對下列應用程式，服務元件會在主節點容錯移轉程序期間自動復原，但作用中的任務可能會失敗，需要重試。

應用程式	主節點容錯移轉期間的可用性	備註
Hive	唯有服務元件可維持高可用性	Hive 需要外部中繼存放區。如需詳細資訊，請參閱 設定適用於 Hive 的外部中繼存放區 。
Hue	唯有服務元件可維持高可用性	Hue 需要外部資料庫。如需詳細資訊，請參閱 使用 Hue 搭配 Amazon RDS 中的遠端資料庫 。
Oozie	唯有服務元件可維持高可用性	需要 Oozie 的外部資料庫。如需詳細資訊，請參閱 使用 Oozie 搭配 Amazon RDS 中的遠端資料庫 。 Oozie-server 僅安裝在一個主節點上，而 oozie-client 安裝在所有三個主節點上。依據預設，oozie-clients 設定為連接到正確的 oozie-server。您可以查看 /etc/oozie/conf.dist/oozie-client-env.sh 檔案中任何主節點的變數 OOZIE_URL，找到安裝 oozie-server 的主節點的私有 DNS 名稱。
Presto	唯有服務元件可維持高可用性	Presto 需要外部 Hive 中繼存放區。您可以使用 Presto 搭配 AWS Glue Data Catalog 或 使用適用於 Hive 的外部 MySQL 資料庫 。

Note

在主節點故障的情況下，Java 資料庫連線 (JDBC) 或開放式資料庫連線 (ODBC) 會終止與主節點的連線。因為 Hive 中繼存放區協助程式可在所有主節點上運作，您仍能連接至任何剩餘的主節點以繼續工作。或者，您可以等待系統替換故障的主節點。

EMR 功能在具多個主節點叢集中的運作方式

使用 SSH 連接至主節點

您可以使用 SSH 連接至 EMR 叢集中三個主節點的任一個，就如同連接至單一主節點一樣。如需詳細資訊，請參閱[使用 SSH 連接至主節點](#)。

若主節點故障，與該主節點間的 SSH 連線就會結束。若要繼續進行工作，您可以連接至另外兩個主節點中的其中一個節點。或者，您可以在 EMR 用新主節點替換故障的主節點後，再存取新的主節點。

Note

替換主節點會維持先前主節點的私有 IP 地址，但替換主節點的公有 IP 地址可能會變更。您可以在主控台中擷取新的 IP 地址，或使用 AWS CLI 中的 `describe-cluster` 命令加以擷取。
NameNode 只可在其中兩個節點上運作。不過，您可以執行 `hdfs` CLI 命令並操作相關工作，藉此存取所有三個主節點上的 HDFS。

在具多個主節點的 EMR 叢集中使用步驟

您可以將步驟提交至具有多個主節點的 EMR 叢集，就如同在具單一主節點叢集中使用步驟的方式一般。如需詳細資訊，請參閱[將工作提交到叢集](#)。

在具有多個主節點的 EMR 叢集中使用步驟時，您應考量下列事項：

- 如果主節點故障，則主節點上執行的步驟會標記為 FAILED，且在本機寫入的任何資料都會遺失。不過，FAILED 狀態可能無法反映各步驟的實際狀態。

- 如果執行中的步驟在主節點故障的情況下啟動 YARN 應用程式，該步驟會繼續進行並成功完成，這是因為系統會自動執行主節點容錯移轉程序。
- 建議您參考工作的輸出結果，以查看各步驟狀態。例如，MapReduce 工作會使用 _SUCCESS 檔案來判斷該工作是否成功完成。
- 建議您將 ActionOnFailure 參數設定為 CONTINUE 或 CANCEL_AND_WAIT，而不是 TERMINATE_JOB_FLOW 或 TERMINATE_CLUSTER。

具多個主節點 EMR 叢集中不支援的功能

具有多個主節點的 EMR 叢集目前無法使用以下 EMR 功能：

- EMR 筆記本
- 執行個體機群

Note

若要在叢集中使用 Kerberos 身分驗證，請務必設定外部 KDC。

從 Amazon EMR 5.27.0 版開始，您可以在 具有多個主節點的 EMR 叢集 上設定 HDFS 透明加密。

如需詳細資訊，請參閱 [Amazon EMR 上使用 HDFS 中的透明加密](#)。

啟動具多個主節點的 EMR 叢集

本主題會提供啟動具有多個主節點的 EMR 叢集時適用的組態詳細資訊與相關範例。

事前準備

- 您可以同時在公有和私有 VPC 子網路中啟動具有多個主節點的 EMR 叢集。不支援 EC2-Classic。您必須在主控台中選取 Auto-assign IPv4 (自動指派 IPv4) 或執行以下命令，使子網路中的執行個體能接收公有 IP 地址，才可在該公有子網路中啟動具有多個主節點的 EMR 叢集。請將 **22XXXX01** 換成您的子網路 ID。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-22XXXX01 --map-public-ip-on-launch
```

- 若要在具有多個主節點的 EMR 叢集上執行 Hive、Hue 或 Oozie，您必須建立外部中繼存放區。如需詳細資訊，請參閱 [配置 Hive 的外部中繼存放區](#)、[使用 Hue 搭配 Amazon RDS 中的遠端資料庫](#)或 [Apache Oozie](#)。
- 若要在叢集中使用 Kerberos 身分驗證，請務必設定外部 KDC。如需詳細資訊，請參閱 [在 Amazon EMR 上設定 Kerberos](#)。

啟動具多個主節點的 EMR 叢集

啟動具有多個主節點的 EMR 叢集時，您必須為三個主節點的執行個體群組指定執行個體計數值。以下範例會示範如何使用預設 AMI 或自訂 AMI 來啟動叢集。

Note

當您使用 AWS CLI 啟動 具有多個主節點的 EMR 叢集 時，您必須指定子網路 ID。請將下方範例中的 **22XXXX01** 換成您的子網路 ID。

Example – 使用預設 AMI 啟動具有多個主節點的 EMR 叢集

```
aws emr create-cluster \
```

```
--name "ha-cluster" \
--release-label emr-5.28.0 \
--instance-groups InstanceGroupType=MASTER,InstanceCount=3,InstanceType=m5.xlarge \
InstanceGroupType=CORE,InstanceCount=4,InstanceType=m5.xlarge \
--ec2-attributes
KeyName=ec2_key_pair_name,InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-22XXXX01 \
--service-role EMR_DefaultRole \
--applications Name=Hadoop Name=Spark
```

Example – 使用自訂 AMI 啟動具有多個主節點的 EMR 叢集

```
aws emr create-cluster \
--name "custom-ami-ha-cluster" \
--release-label emr-5.28.0 \
--instance-groups InstanceGroupType=MASTER,InstanceCount=3,InstanceType=m5.xlarge \
InstanceGroupType=CORE,InstanceCount=4,InstanceType=m5.xlarge \
--ec2-attributes
KeyName=ec2_key_pair_name,InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-22XXXX01 \
--service-role EMR_DefaultRole \
--applications Name=Hadoop Name=Spark \
--custom-ami-id ami-MyAmiID
```

Example – 使用外部 Hive 中繼存放區啟動具有多個主節點的 EMR 叢集

若要在具有多個主節點的 EMR 叢集上執行 Hive，則需為 Hive 指定外部中繼存放區，如下方範例所示：

1. 建立臨時 `hiveConfiguration.json` 檔案，其中包含 Hive 中繼存放區的登入資料。

```
[  
  {  
    "Classification": "hive-site",  
    "Properties": {  
      "javax.jdo.option.ConnectionURL": "jdbc:mysql://hostname:3306/hive?  
createDatabaseIfNotExist=true",  
      "javax.jdo.option.ConnectionDriverName": "org.mariadb.jdbc.Driver",  
      "javax.jdo.option.ConnectionUserName": "username",  
      "javax.jdo.option.ConnectionPassword": "password"  
    }  
  }  
]
```

2. 使用 Hive 中繼存放區啟動叢集。

```
aws emr create-cluster \
--name "ha-cluster-with-hive-metastore" \
--release-label emr-5.28.0 \
--instance-groups InstanceGroupType=MASTER,InstanceCount=3,InstanceType=m5.xlarge \
InstanceGroupType=CORE,InstanceCount=4,InstanceType=m5.xlarge \
--ec2-attributes
KeyName=ec2_key_pair_name,InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-22XXXX01 \
--service-role EMR_DefaultRole \
--applications Name=Hadoop Name= Spark Name=Hive \
--configurations ./hiveConfiguration.json
```

終止具多個主節點的 EMR 叢集

若要終止具有多個主節點的 EMR 叢集，您需要在終止該叢集前停用終止保護功能，如下方範例所示。請將 `j-3KVXXXXXX7UG` 換成您的叢集 ID。

```
aws emr modify-cluster-attributes --cluster-id j-3KVTXXXXXX7UG --no-termination-protected
aws emr terminate-clusters --cluster-id j-3KVTXXXXXX7UG
```

考量事項和最佳實務

具有多個主節點的 EMR 叢集的限制

- 如果有兩個主節點同時故障，EMR 便無法復原該叢集。
- 具多個主節點的 EMR 叢集不能接受可用區域故障的情況。在可用區域執行中斷的情況下，您將無法存取 EMR 叢集。
- 如果開放原始碼應用程式的高可用性功能不在[具多個主節點 EMR 叢集中支援的應用程式 \(p. 47\)](#)中指定的範圍內，則 EMR 無法保證支援該功能。

設定子網路的考量事項：

- 具有多個主節點的 EMR 叢集只可位在一個可用區域或子網路中。執行容錯移轉時，若子網路經過充分利用或有過度訂閱的現象，EMR 即無法替換故障的主節點。為避免這種情況，建議您將整個子網路專門留給 Amazon EMR 叢集使用。此外，請確保子網路提供的私有 IP 地址數量足夠。

設定核心節點的考量事項：

- 建議您至少啟動四個核心節點，從而確保核心節點執行個體群組也擁有相當高的可用性。如果您決定啟動含三個以下核心節點的小型叢集，就需要將 `dfs.replication parameter` 至少設定為 2，以便為 HDFS 配置足夠的 DFS 複寫。如需詳細資訊，請參閱 [HDFS 組態](#)。

在指標上設定警示的考量事項：

- EMR 目前不提供與 HDFS 或 YARN 相關的應用程式特定指標，建議您設定警 示來監控主節點的執行個體計數。如需設定警示，則可使用以下 CloudWatch 指 標：`MultiMasterInstanceGroupNodesRunning`、`MultiMasterInstanceGroupNodesRunningPercentage` 或 `MultiMasterInstanceGroupNodesRequested`。當主節點故障且經過替換時，您就會收到通知。例如：
 - 如果 `MultiMasterInstanceGroupNodesRunningPercentage` 小於 1.0 但大於 0.5，表示叢集可 能缺少一個主節點。在這種情況下，EMR 會嘗試替換主節點。
 - 如果 `MultiMasterInstanceGroupNodesRunningPercentage` 低於 0.5，表示可能有兩個主節點 故障。在這種情況下，仲裁會遺失且該叢集將無法復原。您需要手動操作，才能將資料移出此叢集。

如需詳細資訊，請參閱[在指標上設定警示](#)。

使用 EMR 檔案系統 (EMRFS)

EMR 檔案系統 (EMRFS) 是一種 HDFS 實作，所有 Amazon EMR 叢集會用來從 Amazon EMR 將一般檔 案直接讀取和寫入至 Amazon S3。EMRFS 提供將持久性資料存放在 Amazon S3 的方便性，可讓您與 Hadoop 搭配使用，同時提供一致性檢視和資料加密之類的功能。

一致性檢視提供對清單的一致性檢查和對 Amazon S3 物件的先寫後讀一致性 (適用於新請求)。資料加密可 讓您加密物件，EMRFS 會將其寫入 Amazon S3，並讓 EMRFS 在 Amazon S3 中使用加密的物件。如果您 使用的是 Amazon EMR 發行版本 4.8.0 或更新版本，您可以使用安全組態來設定 Amazon S3 中 EMRFS 物 件的加密，以及其他加密設定。如需更多詳細資訊，請參閱 [加密選項 \(p. 144\)](#)。如果您使用 Amazon EMR 的舊發行版本，您可以手動設定加密設定。如需詳細資訊，請參閱 [使用 EMRFS 屬性來指定 Amazon S3 加密 \(p. 67\)](#)。

使用 Amazon EMR 發行版本 5.10.0 或更新版本時，您可以根據叢集使用者、群組或 Amazon S3 中 EMRFS 資料的位置，來為 EMRFS 請求將不同 IAM 角色用於 Amazon S3。如需更多詳細資訊，請參閱 [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)。

主題

- [一致性檢視 \(p. 53\)](#)
- [授權存取在 Amazon S3 中的 EMRFS 資料 \(p. 66\)](#)
- [使用 EMRFS 屬性來指定 Amazon S3 加密 \(p. 67\)](#)

一致性檢視

EMRFS 一致性是一項選用功能，會在使用 Amazon EMR 發行版本 3.2.1 或更新版本時供您使用。一致性檢視可讓 EMR 叢集對清單進行檢查，並為由 EMRFS 寫入或同步的 Amazon S3 物件檢查先寫後讀一致性。一致性檢視會處理因為 [Amazon S3 資料一致性模式](#) 而產生的問題。例如，如果您在一個操作中將物件新增至 Amazon S3，然後立即在後續操作中列出物件，則清單和處理物件集可能會不完整。對於使用 Amazon S3 做為資料存放區（例如多步驟擷取-轉換載入 (ETL) 資料處理管道）之執行快速、連續步驟的叢集，這是相當常見的問題。

建立已啟用一致性檢視的叢集時，Amazon EMR 會使用 Amazon DynamoDB 資料庫，以存放物件中繼資料和追蹤與 Amazon S3 的一致性。如果一致性檢視判斷在檔案系統操作期間 Amazon S3 是不一致的，它會根據您可以定義的規則來重試該操作。預設情況下，DynamoDB 資料庫有 400 個讀取容量和 100 個寫入容量。您可以根據 EMRFS 追蹤的多種物件以及同時使用中繼資料的節點數來設定讀取/寫入容量設定。您也可以設定其他資料庫和操作參數。使用一致性檢視會產生 DynamoDB 費用，此費用金額通常較小（除了因 Amazon EMR 而產生的費用）。如需詳細資訊，請參閱 [Amazon DynamoDB 定價](#)。

在啟用一致性檢視後，EMRFS 會傳回在 EMRFS 中繼資料存放區中列出的一組物件，以及由 Amazon S3 針對指定路徑而直接傳回的物件。由於 Amazon S3 仍是路徑物件的「資料來源」，EMRFS 可確保在指定 Amazon S3 路徑中的一切項目仍順利處理，無論其是否於中繼資料受到追蹤。不過，EMRFS 一致性檢視只可確保會對您追蹤的資料夾物件進行一致性檢查。

您可以從主節點命令列使用 EMRFS 公用程式 (`emrfs`) 對一致性檢視所追蹤的 Amazon S3 物件執行操作。例如，您可以使用 EMRFS 中繼資料存放區來匯入、刪除和同步 Amazon S3 物件。如需 EMRFS CLI 公用程式的詳細資訊，請參閱 [EMRFS CLI 參考 \(p. 60\)](#)。

如果您直接從在 EMRFS 中繼資料中追蹤的 Amazon S3 刪除物件，EMRFS 會將該物件視為不一致，並在重試用盡後擲出例外狀況。使用 EMRFS 來在使用一致性檢視追蹤的 Amazon S3 中刪除物件。或者，您可以使用 `emrfs` 命令列為已直接刪除的物件清除中繼資料項目，或者您可以在刪除物件後立即與 Amazon S3 同步一致性檢視。

主題

- [啟用一致性檢視 \(p. 53\)](#)
- [了解 EMRFS 一致性檢視如何在 Amazon S3 中追蹤物件 \(p. 54\)](#)
- [重試邏輯 \(p. 55\)](#)
- [EMRFS 一致檢視中繼資料 \(p. 55\)](#)
- [設定 CloudWatch 和 Amazon SQS 的一致性通知 \(p. 57\)](#)
- [設定一致性檢視 \(p. 58\)](#)
- [EMRFS CLI 參考 \(p. 60\)](#)

啟用一致性檢視

您可以使用 AWS Management Console AWS CLI 或 `emrfs-site` 組態分態設定其他設定。

使用主控台設定一致性檢視

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集) , Go to advanced options (前往進階選項)。
3. 針對 Step 1: Software and Steps (步驟 1：軟體和步驟) 和 Step 2: Hardware (步驟 2：硬體) 選擇設定。
4. 針對 Step 3: General Cluster Settings (步驟 3：一般叢集設定) , 在 Additional Options (其他選項) , 選擇 EMRFS consistent view (EMRFS 一致性檢視)。
5. 針對 EMRFS Metadata store (EMRFS 中繼資料存放區) , 輸入中繼資料存放區的名稱。預設值為 **EmrFSMetadata**。如果 EmrFSMetadata 資料表不存在，則會在 DynamoDB 中為您建立。

Note

叢集終止時，Amazon EMR 不會將 EMRFS 中繼資料從 DynamoDB 自動移除。

6. 針對 Number of retries (重試數) , 輸入整數值。如果偵測到不一致，EMRFS 會嘗試以此次數來呼叫 Amazon S3。預設值為 **5**。
7. 針對 Retry period (in seconds) (重試期間 (以秒為單位)) , 輸入整數值。這是 EMRFS 在重試之間等待的時間。預設值為 **10**。

Note

系統會透過指數退避執行後續的重試動作。

若要使用 AWS CLI 啟動已啟用一致性檢視的叢集

我們建議您安裝 AWS CLI 目前版本。若要下載最新版本，請參閱 <https://aws.amazon.com//cli/>。

- Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --instance-type m5.xlarge --instance-count 3 --emrfs
Consistent=true \
--release-label emr-5.28.0 --ec2-attributes KeyName=myKey
```

若要查看是否使用 AWS Management Console 啟用一致性檢視

- 若要檢查是否在主控台上啟用一致性檢視，導覽到 Cluster List (叢集清單) 並選擇您的叢集名稱以檢視 Cluster Details (叢集詳細資訊)。「EMRFS 一致性檢視」欄位的值為 Enabled 或 Disabled。

若要透過檢查 `emrfs-site.xml` 檔案來查看一致性檢視是否已啟用

- 您可以透過檢查叢集的主節點上的 `emrfs-site.xml` 組態檔案中來確認一致性是否啟用。如果 `fs.s3.consistent` 的布林值設為 `true`，則會針對涉及 Amazon S3 的檔案系統操作啟用一致性檢視。

了解 EMRFS 一致性檢視如何在 Amazon S3 中追蹤物件

EMRFS 會透過將這些物件的相關資訊新增至 EMRFS 中繼資料來在 Amazon S3 中建立物件的一致性檢視。EMRFS 會在以下狀況將這些清單新增至中繼資料：

- 在 Amazon EMR 任務過程由 EMRFS 寫入的物件。
- 會使用 EMRFS CLI 將物件與 EMRFS 中繼資料進行同步，或將物件匯入 EMRFS 中繼資料。

EMRFS 讀取的物件不會自動新增到中繼資料。當 EMRFS 刪除物件時，清單仍會維持在中繼資料中，且保持已刪除的狀態，直到使用 EMRFS CLI 將該清單清除為止。若要進一步了解 CLI，請參閱 [EMRFS CLI 參考 \(p. 60\)](#)。如需有關在 EMRFS 中繼資料清除清單的詳細資訊，請參閱 [EMRFS 一致檢視中繼資料 \(p. 55\)](#)。

對於每個 Amazon S3 操作，EMRFS 會檢查中繼資料是否有一致性檢視中一組物件的相關資訊。如果在這些操作中 EMRFS 發現 Amazon S3 是不一致的，則會根據在 emrfs-site 組態屬性中定義的參數重試操作。在 EMRFS 用完重試數後，它會擲出 `ConsistencyException` 或記錄例外狀況並繼續工作流程。如需關於重試日誌的詳細資訊，請參閱 [重試邏輯 \(p. 55\)](#)。您可以在日誌中找到 `ConsistencyExceptions`，例如：

- `listStatus`：沒有適用於中繼資料項目 `/s3_bucket/dir/object` 的 Amazon S3 物件
- `getFileStatus`：金鑰 `dir/file` 存在於中繼資料 (但不在 Amazon S3)

如果您直接從 EMRFS 一致性檢視追蹤的 Amazon S3 中刪除物件，EMRFS 會將該物件視為不一致，因為其仍然存在於 Amazon S3 所列的中繼資料。如果您的中繼資料與 EMRFS 在 Amazon S3 中追蹤的物件不同步，您可以使用 EMRFS CLI 的 `sync` 子命令重設中繼資料以反映 Amazon S3。為了探索中繼資料和 Amazon S3 之間的差異，請使用 `diff`。最後，EMRFS 只有在中繼資料中參考之物件的一致性檢視，可以是同一個 Amazon S3 路徑中的其他物件 (但未受到追蹤)。EMRFS 列出 Amazon S3 路徑中的物件時，會傳回在中繼資料以及該 Amazon S3 路徑中追蹤的物件超集合。

重試邏輯

EMRFS 經特定次數的嘗試，為在中繼資料中追蹤的物件驗證清單一致性。預設為 5。除非 `fs.s3.consistent.throwExceptionOnInconsistency` 是設定為 `false`，其中它只會記錄以不一致的形式而追蹤的物件，否則為避免超過重試次數，原始任務會傳回錯誤。根據預設，EMRFS 使用指數退避重試政策，但您也可以將它設為固定政策。使用者也可以為特定時段而進行嘗試，再繼續其他任務，而無需擲回例外狀況。他們可以透過將 `fs.s3.consistent.throwExceptionOnInconsistency` 設為 `false`、將 `fs.s3.consistent.retryPolicyType` 設為 `fixed` 和將 `fs.s3.consistent.retryPeriodSeconds` 設為所需的值而達成此目的。以下範例會建立已啟用一致性的叢集，其會記錄不一致且將固定重試間隔設為 10 秒：

Example 將重試期間設為固定數量

```
aws emr create-cluster --release-label emr-5.28.0 \
--instance-type m5.xlarge --instance-count 1 \
--emrfs Consistent=true,Args=[fs.s3.consistent.throwExceptionOnInconsistency=false,
fs.s3.consistent.retryPolicyType=fixed,fs.s3.consistent.retryPeriodSeconds=10] --ec2-
attributes KeyName=myKey
```

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

如需更多詳細資訊，請參閱 [一致性檢視 \(p. 53\)](#)。

EMRFS 一致檢視中繼資料

EMRFS 一致性檢視會使用 DynamoDB 資料表來追蹤一致性，以便追蹤 Amazon S3 中的物件是否已與 EMRFS 同步或由 EMRFS 建立。中繼資料會用於追蹤所有操作 (讀取、寫入、更新和副本)，在該應用程式中也沒有存放實際內容。此中繼資料可用來驗證從 Amazon S3 收到的物件或中繼資料是否如預期一樣。這個確認讓 EMRFS 能夠為 EMRFS 寫入 Amazon S3 的新物件或使用 EMRFS 同步的物件，檢查清單一致性和先寫後讀一致性。多個叢集可以共用相同的中繼資料。

如何將項目新增到中繼資料

您可以使用 sync 或 import 子指令以新增項目到中繼資料。sync 會反映 Amazon S3 物件在路徑中的狀態，同時嚴格使用 import 以新增新項目到中繼資料。如需更多詳細資訊，請參閱 [EMRFS CLI 參考 \(p. 60\)](#)。

如何檢查 Amazon S3 內中繼資料和物件的差異

若要檢查中繼資料和 Amazon S3 之間的差異，請使用 EMRFS CLI 的 diff 子指令。如需更多詳細資訊，請參閱 [EMRFS CLI 參考 \(p. 60\)](#)。

如何知道中繼資料操作正在受到節流

EMRFS 集預設會將對中繼資料讀取和寫入操作的輸送量容量限制設在 400 和 100 單位。大型物件或儲存貯體可能會導致操作超過此容量，DynamoDB 在達到此限制時會調節容量。例如，如果您執行的操作是超過這些容量限制，應用程式可能會導致 EMRFS 擲出 ProvisionedThroughputExceededException。在調節時，EMRFS CLI 工具會嘗試使用指數退避以重試寫入 DynamoDB 資料表，直到操作完成或達到將物件從 Amazon EMR 寫入 Amazon S3 的最大重試值。

您也可以在 Amazon CloudWatch 主控台針對 EMRFS 中繼資料檢視 DynamoDB 指標，而您可在該主控台查看讀取和寫入請求的節流數。如果您有非零值節流請求，應用程式可能會為讀取或寫入操作增加分配輸送量容量而受益。如果您發現操作在讀取或寫入很長一段時間後即將接近最大分配輸送量容量，您也可以實現效能優勢。

顯著 EMRFS 操作的輸送量特性

讀取和寫入操作的預設分別是 400 和 100 輸送量容量單位。以下效能特性讓您能掌握特定操作所需的輸送量。使用單一節點的 m3.1.large 叢集執行這些測試。所有操作皆是進行單一執行緒處理。效能會根據特定的應用程式特性而有所不同，且可能需要試驗來最佳化檔案系統操作。

操作	每秒讀取平均值	每秒寫入平均值
建立 (物件)	26.79	6.70
刪除 (物件)	10.79	10.79
刪除 (包含 1000 個物件的目錄)	21.79	338.40
getFileStatus (物件)	34.70	0
getFileStatus (目錄)	19.96	0
listStatus (包含 1 個物件的目錄)	43.31	0
listStatus (包含 10 個物件的目錄)	44.34	0
listStatus (包含 100 個物件的目錄)	84.44	0
listStatus (包含 1,000 個物件的目錄)	308.81	0
listStatus (包含 10,000 個物件的目錄)	416.05	0
listStatus (包含 100,000 個物件的目錄)	823.56	0
listStatus (包含 100 萬個物件的目錄)	882.36	0
mkdir (持續 120 秒)	24.18	4.03
mkdir	12.59	0
重新命名 (物件)	19.53	4.88

操作	每秒讀取平均值	每秒寫入平均值
重新命名 (包含 1000 個物件的目錄)	23.22	339.34

若要提交步驟，以將舊資料從您的中繼資料存放區中清除

使用者可能希望在以 DynamoDB 為基礎的中繼資料中移除特定項目。這可協助降低與資料表關聯的儲存成本。使用者可以透過使用 EMRFS CLI delete 子指令，手動或以程式設計方式清除特定項目。不過，如果您將項目從中繼資料刪除，EMRFS 將不再進行任何一致性檢查。

透過將最後一個步驟提交到叢集 (亦即在 EMRFS CLI 上執行命令)，即可在完成任務後以程式設計的方式完成清除。例如，輸入下列命令來將步驟提交到您的叢集，以刪除保存時間超過兩天的所有項目。

```
aws emr add-steps --cluster-id j-2AL4XXXXXX5T9 --steps Name="emrfsCLI",Jar="command-runner.jar",Args=[ "emrfs", "delete", "--time", "2", "--time-unit", "days"]
{
    "StepIds": [
        "s-B12345678902"
    ]
}
```

使用傳回的 StepId 值來檢查操作的結果日誌。

設定 CloudWatch 和 Amazon SQS 的一致性通知

針對 Amazon S3 最終一致性問題，您可以在 EMRFS 中啟用 CloudWatch 指標和 Amazon SQS 訊息。

CloudWatch

CloudWatch 指標啟用時，會在 FileSystem API 呼叫因為 Amazon S3 最終一致性失敗而推送名為 Inconsistency (不一致) 的指標。

針對 Amazon S3 最終一致性問題檢視 CloudWatch 指標

若要在 CloudWatch 主控台檢視 Inconsistency (不一致) 指標，請選取 EMRFS 指標，接著選取 JobFlowId/Metric Name (指標名稱) 對。例如：j-162XXXXXXM2CU ListStatus 和 j-162XXXXXXM2CU GetFileStatus 等等。

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. 在 Dashboard (儀表板) 的 Metrics (指標) 區段，選擇 EMRFS。
3. 在 Job Flow Metrics (任務流程指標) 窗格中，選擇一或多個 JobFlowId/Metric Name (指標名稱) 對。圖形呈現的指標會顯示在以下視窗中。

Amazon SQS

Amazon SQS 通知啟用時，名稱為 EMRFS-Inconsistency-<jobFlowId> 的 Amazon SQS 佇列會在 EMRFS 初始化時建立。FileSystem API 呼叫由於 Amazon S3 最終一致性失敗時，即會將 Amazon SQS 訊息推至佇列。訊息包含 JobFlowId、API、不一致路徑的清單、堆疊追蹤之類的資訊。您可以使用 Amazon SQS 主控台或使用 EMRFS read-sqs 命令來讀取訊息。

針對 Amazon S3 最終一致性問題管理 Amazon SQS 訊息

您可以使用 EMRFS CLI 讀取 Amazon SQS 訊息，確認是否有 Amazon S3 最終一致性問題。若要從 EMRFS Amazon SQS 佇列讀取訊息，請輸入 read-sqs 命令，並在主節點的本機檔案系統上指定輸出位置以產生輸出檔。

您也可以使用 `delete-sqs` 命令刪除 EMRFS Amazon SQS 佇列。

- 若要從 Amazon SQS 佇列讀取訊息，請輸入下列命令。使用您設定的 Amazon SQS 佇列名稱取代 `queuename`，並以輸出檔的路徑取代 `/path/filename`：

```
emrfs read-sqs --queue-name queuename --output-file /path/filename
```

例如，要從預設佇列讀取和輸出 Amazon SQS 訊息，請輸入：

```
emrfs read-sqs --queue-name EMRFS-Inconsistency-j-162XXXXXXM2CU --output-file /path/filename
```

Note

您也可以使用 `-q` 和 `-o` 捷徑 (而非 `--queue-name` 和 `--output-file`)。

- 若要刪除 Amazon SQS 佇列，請輸入下列命令：

```
emrfs delete-sqs --queue-name queuename
```

例如，若要刪除預設佇列，請輸入：

```
emrfs delete-sqs --queue-name EMRFS-Inconsistency-j-162XXXXXXM2CU
```

Note

您也可以使用 `-q` 捷徑 (而非 `--queue-name`)。

設定一致性檢視

您可以透過使用 `emrfs-site` 屬性的組態屬性來提供其他設定，以設定這些設定來進行一致性檢視使用。例如，您可以透過將以下引數提供給 CLI `--emrfs` 選項，使用 `emrfs-site` 組態分類 (Amazon EMR 發行版本 4.x 和更高版本)，或引導操作在主節點上設定 `emrfs-site.xml` 檔案，以選擇不同的預設 DynamoDB 輸送量：

Example 在叢集啟動時變更預設中繼資料的讀取和寫入值

```
aws emr create-cluster --release-label emr-5.28.0 --instance-type m5.xlarge \
--emrfs Consistent=true,Args=[fs.s3.consistent.metadata.read.capacity=600, \
fs.s3.consistent.metadata.write.capacity=300] --ec2-attributes KeyName=myKey
```

或者，您可以使用以下組態檔案，並將它儲存在本機或 Amazon S3：

```
[  
  {  
    "Classification": "emrfs-site",  
    "Properties": {  
      "fs.s3.consistent.metadata.read.capacity": "600",  
      "fs.s3.consistent.metadata.write.capacity": "300"  
    }  
  }  
]
```

使用透過以下語法而建立的組態：

```
aws emr create-cluster --release-label emr-5.28.0 --applications Name=Hive \
```

```
--instance-type m5.xlarge --instance-count 2 --configurations file://./myConfig.json
```

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

您可以使用組態或 AWS CLI --emrfs 引數設定以下選項。如需有關那些引數的更多資訊，請參閱 [AWS CLI Command Reference](#)。

一致性檢視的 `emrfs-site.xml` 內容

屬性	預設值	敘述
<code>fs.s3.consistent</code>	<code>false</code>	設為 <code>true</code> 時，此屬性會設定 EMRFS 使用 DynamoDB 以提供一致性。
<code>fs.s3.consistent.retryPolicyType</code>	<code>exponential</code>	此屬性會在重試一致性問題時識別要使用的政策。選項包括：指數、固定或無。
<code>fs.s3.consistent.retryPeriodSeconds</code>	<code>10</code>	此屬性會設定在一致性重試次數之間的等待時間長度。
<code>fs.s3.consistent.retryCount</code>	<code>5</code>	此屬性會設定在偵測到不一致時的重試次數上限。
<code>fs.s3.consistent.throwExceptionOnInconsistency</code>		此屬性會決定是否擲出或記錄一致性例外狀況。設為 <code>true</code> 時，即會擲出 <code>ConsistencyException</code> 。
<code>fs.s3.consistent.metadata.autoCreate</code>	<code>true</code>	設為 <code>true</code> 時，此屬性會啟用中繼資料表的自動建立。
<code>fs.s3.consistent.metadata.etag.verify</code>	<code>false</code> (Beta 版)	您可以透過 Amazon EMR 5.26.0 啟用此屬性。啟用時，EMRFS 會使用 S3 ETags 來驗證正在讀取的物件是否為最新的可用版本。此功能適用於更新後讀取的使用案例，其中在 S3 上的檔案被覆寫，同時保有相同名稱。此 ETag 驗證功能目前不適用於 S3 Select。
<code>fs.s3.consistent.metadata.tableName</code>	<code>EmrFSMetadata</code>	此屬性會指定在 DynamoDB 中的中繼資料表名稱。
<code>fs.s3.consistent.metadata.read.capacity</code>	<code>400</code>	此屬性會指定在中繼資料表建立時 DynamoDB 要佈建的讀取容量。
<code>fs.s3.consistent.metadata.write.capacity</code>	<code>100</code>	此屬性會指定在中繼資料表建立時 DynamoDB 要佈建的寫入容量。
<code>fs.s3.consistent.fastList</code>	<code>true</code>	設為 <code>true</code> 時，此屬性會使用多個執行緒列出目錄 (依需要)。必須啟用一致性才能使用此屬性。
<code>fs.s3.consistent.fastList.prefetchMetadata</code>	<code>false</code>	設為 <code>true</code> 時，此屬性可讓中繼資料預先擷取包含超過 20,000 個項目的目錄。

屬性	預設值	敘述
<code>fs.s3.consistent.notification.CloudWatchLogs</code>	<code>false</code>	設為 <code>true</code> 時，會針對因 Amazon S3 最終一致性問題而失敗的 FileSystem API 呼叫啟用 CloudWatch 指標。
<code>fs.s3.consistent.notification.SQS</code>	<code>false</code>	設為 <code>true</code> 時，最終一致性通知會推送至 Amazon SQS 佇列。
<code>fs.s3.consistent.notification.SQS.queueName</code>	<code>EMRFS-Inconsistency- <jobFlowId></code>	變更此屬性可讓您為有關 Amazon S3 最終一致性問題的訊息指定自己的 SQS 佇列名稱。
<code>fs.s3.consistent.notification.SQS.customMessage</code>	<code>null</code>	此屬性可讓您指定在有關 Amazon S3 最終一致性問題之 SQS 訊息中所含的自訂訊息。如果未針對此屬性指定值，訊息中的對應欄位則為空。
<code>fs.s3.consistent.dynamodb.endpoint</code>	<code>none</code>	此屬性可讓您指定自訂的 DynamoDB 端點以供一致性檢視中繼資料使用。

EMRFS CLI 參考

根據預設，EMRFS CLI 會安裝在使用 Amazon EMR 發行版本 3.2.1 或更新版本建立之所有叢集主節點上。您可以使用 EMRFS CLI 來管理一致性檢視的中繼資料。

Note

僅支援使用 VT100 終端模擬以執行 `emrfs` 命令。不過，它可以使用其他終端機模擬器模式。

emrfs 頂層命令

支援以下結構的 `emrfs` 頂層命令。

```
emrfs [describe-metadata | set-metadata-capacity | delete-metadata | create-metadata | \
list-metadata-stores | diff | delete | sync | import] [options] [arguments]
```

如下表所述，指定 [選項]，其中包含或不含 [引數]。如需子命令專屬的 [選項] (`describe-metadata`、`set-metadata-capacity` 等)，請參閱以下每個子命令。

適用於 `emrfs` [選項]

選項	敘述	必要
<code>-a AWS_ACCESS_KEY_ID</code> <code>--access-key</code> <code>AWS_ACCESS_KEY_ID</code>	AWS 存取金鑰，您可用來將物件寫入 Amazon S3 並建立或存取在 DynamoDB 的中繼資料存放區。在預設情況下， <code>AWS_ACCESS_KEY_ID</code> 會設為用來建立叢集的存取金鑰。	否
<code>-s AWS_SECRET_ACCESS_KEY</code> <code>--secret-key</code> <code>AWS_SECRET_ACCESS_KEY</code>	與存取金鑰關聯的 AWS 私密金鑰，您可用該存取金鑰將物件寫入 Amazon S3 並建立或存取在 DynamoDB 的中繼資料存放區。在預設情況下， <code>AWS_SECRET_ACCESS_KEY</code> 會設為用來建立叢集之與存取金鑰關聯的私密金鑰。	否

選項	敘述	必要
<code>-v --verbose</code>	使輸出最詳細。	否
<code>-h --help</code>	顯示 emrfs 命令的協助訊息，內含使用陳述式。	否

emrfs 描述中繼資料子命令

適用於 emrfs 描述中繼資料 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否

Example emrfs 描述中繼資料範例

以下範例說明預設的中繼資料表格。

```
$ emrfs describe-metadata
EmrFSMetadata
  read-capacity: 400
  write-capacity: 100
  status: ACTIVE
  approximate-item-count (6 hour delay): 12
```

emrfs 設定中繼資料容量子命令

適用於 emrfs 設定中繼資料容量 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否
<code>-r READ_CAPACITY --read-capacity READ_CAPACITY</code>	中繼資料資料表的請求讀取輸送量容量。如果未提供 <code>READ_CAPACITY</code> 引數，預設值是 400。	否
<code>-w WRITE_CAPACITY --write-capacity WRITE_CAPACITY</code>	中繼資料資料表的請求寫入輸送量容量。如果未提供 <code>WRITE_CAPACITY</code> 引數，預設值是 100。	否

Example emrfs 設定中繼資料容量範例

以下範例會將讀取輸送量容量設為 600 而寫入容量設為 150 以供名為 EmrMetadataAlt 的中繼資料資料表使用。

```
$ emrfs set-metadata-capacity --metadata-name EmrMetadataAlt --read-capacity 600 --write-capacity 150
  read-capacity: 400
  write-capacity: 100
  status: UPDATING
```

```
approximate-item-count (6 hour delay): 0
```

emrfs 刪除中繼資料子命令

適用於 emrfs 刪除中繼資料 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否

Example emrfs 刪除中繼資料範例

以下範例會刪除預設的中繼資料資料表。

```
$ emrfs delete-metadata
```

emrfs 建立中繼資料子命令

適用於 emrfs 建立中繼資料 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否
<code>-r READ_CAPACITY --read-capacity READ_CAPACITY</code>	中繼資料資料表的請求讀取輸送量容量。如果未提供 <code>READ_CAPACITY</code> 引數，預設值是 400。	否
<code>-w WRITE_CAPACITY --write-capacity WRITE_CAPACITY</code>	中繼資料資料表的請求寫入輸送量容量。如果未提供 <code>WRITE_CAPACITY</code> 引數，預設值是 100。	否

Example emrfs 建立中繼資料範例

以下範例請求建立名為「EmrFSMetadataAlt」的中繼資料資料表。

```
$ emrfs create-metadata -m EmrFSMetadataAlt
Creating metadata: EmrFSMetadataAlt
EmrFSMetadataAlt
  read-capacity: 400
  write-capacity: 100
  status: ACTIVE
  approximate-item-count (6 hour delay): 0
```

emrfs 列出中繼資料存放區子命令

emrfs list-metadata-stores 子命令沒有 [options]。

Example 清單中繼資料存放區範例

以下範例列出您的中繼資料資料表。

```
$ emrfs list-metadata-stores
EmrFSMetadata
```

emrfs 差異子命令

適用於 emrfs 差異 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否
<code>s3://s3Path</code>	Amazon S3 儲存貯體的路徑會與中繼資料資料表相比較。以遞迴的方式同步儲存貯體。	是

Example emrfs 差異範例

以下範例會將預設中繼資料資料表與 Amazon S3 儲存貯體相比較。

```
$ emrfs diff s3://elasticmapreduce/samples/cloudfront
BOTH | MANIFEST ONLY | S3 ONLY
DIR elasticmapreduce/samples/cloudfront
DIR elasticmapreduce/samples/cloudfront/code/
DIR elasticmapreduce/samples/cloudfront/input/
DIR elasticmapreduce/samples/cloudfront/logprocessor.jar
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-14.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-15.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-16.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-17.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-18.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-19.WxYz1234
DIR elasticmapreduce/samples/cloudfront/input/XABCD12345678.2009-05-05-20.WxYz1234
DIR elasticmapreduce/samples/cloudfront/code/cloudfront-loganalyzer.tgz
```

emrfs 刪除子命令

適用於 emrfs 刪除 [選項]

選項	敘述	必要
<code>-m METADATA_NAME --metadata-name METADATA_NAME</code>	<code>METADATA_NAME</code> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <code>METADATA_NAME</code> 引數，預設值是 EmrFSMetadata。	否
<code>s3://s3Path</code>	您追蹤以進行一致性檢視之 Amazon S3 儲存貯體路徑。以遞迴的方式同步儲存貯體。	是
<code>-t TIME --time TIME</code>	過期時間 (使用時間單位引數來解釋)。會針對指定儲存貯體將所有早於 <code>TIME</code> 引數的中繼資料項目予以刪除。	
<code>-u UNIT --time-unit UNIT</code>	用來解譯時間引數 (奈秒、微秒、毫秒、秒、分鐘、小時或天) 的測量。如果未指定任何引數，預設值會是 days 秒。	
<code>--read-consumption READ_CONSUMPTION</code>	用於 delete 操作之可用讀取輸送量的請求量。如果未提供 <code>READ_CONSUMPTION</code> 引數，預設值是 400。	否

選項	敘述	必要
--write-consumption <i>WRITE_CONSUMPTION</i>	用於 delete 操作之可用寫入輸送量的請求量。如果未提供 <i>WRITE_CONSUMPTION</i> 引數，預設值是 100。	否

Example emrfs 刪除範例

以下範例會將 Amazon S3 儲存貯體中的所有物件從一致性檢視的追蹤中繼資料中移除。

```
$ emrfs delete s3://elasticmapreduce/samples/cloudfront
entries deleted: 11
```

emrfs 匯入子命令

適用於 emrfs 匯入 [選項]

選項	敘述	必要
-m <i>METADATA_NAME</i> --metadata-name <i>METADATA_NAME</i>	<i>METADATA_NAME</i> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <i>METADATA_NAME</i> 引數，預設值是 EmrFSMetadata。	否
s3:// <i>s3Path</i>	您追蹤以進行一致性檢視之 Amazon S3 儲存貯體路徑。以遞迴的方式同步儲存貯體。	是
--read-consumption <i>READ_CONSUMPTION</i>	用於 delete 操作之可用讀取輸送量的請求量。如果未提供 <i>READ_CONSUMPTION</i> 引數，預設值是 400。	否
--write-consumption <i>WRITE_CONSUMPTION</i>	用於 delete 操作之可用寫入輸送量的請求量。如果未提供 <i>WRITE_CONSUMPTION</i> 引數，預設值是 100。	否

Example emrfs 匯入範例

以下範例會使用一致性檢視的追蹤中繼資料來匯入 Amazon S3 儲存貯體中的所有物件。所有不明的金鑰皆遭到忽略。

```
$ emrfs import s3://elasticmapreduce/samples/cloudfront
```

emrfs 同步子命令

適用於 emrfs 同步 [選項]

選項	敘述	必要
-m <i>METADATA_NAME</i> --metadata-name <i>METADATA_NAME</i>	<i>METADATA_NAME</i> 是 DynamoDB 中繼資料資料表的名稱。如果未提供 <i>METADATA_NAME</i> 引數，預設值是 EmrFSMetadata。	否
s3:// <i>s3Path</i>	您追蹤以進行一致性檢視之 Amazon S3 儲存貯體路徑。以遞迴的方式同步儲存貯體。	是
--read-consumption <i>READ_CONSUMPTION</i>	用於 delete 操作之可用讀取輸送量的請求量。如果未提供 <i>READ_CONSUMPTION</i> 引數，預設值是 400。	否

選項	敘述	必要
--write-consumption <i>WRITE_CONSUMPTION</i>	用於 delete 操作之可用寫入輸送量的請求量。如果未提供 <i>WRITE_CONSUMPTION</i> 引數，預設值是 100。	否

Example emrfs 同步子命令範例

以下範例會使用一致性檢視的追蹤中繼資料來匯入 Amazon S3 儲存貯體中的所有物件。所有不明的金鑰皆遭到刪除。

```
$ emrfs sync s3://elasticmapreduce/samples/cloudfront
Syncing samples/cloudfront
removed | 0 unchanged
Syncing samples/cloudfront/code/
removed | 0 unchanged
Syncing samples/cloudfront/
removed | 0 unchanged
Syncing samples/cloudfront/input/
removed | 0 unchanged
Done syncing s3://elasticmapreduce/samples/cloudfront
removed | 0 unchanged
creating 3 folder key(s)
folders written: 3
          0 added | 0 updated | 0
          1 added | 0 updated | 0
          2 added | 0 updated | 0
          9 added | 0 updated | 0
         9 added | 0 updated | 1
```

emrfs 讀取 sqs 子命令

適用於 emrfs 讀取 sqs [選項]

選項	敘述	必要
-q <i>QUEUE_NAME</i> --queue-name <i>QUEUE_NAME</i>	<i>QUEUE_NAME</i> 是在 emrfs-site.xml 中設定的 Amazon SQS 佇列名稱。預設值為 EMRFS-Inconsistency-<jobFlowId> 。	是
-o <i>OUTPUT_FILE</i> --output-file <i>OUTPUT_FILE</i>	<i>OUTPUT_FILE</i> 是主節點本機檔案系統上的輸出檔路徑。從佇列中讀取的訊息會寫入這個檔案。	是

emrfs 刪除 sqs 子命令

適用於 emrfs 刪除 sqs [選項]

選項	敘述	必要
-q <i>QUEUE_NAME</i> --queue-name <i>QUEUE_NAME</i>	<i>QUEUE_NAME</i> 是在 emrfs-site.xml 中設定的 Amazon SQS 佇列名稱。預設值為 EMRFS-Inconsistency-<jobFlowId> 。	是

提交 EMRFS CLI 命令做為步驟

以下範例顯示透過利用 AWS CLI 或 API 和 script-runner.jar 來執行 emrfs 命令做為步驟，以在主節點上使用 emrfs 公用程式。範例使用適用於 Python 的 AWS 開發套件 (Boto)，可將步驟新增到叢集，其會將在 Amazon S3 儲存貯體中的物件新增至預設 EMRFS 中繼資料資料表。以叢集的 ID 取代 *j-2AL4XXXXXX5T9#*

```
import json
import boto3
from botocore.exceptions import ClientError

# Assign the ID of an existing cluster to the following variable
job_flow_id = 'CLUSTER_ID'

# Define a job flow step. Assign appropriate values as desired.
job_flow_step_01 = {
    'Name': 'Example EMRFS Sync Step',
    'ActionOnFailure': 'CONTINUE',
    'HadoopJarStep': {
        'Jar': 's3://elasticmapreduce/libs/script-runner/script-runner.jar',
        'Args': [
            '/home/hadoop/bin/emrfs',
            'sync',
            's3://elasticmapreduce/samples/cloudfront'
        ]
    }
}

# Add the step(s)
emr_client = boto3.client('emr')
try:
    response = emr_client.add_job_flow_steps(JobFlowId=job_flow_id,
                                              Steps=[json.dumps(job_flow_step_01)])
except ClientError as e:
    print(e.response['Error']['Message'])
    exit(1)

# Output the IDs of the added steps
print('Step IDs:')
for stepId in response['StepIds']:
    print(stepId)
```

您可以使用傳回的 StepId 值來檢查操作的結果日誌。

授權存取在 Amazon S3 中的 EMRFS 資料

在預設情況下，EC2 的 EMR 角色會決定在 Amazon S3 中存取 EMRFS 資料的許可。連接到這個角色（無論是使用者或群組）IAM 政策套用會透過 EMRFS 來發出請求。預設值為 EMR_EC2_DefaultRole。如需詳細資訊，請參閱 [叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#)。

從 Amazon EMR 發行版本 5.10.0 開始，您也可以使用安全組態來為 EMRFS 指定 IAM 角色。這可讓您為有多個使用者的叢集將 EMRFS 請求的許可自訂為 Amazon S3。您可以為不同使用者和群組，並根據 Amazon S3 中的字首為不同的 Amazon S3 儲存貯體指定不同 IAM 角色。當 EMRFS 對 Amazon S3 發出請求，以符合您指定的使用者、群組或位置，叢集會使用您指定的對應角色，而不是適用於 EC2 的 EMR 角色。如需更多詳細資訊，請參閱 [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)。

或者，如果您的 Amazon EMR 解決方案所要求的已超出 EMRFS 的 IAM 角色所能提供的，您可以定義自訂登入資料供應商類別，其可讓您自訂 Amazon S3 中 EMRFS 資料的存取權。

為 Amazon S3 中的 EMRFS 資料建立自訂登入資料提供者

若要建立自訂登入資料供應商，您實作 [AWS Credentials Provider](#) 和 Hadoop 可設定的類別。

如需此方法的詳細說明，請參閱在 AWS 大數據部落格中 [透過 AWS 帳戶搭配 EMRFS 來安全地分析資料](#)。部落格文章包含的教學課程，可逐步引導您完成從 IAM 角色到啟動叢集的端對端程序。它還提供一個 Java 程式碼範例，其會實作自訂登入資料供應商類別。

基本步驟如下：

若要指定自訂登入資料供應商

1. 建立自訂登入資料供應商類別 (編譯為 JAR 檔案)。
2. 執行指令碼做為引導操作來將自訂登入資料供應商 JAR 檔案複製到在叢集主節點的 /usr/share/aws/emr/emrfs/auxlib 位置。如需引導操作的詳細資訊，請參閱 [\(選用\) 建立引導操作以安裝其他軟體](#)。
3. 自訂 emrfs-site 分類以指定您在 JAR 檔案中實作的類別。如需將組態物件指定至自訂應用程式的詳細資訊，請參閱 Amazon EMR Release Guide 中的 [設定應用程式](#)。

以下範例示範 `create-cluster` 命令，其會啟動 Hive 叢集與常見的組態參數，而且還包括：

- 執行指令碼的引導操作 `copy_jar_file.sh` 會儲存至 Amazon S3 中的 `mybucket`。
- `emrfs-site` 分類，其會指定在 JAR 檔中定義做為 `MyCustomCredentialsProvider` 的自訂登入資料供應商

Note

將 Linux 的行接續字元 () 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --applications Name=Hive \
--bootstrap-actions '[{"Path": "s3://mybucket/copy_jar_file.sh", "Name": "Custom
action"}]' \
--ec2-attributes '{"KeyName": "MyKeyPair", "InstanceProfile": "EMR_EC2_DefaultRole", \
"SubnetId": "subnet-xxxxxxxx", "EmrManagedSlaveSecurityGroup": "sg-xxxxxxxx", \
"EmrManagedMasterSecurityGroup": "sg-xxxxxxxx"}' \
--service-role EMR_DefaultRole --enable-debugging --release-label emr-5.28.0 \
--log-uri 's3n://my-emr-log-bucket/' --name 'test-awscredentialsprovider-emrfs' \
--instance-type=m5.xlarge --instance-count 3 \
--configurations '[{"Classification": "emrfs-site", \
"Properties": {"fs.s3.customAWSCredentialsProvider": "MyAWSCredentialsProviderWithUri"}, \
"Configurations": []}]'
```

使用 EMRFS 屬性來指定 Amazon S3 加密

Important

從 Amazon EMR 4.8.0 發行版本開始，您可以使用安全組態設定來更輕鬆地並透過更多選項套用加密設定。我們建議您使用安全組態。如需資訊，請參閱「[設定資料加密 \(p. 129\)](#)」。本節所述的主控台說明在 4.8.0 之前的發行版本提供。如果您在後續版本中的叢集組態和安全組態使用 AWS CLI 設定 Amazon S3 加密，則安全組態會覆寫叢集組態。

建立叢集時，您可以使用主控台或使用 `emrfs-site` 分類屬性，透過 AWS CLI 或 EMR 軟體開發套件為 Amazon S3 中的 EMRFS 資料指定伺服器端加密 (SSE) 或用戶端加密 (CSE)。Amazon S3 SSE 和 CSE 互斥；您可以選擇其中之一，但無法同時選擇。

如需 AWS CLI 指示，請參閱以下加密類型的適當區段。

若要使用 AWS Management Console 指定 EMRFS 加密選項

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)，Go to advanced options (前往進階選項)。
3. 選擇 4.7.2 或之前的 Release (版本)。
4. 選擇適用於應用程式的 Software and Steps (軟體和步驟) 的其他選項，然後選擇 Next (下一步)。

5. 選擇在 Hardware (硬體) 和 General Cluster Settings (一般叢集設定) 窗格中適用於您的應用程式的設定。
6. 在 Security (安全) 窗格上，在 Authentication and encryption (身份驗證和加密) 下，選取要使用的 S3 Encryption (with EMRFS) (S3 加密 (搭配 EMRFS))。

Note

使用 KMS 金鑰管理的 S3 伺服器端加密 (SSE-KMS) 在使用 Amazon EMR 發行版本 4.4 或更舊版本時無法使用。

- 如果您選擇使用 AWS Key Management (AWS 金鑰管理) 的選項，請選擇 AWS KMS 金鑰 ID (AWS KMS 金鑰 ID)。如需更多詳細資訊，請參閱 [使用適用於 EMRFS 加密的 AWS KMS 客戶主金鑰 \(CMK\) \(p. 68\)](#)。
- 如果您選擇 S3 client-side encryption with custom materials provider (S3 用戶端加密搭配自訂資料供應商)，請提供 Class name (類別名稱) 和 JAR location (JAR 位置)。如需更多詳細資訊，請參閱 [Amazon S3 用戶端加密 \(p. 70\)](#)。

7. 選擇適用於應用程式的其他選項，然後選擇 Create Cluster (建立叢集)。

使用適用於 EMRFS 加密的 AWS KMS 客戶主金鑰 (CMK)

建立 AWS KMS 加密金鑰的區域必須與您搭配 EMRFS 使用之 Amazon EMR 叢集執行個體及 Amazon S3 儲存貯體的區域相同。若您指定之金鑰的所在帳戶與您用來設定叢集的帳戶不同，則您必須使用金鑰的 ARN 來指定金鑰。

Amazon EC2 執行個體描述檔的角色需有權使用您指定的 CMK。Amazon EMR 中執行個體描述檔的預設角色為 `EMR_EC2_DefaultRole`。若您為執行個體描述檔使用其他角色，或向 Amazon S3 請求使用 EMRFS 的 IAM 角色，請務必適當地將每個角色新增為金鑰使用者。此操作能授予角色使用 CMK 的權限。如需詳細資訊，請參閱 AWS Key Management Service Developer Guide 中的 [使用金鑰政策及叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#)。

您可以使用 AWS Management Console 將您的執行個體描述檔或 EC2 執行個體描述檔新增至指定 AWS KMS CMK 的金鑰使用者清單，或是您也可以使用 AWS CLI 或 AWS 開發套件來連接適當的金鑰政策。

下列程序說明如何使用 AWS Management Console 將預設 EMR 執行個體描述檔

「`EMR_EC2_DefaultRole`」新增為金鑰使用者。這裡假設您已建立了 CMK。若要建立新的 CMK，請參閱 AWS Key Management Service Developer Guide 中的 [建立金鑰](#)。

若要將 Amazon EMR 的 EC2 執行個體描述檔新增至加密金鑰使用者的清單

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at <https://console.aws.amazon.com/kms>.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. 選取要修改的 CMK 別名。
4. 在 Key Users (金鑰使用者) 下的金鑰詳細資訊頁面上，選擇 Add (新增)。
5. 在 Attach (連接) 對話方塊中，選取適當的角色。預設角色的名稱為 `EMR_EC2_DefaultRole`。
6. 選擇 Attach (連接)。

Amazon S3 伺服器端加密

當您設定 Amazon S3 伺服器端加密時，Amazon S3 會在將資料寫入磁碟時於物件層級予以加密，並在資料受到存取時予以解密。如需 SSE 的詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的 [「使用伺服器端加密保護資料」](#)。

當您在 Amazon EMR 中指定 SSE 時，您有兩個不同的金鑰管理系統可選擇：

- SSE-S3：Amazon S3 會為您管理金鑰。

- SSE-KMS：您使用透過適用於 AWS KMS 之政策所設定的 Amazon EMR 自訂主要金鑰 (CMK)。如需 Amazon EMR 金鑰需求的詳細資訊，請參閱「[使用適用於加密的 AWS KMS 客戶主金鑰 \(CMK\) \(p. 148\)](#)」。當您使用 AWS KMS 時，將適用儲存體及使用加密金鑰的費用。如需詳細資訊，請參閱 [AWS KMS 定價](#)。

使用客戶提供之金鑰的 SSE (SSE-C) 無法搭配 Amazon EMR 使用。

使用 AWS CLI 建立已啟用 SSE-S3 的叢集

- 輸入以下命令：

```
aws emr create-cluster --release-label emr-4.7.2 or earlier \
--instance-count 3 --instance-type m5.xlarge --emrfs Encryption=ServerSide
```

您也可以透過在 emrfs-site 屬性中將 fs.s3.enableServerSideEncryption 屬性設定為 true 來啟用 SSE-S3。請參閱以下 SSE-KMS 的範例並省略金鑰 ID 屬性。

使用 AWS CLI 建立已啟用 SSE-KMS 的叢集

Note

SSE-KMS 僅能在 Amazon EMR 發行版本 4.5.0 及更新版本中使用。

- 輸入以下 AWS CLI 命令使用 SSE-KMS 建立叢集，其中 **keyID** 為 AWS KMS 客戶主金鑰 (CMK)，例如 **a4567b8-9900-12ab-1234-123a45678901**：

```
aws emr create-cluster --release-label emr-4.7.2 or earlier --instance-count 3 \
--instance-type m5.xlarge --use-default-roles \
--emrfs Encryption=ServerSide,Args=[fs.s3.serverSideEncryption.kms.keyId=keyID]
```

--或--

使用 emrfs-site 分類輸入以下 AWS CLI 命令並提供組態 JSON 檔案，其內容與以下範例中 myConfig.json 所示類似：

```
aws emr create-cluster --release-label emr-4.7.2 or earlier --instance-count 3 \
--instance-type m5.xlarge --applications Name=Hadoop --configurations file:///
myConfig.json --use-default-roles
```

範例內容 myConfig.json：

```
[  
  {  
    "Classification": "emrfs-site",  
    "Properties": {  
      "fs.s3.enableServerSideEncryption": "true",  
      "fs.s3.serverSideEncryption.kms.keyId": "a4567b8-9900-12ab-1234-123a45678901"  
    }  
  }  
]
```

SSE-S3 和 SSE-KMS 組態屬性

可使用 emrfs-site 組態分類以設定這些屬性。SSE-KMS 僅能在 Amazon EMR 發行版本 4.5.0 及更新版本中使用。

屬性	預設值	敘述
<code>fs.s3.enableServerSideEncryption</code>	<code>false</code>	設為 <code>true</code> 時，會使用伺服器端加密對存放於 Amazon S3 的物件加密。如果沒有指定金鑰，則會使用 SSE-S3。
<code>fs.s3.serverSideEncryption.kms.keyId</code>	<code>n/a</code>	指定 AWS KMS 金鑰 ID 或 ARN。如果已指定金鑰，則會使用 SSE-KMS。

Amazon S3 用戶端加密

使用 Amazon S3 用戶端加密，Amazon S3 加密及解密會在您叢集上的 EMRFS 用戶端進行。物件會在上傳至 Amazon S3 前加密，並在下載之後解密。您指定的提供者會提供用戶端使用的加密金鑰。用戶端可使用由 AWS KMS (CSE-KMS) 提供的金鑰或提供用戶端主要金鑰 (CSE-C) 的自訂 Java 類別。CSE-KMS 和 CSE-C 之間的加密特性有些不同，取決於指定的提供者及要解密或加密之物件的中繼資料。如需這些特性差異的詳細資訊，請參閱Amazon Simple Storage Service Developer Guide中的「[使用用戶端加密保護資料](#)」。

Note

Amazon S3 CSE 只會確認與 Amazon S3 交換的 EMRFS 資料已加密。並非叢集執行個體磁碟區上的所有資料都會加密。除此之外，因為 Hue 不使用 EMRFS，所以 Hue S3 檔案瀏覽器寫入 Amazon S3 的物件都不會加密。

使用 AWS CLI 在 Amazon S3 中為 EMRFS 資料指定 CSE-KMS

- 輸入以下命令，並透過要使用的 AWS KMS CMK 之金鑰 ID 或 ARN 取代 `MyKMSKeyId`：

```
aws emr create-cluster --release-label emr-4.7.2 or earlier
--emrfs Encryption=ClientSide,ProviderType=KMS,KMSKeyId=MyKMSKeyId
```

建立自訂金鑰提供者

當您建立自訂金鑰提供者時，應用程式應實作可在 AWS SDK for Java 1.11.0 版及更新版本中使用的 [EncryptionMaterialsProvider 介面](#)。該實作可使用任何策略來提供加密材料。例如，您可以選擇提供靜態加密材料或與更複雜的金鑰管理系統整合。

用於自訂加密材料的加密演算法必須是 AES/GCM/NoPadding。

EncryptionMaterialsProvider 類別會透過加密內容取得加密材料。Amazon EMR 會在執行時間填入加密內容資訊，以協助發起人決定要傳回的正確加密材料。

Example 範例：使用自訂金鑰提供者進行使用 EMRFS 的 Amazon S3 加密

當 Amazon EMR 從 EncryptionMaterialsProvider 類別擷取加密材料以執行加密時，EMRFS 會選擇性地將兩個欄位填入 materialsDescription 引數：物件的 Amazon S3 URI 及叢集的 JobFlowId，這可讓 EncryptionMaterialsProvider 類別用來選擇性的傳回加密材料。

例如，提供者可針對不同的 Amazon S3 URI 字首傳回不同的金鑰。最後使用 Amazon S3 物件儲存的是傳回加密材料的描述，而非由 EMRFS 產生並傳遞給提供者的 materialsDescription 值。在解密 Amazon S3 物件時，會傳遞加密材料描述給 EncryptionMaterialsProvider 類別，以便其可再次選擇性地傳回相符的金鑰來解密物件。

EncryptionMaterialsProvider 參考實作如下所示。另一個自訂提供者 [EMRFSRSAEncryptionMaterialsProvider](#) 的參考實作則提供於 GitHub。

```
import com.amazonaws.services.s3.model.EncryptionMaterials;
import com.amazonaws.services.s3.model.EncryptionMaterialsProvider;
import com.amazonaws.services.s3.model.KMSEncryptionMaterials;
import org.apache.hadoop.conf.Configurable;
import org.apache.hadoop.conf.Configuration;

import java.util.Map;

/**
 * Provides KMSEncryptionMaterials according to Configuration
 */
public class MyEncryptionMaterialsProviders implements EncryptionMaterialsProvider,
Configurable{
    private Configuration conf;
    private String kmsKeyId;
    private EncryptionMaterials encryptionMaterials;

    private void init() {
        this.kmsKeyId = conf.get("my.kms.key.id");
        this.encryptionMaterials = new KMSEncryptionMaterials(kmsKeyId);
    }

    @Override
    public void setConf(Configuration conf) {
        this.conf = conf;
        init();
    }

    @Override
    public Configuration getConf() {
        return this.conf;
    }

    @Override
    public void refresh() {

    }

    @Override
    public EncryptionMaterials getEncryptionMaterials(Map<String, String>
materialsDescription) {
        return this.encryptionMaterials;
    }

    @Override
    public EncryptionMaterials getEncryptionMaterials() {
        return this.encryptionMaterials;
    }
}
```

使用 AWS CLI 指定自訂資料提供者

若要使用 AWS CLI，請將 `Encryption`、`ProviderType`、`CustomProviderClass` 和 `CustomProviderLocation` 引數傳遞給 `emrfs` 選項。

```
aws emr create-cluster --instance-type m5.xlarge --release-label emr-4.7.2 or earlier
--emrfs Encryption=ClientSide,ProviderType=Custom,CustomProviderLocation=s3://mybucket/
myfolder/provider.jar,CustomProviderClass=classname
```

將 `Encryption` 設為 `ClientSide` 會啟用用戶端加密，`CustomProviderClass` 是 `EncryptionMaterialsProvider` 物件的名稱，而 `CustomProviderLocation` 是本機 Amazon S3 位置，Amazon EMR 會從其中將 `CustomProviderClass` 複製到叢集中每個節點並將其置於 `classpath`。

使用軟體開發套件指定自訂資料提供者

若要使用軟體開發套件，您可以設定屬性 `fs.s3.cse.encryptionMaterialsProvider.uri` 將您存放於 Amazon S3 的自訂 `EncryptionMaterialsProvider` 類別下載到叢集中的每個節點。您在 `emrfs-site.xml` 檔案 (已啟用 CSE) 中進行此設定以及自訂的供應商的適當位置。

例如，在 AWS SDK for Java 中使用 `RunJobFlowRequest`，您的程式碼可能如下所示：

```
<snip>
    Map<String, String> emrfsProperties = new HashMap<String, String>();
    emrfsProperties.put("fs.s3.cse.encryptionMaterialsProvider.uri", "s3://mybucket/
MyCustomEncryptionMaterialsProvider.jar");
    emrfsProperties.put("fs.s3.cse.enabled", "true");
    emrfsProperties.put("fs.s3.consistent", "true");

    emrfsProperties.put("fs.s3.cse.encryptionMaterialsProvider", "full.class.name.of.EncryptionMaterialsPro
Configuration myEmrfsConfig = new Configuration()
    .withClassification("emrfs-site")
    .withProperties(emrfsProperties);

    RunJobFlowRequest request = new RunJobFlowRequest()
        .withName("Custom EncryptionMaterialsProvider")
        .withReleaseLabel("emr-5.28.0")
        .withApplications(myApp)
        .withConfigurations(myEmrfsConfig)
        .withServiceRole("EMR_DefaultRole")
        .withJobFlowRole("EMR_EC2_DefaultRole")
        .withLogUri("s3://myLogUri/")
        .withInstances(new JobFlowInstancesConfig()
            .withEc2KeyName("myEc2Key")
            .withInstanceCount(2)
            .withKeepJobFlowAliveWhenNoSteps(true)
            .withMasterInstanceType("m5.xlarge")
            .withSlaveInstanceType("m5.xlarge")
        );
    RunJobFlowResult result = emr.runJobFlow(request);
</snip>
```

自訂 `EncryptionMaterialsProvider` 與引數

您可能需要直接將引數傳遞給供應商。若要這樣做，您可以使用 `emrfs-site` 組態分類與定義為屬性的自訂引數。其中一個範例組態如下所示，其會儲存為檔案 (`myConfig.json`)：

```
[{
    {
        "Classification": "emrfs-site",
        "Properties": {
            "myProvider.arg1": "value1",
            "myProvider.arg2": "value2"
        }
    }
]
```

藉由 AWS CLI 的 `create-cluster` 命令，您可以使用 `--configurations` 選項指定檔案，如下所示：

```
aws emr create-cluster --release-label emr-5.28.0 --instance-type m5.xlarge
--instance-count 2 --configurations file://myConfig.json --emrfs
Encryption=ClientSide,CustomProviderLocation=s3://mybucket/myfolder/
myprovider.jar,CustomProviderClass=classname
```

Amazon S3 用戶端加密的 `emrfs-site.xml` 屬性

屬性	預設值	敘述
<code>fs.s3.cse.enabled</code>	false	設為 <code>true</code> 時，會使用用戶端加密對存放於 Amazon S3 的 EMRFS 物件加密。
<code>fs.s3.cse.encryptionMaterialsProvider.uri</code>	N/A	當使用自訂加密資料。JAR (內含 <code>EncryptionMaterialsProvider</code>) 所在的 Amazon S3 URI。當您提供此 URI，Amazon EMR 會自動將 JAR 下載到叢集中的所有節點。
<code>fs.s3.cse.encryptionMaterialsProvider</code>	N/A	與用戶端加密搭配使用的 <code>EncryptionMaterialsProvider</code> 類別路徑。使用 CSE-KMS 時，指定 <code>com.amazon.ws.emr.hadoop.fs.cse.KMSEncryptionMaterialsProvider</code> 。
<code>fs.s3.cse.materialsDescription.enabled</code>	false	設為 <code>true</code> 時，會使用物件的 Amazon S3 URI 和 JobFlowId 填入加密物件的 <code>materialsDescription</code> 。當使用自訂加密資料時，設為 <code>true</code> 。
<code>fs.s3.cse.kms.keyId</code>	N/A	使用 CSE-KMS 時進行套用。KeyId、ARN 或用於加密 AWS KMS CMK 的別名。
<code>fs.s3.cse.cryptoStorageMode</code>	<code>ObjectMetadata</code>	Amazon S3 儲存模式。預設情況下，加密資訊的描述會儲存在物件中繼資料。您也可以將說明存放在指令檔案。有效值為 <code>ObjectMetadata</code> 和 <code>InstructionFile</code> 。如需詳細資訊，請參閱 使用適用於 Java 的 AWS 開發套件及 Amazon S3 進行用戶端資料加密 。

控制叢集終止

您建立叢集使用時 Amazon EMR，可以選擇建立暫時性叢集在步驟完成後自動終止，也可以建立長時間執行的叢集，持續執行到您刻意終止為止。叢集終止時，叢集中的所有 Amazon EC2 執行個體都會終止，而且執行個體存放區和 EBS 磁碟區中的資料已不再可用，也無法復原。若要開發策略來藉由寫入 Amazon S3 管理和保留資料以及平衡成本，了解和管理叢集終止相當重要。如需如何手動中指叢集的資訊，請參閱 [終止叢集 \(p. 288\)](#)。

您使用自動終止時，叢集會啟動、執行您指定的任何引導操作，然後執行通常輸入資料、處理資料而後產生和儲存輸出的步驟。步驟完成時，Amazon EMR 會自動終止叢集 Amazon EC2 執行個體。這是執行定期處理任務 (例如每日資料處理執行) 的叢集適用的有效模型。自動終止叢集有助於確保您只需為處理資料所需的时间付費。如需步驟的詳細資訊，請參閱 [使用 CLI 和主控台來使用步驟 \(p. 305\)](#)。

對於長時間執行的叢集，叢集會以相同的方式啟動。您可以連同自動終致的叢集指定步驟，但是叢集會在步驟完成後持續執行並累計費用。您需要以互動或自動的方式查詢資料時，或以互動的方式持續使用叢集上託管的大數據應用程式時，此模型有助於提升效率。此外，如果您定期處理大型資料集，或您經常處理資料集，導致無法每次都有效啟動新的叢集並載入資料，則此模型也有助於提升效率。您可以對於長時間執

行的叢集啟用終止保護，以便防止意外關機。您也可以運用自動擴展之類的功能和執行個體機群，藉以動態調整叢集的大小，以便因應工作負載需求而平衡效能和成本。如需更多詳細資訊，請參閱 [調整叢集資源規模 \(p. 290\)](#) 及 [設定執行個體機群 \(p. 105\)](#)。

本節將說明終止保護和自動終止如何運作，以及這些如何與彼此、其他 Amazon EMR 功能和其他資料程序進行互動。

主題

- [設定叢集自動終止或繼續 \(p. 74\)](#)
- [使用終止保護 \(p. 75\)](#)

設定叢集自動終止或繼續

在預設情況下，您使用主控台或 AWS CLI 建立的叢集會持續執行到您關閉這些叢集為止。若要讓叢集在執行步驟後終止，您需要啟用自動終止。相反地，您使用 EMR API 啟動的叢集預設以啟用自動終止。

若要使用 EMR API 停用自動終止

- 使用 [RunJobFlow](#) 動作來建立叢集時，請將 `KeepJobFlowAliveWhenNoSteps` 屬性設定為 `true`。

若要使用 AWS Management Console 中的快速選項啟用自動終止

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Step execution (步驟執行)。
4. 選擇適用於應用程式的其他設定，然後選擇 Create cluster (建立叢集)。

若要使用 AWS Management Console 中的進階選項啟用自動終止

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)。
4. 在 新增步驟 (選用) 下，選擇 Auto-terminate cluster after the last step is completed (最後一個步驟完成後自動終止叢集)。
5. 選擇適用於應用程式的其他設定，然後選擇 Create cluster (建立叢集)。

若要使用 AWS CLI 啟用自動終止

- 當您使用 `--auto-terminate` 命令指定 `create-cluster` 參數來建立暫時性叢集。

以下範例示範的是使用 `--auto-terminate` 參數。您可以輸入下列命令，然後使用 EC2 金鑰對的名稱來取代 `myKey`。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "Test cluster" --release-label emr-5.28.0 \
--applications Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey \
--steps Type=PIG,Name="Pig Program",ActionOnFailure=CONTINUE, \
Args=[-f,s3://mybucket/scripts/pigscript.pig,-p, \
INPUT=s3://mybucket/inputdata/, -p, OUTPUT=s3://mybucket/outputdata/, \
```

```
$INPUT=s3://mybucket/inputdata/, $OUTPUT=s3://mybucket/outputdata/] --instance-type m5.xlarge --instance-count 3 --auto-terminate
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 [AWS CLI 參考](#)。

使用終止保護

在長時間執行的叢集啟用終止保護時，您仍然可以終止叢集，但是必須先明確移除叢集的終止保護。這有助於確保 EC2 執行個體不會由於意外或錯誤而關閉。如果您的叢集可能有在本機磁碟上儲存的資料，而您需要在終止執行個體前復原這些資料，則終止保護相當實用。您可以在建立叢集時啟用終止保護，也可以對於執行中的叢集變更設定。

啟用終止保護後，Amazon EMR API 中的 `TerminateJobFlows` 動作不會有作用。使用者無法使用此 API 或 AWS CLI 的 `terminate-clusters` 命令終止叢集。API 會傳回錯誤，而且 CLI 結束時會出現非零傳回碼。使用 Amazon EMR 主控台來終止叢集時，會提示您進行額外的步驟來關閉終止保護。

Warning

終止保護不保證資料在萬一發生人為錯誤或有解決方法時也能保留，例如，若使用 SSH 在連線到執行個體時，從命令列發出重新開機命令，或者若執行個體上執行的應用程式或指令碼發出重新開機命令，或者若 Amazon EC2 或 Amazon EMR API 被用來停用終止保護。即使啟用終止保護，儲存至執行個體儲存體的資料（包括 HDFS 資料）也可能遺失。請針對您的商業持續性需求適當地將資料輸出寫入到 Amazon S3 位置並建立備份策略。

終止保護不會影響您使用下列動作擴展叢集資源的能力：

- 手動使用 AWS Management Console 或 AWS CLI 調整叢集大小。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#)。
- 使用自動擴展的向內擴展政策，從核心或任務執行個體群組移除執行個體。如需更多詳細資訊，請參閱 [於 Amazon EMR 使用自動調整規模 \(p. 291\)](#)。
- 減少目標容量，從執行個體機群移除執行個體。如需更多詳細資訊，請參閱 [執行個體機群選項 \(p. 105\)](#)。

終止保護和 Amazon EC2

啟用終止保護的 Amazon EMR 叢集會將叢集內所有 Amazon EC2 執行個體均設定 `disableApiTermination` 屬性。如果 Amazon EMR 發出終止請求，而執行個體的 Amazon EMR 和 Amazon EC2 設定衝突，則 Amazon EMR 設定會覆寫 Amazon EC2 設定。例如，如果您對於已停用終止保護的叢集之中的 Amazon EC2 執行個體使用 Amazon EC2 主控台啟用終止保護，則您使用 Amazon EMR 主控台、Amazon EMR 的 AWS CLI 命令或 Amazon EMR API 終止叢集時，Amazon EMR 會將 `DisableApiTermination` 設定為 `false`，並連同其他執行個體終止該執行個體。

Important

如果建立的執行個體屬於有終止保護的 Amazon EMR 叢集，而且 Amazon EC2 API 或 AWS CLI 命令用於修改該執行個體，使得 `DisableApiTermination` 為 `false`，然後 Amazon EC2 API 或 AWS CLI 命令執行 `TerminateInstances` 動作，則 Amazon EC2 執行個體會終止。

終止保護和有問題的 YARN 節點

對於在叢集中的核心和任務 Amazon EC2 執行個體上執行的節點，Amazon EMR 會定期檢查 Apache Hadoop YARN 狀態。[NodeManager Health Checker Service](#) 會報告運作狀態。如果某個節點報告 `UNHEALTHY`，則 Amazon EMR 執行個體控制器會將該節點列入封鎖清單，而且不會將 YARN 容器分配到該節點，直到再次正常運作為止。對於運作狀態不佳的節點，常見的原因是磁碟使用率超過 90%。如需識別運作狀態不佳的節點和恢復的詳細資訊，請參閱 [資源錯誤 \(p. 324\)](#)。

如果節點持續 `UNHEALTHY` 超過 45 分鐘，Amazon EMR 會根據終止保護的狀態採取下列動作。

終止保護	結果
已啟用 (建議使用)	該 Amazon EC2 執行個體仍處於列入封鎖清單狀態，而且持續計入叢集容量。您可以連接到 Amazon EC2 執行個體設定組態和進行資料復原，並調整您的叢集以增加容量。如需更多詳細資訊，請參閱 資源錯誤 (p. 324) 。
已停用	<p>Amazon EC2 執行個體會終止。根據執行個體群組中指定的執行個體數或執行個體機群的目標容量，Amazon EMR 會佈建新的執行個體。如果所有核心節點呈現 UNHEALTHY 超過 45 分鐘，則叢集會終止，並報告 NO_SLAVES_LEFT 狀態。</p> <p>Important</p> <p>如果核心執行個體因為運作狀態不佳的狀態而終止，則 HDFS 資料可能會遺失。如果節點存放未複製到其他節點的區塊，這些區塊會遺失，而可能導致資料遺失。建議您使用終止保護，以便您可以連接到執行個體並且視需要恢復資料。</p>

終止保護、自動終止和步驟執行

自動終止設定優先於終止保護。如果兩者已啟用，則步驟完成執行時，叢集會終止，而不會進入等待狀態。

您將步驟提交到叢集時，可以設定 ActionOnFailure 屬性，以判斷步驟由於錯誤而無法完成執行時會發生什麼情況。這個設定的可能值為 TERMINATE_CLUSTER (對於舊版 TERMINATE_JOB_FLOW)、CANCEL_AND_WAIT 和 CONTINUE。如需更多詳細資訊，請參閱 [使用 CLI 和主控台來使用步驟 \(p. 305\)](#)。

如果 ActionOnFailure 設定為 CANCEL_AND_WAIT 的步驟失敗，在已啟用自動終止的情況下，叢集會終止而不執行後續步驟。

如果 ActionOnFailure 設定為 TERMINATE_CLUSTER 的叢集失敗，請使用下列設定表格來判斷結果。

ActionOnFailure	自動終止	終止保護	結果
TERMINATE_CLUSTER	Enabled	已停用	叢集終止
	Enabled	Enabled	叢集終止
	已停用	Enabled	叢集繼續
	已停用	已停用	叢集終止

終止保護與 Spot 執行個體

在 Spot 價格超出上限時，Amazon EMR 終止保護功能並不會阻止 Amazon EC2 Spot 執行個體終止。

您啟動叢集時設定終止保護

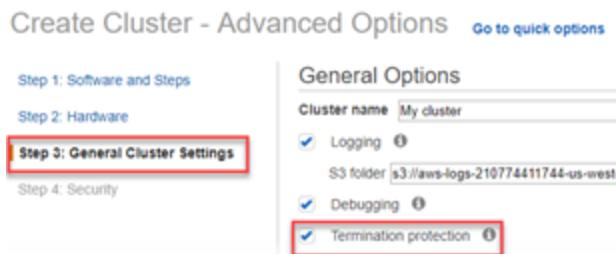
再使用主控台、AWS CLI 或 API 啟動叢集時，可啟用或停用終止保護功能。

預設終止保護設定取決於如何啟動叢集：

- Amazon EMR 主控台快速選項—終止保護預設為已停用。
- Amazon EMR 主控台進階選項—終止保護預設為已啟用。
- 除非指定 `--termination-protected`，否則 AWS CLI `aws emr create-cluster`—終止保護為已停用。
- 除非 `TerminationProtected` 布林值是設定為 `true`，否則 Amazon EMR API `RunJobFlow` 命令—終止保護為已停用。

若要在使用主控台建立叢集時啟用或停用終止保護

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)。
4. 對於 Step 3: General Cluster Settings (步驟 3：一般叢集設定)，在 General Options (一般選項) 下，確定已選取 Termination protection (終止保護) 加以啟用，或清除選取予以停用。



5. 選擇適用於應用程式的其他設定，並選擇 Next (下一步)，然後完成設定叢集。

若要在使用 AWS CLI 建立叢集時啟用終止保護

- 使用 AWS CLI 時，可在啟動叢集時使用 `create-cluster` 命令並使用 `--termination-protected` 參數，即可啟用終止保護功能。終止保護預設為停用。

下列範例會建立終止保護已啟用的叢集：

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "TerminationProtectedCluster" --release-label emr-5.28.0 \
--applications Name=Hadoop Name=Hive Name=Pig \
--use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge \
--instance-count 3 --termination-protected
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

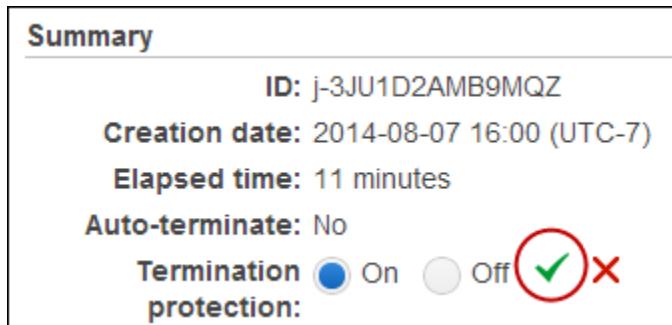
設定執行中叢集的終止保護

您可以使用主控台或 AWS CLI 設定執行中叢集的終止保護功能。

若要在使用主控台執行叢集時啟用或停用終止保護

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.

2. 在 Clusters (叢集) 頁面上，選擇叢集的 Name (名稱)。
3. 在 Summary (摘要) 索引標籤上，對於 Termination protection (終止保護)，選擇 Change (變更)。
4. 若要啟用終止保護，請選擇 On (開啟)。若要停用終止保護，請選擇 Off (關閉)。然後選擇綠色核取標記進行確認。



若要在使用 AWS CLI 執行叢集時啟用或停用終止保護

- 若要使用 AWS CLI 對於執行中叢集啟用終止保護，請使用 `modify-cluster-attributes` 命令與 `--termination-protected` 參數。若要停用，請使用 `--no-termination-protected` 參數。

下列範例會對於 ID `j-3KVTXXXXXX7UG` 的叢集啟用終止保護：

```
aws emr modify-cluster-attributes --cluster-id j-3KVTXXXXXX7UG --termination-protected
```

下列範例會對於同一個叢集停用終止保護：

```
aws emr modify-cluster-attributes --cluster-id j-3KVTXXXXXX7UG --no-termination-protected
```

在 Amazon EMR 中使用 Amazon Linux AMI

Amazon EMR 會使用 Amazon Linux Amazon Machine Image (AMI) 在您建立和啟動叢集時初始化 Amazon EC2 執行個體。AMI 包含每個執行個體代管您的叢集應用程式時，所需的 Amazon Linux 作業系統、其他軟體及組態。

在預設情況下，當您建立叢集時，Amazon EMR 會使用預設的 Amazon Linux AMI，這是專門為您使用的 Amazon EMR 發行版本所建立的。您使用 Amazon EMR 5.7.0 或更新版本時，可以選擇指定自訂 Amazon Linux AMI，而不指定 Amazon EMR 的預設 Amazon Linux AMI。自訂 AMI 可讓您將根設備磁碟區加密，並自訂應用程式和組態，這是使用引導操作的替代選項。

Amazon EMR 會自動連接 Amazon EBS 一般用途 SSD 磁碟區做為所有 AMI 的根裝置磁碟區。使用 EBS 後端 AMI 可增強效能。EBS 的成本是按小時比例計算，以叢集執行所在區域中 gp2 磁碟區的每月 Amazon EBS 費用為基礎。例如，對 EBS 費用為每月 \$0.10/GB 之區域中的每個叢集執行個體上的根磁碟區，每小時的 EBS 成本大約是每小時 \$0.00139 (每月 \$0.10/GB 除以 30 天，除以 24 小時再乘以 10 GB)。無論您使用預設 Amazon Linux AMI 或自訂 Amazon Linux AMI，都可以指定 10-100 GiB 的 EBS 根設備磁碟區大小。

如需 Amazon Linux AMI 的詳細資訊，請參閱 [Amazon Machine Images \(AMI\)](#)。如需 Amazon EMR 執行個體的執行個體儲存體有關的詳細資訊，請參閱 [執行個體儲存體 \(p. 94\)](#)。

主題

- [使用 Amazon EMR 的預設 Amazon Linux AMI \(p. 79\)](#)
- [使用自訂 AMI \(p. 79\)](#)

- 指定 Amazon EBS 根設備磁碟區大小 (p. 84)

使用 Amazon EMR 的預設 Amazon Linux AMI

除非您指定自訂的 AMI，否則每個 Amazon EMR 發行版本都會使用 Amazon EMR 的預設 Amazon Linux AMI。預設 AMI 是以最新的 Amazon EMR 發行時提供的 Amazon Linux AMI 為依據。AMI 通過以大數據應用程式和該發行版本的 Amazon EMR 功能進行的相容性測試。

每個 Amazon EMR 發行版本單對於 Amazon Linux AMI 版本「鎖定」，以維護相容性。這表示，即使有較新的 Amazon Linux AMI 可用，相同的 Amazon Linux AMI 版本也會用於 Amazon EMR 發行版本。因此，除非您需要較舊版本的相容性，而且無法遷移，否則建議您使用最新的 Amazon EMR 發行版本 (目前為 5.28.0)。

如果您由於相容性而必須使用較舊的 Amazon EMR 版本，建議您使用系列的最新版本。例如，如果您必須使用 5.12 系列，請使用 5.12.2，而不使用 5.12.0 或 5.12.1。如果系列有新版本可用，請考慮將應用程式遷移到新的版本。

軟體更新如何受管

在叢集中以 Amazon EMR 的預設 Amazon Linux AMI 為基礎 Amazon EC2 執行個體啟動時，會檢查對於 Amazon Linux 和 Amazon EMR 啟用的套件儲存庫是否有 AMI 版本適用的軟體更新。和其他 Amazon EC2 執行個體一樣，會自動安裝來自這些儲存庫的關鍵和重要安全性更新。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [套件儲存庫](#)。不會安裝其他軟體套件和核心更新，因為這會引起相容性錯誤。

您使用 SSH 連接到執行個體的第一個叢集時，對於該執行個體使用的 Amazon Linux AMI 版本備註、最新 Amazon Linux AMI 版本的通知、啟用的儲存庫提供的更新所適用的套件數通知，以及執行 `sudo yum update` 的指示，畫面輸出前幾行會提供連結。

Important

強烈建議無論是使用 SSH 連接或使用引導操作，都不要在叢集執行個體上執行 `sudo yum update`。這可能會導致不相容的情況發生，因為所有套件一律都會安裝。

管理軟體更新的最佳實務

- 如果您使用較早的 Amazon EMR 發行版本，請考慮和測試最新版本的遷移，再更新軟體套件。
- 如果您遷移到較新版本的版本或您升級軟體套件，請先在非生產環境中測試實作。使用 Amazon EMR 管理主控台複製叢集的選項對此有幫助。
- 對於您的應用程式和 Amazon Linux AMI 的版本分別評估軟體更新。只有在您判斷對於您的安全狀態、應用程式功能或效能絕對有必要的情況下，才需要在生產環境中測試和安裝套件。
- 關注 [Amazon Linux Security Center](#) 的更新。
- 避免使用 SSH 連接到執行個體個別叢集來安裝套件。視需要改為使用引導操作在所有叢集執行個體上安裝和更新套件。這需要您終止叢集並重新啟動。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#)。

使用自訂 AMI

您使用 Amazon EMR 5.7.0 或更新版本時，可以選擇指定自訂 Amazon Linux AMI，而不指定 Amazon EMR 的預設 Amazon Linux AMI。如果您要執行下列動作，可以使用自訂 AMI：

- 預先安裝應用程式，並執行其他自訂項目，而不使用引導操作。這可以改善叢集開始時間並簡化啟動工作流程。如需詳細資訊和範例，請參閱 [從預先設定的執行個體自訂 Amazon Linux AMI \(p. 81\)](#)。
- 實作比引導操作所允許的組態更為複雜的叢集和節點組態。

- 如果您使用的是早於 5.24.0 的 Amazon EMR 版本，加密叢集中 EC2 執行個體的 EBS 根設備磁碟區 (根磁碟區)。如需詳細資訊，請參閱 [建立具有加密 Amazon EBS 根設備磁碟區的自訂 AMI \(p. 83\)](#)。

Note

從 Amazon EMR 5.24.0 版開始，當您指定 AWS KMS 作為您的金鑰提供者時，可以使用安全組態選項以加密 EBS 根設備和儲存磁碟區。如需詳細資訊，請參閱 [本機磁碟加密 \(p. 146\)](#)。

最佳實務和考量

當您為 Amazon EMR 建立自訂 AMI 時，請考慮以下事項：

- 您必須使用 Amazon Linux AMI。不支援 Amazon Linux 2 AMI。目前僅支援 64 位元 Amazon Linux AMI。不支援使用多重 Amazon EBS 磁碟區的 Amazon Linux AMI。
- 以 EBS 支援的最新 [Amazon Linux AMI](#) 為基礎進行自訂。如需 Amazon Linux AMI 和對應 AMI ID 的清單，請參閱 [Amazon Linux AMI](#)。
- 不要複製現有的 Amazon EMR 執行個體快照來建立自訂 AMI。這樣會造成錯誤。
- 只支援 HVM 虛擬化類型以及與 Amazon EMR 相容的執行個體。在進行 AMI 自訂的過程中，務必選取 HVM 映像以及與 Amazon EMR 相容的執行個體類型。如需了解相容的執行個體和虛擬化類型，請參閱 [支援的執行個體類型 \(p. 91\)](#)。
- 您的服務角色必須擁有 AMI 的啟動許可，因此 AMI 必須為公有，或者您必須是 AMI 的擁有者，或是請擁有者與您分享。
- 在 AMI 上建立與應用程式同名的使用者會造成錯誤 (例如 hadoop、hdfs、yarn 或 spark)。
- /tmp、/var 及 /emr 的內容 (如存在 AMI 上) 會在啟動期間分別移至 /mnt/tmp、/mnt/var 和 /mnt/emr。檔案會保留，但如果有多量資料，則啟動時間可能會比預期更久。
- 如果您使用以 Amazon Linux AMI 為基礎的自訂 Amazon Linux AMI，建立日期為 2018-08-11，則 Oozie 伺服器會無法啟動。如果您使用 Oozie，會建立以 Amazon Linux AMI ID 為基礎的自訂 AMI，且建立日期不同。您可以使用以下 AWS CLI 命令傳回所有 2018.03 版本的 HVM Amazon Linux AMI 的映像 ID 清單，以及發行日期，以便您可以選擇適當的 Amazon Linux AMI 做為基礎。以您的區域識別符，例如 us-west-2 來取代 MyRegion。

```
aws ec2 --region MyRegion describe-images --owner amazon --query 'Images[?Name!=`null`]&[?starts_with(Name, `amzn-ami-hvm-2018.03`) == `true`].[CreationDate,ImageId,Name]' --output text | sort -rk1
```

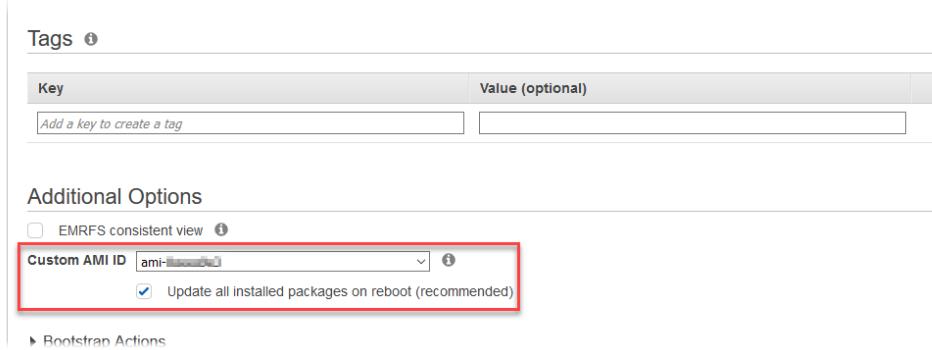
如需詳細資訊，請參閱Amazon EC2 User Guide for Linux Instances中的[建立 Amazon EBS 支援的 Linux AMI](#)。

指定自訂 AMI

您可以在使用 AWS Management Console、AWS CLI、[Amazon CloudWatch](#) 或 Amazon EMR API 建立叢集時，指定自訂的 AMI ID。AMI 必須與您建立的叢集位於相同 AWS 區域。

使用主控台來指定自訂 AMI

- Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
- 選擇 Create cluster (建立叢集)，Go to advanced options (前往進階選項)。
- 在 Software Configuration (軟體組態) 底下，針對 Release (版本) 選擇 emr-5.7.0 (emr-5.7.0) 或更新版本，然後選擇其他適合您應用程式的選項。選擇 Next (下一步)。
- 在 Hardware Configuration (硬體組態) 底下，選取適用於您應用程式的值，然後選擇 Next (下一步)。
- 在 Additional Options (其他選項) 底下，針對 Custom AMI ID (自訂 AMI ID) 輸入值，並且讓更新選項保持選取狀態。如需變更新選項的詳細資訊，請參閱[管理 AMI 套件儲存庫更新 \(p. 81\)](#)。



6. 若要啟動叢集，請選擇 **Next (下一步)** 並完整其他組態選項。

使用 AWS CLI 來指定自訂 AMI

- 在您執行 `--custom-ami-id` 命令時，使用 `aws emr create-cluster` 參數來指定 AMI ID。

以下範例會指定的叢集會使用具有 20 GiB 開機磁碟區的自訂 AMI。如需更多詳細資訊，請參閱 [指定 Amazon EBS 根設備磁碟區大小 \(p. 84\)](#)。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "Cluster with My Custom AMI" \
--custom-ami-id MyAmiID --ebs-root-volume-size 20 \
--release-label emr-5.7.0 --use-default-roles \
--instance-count 2 --instance-type m5.xlarge
```

管理 AMI 套件儲存庫更新

第一次開機時，Amazon Linux AMI 預設會在其他服務啟動之前，先連接至套件儲存庫以安裝安全性更新。根據您的要求，您可以在為 Amazon EMR 指定自訂 AMI 時選擇停用這些更新。停用此功能的選項只有在您使用自訂 AMI 時才可使用。

Warning

我們強烈建議您在指定自訂 AMI 時，選擇在重新開機時更新所有已安裝的套件。選擇不更新套件會產生其他安全風險。

若使用 AWS Management Console，您可以在選擇 Custom AMI ID (自訂 AMI ID) 時，選擇停用更新的選項。

使用 AWS CLI 時，您可以在使用 `create-cluster` 命令時指定 `--repo-upgrade-on-boot NONE` 與 `--custom-ami-id`。

若使用 Amazon EMR API，您可以為 `RepoUpgradeOnBoot` 參數指定 `NONE`。

從預先設定的執行個體自訂 Amazon Linux AMI

預先安裝軟體並執行其他組態，以便為 Amazon EMR 建立自訂 Amazon Linux AMI 的基本步驟如下：

- 從基本 Amazon Linux AMI 啟動執行個體。
- 連接到執行個體以安裝軟體並執行其他自訂。
- 建立您所設定執行個體的新映像 (AMI 快照)。

在您根據自訂的執行個體建立映像之後，您可以將該映像複製到加密的目標，如 [建立具有加密 Amazon EBS 根設備磁碟區的自訂 AMI \(p. 83\)](#) 中所述。

教學課程：從已安裝自訂軟體的執行個體建立 AMI

根據最新的 Amazon Linux AMI 啟動 EC2 執行個體

1. 使用 AWS CLI 執行下列命令，這樣會從現有的 AMI 建立執行個體。將 *MyKeyName* 取代為您用來連線到執行個體的金鑰對，並將 *MyAmiID* 取代為適當的 Amazon Linux AMI ID。如需最新的 AMI ID，請參閱 [Amazon Linux AMI](#)。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws ec2 run-instances --image-id MyAmiID \
--count 1 --instance-type m5.xlarge \
--key-name MyKeyName --region us-west-2
```

InstanceId 輸出值會在下一個步驟中做為 *MyInstanceId* 使用。

2. 執行以下命令：

```
aws ec2 describe-instances --instance-ids MyInstanceId
```

PublicDnsName 輸出值會在下一個步驟中用來連線到執行個體。

連線到執行個體並安裝軟體

1. 使用可讓您在 Linux 執行個體上執行 shell 命令的 SSH 連線。如需更多資訊，請參閱 [Amazon EC2 User Guide for Linux Instances](#) 中的 [使用 SSH 連接至 Linux 執行個體](#)。
2. 進行任何必要的自訂。例如：

```
sudo yum install MySoftwarePackage
sudo pip install MySoftwarePackage
```

從自訂映像建立快照

- 在您自訂執行個體之後，使用 `create-image` 命令從執行個體建立 AMI。

```
aws ec2 create-image --no-dry-run --instance-id MyInstanceId --name MyEmrCustomAmi
```

當您啟動叢集或建立加密快照時，會使用 `imageID` 輸出值。如需更多詳細資訊，請參閱 [指定自訂 AMI \(p. 80\)](#) 及 [建立具有加密 Amazon EBS 根設備磁碟區的自訂 AMI \(p. 83\)](#)。

建立具有加密 Amazon EBS 根設備磁碟區的自訂 AMI

若要在 Amazon EMR 加密 Amazon Linux AMI 的 Amazon EBS 根設備磁碟區，請將快照映像從未加密的 AMI 複製到加密的目標。如需有關建立加密 EBS 磁碟區的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EBS encryption](#)。快照的來源 AMI 可以是基本 Amazon Linux AMI，您也可以從您自訂的基本 Amazon Linux AMI 衍生的 AMI 複製快照。

Note

從 Amazon EMR 5.24.0 版開始，當您指定 AWS KMS 作為您的金鑰提供者時，可以使用安全組態選項以加密 EBS 根設備和儲存磁碟區。如需詳細資訊，請參閱 [本機磁碟加密 \(p. 146\)](#)。

您可以使用外部金鑰提供者或 AWS 客戶主金鑰 (CMK) 來加密 EBS 根磁碟區。Amazon EMR 使用的服務角色 (通常是預設 EMR_DefaultRole) 必須至少能夠加密和解密磁碟區，Amazon EMR 才能使用 AMI 建立叢集。使用 AWS KMS 做為金鑰提供者時，表示必須允許下列動作：

- kms:encrypt
- kms:decrypt
- kms:ReEncrypt*
- kms>CreateGrant
- kms:GenerateDataKeyWithoutPlaintext"
- kms:DescribeKey"

這樣做的最簡單方法，是新增該角色做為金鑰使用者，如以下教學課程所述。如果您需要自訂角色政策，請參考以下提供的範例政策陳述式。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "EmrDiskEncryptionPolicy",  
            "Effect": "Allow",  
            "Action": [  
                "kms:Encrypt",  
                "kms:Decrypt",  
                "kms:ReEncrypt*",  
                "kms>CreateGrant",  
                "kms:GenerateDataKeyWithoutPlaintext",  
                "kms:DescribeKey"  
            ],  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

教學課程：使用 KMS CMK 建立具有加密根設備磁碟區的自訂 AMI

此範例中的第一個步驟是尋找 KMS CMK 的 ARN，或建立新的一項。如需有關建立金鑰的詳細資訊，請參閱 AWS Key Management Service Developer Guide 中的 [建立金鑰](#)。下列程序說明如何將預設服務角色 EMR_DefaultRole 做為金鑰使用者新增至金鑰政策。在您建立或編輯時，記下金鑰的 ARN (ARN) 值。之後您建立 AMI 時會使用 ARN。

使用主控台新增 Amazon EC2 的服務角色至加密金鑰使用者清單

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at <https://console.aws.amazon.com/kms>.

2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. 選擇要使用的 CMK 別名。
4. 在 Key Users (金鑰使用者) 下的金鑰詳細資訊頁面上，選擇 Add (新增)。
5. 在 Attach (連接) 對話方塊中，選擇 Amazon EMR 服務角色。預設角色的名稱為 EMR_DefaultRole。
6. 選擇 Attach (連接)。

使用 AWS CLI 建立加密的 AMI

- 從 AWS CLI 使用 `aws ec2 copy-image` 命令，建立具有加密 EBS 根設備磁碟區以及您所修改金鑰的 AMI。將 `--kms-key-id` 值取代為您稍早建立或修改的完整金鑰 ARN。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws ec2 copy-image --source-image-id MyAmiId \
--source-region us-west-2 --name MyEncryptedEMRAmi \
--encrypted --kms-key-id arn:aws:kms:us-west-2:12345678910:key/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx
```

命令的輸出會提供您建立的 AMI ID，您可以在建立叢集時指定。如需更多詳細資訊，請參閱 [指定自訂 AMI \(p. 80\)](#)。您也可以藉由安裝軟體並執行其他組態選擇自訂此 AMI。如需更多詳細資訊，請參閱 [從預先設定的執行個體自訂 Amazon Linux AMI \(p. 81\)](#)。

指定 Amazon EBS 根設備磁碟區大小

這個選項僅適用於 Amazon EMR 4.x 版及更新版本。使用 AWS Management Console、AWS CLI 或 Amazon EMR API 建立叢集時，您可以指定從 10 GiB (預設) 到最高 100 GiB 的磁碟區大小。此調整僅適用於 EBS 根設備磁碟區，並且會套用至叢集內的所有執行個體。它不適用於儲存磁碟區，您需要在建立叢集時針對每個執行個體類型另外指定儲存磁碟區。

Note

如果您使用預設 AMI，Amazon EMR 會連接一般用途 SSD (gp2) 做為根設備磁碟區類型。自訂 AMI 可能採用不同的根設備磁碟區類型。如需更多詳細資訊，請參閱 [指定自訂 AMI \(p. 80\)](#)。

EBS 根設備磁碟區的成本是按小時比例計算，以叢集執行所在區域中該磁碟區類型的每月 EBS 費用為基礎。儲存磁碟區也一樣。計費單位為 GB，但您指定根磁碟區大小的單位是 GiB，因此建議您估計時將此資訊納入考量 (1 GB 是 0.931323 GiB)。若要估計叢集中 EBS 根設備磁碟區的相關費用，請使用下列公式：

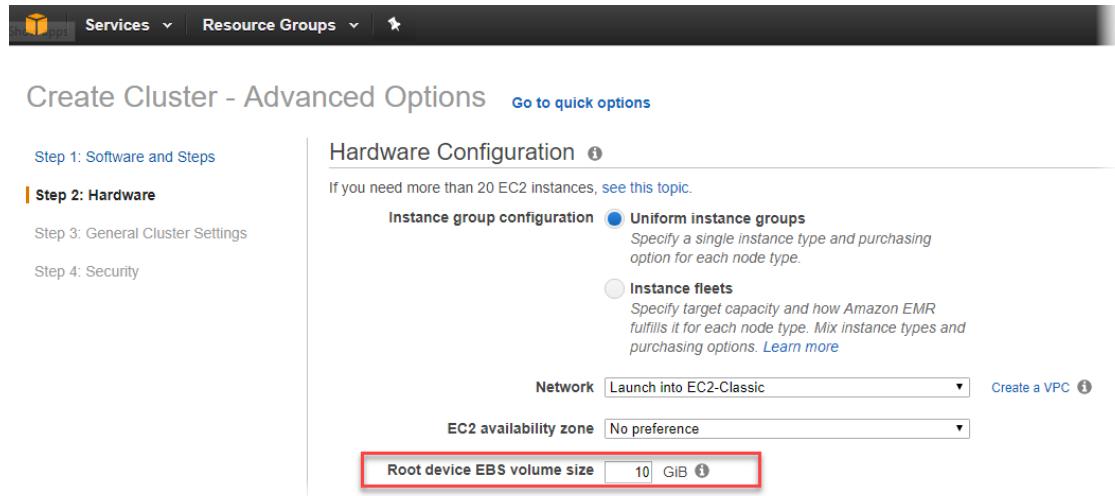
$$(\$/EBS\ GB/month) \times 0.931323 \div 30 \div 24 \times EMR_EBSRootGiB \times InstanceCount$$

以具有主節點、核心節點，且使用具有 10 GiB 根設備磁碟區的基本 Amazon Linux AMI 的叢集為例。如果區域中的 EBS 成本是每月 USD\$0.10/GB，則可計算出每個執行個體每小時約 \$0.00129，而叢集每小時為 \$0.00258 (每月 \$0.10 GB 除以 30 天、除以 24 小時、乘以 10 GB，再乘以 2 個叢集執行個體)。

使用主控台指定 EBS 根設備磁碟區大小

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)。
4. 在 Software Configuration (軟體組態) 底下，針對 Release (版本) 選擇 4.x 或 5.x 值和其他適合您應用程式的選項，然後選擇 Next (下一步)。

5. 在 Hardware Configuration (硬體組態) 底下，針對 Root device EBS volume size (根設備 EBS 磁碟區大小) 輸入介於 10 GiB 到 100 GiB 之間的值。



The screenshot shows the 'Create Cluster - Advanced Options' wizard. On the left, there's a navigation pane with tabs: Step 1: Software and Steps, Step 2: Hardware (which is selected), Step 3: General Cluster Settings, and Step 4: Security. The main area is titled 'Hardware Configuration'. It includes a note about needing more than 20 EC2 instances and links to topics for both 'Uniform instance groups' and 'Instance fleets'. Below these are dropdown menus for 'Network' (set to 'Launch into EC2-Classic') and 'EC2 availability zone' (set to 'No preference'). At the bottom, there's a field labeled 'Root device EBS volume size' with the value '10 GiB' entered, which is highlighted with a red border.

使用 AWS CLI 指定 EBS 根設備磁碟區大小

- 使用 `create-cluster` 命令的 `--ebs-root-volume-size` 參數，如以下範例所示。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --release-label emr-5.7.0 \
--ebs-root-volume-size 20 --instance-groups InstanceGroupType=MASTER, \
InstanceCount=1,InstanceType=m5.xlarge
InstanceGroupType=CORE,InstanceCount=2,InstanceType=m5.xlarge
```

設定叢集軟體

您選取軟體版本時，Amazon EMR 會使用 Amazon Machine Image (AMI) 與 Amazon Linux 以便您啟動叢集時安裝您選擇的軟體，例如 Hadoop、Spark 和 Hive。Amazon EMR 會定期提供新版本、新增新功能、新應用程式和一般更新。我們建議您盡可能使用最新的版本來啟動您的叢集。當您從主控台啟動叢集時，最新版本為預設選項。

如需有關 Amazon EMR 發佈和每次發佈時可使用的軟體版本資訊，請移至 [Amazon EMR Release Guide](#)。如需有關如何編輯安裝在叢集中的應用程式和軟體預設組態資訊，請參閱 [Amazon EMR Release Guide](#) 中的 [設定應用程式](#)。有些包含在 Amazon EMR 版本的開放原始碼 Hadoop 版本和 Spark 生態系統元件擁有修補程式和改進功能，這些都記載在 [Amazon EMR Release Guide](#) 中。

除了可安裝在您叢集上的標準軟體和應用程式外，您可以使用引導操作來安裝自訂軟體。引導操作為叢集啟動時在執行個體上執行的指令碼，且是在叢集建立時新增的新節點上執行。引導操作也可用來在每個節點上叫用 AWS CLI 命令，以從 Amazon S3 複製物件至您叢集中的每個節點。

Note

引導操作在 Amazon EMR 版本 4.x 和更高版本中的使用方式不同。如需關於這些 Amazon EMR AMI 版本 2.x 和 3.x 差異的更多資訊，請參閱 [Amazon EMR Release Guide](#) 中的 [4.x 版本差異介紹](#)。

建立引導操作來安裝其他軟體

您可以使用引導操作安裝其他軟體，或自訂叢集執行個體的組態。引導操作是在 Amazon EMR 使用 Amazon Linux Amazon Machine Image (AMI) 啟動執行個體之後，於叢集上執行的指令碼。引導操作執行的時機是在 Amazon EMR 安裝您建立叢集時指定的應用程式之前，以及叢集節點開始處理資料之前。如果您將節點新增到執行中的叢集，引導操作也會以同樣的方式在這些節點上執行。您可以建立自訂引導操作，並且在建立叢集時指定它們。

Amazon EMR 4.x 版不支援大多數針對 Amazon EMR AMI 版本 2.x 和 3.x 預先定義的引導操作。例如，Amazon EMR 4.x 版不支援 `configure-Hadoop` 和 `configure-daemons`。不過 Amazon EMR 4.x 版原本就支援此功能。如需有關如何將引導操作從 Amazon EMR AMI 2.x 和 3.x 版遷移至 Amazon EMR 4.x 版的詳細資訊，請前往 Amazon EMR Release Guide 中的 [Amazon EMR 4.x 發行版本之間的差異](#)。

主題

- [引導操作基本概念 \(p. 86\)](#)
- [Run If \(執行條件\) 引導操作 \(p. 86\)](#)
- [關機動作 \(p. 87\)](#)
- [使用自訂引導操作 \(p. 87\)](#)

引導操作基本概念

根據預設，引導操作會以 Hadoop 使用者身分執行。您可以使用 `sudo` 以根權限執行引導操作。

所有 Amazon EMR 管理界面都支援引導操作。您可藉由從主控台、AWS CLI 或 API 提供多個 `bootstrap-actions` 參數，為每個叢集最多指定 16 個引導操作。

在建立叢集時，您可以從 Amazon EMR 主控台選擇性地指定引導操作。

使用 CLI 時，您可以在使用 `create-cluster` 命令建立叢集時新增 `--bootstrap-actions` 參數，藉此將引導操作指令碼的參考傳遞至 Amazon EMR。`--bootstrap-actions` 參數的語法如下所示：

AWS CLI

```
--bootstrap-actions Path=s3://mybucket/filename,Args=[arg1,arg2]
```

如果引導操作傳回非零的錯誤代碼，Amazon EMR 會將它視為失敗，並終止執行個體。如果有太多執行個體的引導操作失敗，那麼 Amazon EMR 就會終止叢集。如果只有少數幾個執行個體失敗，Amazon EMR 會嘗試重新配置失敗的執行個體並繼續。使用叢集 `lastStateChangeReason` 錯誤代碼來識別引導操作造成的失敗。

Run If (執行條件) 引導操作

在 `instance.json` 或 `job-flow.json` 檔案中找到執行個體專屬的值時，Amazon EMR 會提供此預先定義的引導操作來執行條件式命令。此命令可參考 Amazon S3 中 Amazon EMR 可下載和執行的檔案。

指令碼的位置是 `s3://elasticmapreduce/bootstrap-actions/run-if`。

以下範例會在節點為主節點時呼應「在主節點上執行」這個字串。

使用 AWS CLI 執行條件式命令

使用 AWS CLI 納入引導操作時，請指定 `Path` 和 `Args` 做為逗號分隔的清單。

- 若要啟動附帶引導操作的叢集，而該引導操作會在 `instance.json` 或 `job-flow.json` 檔案中找到執行個體專屬的值時執行條件式命令，請輸入下列命令，並將 `myKey` 取代為您的 EC2 金鑰對名稱。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 --use-default-roles --ec2-attributes KeyName=myKey --applications Name=Hive --instance-count 1 --instance-type m5.xlarge --bootstrap-actions Path=s3://elasticmapreduce/bootstrap-actions/run-if,Args=[ "instance.isMaster=true", "echo running on master node" ]
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 Amazon EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

關機動作

引導操作指令碼可藉由將指令碼寫入 `/mnt/var/lib/instance-controller/public/shutdown-actions/` 目錄的方式，建立一個或多個關機動作。當叢集終止時，此目錄中的所有指令碼就會平行執行。每個指令碼都必須執行並在 60 秒內完成。

如果節點終止時發生錯誤，則不保證關機動作指令碼會執行。

Note

若使用 Amazon EMR 4.0 版和更新版本，您必須在主節點上手動建立 `/mnt/var/lib/instance-controller/public/shutdown-actions/` 目錄。此目錄並非根據存在的目錄；不過，建立之後，此目錄中的指令碼無論如何都會在關機前執行。如需有關連接主節點以建立目錄的詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

使用自訂引導操作

您可以建立自訂指令碼來執行自訂的引導操作。任何一個 Amazon EMR 界面都可以參考自訂的引導操作。

內容

- [使用 AWS CLI 或 Amazon EMR CLI 新增自訂引導操作 \(p. 87\)](#)
- [使用主控台新增自訂引導操作 \(p. 88\)](#)
- [使用自訂引導操作將物件從 Amazon S3 複製到每個節點 \(p. 88\)](#)

使用 AWS CLI 或 Amazon EMR CLI 新增自訂引導操作

以下範例會使用引導操作指令碼從 Amazon S3 下載壓縮的 TAR 封存，並進行解壓縮。範例指令碼存放於 <http://elasticmapreduce.s3.amazonaws.com/bootstrap-actions/download.sh>。

範例指令碼看起來會像下面這樣：

```
#!/bin/bash
set -e
wget -S -T 10 -t 5 http://elasticmapreduce.s3.amazonaws.com/bootstrap-actions/file.tar.gz
mkdir -p /home/hadoop/contents
tar -xzf file.tar.gz -C /home/hadoop/contents
```

使用 AWS CLI 建立附帶自訂引導操作的叢集

使用 AWS CLI 納入引導操作時，請指定 `Path` 和 `Args` 做為逗號分隔的清單。以下範例不會使用引數清單。

- 若要使用附帶自訂引導操作的叢集，請輸入下列命令，然後將 *myKey* 取代為 EC2 金鑰對的名稱。

- Linux、UNIX 及 Mac OS X 使用者：

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 \
--use-default-roles --ec2-attributes KeyName=myKey \
--applications Name=Hive Name=Pig \
--instance-count 3 --instance-type m5.xlarge \
--bootstrap-actions Path="s3://elasticmapreduce/bootstrap-actions/download.sh"
```

- Windows 使用者：

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.2.0 --use-default-
roles --ec2-attributes KeyName=myKey --applications Name=Hive Name=Pig --instance-
count 3 --instance-type m5.xlarge --bootstrap-actions Path="s3://elasticmapreduce/
bootstrap-actions/download.sh"
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 Amazon EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用主控台新增自訂引導操作

下列程序說明如何使用自己的自訂引導操作。

使用主控台建立附帶自訂引導操作的叢集

- Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
- 選擇 Create cluster (建立叢集)。
- 按一下 Go to advanced options (前往進階選項)。
- 在 Create Cluster - Advanced Options, Steps 1 and 2 (建立叢集 - 進階選項，步驟 1 和 2) 中，選擇所要的選項，然後繼續進行 Step 3: General Cluster Settings (步驟 3：一般叢集設定)。
- 在 Bootstrap Actions (引導操作) 下選取 Configure and add (設定和新增)，以指定引導操作的名稱、JAR 位置和引數。選擇 Add (新增)。
- 您也可以視需要選擇新增更多引導操作。
- 繼續接著建立叢集。您的引導操作會在叢集佈建和初始化完成後執行。

叢集的主節點正在執行時，您可以連接到主節點，並查看引導操作指令碼在 `/mnt/var/log/bootstrap-actions/1` 目錄中產生的日誌檔。

相關主題

- [檢視日誌檔 \(p. 250\)](#)

使用自訂引導操作將物件從 Amazon S3 複製到每個節點

您可以使用引導操作，在應用程式安裝之前將物件從 Amazon S3 複製到叢集中的每個節點。AWS CLI 會安裝於叢集的每個節點，如此您的引導操作就可以呼叫 AWS CLI 命令。

以下範例示範簡單的引導操作指令碼，這會將檔案 myfile.jar 從 Amazon S3 複製到每個叢集節點上的本機資料夾 /mnt1/myfolder 中。指令碼會儲存到 Amazon S3，其檔案名稱為 copymyfile.sh 且包含以下內容。

```
#!/bin/bash
aws s3 cp s3://mybucket/myfilefolder/myfile.jar /mnt1/myfolder
```

當您啟動叢集時，您會指定指令碼。以下 AWS CLI 範例示範此操作：

```
aws emr create-cluster --name "Test cluster" --release-label emr-5.28.0 \
--use-default-roles --ec2-attributes KeyName=myKey \
--applications Name=Hive Name=Pig \
--instance-count 3 --instance-type m5.xlarge \
--bootstrap-actions Path="s3://mybucket/myscriptfolder/copymyfile.sh"
```

設定叢集硬體和聯網

當您建立 EMR 叢集時最重要考量為如何設定 Amazon EC2 執行個體和網路選項。系統會將 EMR 叢集中的 EC2 執行個體組織為節點類型。類型有三種：主節點、核心節點和任務節點。每個節點類型會執行一組在叢集上安裝的分散式應用程式所定義的角色。例如，在 Hadoop MapReduce 或 Spark 任務期間，在核心節點和任務節點上的元件會處理資料、將輸出傳輸到 Amazon S3 或 HDFS，並將狀態中繼資料傳回主節點。有了單一節點叢集，所有元件會在主節點上執行。

主控每個節點的 EC2 執行個體集合也稱為執行個體機群或統一的執行個體群組。您可以在建立叢集時選擇執行個體機群或統一執行個體群組組態。它適用於所有節點類型，而且無法再變更。

您建立叢集時，可選擇最終決定叢集的效能設定檔。本章詳細說明這些選項，並提供這些選項的最佳實務和指導方針。

Note

執行個體併列組態只能在 Amazon EMR 發行版本 4.8.0 及更新版本中使用，不含 5.0.0 及 5.0.3。

主題

- [了解主節點、核心節點和任務節點 \(p. 89\)](#)
- [設定 EC2 執行個體 \(p. 90\)](#)
- [設定網路 \(p. 95\)](#)
- [使用執行個體機群或統一執行個體群組建立叢集 \(p. 104\)](#)
- [叢集組態指南和最佳實務 \(p. 114\)](#)

了解主節點、核心節點和任務節點

您可以透過本節了解 Amazon EMR 如何運用這些節點類型並做為叢集容量規劃的基礎。

主節點

主節點會管理叢集且通常會執行分散式應用程式的主要元件。例如，主節點執行 YARN ResourceManager 服務來管理應用程式的資源，以及 HDFS NameNode 服務。主節點還會追蹤提交至叢集的任務狀態，並監控執行個體群組的運作狀態。

您能夠以 Hadoop 使用者的身分透過 SSH 連接至主節點，藉此監控叢集進度並直接與應用程式互動。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。連接到主節點可讓您直接存取目錄和檔案（例如 Hadoop 日誌檔）。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。您也可以查看當網站在主節

點上執行時應用程式發佈的使用者界面。如需詳細資訊，請參閱檢視 Amazon EMR 叢集上託管的 Web 界面 ([p. 281](#))。

Note

對於 Amazon EMR 5.23.0 和更新版本，您可以啟動具有三個主節點的叢集，以支援 YARN Resource Manager、HDFS Name Node、Spark、Hive 和 Ganglia 等應用程式的高可用性。主節點已不再是此功能潛在的單點失效。如果其中一個主節點故障，Amazon EMR 會自動容錯移轉到待命主節點，並以具有相同組態和引導操作的新主節點來更換故障主節點。如需詳細資訊，請參閱[規劃和設定主節點](#)。

核心節點

核心節點由主節點管理。核心節點執行資料節點協助程式，以在 Hadoop 分散式檔案系統 (HDFS) 過程協調資料儲存。它們還對已安裝應用程式需要的資料執行任務追蹤器協助程式和執行其他平行運算任務。例如，核心節點執行 YARN NodeManager 協助程式、Hadoop MapReduce 任務和 Spark 執行者。

不過，與主節點不同的是，可能會有多個核心節點，因此在執行個體群組或執行個體機群中有許多個 EC2 執行個體。只有一個核心執行個體群組或執行個體機群。您可以透過執行個體群組，在叢集執行中或設定自動擴展時新增和移除 EC2 執行個體。如需有關新增和移除 EC2 執行個體與執行個體群組組態的詳細資訊，請參閱[調整叢集資源規模](#) ([p. 290](#))。您可以使用執行個體機群，透過隨需與 Spot 相應修改執行個體機群的目標容量，來有效地新增和移除執行個體。如需目標容量的詳細資訊，請參閱[執行個體機群選項](#) ([p. 105](#))。

Warning

從執行中的核心節點或移除 HDFS，或終止核心節點資料遺失的風險。設定核心節點使用 Spot 執行個體時必須小心。如需更多詳細資訊，請參閱[我應何時使用 Spot 執行個體？](#) ([p. 115](#))。

任務節點

任務節點是選用的。您可以使用它們來新增對資料執行平行運算任務的能力（例如 Hadoop MapReduce 任務和 Spark 執行者）。任務節點不執行資料節點協助程式，也不會將資料存放在 HDFS 中。您可以使用核心節點，透過將 EC2 執行個體新增至現有統一執行個體群組，或修改任務執行個體機群的目標容量來將任務節點新增至叢集。透過統一執行個體群組組態的叢集總計最多可有 48 個任務執行個體群組。以此種方式新增的統一執行個體群組功能可讓您混合 EC2 執行個體類型和定價選項，例如隨需執行個體和 Spot 執行個體。這讓您能夠以符合成本效益的方式靈活地回應工作負載需求。當您針對叢集使用執行個體機群組態時，混合執行個體類型和購買選項的能力是內建的，所以只有一個任務執行個體機群。

因為 Spot 執行個體經常用來執行任務節點，Amazon EMR 具有用於排定 YARN 工作的預設功能，使得當 Spot 執行個體上執行的任務節點終止時，執行中的工作不會失敗。Amazon EMR 透過允許應用程式主控程序只在核心節點上執行來達成此目的。應用程式主控程序會控制執行中工作，並且需要在工作的生命週期中保持作用中。

Amazon EMR 發行版本 5.19.0 和更新版本使用內建的 [YARN 節點標籤](#) 功能來達成此目的。（較早版本使用的是程式碼修補程式。）`yarn-site` 和 `capacity-scheduler` 組態分類中的屬性會依設設定，使得 YARN 功能排程器和公平排程器會利用節點標籤。Amazon EMR 會自動將核心節點標記 CORE 標籤，並且設定屬性，使得應用程式主控只會排程在具有 CORE 標籤的節點上執行。在 `yarn-site` 和 `capacity-scheduler` 組態分類中手動修改相關屬性，或是直接在相關聯的 XML 檔案中修改，可能會破壞此特性或修改此功能。

如需特定屬性的資訊，請參閱[Amazon EMR 設定可避免由於任務節點 Spot 執行個體終止而造成的任務失敗](#) ([p. 115](#))。

設定 EC2 執行個體

EC2 執行個體提供不同的組態，這些組態稱為執行個體類型。每個執行個體類型都有不同的 CPU、輸入/輸出和儲存容量。除了執行個體類型以外，您可以選擇適用於 EC2 執行個體的不同購買選項。您可以在執行個體群組或執行個體機群中指定不同的執行個體類型和購買選項。如需更多詳細資訊，請參閱[使用執行個體機群或統一執行個體群組建立叢集](#) ([p. 104](#))。如需選擇合適選項的指南，請參閱[叢集組態指南和最佳實務](#) ([p. 114](#))。

Important

使用 AWS Management Console 選擇執行個體類型時，各執行個體類型顯示的 vCPU 數量為該執行個體類型的 YARN vcore 數量，而非該執行個體類型的 EC2 vCPU 數量。如需各執行個體類型的 vCPU 數量詳細資訊，請參閱 [Amazon EC2 執行個體類型](#)。

主題

- [支援的執行個體類型 \(p. 91\)](#)
- [執行個體購買選項 \(p. 92\)](#)
- [執行個體儲存體 \(p. 94\)](#)

支援的執行個體類型

下表說明 Amazon EMR 支援的執行個體類型。如需詳細資訊，請參閱 [Amazon EC2 執行個體](#) 和 [Amazon Linux AMI 執行個體類型矩陣](#)。

並非所有區域皆提供執行個體類型。如果您使用不可用的執行個體類型來建立叢集，您的叢集佈建可能會失敗，或停滯不前。如需有關執行個體可用性的資訊，請參閱 [Amazon EC2 定價頁面](#)，按一下適用於您執行個體購買選項的連結，並依 Region (區域) 篩選來查看您從以下清單中選取的執行個體類型在該區域是否可供使用。

從 Amazon EMR 發行版本 5.13.0 開始，所有執行個體會將 HVM 虛擬化和 EBS 支援儲存用於根磁碟區。當您使用的 Amazon EMR 發行版本早於 5.13.0 之前，某些上一代執行個體會使用 PVM 虛擬化。下表會加以說明。如需詳細資訊，請參閱 [Linux AMI 虛擬化類型](#)。

有些執行個體類型支援增強型聯網。如需詳細資訊，請參閱 [Linux 上增強的聯網功能](#)。

Amazon EMR 支援 ##### 來支援為這些執行個體最佳化但尚未升級的應用程式。如需最這些執行個體類型和升級路徑的詳細資訊，請參閱 [上一代執行個體](#)。

執行個體類別	執行個體類型
一般用途	<i>m1.medium¹ m1.large¹ m1.xlarge¹ m2.xlarge¹ m2.2xlarge¹ m2.4xlarge¹ m3.xlarge¹ m3.2xlarge¹ m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge m5.xlarge m5.2xlarge m5.4xlarge m5.12xlarge m5.24xlarge m5a.xlarge m5a.2xlarge m5a.4xlarge m5a.12xlarge m5a.24xlarge m5d.xlarge³ m5d.2xlarge³ m5d.4xlarge³ m5d.12xlarge³ m5d.24xlarge³</i>
運算優化	<i>c1.medium¹ c1.xlarge¹ c3.xlarge¹ c3.2xlarge¹ c3.4xlarge¹ c3.8xlarge¹ c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c5.xlarge c5.2xlarge c5.4xlarge c5.9xlarge c5.18xlarge c5d.xlarge³ c5d.2xlarge³ c5d.4xlarge³ c5d.9xlarge³ c5d.18xlarge³ c5n.xlarge c5n.2xlarge c5n.4xlarge c5n.9xlarge c5n.18xlarge cc2.8xlarge z1d.xlarge z1d.2xlarge z1d.3xlarge z1d.6xlarge z1d.12xlarge</i>

執行個體類別	執行個體類型
記憶體優化	r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge r5.xlarge ³ r5.2xlarge ³ r5.4xlarge ³ r5.12xlarge ³ r5a.xlarge r5a.2xlarge r5a.4xlarge r5a.12xlarge r5a.24xlarge r5d.xlarge ³ r5d.2xlarge ³ r5d.4xlarge ³ r5d.12xlarge ³ r5d.24xlarge ³ cr1.8xlarge Note 使用 Amazon EMR 5.20.0 版和更新版本時，提供 r5a 系列和 r5d 系列執行個體。
儲存優化	h1.2xlarge h1.4xlarge h1.8xlarge h1.8xlarge hs1.8xlarge¹ i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge i3en.xlarge i3en.2xlarge i3en.3xlarge i3en.6xlarge i3en.12xlarge i3en.24xlarge d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge Note 使用 Amazon EMR 5.9.0 版和更新版本時，提供 i3 系列執行個體。使用 Amazon EMR 5.25.0 版和更新版本時，提供 i3en 系列執行個體。
GPU 執行個體	cg1.4xlarge g2.2xlarge g3.4xlarge g3.8xlarge g3.16xlarge g3s.xlarge p2.xlarge p2.8xlarge p2.16xlarge p3.2xlarge p3.8xlarge p3.16xlarge Note NVIDIA 和 CUDA 驅動程式預設會安裝在 P2 和 P3 執行個體類型。

¹使用 PVM 虛擬化 AMI 與 5.13.0 以前的 Amazon EMR 發行版本。如需詳細資訊，請參閱 [Linux AMI 虛擬化類型](#)。

²不支援 5.15.0 發行版本。

³在發行版本 5.13.0 和更新版本中支援。

執行個體購買選項

當您設定叢集時，您可以選擇適用於 EC2 執行個體的購買選項。您可以選擇使用隨需執行個體、Spot 執行個體或兩者。價格取決於執行個體類型和區域。要了解目前的定價資訊，請參閱 [Amazon EMR 定價](#)。

您在您的叢集中選擇使用執行個體群組或執行個體機群，決定叢集執行時您可如何變更執行個體的購買選項。如果您選擇統一的執行個體群組、執行個體類型和購買選項適用於所有每個執行個體群組中的 EC2 執行個體，而且您僅可以在建立執行個體群組時為其指定購買選項。如果您選擇執行個體機群，您可以在建立執行個體機群後變更購買選項，而且您可以混合購買選項，以滿足您指定的目標容量。如需這些組態的詳細資訊，請參閱 [使用執行個體機群或統一執行個體群組建立叢集 \(p. 104\)](#)。

Important

使用 AWS Management Console 選擇執行個體類型時，各執行個體類型顯示的 vCPU 數量為該執行個體類型的 YARN vcore 數量，而非該執行個體類型的 EC2 vCPU 數量。如需各執行個體類型的 vCPU 數量詳細資訊，請參閱 [Amazon EC2 執行個體類型](#)。

隨需執行個體

使用隨需執行個體，您只需要按小時支付運算容量開銷。或者，您可以讓這些隨需執行個體使用預留執行個體或專用執行個體購買選項。透過預留執行個體，您可以為執行個體進行一次性支付以預留容量。專用執行個體會在主機硬體層級進行實體隔離，與隸屬於其他 AWS 帳戶的執行個體分隔開來。如需購買選項的詳細資訊，請參閱Amazon EC2 User Guide for Linux Instances 中的[執行個體購買選項](#)。

使用預留執行個體

若要在 Amazon EMR 使用預留執行個體，您可以使用 Amazon EC2 來購買預留執行個體，並指定保留的參數（包括適用於區域或可用區域的預留範圍）。如需更多資訊，請參閱[Amazon EC2 預留執行個體](#)以及在Amazon EC2 User Guide for Linux Instances 中的[購買預留執行個體](#)。在您購買預留執行個體後，如果下列所有條件為 True，Amazon EMR 會在叢集啟動時使用預留執行個體：

- 系統會在符合預留執行個體規格的叢集組態中指定隨需執行個體
- 會在執行個體保留的範圍內（可用區域或區域）啟動該叢集
- 預留執行個體的容量仍可供使用

例如，假設您購買一個美國東部區域範圍內之執行個體保留中的 m5.xlarge 預留執行個體。然後，在使用兩個 m5.xlarge 執行個體的美國東部中啟動 EMR 叢集。第一種執行個體會按照預留執行個體的費率來計費，另一種則是會按照隨需執行個體的費率來計費。在任何隨需執行個體建立前已使用預留執行個體容量。

使用專用執行個體

若要使用專用執行個體，您會使用 Amazon EC2 購買專用執行個體，然後使用 Dedicated (專用) 租用屬性來建立 VPC。接著在 Amazon EMR 中指定叢集應在此 VPC 中啟動。在符合專用執行個體規格相之叢集中的任何隨需執行個體使用叢集啟動時可用的專用執行個體。

Note

Amazon EMR 不支援在個別執行個體上設定 dedicated 屬性。

競價型執行個體

Amazon EMR 中的 Spot 執行個體為您提供以降價的方式（與隨需購買相比）購買 Amazon EC2 執行個體容量的選項。使用 Spot 執行個體的缺點是執行個體可能會在價格波動時無預期地終止。如需對於您的應用程式何時適合使用 Spot 執行個體的詳細資訊，請參閱[我應何時使用 Spot 執行個體？\(p. 115\)](#)。

當 Amazon EC2 有未使用的容量，它會以降價的方式提供 EC2 執行個體，稱為 Spot 價格。此價格是根據可用性和需求而有所變化，以及根據區域和可用區域而訂定。當您選擇 Spot 執行個體時，您只需要指定您願意為每個 EC2 執行個體類型支付的 Spot 價格上限。當叢集的可用區域中 Spot 價格低於為執行個體類型指定的 Spot 價格上限，該執行個體即會啟動。執行個體執行時，會根據目前 Spot 價格來向您收費，而非您的 Spot 價格上限。

當您建立含執行個體機群的叢集時，您可以選擇使用定義的持續時間（也稱為 Spot 區塊），其會提供較佳的可預測性。Spot 執行個體會在持續時間結束時終止，但不會在持續時間過期前中斷。本主題說明 Spot 執行個體使用 Amazon EMR 的方式。

要了解目前的定價資訊，請參閱[Amazon EC2 Spot 執行個體定價](#)。如需詳細資訊，請參閱Amazon EC2 User Guide for Linux Instances 中的[Spot 執行個體](#)。當您建立和設定叢集時，您會指定網路選項，其最終會在叢集啟動時判斷可用區域。如需更多詳細資訊，請參閱[設定網路 \(p. 95\)](#)。

Tip

在您使用 Advanced Options (進階選項) 建立叢集時，將滑鼠游標移至 Spot (競價) 購買選項旁的資訊工具提示上，即可在主控台中看到即時 Spot 價格。系統即會顯示在所選區域中每個可用區域的價格。最低價格即為綠色列。由於可用區域間的 Spot 價格會不斷波動，若選擇搭配最低初始價格的

可用區域在叢集的生命週期中可能不會產生最低的價格。對於最佳結果，研究可用區域定價的歷史記錄，再進行選擇。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances中的 [Spot 執行個體定價歷史記錄](#)。

Spot 執行個體選項取決於您在叢集組態中使用的是統一執行個體群組或執行個體機群。

在統一執行個體群組中的 Spot 執行個體

當您在統一執行個體群組中使用 Spot 執行個體時，執行個體群組中的所有執行個體必須是 Spot 執行個體。您可以為叢集指定子網路或可用區域。對於每個執行個體群組，您會指定單一 Spot 執行個體類型和 Spot 價格上限。當叢集的區域和可用區域中 Spot 價格低於 Spot 價格上限，該類型的 Spot 執行個體即會啟動。如果 Spot 價格超過 Spot 價格上限，執行個體即會終止。您只會在設定執行個體群組時設定 Spot 價格上限。您無法在稍後變更該價格。如需更多詳細資訊，請參閱 [使用執行個體機群或統一執行個體群組建立叢集 \(p. 104\)](#)。

執行個體機群中的 Spot 執行個體

當您使用執行個體機群組態，額外的選項可讓您進一步控制 Spot 執行個體 (Spot Instance) 啟動和終止的方式。基本上，執行個體機群是使用非統一執行個體群組的方法來啟動執行個體。它的運作方式是為 Spot 執行個體 (和隨需執行個體) 和高達 5 個執行個體類型建立目標容量。您也可以為每個執行個體類型指定加權容量或使用執行個體類型的 vCPU (YARN vcores) 做為加權容量。在佈建該類型的執行個體時這個加權容量會計入您的目標容量。Amazon EMR 會透過兩種購買選項來佈建執行個體，直到每個目標的目標容量都履行為止。此外，您可以為 Amazon EMR 定義在啟動執行個體時可從中選擇的各種可用區域。您也為每個機群提供額外的 Spot 選項 (包括佈建逾時以及定義的持續時間 (選擇性))。如需更多詳細資訊，請參閱 [設定執行個體機群 \(p. 105\)](#)。

執行個體儲存體

執行個體存放區和/或 EBS 磁碟區儲存空間會用於 HDFS 資料，以及緩衝區、快取、暫存資料及其他暫時內容，一些應用程式可能會將這些內容「溢寫」到本機檔案系統。EMRFS 可協助確保有針對在 Amazon S3 中存放之 HDFS 資料的持久性「真實來源」。

Amazon EBS 在 Amazon EMR 中的運作方式與在一般 Amazon EC2 執行個體中不同。連接到 EMR 叢集的 Amazon EBS 磁碟區是暫時性的：磁碟區會在叢集和執行個體終止時 (例如，當執行個體群組遭到縮減時) 即刪除，因此，請勿預期資料會持續保留。雖然資料是暫時性的，則您能夠根據叢集中的節點數量和專門程度來複寫 HDFS 中的資料。當您新增 EBS 儲存磁碟區時，會將這些磁碟區掛載為額外的磁碟區。他們不是開機磁碟區的一部分。會將 YARN 設定為使用所有其他磁碟區，但您需負責分配額外的磁碟區做為本機儲存 (例如，用於本機日誌檔)。

使用 EMR 叢集使用 Amazon EBS 其他警訥：

- 您無法對 EBS 磁碟區進行快照，然後在 Amazon EMR 中將其還原。若要建立可重複使用的自訂組態，請使用自訂 AMI (在 Amazon EMR 版本 5.7.0 和更新版本上可供使用)。如需詳細資訊，請參閱 [使用自訂 AMI \(p. 79\)](#)。
- 只在使用自訂 AMI 時才支援加密的 EBS 根裝置磁碟區。如需詳細資訊，請參閱 [建立具有加密 Amazon EBS 根設備磁碟區的自訂 AMI \(p. 83\)](#)。目前不支援加密的 EBS 儲存磁碟區。
- 如果您使用 Amazon EMR API 套用標籤，會將這些操作套用到 EBS 磁碟區。
- 每個執行個體的磁碟區限制為 25。

執行個體的預設 EBS 儲存體

Amazon EMR 會為其 AMI 自動連接 Amazon EBS 一般用途 SSD (gp2) 10 GB 的磁碟區做為根裝置來增強效能。此外，對於採用僅限 EBS 儲存體的 EC2 執行個體，Amazon EMR 會將 EBS 儲存磁碟區配置給執行個體。當您使用 Amazon EMR 發行版本 5.22.0 和更新版本建立叢集時，EBS 儲存體的預設數量會根據執行個體的大小增加。此外，我們會將增加的儲存體分割置於多個磁碟區，藉此提升 IOPS 效能，進而提升一些標準化工作負載的效能。如果您想要使用不同的 EBS 執行個體儲存體組態，您可以在建立 EMR 叢集或將節點

新增至現有叢集時加以指定。請參閱下表找出 EBS 儲存磁碟區的預設數量，其大小，以及每個執行個體類型的大小總計。

EBS 的成本是按小時比例計算，以叢集執行所在區域中 gp2 磁碟區的每月 Amazon EBS 費用為基礎。例如，對費用為每月 \$0.10/GB 之區域中的每個叢集節點上的根磁碟區，每小時的 EBS 成本大約是每小時 \$0.00139 (每月 \$0.10/GB 除以 30 天，除以 24 小時再乘以 10 GB)。

Amazon EMR 5.22.0 和更新版本中各執行個體類型的預設 EBS 儲存磁碟區和大小

執行個體大小	磁碟區數目	磁碟區大小 (GiB)	大小總計 (GiB)
*.large	1	32	32
*.xlarge	2	32	64
*.2xlarge	4	32	128
*.4xlarge	4	64	256
*.8xlarge	4	128	512
9xlarge	4	144	576
10xlarge	4	160	640
12xlarge	4	192	768
*.16xlarge	4	256	1024
18xlarge	4	288	1152
24xlarge	4	384	1536

指定其他 EBS 儲存磁碟區

當您在 Amazon EMR 中設定執行個體類型時，您可以指定額外的 EBS 磁碟區，其會新增執行個體存放區 (如果有) 和預設 EBS 磁碟區以外的容量。Amazon EBS 提供以下磁碟區類型：一般用途 (SSD)、佈建 IOPS (SSD)、輸送量最佳化 (HDD)、冷 (HDD) 和磁帶。它們各有不同的效能特性及價格，可讓您根據您應用程式的分析和商業需求來量身打造儲存空間。例如，一些應用程式可能需要溢寫到磁碟，而其他則可以在記憶體內或使用 Amazon S3 安全地運作。

您僅可以在叢集啟動時將 EBS 磁碟區附加到執行個體，除非您只新增額外的任務節點執行個體群組，而您可以在這段期間新增 EBS 磁碟區。如果 EMR 叢集中的執行個體發生故障，則會將執行個體以及連接的 EBS 磁碟區替換為新的。因此，如果您手動分離 EBS 磁碟區，Amazon EMR 會將該磁碟區視為故障，並同時取代執行個體儲存體 (如果適用) 和磁碟區存放區。

設定網路

可能會有兩個網路平台選項供您為叢集選擇：EC2-Classic (EC2-Classic) 和 EC2-VPC (EC2-VPC)。在 EC2-Classic 中，您的執行個體會在與其他客戶共用的單一平面網路中執行。EC2-Classic 僅適用於與特定區域中特定帳戶搭配使用。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2](#) 和 [Amazon VPC](#)。在 EC2-VPC 中，叢集會在與您 AWS 帳戶邏輯隔離的 VPC 中使用 Amazon Virtual Private Cloud (Amazon VPC) 和 EC2 執行個體執行。Amazon VPC 可讓您佈建虛擬私有雲端 (VPC)，其為 AWS 中的隔離區域，您可以在其中設定虛擬網路，以便控制私有 IP 地址範圍、子網路、路由表和網路閘道之類的層面。

VPC 提供下列功能：

- 處理敏感資料

在 VPC 中啟動叢集與使用其他工具 (例如路由表和網路 ACL) 在私有網路中啟動叢集類似，以定義可存取網路的人員。如果您正在處理的是叢集中的敏感資料，您可能需要在 VPC 中啟動叢集所提供的其他存取控制。此外，您可以選擇在私有子網路中啟動資源，其中這些資源都沒有直接的網際網路連線。

- 透過內部網路存取資源

如果您的資料來源位於私有網路，因為傳輸的資料量或由於資料的敏感性質，將該資料上傳到 AWS，以便匯入到 Amazon EMR 將會是不切實際或不理想的。但您可以在 VPC 中啟動叢集，並透過 VPN 將資料中心連接到 VPC，讓叢集可透過內部網路存取資源。例如，如果您在資料中心中有一個 Oracle 資料庫，在透過 VPN 連接到該網路的 VPC 中啟動叢集可讓叢集存取 Oracle 資料庫。

公有和私有子網路

您可以同時在公有和私有 VPC 子網路中啟動 EMR 叢集。這表示您不需要網際網路連線才能執行 EMR 叢集；不過，您可能需要設定網路地址轉譯 (NAT) 和 VPN 通道才能存取服務或位於 VPC 以外的資源，例如在公司內部網路或公有 AWS 服務端點 (如 AWS Key Management Service)。

Important

Amazon EMR 僅支援在版本 4.2 或更高版本中的私有子網路中啟動叢集。

如需 Amazon VPC 的詳細資訊，請參閱 [Amazon VPC User Guide](#)。

主題

- [Amazon VPC 選項 \(p. 96\)](#)
- [設定 VPC 以託管叢集 \(p. 99\)](#)
- [在 VPC 中啟動叢集 \(p. 101\)](#)
- [使用 IAM 限制對 VPC 的許可 \(p. 102\)](#)
- [私有子網路的 Amazon S3 政策下限 \(p. 103\)](#)
- [了解 VPC 的更多資源 \(p. 103\)](#)

Amazon VPC 選項

當您在 VPC 中啟動 Amazon EMR 叢集時，可以公有、私有或共用子網路中啟動它。組態會有些微但顯著的差異，這取決於您為叢集選擇的子網路類型。

公有子網路

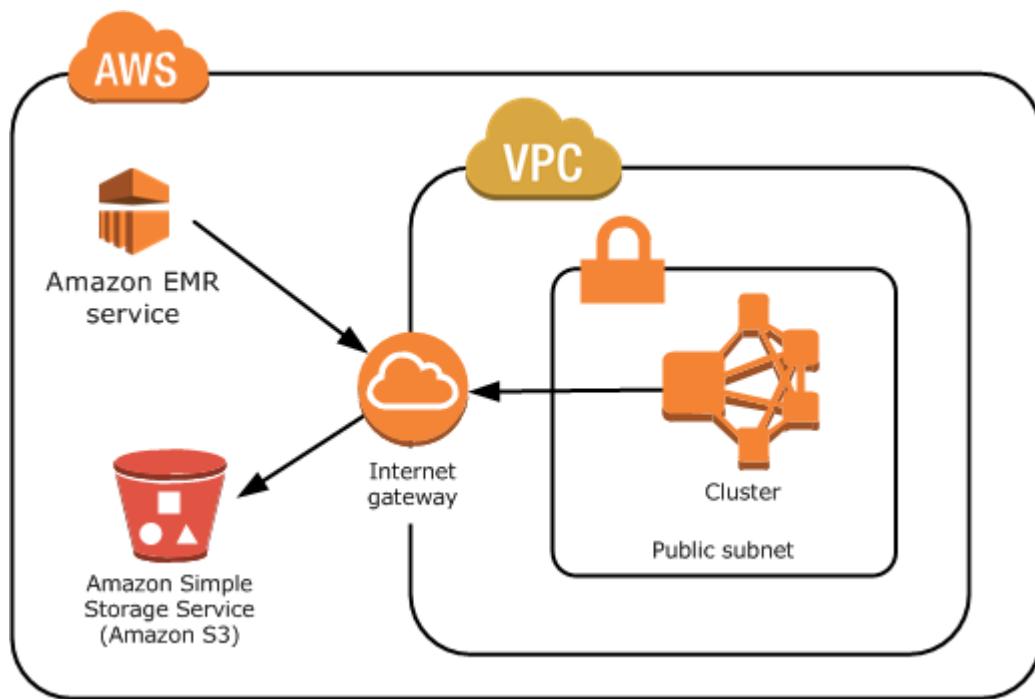
在公有子網路中的 EMR 叢集需要連線網際網路閘道。這是因為 Amazon EMR 叢集必須存取 AWS 服務和 Amazon EMR。如果某服務 (例如 Amazon S3)，可讓您建立 VPC 端點，您可以使用該端點來存取那些服務，而不是透過網際網路閘道存取公有端點。此外，Amazon EMR 無法透過網路地址轉譯 (NAT) 裝置與公有子網路中的叢集通訊。若要達成此目的，則網際網路閘道是必要的，但您仍可以為在更為複雜案例中的其他流量使用 NAT 執行個體或閘道。

在叢集中的所有執行個體會透過 VPC 端點或網際網路閘道來連接至 Amazon S3。目前不支援 VPC 端點的其他 AWS 服務只使用網際網路閘道。

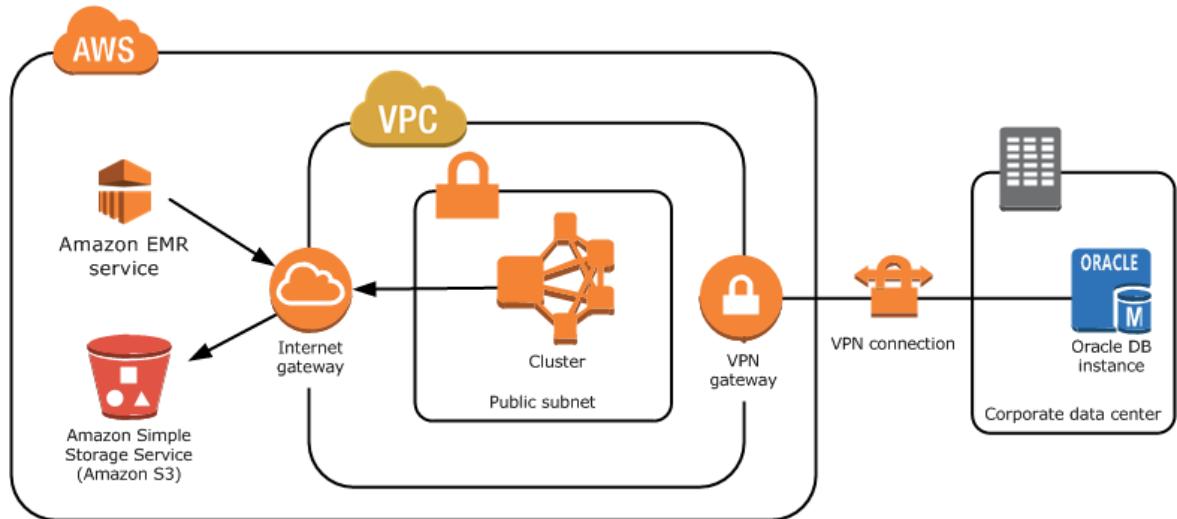
如果您有額外的 AWS 資源，而您不想要將這些資源與網際網路閘道連接，您可以啟動在私有子網路中的那些元件，而該私有子網路是您在 VPC 內所建立的。

公有子網路中執行的叢集中會使用兩個安全群組：一個用於主節點，另一個用於核心節點和任務節點。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

下圖示範 Amazon EMR 叢集如何使用公有子網路在 VPC 中執行。叢集可以透過網際網路閘道連接到其他 AWS 資源 (例如 Amazon S3 儲存貯體)。



下圖示範如何設定 VPC，使該 VPC 中的叢集可以存取您自己網路中的資源 (例如 Oracle 資料庫)。



私有子網路

私有子網路可讓您啟動 AWS 資源，而不需讓子網路擁有連接的網際網路閘道。例如，在後端使用這些私有資源的應用程式中，這可能非常有用。那些資源可以使用位於另一個子網路 (有連接網際網路閘道) 的 NAT 執行個體來啟動傳出流量。如需此情境的詳細資訊，請參閱[案例 2：具公有及私有子網路 \(NAT\) 的 VPC](#)。

Important

Amazon EMR 僅支援在版本 4.2 或更新版本中的私有子網路中啟動叢集。

以下是與公有子網路的差異：

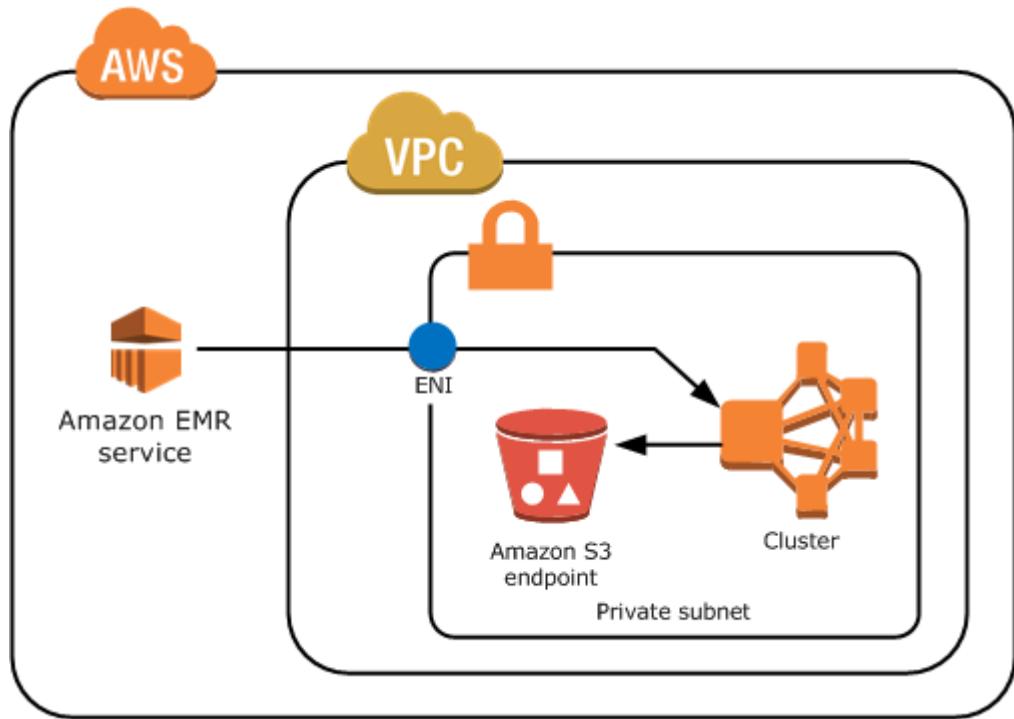
- 若要存取不提供 VPC 端點的 AWS 服務，您仍必須使用 NAT 執行個體或網際網路閘道。

- 至少，您必須提供路由到 Amazon EMR 服務日誌儲存貯體和 Amazon S3 中的 Amazon Linux 儲存庫。如需詳細資訊，請參閱「[私有子網路的 Amazon S3 政策下限 \(p. 103\)](#)」
- 如果您使用的是 EMRFS 功能，您需要有一個 Amazon S3 VPC 端點和從您的私有子網路到 DynamoDB 的路由。
- 如果您提供的是從私有子網路到公有 Amazon SQS 端點的路由，偵錯才適用。
- 僅支援使用 AWS Management Console 透過在公有子網路中的 NAT 執行個體或閘道建立私有子網路組態。增加和設定 NAT 執行個體和 EMR 叢集的 Amazon S3 VPC 端點的最簡單方式是使用 Amazon EMR 主控台中的 VPC Subnets List (VPC 子網路清單) 頁面。若要設定 NAT 閘道，請參閱 Amazon VPC User Guide 中的 [NAT 閘道](#)。
- 您無法將含現有 EMR 叢集的子網路從公開變更為私有，反之亦然。若要尋找私有子網路中的 EMR 叢集，必須在該私有子網路中啟動該叢集。

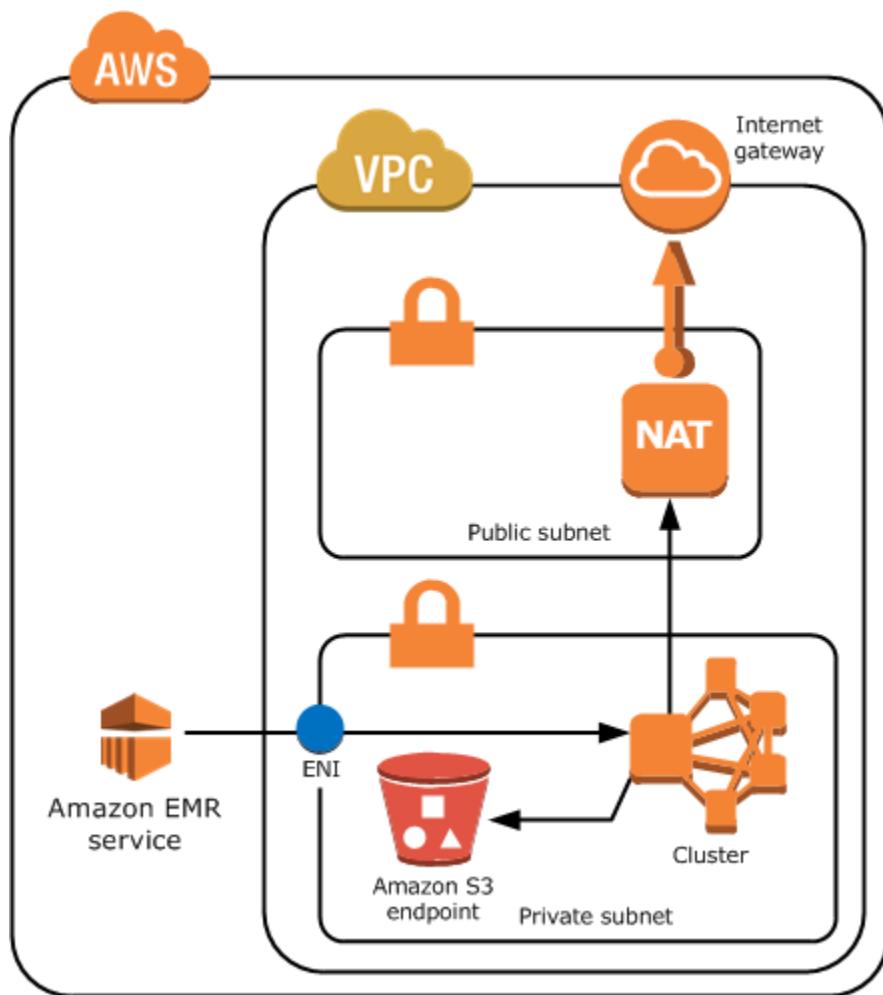
Amazon EMR 在私有子網路中為叢集建立和使用不同的預設安全群組：ElasticMapReduce-Master-Private、ElasticMapReduce-Slave-Private 和 ElasticMapReduce-ServiceAccess。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

如需叢集 NACL 的完整清單，請選擇 Cluster Details (叢集詳細資訊) 頁面 Amazon EMR 主控台上 Security groups for Master (主要的安全群組) 和 Security groups for Core & Task (核心和任務的安全群組)。

下圖示範如何在私有子網路中設定 EMR 叢集。子網路以外的唯一通訊是 Amazon EMR。



下圖示範在位於公有子網路連接到 NAT 執行個體之私有子網路中的 EMR 叢集範例組態。



共用子網路

VPC 共享允許客戶在同一個 AWS 組織內與其他 AWS 帳戶共享子網路。您可以將 Amazon EMR 叢集啟動到公有共用和私有共用子網路，但需注意以下幾點。

子網路擁有者必須與您共享子網路，才能在其中啟動 Amazon EMR 叢集。不過，共用子網路可於日後取消共用。如需詳細資訊，請參閱[使用共用 VPC](#)。當叢集啟動到共用子網路，而該共用子網路隨後取消共用，您可以在子網路未共用時，根據 Amazon EMR 叢集狀態遵守特定行為。

- 叢集成功啟動「之前」子網路未共用 - 如果擁有者在參與者啟動叢集的同時，停止共用 Amazon VPC 或子網路，叢集可能無法啟動或部分初始化而無需佈建所有請求的執行個體。
- 叢集成功啟動「之後」子網路未共用 - 當擁有者停止與參與者共用子網路或 Amazon VPC，參與者的叢集將無法調整以新增執行個體或取代運作狀態不佳的執行個體。

當您啟動 Amazon EMR 叢集時，會建立多個安全群組。在共用子網路中，子網路參與者控制這些安全群組。子網路擁有者可以查看這些安全群組，但無法執行任何動作。如果子網路擁有者想要移除或修改安全群組，建立安全群組的參與者必須採取動作。

設定 VPC 以託管叢集

您可以在 VPC 中啟動叢集前，您必須建立 VPC 和子網路。對於公有子網路，您必須建立網際網路閘道並將它連接到子網路。以下指示說明如何建立可以託管 Amazon EMR 叢集的 VPC。

若要建立子網路來執行 Amazon EMR 叢集

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. 在導覽列上選取要執行您叢集所在的區域。
3. 選擇 Start VPC Wizard (啟動 VPC 精靈)。
4. 選擇以下其中一個選項來選擇 VPC 組態：
 - VPC with a Single Public Subnet (含單一公有子網路的 VPC) — 如果用於叢集適的資料適用於網際網路 (例如，在 Amazon S3 或 Amazon RDS 中)，則選擇此選項。
 - VPC with Public and Private subnets and Hardware VPN Access (含公有和私有子網路以及硬體 VPN 存取的 VPC) — 如果您應用程式的資料是存放在您自己的網路 (例如，在 Oracle 資料庫)，則選取此選項來使用私有子網路。此選項也可讓您在與私有子網路相同的 VPC 包括公有子網路。
5. 確認 VPC 設定。此圖同時顯示單一公有和私有與公有的案例。

Step 2: VPC with a Single Public Subnet

IP CIDR block*: (65531 IP addresses available)
VPC name: My VPC

Public subnet*: (251 IP addresses available)
Availability Zone*: No Preference
Subnet name: Public subnet
You can add more subnets after AWS creates the VPC.

Enable DNS hostnames*: Yes No
Hardware tenancy*: Default

Create VPC

Step 2: VPC with Public and Private Subnets

IP CIDR block*: (65531 IP addresses available)
VPC name:

Public subnet*: (251 IP addresses available)
Availability Zone*: No Preference
Public subnet name: Public subnet

Private subnet*: (251 IP addresses available)
Availability Zone*: No Preference
Private subnet name: Private subnet
You can add more subnets after AWS creates the VPC.

Specify the details of your NAT instance (Instance rates apply).
Instance type*: m1.small
Key pair name: No key pair

Add endpoints for S3 to your subnets
Subnet: None

Enable DNS hostnames*: Yes No
Hardware tenancy*: Default

- 若要使用 Amazon EMR，含公有子網路的 VPC 必須同時有網際網路閘道和子網路。

對於私有子網路中的 VPC，所有 EC2 執行個體必須擁有至少一個透過彈性網路介面對 Amazon EMR 的路由。在主控台中，我們將會自動為您設定。

- 為 VPC 使用私有 IP 地址空間，以確保適當的 DNS 主機名稱解析度，否則，您可能遭遇 Amazon EMR 叢集故障。這包括以下 IP 地址範圍：
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- 選擇 Use a NAT instance instead (改用 NAT 執行個體) 然後選擇適當的選項。
- 選擇性地選擇 Add endpoints for S3 to your subnets (將 S3 端點至新增子網路)。
- 確定 Enable DNS hostnames (啟用 DNS 主機名稱) 已核取。當您建立 VPC 時，您可以選擇啟用 DNS 主機名稱。若要變更 DNS 主機名稱的設定，選擇 VPC 清單中的 VPC，然後選擇詳細資訊窗格中的 Edit (編輯)。若要建立不包含網域名稱的 DNS 項目，為 DHCP Options Set (DHCP 選項設定) 建立一個值，然後將其與您的 VPC 建立關聯。您不能在 DNS 選項設定建立後使用主控台來編輯網域名稱。

如需詳細資訊，請參閱[使用 DNS 與您的 VPC 搭配](#)。

- 這是一項 Hadoop 和相關應用程式的最佳實務，可確保節點完整網域名稱 (FQDN) 的解析度。若要確保適當的 DNS 解析度，您必須設定包含 DHCP 選項集的 VPC，且其參數設定為以下值：
 - domain-name (domain-name) = **ec2.internal**

如果您的區域是 US East (N. Virginia)，請使用 **ec2.internal**。若是其他區域，則使用 **region-name.compute.internal**。如需 us-west-2 的範例，請使用 **us-west-2.compute.internal**。對於 AWS GovCloud (US-West) 區域，請使用 **us-gov-west-1.compute.internal**。

- domain-name-servers (domain-name-servers) = **AmazonProvidedDNS**

如需更多詳細資訊，請參閱 Amazon VPC User Guide 中的 [DHCP 選項集](#)。

6. 選擇 Create VPC (建立 VPC)。如果您要建立 NAT 執行個體，這可能需要花費幾分鐘的時間來完成。

VPC 建立之後，請移至 Subnets (子網路) 頁面，並注意 VPC 其中一個子網路的識別符。當您在 VPC 啟動 EMR 叢集時可以使用此資訊。

在 VPC 中啟動叢集

當您擁有設定為託管 Amazon EMR 叢集的子網路後，透過指定在建立叢集時關聯子網路識別符來在該子網路中啟動叢集。

Note

Amazon EMR 支援在發行版本 4.2 及更新版本中的私有子網路。。

叢集啟動時，Amazon EMR 會根據叢集是在 VPC 私有或公有子網路中啟動來新增安全群組。所有安全群組允許在連接埠 8443 的輸入以與 Amazon EMR 服務通訊，但公有和私有子網路的 IP 地址範圍會有所不同。所有安全群組允許在連接埠 8443 的輸入以與 Amazon EMR 服務通訊，但公有和私有子網路的 IP 地址範圍會有所不同。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

若要在 VPC 中管理叢集，Amazon EMR 會透過此裝置將網路裝置連接到主節點並管理它。您可以使用 Amazon EC2 API 動作 [DescribeInstances](#) 來檢視此裝置。如果您以任何方式修改此裝置，叢集可能會失敗。

使用 Amazon EMR 主控台在 VPC 中啟動叢集

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)。

4. 在 Hardware Configuration (硬體組態) 區段，對於 Network (網路)，選取之前建立的 VPC 網路 ID。
5. 對於 EC2 Subnet (EC2 子網路)，選取之前建立的子網路 ID。
 - a. 如果已使用 NAT 執行個體和 S3 端點選項適當設定您的私有子網路，它會在子網路名稱和識別符上方顯示 (EMR 就緒)。
 - b. 如果您的私有子網路中沒有 NAT 執行個體和/或 S3 端點，您可以透過選擇 Add S3 endpoint and NAT instance (新增 S3 端點和 NAT 執行個體)、Add S3 endpoint (新增 S3 端點) 或 Add NAT instance (新增 NAT 執行個體) 來這麼做。為 NAT 執行個體和 S3 端點選取所需的選項，然後選擇 Configure (設定)。

Important

為了從 Amazon EMR 建立 NAT 執行個體，您需要

ec2:CreateRoute、ec2:RevokeSecurityGroupEgress、ec2:AuthorizeSecurityGroupEgress、cloudformation:CreateStack 許可。

Note

為您的 NAT 裝置啟動 EC2 執行個體會產生額外成本。

6. 繼續建立叢集。

使用 AWS CLI 在 VPC 中啟動叢集

Note

AWS CLI 不提供自動建立 NAT 執行個體並將其連接到私有子網路的方法。不過，若要在子網路建立 S3 端點，您可以使用 Amazon VPC CLI 命令。使用此主控台以建立 NAT 執行個體並在私有子網路中啟動叢集。

在 VPC 設定好後，您可以使用 `create-cluster` 子指令搭配 `--ec2-attributes` 參數，以在其中啟動 EMR 叢集。使用 `--ec2-attributes` 參數來為叢集指定 VPC 子網路。

- 若要在特定子網路中建立叢集，輸入下列命令，使用 EC2 金鑰對的名稱來取代 `myKey`，並使用子網路 ID 來取代 `77XXXX03`。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.2.0 --  
applications Name=Hadoop Name=Hive Name=Pig --use-default-roles --ec2-attributes  
KeyName=myKey,SubnetId=subnet-77XXXX03 --instance-type m5.xlarge --instance-count 3
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都會使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 Amazon EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 [AWS CLI](#)。

使用 IAM 限制對 VPC 的許可

當您在 VPC 中啟動叢集，您可以使用 AWS Identity and Access Management (IAM)，以控制對叢集的存取叢集和使用政策來限制動作，就跟您使用在 EC2-Classic 中啟動的叢集一樣。如需 IAM 的詳細資訊，請參閱 [IAM User Guide](#)。

您也可以使用 IAM 來控制誰可以建立和管理子網路。如需更多在 Amazon EC2 和 Amazon VPC 中有關管理政策和動作的詳細資訊，請參閱 [Amazon EC2 User Guide for Linux Instances](#) 中 [Amazon EC2 的 IAM 政策](#)。

在預設情況下，所有 IAM 使用者可以查看帳戶的所有子網路，且任何使用者可以在任何子網路中啟動叢集。

您可以限制存取管理子網路的能力，同時仍可讓使用者在子網路中啟動叢集。若要這樣做，請建立一個使用者帳戶，其具有可建立和設定子網路的許可，與第二個使用者帳戶，其可以啟動叢集，但無法修改 Amazon VPC 設定。

私有子網路的 Amazon S3 政策下限

對於私有子網路，您至少必須可以讓 Amazon EMR 存取 Amazon Linux 儲存庫和 Amazon EMR 服務支援日誌儲存貯體。下列政策提供這些許可。使用日誌儲存貯體所在的區域取代 *MyRegion*，例如 us-east-1。

Note

從 Amazon EMR 5.25.0 開始，您可以從主控台連線到 Spark 歷程記錄伺服器 UI。若要啟用此選項，您必須將「arn:aws:s3:::prod.*MyRegion*.appinfo.src/*」加入私有子網路的 Amazon S3 政策資源清單，如下列範例所示。

```
{  
    "Version": "2008-10-17",  
    "Statement": [  
        {  
            "Sid": "AmazonLinuxAMIRRepositoryAccess",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": "s3:GetObject",  
            "Resource": [  
                "arn:aws:s3:::packages.*.amazonaws.com/*",  
                "arn:aws:s3:::repo.*.amazonaws.com/*"  
            ]  
        },  
        {  
            "Sid": "AccessToEMRLogBucketsForSupport",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": [  
                "s3:Put*",  
                "s3:Get*",  
                "s3>Create*",  
                "s3:Abort*",  
                "s3>List*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::aws157-logs-prod-MyRegion/*",  
                "arn:aws:s3:::aws157-logs-prod/*",  
                "arn:aws:s3:::prod.MyRegion.appinfo.src/*"  
            ]  
        }  
    ]  
}
```

了解 VPC 的更多資源

若要進一步了解 VPC 與子網路，請參閱下列主題。

- 在 VPC 中的私有子網路
 - [案例 2：含公有和私有子網路 \(NAT\) 的 VPC](#)
 - [NAT 執行個體](#)
 - [Amazon VPC NAT 執行個體的高可用性：範例](#)
- 在 VPC 中的公有子網路

- 案例 1：含單一公有子網路的 VPC
- 一般 VPC 資訊
 - [Amazon VPC User Guide](#)
 - [VPC Peering](#)
 - [使用彈性網路界面搭配 VPC](#)
 - [安全地連接到在私有 VPC 中執行的 Linux 執行個體](#)

使用執行個體機群或統一執行個體群組建立叢集

當您建立叢集並指定主節點、核心節點和任務節點的組態時，您有兩個組態選項。您可以使用執行個體機群或統一執行個體群組。您選擇的組態選項適用於所有節點，它適用於叢集的生命週期，且執行個體機群和執行個體群組不能在叢集中共存。執行個體機群組態在 Amazon EMR 4.8.0 版及更新版本 (不含 5.0.x 的版本) 中可供使用。

您可以使用 EMR 主控台、AWS CLI 或 EMR API 來建立含其中一個組態的頻道。透過 AWS CLI 使用 `create-cluster` 命令時，您可以使用 `--instance-fleets` 參數來使用執行個體機群建立叢集，或者您可以使用 `--instance-groups` 參數來使用統一的執行個體群組將其建立。

使用 EMR API 的方式也是一樣。您使用 `InstanceGroups` 組態來指定一系列的 `InstanceGroupConfig` 物件，或您使用 `InstanceFleets` 組態來指定一系列的 `InstanceFleetConfig` 物件。

在 EMR 主控台中，如果您在建立叢集時使用預設的 Quick Options (快速選項) 設定，Amazon EMR 會將統一執行個體群組組態套用到叢集並使用隨需執行個體。若要使用 Spot 執行個體與統一的執行個體群組，或是要設定執行個體機群和其他自訂項目，請選擇 Advanced Options (進階選項)。

Tip

若要快速簡單地複製您已經建立的叢集，Amazon EMR 在主控台中提供兩個選項。您可以複製叢集或產生 `create cluster` CLI 命令。首先，選擇 Cluster list (叢集清單)，然後選擇您想要複製的叢集。選擇 AWS CLI export (AWS CLI 讀出) 以讓 Amazon EMR 產生對等的叢集 `create cluster` CLI 命令，您之後可以將其複製並貼上。選擇 Clone (複製) 按鈕，讓 Amazon EMR 複製您的主控台設定。Amazon EMR 會提供您 Advanced Options (進階選項) 的最後一個步驟來確認叢集的組態。

您可以選擇 Create cluster (建立叢集)，以建立新叢集 (使用相同的名稱和不同的叢集 ID)，或者您可以選擇 Previous (上一步) 以返回並變更設定。

執行個體機群

執行個體機群組態提供各種佈建 EC2 執行個體的選項。每個節點類型都有單一執行個體機群，而任務執行個體機群是選用的。對於每個執行個體機群，您可以指定最多 5 個執行個體類型，它可以佈建為隨需和 Spot 執行個體。對於核心節點和任務執行個體機群，您會為隨需執行個體指定一個目標容量，而為 Spot 執行個體指定另一個目標容量。Amazon EMR 選擇混合 5 個執行個體類型以滿足目標容量，同時佈建隨需和 Spot 執行個體。對於主節點類型，Amazon EMR 從清單中選擇至多五個單一執行個體類型，而且您會指定它是否佈建為隨需或 Spot 執行個體。執行個體機群還提供額外的 Spot 執行個體購買選項，其中包含定義的持續時間 (也稱為 spot 區塊) 和指定 Spot 容量無法佈建時要採取動作的逾時值。如需更多詳細資訊，請參閱 [設定執行個體機群 \(p. 105\)](#)。

統一執行個體群組

統一執行個體群組提供簡化的設定。每個 Amazon EMR 叢集可包含最多 50 個執行個體群組：一個主執行個體群組，其中包含一個 EC2 執行個體，核心執行個體群組，包含一或多個 EC2 執行個體，以及最多可達 48 可選任務執行個體群組。每個核心和任務執行個體群組可以包含任意數量的 EC2 執行個體。您可以透過手動新增和移除 EC2 執行個體來擴展每個執行個體群組，或者您可以設定自動擴展。如需設定統一執行個體群組的詳細資訊，請參閱 [設定統一執行個體群組 \(p. 112\)](#)。如需有關新增和移除執行個體的詳細資訊，請參閱 [調整叢集資源規模 \(p. 290\)](#)。

主題

- [設定執行個體機群 \(p. 105\)](#)
- [設定統一執行個體群組 \(p. 112\)](#)

設定執行個體機群

叢集的執行個體機群組態提供各種佈建 EC2 執行個體的選項。使用執行個體機群時，您可以為每個機群中的隨需執行個體與 Spot 執行個體指定目標容量。當叢集啟動時，Amazon EMR 會佈建執行個體，直到目標滿足為止。您可在每個機群最多可以指定 5 個 EC2 執行個體類型，以便 Amazon EMR 在滿足目標時使用。您也可以為不同可用區域選擇多個子網路。當 Amazon EMR 啓動叢集時，它會在這些子網路中尋找您指定的執行個體和購買選項。

當叢集執行時，如果 Amazon EC2 由於價格增加或執行個體失敗而回收 Spot 執行個體，則 Amazon EMR 會嘗試用您指定的任何執行個體類型來替換執行個體。這能讓 Spot 定價高峰期間重新獲得容量變得更容易。執行個體機群可讓您為每個節點類型制定靈活有彈性的資源分配策略。例如，在特定機群內，如果可用，您可以擁有透過較低成本的 Spot 容量補充的隨需容量核心；而如果以您的價格無法提供 Spot，則會切換至隨需容量。

Note

執行個體併列組態只能在 Amazon EMR 發行版本 4.8.0 及更新版本中使用，不含 5.0.0 及 5.0.3。

重要功能的摘要

- 每個節點類型 (主要、核心、任務) 的一個執行個體機群和一個唯一。可為每個機群指定最多 5 個 EC2 執行個體類型。
- Amazon EMR 選擇任一或所有 5 個 EC2 執行個體類型來同時使用 Spot 和隨需購買選項進行佈建。
- 針對核心機群和任務機群建立適用於 Spot 和隨需執行個體的目標容量。使用計入目標的 vCPU 或指派給每個 EC2 執行個體的一般單位。直到每個目標容量完全履行為止，Amazon EMR 會佈建執行個體。針對主機群，目標一律為一個。
- 選擇一個子網路 (可用區域) 或範圍。Amazon EMR 會在最符合的可用區域中佈建容量。
- 當您為 Spot 執行個體指定目標容量時：
 - 針對每種執行個體類型，指定最大的 Spot 價格。如果 Spot 價格低於最大 Spot 價格，Amazon EMR 會佈建 Spot 執行個體。您僅需支付該 Spot 價格。
 - 你也可為每個機群選擇性地指定已定義的持續時間 (也稱為 Spot 區塊)。Spot 執行個體只會在已定義持續時間過期後才終止。
 - 針對每個機群，定義逾時期間以佈建 Spot 執行個體。如果 Amazon EMR 無法佈建 Spot 容量，您可以終止叢集或切換到佈建的隨需容量。

執行個體機群選項

請使用下列準則以了解執行個體機群選項。

設定目標容量

指定您需要的核心機群和任務機群目標容量。在您執行此作業時，即會決定隨需執行個體的數量和 Amazon EMR 佈建的 Spot 執行個體。當您指定執行個體時，您將決定每個執行個體計入目標的數量。當隨需執行個體 (On-Demand Instance) 已完成佈建，它會計入隨需的目標。Spot 執行個體也是一樣。與核心和任務機群不同，主機群一律是一個執行個體。因此，針對主機群的目標容量一律為一個。

當您使用主控台時，EC2 執行個體類型的 vCPU 依預設會用做目標容量的計數。您可以變更此為 Generic units (一般單位)，然後為每個 EC2 執行個體類型指定計數。當您使用 AWS CLI 時，您將手動為每個執行個體類型指派一般單位。

Important

使用 AWS Management Console 選擇執行個體類型時，各執行個體類型顯示的 vCPU 數量為該執行個體類型的 YARN vcore 數量，而非該執行個體類型的 EC2 vCPU 數量。如需各執行個體類型的 vCPU 數量詳細資訊，請參閱 [Amazon EC2 執行個體類型](#)。

針對每個機群，您可指定最多 5 個 EC2 執行個體類型。Amazon EMR 會選擇這些 EC2 執行個體類型的任意組合，以滿足您的目標容量。由於 Amazon EMR 想要完全滿足目標容量，故可能發生超額。例如，如果有兩個未滿足的單位，而 Amazon EMR 只能以 5 個單位的計數佈建執行個體，該執行個體仍會佈建，這表示該目標容量已超過三個單位。

如果您降低目標容量以調整執行中叢集的大小，Amazon EMR 會嘗試完成應用程式任務，並終止執行個體以滿足新的目標。如需詳細資訊，請參閱 [於任務完成時終止 \(p. 303\)](#)。Amazon EMR 有 60 分鐘的逾時，以完成大小調整操作。在某些情況下，一個節點可能會在 60 分鐘之後仍有任務執行，而 Amazon EMR 會報告大小調整操作不成功，而且並未滿足新的目標。

Spot 執行個體選項

您可以為一個機群中的每 5 個執行個體類型指定 Maximum Spot price (最高 Spot 價格)。您可以依隨需價格的百分比或特定的金額來設定此價格。如果目前可用區域中的 Spot 價格低於您的最大 Spot 價格，則 Amazon EMR 會佈建 Spot 執行個體。您僅需支付該 Spot 價格。

您可以為機群中的 Spot 執行個體指定 Defined duration (定義的持續時間)。當 Spot 價格改變時，直到 Defined duration (定義的持續時間) 過期之前，Amazon EMR 都不會終止執行個體。已定義持續時間定價適用於您選取此選項時。如果您不指定已定義的持續時間、執行個體會在 Spot 價格超過 Spot 價格上限時即終止。如需詳細資訊，請參閱 [為您的 Spot 執行個體指定期間](#) 和 [Amazon EC2 Spot 執行個體定價](#)，以了解定義的持續時間定價。

對於每個機群，您還可以定義一個 Provisioning timeout (佈建逾時)。當叢集已建立而正在佈建容量，且無法依您的規格佈建足夠的 Spot 執行個體來滿足目標容量時，則會套用逾時。您會指定逾時期間和將採取的動作。您可以讓叢集終止或切換到佈建的隨需容量來滿足剩餘的 Spot 執行個體容量。當您選擇切換到隨需執行個體時，該剩餘的 Spot 執行個體容量，會在逾時過期後有效地新增到隨需執行個體的目標容量。

有關更多 Spot 執行個體的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Spot 執行個體](#)。

多個子網路 (可用區域) 選項

當您使用執行個體機群時，可以指定 VPC 中的多個 EC2 子網路，每個對應到不同的可用區域。如果您使用的是 EC2-Classic，您會明確指定可用區域。根據您的機群規格，Amazon EMR 會識別啟動執行個體的最佳可用區域。僅一律在一個可用區域中佈建執行個體。您可以選擇私有子網路或公有子網路，但您無法混合兩者，以及您指定的子網路必須位於相同的 VPC。

主節點組態

由於主執行個體機群是僅單一執行個體，它的組態與核心和任務執行個體機群稍有不同。您只需為主執行個體機群選取隨需或 Spot，因為它只包含一個執行個體。如果您使用主控台來建立執行個體機群，您選取之購買選項的目標容量會設為 1。如果您使用 AWS CLI，一律將 TargetSpotCapacity 或 TargetOnDemandCapacity 設定為 1。您仍可以為主執行個體機群選擇最多 5 個執行個體類型。不過，與核心和任務執行個體機群不同，其中 Amazon EMR 可能佈建不同類型的多個執行個體，Amazon EMR 會選取單一執行個體類型來為主執行個體機群進行佈建。

使用主控台來設定執行個體機群

若要使用執行個體機群建立叢集，請使用在 Amazon EMR 主控台的 Advanced options (進階選項) 組態。

使用主控台建立含執行個體機群的叢集

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.

2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)，輸入 Software Configuration (軟體組態) 選項，接著選擇 Next (下一步)。
4. 選擇 Instance fleets (執行個體機群)。
5. 對於 Network (網路)，輸入值。如果您選擇 Network (網路) 的 VPC，選擇單一 EC2 Subnet (EC2 子網路) 或按 CTRL + 按一下以選擇多個 EC2 子網路。您選擇的子網路必須為相同類型 (公有或私有)。如果您只選擇一個，您的叢集會在該子網路中啟動。如果您選擇群組，會在叢集啟動時從群組中選取最符合的子網路。

Note

您的帳戶和區域可能會提供您選項，讓您為 Network (網路) 選擇 Launch into EC2-Classic (啟動至 EC2-Classic)。如果您選擇該選項，請從 EC2 Availability Zones (EC2 可用區域) (而不是從 EC2 Subnets (EC2 子網路)) 選擇一或多個。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2](#) 和 [Amazon VPC](#)。

6. 在每個節點類型列的 Node type (節點類型) 下，如果您要變更執行個體機群的預設名稱，請按一下鉛筆圖示，然後輸入好記的名稱。如果想要移除 Task (任務) 執行個體機群，按一下 X 圖示。
7. 在 Target capacity (目標容量) 底下，根據下列指導方針選擇選項：
 - 選擇您要如何定義 Target capacity (目標容量)。如果您選擇 vCPU (vCPU)，會將每個 Fleet instance type (機群執行個體類型) 之 YARN vcores 數用做為其加權容量。如果您選擇 Generic units (一般單位)，您會為每個目標容量指定自訂數量，然後將自訂加權容量指派至每個執行個體類型。此用途的欄位會針對您在 Fleet instance type (機群執行個體類型) 下新增的每個執行個體顯示。
 - 對於 Master (主) 節點，選擇該執行個體是 On-demand (隨需) 或 Spot (Spot)。
 - 對於 Core (核心) 和 Task (任務) 節點，請輸入適用於 On-demand (隨需) 和 Spot (Spot) 的目標容量。Amazon EMR 會佈建您指定的 Fleet instance types (機群執行個體類型)，直到這些容量皆獲得履行。
8. 在每個 Node type (節點類型) 的 Fleet instance types (機群執行個體類型) 底下，根據下列指導方針選擇選項：
 - 選擇 Add/remove instance types to fleet (將執行個體類型新增/移除到叢集)，然後從清單選擇最多 5 個執行個體類型。Amazon EMR 在啟動叢集時，可以選擇佈建這些執行個體類型的混合。
 - 如果使用 Spot (Spot) 的 Target capacity (目標容量) 來設定節點類型，請選擇 Maximum Spot price (Spot 價格上限) 選項。您可以以 % of On-Demand (隨需定價的 %) 的形式輸入 Spot 價格上限，或者您可以輸入以 USD 為單位的 Dollars (\$) (美元 (USD)) 金額。

Tip

移至 Maximum Spot price (Spot 價格上限) 的資訊工具提示以了解目前區域中所有可用區域的 Spot 價格。最低 Spot 價格會以綠色顯示。您可以使用此資訊來通知 EC2 Subnet (EC2 子網路) 選項。

- 如果您選擇 Default units (預設單位) 做為 Target capacity (目標容量)，在 Each instance counts as (每個執行個體的計數為) 方塊中輸入您要指派給每個執行個體類型的加權容量。
- 若要在佈建執行個體類型時讓 EBS 磁碟區連接到其中時，按一下 EBS Storage (EBS 儲存) 旁的鉛筆，然後輸入 EBS 組態選項。
9. 如果您為 Spot (Spot) 建立了 Target capacity (目標容量)，請根據下列指導方針選擇 Advanced Spot options (進階 Spot 選項)：
 - Defined duration (定義的持續時間) - 如果將其保持為預設值 Not set (未設定)，在 Spot 價格上升超過 Spot 價格上限或在叢集終止時 Spot 執行個體即會終止。如果您設定值，Spot 執行個體在持續時間過期前都不會終止。

Important

如果您設定 Defined duration (定義的持續時間)，特殊定義的持續時間定價會適用。如需定價詳情，請參閱 [Amazon EC2 Spot 執行個體定價](#)。

- Provisioning timeout (佈建逾時)—使用這些設定，以控制 Amazon EMR 在無法從您指定的 Fleet instance types (機群執行個體類型) 中佈建 Spot 執行個體時會執行的動作。您在幾分鐘內輸入逾時時間，然後選擇是否要 Terminate the cluster (終止叢集) 或 Switch to provisioning On-Demand Instances (切換為佈建隨需執行個體)。如果您選擇切換到隨需執行個體，隨需執行個體的加權容量會計入 Spot 執行個體的目標容量，且 Amazon EMR 會在 Spot 執行個體目標容量履行前佈建隨需執行個體。

10. 請選擇 Next (下一步)，修改其他叢集設定，接著啟動叢集。

使用 CLI 來設定執行個體機群

- 若要建立和啟動叢集和執行個體叢集，請使用 `create-cluster` 命令以及 `--instance-fleet` 參數。
- 若要取得叢集中執行個體機群之組態的詳細資訊，請使用 `list-instance-fleets` 命令。
- 若要對執行個體機群的目標容量進行變更，請使用 `modify-instance-fleet` 命令。
- 若要將任務執行個體機群新增至尚未擁有任務執行個體機群的叢集中，請使用 `add-instance-fleet` 命令。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

使用執行個體機群組態來建立叢集

以下範例示範 `create-cluster` 命令，其中您可以結合多種選項。

Note

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請使用 `aws emr create-default-roles` 來建立這些設定檔，接著再使用 `create-cluster` 命令。

Example 範例：隨需執行個體主要、含單一執行個體類型的隨需核心、預設 VPC

```
aws emr create-cluster --release-label emr-5.3.1 --service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
--instance-fleets
  InstanceFleetType=MASTER,TargetOnDemandCapacity=1,InstanceTypeConfigs=['{InstanceType=m5.xlarge}']
  \
  InstanceFleetType=CORE,TargetOnDemandCapacity=1,InstanceTypeConfigs=['{InstanceType=m5.xlarge}']
```

Example 範例：Spot 主要、含單一執行個體類型的 Spot 核心、預設 VPC

```
aws emr create-cluster --release-label emr-5.3.1 --service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
--instance-fleets
  InstanceFleetType=MASTER,TargetSpotCapacity=1,InstanceTypeConfigs=['{InstanceType=m5.xlarge,BidPrice=0.5}']
  \
  InstanceFleetType=CORE,TargetSpotCapacity=1,InstanceTypeConfigs=['{InstanceType=m5.xlarge,BidPrice=0.5}']
```

Example 範例：隨需執行個體主要、含單一執行個體類型的混合核心、單一 EC2 子網路

```
aws emr create-cluster --release-label emr-5.3.1 --service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,SubnetIds=['subnet-ab12345c'] \
--instance-fleets
  InstanceFleetType=MASTER,TargetOnDemandCapacity=1,InstanceTypeConfigs=[{'InstanceType=m5.xlarge'}]
  \
  InstanceFleetType=CORE,TargetOnDemandCapacity=2,TargetSpotCapacity=6,InstanceTypeConfigs=[{'InstanceType=m5.xlarge'}]
```

Example 範例：隨需主要，含多個加權執行個體類型的 Spot 核心、定義的持續期間和 Spot 的逾時、EC2 子網路的範圍

```
aws emr create-cluster --release-label emr-5.3.1 --service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,SubnetIds=['subnet-ab12345c','subnet-de67890f'] \
--instance-fleets
  InstanceFleetType=MASTER,TargetOnDemandCapacity=1,InstanceTypeConfigs=[{'InstanceType=m5.xlarge'}]
  \
  InstanceFleetType=CORE,TargetSpotCapacity=11,InstanceTypeConfigs=[{'InstanceType=m5.xlarge,BidPrice=0.5',
  \
  '{InstanceType=m4.2xlarge,BidPrice=0.9,WeightedCapacity=5'}],\
  LaunchSpecifications={SpotSpecification={'TimeoutDurationMinutes=120,TimeoutAction=SWITCH_TO_ON_DEMAND'}}
```

Example 範例：隨需主要，含多個加權執行個體類型的混合核心和任務、定義的持續期間和核心 Spot 執行個體的逾時、EC2 子網路的範圍

```
aws emr create-cluster --release-label emr-5.3.1 --service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,SubnetIds=['subnet-ab12345c','subnet-de67890f'] \
--instance-fleets
  InstanceFleetType=MASTER,TargetOnDemandCapacity=1,InstanceTypeConfigs=[{'InstanceType=m5.xlarge'}]
  \
  InstanceFleetType=CORE,TargetOnDemandCapacity=8,TargetSpotCapacity=6,\
  InstanceTypeConfigs=[{'InstanceType=m5.xlarge,BidPrice=0.5,WeightedCapacity=3'},\
  '{InstanceType=m4.2xlarge,BidPrice=0.9,WeightedCapacity=5'}],\
  LaunchSpecifications={SpotSpecification={'TimeoutDurationMinutes=120,TimeoutAction=SWITCH_TO_ON_DEMAND'}}
  \
  InstanceFleetType=TASK,TargetOnDemandCapacity=3,TargetSpotCapacity=3,\
  InstanceTypeConfigs=[{'InstanceType=m5.xlarge,BidPrice=0.5,WeightedCapacity=3'}]
```

Example 範例：Spot 主要、無核心或任務、EBS 組態、預設 VPC

```
aws emr create-cluster --release-label emr 5.3.1 -service-role EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
--instance-fleets InstanceFleetType=MASTER,TargetSpotCapacity=1,\
LaunchSpecifications={SpotSpecification={'TimeoutDurationMinutes=60,TimeoutAction=TERMINATE_CLUSTER'}},\
  \
  InstanceTypeConfigs=[{'InstanceType=m5.xlarge,BidPrice=0.5, \
  EbsConfiguration={EbsOptimized=true,EbsBlockDeviceConfigs=[{VolumeSpecification={VolumeType=gp2,
  \
  SizeIn GB=100},{VolumeSpecification={VolumeType=io1,SizeInGB=100,Iop
  s=100},VolumesPerInstance=4}]}}]'
```

Example 使用 JSON 組態檔案

您可以在 JSON 檔案中設定執行個體機群參數，然後參考 JSON 檔案做為執行個體機群的唯一參數。例如，以下命令會參考 JSON 組態檔案 (my-fleet-config.json)：

```
aws emr create-cluster --release-label emr-5.2.0 --servicerole EMR_DefaultRole \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
--instance-fleets file://my-fleet-config.json
```

my-fleet-config.json 會指定主要、核心和任務執行個體機群，如下所示。核心執行個體機群以隨需的百分比形式使用 Spot 價格上限 (BidPrice)，同時任務和主要執行個體機群以 USD 的字串形式使用 Spot 價格上限 (BidPriceAsPercentageofOnDemandPrice)。

```
[  
  {  
    "Name": "Masterfleet",  
    "InstanceFleetType": "MASTER",  
    "TargetSpotCapacity": 1,  
    "LaunchSpecifications": {  
      "SpotSpecification": {  
        "TimeoutDurationMinutes": 120,  
        "TimeoutAction": "SWITCH_TO_ON_DEMAND"  
      }  
    },  
    "InstanceTypeConfigs": [  
      {  
        "InstanceType": "m5.xlarge",  
        "BidPrice": "0.89"  
      }  
    ]  
  },  
  {  
    "Name": "Corefleet",  
    "InstanceFleetType": "CORE",  
    "TargetSpotCapacity": 1,  
    "LaunchSpecifications": {  
      "SpotSpecification": {  
        "TimeoutDurationMinutes": 120,  
        "TimeoutAction": "TERMINATE_CLUSTER"  
      }  
    },  
    "InstanceTypeConfigs": [  
      {  
        "InstanceType": "m5.xlarge",  
        "BidPriceAsPercentageOfOnDemandPrice": 100  
      }  
    ]  
  },  
  {  
    "Name": "Taskfleet",  
    "InstanceFleetType": "TASK",  
    "TargetSpotCapacity": 1,  
    "LaunchSpecifications": {  
      "SpotSpecification": {  
        "TimeoutDurationMinutes": 120,  
        "TimeoutAction": "TERMINATE_CLUSTER"  
      }  
    },  
    "InstanceTypeConfigs": [  
      {  
        "InstanceType": "m5.xlarge",  
        "BidPrice": "0.89"  
      }  
    ]  
  }]
```

取得叢集中執行個體機群的組態詳細資訊

使用 `list-instance-fleets` 命令來取得叢集中執行個體機群之組態的詳細資訊。此命令會將叢集 ID 做為輸入。以下範例會針對包含主要任務執行個體群組和核心任務執行個體群組的叢集示範命令及其輸出。如需完整的回應語法，請參閱 Amazon EMR API Reference 中的 [ListInstanceFleets](#)。

```
list-instance-fleets --cluster-id 'j-12ABCDEFHI34JK'
```

```
{  
    "InstanceFleets": [  
        {  
            "Status": {  
                "Timeline": {  
                    "ReadyDateTime": 1488759094.637,  
                    "CreationDateTime": 1488758719.811  
                },  
                "State": "RUNNING",  
                "StateChangeReason": {  
                    "Message": ""  
                }  
            },  
            "ProvisionedSpotCapacity": 6,  
            "Name": "CORE",  
            "InstanceFleetType": "CORE",  
            "LaunchSpecifications": {  
                "SpotSpecification": {  
                    "TimeoutDurationMinutes": 60,  
                    "TimeoutAction": "TERMINATE_CLUSTER"  
                }  
            },  
            "ProvisionedOnDemandCapacity": 2,  
            "InstanceTypeSpecifications": [  
                {  
                    "BidPrice": "0.5",  
                    "InstanceType": "m5.xlarge",  
                    "WeightedCapacity": 2  
                }  
            ],  
            "Id": "if-1ABC2DEFGHIJ3"  
        },  
        {  
            "Status": {  
                "Timeline": {  
                    "ReadyDateTime": 1488759058.598,  
                    "CreationDateTime": 1488758719.811  
                },  
                "State": "RUNNING",  
                "StateChangeReason": {  
                    "Message": ""  
                }  
            },  
            "ProvisionedSpotCapacity": 0,  
            "Name": "MASTER",  
            "InstanceFleetType": "MASTER",  
            "ProvisionedOnDemandCapacity": 1,  
            "InstanceTypeSpecifications": [  
                {  
                    "BidPriceAsPercentageOfOnDemandPrice": 100.0,  
                    "InstanceType": "m5.xlarge",  
                    "WeightedCapacity": 1  
                }  
            ]  
        }  
    ]  
}
```

```
        ],
        "Id": "if-2ABC4DEFGHIJ4"
    }
}
```

修改執行個體機群的目標容量

使用 `modify-instance-fleet` 命令來指定執行個體機群的新目標容量。您必須指定叢集 ID 和執行個體機群 ID。使用 `list-instance-fleets` 命令來擷取執行個體機群 ID。

```
aws emr modify-instance-fleet --cluster-id 'j-12ABCDEFHGI34JK' /
--instance-fleet
    InstanceFleetId='if-2ABC4DEFGHIJ4',TargetOnDemandCapacity=1,TargetSpotCapacity=1
```

將任務執行個體機群新增至叢集

如果叢集僅有主要和核心執行個體機群，您可以使用 `add-instance-fleet` 命令來新增任務執行個體機群。您只能使用此命令來新增任務執行個體機群。

```
aws emr add-instance-fleet --cluster-id 'j-12ABCDEFHGI34JK' --instance-fleet
    InstanceFleetType=TASK,TargetSpotCapacity=1,/
    LaunchSpecifications={SpotSpecification='{TimeoutDurationMinutes=20,TimeoutAction=TERMINATE_CLUSTER}'},
    InstanceTypeConfigs=['{InstanceType=m5.xlarge,BidPrice=0.5}']
```

設定統一執行個體群組

使用執行個體群組組態，每個節點類型（主要、核心或任務）包含相同的執行個體類型和適用於以下執行個體的相同購買選項：隨需或 Spot。您建立執行個體群組時，您會指定這些設定。這些設定稍後無法變更。不過，您可以將相同類型的執行個體和購買選項新增到核心和任務執行個體群組。您也可以移除執行個體。

若要在叢集建立後新增不同的執行個體類型，您可以新增額外的任務執行個體群組。您可以選擇適用於每個執行個體群組的不同執行個體類型與購買選項。如需更多詳細資訊，請參閱 [調整叢集資源規模 \(p. 290\)](#)。

這個區段涵蓋建立含統一執行個體群組的叢集。如需透過手動新增或移除執行個體或透過自動擴展來修改現有執行個體群組的更多資訊，請參閱 [管理叢集 \(p. 241\)](#)。

使用主控台來設定統一執行個體群組

下列程序涵蓋當您建立叢集時的 Advanced options (進階選項)。使用 Quick options (快速選項) 也會建立含執行個體群組組態的叢集。如需有關使用 Quick Options (快速選項) 的詳細資訊，請參閱入門教學課程。

使用主控台建立含統一執行個體群組的叢集

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)，輸入 Software Configuration (軟體組態) 選項，接著選擇 Next (下一步)。
4. 在 Hardware Configuration (硬體組態) 畫面中，將 Uniform instance groups (統一執行個體群組) 保持為選取。

- 選擇 Network (網路)，然後為您的叢集選擇 EC2 Subnet (EC2 子網路)。您選擇的子網路會關聯至可用性群組，這會與每個子網路一同列出。如需更多詳細資訊，請參閱 [設定網路 \(p. 95\)](#)。

Note

您的帳戶和區域可能會提供您選項，讓您為 Network (網路) 選擇 Launch into EC2-Classic (啟動至 EC2-Classic)。如果您選擇該選項，請選擇 EC2 Availability Zone (EC2 可用區域) (而不是 EC2 Subnet (EC2 子網路))。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2 和 Amazon VPC](#)。

- 在每個 Node type (節點類型) 資料列中：

- 在 Node type (節點類型) 下，如果想要變更執行個體群組的預設名稱，請按一下鉛筆圖示，然後輸入好記的名稱。如果想要移除 Task (任務) 執行個體群組，按一下 X 圖示。選擇 Add task instance group (新增任務執行個體群組) 新增額外的 Task (任務) 執行個體群組。
- 在 Instance type (執行個體類型) 中，按一下鉛筆圖示，然後選擇您想要用在該節點類型的執行個體類型。

Important

使用 AWS Management Console 選擇執行個體類型時，各執行個體類型顯示的 vCPU 數量為該執行個體類型的 YARN vcore 數量，而非該執行個體類型的 EC2 vCPU 數量。如需各執行個體類型的 vCPU 數量詳細資訊，請參閱 [Amazon EC2 執行個體類型](#)。

- 在 Instance type (執行個體類型) 中，針對 Configurations (組態) 按一下鉛筆圖示，然後編輯每個執行個體群組的應用程式組態。
- 在 Instance count (執行個體計數) 下，為每個節點類型輸入要使用的執行個體數量。
- 在 Purchasing option (購買選項) 下，請選擇 On-demand (隨需) 或 Spot (Spot)。如果您選擇 Spot (Spot)，則需選擇 Spot 執行個體的最高價格選項。在預設情況下，Use on-demand as max price (使用隨需做為最高價格) 會被選取。您可以選擇 Set max \$/hr (設定最高 USD/hr)，然後輸入您的最高價。您選擇的 EC2 Subnet (EC2 子網路) 可用區域低於 Maximum Spot price (最大 Spot 價格)。

Tip

將滑鼠移至 Spot (Spot) 的資訊工具提示以查看目前區域中可用區域的目前 Spot 價格。最低 Spot 價格會以綠色顯示。建議您使用此資訊來變更 EC2 Subnet (EC2 子網路) 選項。

- 在 Auto Scaling for Core and Task node types (核心和任務節點類型的 Auto Scaling)，選擇鉛筆圖示，然後設定自動擴展選項。如需更多詳細資訊，請參閱 [於 Amazon EMR 使用自動調整規模 \(p. 291\)](#)。

- 視需要選擇 Add task instance group (新增任務執行個體群組)，並依前一步驟所述進行設定。
- 請選擇 Next (下一步)，修改其他叢集設定，接著啟動叢集。

使用 AWS CLI 建立含統一執行個體群組的叢集

若要使用 AWS CLI 指定叢集的執行個體群組設定，請使用 `create-cluster` 命令和 `--instance-groups` 參數。Amazon EMR 會假設使用隨需購買選項，除非您為執行個體群組指定 `BidPrice` 引數。如需 `create-cluster` 命令的範例，該命令會啟動含隨需執行個體的統一執行個體群組與各種叢集選項，在命令列中輸入 `aws emr create-cluster help` 或請參閱 AWS CLI Command Reference 中的 `create-cluster`。

您可以使用 AWS CLI 來在使用 Spot 執行個體的叢集中建立統一執行個體群組。提供的 Spot 價格取決於可用區域。當您使用 CLI 或 API，您可以透過 `AvailabilityZone` 引數 (如果您使用的是 EC2-classic 網路) 或 `--ec2-attributes` 參數的 `SubnetID` 引數來指定可用區域。您選擇的可用區域或子網路會套用至叢集，因此會將其用於所有執行個體群組。如果您不是明確指定可用區域或子網路，Amazon EMR 會在啟動叢集時選取 Spot 價格最低的可用區域。

以下範例示範 `create-cluster` 命令，該命令會建立主要、核心和兩個任務執行個體群組，而這些群組都使用 Spot 執行個體。以 EC2 金鑰對名稱取代 `myKey`。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "MySpotCluster" --release-label emr-5.28.0 \
--use-default-roles --ec2-attributes KeyName=myKey \
--instance-groups
  InstanceGroupType=MASTER,InstanceType=m5.xlarge,InstanceCount=1,BidPrice=0.25 \
  InstanceGroupType=CORE,InstanceType=m5.xlarge,InstanceCount=2,BidPrice=0.03 \
  InstanceGroupType=TASK,InstanceType=m5.xlarge,InstanceCount=4,BidPrice=0.03 \
  InstanceGroupType=TASK,InstanceType=m5.xlarge,InstanceCount=2,BidPrice=0.04
```

使用 Java 軟體開發套件來建立執行個體群組

您會將 `InstanceGroupConfig` 物件個體化，該物件會指定叢集的執行個體群組組態。若要使用 Spot 執行個體，您會針對 `withBidPrice` 物件設定 `withMarket` 和 `InstanceGroupConfig` 屬性。以下程式碼示範如何定義執行 Spot 執行個體的主要、核心和任務執行個體群組。

```
InstanceGroupConfig instanceGroupConfigMaster = new InstanceGroupConfig()
    .withInstanceCount(1)
    .withInstanceRole("MASTER")
    .withInstanceType("m4.large")
    .withMarket("SPOT")
    .withBidPrice("0.25");

InstanceGroupConfig instanceGroupConfigCore = new InstanceGroupConfig()
    .withInstanceCount(4)
    .withInstanceRole("CORE")
    .withInstanceType("m4.large")
    .withMarket("SPOT")
    .withBidPrice("0.03");

InstanceGroupConfig instanceGroupConfigTask = new InstanceGroupConfig()
    .withInstanceCount(2)
    .withInstanceRole("TASK")
    .withInstanceType("m4.large")
    .withMarket("SPOT")
    .withBidPrice("0.10");
```

叢集組態指南和最佳實務

使用此區段中的指導方針，以協助您判斷執行個體類型、購買選項，以及在 EMR 叢集中每個節點類型要佈建的儲存量。

我應該使用哪一種執行個體類型？

將 EC2 執行個體新增到叢集的方法有很多，這取決於您使用的是執行個體群組組態或叢集的執行個體機群組態。

- 執行個體群組
 - 手動將相同類型的執行個體新增到現有核心和任務執行個體群組。
 - 手動新增任務執行個體群組，這些群組可以使用不同的執行個體類型。
 - 在 Amazon EMR 中為執行個體群組設定自動擴展，根據您指定的 Amazon CloudWatch 指標值來自動新增和移除執行個體。如需更多詳細資訊，請參閱 [調整叢集資源規模 \(p. 290\)](#)。
- 執行個體機群

- 新增單一任務執行個體機群。
- 針對現有核心和任務執行個體機群，變更隨需和 Spot 執行個體的目標容量。如需更多詳細資訊，請參閱 [設定執行個體機群 \(p. 105\)](#)。

計劃叢集執行個體的其中一種方法即是使用代表範例資料集來執行測試叢集並監控叢集中節點的使用率。如需更多詳細資訊，請參閱 [查看和監控叢集 \(p. 241\)](#)。另一個方式是計算您考慮使用之執行個體的容量，並再將該值與您的資料大小進行比對。

一般而言，主節點類型，它會將任務，不需要大量的 EC2 執行個體的處理能力；適用於 EC2 執行個體的核心節點類型，處理任務，並將資料存放在 HDFS，需要兩個處理能力和儲存容量，適用於 EC2 執行個體的任務節點類型，也不會存放資料，只需處理能力。如需有關可用 EC2 執行個體及其組態的詳細資訊，請參閱指導方針 [設定 EC2 執行個體 \(p. 90\)](#)。

以下準則適用於大部分 Amazon EMR 叢集。

- 主節點不會有大量的運算要求。對於大多數 50 個或更少節點的叢集，請考慮使用 m5.xlarge 執行個體。對於超過 50 個節點的叢集，請考慮使用 m4.xlarge。
- 核心和任務節點的運算需求取決於應用程式所執行的處理類型。您可以在 m5.xlarge 執行個體類型上執行許多任務，其會根據 CPU、磁碟空間和輸入/輸出提供平衡和效能。如果您的應用程式有會造成延遲（例如 Web 爬取以收集資料）的外部依存項目，您可以在 t2.medium 執行個體上執行叢集以降低成本，同時執行個體會等待依存項目完成。對於提升效能，請考慮對核心和任務節點使用 m4.xlarge 執行個體來執行叢集。如果叢集的不同階段有不同的容量需求，您可以先從小量的核心節點開始，然後增加或降低任務節點數以滿足任務流程的各種容量需求。
- 大多數 Amazon EMR 叢集可以在標準 EC2 執行個體類型（例如 m5.xlarge 和 m4.xlarge）上執行。運算密集型叢集可能受惠於在 CPU 密集型執行個體上（其在擁有的 CPU 比例大於 RAM）。資料庫和記憶體快取應用程式可能受益於在記憶體密集型執行個體上執行。網路密集型和 CPU 密集型應用程式（如剖析、NLP 和機器學習）可能會受益於在叢集運算執行個體上執行，其會提供較高比例的 CPU 資源與更高的網路效能。
- 您可以處理的資料量取決於核心節點的容量與處理期間做為輸入和輸出之資料的大小。中繼的輸入和輸出資料集在處理期間皆位於叢集中。
- 在預設情況下，您在單一 AWS 帳戶上可以執行的 EC2 執行個體總數為 20 個。這表示您在叢集中可以擁有的節點總數為 20。如需如何為帳戶要求提高限制的詳細資訊，請參閱 [AWS 限制](#)。

我應何時使用 Spot 執行個體？

在 Amazon EMR 中啟動叢集時，您可以選擇在 Spot 執行個體上啟動主要、核心或任務執行個體。由於每種執行個體群組在叢集中扮演不同的角色，因此會在 Spot 執行個體上啟動每個節點類型。叢集執行時，您無法變更執行個體的購買選項。若要將隨需執行個體變更為 Spot 執行個體（或反之亦然），對於主節點和核心節點，您必須終止叢集並啟動新的叢集。對於任務節點，您可以啟動新的任務執行個體群組或執行個體機群，並移除舊的任務執行個體群組或執行個體機群。

主題

- [Amazon EMR 設定可避免由於任務節點 Spot 執行個體終止而造成的任務失敗 \(p. 115\)](#)
- [Spot 執行個體上的主節點 \(p. 116\)](#)
- [Spot 執行個體上的核心節點 \(p. 116\)](#)
- [Spot 執行個體上的任務節點 \(p. 116\)](#)
- [應用程式案例的執行個體組態 \(p. 117\)](#)

Amazon EMR 設定可避免由於任務節點 Spot 執行個體終止而造成的任務失敗

因為 Spot 執行個體經常用來執行任務節點，Amazon EMR 具有用於排定 YARN 工作的預設功能，使得當 Spot 執行個體上執行的任務節點終止時，執行中的工作不會失敗。Amazon EMR 透過允許應用程式主控程

序只在核心節點上執行來達成此目的。應用程式主控程序會控制執行中工作，並且需要在工作的生命週期中保持作用中。

Amazon EMR 發行版本 5.19.0 和更新版本使用內建的 **YARN 節點標籤** 功能來達成此目的。(較早版本使用的是程式碼修補程式。) `yarn-site` 和 `capacity-scheduler` 組態分類中的屬性會依設設定，使得 YARN 功能排程器和公平排程器會利用節點標籤。Amazon EMR 會自動將核心節點標記 CORE 標籤，並且設定屬性，使得應用程式主控只會排程在具有 CORE 標籤的節點上執行。在 `yarn-site` 和 `capacity-scheduler` 組態分類中手動修改相關屬性，或是直接在相關聯的 XML 檔案中修改，可能會破壞此特性或修改此功能。

Amazon EMR 預設會設定下列屬性和值。設定這些屬性時請務必小心。

- 所有節點上的 `yarn-site` (`yarn-site.xml`)
 - `yarn.node-labels.enabled: true`
 - `yarn.node-labels.am.default-node-label-expression: 'CORE'`
 - `yarn.node-labels.fs-store.root-dir: '/apps/yarn/nodelabels'`
 - `yarn.node-labels.configuration-type: 'distributed'`
- 主節點和核心節點上的 `yarn-site` (`yarn-site.xml`)
 - `yarn.nodemanager.node-labels.provider: 'config'`
 - `yarn.nodemanager.node-labels.provider.configured-node-partition: 'CORE'`
- 所有節點上的 `capacity-scheduler` (`capacity-scheduler.xml`)
 - `yarn.scheduler.capacity.root.accessible-node-labels: '*'`
 - `yarn.scheduler.capacity.root.accessible-node-labels.CORE.capacity: 100`
 - `yarn.scheduler.capacity.root.default.accessible-node-labels: '*'`
 - `yarn.scheduler.capacity.root.default.accessible-node-labels.CORE.capacity: 100`

Spot 執行個體上的主節點

主節點會控制和引導叢集。主節點終止時，叢集便會結束，因此如果您執行的叢集可接受突然的終止時，您應僅以 Spot 執行個體的形式啟動主節點。如果您測試的是新應用程式就可能適用此狀況，讓叢集定期將資料保存在外部存放區 (例如 Amazon S3) 或執行的是成本較確保叢集完成還重要的叢集。

當您以 Spot 執行個體啟動主要執行個體群組，叢集在 Spot 執行個體要求履行前都不會啟動。這是在選取 Spot 價格上限時需考量的因素。

您只能在啟動叢集時新增 Spot 執行個體主要結點。您無法從執行中叢集新增或移除主節點。

一般而言，如果您以 Spot 執行個體的形式執行整個叢集 (所有執行個體群組)，您只會以 Spot 執行個體的形式執行主節點。

Spot 執行個體上的核心節點

核心節點會使用 HDFS 來處理資料和存放資訊。終止核心執行個體會導致資料遺失的風險。因此，只有在能夠承受部分 HDFS 資料遺失的情況下，才應該在 Spot 執行個體上執行核心節點。

以 Spot 執行個體的形式啟動核心執行個體群組時，Amazon EMR 在啟動執行個體群組前，會等待直到其可以佈建所有要求的核心執行個體。換句話說，如果您請求 6 個 Amazon EC2 節點，而且只有 5 個執行個體適用於或低於您的最大 Spot 價格，執行個體群組不會啟動。Amazon EMR 會持續等候到所有 6 個 Amazon EC2 節點可供使用或您終止叢集為止。您可以變更核心執行個體群組中的 Spot 執行個體數量，以便增加執行中叢集的容量。如需使用執行個體群組以及 Spot 執行個體如何使用執行個體機群的詳細資訊，請參閱[the section called “設定執行個體機群或執行個體群組” \(p. 104\)](#)。

Spot 執行個體上的任務節點

任務節點會處理資料，但不會在 HDFS 中保存持久性資料。如果因為 Spot 價格已超出您的 Spot 價格上限，而導致任務節點終止，則資料不會遺失，且對您叢集的影響可降到最低。

當您以 Spot 執行個體的形式啟動一或多個任務執行個體群組，Amazon EMR 會使用您的 Spot 價格上限來盡可能佈建任務節點。這表示如果您請求的任務執行個體群組有六個節點，而且只有 5 個執行個體適用於或低於您的最大 Spot 價格，Amazon EMR 啟動有 5 個節點的執行個體群組，並在隨後新增第六個節點。

以 Spot 執行個體的形式啟動任務執行個體群組是一種策略，可讓您擴展叢集容量，並同時將成本降到最低。如果您以隨需執行個體的形式啟動主節點和核心執行個體群組，即可保證其容量足以執行叢集。您可以視需要將任務執行個體新增到您的任務執行個體群組，來處理尖峰流量或加快資料處理的速度。

您可以使用主控台、AWS CLI 或 API 來新增或移除任務節點。您也可以新增額外的任務群組，但您無法在建立任務群組之後將其移除。

應用程式案例的執行個體組態

下表是節點類型購買選項和設定的快速參考，這些選項和設定通常適用於各種應用程式案例。選擇連結檢視有關每個案例類型的詳細資訊。

應用程式案例	主節點購買選項	核心節點購買選項	任務節點購買選項
長時間執行的叢集和資料倉儲 (p. 117)	隨需	隨需執行個體或執行個體機群的混合	Spot 或執行個體機群的混合
成本導向工作負載 (p. 117)	Spot	Spot	Spot
資料關鍵工作負載 (p. 117)	隨需	隨需	Spot 或執行個體機群的混合
應用程式測試 (p. 117)	Spot	Spot	Spot

在某些情況下，Spot 執行個體 (Spot Instance) 對於執行 Amazon EMR 叢集很有用。

長時間執行的叢集和資料倉儲

如果您執行的持久性 Amazon EMR 叢集在運算容量具有可預測變異 (例如資料倉儲)，您可以使用 Spot 執行個體以較低的成本來處理峰值需求。您可以隨需執行個體的形式啟動主要和核心執行個體群組來處理正常的容量，並以 Spot 執行個體的形式啟動任務執行個體群組來處理您的最高負載需求。

成本導向工作負載

如果您執行的是暫時性叢集，其中降低成本較完成時間更為重要，以及遺失部分工作是可接受的，您可以Spot 執行個體的形式執行整個叢集 (主要、核心和任務執行個體群組)，來獲得節省最多成本的好處。

資料關鍵工作負載

如果您執行的是叢集，其中降低成本較完成時間更為重要，但不可遺失部分工作時，以隨需方式來執行主要和核心執行個體群組，並透過 Spot 執行個體的一或多個任務執行個體群組補充。以隨需的形式執行主要和核心執行個體群組來確保您的資料可保存在 HDFS 中且叢集會受因 Spot 市場波動而終止的保護，同時因以 Spot 執行個體的形式執行任務執行個體群組而節省成本。

應用程式測試

當您測試新的應用程式，以便準備讓其在生產環境中啟動，您可透過 Spot 執行個體的形式執行整個叢集 (主要、核心和任務執行個體群組) 來降低測試成本。

計算叢集的必要 HDFS 容量

您叢集可用的 HDFS 儲存量取決於這些因素：

- 用於核心節點的 EC2 執行個體數。

- 會針對執行個體類型使用 EC2 執行個體存放區的容量。如需執行個體存放區磁碟區的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2 執行個體存放區](#)。
- 連接到核心節點之 EBS 磁碟區的數量和大小。
- 複寫係數，其會針對類似 RAID 的備援計算在 HDFS 上每個資料區塊的存放方式。根據預設，對 10 個或多個核心節點的叢集複寫係數是三，對於 4-9 個核心節點的叢集是二，以及三個或較少的節點的叢集是一。

若要對每個核心節點計算叢集的 HDFS 容量，將執行個體存放區磁碟區容量新增至 EBS 儲存容量 (如果有使用的話)。將結果乘以核心節點數，然後根據核心節點數將總數除以複寫係數。例如，含類型為 i2.xlarge 之 10 個核心節點叢集，其中有 800 GB 執行個體儲存體，而沒有任何連接的 EBS 磁碟區，總共會有大約 2,666 GB 可用於 HDFS (10 個節點 \times 800 GB \div 3 複寫係數)。

如果計算 HDFS 容量值小於您的資料，您可以透過下列方式增加 HDFS 儲存量：

- 建立含額外 EBS 磁碟區的叢集或新增含對現有叢集有連接 EBS 磁碟區的執行個體群組
- 新增更多核心節點
- 選擇含更多儲存容量的 EC2 執行個體類型
- 使用資料壓縮
- 變更 Hadoop 組態設定以減少複寫係數

請務必小心減少複寫因素，因為其會減少 HDFS 資料備援，以及您從遺失或毀損的 HDFS 區塊中復原的叢集能力。

設定叢集記錄和除錯

在您規劃叢集時，要決定的一件事便是您要提供多少除錯支援。在您第一次開發您的資料處理應用程式時，我們建議在叢集上測試該應用程式，處理小型但具有代表性的資料子集。當您執行此操作時，您可能會想要利用所有 Amazon EMR 提供的除錯工具 (例如存檔日誌檔案) 紿 Amazon S3。

當您完成開發，並將您的資料處理應用程式投入全面生產時，您可以選擇縮減除錯。如此一來可以節省在 Amazon S3 中儲存日誌檔案封存的成本，並減少叢集上的處理負載，因為它不再需要將狀態寫入 Amazon S3。當然，做為取捨，如果出現問題，您可以用來調查問題的工具便少了些。

預設日誌檔案

在預設情況下，每個叢集會在主節點上寫入日誌檔。這些會寫入至 `/mnt/var/log/` 目錄。您可以使用 SSH 來連接到主節點以存取它們，如 [使用 SSH 連接至主節點 \(p. 277\)](#) 所述。由於這些日誌都存在於主節點上，所以當節點終止時 (無論是叢集關閉還是發生錯誤)，這些日誌檔案都不再能使用。

您不需要啟用任何功能以在主節點上寫入日誌檔案。這是 Amazon EMR 與 Hadoop 預設的行為。

一個叢集會產生多種類型的日誌檔，包括：

- Step logs (步驟日誌) — 這些日誌是由 Amazon EMR 服務所產生，且包含有關叢集和每個步驟結果的資訊。該日誌檔案存放於主節點上的 `/mnt/var/log/hadoop/steps/` 目錄中。每個步驟都將其結果記錄在一個單獨編號的子目錄中：第一個步驟為 `/mnt/var/log/hadoop/steps/s-stepId1/`，第二個步驟為 `/mnt/var/log/hadoop/steps/s-stepId2/`，以此類推。13 個字元的步驟識別符 (例如 stepId1、stepId2) 對叢集來說是唯一的。
- Hadoop and YARN component logs (Hadoop 與 YARN 元件日誌) — 例如，與 Apache YARN 和 MapReduce 關聯的元件日誌，是包含在 `/mnt/var/log` 的單獨資料夾中。`/mnt/var/log` 下的 Hadoop 元件日誌檔案位置如下：`hadoop-hdfs`, `hadoop-mapreduce`, `hadoop-httpsfs` 與 `hadoop-yarn`. `hadoop-state-pusher` 目錄用於 Hadoop 狀態推送器程序的輸出。

- Bootstrap action logs (引導操作日誌) — 如果您的任務使用引導操作，這些動作的結果都會加以記錄。日誌檔會存放在主節點上的 /mnt/var/log/bootstrap-actions/。每個引導操作都將其結果記錄在一個單獨編號的子目錄中：第一個引導操做為 /mnt/var/log/bootstrap-actions/1/，第二個引導操做為 /mnt/var/log/bootstrap-actions/2/，以此類推。
- Instance state logs (執行個體狀態日誌) — 這些日誌提供有關節點的 CPU、記憶體狀態和廢棄項目收集器執行緒資訊。該日誌檔案存放於主節點上的 /mnt/var/log/instance-state/ 中。

封存日誌檔到 Amazon S3

Note

您目前不能以 `yarn logs` 公用程式使用日誌彙整到 Amazon S3。

您可以設定叢集，以將存放在主節點上的日誌檔案定期封存到 Amazon S3。這可確保日誌檔案在叢集終止（無論是透過正常關閉還是由於錯誤關閉）後仍可使用。Amazon EMR 會以 5 分鐘為間隔將日誌檔封存到 Amazon S3。

要將日誌檔封存到 Amazon S3，當您啟動叢集時便必須啟用此功能。您可以使用主控台、CLI 或 API 來執行這項作業。在預設情況下，使用主控台啟動的叢集便已啟用了日誌封存。對於使用 CLI 或 API 啟動的叢集，則必須手動啟用對 Amazon S3 的記錄。

使用主控台封存日誌檔至 Amazon S3

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)。
3. 選擇 Go to advanced options (前往進階選項)。
4. 在 Cluster Configuration (叢集組態) 部分，在 Logging (紀錄) 欄位中，接受預設選項：Enabled (啟用)。這可判斷 Amazon EMR 是否要擷取詳細日誌資料給 Amazon S3。您只能在叢集建立時予以設定。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。
5. 在 Log folder S3 location (日誌資料夾 S3 位置) 欄位中，鍵入 (或瀏覽到) Amazon S3 路徑來存放您的日誌。您也可以允許主控台為您產生 Amazon S3 路徑。如果您鍵入的資料夾名稱並不存在於儲存貯體，則會建立該資料夾。

當此值已設定，Amazon EMR 會將叢集中的 EC2 執行個體日誌檔案複製到 Amazon S3。這可避免日誌檔案在叢集結束且託管叢集的 EC2 執行個體終止時遺失。這些日誌對於故障排除非常實用。

如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

6. 按照 [規劃和設定叢集 \(p. 31\)](#) 中所述繼續建立叢集。

使用 AWS CLI 封存日誌檔至 Amazon S3

若要使用 AWS CLI 封存日誌檔至 Amazon S3，使用 `--log-uri` 參數鍵入 `create-cluster` 命令並指定 Amazon S3 日誌路徑。

- 若要紀錄檔案至 Amazon S3，鍵入下列命令，並以您的 EC2 金鑰對名稱來取代 `myKey`。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 --log-uri s3://mybucket/logs/ --applications Name=Hadoop Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge --instance-count 3
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用 AWS CLI 在 Amazon S3 中彙總日誌

Note

您目前不能以 `yarn logs` 公用程式使用日誌彙整。您僅能使用此程序支援的彙總。

日誌彙總 (Hadoop 2.x) 會將來自個別應用程式的所有容器日誌編譯為單一檔案。若要使用 Amazon S3 啟用日誌彙總到 AWS CLI，您要在叢集啟動時使用引導操作來啟用日誌彙總，並指定存放日誌的儲存貯體。

- **Important**

此設定在過去的 EMR 4.x 版本中不起作用。如果您想設定此選項，請使用大於 4.3.0 的版本。

若要啟用日誌彙整建立以下組態檔案，`myConfig.json`，其中包含下列項目：

```
[  
  {  
    "Classification": "yarn-site",  
    "Properties": {  
      "yarn.log-aggregation-enable": "true",  
      "yarn.log-aggregation.retain-seconds": "-1",  
      "yarn.nodemanager.remote-app-log-dir": "s3://mybucket/logs"  
    }  
  }  
]
```

輸入下列命令，然後使用 EC2 金鑰對的名稱來取代 `myKey`。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.5.0 --applications Name=Hadoop --use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge --instance-count 3 --configurations file://./myConfig.json
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

啟用除錯工具

除錯工具可讓您從 EMR 主控台更輕鬆地瀏覽日誌檔案。如需更多詳細資訊，請參閱 [在除錯工具中檢視日誌檔 \(p. 253\)](#)。在叢集上啟用除錯時，Amazon EMR 會將日誌檔案封存到 Amazon S3，然後對這些檔案編制索引。然後，您可以使用主控台以直覺的方式瀏覽叢集的步驟、工作、任務和任務嘗試日誌。

若要在 EMR 主控台中使用除錯工具，在您使用主控台、CLI 或 API 啟動叢集時，您必須啟用除錯功能。

使用 Amazon EMR 主控台啟用除錯工具

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
 2. 選擇 Create cluster (建立叢集)。
 3. 選擇 Go to advanced options (前往進階選項)。
 4. 在 Cluster Configuration (叢集組態) 部分，在 Logging (紀錄) 欄位中，選擇 Enabled (啟用)。您不能在未啟用紀錄的情況下啟用除錯功能。
 5. 在 Log folder S3 location (日誌資料夾 S3 位置) 欄位中，鍵入 Amazon S3 路徑來存放您的日誌。
 6. 在 Debugging (除錯功能) 欄位中，選擇 Enabled (啟用)。
- 除錯功能選項會建立 Amazon SQS 交換，以將除錯訊息發佈到 Amazon EMR 服務後端。可能需付發佈訊息交換的費用。如需詳細資訊，請參閱 <https://aws.amazon.com/sqs>。
7. 按照 [規劃和設定叢集 \(p. 31\)](#) 中所述繼續建立叢集。

使用 AWS CLI 啟用除錯工具

若要使用 AWS CLI 啟用除錯，使用 `--enable-debugging` 參數鍵入 `create-cluster` 子命令。在啟用除錯時，您也必須指定 `--log-uri` 參數。

- 若要使用 AWS CLI 啟用除錯，鍵入下列命令並以您的 EC2 金鑰對名稱來取代 `myKey`。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.1.0 --log-uri s3://mybucket/logs/ --enable-debugging --applications Name=Hadoop Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge --instance-count 3
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

Example 使用 Java 軟體開發套件啟用除錯

使用以下 StepConfig 啟用除錯：

```
StepFactory stepFactory = new StepFactory();
StepConfig enabledebugging = new StepConfig()
    .withName("Enable debugging")
    .withActionOnFailure("TERMINATE_JOB_FLOW")
    .withHadoopJarStep(stepFactory.newEnableDebuggingStep());
```

除錯選項資訊

4.1 或更高版本 Amazon EMR 在所有區域支援除錯。

Amazon EMR 會建立一個 Amazon SQS 佇列來處理除錯資料。可能需支付訊息費用。不過，Amazon SQS 有最多提供 1,000,000 個請求的免費方案。如需詳細資訊，請參閱 [Amazon SQS 詳細資訊頁面](#)。

除錯需要使用角色；您的服務角色和執行個體描述檔必須允許您使用所有 Amazon SQS API 操作。如果您的角色是連接到 Amazon EMR 受管政策，您便不需要修改您的角色。如果您有自訂的角色，您需要

新增 sqs:* 許可。如需更多詳細資訊，請參閱 [將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。

標籤叢集

此方法非常便利，可讓您以不同的方式分類您的 AWS 資源，例如依據目的、擁有者或環境。您可以透過使用標籤來將自訂中繼資料指派到 Amazon EMR 叢集以在 Amazon EMR 中達成此目的。每個標籤皆包含由您定義的金鑰和值。對於 Amazon EMR，叢集是您可以新增標籤的資源層級。例如，您可以為帳戶叢集定義一組標籤，可協助您追蹤每個叢集的擁有者或識別生產叢集和測試叢集。我們建議您建立一組一致的標籤，以滿足您組織的需求。

當您將標籤新增到 Amazon EMR 叢集時，該標籤也會傳播到與該叢集相關聯的每個作用中的 Amazon EC2 執行個體。同樣地，當您從 Amazon EMR 叢集移除某個標籤，會將該標籤從每個相關作用中的 Amazon EC2 執行個體中移除。

Important

使用 Amazon EMR 主控台或 CLI 來管理屬於某叢集（而不是 Amazon EC2 主控台或 CLI）之 Amazon EC2 執行個體上的標籤，因為您在 Amazon EC2 中所做的變更未與 Amazon EMR 標記系統同步。

您可以透過尋找以下系統標籤來識別屬於 Amazon EMR 叢集的 Amazon EC2 執行個體。在這個範例中，**CORE** 是執行個體群組角色的值，而 **j-12345678** 是範例任務流程（叢集）的識別符值：

- aws:elasticmapreduce:instance-group-role=**CORE**
- aws:elasticmapreduce:job-flow-id=**j-12345678**

Note

Amazon EMR 和 Amazon EC2 將您的標籤解釋為字元字串，而不含任何語意。

您可以使用 AWS Management Console、CLI 和 API 來使用標籤。

您可以在建立新 Amazon EMR 叢集時新增標籤，您可以從執行中 Amazon EMR 叢集中新增、編輯或移除標籤。編輯標籤這個概念適用於 Amazon EMR 主控台，但若使用 CLI 和 API 來編輯標籤，會移除舊標籤並新增標籤。您可以編輯標籤金鑰和數值，並且可以在叢集執行時將標籤從資源中移除。不過，您無法從先前與仍作用中的叢集相關聯之終止叢集或終止執行個體中新增、編輯或移除標籤。此外，您可以將標籤的值設為空白字串，但您無法將標籤的值設為 null。

如果您使用的是 AWS Identity and Access Management (IAM) 與依標籤以資源為基礎之許可的 Amazon EC2 執行個體，則 IAM 政策會套用到叢集，Amazon EMR 會將該叢集傳播到叢集的 Amazon EC2 執行個體。對於傳播到 Amazon EMR 執行個體的 Amazon EC2 標籤，IAM 的 Amazon EC2 政策需要允許許可，才能呼叫 Amazon EC2 CreateTags 和 DeleteTags API。此外，傳播標籤會影響 Amazon EC2 以資源為基礎的許可。可將傳播到 Amazon EC2 的標籤讀取做為 IAM 政策中的條件，就像其他 Amazon EC2 標籤。在將標籤新增到 Amazon EMR 叢集時，需謹記 IAM 政策，以避免 IAM 使用者擁有不正確的叢集許可。為了避免問題，確保 IAM 政策不包含您計劃對 Amazon EMR 叢集使用的標籤條件。如需詳細資訊，請參閱 [控制對 Amazon EC2 資源的存取](#)。

標籤限制

以下基本限制適用於標籤：

- 適用於 Amazon EC2 資源的限制也適用於 Amazon EMR。如需詳細資訊，請參閱 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html#tag-restrictions。
- 標籤名稱和值不可使用 aws：字首，因為它只保留給 AWS 使用。此外，您不可編輯或刪除具此字首的標籤名稱或值。
- 您無法在已終止的叢集變更或編輯標籤。

- 標籤值可以為空白字串，但不得是 null。此外，標籤金鑰不得為空白字串。
- 金鑰和值可包含任何語言的字母字元、數字字元、空格、隱藏分隔符號和下列符號：`_ . : / = + - @`

如需有關使用 AWS Management Console 加入標記的更多資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [在主控台中使用標籤](#)。有關使用 Amazon EC2 API 或命令列加入標記的更多資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [API 和 CLI 概觀](#)。

帳單的標籤資源

您可以使用標籤整理您的 AWS 帳單，藉以反映您自己的成本結構。方式是註冊以取得包含標籤鍵值的 AWS 帳戶帳單。您可以依標籤金鑰來組織帳單資訊，藉此查看您的組合資源成本。雖然 Amazon EMR 和 Amazon EC2；有不同的帳單，每個叢集上的標籤也會放置在每個相關執行個體，因此您可以使用標籤來連結相關 Amazon EMR 和 Amazon EC2 成本。

例如，您可以使用特定應用程式名稱來標記數個資源，然後整理帳單資訊以查看該應用程式跨數項服務的總成本。如需詳細資訊，請參閱 AWS Billing and Cost Management User Guide 中的 [成本分配和標記](#)。

將標籤新增到新叢集

您可以在建立叢集時將標籤新增到其中。

若要在使用主控台新建叢集時新增標籤

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)，Go to advanced options (前往進階選項)。
3. 在 Step 3: General Cluster Settings (步驟 3：一般叢集設定) 頁面的 Tags (標籤) 區段中，為您的標籤輸入 Key (索引鍵)。

當您開始輸入 Key (索引鍵) 時，會自動顯示新的一列，以提供下一個新標籤的空間。

4. 或者，輸入標籤的 Value (值)。
5. 為每個標籤金鑰/值對重複之前步驟，以將其新增到叢集。叢集啟動時，您輸入的任何標籤會自動關聯到叢集。

若要在使用 AWS CLI 新建叢集時新增標籤

以下範例示範如何使用 AWS CLI 將標籤新增到叢集。若要在建立叢集時新增標籤，輸入含 `create-cluster` 參數的 `--tags` 子命令。

- 若要在建立叢集時使用鍵值 `marketing` 來新增名為 `costCenter` 的標籤，請輸入以下命令，並使用 EC2 金鑰對來取代 `myKey`。

```
aws emr create-cluster --name "Test cluster" --release-label emr-4.0.0 --applications Name=Hadoop Name=Hive Name=Pig --tags "costCenter=marketing" --use-default-roles --ec2-attributes KeyName=myKey --instance-type m5.xlarge --instance-count 3
```

若您未使用 `--instance-groups` 參數指定執行個體計數，即會啟動單一主節點，且剩餘執行個體會以核心節點的形式啟動。所有節點都將使用命令中指定的執行個體類型。

Note

如果您先前尚未建立預設 EMR 服務角色和 EC2 執行個體描述檔，請先輸入 `aws emr create-default-roles` 來建立這些設定檔，接著再輸入 `create-cluster` 子命令。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

將標籤新增到現有的叢集

您也可以將標籤新增到現有的叢集。

若要使用主控台將標籤至現有叢集

1. 在 Amazon EMR 主控台中，選擇 Cluster List (叢集清單) 頁面，然後按一下要將標籤新增至其中的叢集。
2. 在 Cluster Details (叢集詳細資訊) 頁面的 Tags (標籤) 欄位，按一下 View All/Edit (查看所有/編輯)。
3. 在 View All/Edit (查看所有/編輯) 頁面，按一下 Add (新增)。
4. 按一下 Key (金鑰) 欄的空欄位，並輸入金鑰名稱。
5. 或者，按一下 Value (值) 欄的空欄位，並輸入值名稱。
6. 隨著您開始使用的每個新標籤，另一個空的標籤列會出現在您目前編輯的標籤底下。為要新增之每個標籤的新標籤列重複之前的步驟。

若要使用 AWS CLI 將標籤新增至執行中的叢集

以下範例示範如何使用 AWS CLI 將標籤新增到執行中的叢集。輸入 add-tags 子指令和 --tag 參數來將標籤指派到資源識別符 (叢集 ID)。資源 ID 是可透過主控台或 list-clusters 命令取得的叢集識別符。

Note

add-tags 子指令目前僅接受一個資源 ID。

- 若要將兩個標籤新增至執行中的叢集 (一個未含值之名為 *production* 的金鑰，和內含 *marketing* 之名為 *costCenter* 的金鑰)，輸入以下命令並使用叢集 ID 取代 *j-KT4XXXXXXXXX1NM*。

```
aws emr add-tags --resource-id j-KT4XXXXXXXXX1NM --tag "costCenter=marketing" --tag "other=accounting"
```

Note

使用 AWS CLI 新增標籤時，沒有來自命令的輸出。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

查看叢集上的標籤

如果您想要查看所有與叢集相關聯的標籤，您可以在主控台或 CLI 中進行查看。

使用主控台檢視叢集標籤

1. 在 Amazon EMR 主控台中，選擇 Cluster List (叢集清單) 頁面，然後按一下叢集以檢視標籤。
2. 在 Cluster Details (叢集詳細資訊) 頁面的 Tags (標籤) 欄位中會顯示一些標籤。按一下 View All/Edit (查看所有/編輯) 以顯示叢集上所有的可用標籤。

使用 AWS CLI 檢視叢集標籤

若要使用 AWS CLI 檢視叢集標籤，請輸入含 --query 參數的 describe-cluster 子命令。

- 要查看叢集的標籤，輸入下列命令，並使用叢集 ID 取代 *j-KT4XXXXXXXXX1NM*。

```
aws emr describe-cluster --cluster-id j-KT4XXXXXXXXX1NM --query Cluster.Tags
```

此輸出會顯示與以下類似之叢集的所有標籤資訊：

Value: accounting	Value: marketing
Key: other	Key: costCenter

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

從叢集移除標籤

如果您不再需要標籤，您可以將其從叢集中移除。

使用主控台將標籤從叢集中移除

1. 在 Amazon EMR 主控台中，選擇 Cluster List (叢集清單) 頁面，然後按一下要從中移除標籤的叢集。
2. 在 Cluster Details (叢集詳細資訊) 頁面的 Tags (標籤) 欄位，按一下 View All/Edit (查看所有/編輯)。
3. 在 View All/Edit (查看全部/編輯) 對話方塊，按一下要刪除之標籤旁的 X (X) 圖示，然後按一下 Save (儲存)。
4. (選用) 為每個金鑰/值對重複之前的步驟，以將其從叢集中移除。

使用 AWS CLI 將標籤從叢集中移除

若要使用 AWS CLI 將標籤從叢集中移除，請輸入含 --tag-keys 參數的 remove-tags 子命令。移除標籤時，只需要金鑰名稱即可。

- 要將標籤從叢集中移除，輸入下列命令，並使用叢集 ID 取代 *j-KT4XXXXXXXX1NM*。

```
aws emr remove-tags --resource-id j-KT4XXXXXXXX1NM --tag-keys "costCenter"
```

Note

您目前無法使用單一命令來移除多個標籤。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

驅動程式和第三方應用程式整合

您只要支付使用定價，就可以在 Amazon EMR 上執行數種熱門的大數據應用程式。這表示，您在叢集執行的同時支付定額的每小時使用費，就可以使用第三方應用程式。如此您就能使用應用程式，而不需要每年購買授權。下列章節說明可搭配 EMR 使用的一些工具。

主題

- [使用商業智慧工具搭配 Amazon EMR \(p. 125\)](#)

使用商業智慧工具搭配 Amazon EMR

您可以使用熱門的商業智慧工具（如 Microsoft Excel、MicroStrategy、QlikView 和 Tableau）搭配 Amazon EMR 來探索和視覺化您的資料。這些工具當中多數都需要 ODBC (開放式資料庫連線) 或 JDBC (Java 資料庫連線) 驅動程式。您可以從下方連結下載並安裝必要的驅動程式：

- <http://awssupportdatasvcs.com/bootstrap-actions/Simba/AmazonHiveJDBC-1.0.9.1060.zip>
- http://awssupportdatasvcs.com/bootstrap-actions/Simba/Hive_ODBC_1.2.2.1018.zip
- <http://amazon-odbc-jdbc-drivers.s3.amazonaws.com/public/HBaseODBC.zip>

如需有關如何將 Microsoft Excel 這類商業智慧工具連線到 Hive 的詳細資訊，請瀏覽 http://cdn.simba.com/products/Hive/doc/Simba_Hive_ODBC_Quickstart.pdf。

Amazon EMR 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。[共同的責任模型](#) 將此描述為雲端本身的安全和雲端內部的安全：

- 雲端本身的安全 – AWS 負責保護執行 AWS 雲端內 AWS 服務的基礎設施。AWS 提供的服務，也可讓您安全使用。在 [AWS 合規計劃](#) 中，第三方稽核員會定期測試並驗證我們安全性的功效。若要進一步了解適用於 Amazon EMR 的合規計劃，請參閱 [合規計劃範圍內的 AWS 服務](#)。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。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。

本文件有利於您了解，共同責任模型在使用 Amazon EMR 時的適用情形。當您在 Amazon EMR 上開發解決方案時，使用下列技術來協助您根據業務需求來保護叢集資源和資料。此章節中的主題說明如何設定 Amazon EMR 和使用其他 AWS 服務，以滿足您的安全和合規目標。

安全組態

Amazon EMR 中的安全組態是不同安全設定的範本。您可以建立安全組態，如此就能在每次建立叢集時，便利地重複使用安全設定。如需更多詳細資訊，請參閱 [使用安全組態設定叢集安全性 \(p. 128\)](#)。

資料保護

您可以建置資料加密機制，來協助保護 Amazon S3 中的靜態資料、叢集執行個體儲存體中的靜態資料，及傳輸中的資料。如需更多詳細資訊，請參閱 [加密靜態和傳輸中的資料 \(p. 144\)](#)。

AWS Identity and Access Management 取代為 Amazon EMR

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制 AWS 資源的存取。IAM 管理員可以控制能進行身份驗證（登入）及獲得授權（具備許可）以使用 Amazon EMR 資源的人員。IAM 是一種 AWS 服務，無須支付任何額外的費用即可使用。

- IAM 以身分為基礎的政策 – IAM 政策會允許或拒絕 IAM 使用者和群組執行動作的許可。政策可與標籤結合，以各自叢集的基礎控制存取。如需詳細資訊，請參閱 [適用於 Amazon EMR 的 AWS Identity and Access Management \(p. 151\)](#)。
- IAM 角色 – Amazon EMR 服務角色、執行個體描述檔和服務連結角色可控管 Amazon EMR 如何能夠存取其他 AWS 服務。如需詳細資訊，請參閱 [將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。
- 向 Amazon S3 請求使用 EMRFS 的 IAM 角色 – 在 Amazon EMR 存取 Amazon S3 時，您可以指定要根據使用者、群組或 Amazon S3 中 EMRFS 資料的位置使用的 IAM 角色。這可讓您精準控制叢集使用者是否可以存取 Amazon EMR 中的檔案。如需詳細資訊，請參閱 [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)。

Kerberos

您可以設定 Kerberos，透過私密金鑰加密法來提供強式身份驗證機制。如需詳細資訊，請參閱 [使用 Kerberos 身份驗證 \(p. 190\)](#)。

Lake Formation

您可以將 Lake Formation 許可與 AWS Glue 資料目錄 搭配使用以提供對 AWS Glue 資料型錄中的資料庫和資料表的精細分級存取。Lake Formation 可使同盟從企業身分系統單一登入 EMR Notebooks 或 Apache Zeppelin。如需詳細資訊，請參閱 [Amazon EMR 與 AWS Lake Formation 整合 \(Beta 版\) \(p. 214\)](#)。

安全通訊殼層 (SSH)

SSH 協助提供安全的方法，讓使用者能夠在叢集執行個體上連線到命令列。它也提供通道，以檢視應用程式在主節點上執行的 Web 界面。用戶端可以使用 Kerberos 或 Amazon EC2 金鑰對來驗證。如需更多詳細資訊，請參閱 [使用 SSH 登入資料的 Amazon EC2 金鑰對 \(p. 190\)](#) 及 [連接叢集 \(p. 276\)](#)。

Amazon EC2 安全群組

安全群組就像是 EMR 叢集執行個體的虛擬防火牆，可限制傳入及傳出的網路流量。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

適用於 Amazon EMR 的預設 Amazon Linux AMI 更新

如果 Amazon EC2 執行個體位於使用預設 Amazon EMR 適用 Amazon Linux AMI 的叢集中，而此執行個體是首次啟動，則預設會安裝重要的安全更新。其他的更新不會安裝。取決於您應用程式的安全狀態和叢集執行的時間長度，您可以選擇定期重新啟動您的叢集，以套用安全性更新，或是建立引導操作，來自訂套件安裝與更新。您也可以選擇進行測試，然後在執行中的叢集執行個體上，安裝選取的安全性更新。如需詳細資訊，請參閱 [使用 Amazon EMR 的預設 Amazon Linux AMI \(p. 79\)](#)。

使用安全組態設定叢集安全性

在 Amazon EMR 4.8.0 發行版本或更新版本中，您可以使用安全組態設定資料加密、Kerberos 身份驗證（在 5.10.0 發行版本和更新版本中可供使用）和 EMRFS 的 Amazon S3 授權（在 5.10.0 發行版本或更新版本中可供使用）。

建立安全組態後，您在建立叢集時指定它，並可在任何數量的叢集中重複使用。

您可以使用主控台、AWS Command Line Interface (AWS CLI) 或 AWS 開發套件來建立安全組態。您也可以使用 AWS CloudFormation 範本來建立安全組態。如需詳細資訊，請參閱 [AWS CloudFormation User Guide](#) 和 [AWS::EMR::SecurityConfiguration](#) 的範本參考。

主題

- [建立安全組態 \(p. 129\)](#)
- [指定適用於叢集的安全組態 \(p. 142\)](#)

建立安全組態

此主題涵蓋使用 EMR 主控台和 AWS CLI 建立安全組態的一般程序，並接續說明構成加密、身份驗證和 EMRFS IAM 角色的參數參考。如需這些功能的詳細資訊，請參閱下列主題：

- [加密靜態和傳輸中的資料 \(p. 144\)](#)
- [使用 Kerberos 身份驗證 \(p. 190\)](#)
- [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)

使用主控台建立安全組態

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 在導覽窗格中，選擇 Security Configurations (安全組態)、Create security configuration (建立安全組態)。
3. 輸入安全組態的 Name (名稱)。
4. 選擇下列段落中所述的 Encryption (加密) 和 Authentication (身份驗證) 選項，然後選擇 Create (建立)。

使用 AWS CLI 建立安全組態

- 使用 `create-security-configuration` 指令，如下列範例所示。
 - 針對 `SecConfigName`，指定安全組態的名稱。這是您在建立使用此安全組態的叢集時所指定的名稱。
 - 針對 `SecConfigDef`，指定內嵌的 JSON 結構或是本機 JSON 檔案的路徑，例如 `file:///MySecConfig.json`。如下列段落所述，JSON 參數會定義 Encryption (加密)、IAM Roles for EMRFS access to Amazon S3 (用來對 Amazon S3 進行 EMRFS 存取的 IAM 角色) 與 Authentication (身份驗證) 的選項。

```
aws emr create-security-configuration --name "SecConfigName" --security-configuration SecConfigDef
```

設定資料加密

在安全組態中設定加密前，請建立用於加密的金鑰和憑證。如需更多詳細資訊，請參閱 [使用 Amazon EMR 提供靜態資料的加密金鑰 \(p. 148\)](#) 及 [使用 Amazon EMR 加密提供傳輸中資料的加密憑證 \(p. 150\)](#)。

您在建立安全組態時指定兩組加密選項：靜態資料加密和傳輸中資料加密。靜態資料加密選項包含 EMRFS 和本機磁碟加密的 Amazon S3。傳輸中加密選項啟用支援 Transport Layer Security (TLS) 特定應用程式的開放原始碼功能。靜態和傳輸中的選項可同時啟用或分別啟用。如需更多詳細資訊，請參閱 [加密靜態和傳輸中的資料 \(p. 144\)](#)。

使用主控台指定加密選項

在 Encryption (加密) 中，根據下列的準則來選擇選項。

- 選擇 At rest encryption (靜態加密) 下的選項來加密存放於檔案系統中的資料。

您可以選擇加密 Amazon S3、本機磁碟或兩者的資料。
- 在 S3 data encryption (S3 資料加密) 下，針對 Encryption mode (加密模式) 選擇值，來決定 Amazon EMR 如何使用 EMRFS 將資料 Amazon S3 資料加密。

您接下來要執行的動作取決於您選擇的加密模式：

- SSE-S3 (SSE-S3)

指定 [伺服器端加密 \(使用 Amazon S3 受管加密金鑰\)](#)。您不必再進行任何操作，因為 Amazon S3 會為您處理金鑰。

- SSE-KMS (SSE-KMS) 或 CSE-KMS (CSE-KMS)

指定 [伺服器端加密 \(使用 AWS KMS 受管金鑰\) \(SSE-KMS\)](#) 或 [用戶端加密 \(使用 AWS KMS 受管金鑰\) \(CSE-KMS\)](#)。針對 AWS KMS Key (AWS KMS 金鑰)，選取金鑰。金鑰必須與您的 EMR 叢集位於相同的區域中。如需金鑰需求，請參閱「[使用適用於加密的 AWS KMS 客戶主金鑰 \(CMK\) \(p. 148\)](#)」。

- CSE-Custom (自訂 CSE)

指定 [使用自訂用戶端主金鑰 \(自訂 CSE\) 的用戶端加密](#)。針對 S3 object (S3 物件)，輸入 Amazon S3 中的位置，或是您自訂金鑰提供者 JAR 檔案的 Amazon S3 ARN。接著，針對 Key provider class (金鑰提供者類別)，輸入在實作 EncryptionMaterialsProvider 界面的應用程式中，所宣告類別的完整類別名稱。

- 在 Local disk encryption (本機磁碟加密) 下，選擇 Key provider type (金鑰提供者類型) 的值。
 - AWS KMS

選擇此選項來指定 AWS KMS 客戶主金鑰 (CMK)。針對 AWS KMS customer master key (AWS KMS 客戶主金鑰)，選取金鑰。金鑰必須與您的 EMR 叢集位於相同的區域中。如需金鑰需求的詳細資訊，請參閱「[使用適用於加密的 AWS KMS 客戶主金鑰 \(CMK\) \(p. 148\)](#)」。

EBS 加密

當您指定 AWS KMS 做為金鑰提供者時，您可以啟用 EBS 加密來加密 EBS 根設備和儲存磁碟區。若要啟用這類選項，您必須授予 EMR EMR_DefaultRole 服務角色使用您指定的客戶主金鑰 (CMK) 的許可。如需金鑰需求的詳細資訊，請參閱「[為 AWS KMS CMK 提供額外的許可來啟用 EBS 加密 \(p. 149\)](#)」。

- Custom (自訂)

選擇此選項來指定自訂金鑰提供者。針對 S3 object (S3 物件)，輸入 Amazon S3 中的位置，或是您自訂金鑰提供者 JAR 檔案的 Amazon S3 ARN。針對 Key provider class (金鑰提供者類別)，輸入在實作 EncryptionMaterialsProvider 界面的應用程式中，所宣告類別的完整類別名稱。您在這裡提供的類別名稱必須不同於為自訂 CSE 提供的類別名稱。

- 選擇 In-transit encryption (傳輸中加密)，來啟用傳輸中資料的開放原始碼 TLS 加密功能。根據下列的準則來選擇 Certificate provider type (憑證提供者類型)：
 - PEM (PEM)

選擇此選項來使用您在 zip 檔案中提供的 PEM 檔案。在 zip 檔案中需要兩個成品：privateKey.pem 和 certificateChain.pem。第三個檔案的 trustedCertificates.pem 為選用。如需詳細資訊，請參閱「[使用 Amazon EMR 加密提供傳輸中資料的加密憑證 \(p. 150\)](#)」。針對 S3 object (S3 物件)，指定 Amazon S3 中的位置，或指定 zip 檔案欄位的 Amazon S3 ARN。

- Custom (自訂)

選擇此選項來指定自訂憑證提供者，然後針對 S3 object (S3 物件)，輸入 Amazon S3 中的位置，或是您自訂憑證提供者 JAR 檔案的 Amazon S3 ARN。針對 Key provider class (金鑰提供者類別)，輸入在實作 TLSArtifactsProvider 界面的應用程式中，所宣告類別的完整類別名稱。

使用 AWS CLI 指定加密選項

下列的段落使用了案例範例，來說明不同組態和金鑰提供者的正確格式 --security-configuration JSON，以及 JSON 參數和適當值的參考。

傳輸中資料加密選項範例

以下範例說明以下案例：

- 傳輸中資料加密啟用而靜態資料加密停用。
- 會使用 Amazon S3 中包含憑證的 zip 檔案，來做為金鑰提供者 (關於憑證的要求，請參閱[使用 Amazon EMR 加密提供傳輸中資料的加密憑證 \(p. 150\)](#))。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{  
    "EncryptionConfiguration": {  
        "EnableInTransitEncryption" : true,  
        "EnableAtRestEncryption" : false,  
        "InTransitEncryptionConfiguration" : {  
            "TLSCertificateConfiguration" : {  
                "CertificateProviderType" : "PEM",  
                "S3Object" : "s3://MyConfigStore/artifacts/MyCerts.zip"  
            }  
        }  
    }  
}'
```

以下範例說明以下案例：

- 傳輸中資料加密啟用而靜態資料加密停用。
- 使用自訂金鑰提供者 (如需憑證需求，請參閱「[使用 Amazon EMR 加密提供傳輸中資料的加密憑證 \(p. 150\)](#)」)。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{  
    "EncryptionConfiguration": {  
        "EnableInTransitEncryption" : true,  
        "EnableAtRestEncryption" : false,  
        "InTransitEncryptionConfiguration" : {  
            "TLSCertificateConfiguration" : {  
                "CertificateProviderType" : "Custom",  
                "S3Object" : "s3://MyConfig/artifacts/MyCerts.jar",  
                "CertificateProviderClass" : "com.mycompany.MyCertProvider"  
            }  
        }  
    }  
}'
```

靜態資料加密選項範例

以下範例說明以下案例：

- 傳輸中資料加密停用而靜態資料加密啟用。
- SSE-S3 用於 Amazon S3 加密。
- 本機磁碟加密使用 AWS KMS 做為金鑰提供者。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{  
    "EncryptionConfiguration": {  
        "EnableInTransitEncryption" : false,  
        "EnableAtRestEncryption" : true,  
        "AtRestEncryptionConfiguration" : {  
            "S3EncryptionConfiguration" : {  
                "EncryptionMode" : "SSE-S3"  
            },  
            "LocalDiskEncryptionConfiguration" : {  
                "EncryptionMode" : "AWS-KMS"  
            }  
        }  
    }  
}'
```

```
    "EncryptionKeyProviderType" : "AwsKms",
    "AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
}
}
}
}'
```

以下範例說明以下案例：

- 傳輸中資料加密啟用，並使用 ARN 參考 Amazon S3 中 PEM 憑證的 zip 檔案。
- SSE-KMS 用於 Amazon S3 加密。
- 本機磁碟加密使用 AWS KMS 做為金鑰提供者。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{
"EncryptionConfiguration": {
"EnableInTransitEncryption" : true,
"EnableAtRestEncryption" : true,
"InTransitEncryptionConfiguration" : {
"TLSCertificateConfiguration" : {
"CertificateProviderType" : "PEM",
"S3Object" : "arn:aws:s3:::MyConfigStore/artifacts/MyCerts.zip"
},
},
"AtRestEncryptionConfiguration" : {
"S3EncryptionConfiguration" : {
"EncryptionMode" : "SSE-KMS",
"AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
},
"LocalDiskEncryptionConfiguration" : {
"EncryptionKeyProviderType" : "AwsKms",
"AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
}
}
}
}'
```

以下範例說明以下案例：

- 傳輸中資料加密啟用，並參考 Amazon S3 中 PEM 憑證的 zip 檔案。
- CSE-KMS 用於 Amazon S3 加密。
- 本機磁碟加密使用其 ARN 參考的自訂金鑰提供者。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{
"EncryptionConfiguration": {
"EnableInTransitEncryption" : true,
"EnableAtRestEncryption" : true,
"InTransitEncryptionConfiguration" : {
"TLSCertificateConfiguration" : {
"CertificateProviderType" : "PEM",
"S3Object" : "s3://MyConfigStore/artifacts/MyCerts.zip"
},
},
"AtRestEncryptionConfiguration" : {
"S3EncryptionConfiguration" : {
```

```
"EncryptionMode" : "CSE-KMS",
"AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
},
"LocalDiskEncryptionConfiguration" : {
"EncryptionKeyProviderType" : "Custom",
"S3Object" : "arn:aws:s3:::artifacts/MyKeyProvider.jar",
"EncryptionKeyProviderClass" : "com.mycompany.MyKeyProvider.jar"
}
}
}'
```

以下範例說明以下案例：

- 傳輸中資料加密以自訂金鑰提供者啟用。
- 自訂 CSE 用於 Amazon S3 資料。
- 本機磁碟加密使用自訂金鑰提供者。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{
"EncryptionConfiguration": {
"EnableInTransitEncryption" : "true",
"EnableAtRestEncryption" : "true",
"InTransitEncryptionConfiguration" : {
"TLSCertificateConfiguration" : {
"CertificateProviderType" : "Custom",
"S3Object" : "s3://MyConfig/artifacts/MyCerts.jar",
"CertificateProviderClass" : "com.mycompany.MyCertProvider"
}
},
"AtRestEncryptionConfiguration" : {
"S3EncryptionConfiguration" : {
"EncryptionMode" : "CSE-Custom",
"S3Object" : "s3://MyConfig/artifacts/MyCerts.jar",
"EncryptionKeyProviderClass" : "com.mycompany.MyKeyProvider"
},
"LocalDiskEncryptionConfiguration" : {
"EncryptionKeyProviderType" : "Custom",
"S3Object" : "s3://MyConfig/artifacts/MyCerts.jar",
"EncryptionKeyProviderClass" : "com.mycompany.MyKeyProvider"
}
}
}
}'
```

以下範例說明以下案例：

- 傳輸中資料加密停用而靜態資料加密啟用。
- Amazon S3 加密會透過 SSE-KMS 啟用，而加密例外會套用到個別 S3 儲存貯體。
- 停用本機磁碟加密。

```
aws emr create-security-configuration --name "MySecConfig" --security-configuration '{
"EncryptionConfiguration": {
"AtRestEncryptionConfiguration": {
"S3EncryptionConfiguration": {
"EncryptionMode" : "SSE-KMS",
"AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012",
}}
```

```
"Overrides" : [
    {
        "BucketName" : "sse-s3-bucket-name",
        "EncryptionMode" : "SSE-S3"
    },
    {
        "BucketName" : "cse-kms-bucket-name",
        "EncryptionMode" : "CSE-KMS",
        "AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    {
        "BucketName" : "sse-kms-bucket-name",
        "EncryptionMode" : "SSE-KMS",
        "AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    }
],
},
],
},
},
"EnableInTransitEncryption": false,
"EnableAtRestEncryption": true
},
}
}'
```

以下範例說明以下案例：

- 傳輸中資料加密停用而靜態資料加密啟用。
- 使用 SSE-S3 啟用 Amazon S3 加密，且本機磁碟加密已停用。

```
aws emr create-security-configuration --name "MyS3EncryptionConfig" --security-
configuration '{
    "EncryptionConfiguration": {
        "EnableInTransitEncryption" : false,
        "EnableAtRestEncryption" : true,
        "AtRestEncryptionConfiguration" : {
            "S3EncryptionConfiguration" : {
                "EncryptionMode" : "SSE-S3"
            }
        }
    }
}'
```

以下範例說明以下案例：

- 傳輸中資料加密停用而靜態資料加密啟用。
- 本機磁碟加密以 AWS KMS 為金鑰提供者啟用，且 Amazon S3 加密已停用。

```
aws emr create-security-configuration --name "MyLocalDiskEncryptionConfig" --security-
configuration '{
    "EncryptionConfiguration": {
        "EnableInTransitEncryption" : false,
        "EnableAtRestEncryption" : true,
        "AtRestEncryptionConfiguration" : {
            "LocalDiskEncryptionConfiguration" : {
                "EncryptionKeyProviderType" : "AwsKms",
                "AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
            }
        }
}'
```

```
    }
}'
```

以下範例說明以下案例：

- 傳輸中資料加密停用而靜態資料加密啟用。
- 本機磁碟加密以 AWS KMS 為金鑰提供者啟用，且 Amazon S3 加密已停用。
- EBS 加密已啟用。

```
aws emr create-security-configuration --name "MyLocalDiskEncryptionConfig" --security-configuration '{
    "EncryptionConfiguration": {
        "EnableInTransitEncryption" : false,
        "EnableAtRestEncryption" : true,
        "AtRestEncryptionConfiguration" : {
            "LocalDiskEncryptionConfiguration" : {
                "EnableEbsEncryption" : true,
                "EncryptionKeyProviderType" : "AwsKms",
                "AwsKmsKey" : "arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
            }
        }
    }
}'
```

適用於加密設定的 JSON 參考

下表列出加密設定的 JSON 參數，並提供每個參數可接受值的說明。

參數	描述
"EnableInTransitEncryption" : true false	指定 true 以啟用傳輸中加密，指定 false 以停用。若省略，則會採用 false，並停用傳輸中加密。
"EnableAtRestEncryption" : true false	指定 true 以啟用靜態加密，指定 false 以停用。若省略，則會採用 false，並停用靜態加密。
傳輸中加密參數	
"InTransitEncryptionConfiguration" :	當 EnableInTransitEncryption 為 true 時，指定用於設定傳輸中加密的值集合。
"CertificateProviderType" : "PEM" "Custom"	指定是否要使用參考壓縮檔案的 PEM 憑證或 Custom 憑證提供者。如果指定 PEM，S3Object 必須參考 Amazon S3 中 zip 檔案的位置 (該 zip 檔案包含憑證)。如果指定 Custom (自訂)，S3Object 必須參考 Amazon S3 中 JAR 檔案的位置，後面接著 CertificateProviderClass 項目。
"S3Object" : " <i>ZipLocation</i> " " <i>JarLocation</i> "	在指定 PEM 時，提供 Amazon S3 中至 zip 檔案的位置，或是在指定 Custom 時，提供至 JAR 檔案的位置。格式可以是路徑 (例如，s3://MyConfig/artifacts/CertFiles.zip) 或是 ARN (例如，arn:aws:s3:::Code/MyCertProvider.jar))。如果指定 zip 檔案，其必須包含命名方式與 privateKey.pem 和

參數	描述
	<code>certificateChain.pem</code> 完全相同的檔案。命名為 <code>trustedCertificates.pem</code> 的檔案為選用。
<code>"CertificateProviderClass" : "MyClassID"</code>	只有當 <code>CertificateProviderType</code> 指定為 <code>Custom</code> 時才需要。 <code>MyClassID</code> 會指定在 JAR 檔案中所宣告的完整類別名稱，該檔案實作了 <code>TLSArtifactsProvider</code> 界面。例如， <code>com.mycompany.MyCertProvider</code> 。
靜態加密參數	
<code>"AtRestEncryptionConfiguration" :</code>	在 <code>EnableAtRestEncryption</code> 為 <code>true</code> 時，指定靜態加密值的集合，包括 Amazon S3 加密和本機磁碟加密。
Amazon S3 加密參數	
<code>"S3EncryptionConfiguration" :</code>	指定用於 EMR 檔案系統 (EMRFS) Amazon S3 加密的值集合。
<code>"EncryptionMode" : "SSE-S3" "SSE-KMS" "CSE-KMS" "CSE-Custom"</code>	指定要使用的 Amazon S3 加密類型。如果指定 <code>SSE-S3</code> ，就不再需要其他的 Amazon S3 加密值。如果指定 <code>SSE-KMS</code> 或 <code>CSE-KMS</code> ，則 AWS KMS 客戶主金鑰 (CMK) ARN 必須指定為 <code>AwsKmsKey</code> 值。如果指定 <code>CSE-Custom</code> ，則必須指定 <code>S3Object</code> 和 <code>EncryptionKeyProviderClass</code> 的值。
<code>"AwsKmsKey" : "MyKeyARN"</code>	只有當 <code>EncryptionMode</code> 指定為 <code>SSE-KMS</code> 或 <code>CSE-KMS</code> 時才需要。 <code>MyKeyARN</code> 必須是金鑰完整指定的 ARN (例如 <code>arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012</code>)。
<code>"S3Object" : "JarLocation"</code>	只有當 <code>CertificateProviderType</code> 指定為 <code>CSE-Custom</code> 時才需要。 <code>JarLocation</code> 提供 Amazon S3 中至 JAR 檔案的位置。格式可以是路徑 (例如， <code>s3://MyConfig/artifacts/MyKeyProvider.jar</code>) 或是 ARN (例如， <code>arn:aws:s3:::Code/MyKeyProvider.jar</code>)。
<code>"EncryptionKeyProviderClass" : "MyS3KeyClassID"</code>	只有當 <code>EncryptionMode</code> 指定為 <code>CSE-Custom</code> 時才需要。 <code>MyS3KeyClassID</code> 指定在實作 <code>EncryptionMaterialsProvider</code> 界面的應用程式中，所宣告類別的完整類別名稱，例如， <code>com.mycompany.MyS3KeyProvider</code> 。
本機磁碟加密參數	
<code>"LocalDiskEncryptionKeyProvider"</code>	指定用於本機磁碟加密的金鑰提供者和對應的值。
<code>"Type" : "AwsKms" "Custom"</code>	指定金鑰提供者。如果指定 <code>AwsKms</code> ，則必須將 AWS KMS CMK ARN 指定為 <code>AwsKmsKey</code> 值。如果指定 <code>Custom</code> ，則必須指定 <code>S3Object</code> 和 <code>EncryptionKeyProviderClass</code> 的值。

參數	描述
"AwsKmsKey" : "MyKeyARN"	只有當 Type 指定為 AwsKms 時才需要。 <i>MyKeyARN</i> 必須是金鑰完整指定的 ARN (例如 arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-4
"S3Object" : "JarLocation"	只有當 CertificateProviderType 指定為 CSE-Custom 時才需要。 <i>JarLocation</i> 提供 Amazon S3 中至 JAR 檔案的位置。格式可以是路徑 (例如, s3://MyConfig/artifacts/MyKeyProvider.jar) 或是 ARN (例如, arn:aws:s3:::Code/MyKeyProvider.jar)。
"EncryptionKeyProviderClass" : "MyLocalDiskKeyClassID"	只有當 Type 指定為 Custom 時才需要。 <i>MyLocalDiskKeyClassID</i> 指定在實作 EncryptionMaterialsProvider 界面的應用程式中, 所宣告類別的完整類別名稱, 例如, com.mycompany.MyLocalDiskKeyProvider。

設定 Kerberos 身份驗證

Kerberos 設定的安全組態只能由以 Kerberos 屬性建立的叢集使用，否則會發生錯誤。如需更多詳細資訊，請參閱 [使用 Kerberos 身份驗證 \(p. 190\)](#)。Kerberos 僅能在 Amazon EMR 5.10.0 發行版本和更新版本中使用。

使用主控台指定 Kerberos 設定

根據下列的準則，在 Kerberos authentication (Kerberos 身份驗證) 中選擇選項。

參數	描述
Kerberos	指定使用此安全組態的叢集啟用 Kerberos。如果有叢集使用此安全組態，則該叢集也必須指定 Kerberos 設定，否則會發生錯誤。
提供者	叢集專用 KDC 如有需要，您可以從其他叢集參考這個 KDC。使用不同的安全組態建立這些叢集，指定外部 KDC，並且使用您為叢集專用 KDC 指定的領域名稱和 KDC 管理員密碼。
	外部 KDC 僅適用於 Amazon EMR 5.20.0 和更新版本。指定使用此安全組態的叢集透過叢集外的 KDC 伺服器來驗證 Kerberos 主體。KDC 不在叢集上建立。在建立叢集時，您可以指定外部 KDC 的領域名稱和 KDC 管理員密碼。
票證生命週期	選用。指定 KDC 所發行之 Kerberos 票證在使用此安全組態之叢集上有效的期間。 由於安全理由，票證的生命週期有限。叢集應用程式和服務會在票證過期後自動續約。使用 Kerberos 登入資料透過 SSH 連接至叢集的使用者，必須從主節點命令列執行 <code>kinit</code> ，以在票證過期後續約。

參數	描述	
跨域信任	<p>針對在不同 Kerberos 領域內使用此安全組態和 KDC 的叢集，指定其中叢集專用 KDC 之間的跨域信任。</p> <p>來自另一個領域的委託人 (通常為使用者) 就會通過使用此組態之叢集的驗證。另一個 Kerberos 領域則必須額外設定。如需更多詳細資訊，請參閱 教學課程：使用 Active Directory 網域設定跨域信任 (p. 210)。</p>	
跨域信任屬性	領域	為信任關係中的另一個領域指定 Kerberos 領域名稱。根據慣例，Kerberos 領域名稱與網域名稱相同，但全部採用大寫字母。
	網域	為信任關係中的另一個領域指定網域名稱。
	管理伺服器	為信任關係中的另一個領域指定管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 749)。
	KDC 伺服器	為信任關係中的另一個領域指定 KDC 伺服器的完整網域名稱 (FQDN) 或 IP 地址。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 88)。
外部 KDC	指定該叢集外部 KDC 應由該叢集使用。	
外部 KDC 屬性	管理伺服器	指定外部管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 749)。
	KDC 伺服器	指定外部 KDC 伺服器的完整網域名稱 (FQDN)。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 88)。
	Active Directory 整合	指定 Kerberos 主體身份驗證與 Microsoft Active Directory 網域整合。
Active Directory 整合屬性	Active Directory 領域	指定 Active Directory 網域的 Kerberos 領域名稱。根據慣例，Kerberos 領域名稱通常與網域名稱相同，但全部採用大寫字母。

參數		描述
	Active Directory 網域	指定 Active Directory 網域名稱。
	Active Directory 伺服器	指定 Microsoft Active Directory 網域控制站的完整網域名稱 (FQDN)。

使用 AWS CLI 指定 Kerberos 設定

以下參考資料表顯示安全組態中，Kerberos 設定的 JSON 參數。如需組態範例，請參閱[組態範例 \(p. 203\)](#)。

參數		描述
"AuthenticationConfiguration": {		為 Kerberos 的必要項目。指定身份驗證設定是此安全組態的一部分。
"KerberosConfiguration": {		為 Kerberos 的必要項目。指定 Kerberos 的組態屬性。
	<p>"Provider": <code>ClusterDedicatedKdc</code>,</p> <p>—或—</p> <p>"Provider": "ExternalKdc",</p>	<p><code>ClusterDedicatedKdc</code> 會指定 Amazon EMR 在任何使用此安全組態的主節點上建立 KDC。在建立叢集時，您可以指定領域名稱和 KDC 管理員密碼。如有需要，您可以從其他叢集參考這個 KDC。使用不同的安全組態建立這些叢集，指定外部 KDC，並且使用您在建立搭配叢集專用 KDC 的叢集時所指定的領域名稱和 KDC 管理員密碼。</p> <p><code>ExternalKdc</code> 會指定該叢集使用外部 KDC。Amazon EMR 不會在主節點上建立 KDC。使用此安全組態的叢集必須指定該外部 KDC 的領域名稱和 KDC 管理員密碼。</p>
"ClusterDedicatedKdcConfiguration": {	"TicketLifetimeInHours": 24,	<p>選用。指定 KDC 所發行之 Kerberos 票證在使用此安全組態之叢集上有效的期間。</p> <p>由於安全理由，票證的生命週期有限。叢集應用程式和服務會在票證過期後自動續約。使用 Kerberos 登入資料透過 SSH 連接至叢集的使用者，必須從主節點命令列執行 <code>kinit</code>，以在票證過期後續約。</p>
"CrossRealmTrustConfiguration": {		針對在不同 Kerberos 領域內使用此安全組態和 KDC 的叢集，指定其中叢集專用 KDC 之間的跨域信任。

參數	描述
	來自另一個領域的委託人 (通常為使用者) 就會通過使用此組態之叢集的驗證。另一個 Kerberos 領域則必須額外設定。如需更多詳細資訊，請參閱 教學課程：使用 Active Directory 網域設定跨域信任 (p. 210) 。
	"Realm": <i>"KDC2.COM"</i> ,
	"Domain": <i>"kdc2.com"</i> ,
	"AdminServer": <i>"kdc.com:749"</i> ,
	為信任關係中的另一個領域指定管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如， <i>domain.example.com:749</i>)。
	"KdcServer": <i>"kdc.com:88"</i>
	為信任關係中的另一個領域指定 KDC 伺服器的完整網域名稱 (FQDN) 或 IP 地址。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如， <i>domain.example.com:88</i>)。
	}
	}
"ExternalKdcConfiguration": {	指定 <i>ExternalKdc</i> 時為必要。
	"TicketLifetimeInHours": <i>24</i> ,
	選用。指定 KDC 所發行之 Kerberos 票證在使用此安全組態之叢集上有效的期間。 由於安全理由，票證的生命週期有限。叢集應用程式和服務會在票證過期後自動續約。使用 Kerberos 登入資料透過 SSH 連接至叢集的使用者，必須從主節點命令列執行 <i>kinit</i> ，以在票證過期後續約。
	"KdcServerType": <i>"Single"</i> ,
	指定該單一 KDC 伺服器應予以參考。目前唯一支援的值是 Single。

參數	描述
	"AdminServer": " <i>kdc.com:749</i> ",
	指定外部管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如， <i>domain.example.com:749</i>)。
	"KdcServer": " <i>kdc.com:88</i> ",
	指定外部 KDC 伺服器的完整網域名稱 (FQDN)。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如， <i>domain.example.com:88</i>)。
	"AdIntegrationConfiguration": {
	"AdRealm": " <i>AD.DOMAIN.COM</i> ",
	"AdDomain": " <i>ad.domain.com</i> "
	}
	}
	}

設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色

EMRFS 的 IAM 角色可讓您針對 Amazon S3 中的 EMRFS 資料，提供不同的許可。存取請求包含您指定的識別符時，建立指定用於提供許可 IAM 角色的映射。識別符可以是 Hadoop 使用者或角色，或 Amazon S3 前綴。

如需更多詳細資訊，請參閱 [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)。

使用 AWS CLI 來指定 EMRFS 的 IAM 角色

下列所舉的 JSON 程式碼片段範例，可在安全組態中為 EMRFS 指定自訂 IAM 角色。其示範了三個不同識別符類型的角色對應，並接續說明參數參考。

```
{
    "AuthorizationConfiguration": {
        "EmrFsConfiguration": {
```

```

    "RoleMappings": [
        {
            "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_for_user1",
            "IdentifierType": "User",
            "Identifiers": [ "user1" ]
        },
        {
            "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_to_MyBuckets",
            "IdentifierType": "Prefix",
            "Identifiers": [ "s3://MyBucket/", "s3://MyOtherBucket/" ]
        },
        {
            "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_for_AdminGroup",
            "IdentifierType": "Group",
            "Identifiers": [ "AdminGroup" ]
        }
    ]
}
}

```

參數	描述
"AuthorizationConfiguration":	必要.
"EmrFsConfiguration":	必要. 包含角色對應。
"RoleMappings":	必要. 包含一或多個角色對應定義。並會依角色對應出現的順序，由上而下對其評估。若系統在 Amazon S3 中針對資料的 EMRFS 呼叫將角色對應評估為 true，則不會繼續評估角色對應，且 EMRFS 會使用要求的特定 IAM 角色。角色對應包含下列必要參數：
"Role":	指定 IAM 角色的 ARN 識別符，格式為 <code>arn:aws:iam::account-id:role/role-name</code> 。這是在 EMRFS 向 Amazon S3 發出之要求符合任何指定的 Identifiers 時，Amazon EMR 使用的 IAM 角色。
"IdentifierType":	可為下列其中之一： <ul style="list-style-type: none"> "User" 指定識別符為一或多個 Hadoop 使用者，其可為 Linux 帳戶使用者或 Kerberos 委託人。當 EMRFS 在指定使用者的情況下發出要求時，就會使用 IAM 角色。 "Prefix" 指定識別符為 Amazon S3 位置。IAM 角色會用於對具有指定字首之位置的呼叫。例如，字首 <code>s3://mybucket/</code> 與 <code>s3://mybucket/mydir</code> 及 <code>s3://mybucket/yetanotherdir</code> 相符。 "Group" 指定識別符為一或多個 Hadoop 群組。當要求來自指定群組中的使用者時，就會使用 IAM 角色。
"Identifiers":	指定一或多個適當識別符類型的識別符。並使用逗號以不含空格的方式分隔多個識別符。

指定適用於叢集的安全組態

指定安全組態來建立叢集時，您可以指定加密設定。您可以使用 AWS Management Console 或 AWS CLI。

使用主控台指定安全組態

使用 AWS 主控台來建立 EMR 叢集時，您會在進階選項建立程序的 Step 4: Security (步驟 4：安全性) 期間，選擇安全組態。

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)，然後選擇 Go to advanced options (前往進階選項)。
3. 在 Step 1: Software and Steps (步驟 1：軟體和步驟) 的畫面上，從 Release (版本) 清單中，選擇 emr-4.8.0 (emr-4.8.0) 或較新的版本。選擇您想要的設定，然後選擇 Next (下一步)。
4. 在 Step 2: Hardware (步驟 2：硬體) 的畫面上，選擇您想要的設定，接著選擇 Next (下一步)。對 Step 3: General Cluster Settings (步驟 3：一般叢集設定) 執行相同的步驟。
5. 在 Step 4: Security (步驟 4：安全性) 的畫面上的 Encryption Options (加密選項) 中，選擇 Security configuration (安全組態) 的值。
6. 視需要設定其他安全選項，然後選擇 Create cluster (建立叢集)。

使用 CLI 指定安全組態

使用 `aws emr create-cluster` 時，您可以使用 `--security-configuration MySecConfig` 選擇性套用安全組態，其中 `MySecConfig` 是安全組態的名稱，如以下範例所示。指定的 `--release-label` 必須是 4.8.0 或更新版本，且 `--instance-type` 可以是任何可用。

```
aws emr create-cluster --instance-type m5.xlarge --release-label emr-5.0.0 --security-configuration mySecConfig
```

Amazon EMR 的資料保護

Amazon EMR 會遵循 AWS [共同責任模型](#)，此模型包含資料保護的法規和指導。AWS 會負責保護執行所有 AWS 服務的全球基礎設施。AWS 會維持對此基礎設施上託管資料的控制，包含處理客戶內容和個人資料的安全性組態控制。身為資料控制者或資料處理者的 AWS 客戶和 APN 合作夥伴都需負責保護在 AWS 雲端中放置的任何個人資料。

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) 設定個別使用者帳戶，以便每個使用者都只獲得完成其任務所需的許可。我們也建議您以下列方式保護資料：

- 使用 Amazon EMR 加密選項來加密靜態和傳輸中的資料。如需更多詳細資訊，請參閱 [加密靜態和傳輸中的資料 \(p. 144\)](#)。
- 每個帳戶都使用多重驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用進階的受管安全服務，例如 Amazon Macie，其可協助探索和保護存放在 Amazon S3 的個人資料。

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，如 Name (名稱) 欄位。這包括當您使用 Amazon EMR 或使用主控台、API、AWS CLI 或 AWS 開發套件的其他 AWS 服務。您輸入 Amazon EMR 或其他服務的任何資料都可能被選入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在 URL 中包含登入資料資訊，以驗證您對該伺服器的請求。

如需資料保護的詳細資訊，請參閱 AWS 安全性部落格上的 [AWS 共同保護模型和 GDPR 部落格文章](#)。

加密靜態和傳輸中的資料

資料加密有助於防止未經授權的使用者讀取叢集上的資料和相關的資料儲存體系統。這包括儲存到持久性媒體的資料（稱為靜態資料），以及透過網路傳送時可能會被攔截的資料（稱為傳輸中資料）。

從 Amazon EMR 4.8.0 版本開始，您可以使用 Amazon EMR 安全組態設定，更輕鬆地進行叢集的資料加密設定。安全組態提供的設定，可讓傳輸中的資料，以及 Amazon Elastic Block Store (Amazon EBS) 磁碟區中和 Amazon S3 上 EMRFS 中的靜態資料，獲得安全的保障。

或者，從 Amazon EMR 發行版本 4.1.0 和更新版本開始，您可選擇在 HDFS 中設定透明加密，此加密不是使用安全組態進行設定。如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [在 Amazon EMR 上使用 HDFS 中的透明加密](#)。

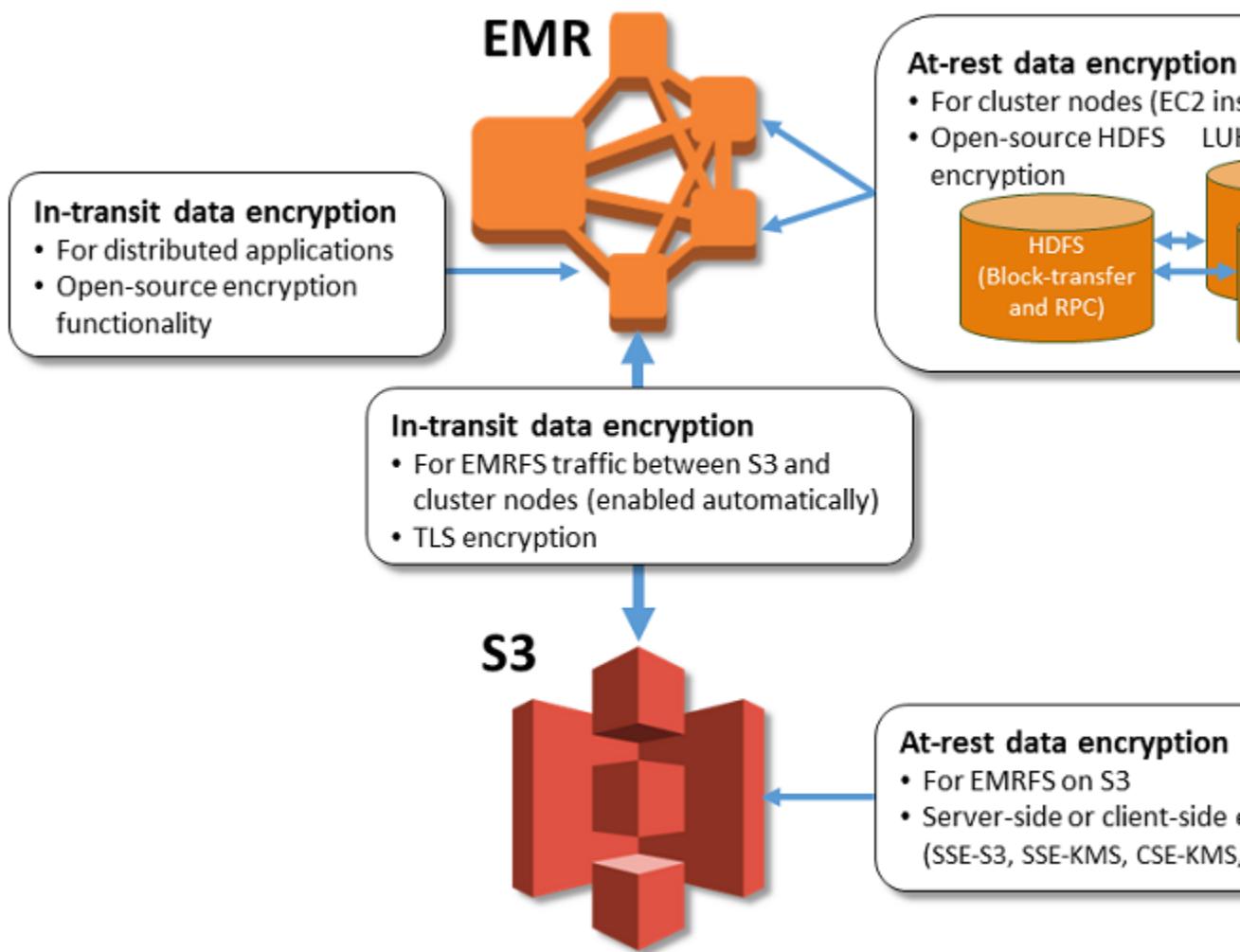
主題

- [加密選項 \(p. 144\)](#)
- [建立資料加密的金鑰和憑證 \(p. 148\)](#)

加密選項

您可以透過 Amazon EMR 4.8.0 版或更新版本，來使用安全組態指定傳輸中資料、靜態資料或兩者的加密設定。啟用靜態資料加密時，您可以選擇對在 Amazon S3 的 EMRFS 資料，在本機磁碟的資料或兩者進行加密。您建立的每個安全組態都存放在 Amazon EMR 中，而非叢集組態中，因此無論何時建立叢集，都可以輕鬆重複使用組態來指定資料加密設定。如需更多詳細資訊，請參閱 [建立安全組態 \(p. 129\)](#)。

下圖顯示安全組態提供的不同資料加密選項。



以下加密選項也可供使用，且未使用安全組態來設定：

- 或者，您可以使用 Amazon EMR 4.1.0 版和更新版本，來選擇在 HDFS 中設定透明加密。如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [在 Amazon EMR 上使用 HDFS 中的透明加密](#)。
- 如果您使用的是不支援安全組態的 Amazon EMR 發行版本，可以在 Amazon S3 中手動設定 EMRFS 資料的加密。如需詳細資訊，請參閱 [使用 EMRFS 屬性來指定 Amazon S3 加密 \(p. 67\)](#)。
- 如果您使用的 Amazon EMR 早於版本 5.24.0，則只有在使用自訂 AMI 時，才支援加密的 EBS 根設備磁碟區。如需詳細資訊，請參閱 Amazon EMR Management Guide 中的 [使用加密的 Amazon EBS 根設備磁碟區建立自訂 AMI](#)。

Note

從 Amazon EMR 5.24.0 版開始，當您指定 AWS KMS 作為您的金鑰提供者時，可以使用安全組態選項以加密 EBS 根設備和儲存磁碟區。如需詳細資訊，請參閱 [本機磁碟加密 \(p. 146\)](#)。

資料加密需要金鑰和憑證。安全組態可讓您以彈性的方式，從數個選項中選擇，包括 AWS Key Management Service 所管理的金鑰、Amazon S3 所管理的金鑰，以及來自您所提供之自訂提供者的金鑰和憑證。使用 AWS KMS 做為您的金鑰提供者時，將適用儲存體及使用加密金鑰的費用。如需詳細資訊，請參閱 [AWS KMS 定價](#)。

指定加密選項前，請決定您想使用的金鑰和憑證管理系統，才能先建立金鑰和憑證或您指定為加密設定一部分的自訂提供者。

Amazon S3 中 EMRFS 資料的靜態加密

Amazon S3 加密適用於讀取和寫入至 Amazon S3 的 EMR 檔案系統 (EMRFS) 物件。啟用靜態加密時，會指定 Amazon S3 伺服器端加密 (SSE) 或用戶端加密 (CSE) 作為 Default encryption mode (預設加密模式)。或者，您可以使用 Per bucket encryption overrides (每個儲存貯體加密覆寫) 為個別儲存貯體指定不同的加密方法。無論是否啟用了 Amazon S3 加密功能，Transport Layer Security (TLS) 都會將 EMR 叢集節點和 Amazon S3 之間傳送中的 EMRFS 物件加密。如需關於 Amazon S3 加密的深入詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的 [使用加密來保護資料](#)。

Amazon S3 伺服器端加密

當您設定 Amazon S3 伺服器端加密時，Amazon S3 會在將資料寫入磁碟時於物件層級予以加密，並在資料受到存取時予以解密。如需 SSE 的詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的「[使用伺服器端加密保護資料](#)」。

當您 在 Amazon EMR 中指定 SSE 時，您有兩個不同的金鑰管理系統可選擇：

- SSE-S3：Amazon S3 會為您管理金鑰。
- SSE-KMS：您使用透過適用於 AWS KMS 之政策所設定的 Amazon EMR 自訂主要金鑰 (CMK)。如需 Amazon EMR 金鑰需求的詳細資訊，請參閱「[使用適用於加密的 AWS KMS 客戶主金鑰 \(CMK\) \(p. 148\)](#)」。當您使用 AWS KMS 時，將適用儲存體及使用加密金鑰的費用。如需詳細資訊，請參閱 [AWS KMS 定價](#)。

使用客戶提供之金鑰的 SSE (SSE-C) 無法搭配 Amazon EMR 使用。

Amazon S3 用戶端加密

使用 Amazon S3 用戶端加密，Amazon S3 加密及解密會在您叢集上的 EMRFS 用戶端進行。物件會在上傳至 Amazon S3 前加密，並在下載之後解密。您指定的提供者會提供用戶端使用的加密金鑰。用戶端可使用由 AWS KMS (CSE-KMS) 提供的金鑰或提供用戶端主要金鑰 (CSE-C) 的自訂 Java 類別。CSE-KMS 和 CSE-C 之間的加密特性有些不同，取決於指定的提供者及要解密或加密之物件的中繼資料。如需這些特性差異的詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的「[使用用戶端加密保護資料](#)」。

Note

Amazon S3 CSE 只會確認與 Amazon S3 交換的 EMRFS 資料已加密。並非叢集執行個體磁碟區上的所有資料都會加密。除此之外，因為 Hue 不使用 EMRFS，所以 Hue S3 檔案瀏覽器寫入 Amazon S3 的物件都不會加密。

本機磁碟加密

當您使用 Amazon EMR 安全組態啟用本機磁碟加密時，下列機制會一起運作來加密本機磁碟。

開放原始碼 HDFS 加密

HDFS 會在分散式處理期間，在叢集執行個體之間交換資料。它也會讀取和寫入資料至執行個體存放磁碟區以及連接到執行個體的 EBS 磁碟區。您啟用本機磁碟加密時，會啟動以下的開放原始碼 Hadoop 加密選項：

- **安全 Hadoop RPC** 設定為「Privacy」，此選項使用 Simple Authentication Security Layer (SASL)。
- **HDFS 區塊資料傳輸的資料加密** 設為 true 並設定為使用 AES 256 加密。

Note

您可以透過啟用傳輸中加密，啟動額外的 Apache Hadoop 加密 (請參閱「[傳輸中加密 \(p. 147\)](#)」)。這些加密設定不會啟動您可手動設定的 HDFS 透明加密。如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [在 Amazon EMR 上使用 HDFS 中的透明加密](#)。

執行個體存放區加密

對於使用 NVMe 型的 SSDs 作為執行個體存放區磁碟區的 EC2 執行個體類型，無論 Amazon EMR 加密設定為何，都會使用 NVMe 加密。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [NVMe SSD 磁碟區](#)。對於其他執行個體存放磁碟區，當本機磁碟加密啟用時，Amazon EMR 使用 LUKS 加密執行個體存放區磁碟區，無論 EBS 磁碟區是使用 EBS 加密或 LUKS 來加密。

EBS 磁碟區加密

如果您在帳戶預設啟用 EBS 磁碟區 Amazon EC2 加密的區域中建立叢集，即使本機磁碟未啟用加密，EBS 磁碟區仍會加密。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [預設加密](#)。當安全組態中啟用本機磁碟加密時，Amazon EMR 設定會優先於叢集 EC2 執行個體的 Amazon EC2 預設加密設定。

下列選項可用於使用安全組態加密 EBS 磁碟區：

- EBS 加密 – 從 Amazon EMR 版本 5.24.0 開始，您可以選擇啟用 EBS 加密。EBS 加密選項會加密 EBS 根設備磁碟區和連接的儲存磁碟區。EBS 加密選項僅在您將 AWS Key Management Service 指定為金鑰提供者時可用。建議使用 EBS 加密。
- LUKS 加密 – 如果您針對 Amazon EBS 選擇使用 LUKS 加密，LUKS 加密只會套用至連接的儲存磁碟區，而不會套用至跟設備跟設備儲存區。如需關於 LUKS 加密的詳細資訊，請參閱 [磁碟上 LUKS 規格](#)。

針對您的金鑰提供者，您可以設定 AWS KMS 客戶主金鑰 (CMK) 適合 Amazon EMR 的政策，或使用提供加密成品的自訂 Java 類別。當您使用 AWS KMS 時，將適用儲存體及使用加密金鑰的費用。如需詳細資訊，請參閱 [AWS KMS 定價](#)。

Note

若要檢查您的叢集是否已啟用 EBS 加密，建議您使用 `DescribeVolumes` API 呼叫。如需詳細資訊，請參閱 [DescribeVolumes](#)。在叢集上執行 `lsblk` 只會檢查 LUKS 加密的狀態，而非 EBS 加密。

傳輸中加密

數種加密機制在使用傳輸中加密時啟用。這些是開放原始碼功能，僅適用特定應用程式，可能會隨 Amazon EMR 版本而異。使用安全組態可啟用下列應用程式專屬加密功能：

- Hadoop (如需詳細資訊，請參閱 Apache Hadoop 文件中的 [處於安全模式的 Hadoop](#))：
 - [Hadoop MapReduce 加密混洗](#)使用 TLS。
 - [安全 Hadoop RPC](#) 設定為「隱私」，並使用 SASL (靜態加密啟用時在 Amazon EMR 中啟動)。
 - [HDFS 區塊資料傳輸的資料加密](#)使用 AES 256 (以安全組態啟用靜態加密時，會在 Amazon EMR 中啟動)。
- HBase：
 - 當 Kerberos 啟用時，`hbase.rpc.protection` 屬性是設為 `privacy` 以用於加密通訊。如需詳細資訊，請參閱 Apache HBase 文件中的 [適用於安全操作的用戶端組態](#)。如需關於 Kerberos 搭配 Amazon EMR 的詳細資訊，請參閱 [使用 Kerberos 身份驗證 \(p. 190\)](#)。
- Presto：
 - Presto 節點之間的內部通訊使用 SSL/TLS (僅限 Amazon EMR 5.6.0 版本和更新版本)。
- Tez：

- Tez 混洗處理常式使用 TLS (`tez.runtime.ssl.enable`)。
- Spark (如需詳細資訊，請參閱 [Spark 安全設定](#))：
 - 會使用在 Amazon EMR 5.9.0 版本和更新版本中的 AES-256 密碼來加密 Spark 元件之間的內部 RPC 通訊 (例如區塊傳輸服務和外部混洗服務)。在較早版本中，內部 RPC 通訊使用 SASL 搭配 DIGEST-MD5 做為密碼進行加密。
 - HTTP 協定通訊具有例如 Spark 歷史記錄伺服器和已啟用 HTTPS 檔案伺服器的使用者介面，使用 Spark 的 SSL 組態進行加密。如需詳細資訊，請參閱 [Spark 文件中的 SSL 組態](#)。

您可透過下列兩種方法之一指定用於傳輸中加密的加密成品：提供您上傳到 Amazon S3 的憑證壓縮檔案，或參考提供加密成品的自訂 Java 類別。如需更多詳細資訊，請參閱 [使用 Amazon EMR 加密提供傳輸中資料的加密憑證 \(p. 150\)](#)。

建立資料加密的金鑰和憑證

使用安全組態指定加密選項之前，決定您想要使用的金鑰和加密成品提供者。例如，您可以使用 AWS KMS 或您建立的自訂提供者。接著，如本區段所述，建立金鑰或金鑰提供者。

使用 Amazon EMR 提供靜態資料的加密金鑰

您可以針對 Amazon EMR 中的靜態資料加密，使用 AWS Key Management Service (AWS KMS) 或自訂的金鑰提供者。當您使用 AWS KMS 時，將適用儲存體及使用加密金鑰的費用。如需詳細資訊，請參閱 [AWS KMS 定價](#)。

本主題提供金鑰政策的詳細資訊，AWS KMS CMK 搭配 Amazon EMR 使用時會用到，並提供準則和程式碼範例，以說明如何針對 Amazon S3 加密編寫自訂的金鑰提供者類別。如需建立資料的詳細資訊，請參閱 [AWS Key Management Service Developer Guide](#)中的 [建立金鑰](#)。

使用適用於加密的 AWS KMS 客戶主金鑰 (CMK)

建立 AWS KMS 加密金鑰的區域必須與您搭配 EMRFS 使用之 Amazon EMR 叢集執行個體及 Amazon S3 儲存貯體的區域相同。若您指定之金鑰的所在帳戶與您用來設定叢集的帳戶不同，則您必須使用金鑰的 ARN 來指定金鑰。

Amazon EC2 執行個體描述檔的角色需有權使用您指定的 CMK。Amazon EMR 中執行個體描述檔的預設角色為 `EMR_EC2_DefaultRole`。若您為執行個體描述檔使用其他角色，或向 Amazon S3 請求使用 EMRFS 的 IAM 角色，請務必適當地將每個角色新增為金鑰使用者。此操作能授予角色使用 CMK 的權限。如需詳細資訊，請參閱 [AWS Key Management Service Developer Guide](#)中的 [使用金鑰政策及叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#)。

您可以使用 AWS Management Console 將您的執行個體描述檔或 EC2 執行個體描述檔新增至指定 AWS KMS CMK 的金鑰使用者清單，或是您也可以使用 AWS CLI 或 AWS 開發套件來連接適當的金鑰政策。

下列程序說明如何使用 AWS Management Console 將預設 EMR 執行個體描述檔「`EMR_EC2_DefaultRole`」新增為金鑰使用者。這裡假設您已建立了 CMK。若要建立新的 CMK，請參閱 [AWS Key Management Service Developer Guide](#)中的 [建立金鑰](#)。

若要將 Amazon EMR 的 EC2 執行個體描述檔新增至加密金鑰使用者的清單

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at <https://console.aws.amazon.com/kms>.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. 選取要修改的 CMK 別名。
4. 在 Key Users (金鑰使用者) 下的金鑰詳細資訊頁面上，選擇 Add (新增)。
5. 在 Attach (連接) 對話方塊中，選取適當的角色。預設角色的名稱為 `EMR_EC2_DefaultRole`。

6. 選擇 Attach (連接)。

為 AWS KMS CMK 提供額外的許可來啟用 EBS 加密

從 Amazon EMR 版本 5.24.0 開始，您可以使用安全組態選項來加密 EBS 根設備和儲存磁碟區。若要啟用這類選項，您必須指定 AWS KMS 做為您的金鑰提供者。此外，您必須授予 EMR 服務角色 `EMR_DefaultRole` 使用您指定的客戶主金鑰 (CMK) 的許可。

您可以使用 AWS Management Console 將 EMR 服務角色新增至指定 AWS KMS CMK 的金鑰使用者清單，或者您可以使用 AWS CLI 或 AWS 開發套件來連接適當的金鑰政策。

下列程序說明如何使用 AWS Management Console 將預設 EMR 服務角色「`EMR_DefaultRole`」新增為金鑰使用者。這裡假設您已建立了 CMK。若要建立新的 CMK，請參閱 AWS Key Management Service Developer Guide 中的[建立金鑰](#)。

將 EMR 服務角色新增至加密金鑰使用者清單

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at <https://console.aws.amazon.com/kms>.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. 選取要修改的 CMK 別名。
4. 在 Key Users (金鑰使用者) 下的金鑰詳細資訊頁面上，選擇 Add (新增)。
5. 在 Attach (連接) 對話方塊中，選取適當的角色。預設 EMR 服務角色的名稱為 `EMR_DefaultRole`。
6. 選擇 Attach (連接)。

建立自訂金鑰提供者

使用安全組態時，您必須為本機磁碟加密和 Amazon S3 加密指定不同的提供者類別名稱。

當您建立自訂金鑰提供者時，應用程式應實作可在 AWS SDK for Java 1.11.0 版及更新版本中使用的 [EncryptionMaterialsProvider 介面](#)。該實作可使用任何策略來提供加密材料。例如，您可以選擇提供靜態加密材料或與更複雜的金鑰管理系統整合。

用於自訂加密材料的加密演算法必須是 AES/GCM/NoPadding。

EncryptionMaterialsProvider 類別會透過加密內容取得加密材料。Amazon EMR 會在執行時間填入加密內容資訊，以協助發起人決定要傳回的正確加密材料。

Example 範例：使用自訂金鑰提供者進行使用 EMRFS 的 Amazon S3 加密

當 Amazon EMR 從 EncryptionMaterialsProvider 類別擷取加密材料以執行加密時，EMRFS 會選擇性地將兩個欄位填入 materialsDescription 引數：物件的 Amazon S3 URI 及叢集的 JobFlowId，這可讓 EncryptionMaterialsProvider 類別用來選擇性的傳回加密材料。

例如，提供者可針對不同的 Amazon S3 URI 字首傳回不同的金鑰。最後使用 Amazon S3 物件儲存的是傳回加密材料的描述，而非由 EMRFS 產生並傳遞給提供者的 materialsDescription 值。在解密 Amazon S3 物件時，會傳遞加密材料描述給 EncryptionMaterialsProvider 類別，以便其可再次選擇性地傳回相符的金鑰來解密物件。

EncryptionMaterialsProvider 參考實作如下所示。另一個自訂提供者 [EMRFSRSAEncryptionMaterialsProvider](#) 的參考實作則提供於 GitHub。

```
import com.amazonaws.services.s3.model.EncryptionMaterials;
import com.amazonaws.services.s3.model.EncryptionMaterialsProvider;
import com.amazonaws.services.s3.model.KMSEncryptionMaterials;
import org.apache.hadoop.conf.Configurable;
```

```
import org.apache.hadoop.conf.Configuration;
import java.util.Map;

/**
 * Provides KMSEncryptionMaterials according to Configuration
 */
public class MyEncryptionMaterialsProvider implements EncryptionMaterialsProvider,
Configurable{
    private Configuration conf;
    private String kmsKeyId;
    private EncryptionMaterials encryptionMaterials;

    private void init() {
        this.kmsKeyId = conf.get("my.kms.key.id");
        this.encryptionMaterials = new KMSEncryptionMaterials(kmsKeyId);
    }

    @Override
    public void setConf(Configuration conf) {
        this.conf = conf;
        init();
    }

    @Override
    public Configuration getConf() {
        return this.conf;
    }

    @Override
    public void refresh() {

    }

    @Override
    public EncryptionMaterials getEncryptionMaterials(Map<String, String>
materialsDescription) {
        return this.encryptionMaterials;
    }

    @Override
    public EncryptionMaterials getEncryptionMaterials() {
        return this.encryptionMaterials;
    }
}
```

使用 Amazon EMR 加密提供傳輸中資料的加密憑證

使用 Amazon EMR 4.8.0 版本或更新版本時，對於使用安全組態的傳輸中資料加密，指定成品的選項有兩種：

- 您可以手動建立 PEM 憑證，將這些憑證包含在 zip 檔案內，然後在 Amazon S3 中參考此 zip 檔案。
- 您可以實作自訂憑證提供者為 Java 類別。您可以在 Amazon S3 中指定應用程式的 JAR 檔案，然後提供如應用程式中所宣告的提供者完整類別名稱。此類別必須實作從 AWS SDK for Java 1.11.0 版開始提供的 [TLSArtifactsProvider](#) 界面。

Amazon EMR 會自動下載成品到叢集中的每個節點，並在稍後用於實作開放原始碼的傳輸中加密功能。如需可用選項的詳細資訊，請參閱「[傳輸中加密 \(p. 147\)](#)」。

使用 PEM �凭證

您為傳輸中加密指定 zip 檔案時，安全組態預期該 zip 檔案中的 PEM 檔案會完全以下方所顯示的命名：

傳輸中加密憑證

檔案名稱	必要/選用	詳細資訊
privateKey.pem	必要	私有金鑰
certificateChain.pem	必要	憑證鏈
trustedCertificates.pem	選用	若提供的憑證不是由 Java 預設信任的根認證機構 (CA) 所簽署，或由可連結至 Java 預設信任根 CA 的中繼 CA 所簽署，則此為必要。Java 預設可信任的根 CA 可在 <code>jre/lib/security/cacerts</code> 中找到。

您可能會想要設定私有金鑰 PEM 檔案為萬用字元憑證，以允許存取您叢集執行個體所在的 Amazon VPC 網域。例如，如果您的叢集位於 us-east-1 (維吉尼亞北部)，您可能會選擇在憑證組態中指定常見名稱，該組態會透過在憑證主體定義中指定 `CN=*.ec2.internal`，來允許存取該叢集。如果您的叢集位於 us-west-2 (奧勒岡)，可以指定 `CN=*.us-west-2.compute.internal`。如需 Amazon VPC 內 EMR 叢集組態的詳細資訊，請參閱[選擇叢集的 Amazon VPC 子網路](#)。

下列範例示範如何使用 OpenSSL 來產生自簽 X.509 憑證 (使用 1024 位元的 RSA 私密金鑰)。金鑰可允許存取發行者在 us-west-2 (奧勒岡) 區域中的 Amazon EMR 叢集執行個體，如 `*.us-west-2.compute.internal` 將網域名稱指定為常見名稱。

也會指定選用的其他主體項目，例如國家/地區 (C)、州 (S)、地區 (L)。由於已經產生自我簽署憑證，範例中的第二個指令會將 `certificateChain.pem` 檔案複製到 `trustedCertificates.pem` 檔案。第三個指令會使用 `zip` 來建立包含憑證的 `my-certs.zip` 檔案。

Important

此範例僅為概念驗證示範。自我簽署憑證並不建議使用，且可能具有安全風險。若為生產系統，請使用信任的憑證授權機構 (CA) 發行憑證。

```
$ openssl req -x509 -newkey rsa:1024 -keyout privateKey.pem -out certificateChain.pem
  -days 365 -nodes -subj '/C=US/ST=Washington/L=Seattle/O=MyOrg/OU=MyDept/CN=*.us-
west-2.compute.internal'
$ cp certificateChain.pem trustedCertificates.pem
$ zip -r -X my-certs.zip certificateChain.pem privateKey.pem trustedCertificates.pem
```

適用於 Amazon EMR 的 AWS Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制 AWS 資源的存取。IAM 管理員可以控制能進行身份驗證 (登入) 及獲得授權 (具備許可) 以使用 Amazon EMR 資源的人員。IAM 是一種 AWS 服務，無須支付任何額外的費用即可使用。

主題

- [對象 \(p. 152\)](#)
- [使用身分來驗證 \(p. 152\)](#)
- [使用政策管理存取權 \(p. 153\)](#)
- [Amazon EMR 如何搭配 IAM 運作 \(p. 154\)](#)

- 將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 (p. 156)
- Amazon EMR 身分類型政策範例 (p. 179)

對象

根據您在 Amazon EMR 中所進行的工作而定，AWS Identity and Access Management (IAM) 的使用方式會不同。

服務使用者 – 若您使用 Amazon EMR 來執行您的作業，您的管理員可以提供您需要的登入資料和許可。隨著您為了執行作業而使用的 Amazon EMR 功能數量變多，您可能會需要額外的許可。了解存取控制的管理方式可協助您向管理員請求正確的許可。

服務管理員 – 若您是負責管理您公司的 Amazon EMR 資源，您應該會具備 Amazon EMR 的完整存取權限。您的任務是判斷您員工應存取的 Amazon EMR 功能及資源。您接著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。若要進一步了解您公司可搭配 IAM 使用 Amazon EMR 的方式，請參閱 [Amazon EMR 如何搭配 IAM 運作 \(p. 154\)](#)。

IAM 管理員 – 如果您是 IAM 管理員，請了解如何撰寫政策來管理 Amazon EMR 存取的詳細資訊。若要檢視您可以在 IAM 中使用的範例 Amazon EMR 身分類型政策，請參閱 [Amazon EMR 身分類型政策範例 \(p. 179\)](#)。

使用身分來驗證

身份驗證是使用身分登入資料登入 AWS 的方式。如需使用 AWS Management Console 登入的詳細資訊，請參閱 IAM User Guide 中的 [IAM 主控台及登入頁面](#)。

您必須以 AWS account root user、IAM 使用者，或取得 IAM 角色身分的方式進行身份驗證 (登入 AWS)。您也可以使用貴公司的單一登入身分驗證，甚至使用 Google 或 Facebook 進行登入。在上述案例中，您的管理員會使用 IAM 角色預先設定聯合身分。當您使用來自其他公司的身份驗證來存取 AWS 時，您是間接地擔任角色。

若要直接登入 [AWS Management Console](#)，請使用您的密碼及您的 root user 電子郵件或您的 IAM 使用者名稱。您可以使用您的 root user 或 IAM 使用者存取金鑰，透過編寫程式的方式存取 AWS。AWS 提供軟體開發套件和命令列工具，以加密的方式使用您的登入資料簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。請使用 Signature 第 4 版來執行此作業，它是針對傳入 API 請求進行身份驗證的通訊協定。如需驗證請求的詳細資訊，請參閱 AWS General Reference 中的 [Signature 第 4 版簽署程序](#)。

無論您使用何種身份驗證方法，您可能還需要提供額外的安全性資訊。例如，AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全。若要進一步了解，請參閱 IAM User Guide 中的 [在 AWS 中使用多重驗證 \(MFA\)](#)。

AWS Account Root User

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](#). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶中的一種實體，具備單一人員或應用程式的特定許可。IAM 使用者可有長期登入資料 (例如，使用者名稱和密碼或一組存取金鑰)。若要了解如何產生存取金鑰，請參閱 IAM User Guide 中的 [管理 IAM 使用者的存取金鑰](#)。當您產生 IAM 使用者的存取金鑰時，請確認您已檢視且安全地儲存金鑰對。您在這之後便無法復原私密存取金鑰。屆時您必須改為產生新的存取金鑰對。

IAM 群組是一種指定 IAM 使用者集合的實體。您無法以群組身分登入。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過程變得更為容易。例如，您可以擁有一個名為 IAMAdmin 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登入資料，但角色僅提供暫時登入資料。若要進一步了解，請參閱 IAM User Guide 中的 [建立 IAM 使用者 \(而非角色\) 的時機](#)。

IAM 角色

IAM 角色是您 AWS 帳戶中的一種實體，具備特定許可。它與 IAM 使用者相似，但是不會與特定人員建立關聯。您可以在 AWS Management Console 中透過[切換角色](#)來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱 IAM User Guide 中的 [使用 IAM 角色](#)。

使用臨時登入資料的 IAM 角色在下列情況中非常有用：

- **暫時 IAM 使用者許可** – IAM 使用者可以取得 IAM 角色來暫時針對特定任務具備不同的許可。
- **聯合身分使用者存取** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an [identity provider](#). For more information about federated users, see [Federated Users and Roles](#) in the IAM User Guide.
- **跨帳戶存取** – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶的資源。角色是授予跨帳戶存取的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色做為代理)。若要了解跨帳戶存取角色和資源類型政策間的差異，請參閱 IAM User Guide 中的 [IAM 角色與資源類型政策的差異](#)。
- **AWS 服務存取** – A service role is an IAM role that a service assumes to perform actions in your account on your behalf. When you set up some AWS service environments, you must define a role for the service to assume. This service role must include all the permissions that are required for the service to access the AWS resources that it needs. Service roles vary from service to service, but many allow you to choose your permissions as long as you meet the documented requirements for that service. Service roles provide access only within your account and cannot be used to grant access to services in other accounts. You can create, modify, and delete a service role from within IAM. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see [Creating a Role to Delegate Permissions to an AWS Service](#) in the IAM User Guide.
- **在 Amazon EC2 上執行的應用程式** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances](#) in the IAM User Guide.

若要了解是否要使用 IAM 角色，請參閱 IAM User Guide 中的 [建立 IAM 角色 \(而非使用者\) 的時機](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到 IAM 身分或 AWS 資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和實體或資源建立關聯時，便可定義其許可。AWS 會在實體 (root user、IAM 使用者或 IAM 角色) 發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式存放在 AWS 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM User Guide 中的 [JSON 政策概觀](#)。

IAM 管理員可以使用政策指定能存取 AWS 資源的人員，以及他們能在這些資源上執行的動作。每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。換句話說，根據預設，使用者無法執行任何作業，甚至也無法變更

他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策連接到使用者。或者，管理員可以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

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。具備該政策的使用者便可以從 AWS Management Console、AWS CLI 或 AWS API 取得使用者資訊。

以身分為基礎的政策

身分類型政策是您可以連接到身分（例如 IAM 使用者、角色或群組）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。若要了解如何建立身分類型政策，請參閱 IAM User Guide 中的 [建立 IAM 政策](#)。

身分類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。受管政策則是獨立的政策，您可以將這些政策連接到 AWS 帳戶中的多個使用者、群組和角色。受管政策包含 AWS 受管政策和客戶受管政策。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM User Guide 中的 [在受管政策和內嵌政策間選擇](#)。

其他政策類型

AWS 支援其他較少見的政策類型。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 – 許可界限是一種進階功能，可供您設定身分類型政策能授予 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類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類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 User Guide》中的 [IAM 實體的許可界限](#)。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位的最大許可。AWS Organizations 是一種用來群組和集中管理您商業所擁有多個 AWS 的一項服務。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 AWS account root user。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations User Guide》中的 [SCP 的運作方式](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合身分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類型政策和工作階段政策的交集。許可也可以來自資源類型政策。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 User Guide 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 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱 IAM User Guide 中的 [政策評估邏輯](#)。

Amazon EMR 如何搭配 IAM 運作

使用 IAM 身分類型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下會允許或拒絕動作。Amazon EMR 支援特定動作、資源及條件金鑰。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM User Guide 中的 [IAM JSON 政策元素參考](#)。

Amazon EMR 不支援資源類型政策。

動作

IAM 身分類型政策的 Action 元素會描述政策將允許或拒絕的特定動作。政策動作的名稱通常會和相關聯的 AWS API 操作相同。政策會使用動作來授予執行相關聯操作的許可。

Amazon EMR 中的政策動作會在動作前使用以下前綴：`elasticmapreduce:`。例如，若要授予某人使用 `RunJobFlow` API 操作建立叢集的許可，請在其政策中加入 `elasticmapreduce:RunJobFlow` 動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon EMR 會定義一組自己的動作，來描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

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

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "elasticmapreduce:Describe*"
```

若要查看 Amazon EMR 動作的清單，請參閱 IAM User Guide中的 [Actions Defined by Amazon EMR](#)。

資源

`Resource` 元素可指定動作套用的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。您可以使用 ARN 來指定資源，或是使用萬用字元 (*) 來指定陳述式套用到所有資源。

若要查看 Amazon EMR 資源類型的清單及其 ARN，請參閱 IAM User Guide中的 [Resources Defined by Amazon EMR](#)。您若要了解您可以使用哪些動作指定每項資源的 ARN，請參閱 [Actions Defined by Amazon EMR](#)。

條件金鑰

`Condition` 元素 (或 `Condition` 「區塊」) 可讓您指定使陳述式生效的條件。`Condition` 元素是選用的。您可以建置使用 [條件運算子](#) 的條件表達式 (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` 元素中指定多個金鑰，AWS 會使用邏輯 AND 操作評估他們。若您為單一條件金鑰指定多個值，AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才會授予陳述式的許可。

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。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

Amazon EMR 會定義自己的一組條件金鑰，也支援一些全域條件金鑰的使用。若要查看所有 AWS 全域條件金鑰，請參閱 IAM User Guide中的 [AWS 全域條件內容金鑰](#)。

所有 Amazon EC2 動作均支援 `aws:RequestedRegion` 和 `ec2:Region` 條件金鑰。如需詳細資訊，請參閱範例：[將存取限制在特定區域](#)。

若要查看 Amazon EMR 條件金鑰的清單，請參閱 IAM User Guide中的 [Condition Keys for Amazon EMR](#)。若要了解您可以針對何種動作及資源使用條件金鑰，請參閱 [Actions Defined by Amazon EMR](#)。

使用叢集和筆記本標籤搭配 IAM 政策來進行存取控制

可使用以標籤為基礎的存取控制搭配以身分為基礎的 IAM 政策來微調與 EMR 筆記本 和 EMR 叢集關聯的 Amazon EMR 動作許可。您可以利用 `Condition` 元素 (也稱為 `Condition` 區塊) 中的條件金鑰，只在筆記本、叢集或這兩者，皆具有特定的標籤索引鍵或索引鍵/值的組合時，才允許某些動作。您也可以限制 `CreateEditor` 動作 (此動作會建立 EMR 筆記本) 和 `RunJobFlow` 動作 (此動作會建立叢集)，在資源建立時必須提交標籤的請求。

在 Amazon EMR 中，可在 `Condition` 元素中使用的條件金鑰只適用於 `ClusterID` 或 `NotebookID` 是必要請求參數的 Amazon EMR API 動作。例如，[ModifyInstanceGroups](#) 動作不支援上下文索引鍵，因為 `ClusterID` 是一個選用的參數。

建立 EMR 筆記本時，會套用預設的標籤，將索引鍵字串 `creatorUserId` 設定為 IAM 使用者 ID (建立筆記本的使用者) 的值。在施加限制，只允許筆記本的建立者執行動作時，這項功能非常地實用。

Amazon EMR 中提供以下條件金鑰：

- 利用 `elasticmapreduce:ResourceTag/TagKeyString` 條件上下文索引鍵，來允許或拒絕使用者對叢集或筆記本 (其標籤具有您所指定 `TagKeyString`) 所進行的動作。如果動作會同時傳遞 `clusterID` 和 `NotebookID`，則條件同時適用於叢集和筆記本。這代表兩個資源都必須具有您指定的標籤索引鍵字串或索引鍵/值組合。您可以使用 `Resource` 元素來限制陳述式，如此就能根據需要，只套用到叢集或筆記本。如需詳細資訊，請參閱 [Amazon EMR 身分類型政策範例 \(p. 179\)](#)。
- 使用 `elasticmapreduce:RequestTag/TagKeyString` 條件內容金鑰，要求具有動作/API 呼叫的特定標籤。例如，您可以利用此條件上下文索引鍵和 `CreateEditor` 動作，來要求將具有 `TagKeyString` 的索引鍵，在筆記本建立時套用到其中。

範例

若要檢視 Amazon EMR 身分類型政策的範例，請參閱 [Amazon EMR 身分類型政策範例 \(p. 179\)](#)。

將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源

Amazon EMR 和應用程式 (例如 Hadoop 和 Spark) 需要許可，才可存取其他 AWS 資源和在它們執行時執行動作。Amazon EMR 中的每個叢集都必須有服務角色和適用於 Amazon EC2 執行個體描述檔的角色。連接到這些角色的 IAM 政策提供對叢集的許可，可代表使用者與其他 AWS 服務相互運作。

如果您的叢集在 Amazon EMR 中使用自動擴展，則需要額外的角色 (Auto Scaling 角色)。如果您使用 EMR 筆記本，EMR 筆記本的 AWS 服務角色是必要的。如需詳細資訊，請參閱 [IAM User Guide 中的 IAM 角色和使用執行個體描述檔](#)。

Amazon EMR 為每個決定許可的角色提供預設角色和預設的受管政策。AWS 會建立和維護受管政策，所以如果服務需求改變，這些政策也會自動更新。

如果您是第一次在帳戶中建立叢集或筆記本，Amazon EMR 的角色尚未存在。在您建立它們後，您可以查看角色、連接到他們的政策，以及政策在 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 中允許或拒絕的許可。您可以指定要讓 Amazon EMR 建立和使用的預設角色，可以在建立叢集以自訂許可時建立自己的角色並個別指定，也可以指定使用 AWS CLI 建立叢集時要使用的預設角色。如需詳細資訊，請參閱 [自訂 IAM 規則 \(p. 171\)](#)。

修改以身分為基礎的政策以許可傳遞 Amazon EMR 的服務角色

叢集使用者需要應用程式的許可，才能代表他們傳遞 Amazon EMR 的服務角色。`AmazonElasticMapReduceFullAccess` 許可政策是預設受管政策，可讓使用者擁有 `iam:PassRole` 的完整許可，且該政策所包含的陳述式允許所有資源的 Amazon EMR 許可。此陳述式允許使用者將任何角色傳遞給其他 AWS 服務，使 Amazon EMR 可代表該使用者與那些服務互動。

若要實作更具限制性的政策，請將允許 `iam:PassRole` 只能傳遞 Amazon EMR 角色的內嵌政策連接到適當的使用者或群組。下列範例示範僅允許 `iam:PassRole` 許可傳遞以下預設 Amazon EMR 角色的陳述式：`EMR_DefaultRole`、`EMR_EC2_DefaultRole` 及 `EMR_AutoScalingDefaultRole`。若您使用自訂角色，請將預設角色名稱取代為您的自訂角色名稱。

```
{  
    "Action": "iam:PassRole",  
    "Effect": "Allow",  
    "Resource": [  
        "arn:aws:iam::*:role/EMR_DefaultRole",  
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",  
        "arn:aws:iam::*:role/EMR_AutoScalingDefaultRole",  
    ]  
}
```

```
    "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",  
    "arn:aws:iam::*:role/EMR_Notebooks_DefaultRole  
}  
]
```

服務角色摘要

下表列出 Amazon EMR 相關的 IAM 服務角色以供快速參考。

函數	預設角色	敘述	預設受管政策
Amazon EMR 服務角色 (EMR 角色) (p. 159)	<code>EMR_DefaultRole</code>	允許 Amazon EMR 在佈建資源和執行服務層級動作時代表您呼叫其他 AWS 服務。所有叢集皆需要這個角色。	<code>AmazonElasticMapReduceRole</code> Important 請求 Spot 執行個體需要服務連結角色。如果此角色不存在，則 EMR 服務角色必須有建立之的許可，否則會發生許可錯誤。 受管政策包含陳述式，以允許此動作。如果您自訂此角色或政策，請務必包含陳述式，其可建立此服務連結的角色。如需詳細資訊，請參閱在 Amazon EC2 User Guide for Linux Instances 中的 Amazon EMR 服務角色 (EMR 角色) (p. 159) 和 Spot 執行個體請求的服務連結角色 。
叢集 EC2 執行個體的服務角色 (EC2 執行個體描述檔) (p. 161)	<code>EMR_EC2_DefaultRole</code>	在叢集執行個體的 Hadoop 生態系統上執行的應用程式程序會在呼叫其他 AWS 服務時使用此角色。對於使用 EMRFS 在 Amazon S3 中存取資料，您可以根據發出請求的使用者或群組或根據在 Amazon S3 中的資料位置來指定要擔任的不同角色。如需更多詳細資訊，請參閱 設定用來向 Amazon S3 請求使用 EMRFS 的	<code>AmazonElasticMapReduceforEC2Role</code> 如需詳細資訊，請參閱 叢集 EC2 執行個體的服務角色 (EC2 執行個體描述檔) (p. 161) 。

函數	預設角色	敘述	預設受管政策
		IAM 角色 (p. 174)。 所有叢集皆需要這個角色。	
EMR 中自動擴展的服務角色 (自動擴展角色) (p. 165)	EMR_AutoScaling_DefaultRole	預允許其他動作來動態擴展環境。對於在 Amazon EMR 中使用自動擴展的叢集才需要此項目。如需更多詳細資訊，請參閱 於 Amazon EMR 使用自動調整規模 (p. 291) 。	AmazonElasticMapReduceforAutoScalingPolicy 如需詳細資訊，請參閱 EMR 中自動擴展的服務角色 (自動擴展角色) (p. 165) 。
EMR 筆記本 的服務角色 (p. 165)	EMR_Notebooks_DefaultRole	提供 EMR 筆記本 存取其他 AWS 資源和執行動作所需的許可。只有在使用 EMR 筆記本 時需要。	AmazonElasticMapReduceEditorsPolicy 如需更多詳細資訊，請參閱 EMR 筆記本 的服務角色 (p. 165) 。 根據預設，也會連接 S3FullAccessPolicy。此政策的內容顯示如下。 <pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "s3:*", "Resource": "*" }] }</pre>
服務連結角色 (p. 166)	AWSServiceRoleForEMR	Amazon EMR 會自動建立服務連結角色。如果 Amazon EMR 服務已失去清除 Amazon EC2 資源的能力，Amazon EMR 可以使用此角色來清除。如果叢集使用 Spot 執行個體，連接到 Amazon EMR 服務角色 (EMR 角色) (p. 159) 的許可政策必須允許建立服務連結角色。如需詳細資訊，請參閱 Amazon EMR 服務連結角色許可 (p. 167) 。	AmazonEMRCleanupPolicy

主題

- [Amazon EMR 使用的 IAM 服務角色 \(p. 159\)](#)

- 自訂 IAM 規則 (p. 171)
 - 設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 (p. 174)
 - 使用 Amazon EMR Access to AWS Glue 資料目錄 的資源類型政策 (p. 177)
 - 使用 IAM 角色搭配會直接呼叫 AWS 服務的應用程式 (p. 178)
 - 允許使用者和群組以建立和修改角色 (p. 178)

Amazon EMR 使用的 IAM 服務角色

Amazon EMR 在佈建叢集資源、執行應用程式、動態擴展資源，以及建立和執行 EMR 筆記本 時，代表您使用 IAM 服務角色執行動作。Amazon EMR 與其他與 AWS 服務互動時使用以下角色。每個角色在 Amazon EMR 內都有唯一的函數。本節的主題描述角色函數，並提供每個角色的預設角色和許可政策。

如果您在叢集上有會直接呼叫 AWS 的應用程式程式碼，您可能需要使用軟體開發套件來指定角色。如需更多詳細資訊，請參閱 [使用 IAM 角色搭配會直接呼叫 AWS 服務的應用程式 \(p. 178\)](#)。

主題

- Amazon EMR 服務角色 (EMR 角色) (p. 159)
 - 叢集 EC2 執行個體的服務角色 (EC2 執行個體描述檔) (p. 161)
 - EMR 中自動擴展的服務角色 (自動擴展角色) (p. 165)
 - EMR 筆記本 的服務角色 (p. 165)
 - 使用 Amazon EMR 的服務連結角色 (p. 166)

Amazon EMR 服務角色 (EMR 角色)

EMR 角色會在佈建資源和執行服務層級的任務 (這些任務不會在執行叢集之 EC2 執行個體的細節中執行) 時，定義 Amazon EMR 允許的動作。例如，服務角色用於在叢集啟動時佈建 EC2 執行個體。

- 預設角色為 EMR_DefaultRole。
 - 連接到 EMR_DefaultRole 的預設受管政策是 AmazonElasticMapReduceRole

AmazonElasticMapReduceRole 第 9 版內容如下所示。

```
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeSpotPriceHistory",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcs",
"ec2:DetachNetworkInterface",
"ec2:ModifyImageAttribute",
"ec2:ModifyInstanceStateAttribute",
"ec2:RequestSpotInstances",
"ec2:RevokeSecurityGroupEgress",
"ec2:RunInstances",
"ec2:TerminateInstances",
"ec2:DeleteVolume",
"ec2:DescribeVolumeStatus",
"ec2:DescribeVolumes",
"ec2:DetachVolume",
"iam:GetRole",
"iam:GetRolePolicy",
"iam>ListInstanceProfiles",
"iam>ListRolePolicies",
"iam:PassRole",
"s3>CreateBucket",
"s3:Get*",
"s3>List*",
"sdb:BatchPutAttributes",
"sdb:Select",
"sqs>CreateQueue",
"sqs>Delete*",
"sqs:GetQueue*",
"sqs:PurgeQueue",
"sqs:ReceiveMessage",
"cloudwatch:PutMetricAlarm",
"cloudwatch:DescribeAlarms",
"cloudwatch:DeleteAlarms",
"application-autoscaling:RegisterScalableTarget",
"application-autoscaling:DeregisterScalableTarget",
"application-autoscaling:PutScalingPolicy",
"application-autoscaling:DeleteScalingPolicy",
"application-autoscaling:Describe*"
]
},
{
    "Effect": "Allow",
    "Action": "iam>CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/AWSServiceRoleForEC2Spot*",
    "Condition": {
        "StringLike": {
            "iam:AWSPropertyName": "spot.amazonaws.com"
        }
    }
}
]
```

叢集 EC2 執行個體的服務角色 (EC2 執行個體描述檔)

叢集 EC2 執行個體的服務角色（也稱為 Amazon EMR 的 EC2 執行個體設定檔）是一種特殊類型的服務角色，它會在執行個體啟動時指派給 Amazon EMR 叢集中的每個 EC2 執行個體。在 Hadoop 生態系統上執行的應用程式會擔任此角色，以取得與其他 AWS 服務互動的許可。

如需有關 EC2 執行個體服務角色的詳細資訊，請參閱 IAM User Guide 中的 [使用 IAM 角色將許可授予給 Amazon EC2 執行個體上執行的應用程式](#)。

Important

其使用的預設叢集 EC2 執行個體的服務角色和受管政策所設定的許可可讓您輕鬆地建立功能完整的叢集。我們強烈建議您修改此政策，以提供應用程式所需的最低權限。如需詳細資訊，請參閱 [為叢集 EC2 執行個體建立擁有最低權限許可的服務角色 \(p. 162\)](#)。

預設角色和受管政策

- 預設角色為 EMR_EC2_DefaultRole。
 - 連接到 EMR EC2 DefaultRole 的預設受管政策是 AmazonElasticMapReduceforEC2Role

AmazonElasticMapReduceforEC2Role 第 3 版內容如下所示。

```
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue>CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
    ]
}
]
```

為叢集 EC2 執行個體建立擁有最低權限許可的服務角色

根據最佳實務，我們強烈建議您建立 叢集 EC2 執行個體的服務角色 和許可政策，使其具有應用程式所需之其他 AWS 服務的最低權限。

預設受管政策 `AmazonElasticMapReduceforEC2Role` 提供許可，可讓您輕鬆地啟動初始叢集。不過，Amazon EMR 不需要任何許可便能啟動、監控和管理基本叢集。如果您在沒有許可的情況下啟動叢集，仍會建立叢集，且會使用另一種授權方法產生系統記錄並推送到 Amazon EMR 所擁有的 Amazon S3 儲存貯體。不過，叢集應用程式無法與其他 AWS 服務互動。例如，叢集將無法讀取或寫入 Amazon S3。

以下政策陳述式提供 Amazon EMR 不同功能所需的許可。我們建議您使用這些許可來建立許可政策，限制只能存取您的叢集所需的功能和資源。所有政策陳述式範例使用 `us-west-2` 區域和虛構的 AWS 帳戶 ID `123456789012`。請針對您的叢集適當替換。

如需有關建立和指定自訂角色的詳細資訊，請參閱 [自訂 IAM 規則 \(p. 171\)](#)。

Note

請遵照基本工作流程為 EC2 建立自訂的 EMR 角色，即可自動建立相同名稱的執行個體描述檔。Amazon EC2 能讓您使用不同名稱建立執行個體描述檔和角色。然而，Amazon EMR 並不支援此組態，且會在您建立叢集時，導致「無效的執行個體描述檔」錯誤。

使用 EMRFS 在 Amazon S3 中讀取和寫入資料

當 Amazon EMR 叢集上執行的應用程式參考使用 `s3://mydata` 格式的資料，Amazon EMR 將使用 EMRFS 發出請求。叢集通常以這種方式在 Amazon S3 中讀取和寫入資料，而且 EMRFS 會使用 叢集 EC2 執行個體的服務角色預設連接的許可。當您有多個叢集使用者和多個資料存放區時，您可能希望使用者對 Amazon S3 中的 EMRFS 資料有不同的許可。若要這樣做，您可以使用 EMRFS 的 IAM 角色。這樣可讓 EMRFS 擔任不同角色搭配不同的許可政策 (根據發出請求的使用者或群組或 Amazon S3 中 EMRFS 資料的位置)。如需更多詳細資訊，請參閱 [設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色 \(p. 174\)](#)。

由於 EMRFS 的 IAM 角色會回復為連接到 叢集 EC2 執行個體的服務角色 的許可，做為最佳實務，我們建議您使用 EMRFS 的 IAM 角色，並限制 EMRFS 和連接到 叢集 EC2 執行個體的服務角色 的 Amazon S3 許可。

以下範例陳述式展示 EMRFS 向 Amazon S3 發出請求所需要的許可。

- `my-data-bucket-in-s3-for-emrfs-reads-and-writes` 指定 Amazon S3 中的儲存貯體，其中的叢集將讀取及寫入資料和使用 `/*` 的所有子資料夾。只新增您的應用程式需要的儲存貯體和資料夾。
- 允許 dynamodb 動作的政策陳述式只在啟用 EMRFS 一致性檢視時需要。`EmrFSMetadata` 指定 EMRFS 一致性檢視的預設資料夾。如需詳細資訊，請參閱 [啟用一致性檢視 \(p. 53\)](#)。

```
{
    "Version": "2012-10-17",
```

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "s3:AbortMultipartUpload",
            "s3>CreateBucket",
            "s3>DeleteObject",
            "s3:GetBucketVersioning",
            "s3.GetObject",
            "s3:GetObjectTagging",
            "s3.GetObjectVersion",
            "s3>ListBucket",
            "s3>ListBucketMultipartUploads",
            "s3>ListBucketVersions",
            "s3>ListMultipartUploadParts",
            "s3:PutBucketVersioning",
            "s3:PutObject",
            "s3:PutObjectTagging"
        ],
        "Resource": [
            "arn:aws:s3:::my-data-bucket-in-s3-for-emrfs-reads-and-writes",
            "arn:aws:s3:::my-data-bucket-in-s3-for-emrfs-reads-and-writes/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "dynamodb CreateTable",
            "dynamodb BatchGetItem",
            "dynamodb BatchWriteItem",
            "dynamodb PutItem",
            "dynamodb DescribeTable",
            "dynamodb DeleteItem",
            "dynamodb GetItem",
            "dynamodb Scan",
            "dynamodb Query",
            "dynamodb UpdateItem",
            "dynamodb DeleteTable",
            "dynamodb UpdateTable"
        ],
        "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/EmrFSMetadata"
    },
    {
        "Effect": "Allow",
        "Action": [
            "cloudwatch PutMetricData",
            "dynamodb ListTables",
            "s3:HeadBucket"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "sns GetQueueUrl",
            "sns DeleteMessageBatch",
            "sns ReceiveMessage",
            "sns DeleteQueue",
            "sns SendMessage",
            "sns CreateQueue"
        ],
        "Resource": "arn:aws:sns:us-west-2:123456789012:EMRFS-Inconsistency-*"
    }
]
```

將日誌檔案封存至 Amazon S3

以下政策陳述式允許 Amazon EMR 叢集將日誌檔封存到指定的 Amazon S3 位置。在以下範例中，當叢集建立時，將使用主控台中的日誌資料夾 S3 位置、使用 AWS CLI 的 `--log-uri` 選項，或使用 `RunJobFlow` 命令中的 `LogUri` 參數指定 `s3://MyLoggingBucket/MyEMRClusterLogs`。如需詳細資訊，請參閱 [封存日誌檔到 Amazon S3 \(p. 119\)](#)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::MyLoggingBucket/MyEMRClusterLogs/*"
        }
    ]
}
```

使用除錯工具

以下政策陳述式允許啟用 Amazon EMR 除錯工具時需要的動作。將日誌檔封存至 Amazon S3，和上述範例中顯示的關聯許可，都是除錯所需。如需詳細資訊，請參閱 [啟用除錯工具 \(p. 120\)](#)。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "sns:Publish",  
                "sns:DeleteTopic"  
            ],  
            "Resource": "arn:aws:sns:us-west-2:123456789012:AWS-ElasticMapReduce-*"  
        }  
    ]  
}
```

使用 AWS Glue 資料目錄

以下政策陳述式允許您使用 AWS Glue 資料目錄 做為應用程式中繼存放區時所需要的動作。如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [使用 AWS Glue 資料目錄 做為 Spark SQL 的中繼存放區](#)、[使用 AWS Glue 資料目錄 做為 Hive 的中繼存放區](#)，以及 [使用 Presto 搭配 AWS Glue 資料目錄](#)。

```
        "glue:GetTableVersions",
        "glue>CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue>CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
    ]
}
]
```

EMR 中自動擴展的服務角色 (自動擴展角色)

適用於 EMR 的自動擴展角色會執行與服務角色類似的函數，但會允許動態擴展環境的其他動作。

- 預設角色為 `EMR_AutoScaling_DefaultRole`。
- 連接到 `EMR_AutoScaling_DefaultRole` 的預設受管政策是 `AmazonElasticMapReduceforAutoScalingRole`。

`AmazonElasticMapReduceforAutoScalingRole` 第 1 版內容如下所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce>ListInstanceGroups",
        "elasticmapreduce>ModifyInstanceGroups"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

EMR 筆記本 的服務角色

每個 EMR 筆記本 都需要許可，才能存取其他的 AWS 資源和執行動作。連接到此服務角色的 IAM 政策，會提供許可給此筆記本，來和其他 AWS 服務交互運作。使用 AWS Management Console 建立筆記本時，您會指定 AWS 服務角色。您可以使用預設的角色 `EMR_Notebooks_DefaultRole` 或指定您建立的角色。如果先前未建立筆記本，您可以選擇建立預設的角色。

- 預設角色為 `EMR_Notebooks_DefaultRole`。
- 連接到 `EMR_Notebooks_DefaultRole` 的預設受管政策是 `AmazonElasticMapReduceEditorsRole`。

`AmazonElasticMapReduceEditorsRole` 第 1 版內容如下所示。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2>CreateSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:RevokeSecurityGroupEgress",
            "ec2>CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2>DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:DescribeTags",
            "ec2:DescribeInstances",
            "ec2:DescribeSubnets",
            "elasticmapreduce>ListInstances",
            "elasticmapreduce>DescribeCluster"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ec2>CreateTags",
        "Resource": "arn:aws:ec2:*:*:network-interface/*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "aws:elasticmapreduce:editor-id",
                    "aws:elasticmapreduce:job-flow-id"
                ]
            }
        }
    }
]
```

當您將 Git 儲存庫連結到筆記本並需要為儲存庫建立私密金鑰時，您必須在連接到 EMR Notebooks 服務角色的 IAM 政策中建立 secretsmanager:GetSecretValue 權限。範例政策如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

使用 Amazon EMR 的服務連結角色

Amazon EMR 能夠使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Amazon EMR 的一種特殊 IAM 角色類型。服務連結角色是由 Amazon EMR 預先定義，且包含 Amazon EMR 代您呼叫 Amazon EC2 以清除不再使用的叢集資源所需的許可。此服務連結角色會與 Amazon EMR 服務角色和 Amazon EMR 的 Amazon EC2 執行個體描述檔搭配運作。如需服務角色和執行個體描述檔的詳細資訊，請參閱[將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。

Amazon EMR 會定義此服務連結角色的許可，除非另外定義，否則只有 Amazon EMR 才能擔任此角色。定義的許可包含信任政策和許可政策，而該許可政策不能連接至任何其他 IAM 實體。您只有在終止帳戶內的所有 EMR 叢集後，才能刪除此角色。

如需支援服務連結角色之其他服務的資訊，請參閱「[可搭配 IAM 運作的 AWS 服務](#)」，並尋找 Service-Linked Role (服務連結角色) 欄顯示 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

Amazon EMR 服務連結角色許可

Amazon EMR 會使用 AWSServiceRoleForEMRCleanup (AWSServiceRoleForEMRCleanup) 角色，也就是 service-based role that allows Amazon EMR to terminate and delete Amazon EC2 resources on your behalf if the Amazon EMR service role has lost that ability. Amazon EMR creates the role automatically during cluster creation if it does not already exist.

AWSServiceRoleForEMRCleanup 服務連結角色信任下列服務以擔任角色：

- elasticmapreduce.amazonaws.com

AWSServiceRoleForEMRCleanup 服務連結角色許可政策允許 Amazon EMR 對指定資源完成下列動作：

- 動作：DescribeInstancesonec2
- 動作：DescribeSpotInstanceRequestsonec2
- 動作：ModifyInstanceAttributeonec2
- 動作：TerminateInstancesonec2
- 動作：CancelSpotInstanceRequestsonec2
- 動作：DeleteNetworkInterfaceonec2
- 動作：DescribeInstanceAttributeonec2
- 動作：DescribeVolumeStatusonec2
- 動作：DescribeVolumesonec2
- 動作：DetachVolumeonec2
- 動作：DeleteVolumeonec2

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。

允取 IAM 實體建立 AWSServiceRoleForEMRCleanup 服務連結角色

將下列陳述式新增至 IAM 實體建立服務連結角色所需的許可政策：

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam:CreateServiceLinkedRole",  
        "iam:PutRolePolicy"  
    ],  
    "Resource": "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com*/  
AWSServiceRoleForEMRCleanup*",  
    "Condition": {  
        "StringLike": {  
            "iam:AWSServiceName": [  
                "elasticmapreduce.amazonaws.com",  
                "elasticmapreduce.amazonaws.com.cn"  
            ]  
        }  
    }  
}
```

}

允取 IAM 實體編輯 AWSServiceRoleForEMRCleanup 服務連結角色的描述。

將下列陳述式新增至 IAM 實體編輯服務連結角色描述所需的許可政策：

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam:UpdateRoleDescription"  
    ],  
    "Resource": "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com*/  
AWSServiceRoleForEMRCleanup*",  
    "Condition": {  
        "StringLike": {  
            "iam:AWSServiceName": [  
                "elasticmapreduce.amazonaws.com",  
                "elasticmapreduce.amazonaws.com.cn"  
            ]  
        }  
    }  
}
```

允取 IAM 實體刪除 AWSServiceRoleForEMRCleanup 服務連結角色

將下列陳述式新增至 IAM 實體刪除服務連結角色所需的許可政策：

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam>DeleteServiceLinkedRole",  
        "iam:GetServiceLinkedRoleDeletionStatus"  
    ],  
    "Resource": "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com*/  
AWSServiceRoleForEMRCleanup*",  
    "Condition": {  
        "StringLike": {  
            "iam:AWSServiceName": [  
                "elasticmapreduce.amazonaws.com",  
                "elasticmapreduce.amazonaws.com.cn"  
            ]  
        }  
    }  
}
```

建立 的服務連結角色Amazon EMR

您無須手動建立 AWSServiceRoleForEMRCleanup 角色。當您 launch a cluster, either for the first time or when a service-linked role is not present 時，Amazon EMR 會為您建立服務連結角色。您必須具備許可才能建立服務連結角色。如需新增此功能至 IAM 實體 (例如使用者、群組或角色) 許可政策的範例陳述式，請參閱 [Amazon EMR 服務連結角色許可 \(p. 167\)](#)。

Important

若您於 October 24, 2017 前就在使用 Amazon EMR，那麼不再支援服務連結角色時，Amazon EMR 會於您帳戶中建立 AWSServiceRoleForEMRCleanup 角色。如需詳細資訊，請參閱 [我的 IAM 帳戶出現的新角色](#)。

編輯 Amazon EMR 的服務連結角色

Amazon EMR 不允許您編輯 AWSServiceRoleForEMRCleanup 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。

編輯服務連結角色說明 (IAM 主控台)

You can use the IAM console to edit the description of a service-linked role.

To edit the description of a service-linked role (console)

1. In the navigation pane of the IAM console, choose Roles.
2. Choose the name of the role to modify.
3. To the right of the Role description, choose Edit.
4. Enter a new description in the box and choose Save changes.

編輯服務連結角色說明 (IAM CLI)

You can use IAM commands from the AWS Command Line Interface to edit the description of a service-linked role.

To change the description of a service-linked role (CLI)

1. (Optional) To view the current description for a role, use the following commands:

```
$ aws iam get-role --role-name role-name
```

Use the role name, not the ARN, to refer to roles with the CLI commands. For example, if a role has the following ARN: arn:aws:iam::123456789012:role/myrole, you refer to the role as **myrole**.

2. To update a service-linked role's description, use one of the following commands:

```
$ aws iam update-role-description --role-name role-name --description description
```

編輯服務連結角色說明 (IAM API)

You can use the IAM API to edit the description of a service-linked role.

To change the description of a service-linked role (API)

1. (Optional) To view the current description for a role, use the following command:

IAM API: [GetRole](#)

2. To update a role's description, use the following command:

IAM API: [UpdateRoleDescription](#)

刪除 Amazon EMR 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，務必清除您的服務連結角色，之後才能將其刪除。

清除服務連結角色

您必須先確認服務連結角色沒有作用中的工作階段，並移除該角色使用的資源，之後才能使用 IAM 將其刪除。

檢查服務連結角色是否於 IAM 主控台有作用中的工作階段

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.

2. 在導覽窗格中，選擇 Roles (角色)。選取 AWSServiceRoleForEMRCleanup 角色的名稱 (而非核取方塊)。
3. 在所選角色的 Summary (摘要) 頁面中，選擇 Access Advisor (存取 Advisor)。
4. 在 Access Advisor (存取 Advisor) 標籤中，檢閱服務連結角色的近期活動。

Note

如果您不確定 Amazon EMR 是否正在使用 AWSServiceRoleForEMRCleanup 角色，您可以嘗試刪除該角色。如果服務正在使用該角色，則刪除會失敗，而您可以檢視正在使用該角色的區域。如果服務正在使用該角色，您必須先等到工作階段結束，才能刪除該角色。您無法撤銷服務連結角色的工作階段。

移除 AWSServiceRoleForEMRCleanup 所使用的 Amazon EMR 資源

- 終止您帳戶內的所有叢集。如需更多詳細資訊，請參閱 [終止叢集 \(p. 288\)](#)。

刪除服務連結角色 (IAM 主控台)

您可以使用 IAM 主控台刪除服務連結角色。

刪除服務連結角色 (主控台)

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. 在導覽窗格中，選擇 Roles (角色)。選取 AWSServiceRoleForEMRCleanup 旁的核取方塊，而非名稱或資料列本身。
3. 針對頁面頂端的 Role actions (角色動作)，選擇 Delete role (刪除角色)。
4. 在確認對話方塊中，檢閱服務上次存取資料，以顯示每個所選取角色上次存取 AWS 服務的時間。這可協助您確認角色目前是否作用中。若要繼續，請選擇 Yes, Delete (是，刪除)。
5. 監看 IAM 主控台通知，監視服務連結角色刪除的進度。因為 IAM 服務連結角色刪除不同步，所以在您提交角色進行刪除之後，刪除任務可能會成功或失敗。如果任務失敗，您可以從通知中選擇 View details (檢視詳細資訊) 或 View Resources (檢視資源)，以了解刪除失敗的原因。如果刪除因角色使用服務中資源而失敗，則失敗原因會包含資源清單。

刪除服務連結角色 (IAM CLI)

您可以從 AWS Command Line Interface 使用 IAM 命令，刪除服務連結角色。因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則該要求可能遭拒。

刪除服務連結角色 (CLI)

1. 若要檢查刪除任務的狀態，您必須從回應中擷取 deletion-task-id。鍵入下列命令，以提交服務連結角色刪除要求：

```
$ aws iam delete-service-linked-role --role-name AWSServiceRoleForEMRCleanup
```

2. 鍵入下列命令，以檢查刪除任務的狀態：

```
$ aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

刪除任務的狀態可以是 NOT_STARTED、IN_PROGRESS、SUCCEEDED 或 FAILED。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

刪除服務連結角色 (IAM API)

您可以使用 IAM API 刪除服務連結角色。因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則該要求可能遭拒。

刪除服務連結角色 (API)

- 若要提交服務連結角色的刪除請求，請呼叫 [DeleteServiceLinkedRole](#)。在要求中，指定 AWSServiceRoleForEMRCleanup 角色名稱。

若要檢查刪除任務的狀態，您必須從回應中擷取 `DeletionTaskId`。

- 若要檢查刪除的狀態，請呼叫 [GetServiceLinkedRoleDeletionStatus](#)。在要求中，指定 `DeletionTaskId`。

刪除任務的狀態可以是 NOT_STARTED、IN_PROGRESS、SUCCEEDED 或 FAILED。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

Amazon EMR 服務連結角色的支援區域

Amazon EMR 在下列區域支援使用服務連結角色。

區域名稱	區域身分	在 Amazon EMR 中支援
US East (N. Virginia)	us-east-1	是
US East (Ohio)	us-east-2	是
US West (N. California)	us-west-1	是
US West (Oregon)	us-west-2	是
Asia Pacific (Mumbai)	ap-south-1	是
Asia Pacific (Osaka-Local)	ap-northeast-3	是
Asia Pacific (Seoul)	ap-northeast-2	是
Asia Pacific (Singapore)	ap-southeast-1	是
Asia Pacific (Sydney)	ap-southeast-2	是
Asia Pacific (Tokyo)	ap-northeast-1	是
Canada (Central)	ca-central-1	是
EU (Frankfurt)	eu-central-1	是
EU (Ireland)	eu-west-1	是
EU (London)	eu-west-2	是
EU (Paris)	eu-west-3	是
South America (São Paulo)	sa-east-1	是

自訂 IAM 規則

您可能想要自訂 IAM 服務角色和權限，以根據您的安全要求限制許可。若要自訂許可，我們建議您建立新角色和政策。從預設角色之受管政策中的許可開始（例如，`AmazonElasticMapReduceforEC2Role` 和

AmazonElasticMapReduceRole)。然後，複製內容並將其貼到新政策陳述式、修改適當的許可，並將修改的許可政策連接到您建立的角色。您必須擁有適當的 IAM 許可，才可處理角色和政策。如需更多詳細資訊，請參閱 [允許使用者和群組以建立和修改角色 \(p. 178\)](#)。

請遵照基本工作流程為 EC2 建立自訂的 EMR 角色，即可自動建立相同名稱的執行個體描述檔。Amazon EC2 能讓您使用不同名稱建立執行個體描述檔和角色。然而，Amazon EMR 並不支援此組態，且會在您建立叢集時，導致「無效的執行個體描述檔」錯誤。

Important

內嵌政策不會在服務需求變更時自動更新。若您建立並連接了內嵌政策，請注意系統可能會更新服務，突然造成權限錯誤。如需詳細資訊，請參閱 IAM User Guide 中的「[受管政策及內嵌政策](#)」及「[建立叢集時指定自訂 IAM 角色 \(p. 172\)](#)」。

如需關於使用 IAM 角色的詳細資訊，請參閱 IAM User Guide 中的下列主題：

- [建立角色以將許可委派給 AWS 服務](#)
- [修改角色](#)
- [刪除角色](#)

建立叢集時指定自訂 IAM 角色

您可以在建立叢集時指定 Amazon EMR 的服務角色和 Amazon EC2 執行個體描述檔的角色。建立叢集的使用者需要許可才能擷取角色並將其指派至 Amazon EMR 和 EC2 執行個體。否則，User account is not authorized to call EC2 (使用者帳戶無權呼叫 EC2) 錯誤會發生。如需更多詳細資訊，請參閱 [允許使用者和群組以建立和修改角色 \(p. 178\)](#)。

使用主控台來指定自訂規則

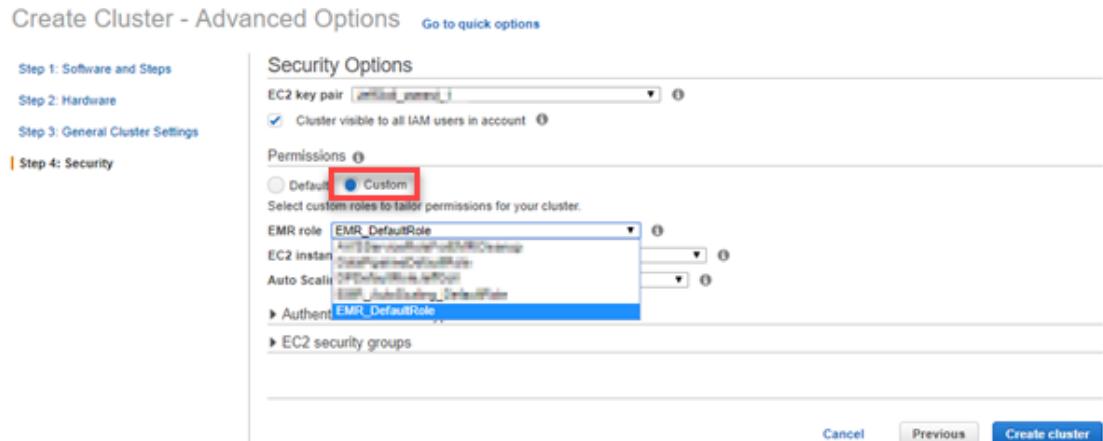
建立叢集時，您可以使用 Advanced options (進階選項) 指定 Amazon EMR 的自訂服務角色、EC2 執行個體描述檔的自訂角色和自訂 Auto Scaling 角色。使用 Quick options (快速選項) 時，會指定 EC2 執行個體描述檔的預設服務角色和預設角色。如需詳細資訊，請參閱 [Amazon EMR 使用的 IAM 服務角色 \(p. 159\)](#)。

使用主控台來指定自訂 IAM 角色

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)，Go to advanced options (前往進階選項)。
3. 選擇適用於應用程式的叢集設定，直到您達到 Security Options (安全選項)。

在 Permissions (許可) 下，Amazon EMR 的 Default (預設) 角色會被選取。

4. 選擇 Custom (自訂)。
5. 對於每個角色類型，從清單中選取一個角色。只有在帳戶中具有該角色類型之適當信任政策的角色才會列出。



6. 選擇適用於叢集的其他選項，然後選擇 Create Cluster (建立叢集)。

使用 AWS CLI 來指定自訂規則

您可以使用選項搭配 AWS CLI 的 `create-cluster` 命令來明確指定 EMR 的服務角色和 叢集 EC2 執行個體的服務角色。使用 `--service-role` 選項來指定服務角色。使用 `InstanceProfile` 選項的 `--ec2-attributes` 引數，來指定 EC2 執行個體描述檔的角色。

會使用單獨的選項 (`--auto-scaling-role`) 來指定 Auto Scaling 角色。如需更多詳細資訊，請參閱 [於 Amazon EMR 使用自動調整規模 \(p. 291\)](#)。

使用 AWS CLI 來指定自訂 IAM 角色

- 以下命令會在啟動叢集時，指定自訂服務角色 (`MyCustomServiceRoleForEMR`) 以及 EC2 執行個體描述檔的自訂角色 (`MyCustomServiceRoleForClusterEC2Instances`)。這個範例會使用預設 Amazon EMR 角色。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "Test cluster" --release-label emr-5.28.0 \
--applications Name=Hive Name=Pig --service-role MyCustomServiceRoleForEMR \
--ec2-attributes InstanceProfile=MyCustomServiceRoleForClusterEC2Instances, \
KeyName=myKey --instance-type m5.xlarge --instance-count 3
```

您可以使用這些選項 (而不是使用 `--use-default-roles` 選項) 來明確指定預設角色。`--use-default-roles` 選項指定服務角色和 AWS CLI 的 config 檔案中定義的 EC2 執行個體設定檔。。

以下範例示範指定 Amazon EMR 自訂角色之 AWS CLI 的 config 檔案的內容。有了這項組態檔案，指定 `--use-default-roles` 選項時，將使用 `MyCustomServiceRoleForEMR` 和 `MyCustomServiceRoleForClusterEC2Instances` 建立叢集。根據預設，config 檔案指定預設的 `service_role` 為 `AmazonElasticMapReduceRole`，且預設的 `instance_profile` 為 `EMR_EC2_DefaultRole`。

```
[default]
output = json
region = us-west-1
aws_access_key_id = myAccessKeyId
aws_secret_access_key = mySecretAccessKey
emr =
```

```
service_role = MyCustomServiceRoleForEMR
instance_profile = MyCustomServiceRoleForClusterEC2Instances
```

設定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色

當 Amazon EMR 叢集上執行的應用程式參考使用 `s3://mydata` 格式的資料，Amazon EMR 將使用 EMRFS 發出請求。若要與 Amazon S3 互動，EMRFS 將擔任叢集建立時所指定之 [叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#) 連接的許可政策。無論使用應用程式的使用者或群組，或 Amazon S3 中資料的位置為何。同樣都使用 叢集 EC2 執行個體的服務角色。如果您的叢集有多個使用者，他們需要透過 EMRFS 對 Amazon S3 中的資料有不同層級的存取，您可以設定含 EMRFS 的 IAM 角色的安全組態。EMRFS 可以根據發出請求的使用者或群組或是根據 Amazon S3 中資料的位置擔任不同的 叢集 EC2 執行個體的服務角色。針對存取 Amazon S3 中的資料，EMRFS 的每個 IAM 角色可以擁有不同的許可。

EMRFS 的 IAM 角色可在 Amazon EMR 發行版本 5.10.0 和更新版本中使用。如果您使用舊發行版本或您的要求超出 EMRFS 的 IAM 角色所能提供，可以改為建立自訂登入資料提供者。如需詳細資訊，請參閱 [授權存取在 Amazon S3 中的 EMRFS 資料 \(p. 66\)](#)。如需 EMRFS 的詳細資訊，請參閱 [使用 EMR 檔案系統 \(EMRFS\) \(p. 52\)](#)。

您使用安全組態來指定 EMRFS 的 IAM 角色時，便設定角色映射。每個角色映射指定對應至識別符的 IAM 角色。這些識別符決定透過 EMRFS 存取 Amazon S3 的基礎。識別符可以是使用者、群組或顯示資料位置的 Amazon S3 前綴。當 EMRFS 向 Amazon S3 發出請求時，如果請求符合存取基準，EMRFS 便可讓叢集 EC2 執行個體擔任請求的對應 IAM 角色。將套用連接到該角色的 IAM 許可，而不是連接到 叢集 EC2 執行個體的服務角色 的 IAM 許可。

角色映射中的使用者和群組是叢集上定義的 Hadoop 使用者和群組。在應用程式使用 EMRFS 的情況下，使用者和群組會傳送給 EMRFS (例如，YARN 使用者模擬)。Amazon S3 前綴可以是任何深度的儲存貯體指標 (例如，`s3://mybucket` 或 `s3://mybucket/myproject/mydata`)。您可以在單一角色映射中指定多個識別符，但識別符必須全部都是相同的類型。

Important

EMRFS 的 IAM 角色在應用程式使用者之間提供應用程式層級隔離。它不提供主機上使用者之間的主機層級隔離。任何有權存取叢集的使用者，都可以略過隔離以承擔任何角色。

叢集應用程式透過 EMRFS 向 Amazon S3 提出請求時，EMRFS 會依角色映射出現在安全組態中的順序，由上而下進行評估。如果透過 EMRFS 提出的請求不符合任何識別符，EMRFS 回退至使用 叢集 EC2 執行個體的服務角色。因此，我們建議將政策連接到可用 Amazon S3 的此角色限制許可。如需詳細資訊，請參閱 [叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#)。

設定角色

使用 EMRFS 的 IAM 角色設定安全組態前，請計畫並建立角色和要連接到角色的許可政策。如需詳細資訊，請參閱 IAM User Guide 中的 [EC2 執行個體的角色如何運作？](#)。建立許可政策時，我們建議您從連接到 EC2 預設 EMR 角色的受管政策開始，接著根據您的需求編輯此政策。預設角色是 `EMR_EC2_DefaultRole`，而需編輯的預設受管政策是 `AmazonElasticMapReduceforEC2Role`。如需詳細資訊，請參閱 [叢集 EC2 執行個體的服務角色 \(EC2 執行個體描述檔\) \(p. 161\)](#)。

更新承擔角色許可的信任政策

EMRFS 使用的每個角色都必須擁有信任政策，以允許 EC2 的叢集 EMR 角色來擔任此角色。同樣的，EC2 的叢集 EMR 角色也必須擁有信任政策，以允許 EMRFS 角色來擔任此角色。

以下範例信任政策連接到 EMRFS 的角色。陳述式允許 EC2 的預設 EMR 角色擔任此角色。例如，如果您有兩個虛構的 EMRFS 角色：`EMRFSRole_First` 和 `EMRFSRole_Second`，此政策陳述式會新增到這兩個角色的信任政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AWSAcctID:role/EMR_EC2_DefaultRole"  
    },  
    "Action": "sts:AssumeRole"  
}  
]  
}
```

此外，以下範例信任政策陳述式新增到 EMR_EC2_DefaultRole 以允許兩個虛構的 EMRFS 角色擔任此角色。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": ["arn:aws:iam::AWSAcctID:role/EMRFSRole_First",  
                        "arn:aws:iam::AWSAcctID:role/EMRFSRole_Second"]  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

更新 IAM 角色的信任政策

Open the IAM console at <https://console.aws.amazon.com/iam/>.

1. 選擇 Roles (角色)、在 Search (搜尋) 中輸入角色的名稱，然後選取它的 Role name (角色名稱)。
2. 選擇 Trust relationships (信任關係)、Edit trust relationship (編輯信任關係)。
3. 依照上述指導方針，根據 Policy Document (政策文件) 新增信任陳述式，然後選擇 Update Trust Policy (更新信任政策)。

指定角色做為金鑰使用者

如果角色允許存取 Amazon S3 中的位置，而此位置已使用 AWS Key Management Service 客戶主金鑰 (CMK) 加密，請確定已將該角色指定為金鑰使用者。這會授予角色使用 CMK 的許可。如需詳細資訊，請參閱 AWS Key Management Service Developer Guide 中的 [使用金鑰政策](#)。

使用 EMRFS 的 IAM 角色設定安全組態

Important

如果您指定 EMRFS 的 IAM 角色皆不套用，EMRFS 回退至 EC2 的 EMR 角色。請考慮自訂此角色，來為您的應用程式適當地限制對 Amazon S3 的許可，然後在建立叢集時指定此自訂角色，而非指定 EMR_EC2_DefaultRole。如需更多詳細資訊，請參閱 [自訂 IAM 規則 \(p. 171\)](#) 及 [建立叢集時指定自訂 IAM 角色 \(p. 172\)](#)。

使用主控台指定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色

1. 建立指定角色映射的安全組態：
 - a. 在 Amazon EMR 主控台中，選擇 Security configurations (安全組態)、Create (建立)。
 - b. 輸入安全組態的 Name (名稱)。您建立叢集時會使用此名稱來指定安全組態。
 - c. 選擇 Use IAM roles for EMRFS requests to Amazon S3 (用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色)。

- d. 選擇要套用的 IAM role (IAM 角色) , 接著在 Basis for access (存取的基準) 中 , 從清單選擇識別符類型 (Users (使用者)、Groups (群組) 或 S3 prefixes (S3 前綴)) , 然後輸入對應的識別符。如果您使用多個識別符 , 以逗號和不含空格的方式分隔識別符。如需每個識別符類型的詳細資訊 , 請參閱下面的 「[JSON 組態參考 \(p. 176\)](#)」。
 - e. 選擇 Add role (新增角色) , 來設定如先前步驟中所述的額外角色對應。
 - f. 適當地設定其他的安全組態選項 , 然後選擇 Create (建立)。如需更多詳細資訊 , 請參閱 [建立安全組態 \(p. 129\)](#)。
2. 建立叢集時指定您在上面建立的安全組態。如需更多詳細資訊 , 請參閱 [指定適用於叢集的安全組態 \(p. 142\)](#)。

使用 AWS CLI 指定用來向 Amazon S3 請求使用 EMRFS 的 IAM 角色

1. 使用 `aws emr create-security-configuration` 命令 , 指定安全組態的名稱 , 以及採用 JSON 格式的安全組態詳細資訊。

以下所示範例命令建立名稱為 `EMRFS_Roles_Security_Configuration` 的安全組態。這是以 `MyEmrFsSecConfig.json` 檔案中的 JSON 結構為基礎 , 其儲存在與命令執行的相同目錄中。

```
aws emr create-security-configuration --name EMRFS_Roles_Security_Configuration --  
security-configuration file://MyEmrFsSecConfig.json.
```

關於 `MyEmrFsSecConfig.json` 檔案的結構 , 請遵循下列的準則。您可以指定此結構以及其他安全組態選項的結構。如需更多詳細資訊 , 請參閱 [建立安全組態 \(p. 129\)](#)。

下列所舉的 JSON 程式碼片段範例 , 可在安全組態中為 EMRFS 指定自訂 IAM 角色。其示範了三個不同識別符類型的角色對應 , 並接續說明參數參考。

```
{  
    "AuthorizationConfiguration": {  
        "EmrFsConfiguration": {  
            "RoleMappings": [{  
                "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_for_user1",  
                "IdentifierType": "User",  
                "Identifiers": [ "user1" ]  
            }, {  
                "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_to_MyBuckets",  
                "IdentifierType": "Prefix",  
                "Identifiers": [ "s3://MyBucket/", "s3://MyOtherBucket/" ]  
            }, {  
                "Role": "arn:aws:iam::123456789101:role/allow_EMRFS_access_for_AdminGroup",  
                "IdentifierType": "Group",  
                "Identifiers": [ "AdminGroup" ]  
            }]  
        }  
    }  
}
```

參數	描述
<code>"AuthorizationConfiguration":</code>	必要.
<code>"EmrFsConfiguration":</code>	必要. 包含角色對應。
<code>"RoleMappings":</code>	必要. 包含一或多個角色對應定義。並會依角色對應出現的順序 , 由上而下對其評估。若系統在 Amazon S3 中針對資料的 EMRFS 呼叫將角色對應評估為 true , 則不會繼續評估角色對應 , 且

參數	描述
	EMRFS 會使用要求的特定 IAM 角色。角色對應包含下列必要參數：
"Role":	指定 IAM 角色的 ARN 識別符，格式為 <code>arn:aws:iam::account-id:role/role-name</code> 。這是在 EMRFS 向 Amazon S3 發出之要求符合任何指定的 Identifiers 時，Amazon EMR 使用的 IAM 角色。
"IdentifierType":	可為下列其中之一： <ul style="list-style-type: none"> "User" 指定識別符為一或多個 Hadoop 使用者，其可為 Linux 帳戶使用者或 Kerberos 委託人。當 EMRFS 在指定使用者的情況下發出要求時，就會使用 IAM 角色。 "Prefix" 指定識別符為 Amazon S3 位置。IAM 角色會用於對具有指定字首之位置的呼叫。例如，字首 <code>s3://mybucket/</code> 與 <code>s3://mybucket/mydir</code> 及 <code>s3://mybucket/yetanotherdir</code> 相符。 "Group" 指定識別符為一或多個 Hadoop 群組。當要求來自指定群組中的使用者時，就會使用 IAM 角色。
"Identifiers":	指定一或多個適當識別符類型的識別符。並使用逗號以不含空格的方式分隔多個識別符。

2. 使用 `aws emr create-cluster` 命令來建立叢集並指定您在上一個步驟建立的安全組態。

以下範例在安裝預設核心 Hadoop 應用程式下建立叢集。該叢集會使用上面建立為 `EMRFS_Roles_Security_Configuration` 的安全組態，也會使用 EC2 的自訂 EMR 角色 `EC2_Role_EMR_Restrict_S3`，這個角色是透過 `--ec2-attributes` 參數的 `InstanceProfile` 引數所指定。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name MyEmrFsS3RolesCluster \
--release-label emr-5.28.0 --ec2-attributes
  InstanceProfile=EC2_Role_EMR_Restrict_S3,KeyName=MyKey \
--instance-type m5.xlarge --instance-count 3 \
--security-configuration EMRFS_Roles_Security_Configuration
```

使用 Amazon EMR Access to AWS Glue 資料目錄 的資源類型政策

如果您在 Amazon EMR 中使用 AWS Glue 搭配 Hive、Spark 或 Presto，AWS Glue 支援資源式政策來控制對資料目錄 資源的存取。這些資源包括資料庫、資料表、連接和使用者定義的功能。如需詳細資訊，請參閱《AWS Glue Developer Guide》中的 [AWS Glue 資源政策](#)。

使用以資源為基礎的政策從 Amazon EMR 內限制對 AWS Glue 的存取時，您在許可政策中指定的委託人必須是與建立叢集時指定的 EC2 執行個體描述檔關聯的角色 ARN。例如，對於已連接至型錄的資源型政策，

您可以使用以下範例所示的格式，將預設叢集 EC2 執行個體的服務角色, [EMR_EC2_DefaultRole](#) 的角色 ARN 指定為 Principal：

```
arn:aws:iam::acct-id:role/EMR\_EC2\_DefaultRole
```

acct-id 可以與 AWS Glue 帳戶 ID 不同。這可從不同帳戶中的 EMR 叢集進行存取。您可以指定多個委託人，每個來自不同的帳戶。

使用 IAM 角色搭配會直接呼叫 AWS 服務的應用程式

在叢集 EC2 執行個體上執行的應用程式可以使用 EC2 執行個體描述檔，來在呼叫 AWS 服務時取得臨時安全登入資料。

可與 Amazon EMR 2.3.0 版和更新版本搭配使用的 Hadoop 版本已更新為可使用 IAM 角色。如果應用程式是基於 Hadoop 架構來嚴格執行，且不會在 AWS 中直接呼叫任何服務，它應能夠使用 IAM 角色，而無需修改。

如果應用程式會直接呼叫 AWS 中的服務，您需要將其更新，才能利用 IAM 角色。這表示，與其在叢集中 EC2 執行個體上透過 /etc/hadoop/conf/core-site.xml 取得帳戶登入資料，應用程式會使用軟體開發套件來使用 IAM 角色存取資源，或是呼叫 EC2 執行個體中繼資料，以取得臨時登入資料。

若要使用軟體開發套件存取含 IAM 角色的 AWS 資源

- 下列主題示範如何使用多種 AWS 開發套件以使用 IAM 角色存取臨時登入資料。每個主題以應用程式的版本開始 (該應用程式不會使用 IAM 角色)，然後逐步引導您將該應用程式轉換為使用 IAM 角色的程序。
 - AWS SDK for Java Developer Guide中的[使用適用於 Java 之開發套件的 Amazon EC2 執行個體的 IAM 角色](#)
 - AWS SDK for .NET Developer Guide中的[使用適用於 .NET 之開發套件的 Amazon EC2 執行個體的 IAM 角色](#)
 - AWS SDK for PHP Developer Guide中的[使用適用於 PHP 之開發套件的 Amazon EC2 執行個體的 IAM 角色](#)
 - AWS SDK for Ruby Developer Guide中的[使用適用於 Ruby 之開發套件的 Amazon EC2 執行個體的 IAM 角色](#)

若要從 EC2 執行個體中繼資料取得臨時登入資料

- 從使用指定 IAM 角色執行的 EC2 執行個體中呼叫以下 URL，會傳回關聯的臨時安全登入資料 (AccessKeyId、SecretAccessKey、SessionToken 和 Expiration)。以下範例使用 Amazon EMR 預設的執行個體設定檔 [EMR_EC2_DefaultRole](#)。

```
GET http://169.254.169.254/latest/meta-data/iam/security-credentials/EMR\_EC2\_DefaultRole
```

如需有關使用 IAM 角色之應用程式的編寫詳細資訊，請參閱[授與在 Amazon EC2 執行個體上執行之應用程式對 AWS 資源的存取權](#)。

如需暫時安全登入資料的詳細資訊，請參閱 [Using Temporary Security Credentials](#)中的[使用暫時安全登入資料](#)。

允許使用者和群組以建立和修改角色

必須允許建立、修改和指定叢集角色 (包括預設角色) 的 IAM 委託人 (使用者和群組) 執行以下動作。如需每個動作的詳細資訊，請參閱 IAM API Reference 中的[動作](#)。

- iam:CreateRole
- iam:PutRolePolicy
- iam>CreateInstanceProfile
- iam:AddRoleToInstanceProfile
- iam>ListRoles
- iam:GetPolicy
- iam:GetInstanceProfile
- iam:GetPolicyVersion
- iam:AttachRolePolicy
- iam:PassRole

iam:PassRole 許可會允許叢集建立。剩餘的許可允許預設角色的建立。

Amazon EMR 身分類型政策範例

根據預設，IAM 使用者和角色不具備建立或修改 Amazon EMR 資源的許可。他們也無法使用 AWS Management Console、AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授予使用者和角色在他們所需指定資源上執行特定 API 操作的許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分類型政策，請參閱《IAM User Guide》中的[在 JSON 標籤上建立政策](#)。

主題

- [Amazon EMR 政策最佳實務 \(p. 179\)](#)
- [允許使用者檢視他們自己的許可 \(p. 180\)](#)
- [Amazon EMR 受管政策 \(p. 180\)](#)
- [IAM 叢集和 EMR 筆記本以標籤為基礎的存取政策 \(p. 183\)](#)

Amazon EMR 政策最佳實務

身分類型政策相當強大。他們可以判斷您帳戶中的某個人員是否可以建立、存取或刪除 Amazon EMR 資源。這些動作可能會讓您的 AWS 帳戶產生成本。當您建立或編輯身分類型政策時，請遵循下列準則及建議事項：

- [開始使用 AWS 受管政策 – 若要快速地開始使用 Amazon EMR，請使用 AWS 受管政策來給予您的員工他們需要的許可。這些政策已在您的帳戶中提供，並由 AWS 維護和更新。如需詳細資訊，請參閱 IAM User Guide中的\[開始搭配 AWS 受管政策使用許可\]\(#\)和\[Amazon EMR 受管政策 \\(p. 180\\)\]\(#\)。](#)
- [授予最低權限 – 當您建立自訂政策時，請只授予執行任務所需要的許可。以最小一組許可開始，然後依需要授予額外的許可。這比一開始使用太寬鬆的許可，稍後再嘗試將他們限縮更為安全。如需詳細資訊，請參閱《IAM User Guide》中的\[授予最低權限\]\(#\)。](#)
- [為敏感操作啟用 MFA – 為了增加安全，請要求 IAM 使用者使用多重驗證 \(MFA\) 存取敏感資源或 API 操作。如需詳細資訊，請參閱《IAM User Guide》中的\[在 AWS 中使用多重驗證 \\(MFA\\)\]\(#\)。](#)
- [使用政策條件以增加安全 – 在切實可行的範圍中，請定義您身分類型政策允許存取資源的條件。例如，您可以撰寫條件，指定請求必須來自一定的允許 IP 地址範圍。您也可以撰寫條件，只在指定的日期或時間範圍內允許請求，或是要求使用 SSL 或 MFA。如需詳細資訊，請參閱 IAM User Guide中的\[IAM JSON 政策元素：條件\]\(#\)。](#)

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台上，或是使用 AWS CLI 或 AWS API 透過編寫程式的方式完成此動作的許可。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "ViewOwnUserInfo",  
            "Effect": "Allow",  
            "Action": [  
                "iam:GetUserPolicy",  
                "iam>ListGroupsForUser",  
                "iam>ListAttachedUserPolicies",  
                "iam>ListUserPolicies",  
                "iam GetUser"  
            ],  
            "Resource": [  
                "arn:aws:iam::*:user/${aws:username}"  
            ]  
        },  
        {  
            "Sid": "NavigateInConsole",  
            "Effect": "Allow",  
            "Action": [  
                "iam:GetGroupPolicy",  
                "iam:GetPolicyVersion",  
                "iam GetPolicy",  
                "iam>ListAttachedGroupPolicies",  
                "iam>ListGroupPolicies",  
                "iam>ListPolicyVersions",  
                "iam>ListPolicies",  
                "iam>ListUsers"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Amazon EMR 受管政策

如果想針對必要的 Amazon EMR 動作，授予完整的存取或唯讀存取權限，最簡單的方法就是使用 Amazon EMR 的 IAM 受管政策。受管政策提供的好處是，許可需求變更時會自動更新。若您使用內嵌政策，可能會發生服務變更，並造成許可錯誤出現。

這些政策不僅包含 Amazon EMR 的動作，也包含 Amazon EC2、Amazon S3 和 Amazon CloudWatch 的動作，Amazon EMR 可用來執行動作，例如啟動執行個體、寫入日誌檔案和管理 Hadoop 的工作與任務。

叢集使用者需要應用程式的許可，才能代表他們傳遞 Amazon EMR 的服務角色。AmazonElasticMapReduceFullAccess 許可政策是預設受管政策，可讓使用者擁有 iam:PassRole 的完整許可，且該政策所包含的陳述式允許所有資源的 Amazon EMR 許可。此陳述式允許使用者將任何角色傳遞給其他 AWS 服務，使 Amazon EMR 可代表該使用者與那些服務互動。

若要實作更具限制性的政策，請將允許 iam:PassRole 只能傳遞 Amazon EMR 角色的內嵌政策連接到適當的使用者或群組。下列範例示範僅允許 iam:PassRole 許可傳遞以下預設 Amazon EMR 角色的陳述式：EMR_DefaultRole、EMR_EC2_DefaultRole 及 EMR_AutoScalingDefaultRole。若您使用自訂角色，請將預設角色名稱取代為您的自訂角色名稱。

```
{
```

```
"Action": "iam:PassRole",
"Effect": "Allow",
"Resource": [
    "arn:aws:iam::*:role/EMR_DefaultRole",
    "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
    "arn:aws:iam::*:role/EMR_Notebooks_DefaultRole
]
}
```

若要建立自訂政策，我們建議您從受管政策開始，並根據需求編輯這些政策。

關於將政策連接到 IAM 使用者（主體）的方法，詳細資訊請參閱 IAM User Guide 中的 [透過 AWS Management Console 來使用受管政策](#)。

IAM 受管政策的完整存取

若要授予 Amazon EMR 的所有必要動作，請連接 AmazonElasticMapReduceFullAccess 受管政策。此政策陳述式的內容顯示如下。它顯示 Amazon EMR 在其他服務中需要的所有動作。

此政策第 6 版的內容顯示如下。由於 AmazonElasticMapReduceFullAccess 政策會自動更新，此處所示的政策可能已過期。使用 AWS Management Console 以檢視目前的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudwatch:*",
                "cloudformation>CreateStack",
                "cloudformation>DescribeStackEvents",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:CancelSpotInstanceRequests",
                "ec2>CreateRoute",
                "ec2>CreateSecurityGroup",
                "ec2>CreateTags",
                "ec2>DeleteRoute",
                "ec2>DeleteTags",
                "ec2>DeleteSecurityGroup",
                "ec2>DescribeAvailabilityZones",
                "ec2>DescribeAccountAttributes",
                "ec2>DescribeInstances",
                "ec2>DescribeKeyPairs",
                "ec2>DescribeRouteTables",
                "ec2>DescribeSecurityGroups",
                "ec2>DescribeSpotInstanceRequests",
                "ec2>DescribeSpotPriceHistory",
                "ec2>DescribeSubnets",
                "ec2>DescribeVpcAttribute",
                "ec2>DescribeVpcs",
                "ec2>DescribeRouteTables",
                "ec2>DescribeNetworkAcls",
                "ec2>CreateVpcEndpoint",
                "ec2>ModifyImageAttribute",
                "ec2>ModifyInstanceState",
                "ec2>RequestSpotInstances",
                "ec2>RevokeSecurityGroupEgress",
                "ec2>RunInstances",
                "ec2>TerminateInstances",
                "elasticmapreduce:*",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:ListPolicies"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

```
        "iam>ListRoles",
        "iam:PassRole",
        "kms>List*",
        "s3:*",
        "sdb:*",
        "support>CreateCase",
        "support>DescribeServices",
        "support>DescribeSeverityLevels"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "iam>CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "iam:AWSPropertyName": [
                "elasticmapreduce.amazonaws.com",
                "elasticmapreduce.amazonaws.com.cn"
            ]
        }
    }
}
]
```

Note

`ec2:TerminateInstances` 動作可讓 IAM 使用者終止與 IAM 帳戶相關聯的任何 Amazon EC2 執行個體 (即使這些並非是 EMR 叢集一部分)。

IAM 受管政策的唯讀存取

若要授予唯讀權限給 Amazon EMR，請連接 `AmazonElasticMapReduceReadOnlyAccess` 受管政策。此政策陳述式的內容顯示如下。`elasticmapreduce` 元素的萬用字元指定只允許以指定字串開頭的動作。請切記，因為此政策並未明確拒絕動作，不同的政策陳述式仍有可能用於授予指定動作存取權。

Note

由於 `AmazonElasticMapReduceReadOnlyAccess` 政策會自動更新，因此此處所示的政策可能已過期。使用 AWS Management Console 以檢視目前的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticmapreduce:Describe*",
                "elasticmapreduce>List*",
                "elasticmapreduce>ViewEventsFromAllClustersInConsole",
                "s3:GetObject",
                "s3>ListAllMyBuckets",
                "s3>ListBucket",
                "sdb>Select",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": "*"
        }
    ]
}
```

}

IAM 叢集和 EMR 筆記本以標籤為基礎的存取政策

您可以在身分類型政策中使用條件，來根據標籤控制對叢集和 EMR 筆記本的存取。

如需將標籤新增至叢集的詳細資訊，請參閱 [標記 EMR 叢集](#)。如需這些條件鍵的詳細資訊，請參閱 [條件金鑰 \(p. 155\)](#)。

以下範例示範以 Amazon EMR 條件金鑰使用條件運算子的不同情況和方式。這些 IAM 政策陳述式僅作示範用途，不應用於生產環境。有多種方法可以結合政策陳述式，以根據您的需求授予和拒絕許可。關於規劃與測試 IAM 政策，詳細資訊請參閱 [IAM User Guide](#)。

叢集的範例身分類型政策陳述式

以下範例示範會身分類型許可政策，這些政策會用來控制允許與 EMR 叢集搭配使用的動作。

僅在具有特定標籤值的叢集上允許動作

以下範例示範一個政策，讓使用者可根據有 *department* 值的 *dev* 叢集標籤執行動作，也讓使用者可用相同標籤標記叢集。最後一個政策範例示範如何在標記 EMR 叢集時，對該相同標籤以外的標籤拒絕權限。

Important

標記動作的明確拒絕許可是項重要的考量條件。這會防止使用者透過原本不要授予的叢集標籤，授予自身許可。若最後一個範例中所示的動作未遭到拒絕，使用者可以在任何叢集新增和移除想要的標籤，規避上述政策的意圖。

在以下政策範例中，`StringEquals` 條件運算子嘗試以 *dev* 標籤的值符合 *department*。若 *department* 標籤尚未新增到叢集，或不包含 *dev* 值，政策將無法套用，此政策也不允許動作。如果沒有其他政策陳述式允許動作，使用者只能使用具有此值標籤的叢集。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt12345678901234",  
            "Effect": "Allow",  
            "Action": [  
                "elasticmapreduce:DescribeCluster",  
                "elasticmapreduce>ListSteps",  
                "elasticmapreduce:TerminateJobFlows",  
                "elasticmapreduce:SetTerminationProtection",  
                "elasticmapreduce>ListInstances",  
                "elasticmapreduce>ListInstanceGroups",  
                "elasticmapreduce>ListBootstrapActions",  
                "elasticmapreduce:DescribeStep"  
            ],  
            "Resource": [  
                "*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:ResourceTag/department": "dev"  
                }  
            }  
        }  
    ]  
}
```

您也可以使用條件運算子來指定多個標籤值。例如，若要在 *department* 標籤包含 *dev* 或 *test* 值的叢集上允許所有動作，您可以用下列內容取代先前範例中的條件區塊。

```
"Condition": {  
    "StringEquals": {  
        "elasticmapreduce:ResourceTag/department": ["dev", "test"]  
    }  
}
```

如同在上述範例中，以下範例政策也尋找同樣符合的標籤：*dev* 標籤的 *department* 值。不過，在這種情況下，RequestTag 條件金鑰指定政策套用於標籤建立期間，因此使用者必須建立符合指定值的標籤。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1479334524000",  
            "Effect": "Allow",  
            "Action": [  
                "elasticmapreduce:RunJobFlow",  
                "iam:PassRole"  
            ],  
            "Resource": [  
                "*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:RequestTag/department": "dev"  
                }  
            }  
        }  
    ]  
}
```

在下列範例中，允許新增和移除標籤的 EMR 動作會結合指定在先前範例看過 StringNotEquals 標籤的 *dev* 運算子。此政策的效果是拒絕使用者在以包含 *department* 值的 *dev* 標籤所標記的 EMR 叢集上，新增或移除任何標籤的許可。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "elasticmapreduce:AddTags",  
                "elasticmapreduce:RemoveTags"  
            ],  
            "Condition": {  
                "StringNotEquals": {  
                    "elasticmapreduce:ResourceTag/department": "dev"  
                }  
            },  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

不論標籤值為何，在具有特定標籤的叢集上允許動作

您也可以只在具有特定標籤的叢集上允許動作，無論標籤的值為何。若要執行此操作，您可以使用 Null 運算子。如需詳細資訊，請參閱 IAM User Guide 中的 [用來檢查條件索引鍵是否存在的條件運算子](#)。例如，若只在具有 `department` 標籤的 EMR 叢集上允許動作，無論其包含的值為何，您可以用以下內容取代先前範例中的條件區塊。Null 運算子會在 EMR 叢集上尋找 `department` 標籤的存在。如果標籤存在，Null 陳述式會判斷為 `false`，符合此政策陳述式中指定的條件，並允許適當的動作。

```
"Condition": {  
    "Null": {  
        "elasticmapreduce:ResourceTag/department": "false"  
    }  
}
```

以下政策陳述式可讓使用者只在叢集具有可以包含任何值的 `department` 標籤時，才能建立 EMR 叢集。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "elasticmapreduce:RunJobFlow",  
                "iam:PassRole"  
            ],  
            "Condition": {  
                "Null": {  
                    "elasticmapreduce:RequestTag/department": "false"  
                }  
            },  
            "Effect": "Allow",  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

使用者需要在建立叢集時新增標籤

以下政策陳述式可讓使用者只在叢集建立時具有包含 `dev` 值的 `department` 標籤時，才能建立 EMR 叢集。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "elasticmapreduce:RunJobFlow",  
                "iam:PassRole"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:RequestTag/department": "dev"  
                }  
            },  
            "Effect": "Allow",  
            "Resource": [  
                "*"  
            ]  
        }  
    ]  
}
```

```
        "Resource": [
            "*"
        ]
    }
}
```

EMR 筆記本 的身分類型政策陳述式範例

本段中的 IAM 政策陳述式範例示範了常見的案例，利用索引鍵來限制使用 EMR 筆記本 時的允許動作。只要沒有其他的政策和允許動作的委託人 (使用者) 具有關聯，條件上下文索引鍵就會如範例所示，限制允許的動作。

Example – 只允許存取使用者利用標記所建立的筆記本

下列的範例政策陳述式在連接到角色或使用者時，會允許 IAM 使用者只使用自己已經建立的筆記本。此政策陳述式會使用在筆記本建立時套用的預設標籤。

在此範例中，`StringEquals` 條件運算子會嘗試將代表目前使用者 IAM 使用者 ID (`{aws:userId}`) 的變數，和 `creatorUserID` 標籤的值配對。如果 `creatorUserID` 標籤尚未新增到筆記本，或是未包含目前使用者 ID 的值，政策將無法套用，此政策也不允許動作。如果沒有其他政策陳述式允許這些動作，則使用者只能使用具有此標籤和此值的筆記本。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticmapreduce:DescribeEditor",
                "elasticmapreduce:StartEditor",
                "elasticmapreduce:StopEditor",
                "elasticmapreduce:DeleteEditor",
                "elasticmapreduce:OpenEditorInConsole"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:ResourceTag/creatorUserID": "${aws:userId}"
                }
            }
        }
    ]
}
```

Example – 在筆記本建立時要求筆記本標記

在此範例中使用了 `RequestTag` 上下文索引鍵。只有在使用者未變更或刪除預設新增的 `creatorUserID` 標籤時，才會允許 `CreateEditor` 動作。變數 `${aws:userId}` 會指定目前有效使用者的使用者 ID，這是標籤的預設值。

此政策陳述式可用來協助確保使用者不會移除 `createUserId` 標籤或變更其值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticmapreduce:CreateEditor"
            ],

```

```

        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:RequestTag/creatorUserId": "${aws:userid}"
            }
        }
    ]
}

```

此範例要求使用者建立叢集，此叢集的標籤包含索引鍵字串 `dept`，而且其值設定為下列其中一項：`datascience`、`analytics`、`operations`。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticmapreduce>CreateEditor"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:RequestTag/dept": [
                        "datascience",
                        "analytics",
                        "operations"
                    ]
                }
            }
        ]
    ]
}

```

Example – 限制只有加上標籤的叢集才能建立筆記本，而且要求筆記本標籤

只有當筆記本在建立時使用標籤，而此標籤包含索引鍵字串 `owner`，且設定為其中一個指定值時，此範例才會允許建立筆記本。此外，只有叢集的標籤包含索引鍵字串 `department`，且設定為其中一個指定值時，才可以建立筆記本。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticmapreduce>CreateEditor"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:RequestTag/owner": [
                        "owner1",
                        "owner2",
                        "owner3"
                    ],
                    "elasticmapreduce:ResourceTag/department": [
                        "dep1",
                        "dep3"
                    ]
                }
            }
        ]
    ]
}

```

```
        }
    ]
}
```

Example – 根據標籤來限制啟動筆記本的能力

此範例會設下限制，只有當筆記本的標籤包含索引鍵字串 `owner`，且設定為其中一個指定值時，才會讓這些筆記本擁有啟動筆記本的能力。由於 `Resource` 元素只用來指定 `editor`，因此條件不適用於叢集，而且不需要加上標籤。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "elasticmapreduce:StartEditor"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:elasticmapreduce:*:123456789012:editor/*",
      "Condition": {
        "StringEquals": {
          "elasticmapreduce:ResourceTag/owner": [
            "owner1",
            "owner2"
          ]
        }
      }
    ]
  }
}
```

此範例與上述的範例類似。不過，限制僅適用於加上標籤的叢集，而不適用於筆記本。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "elasticmapreduce:StartEditor"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:elasticmapreduce:*:123456789012:cluster/*",
      "Condition": {
        "StringEquals": {
          "elasticmapreduce:ResourceTag/department": [
            "dep1",
            "dep3"
          ]
        }
      }
    ]
  }
}
```

此範例使用不同的一組筆記本和叢集標籤。只有在下列的情況中，此範例才會允許筆記本啟動：

- 筆記本的標籤包含索引鍵字串 `owner`，且設定為任一指定值
—而且—
- 叢集的標籤包含索引鍵字串 `department`，且設定為任一指定值。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "elasticmapreduce:StartEditor"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:elasticmapreduce:*:123456789012:editor/*",  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:ResourceTag/owner": [  
                        "user1",  
                        "user2"  
                    ]  
                }  
            }  
        },  
        {  
            "Action": [  
                "elasticmapreduce:StartEditor"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:elasticmapreduce:*:123456789012:cluster/*",  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:ResourceTag/department": [  
                        "datascience",  
                        "analytics"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

Example – 根據標籤來限制開啟筆記本編輯器的能力

只有在下列的情況中，此範例才會允許開啟筆記本編輯器：

- 筆記本的標籤包含索引鍵字串 `owner`，且設定為任一指定值。
—而且—
- 叢集的標籤包含索引鍵字串 `department`，且設定為任一指定值。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "elasticmapreduce:OpenEditorInConsole"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:elasticmapreduce:*:123456789012:editor/*",  
            "Condition": {  
                "StringEquals": {  
                    "elasticmapreduce:ResourceTag/owner": [  
                        "user1",  
                        "user2"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```
        },
        {
            "Action": [
                "elasticmapreduce:OpenEditorInConsole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:elasticmapreduce:*:123456789012:cluster/*",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:ResourceTag/department": [
                        "datascience",
                        "analytics"
                    ]
                }
            }
        }
    ]
}
```

對 Amazon EMR 叢集節點進行驗證

SSH 用戶端可以使用 Amazon EC2 金鑰對來對叢集執行個體進行驗證。或者，搭配 Amazon EMR 5.10.0 發行版本或更新版本，您可以設定 Kerberos 來驗證使用者和連接到主節點的 SSH 連線。如需詳細資訊，請參閱 [使用 Kerberos 身份驗證 \(p. 190\)](#)。

主題

- [使用 SSH 登入資料的 Amazon EC2 金鑰對 \(p. 190\)](#)
- [使用 Kerberos 身份驗證 \(p. 190\)](#)

使用 SSH 登入資料的 Amazon EC2 金鑰對

Amazon EMR 叢集節點會在 Amazon EC2 執行個體上執行。您可以使用與連接到 Amazon EC2 執行個體的相同方式來連接叢集節點。您可以使用 Amazon EC2 建立金鑰對，也可以匯入金鑰對。建立叢集時，您可以指定對所有叢集執行個體的 SSH 連接所用的 Amazon EC2 金鑰對。您也可以不使用金鑰對建立叢集。這通常是透過會自動啟動、執行步驟，然後終止的暫時性叢集來完成。

您用於連接至叢集的 SSH 用戶端需要與此金鑰對相關的私有金鑰檔案。這個 .pem 檔案適用於使用 Linux、Unix 和 macOS 的 SSH 用戶端。您必須設定許可，只讓金鑰擁有者擁有檔案的存取許可。此為使用 Windows 的 SSH 用戶端 .ppk 檔案，而 .ppk 檔案通常是建立自 .pem 檔案。

- 如需關於建立 Amazon EC2 金鑰對的詳細資訊，請參閱 [Amazon EC2 User Guide for Linux Instances](#) 中的 [Amazon EC2 金鑰對](#)。
- 關於使用 PuTTYgen，從 .pem 檔案建立 .ppk 檔案，如需說明請參閱 [Amazon EC2 User Guide for Linux Instances](#) 中的 [使用 PuTTYgen 來轉換您的私密金鑰](#)。
- 關於設定 .pem 檔案許可，以及如何使用不同的方法，來連線到 EMR 叢集的主節點（包括從 Linux 或 macOS 使用 ssh、從 Windows 使用 PuTTY，或是從任何支援的作業系統使用 AWS CLI），請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

使用 Kerberos 身份驗證

Amazon EMR 5.10.0 發行版本和更新版本支援 Kerberos，此為由麻省理工學院 (MIT) 打造的網路身份驗證協定。Kerberos 使用私密金鑰加密，提供強式身份驗證，因此密碼或其他登入資料不會以未加密的格式透過網路傳送。

Kerberos 中需要驗證的服務和使用者稱為主體。主體存在於 Kerberos 領域中。在該領域中，稱為 金鑰分發中心 (KDC) 的 Kerberos 伺服器，會提供為主體進行身份驗證的方法。KDC 的做法是發出 票證 來進行身份驗證。KDC 維護在其領域中的主體資料庫、主體的密碼以及每個主體的其他管理資訊。KDC 也可接受來自其他領域中主體的身份驗證登入資料，這稱為 跨域信任。此外，EMR 叢集可以使用外部 KDC 來驗證主體。

建立跨域信任或使用外部 KDC 的常見案例是從 Active Directory 網域對使用者進行身份驗證。這可讓使用者在使用 SSH 連接到叢集或使用大數據應用程式時，使用他們的網域使用者帳戶來存取 EMR 叢集。

使用 Kerberos 身份驗證時，Amazon EMR 會為安裝在叢集上的應用程式、元件和子系統設定 Kerberos，使其可互相進行身份驗證。

Important

Amazon EMR 在跨域信任中不支援 AWS Directory Service for Microsoft Active Directory 或將其做為外部 KDC。

使用 Amazon EMR 設定 Kerberos 之前，我們建議您先熟悉 Kerberos 概念、在 KDC 上執行的服務、管理 Kerberos 服務的工具。如需詳細資訊，請參閱由 [Kerberos 聯盟](#) 發佈的 [MIT Kerberos 文件](#)。

主題

- [支援的應用程式 \(p. 191\)](#)
- [Kerberos 架構選項 \(p. 192\)](#)
- [在 Amazon EMR 上設定 Kerberos \(p. 200\)](#)
- [使用 SSH 連接到 Kerberos 化叢集 \(p. 207\)](#)
- [教學課程：設定叢集專用 KDC \(p. 208\)](#)
- [教學課程：使用 Active Directory 網域設定跨域信任 \(p. 210\)](#)

支援的應用程式

在 EMR 叢集中，Kerberos 主體是在所有叢集節點上執行的大數據應用程式服務和子系統。Amazon EMR 可以設定下列的應用程式和元件使用 Kerberos。每個應用程式都有與其相關的 Kerberos 使用者主體。

Amazon EMR 不支援將跨域信任用於 AWS Directory Service for Microsoft Active Directory。

Amazon EMR 只會針對下列的應用程式和元件，設定開放原始碼 Kerberos 身份驗證功能。任何其他安裝的應用程式都未 Kerberos 化，可能導致無法與 Kerberos 化的元件通訊，並造成應用程式錯誤。未 Kerberos 化的應用程式和元件無法啟用身份驗證。支援的應用程式和元件可能會因 Amazon EMR 發行版本而有所差異。

託管於叢集上的 Web 使用者界面皆未 Kerberos 化。

- HDFS
- YARN
- Tez
- Hadoop MapReduce
- Hbase
- HCatalog
- Hive
 - 請不要使用 LDAP 身份驗證啟用 Hive。這可能會導致和 Kerberos 化 YARN 的通訊問題。
- Hue
 - Hue 使用者身份驗證未自動設定，可使用組態 API 以設定。

- Hue 伺服器已 Kerberos 化。Hue 前端 (UI) 並未為身份驗證設定。可為 Hue UI 設定 LDAP 身份驗證。
- Livy
- Oozie
- Spark
- Zeppelin
 - Zeppelin 只會設定為以 Spark 解譯器搭配 Kerberos 使用。其並未為其他轉譯器設定。
 - Kerberos 的 Zeppelin 模擬不受支援。登入 Zeppelin 的所有使用者使用相同的 Zeppelin 使用者主體，以執行 Spark 任務並驗證 YARN。
- Zookeeper
 - Zookeeper 用戶端不受支援。

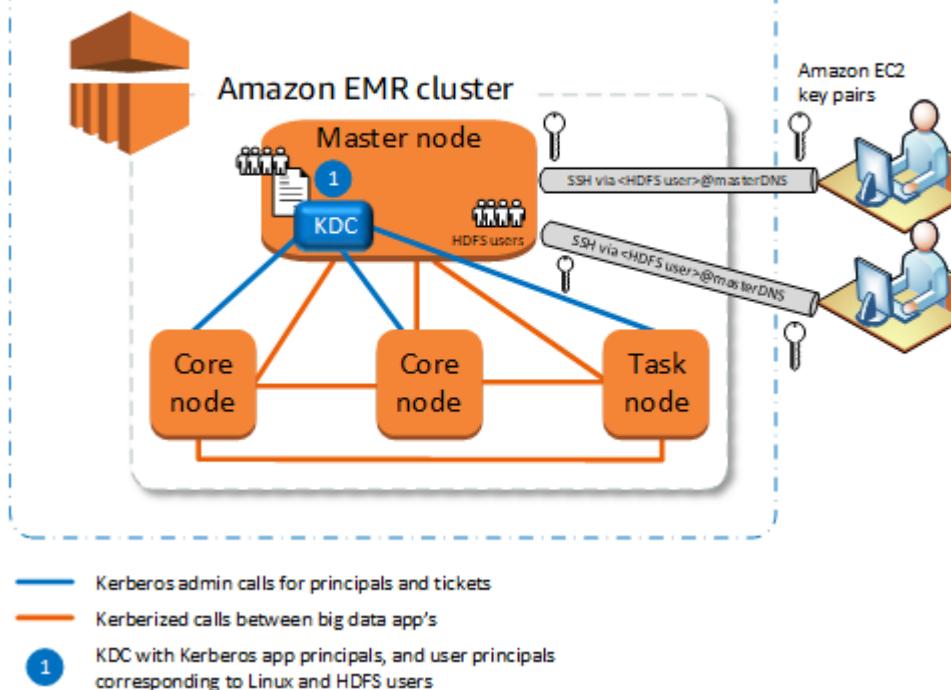
Kerberos 架構選項

使用 Kerberos 搭配 Amazon EMR 時，您可以從本節所列的架構中進行選擇。無論選擇哪個架構，請使用相同的步驟來設定 Kerberos。您建立安全組態、在建立叢集時指定安全組態和相容的叢集特定 Kerberos 選項，並在符合 KDC 中使用者主體的叢集上，為 Linux 使用者建立 HDFS 目錄。如需組態選項的說明和每個架構的範例組態，請參閱在 [Amazon EMR 上設定 Kerberos \(p. 200\)](#)。

叢集專用 KDC (主節點上的 KDC)

這個組態可在 Amazon EMR 5.10.0 發行版本和更新版本中使用。

--- Kerberos realm (for example, EC2.INTERNAL) ---



優點

- Amazon EMR 具有完整的 KDC 擁有權。

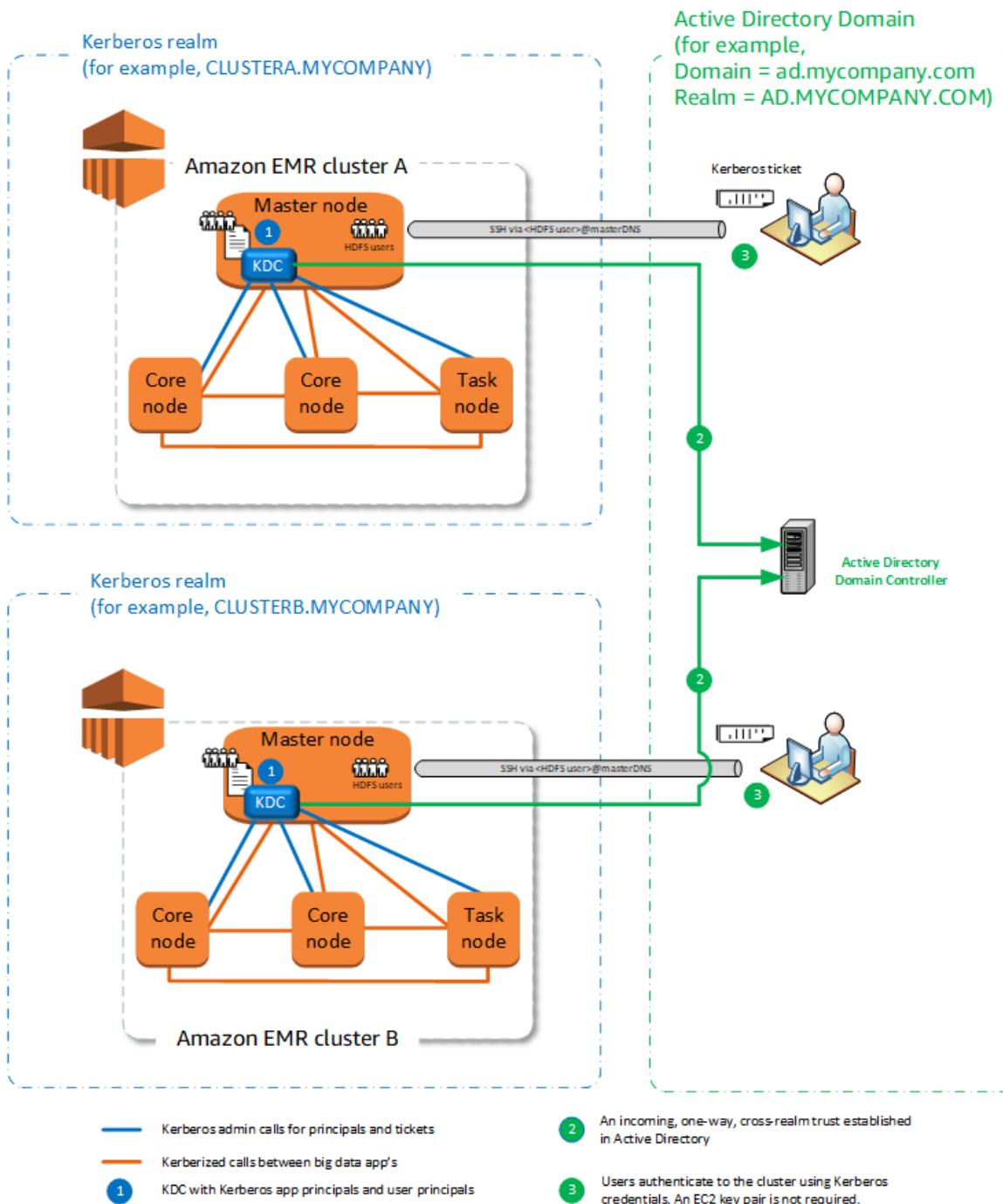
- EMR 叢集上的 KDC 獨立於集中式 KDC 實作，例如 Microsoft Active Directory 或 AWS Managed Microsoft AD。
- 對效能的影響微乎其微，因為 KDC 僅管理叢集中本機節點的身份驗證。
- 或者，其他 Kerberos 化的叢集可以參考 KDC 做為外部 KDC。如需更多詳細資訊，請參閱 [外部 KDC—不同叢集上的主節點 \(p. 196\)](#)。

考量事項與限制

- Kerberos 化叢集不能相互驗證，所以應用程式無法相互運作。如果叢集應用程式需要相互運作，您必須在叢集之間建立跨域信任，或設定一個叢集做為其他叢集的外部 KDC。如果建立跨域信任，KDC 必須有不同的 Kerberos 領域。
- 您必須在對應到 KDC 使用者主體的主節點 EC2 執行個體上建立 Linux 使用者，以及每個使用者 HDFS 目錄。
- 使用者主體必須使用 EC2 私有金鑰檔案和 `kinit` 登入資料，以使用 SSH 連接到叢集。

跨域信任

在這個組態中，來自不同 Kerberos 領域的主體 (通常是使用者) 會向 Kerberos 化 EMR 叢集上的應用程式元件進行驗證，此叢集具有自己的 KDC。主節點上的 KDC 會使用同時存在兩個 KDC 中的 跨域主體，與另一個 KDC 建立信任關係。每個 KDC 中的主體名稱和密碼完全相符。跨域信任最常用於 Active Directory 實作，如下圖所示。也支援在外部 MIT KDC 或另一個 Amazon EMR 叢集上之 KDC 的跨域信任。



優點

- 安裝 KDC 的 EMR 叢集保有 KDC 的完整擁有權。
- 使用 Active Directory 時，Amazon EMR 會自動建立對應至 KDC 上使用者主體的 Linux 使用者。您仍必須為每個使用者建立 HDFS 目錄。此外，Active Directory 網域中的使用者主體可以使用 kinit 登入資料來存取 Kerberos 化叢集，無需使用 EC2 私有金鑰檔案。如此就無需在叢集使用者之間共用私有金鑰檔案。
- 因為每個叢集 KDC 管理叢集中節點的身份驗證，因此網路延遲和處理成本對叢集中大量節點的影響可降至最低。

考量事項與限制

- 如果您要與 Active Directory 領域建立信任，您必須提供當您建立叢集時具備將主體加入網域之許可的 Active Directory 使用者名稱和密碼。
- 跨域信任無法在具有相同名稱的 Kerberos 領域之間建立。
- 跨域信任必須明確建立。例如，如果叢集 A 和叢集 B 都與 KDC 建立跨域信任，他們本質上並不會彼此信任，其應用程式也無法相互進行身份驗證以相互運作。
- KDC 必須獨立地加以維持和協調，使用者主體的登入資料才能完全相符。

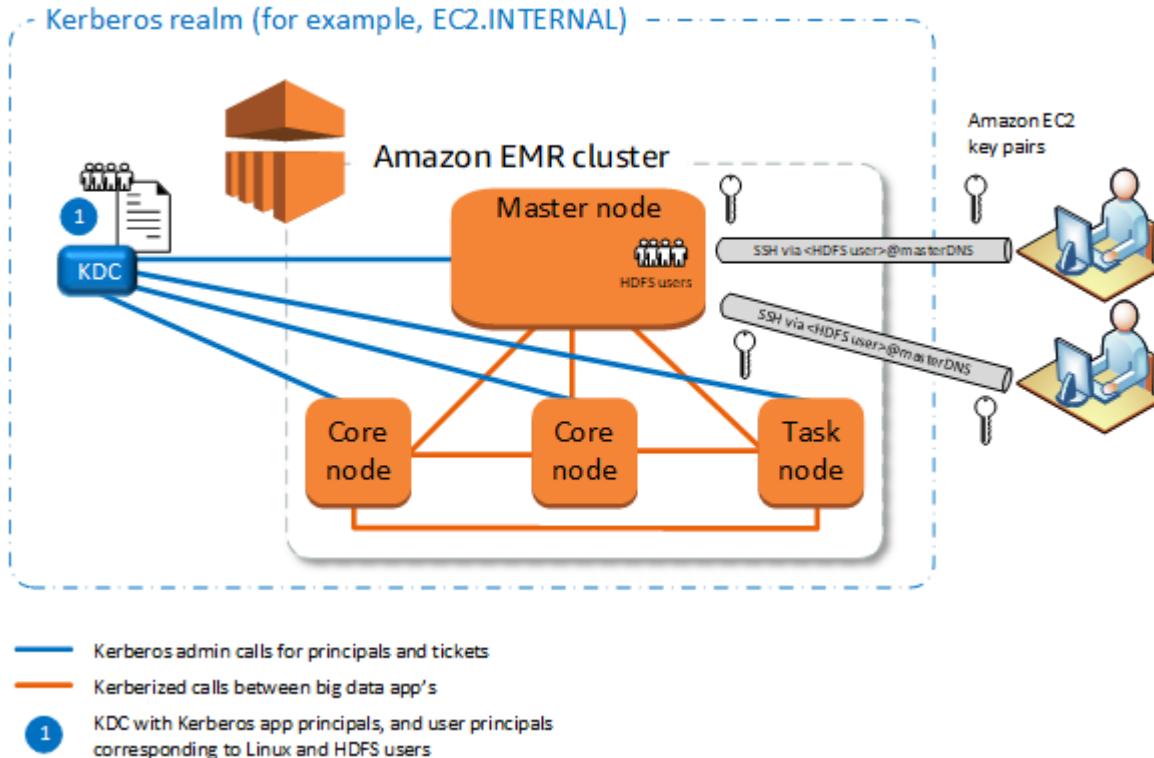
外部 KDC

Amazon EMR 5.20.0 和更高版本支援搭配外部 KDC 的組態。

- [外部 KDC—MIT KDC \(p. 195\)](#)
- [外部 KDC—不同叢集上的主節點 \(p. 196\)](#)
- [外部 KDC—叢集 KDC 位於具有 Active Directory 跨域信任的不同叢集上 \(p. 198\)](#)

外部 KDC—MIT KDC

此組態允許一或多個 EMR 叢集使用在 MIT KDC 伺服器中定義和維護的主體。



優點

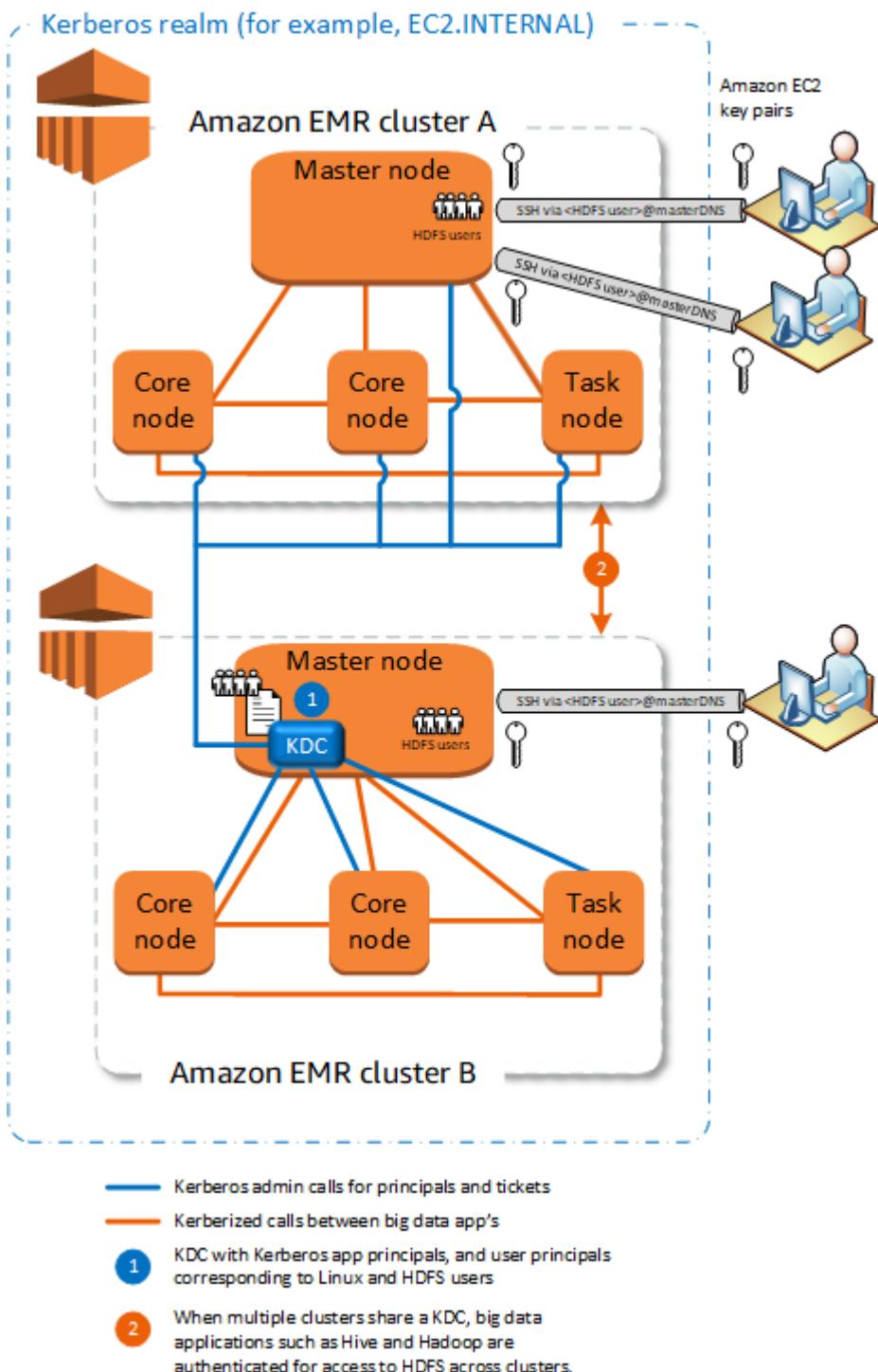
- 主體管理已整合至單一 KDC。
- 多個叢集可以使用相同 Kerberos 領域中的相同 KDC。與跨域信任相較，這可讓叢集應用程式相互運作，並簡化叢集之間的通訊身份驗證。
- Kerberos 化叢集上的主節點無須承受維護 KDC 的相關效能負擔。

考量事項與限制

- 您必須在對應到 KDC 使用者主體之每個 Kerberos 化叢集主節點的 EC2 執行個體上建立 Linux 使用者，以及每個使用者 HDFS 目錄。
- 使用者主體必須使用 EC2 私有金鑰檔案和 kinit 登入資料，以使用 SSH 連接到 Kerberos 化叢集。
- Kerberos 化 EMR 叢集中的每個節點都必須有連到 KDC 的網路路由。
- Kerberos 化叢集中的每個節點都會對外部 KDC 造成身份驗證負擔，因此 KDC 的組態會影響叢集效能。設定 KDC 伺服器的硬體時，請考慮能同時支援的最大 Amazon EMR 節點數。
- 叢集效能取決於 Kerberos 化叢集中節點和 KDC 之間的網路延遲。
- 由於不同的因素相互牽連，疑難排解會比較困難。

外部 KDC—不同叢集上的主節點

此組態幾乎等同於上述的外部 MIT KDC 實作，除了 KDC 位於 EMR 叢集的主節點上。如需更多詳細資訊，請參閱 [叢集專用 KDC \(主節點上的 KDC\) \(p. 192\)](#) 及 [教學課程：使用 Active Directory 網域設定跨域信任 \(p. 210\)](#)。



優點

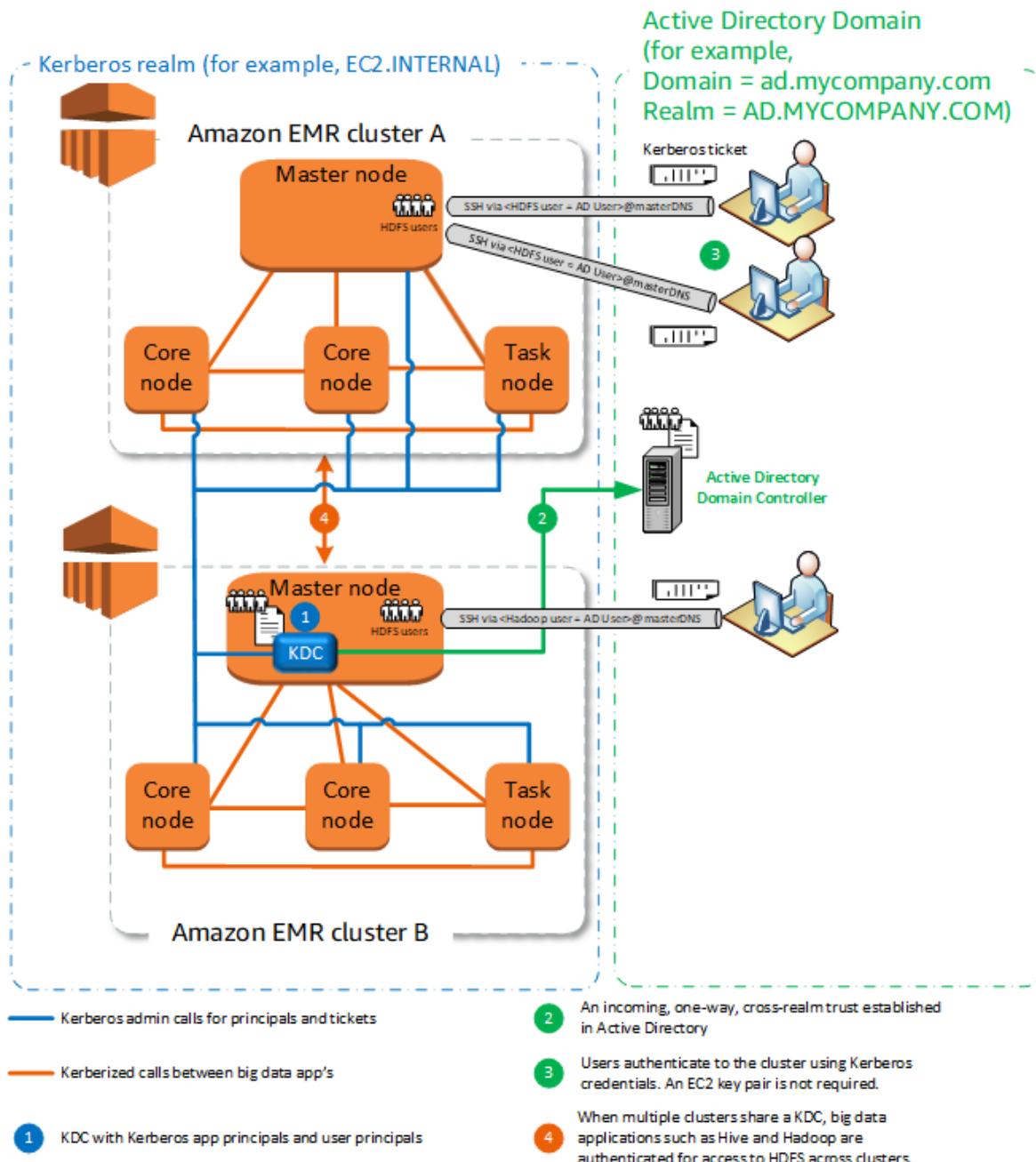
- 主體管理已整合至單一 KDC。
- 多個叢集可以使用相同 Kerberos 領域中的相同 KDC。這可讓叢集應用程式與 Kerberos 化叢集相互運作。相較於跨域信任，它還能簡化叢集間通訊的身份驗證。

考量事項與限制

- 您必須在對應到 KDC 使用者主體之每個 Kerberos 化叢集主節點的 EC2 執行個體上建立 Linux 使用者，以及每個使用者 HDFS 目錄。
- 使用者主體必須使用 EC2 私有金鑰檔案和 kinit 登入資料，以使用 SSH 連接到 Kerberos 化叢集。
- 每個 EMR 叢集中的每個節點都必須有連到 KDC 的網路路由。
- Kerberos 化叢集中的每個 Amazon EMR 節點都會對外部 KDC 帶來身份驗證負擔，因此 KDC 的組態會影響叢集效能。設定 KDC 伺服器的硬體時，請考慮能同時支援的最大 Amazon EMR 節點數。
- 叢集效能取決於叢集中節點和 KDC 之間的網路延遲。
- 由於不同的因素相互牽連，疑難排解會比較困難。

外部 KDC—叢集 KDC 位於具有 Active Directory 跨域信任的不同叢集上

在這個組態中，您先使用與 Active Directory 具有單向跨域信任的叢集專用 KDC，來建立叢集。如需詳細教學，請參閱[教學課程：使用 Active Directory 網域設定跨域信任 \(p. 210\)](#)。接著啟動其他叢集，參考具有信任的叢集 KDC 做為外部 KDC。如需範例，請參閱「[外部叢集 KDC 搭配 Active Directory 跨域信任 \(p. 204\)](#)」。這可讓使用外部 KDC 的每個 Amazon EMR 叢集，驗證在 Microsoft Active Directory 網域中定義和維護的主體。



優點

- 管理主體已合併至 Active Directory 網域。
- Amazon EMR 加入 Active Directory 領域，因此無須建立對應至 Active Directory 使用者的 Linux 使用者。您仍必須為每個使用者建立 HDFS 目錄。
- 多個叢集可以使用相同 Kerberos 領域 (不同於 Active Directory 領域) 中的相同 KDC。這可讓叢集應用程式相互運作。
- Active Directory 網域中的使用者主體可以使用 kinit 登入資料來存取 Kerberos 化叢集，無需使用 EC2 私有金鑰檔案。這讓您不必在叢集使用者之間共用私有金鑰檔案。

- 只有一個 Amazon EMR 主節點需負擔維護 KDC 的責任，而且只有該叢集必須使用 Active Directory 登入資料來建立 KDC 和 Active Directory 之間的跨域信任。

考量事項與限制

- 每個 EMR 叢集中的每個節點都必須有連到 KDC 和 Active Directory 網域控制器的網路路由。
- 每個 Amazon EMR 節點都會對外部 KDC 造成身份驗證負擔，因此 KDC 的組態會影響叢集效能。設定 KDC 伺服器的硬體時，請考慮能同時支援的最大 Amazon EMR 節點數。
- 叢集效能取決於叢集中節點和 KDC 伺服器之間的網路延遲。
- 由於不同的因素相互牽連，疑難排解會比較困難。

在 Amazon EMR 上設定 Kerberos

本節提供使用常見架構設定 Kerberos 的組態詳細資訊和範例。無論您選擇哪個架構，組態基本知識都相同，並以三個步驟完成。如果您使用外部 KDC 或設定跨域信任，您必須確保叢集中的每個節點都有連到外部 KDC 的網路路由，包括設定適用的安全群組，以允許傳入和傳出 Kerberos 流量。

步驟 1：使用 Kerberos 屬性建立安全組態

安全組態指定 Kerberos KDC 的詳細資訊，並允許每次建立叢集時重複使用 Kerberos 組態。您可以使用 Amazon EMR 主控台、AWS CLI 或 MR API 來建立安全組態。安全組態也可以包含其他安全性選項，例如加密。如需建立安全組態以及在建立叢集時指定安全組態的詳細資訊，請參閱 [使用安全組態設定叢集安全性 \(p. 128\)](#)。如需安全組態中 Kerberos 屬性的詳細資訊，請參閱 [安全組態的 Kerberos 設定 \(p. 201\)](#)。

步驟 2：建立叢集，並指定叢集特定的 Kerberos 屬性

當您建立叢集時，需指定 Kerberos 安全組態以及叢集特定的 Kerberos 選項。使用 Amazon EMR 主控台時，只能使用與指定之安全組態相容的 Kerberos 選項。使用 AWS CLI 或 Amazon EMR API 時，請務必只指定與所指定安全組態相容的 Kerberos 選項。例如，如果使用 CLI 建立叢集時，指定了跨域信任的主體密碼，但指定的安全組態並非使用跨域信任參數來設定，就會發生錯誤。如需更多詳細資訊，請參閱 [叢集的 Kerberos 設定 \(p. 202\)](#)。

步驟 3：設定叢集主節點

根據您的架構和實作需求，可能需在叢集上進行其他設定。您可以在建立之後再進行設定，或在建立過程中使用步驟或引導操作。

對於每個使用 SSH 連接到叢集的 Kerberos 驗證使用者，您必須確保建立對應到 Kerberos 使用者的 Linux 使用者帳戶。如果使用者主體由 Active Directory 網域控制器提供（以外部 KDC 的形式或透過跨域信任的方式），Amazon EMR 會自動建立 Linux 使用者帳戶。如果未使用 Active Directory，您必須為每個對應到 Linux 使用者的使用者建立主體。如需更多詳細資訊，請參閱 [為 Kerberos 驗證的 HDFS 使用者和 SSH 連線設定叢集 \(p. 205\)](#)。

每個使用者還必須擁有自己的 HDFS 使用者目錄，您也必須建立這些目錄。此外，SSH 必須設定為啟用 GSSAPI，以允許來自 Kerberos 驗證使用者的連線。主節點上必須啟用 GSSAPI，且必須設定用戶端 SSH 應用程式為使用 GSSAPI。如需更多詳細資訊，請參閱 [為 Kerberos 驗證的 HDFS 使用者和 SSH 連線設定叢集 \(p. 205\)](#)。

Amazon EMR 上的 Kerberos 安全組態和叢集設定

當您建立 Kerberos 化叢集時，便指定安全組態以及專屬於叢集的 Kerberos 屬性。您不能指定其中一組而不指定另一組，否則會發生錯誤。

本主題提供當您建立安全組態和叢集時，可用於 Kerberos 的組態參數概觀。此外，也為常見架構提供建立相容安全組態和叢集的 CLI 範例。

安全組態的 Kerberos 設定

您可以使用 Amazon EMR 主控台、AWS CLI 或 EMR API，來建立指定 Kerberos 屬性的安全組態。安全組態也可以包含其他安全性選項，例如加密。如需更多詳細資訊，請參閱 [建立安全組態 \(p. 129\)](#)。

使用以下參考以了解您所選 Kerberos 架構的可用安全組態設定。顯示的是 Amazon EMR 主控台設定。如需對應的 CLI 選項，請參閱 [使用 AWS CLI 指定 Kerberos 設定 \(p. 139\)](#) 或 [組態範例 \(p. 203\)](#)。

參數	描述
Kerberos	指定使用此安全組態的叢集啟用 Kerberos。如果有叢集使用此安全組態，則該叢集也必須指定 Kerberos 設定，否則會發生錯誤。
提供者	叢集專用 KDC 指定 Amazon EMR 在任何使用此安全組態的主節點上建立 KDC。在建立叢集時，您可以指定領域名稱和 KDC 管理員密碼。 如有需要，您可以從其他叢集參考這個 KDC。使用不同的安全組態建立這些叢集，指定外部 KDC，並且使用您為叢集專用 KDC 指定的領域名稱和 KDC 管理員密碼。
	外部 KDC 僅適用於 Amazon EMR 5.20.0 和更新版本。指定使用此安全組態的叢集透過叢集外的 KDC 伺服器來驗證 Kerberos 主體。KDC 不在叢集上建立。在建立叢集時，您可以指定外部 KDC 的領域名稱和 KDC 管理員密碼。
票證生命週期	選用。指定 KDC 所發行之 Kerberos 票證在使用此安全組態之叢集上有效的期間。 由於安全理由，票證的生命週期有限。叢集應用程式和服務會在票證過期後自動續約。使用 Kerberos 登入資料透過 SSH 連接至叢集的使用者，必須從主節點命令列執行 <code>kinit</code> ，以在票證過期後續約。
跨域信任	針對在不同 Kerberos 領域內使用此安全組態和 KDC 的叢集，指定其中叢集專用 KDC 之間的跨域信任。 來自另一個領域的委託人 (通常為使用者) 就會通過使用此組態之叢集的驗證。另一個 Kerberos 領域則必須額外設定。如需更多詳細資訊，請參閱 教學課程：使用 Active Directory 網域設定跨域信任 (p. 210) 。
跨域信任屬性	領域 為信任關係中的另一個領域指定 Kerberos 領域名稱。根據慣例，Kerberos 領域名稱與網域名稱相同，但全部採用大寫字母。
	網域 為信任關係中的另一個領域指定網域名稱。
	管理伺服器 為信任關係中的另一個領域指定管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如， <code>domain.example.com:749</code>)。

參數	描述	
	KDC 伺服器	為信任關係中的另一個領域指定 KDC 伺服器的完整網域名稱 (FQDN) 或 IP 地址。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 88)。
外部 KDC		指定該叢集外部 KDC 應由該叢集使用。
外部 KDC 屬性	管理伺服器	指定外部管理伺服器的完整網域名稱 (FQDN) 或 IP 地址。管理伺服器和 KDC 伺服器通常會在相同機器上執行，並使用同樣的 FQDN，但會透過不同連接埠進行通訊。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 749。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 749)。
	KDC 伺服器	指定外部 KDC 伺服器的完整網域名稱 (FQDN)。KDC 伺服器和管理伺服器通常會以相同 FQDN 在相同機器上執行，但使用不同的連接埠。 如未指定連接埠，則系統會使用 Kerberos 預設的連接埠 88。或者，您亦可以選擇指定連接埠 (例如，domain.example.com: 88)。
Active Directory 整合		指定 Kerberos 主體身份驗證與 Microsoft Active Directory 網域整合。
Active Directory 整合屬性	Active Directory 領域	指定 Active Directory 網域的 Kerberos 領域名稱。根據慣例，Kerberos 領域名稱通常與網域名稱相同，但全部採用大寫字母。
	Active Directory 網域	指定 Active Directory 網域名稱。
	Active Directory 伺服器	指定 Microsoft Active Directory 網域控制站的完整網域名稱 (FQDN)。

叢集的 Kerberos 設定

您可以在使用 Amazon EMR 主控台、AWS CLI 或 EMR API 建立叢集時，指定 Kerberos 設定。

使用以下參考以了解您所選 Kerberos 架構的可用叢集組態設定。顯示的是 Amazon EMR 主控台設定。如需對應的 CLI 選項，請參閱 [組態範例 \(p. 203\)](#)。

參數	描述
Realm (領域)	叢集的 Kerberos 領域名稱。Kerberos 慣例是將此設定為與網域名稱相同，但採用大寫字母。例如，若為 ec2.internal 網域，則使用 EC2.INTERNAL 為領域名稱。

參數	描述
KDC 管理員密碼	用於 kadmin 或 kadmin.local 叢集中的密碼。這些是 Kerberos V5 管理系統的命令列界面，維護 Kerberos 主體、密碼政策、叢集的 keytab。
跨域信任主體密碼 (選用)	建立跨域信任時為必要。跨域主體密碼在各領域中必須毫無二致。使用高強度密碼。
Active Directory 網域參與使用者 (選用)	在跨域信任使用 Active Directory 時為必要。這是 Active Directory 帳戶的使用者登入名稱，並具有將電腦加入網域的許可。Amazon EMR 會使用此身分來將叢集加入網域。如需更多詳細資訊，請參閱 the section called “步驟 3：新增使用者帳戶到 EMR 叢集的網域” (p. 211) 。
Active Directory 網域參與密碼 (選用)	Active Directory 網域參與使用者的密碼。如需更多詳細資訊，請參閱 the section called “步驟 3：新增使用者帳戶到 EMR 叢集的網域” (p. 211) 。

組態範例

以下範例示範常見情況的安全組態和叢集組態。為簡潔起見，顯示的是 AWS CLI 命令。

本機 KDC

以下命令使用在主節點上執行的叢集專用 KDC 來建立叢集。可能需要在叢集上設定其他組態。如需更多詳細資訊，請參閱 [為 Kerberos 驗證的 HDFS 使用者和 SSH 連線設定叢集 \(p. 205\)](#)。

建立安全組態

```
aws emr create-security-configuration --name LocalKDCSecurityConfig \
--security-configuration '[{"AuthenticationConfiguration": \
{"KerberosConfiguration": {"Provider": "ClusterDedicatedKdc", \
"ClusterDedicatedKdcConfiguration": {"TicketLifetimeInHours": 24 }}}}'
```

建立叢集

```
aws emr create-cluster --release-label emr-5.28.0 \
--instance-count 3 --instance-type m5.xlarge \
--applications Name=Hadoop Name=Hive --ec2-attributes \
InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2Key \
--service-role EMR_DefaultRole \
--security-configuration LocalKDCSecurityConfig \
--kerberos-attributes Realm=EC2.INTERNAL,KdcAdminPassword=MyPassword
```

叢集專用 KDC 搭配 Active Directory 跨域信任

以下命令使用在主節點上執行的叢集專用 KDC，搭配 Active Directory 網域的跨域信任來建立叢集。可能需要在叢集和 Active Directory 上設定其他組態。如需更多詳細資訊，請參閱 [教學課程：使用 Active Directory 網域設定跨域信任 \(p. 210\)](#)。

建立安全組態

```
aws emr create-security-configuration --name LocalKDCWithADTrustSecurityConfig \
--security-configuration '[{"AuthenticationConfiguration": \
{"KerberosConfiguration": {"Provider": "ClusterDedicatedKdc", \
```

```
"ClusterDedicatedKdcConfiguration": {"TicketLifetimeInHours": 24, \
"CrossRealmTrustConfiguration": {"Realm":"AD.DOMAIN.COM", \
"Domain":"ad.domain.com", "AdminServer":"ad.domain.com", \
"KdcServer":"ad.domain.com"}}}}'
```

建立叢集

```
aws emr create-cluster --release-label emr-5.28.0 \
--instance-count 3 --instance-type m5.xlarge --applications Name=Hadoop Name=Hive \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2Key \
--service-role EMR_DefaultRole --security-configuration KDCWithADTrustSecurityConfig \
--kerberos-attributes Realm=EC2.INTERNAL,KdcAdminPassword=MyClusterKDCAdminPassword, \
ADDomainJoinUser=ADUserLogonName,ADDomainJoinPassword=ADUserPassword, \
CrossRealmTrustPrincipalPassword=MatchADTrustPassword
```

不同叢集上的外部 KDC

以下命令會建立叢集，參考不同叢集之主節點上的叢集專用 KDC，以驗證主體身分。可能需要在叢集上設定其他組態。如需更多詳細資訊，請參閱 [為 Kerberos 驗證的 HDFS 使用者和 SSH 連線設定叢集 \(p. 205\)](#)。

建立安全組態

```
aws emr create-security-configuration --name ExtKDCOnDifferentCluster \
--security-configuration '{"AuthenticationConfiguration": \
{"KerberosConfiguration": {"Provider": "ExternalKdc", \
"ExternalKdcConfiguration": {"KdcServerType": "Single", \
"AdminServer": "MasterDNSOfKDCMaster:749", \
"KdcServer": "MasterDNSOfKDCMaster:88"}}}}'
```

建立叢集

```
aws emr create-cluster --release-label emr-5.28.0 \
--instance-count 3 --instance-type m5.xlarge \
--applications Name=Hadoop Name=Hive \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2Key \
--service-role EMR_DefaultRole --security-configuration ExtKDCOnDifferentCluster \
--kerberos-attributes Realm=EC2.INTERNAL,KdcAdminPassword=KDCOnMasterPassword
```

外部叢集 KDC 搭配 Active Directory 跨域信任

下列命令會建立不含 KDC 的叢集。叢集會參考在其他叢集之主節點上執行的叢集專用 KDC，以驗證主體身分。KDC 與 Active Directory 網域控制站具有跨域信任。可能需要在具有 KDC 的主節點上設定其他組態。如需更多詳細資訊，請參閱 [教學課程：使用 Active Directory 網域設定跨域信任 \(p. 210\)](#)。

建立安全組態

```
aws emr create-security-configuration --name ExtKDCWithADIntegration \
--security-configuration '{"AuthenticationConfiguration": \
{"KerberosConfiguration": {"Provider": "ExternalKdc", \
"ExternalKdcConfiguration": {"KdcServerType": "Single", \
"AdminServer": "MasterDNSofClusterKDC:749", \
"KdcServer": "MasterDNSofClusterKDC.com:88", \
"AdIntegrationConfiguration": {"AdRealm":"AD.DOMAIN.COM", \
"AdDomain":"ad.domain.com"}}}}'
```

建立叢集

```
aws emr create-cluster --release-label emr-5.28.0 \
```

```
--instance-count 3 --instance-type m5.xlarge --applications Name=Hadoop Name=Hive \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2Key \
--service-role EMR_DefaultRole --security-configuration ExtKDCWithADIntegration \
--kerberos-attributes Realm=EC2.INTERNAL,KdcAdminPassword=KDCOnMasterPassword, \
ADDDomainJoinUser=MyPrivilegedADUserName,ADDDomainJoinPassword=PasswordForADDomainJoinUser
```

為 Kerberos 驗證的 HDFS 使用者和 SSH 連線設定叢集

Amazon EMR 會為叢集上執行的應用程式，建立 Kerberos 驗證的使用者用戶端—例如，hadoop 使用者和 spark 使用者等。您也可以新增使用 Kerberos 驗證至叢集程序的使用者。已驗證的使用者接著可以使用其 Kerberos 登入資料連接到叢集並使用應用程式。對於要對叢集進行驗證的使用者，需要以下組態：

- 叢集上必須存在符合 KDC 中 Kerberos 主體的 Linux 使用者帳戶。Amazon EMR 會在與 Active Directory 整合的架構中自動完成這個步驟。
- 您必須在主節點上為每個使用者建立 HDFS 使用者目錄，並提供該目錄的使用者許可。
- 您必須設定 SSH 服務，以便在主節點上啟用 GSSAPI。此外，使用者必須有啟用 GSSAPI 的 SSH 用戶端。

將 Linux 使用者和 Kerberos 主體新增至主節點

如果您不使用 Active Directory，您必須在叢集主節點上建立 Linux 帳戶，並將這些 Linux 使用者的主體新增到 KDC。這包含主節點的 KDC 主體。除了使用者主體，主節點上執行的 KDC 需要本機主機的主體。

當您的架構包含 Active Directory 整合，系統會自動建立本機 KDC 上的 Linux 使用者和主體 (如果適用)。您可以略過此步驟。如需更多詳細資訊，請參閱 [跨域信任 \(p. 193\)](#) 及 [外部 KDC—叢集 KDC 位於具有 Active Directory 跨域信任的不同叢集上 \(p. 198\)](#)。

Important

由於主節點使用暫時性儲存區，所以主節點終止時，KDC 和委託人的資料庫都會遺失。如果您為 SSH 連接建立使用者，建議您可以與設定為高可用性的外部 KDC 建立跨域信任機制。或者，如果您以 Linux 使用者帳戶為 SSH 連接建立使用者，請使用引導操作和指令碼自動化帳戶建立程序，讓您建立新叢集時可以重複。

在建立時或建立叢集後提交步驟到叢集，是新增使用者和 KDC 主體的最簡單方法。或者，您也可以使用 EC2 金鑰對連接到主節點，做為執行命令的預設 hadoop 使用者。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

以下範例會將 bash 指令碼 `configureCluster.sh` 提交至已存在的叢集 (參考其叢集 ID)。指令碼會儲存至 Amazon S3。

```
aws emr add-steps --cluster-id j-01234567 \
--steps Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE, \
Jar=s3://myregion.elasticmapreduce/libs/script-runner/script-runner.jar, \
Args=[ "s3://mybucket/configureCluster.sh" ]
```

以下範例示範 `configureCluster.sh` 指令碼的內容。指令碼也會處理建立 HDFS 使用者目錄並啟用 SSH 的 GSSAPI，這些程序將在以下章節中介紹。

```
#!/bin/bash
#Add a principal to the KDC for the master node, using the master node's returned host name
sudo kadmin.local -q "ktadd -k /etc/krb5.keytab host/`hostname -f`"
#Declare an associative array of user names and passwords to add
declare -A arr
arr=(["lijuan"]=pwd1 ["marymajor"]=pwd2 ["richardroe"]=pwd3)
for i in ${!arr[@]}; do
```

```
#Assign plain language variables for clarity
name=${i}
password=${arr[$i]}

# Create a principal for each user in the master node and require a new password on
first logon
sudo kadmin.local -q "addprinc -pw $password +needchange $name"

#Add hdfs directory for each user
hdfs dfs -mkdir /user/$name

#Change owner of each user's hdfs directory to that user
hdfs dfs -chown $name:$name /user/$name
done

# Enable GSSAPI authentication for SSH and restart SSH service
sudo sed -i 's/^.*GSSAPIAuthentication.*$/GSSAPIAuthentication yes/' /etc/ssh/sshd_config
sudo sed -i 's/^.*GSSAPICleanupCredentials.*$/GSSAPICleanupCredentials yes/' /etc/ssh/
sshd_config
sudo /etc/init.d/sshd restart
```

新增使用者 HDFS 目錄

若要讓您的使用者登入叢集以執行 Hadoop 任務，您必須為 Linux 使用者帳戶新增 HDFS 使用者目錄，並授予每位使用者目錄的所有權。

在建立時或建立叢集後提交步驟到叢集，是建立 HDFS 目錄的最簡單方法。或者，您也可以使用 EC2 金鑰對連接到主節點，做為執行命令的預設 hadoop 使用者。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

以下範例會將 bash 指令碼 AddHDFSUsers.sh 提交至已存在的叢集 (參考其叢集 ID)。指令碼會儲存至 Amazon S3。

```
aws emr add-steps --cluster-id ClusterID \
--steps Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE, \
Jar=s3://MyRegion.elasticmapreduce/libs/script-runner/script-runner.jar,Args=[ "s3:// \
MyBucketPath/AddHDFSUsers.sh" ]
```

以下範例示範 AddHDFSUsers.sh 指令碼的內容。

```
#!/bin/bash
# AddHDFSUsers.sh script

# Initialize an array of user names from AD, or Linux users created manually on the cluster
ADUSERS=("lijuan" "marymajor" "richardroe" "myusername")

# For each user listed, create an HDFS user directory
# and change ownership to the user

for username in ${ADUSERS[@]}; do
    hdfs dfs -mkdir /user/$username
    hdfs dfs -chown $username:$username /user/$username
done
```

為 SSH 啟用 GSSAPI

Kerberos 驗證的使用者若要使用 SSH 連接到主節點，SSH 服務必須已啟用 GSSAPI 身份驗證。若要啟用 GSSAPI，請從主節點命令列執行以下命令，或使用步驟將其做為指令碼來執行。重新設定 SSH 後，您必須重新啟動服務。

```
sudo sed -i 's/^.*GSSAPIAuthentication.*$/GSSAPIAuthentication yes/' /etc/ssh/sshd_config
sudo sed -i 's/^.*GSSAPICleanupCredentials.*$/GSSAPICleanupCredentials yes/' /etc/ssh/
sshd_config
sudo /etc/init.d/sshd restart
```

使用 SSH 連接到 Kerberos 化叢集

本節示範 Kerberos 驗證使用者連接到 EMR 叢集主節點的步驟。

用於 SSH 連線的每部電腦必須安裝 SSH 用戶端和 Kerberos 用戶端應用程式。Linux 電腦很可能預設已包含這些項目。例如，大多數的 Linux、Unix 和 macOS 作業系統都會安裝 OpenSSH。您可以藉由在命令列鍵入 ssh 來檢查 SSH 用戶端。若您的電腦無法識別該命令，請安裝 SSH 用戶端以連線到主節點。OpenSSH 專案提供 SSH 工具完整套件的免費實作。如需詳細資訊，請參閱 [OpenSSH 網站](#)。Windows 使用者可以使用應用程式（例如 PuTTY）做為 SSH 用戶端。

如需 SSH 連線的詳細資訊，請參閱「[連接叢集 \(p. 276\)](#)」。

SSH 使用 GSSAPI 來驗證 Kerberos 用戶端，而您必須在叢集主節點上為 SSH 服務啟用 GSSAPI 身份驗證。如需更多詳細資訊，請參閱 [為 SSH 啟用 GSSAPI \(p. 206\)](#)。SSH 用戶端也必須使用 GSSAPI。

在下列範例中，若為 *MasterPublicDNS*，請使用叢集詳細資訊窗格之 Summary (摘要) 標籤上 Master public DNS (主要公有 DNS) 中顯示的值—例如 *ec2-11-222-33-44.compute-1.amazonaws.com*。

krb5.conf 的先決條件 (非 Active Directory)

使用未與 Active Directory 整合的組態時，除了 SSH 用戶端和 Kerberos 用戶端應用程式，每個用戶端電腦還必須擁有符合叢集主節點上 /etc/krb5.conf 檔案的 /etc/krb5.conf 檔案副本。

複製 krb5.conf 檔案

1. 使用 EC2 金鑰對和預設 hadoop 使用者，以 SSH 連接到主節點—例如 *hadoop@MasterPublicDNS*。如需詳細說明，請參閱 [連接叢集 \(p. 276\)](#)。
2. 從主節點，複製 /etc/krb5.conf 檔案的內容。如需更多詳細資訊，請參閱 [連接叢集 \(p. 276\)](#)。
3. 在每個將連接到叢集的用戶端電腦上，根據您在上一個步驟所製作的副本，建立相同的 /etc/krb5.conf 檔案。

使用 Kinit 和 SSH

每次使用者從用戶端電腦使用 Kerberos 登入資料進行連線時，使用者必須先在用戶端電腦上為其使用者續約 Kerberos 票證。此外，SSH 用戶端也必須設定為使用 GSSAPI 身份驗證。

使用 SSH 連接到 Kerberos 化 EMR 叢集

1. 使用 kinit 繼約您的 Kerberos 票證，如下列範例所示

```
kinit user1
```

2. 使用 ssh 用戶端以及您在叢集專用 KDC 中建立的主體或 Active Directory 使用者名稱。請確定已啟用 GSSAPI 身份驗證，如下範例所示。

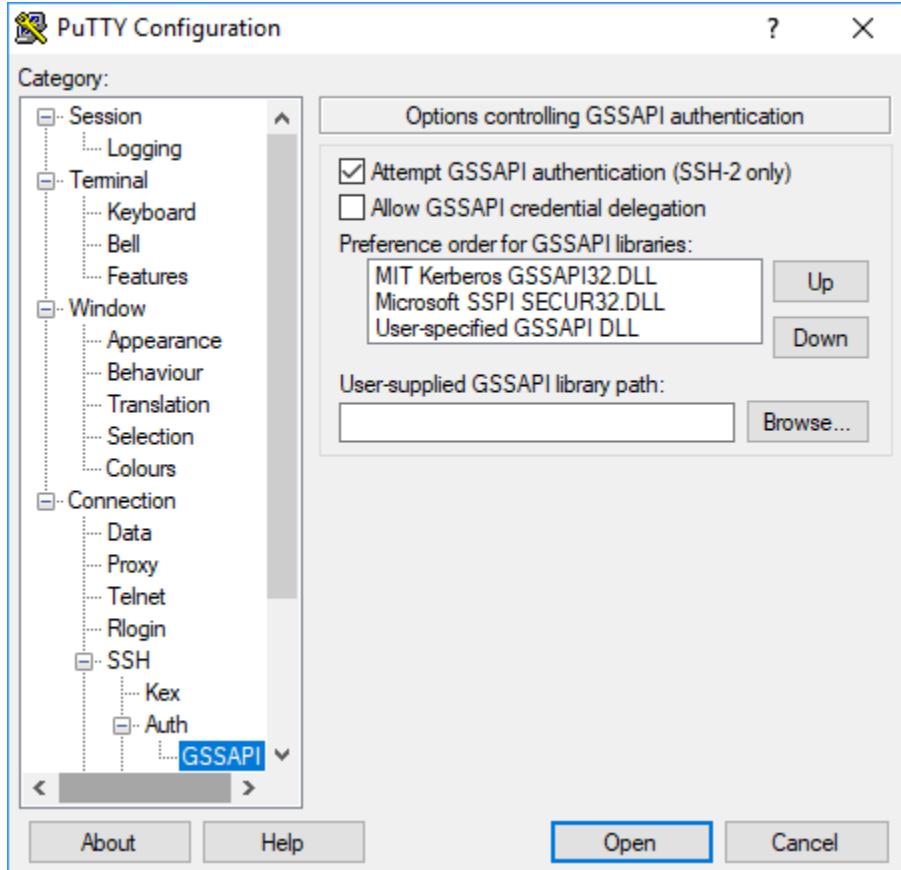
範例：Linux 使用者

-K 選項指定 GSSAPI 身份驗證。

```
ssh -K user1@MasterPublicDNS
```

範例：Windows 使用者 (PuTTY)

請確定已啟用工作階段的 GSSAPI 身份驗證選項，如下所示：



教學課程：設定叢集專用 KDC

本主題引導您使用叢集專用 KDC 來建立叢集、手動新增 Linux 使用者帳戶至所有叢集節點，新增 Kerberos 主體至主節點上的 KDC，並確保用戶端電腦已安裝 Kerberos 用戶端。

步驟 1：建立 Kerberos 化叢集

1. 建立可使用 Kerberos 的安全組態。下列範例示範 `create-security-configuration` 指令，此指令使用 AWS CLI (指定安全組態做為內嵌 JSON 架構)。您也可以參考儲存在本機的檔案。

```
aws emr create-security-configuration --name MyKerberosConfig \
--security-configuration '{"AuthenticationConfiguration": {"KerberosConfiguration": \
{"Provider": "ClusterDedicatedKdc", "ClusterDedicatedKdcConfiguration": \
{"TicketLifetimeInHours": 24}}}}
```

2. 建立參考安全組態的叢集，為叢集建立 Kerberos 屬性，並使用引導操作新增 Linux 帳戶。下列範例示範使用 AWS CLI 的 `create-cluster` 指令。命令參考您在上面建立的安全組態 MyKerberosConfig。此指令也會參考簡單的指令碼 `createlinuxusers.sh` 做為引導操作 (您在建立叢集之前就建立和上傳到 Amazon S3 的引導操作)。

```
aws emr create-cluster --name "MyKerberosCluster" \
```

```
--release-label emr-5.28.0 \
--instance-type m5.xlarge \
--instance-count 3 \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2KeyPair \
--service-role EMR_DefaultRole \
--security-configuration MyKerberosConfig \
--applications Name=Hadoop Name=Hive Name=Oozie Name=Hue Name=HCatalog Name=Spark \
--kerberos-attributes Realm=EC2.INTERNAL, \
KdcAdminPassword=MyClusterKDCAdminPwd \
--bootstrap-actions Path=s3://mybucket/createlinuxusers.sh
```

以下範例示範 `createlinuxusers.sh` 指令碼的內容，其新增 user1、user2 和 user3 至叢集中的每個節點。在下一個步驟中，您會新增這些使用者為 KDC 主體。

```
#!/bin/bash
sudo adduser user1
sudo adduser user2
sudo adduser user3
```

步驟 2：新增主體至 KDC、建立 HDFS 使用者目錄和設定 SSH

在主節點上執行的 KDC 需要為本機主機和每個您在叢集上建立的使用者新增主體。如果使用者需要連接到叢集並執行 Hadoop 任務，您也可以為每個使用者建立 HDFS 目錄。同樣地，設定 SSH 服務，以啟用 Kerberos 所需的 GSSAPI 驗證。啟用 GSSAPI 後，重新啟動 SSH 服務。

完成這些任務的最簡單方式是將步驟提交至叢集。以下範例會將 bash 指令碼 `configurekdc.sh` 提交至您在上一個步驟建立的叢集，並參考其叢集 ID。指令碼會儲存至 Amazon S3。或者，您可以使用 EC2 金鑰對連接到主節點，在叢集建立期間執行命令或提交步驟。

```
aws emr add-steps --cluster-id j-01234567 --steps
  Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE,Jar=s3://
  myregion.elasticmapreduce/libs/script-runner/script-runner.jar,Args=[ "s3://mybucket/
  configurekdc.sh" ]
```

以下範例示範 `configurekdc.sh` 指令碼的內容。

```
#!/bin/bash
#Add a principal to the KDC for the master node, using the master node's returned host name
sudo kadmin.local -q "ktadd -k /etc/krb5.keytab host/`hostname -f`"
#Declare an associative array of user names and passwords to add
declare -A arr
arr=( [user1]=pwd1 [user2]=pwd2 [user3]=pwd3)
for i in ${!arr[@]}; do
    #Assign plain language variables for clarity
    name=${i}
    password=${arr[$i]}

    # Create principal for sshuser in the master node and require a new password on first
    logon
    sudo kadmin.local -q "addprinc -pw $password +needchange $name"

    #Add user hdfs directory
    hdfs dfs -mkdir /user/$name

    #Change owner of user's hdfs directory to user
    hdfs dfs -chown $name:$name /user/$name
done

# Enable GSSAPI authentication for SSH and restart SSH service
```

```
sudo sed -i 's/^.*GSSAPIAuthentication.*$/GSSAPIAuthentication yes/' /etc/ssh/sshd_config
sudo sed -i 's/^.*GSSAPICleanupCredentials.*$/GSSAPICleanupCredentials yes/' /etc/ssh/
sshd_config
sudo /etc/init.d/sshd restart
```

您新增的使用者現在應該可以使用 SSH 連接到叢集。如需更多詳細資訊，請參閱 [使用 SSH 連接到 Kerberos 化叢集 \(p. 207\)](#)。

教學課程：使用 Active Directory 網域設定跨域信任

當您設定跨域信任時，可允許來自不同 Kerberos 領域的主體（通常為使用者）來驗證在 EMR 叢集上的應用程式元件。叢集專用的 KDC 會使用同時存在兩個 KDC 中的 跨域主體，來和另一個 KDC 建立信任關係。主體名稱和密碼完全相符。

跨域信任需要 KDC 可以透過網路連接彼此，並解析各自的網域名稱。以下提供使用以 EC2 執行個體方式執行的 Microsoft AD 網域控制站來建立跨域信任關係的步驟，以及提供需要連線能力和網域名稱解析的網路設定範例。任何允許 KDC 之間所需網路流量的網路設定都是可以接受的。

或者，在您使用一個叢集上的 KDC 與 Active Directory 建立跨域信任後，您可以使用參考第一個叢集上 KDC 做為外部 KDC 的不同安全組態來建立另一個叢集。如需安全組態和叢集設定範例，請參閱 [外部叢集 KDC 搭配 Active Directory 跨域信任 \(p. 204\)](#)。

Important

Amazon EMR 不支援與 AWS Directory Service for Microsoft Active Directory 的跨域信任。

[步驟 1：設定 VPC 和子網路 \(p. 210\)](#)

[步驟 2：啟動和安裝 Active Directory 網域控制站 \(p. 211\)](#)

[步驟 3：新增使用者帳戶到 EMR 叢集的網域 \(p. 211\)](#)

[步驟 4：設定在 Active Directory 網域控制站上的連入信任 \(p. 212\)](#)

[步驟 5：使用 DHCP 選項集指定 Active Directory 網域控制站為 VPC DNS 伺服器 \(p. 212\)](#)

[步驟 6：啟動 Kerberos 化 EMR 叢集 \(p. 212\)](#)

[步驟 7：建立 HDFS 使用者並在 Active Directory 使用者帳戶的叢集上設定許可 \(p. 213\)](#)

步驟 1：設定 VPC 和子網路

以下步驟示範建立 VPC 和子網路，讓叢集專用 KDC 可以連接 Active Directory 網域控制站並解析其網域名稱。在這些步驟中，透過參考 Active Directory 網域控制站做為在 DHCP 選項集中的網域名稱伺服器，提供網域名稱解析。如需更多詳細資訊，請參閱 [步驟 5：使用 DHCP 選項集指定 Active Directory 網域控制站為 VPC DNS 伺服器 \(p. 212\)](#)。

KDC 和 Active Directory 網域控制站必須能夠解析另一個網域名稱。如此一來，Amazon EMR 可將電腦加入網域，並在叢集執行個體上自動設定對應的 Linux 使用者帳戶和 SSH 參數。

如果 Amazon EMR 無法解析網域名稱，您可以使用 Active Directory 網域控制站的 IP 地址參考信任。不過，您必須手動新增 Linux 使用者帳戶、新增對應的主體至叢集專用 KDC 和設定 SSH。

設定 VPC 和子網路

1. 建立具有單一公有子網路的 Amazon VPC。如需詳細資訊，請參閱 Amazon VPC Getting Started Guide 中的 [步驟 1：建立 VPC](#)。

Important

當您使用 Microsoft Active Directory 網域控制站時，請選擇 EMR 叢集的 CIDR 區塊，讓所有 IPv4 地址的長度少於 9 個字元（例如 10.0.0.0/16）。這是因為電腦加入 Active Directory 目錄時，會使用叢集電腦的 DNS 名稱。AWS 會根據 IPv4 地址來指派 **DNS 主機名稱**，其中較長的 IP 地址可能導致 DNS 名稱超過 15 個字元。Active Directory 限制註冊加入電腦名稱為 15 個字元，而截斷較長的名稱可能會導致無法預測的錯誤。

2. 移除指派至 VPC 的預設 DHCP 選項集。如需詳細資訊，請參閱[變更 VPC 以使用無 DHCP 選項](#)。之後，新增指定 Active Directory 網域控制站為 DNS 伺服器的新 VPC。
3. 確認 DNS 支援已為 VPC 啟用，也就是說，該 DNS 主機名稱和 DNS 解析都已啟用。預設為皆啟用。如需詳細資訊，請參閱[更新 VPC 的 DNS 支援](#)。
4. 確認您的 VPC 已連接到網際網路閘道，此為預設。如需詳細資訊，請參閱[建立和連接網際網路閘道](#)。

Note

此範例中使用網際網路閘道，因為您正在為 VPC 建立新的網域控制站。您的應用程式可能不需要網際網路閘道。唯一的要求是，叢集專用 KDC 可以存取 Active Directory 網域控制站。

5. 建立自訂路由表，新增以網際網路閘道為目標的路由，然後將其連接到您的子網路。如需詳細資訊，請參閱[建立自訂路由表](#)。
6. 當您為網域控制站啟動 EC2 執行個體時，其必須擁有靜態公有 IPv4 地址，讓您可使用 RDP 連接到該執行個體。最簡單的方法是設定您的子網路為自動指派公有 IPv4 地址。這不是子網路建立時的預設設定。如需詳細資訊，請參閱[修改子網路的公有 IPv4 定址屬性](#)。您可以選擇在啟動執行個體時指派地址。如需詳細資訊，請參閱[在執行個體啟動期間指派公有 IPv4 地址](#)。
7. 完成後，請記下您的 VPC 和子網路 ID。您稍後啟動 Active Directory 網域控制站和叢集時，便可以使用。

步驟 2：啟動和安裝 Active Directory 網域控制站

1. 根據 Microsoft Windows Server 2016 Base AMI 啟動 EC2 執行個體。我們建議使用 m4.xlarge 或更好的執行個體類型。如需詳細資訊，請參閱 Amazon EC2 User Guide for Windows Instances 中的 [啟動 AWS Marketplace 執行個體](#)。
2. 請記下與 EC2 執行個體相關聯之安全群組的 Group ID (群組 ID)。您需要它用於 [步驟 6：啟動 Kerberos 化 EMR 叢集 \(p. 212\)](#)。我們使用 `sg-012xrlmdomain345`。或者，您可以為 EMR 叢集指定不同的安全群組，以及這個執行個體允許它們之間的流量。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的適用於 [Amazon EC2Linux 執行個體的安全群組](#)。
3. 使用 RDP 連接到 EC2 執行個體。如需詳細資訊，請參閱 Amazon EC2 User Guide for Windows Instances 中的 [連線至您的 Windows 執行個體](#)。
4. 啟動 Server Manager (伺服器管理員)，在伺服器上安裝和設定 Active Directory 網域服務角色。將伺服器升級為網域控制站並指派網域名稱（此處使用的範例是 `ad.domain.com`）。請記下網域名稱，因為您稍後建立 EMR 安全組態和叢集時會需要此網域名稱。如果您是第一次設定 Active Directory，可以遵循 [如何在 Windows Server 2016 中設定 Active Directory \(AD\)](#) 中的說明。

執行個體在您完成後會重新啟動。

步驟 3：新增使用者帳戶到 EMR 叢集的網域

RDP 到 Active Directory 網域控制站為每個叢集使用者在 Active Directory 使用者和電腦中建立使用者帳戶。如需說明，請參閱 [在 Active Directory 使用者和電腦中建立使用者帳戶](#)。請記下每個使用者的 User logon name (使用者登入名稱)。您稍後在設定叢集時需要這些使用者登入名稱。

此外，建立具備足夠權限的使用者帳戶，可將電腦加入網域。您會在建立叢集時指定此帳戶。Amazon EMR 會利用該帳戶來將叢集執行個體加入網域。您會在 [步驟 6：啟動 Kerberos 化 EMR 叢集 \(p. 212\)](#) 中指定此帳戶和其密碼。若要委派電腦加入權限給使用者帳戶，我們建議您建立具備加入權限的群組，再將使用者指派給群組。如需說明，請參閱 AWS Directory Service Administration Guide 中的 [委派目錄加入權限](#)。

步驟 4：設定在 Active Directory 網域控制站上的連入信任

以下的範例命令在 Active Directory 中建立信任，這是具有叢集專用 KDC 的單向、連入、非轉移、領域信任。我們用於叢集領域的範例為 **EC2.INTERNAL**。將 **KDC-FQDN** 取代為託管 KDC 的 Amazon EMR 主節點所列出的 Public DNS (公有 DNS) 名稱。passwordt 參數會指定 cross-realm principal password (跨域主體密碼)，這是您在建立叢集時，連同叢集 realm (領域) 一起指定的項目。領域名稱衍生自叢集的 us-east-1 中的預設網域名稱。該 Domain 是您在建立信任時的 Active Directory 網域，慣例為小寫。該範例使用 **ad.domain.com**。

以管理員權限開啟 Windows 命令提示，輸入下列命令，在 Active Directory 網域控制站上建立信任關係：

```
C:\Users\Administrator> ksetup /addkdc EC2.INTERNAL KDC-FQDN
C:\Users\Administrator> netdom trust EC2.INTERNAL /Domain:ad.domain.com /add /realm /
passwordt:MyVeryStrongPassword
C:\Users\Administrator> ksetup /SetEncTypeAttr EC2.INTERNAL AES256-CTS-HMAC-SHA1-96
```

步驟 5：使用 DHCP 選項集指定 Active Directory 網域控制站為 VPC DNS 伺服器

現在 Active Directory 網域控制站已設定，您必須設定 VPC，以將其做為您 VPC 中名稱解析的網域名稱伺服器。若要執行此操作，連接 DHCP 選項集。指定 Domain name (網域名稱) 做為您叢集的網域名稱，例如，如果您的叢集位於 us-east-1 或其他區域的 **region.compute.internal**，則指定 **ec2.internal**。針對 Domain name servers (網域名稱伺服器)，您必須指定 Active Directory 網域控制器的 IP 地址 (必須能夠從叢集存取) 做為第一個項目，接著是 AmazonProvidedDNS (AmazonProvidedDNS) (例如 **xx.xx.xx.xx**、AmazonProvidedDNS)。如需詳細資訊，請參閱[變更 DHCP 選項集](#)。

步驟 6：啟動 Kerberos 化 EMR 叢集

- 在 Amazon EMR 中建立安全組態，其指定您在先前步驟中建立的 Active Directory 網域控制站。範例命令顯示如下：以您在 **ad.domain.com** 中指定的網域名稱取代 [步驟 2：啟動和安裝 Active Directory 網域控制站 \(p. 211\)](#) 網域。

```
aws emr create-security-configuration --name MyKerberosConfig \
--security-configuration '{
  "AuthenticationConfiguration": {
    "KerberosConfiguration": {
      "Provider": "ClusterDedicatedKdc",
      "ClusterDedicatedKdcConfiguration": {
        "TicketLifetimeInHours": 24,
        "CrossRealmTrustConfiguration": {
          "Realm": "AD.DOMAIN.COM",
          "Domain": "ad.domain.com",
          "AdminServer": "ad.domain.com",
          "KdcServer": "ad.domain.com"
        }
      }
    }
  }
}'
```

- 使用下列屬性建立一個叢集：

- 使用 **--security-configuration** 選項來指定您建立的安全組態。我們在範例中使用 **MyKerberosConfig**。
- 使用的 **--ec2-attributes** option 的 SubnetId 屬性來指定您在 [步驟 1：設定 VPC 和子網路 \(p. 210\)](#) 中建立的子網路。我們在範例中使用 **step1-subnet**。
- 使用 **--ec2-attributes** 選項的 AdditionalMasterSecurityGroups 和 AdditionalSlaveSecurityGroups，指定從 [步驟 2：啟動和安裝 Active Directory 網域控制站 \(p. 211\)](#) 和 AD 網域控制站相關聯的安全群組與叢集主節點、核心節點和任務節點相關聯。我們在範例中使用 **sg-012xrlmdomain345**。

使用 `--kerberos-attributes` 指定下列叢集特定的 Kerberos 屬性：

- 您設定 Active Directory 網域控制站時指定的叢集領域。
- 您在 `passwordt` 中指定為 [步驟 4：設定在 Active Directory 網域控制站上的連入信任 \(p. 212\)](#) 的跨域信任主體密碼。
- 您可用來管理叢集專用 KDC 的 `KdcAdminPassword`。
- 您在 [步驟 3：新增使用者帳戶到 EMR 叢集的網域 \(p. 211\)](#) 中建立具有電腦加入權限的 Active Directory 帳戶使用者登入名稱和密碼。

以下範例啟動 kerberos 化叢集。

```
aws emr create-cluster --name "MyKerberosCluster" \
--release-label emr-5.10.0 \
--instance-type m5.xlarge \
--instance-count 3 \
--ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,KeyName=MyEC2KeyPair, \
SubnetId=step1-subnet, AdditionalMasterSecurityGroups=sg-012xrlmdomain345, \
AdditionalSlaveSecurityGroups=sg-012xrlmdomain345 \
--service-role EMR_DefaultRole \
--security-configuration MyKerberosConfig \
--applications Name=Hadoop Name=Hive Name=Oozie Name=Hue Name=HCatalog Name=Spark \
--kerberos-attributes Realm=EC2.INTERNAL, \
KdcAdminPassword=MyClusterKDCAdminPwd, \
ADDDomainJoinUser=ADUserLogonName, ADDDomainJoinPassword=ADUserPassword, \
CrossRealmTrustPrincipalPassword=MatchADTrustPwd
```

步驟 7：建立 HDFS 使用者並在 Active Directory 使用者帳戶的叢集上設定許可

使用 Active Directory 設定信任關係時，Amazon EMR 會為每個 Active Directory 使用者帳戶在叢集上建立 Linux 使用者。例如，在 Active Directory 中的 LiJuan 使用者登入名稱擁有 lijuan 的 Linux 使用者帳戶。Active Directory 使用者名稱可包含大寫字母，但 Linux 不會使用 Active Directory 的大小寫。

若要讓您的使用者登入叢集以執行 Hadoop 任務，您必須為 Linux 使用者帳戶新增 HDFS 使用者目錄，並授予每位使用者目錄的所有權。若要執行此操作，我們建議您執行以叢集步驟儲存至 Amazon S3 的指令碼。或者，您可以執行以下指令碼中的命令，其來自主節點的命令列。使用您建立叢集時所指定的 EC2 金鑰對，透過 SSH 連接到主節點，以做為 Hadoop 使用者。如需更多詳細資訊，請參閱 [使用 SSH 登入資料的 Amazon EC2 金鑰對 \(p. 190\)](#)。

執行下列的指令，來將步驟新增到執行 `AddHDFSUsers.sh` 指令碼的叢集。

```
aws emr add-steps --cluster-id ClusterID \
--steps Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE, \
Jar=s3://MyRegion.elasticmapreduce/libs/script-runner/script-runner.jar,Args=[ "s3:// \
MyBucketPath/AddHDFSUsers.sh" ]
```

`AddHDFSUsers.sh` 檔案的內容如下。

```
#!/bin/bash
# AddHDFSUsers.sh script

# Initialize an array of user names from AD or Linux users and KDC principals created
# manually on the cluster
ADUSERS=("lijuan" "marymajor" "richardroe" "myusername")

# For each user listed, create an HDFS user directory
# and change ownership to the user

for username in ${ADUSERS[@]}; do
```

```
hdfs dfs -mkdir /user/$username
hdfs dfs -chown $username:$username /user/$username
done
```

Active Directory 群組對應至 Hadoop 群組

Amazon EMR 使用系統安全服務協助程式 (SSD)，以對應 Active Directory 群組至 Hadoop 群組。若要確認群組對應，如 [使用 SSH 連接到 Kerberos 化叢集 \(p. 207\)](#) 所述登入主節點後，您可以使用 `hdfs groups` 命令，確認您 Active Directory 帳戶所屬的 Active Directory 群組已對應至叢集上對應 Hadoop 使用者的 Hadoop 群組。您也可以使用命令，例如 `hdfs groups lijuan`，指定一個或多個使用者名稱，查看其他使用者的群組映射。如需詳細資訊，請參閱 [Apache HDFS 指令指南](#) 中的 [群組](#)。

Amazon EMR 與 AWS Lake Formation 整合 (Beta 版)

從 Amazon EMR 5.26.0 開始，您可以啟動與 AWS Lake Formation 整合的叢集。這項功能已開放公開測試版使用。

AWS Lake Formation 是一項受管服務，可簡化資料湖的設定、保護和管理工作。AWS Lake Formation 可協助您探索、編目、清理和保護 Amazon Simple Storage Service (Amazon S3) 資料湖中的資料。如需詳細資訊，請參閱 [AWS Lake Formation](#)。

整合 Amazon EMR 與 AWS Lake Formation 可提供下列主要優點：

- 提供對 AWS Glue Data Catalog 中的資料庫和資料表的精細分級存取。
- 可以從與安全性聲明標記語言 (SAML) 2.0 相容的企業身分系統對 EMR Notebooks 或 Apache Zeppelin 啟用同盟單一登入。

本節提供 Amazon EMR 與 Lake Formation 整合的概念性概觀，也提供啟動與 Lake Formation 整合之 Amazon EMR 叢集所需的先決條件和步驟。

主題

- [Amazon EMR 與 Lake Formation 整合的概念性概觀 \(p. 214\)](#)
- [支援的應用程式和功能 \(p. 218\)](#)
- [開始之前 \(p. 219\)](#)
- [使用 Lake Formation 啟動 Amazon EMR 叢集 \(p. 225\)](#)

Amazon EMR 與 Lake Formation 整合的概念性概觀

透過整合 Amazon EMR 與 AWS Lake Formation，您可以啟用使用公司登入資料的 SAML 型身分驗證，並根據 AWS Lake Formation 中所定義的政策強制執行更精細的資料欄層級存取控制。

若要整合 Amazon EMR 和 Lake Formation，您的組織必須符合下列要求：

- 使用現有的 SAML 型身分供應商管理您的公司身分，例如 Active Directory Federation Services (AD FS)。如需詳細資訊，請參閱 [SAML 支援的第三方供應商 \(p. 223\)](#)。
- 使用 AWS Glue Data Catalog 做為中繼資料存放區。
- 使用 EMR Notebooks 或 Apache Zeppelin 來存取由 AWS Glue 和 Lake Formation 管理的資料。
- 在 Lake Formation 中定義和管理許可，以存取 AWS Glue Data Catalog 中的資料庫、資料表和資料欄。如需詳細資訊，請參閱 [AWS Lake Formation](#)。

啟動與 Lake Formation 整合的叢集之前，您需要設定身分供應商 (IdP) 和 AWS Access and Identity Management (IAM) 角色來啟用以 SAML 2.0 為基礎的聯合。您也需要為 Amazon EMR 叢集設定適當的安全控制。如需詳細資訊，請參閱 [開始之前 \(p. 219\)](#) 及 [使用 Lake Formation 啟動 Amazon EMR 叢集 \(p. 225\)](#)。

主題

- [術語和概念 \(p. 215\)](#)
- [在 Lake Formation 中存取資料的運作方式 \(p. 215\)](#)
- [Amazon EMR 元件 \(p. 216\)](#)
- [啟用 SAML 的單一登入和精細存取控制架構 \(p. 217\)](#)

術語和概念

本節概述 Amazon EMR 與 AWS Lake Formation 整合時所使用的概念和術語。

身分驗證

建立使用者身分的程序。透過整合 Amazon EMR 和 Lake Formation，您的使用者可以使用他們的公司登入資料登入 EMR Notebooks 和 Apache Zeppelin。

授權

驗證特定使用者可以對特定資源採取的動作的程序。整合 Amazon EMR 叢集與 Lake Formation 時，資料庫和資料表的存取權是使用 Lake Formation 政策來授權。此程序可確保使用者只能查詢和分析他們獲授權存取的資料表或資料欄。

聯合

在外部身分供應商和 AWS Identity and Access Management (IAM) 之間建立信任關係。使用者也可以登入與安全性聲明標記語言 (SAML) 2.0 相容的企業身分系統，例如 Microsoft Active Directory Federation Services。如需詳細資訊，請參閱 [SAML 支援的第三方供應商 \(p. 223\)](#)。當您使用 SAML 2.0 設定這些外部身分供應商與 IAM 之間的信任關係，會將該使用者指派給 IAM 角色。使用者也可以接收臨時登入資料，其允許使用者存取您的 AWS Lake Formation 資源。

信任政策

使用 [JSON](#) 格式的文件，您會在其中定義允許擔任角色的人員。此受信任實體包含在政策中做為文件中的「委託人」元素。文件的撰寫會根據 [IAM 政策語言](#) 的規則。

許可政策

使用 [JSON](#) 格式的許可文件，您會在其中定義角色可以存取哪些動作和資源。文件的撰寫會根據 [IAM 政策語言](#) 的規則。

委託人

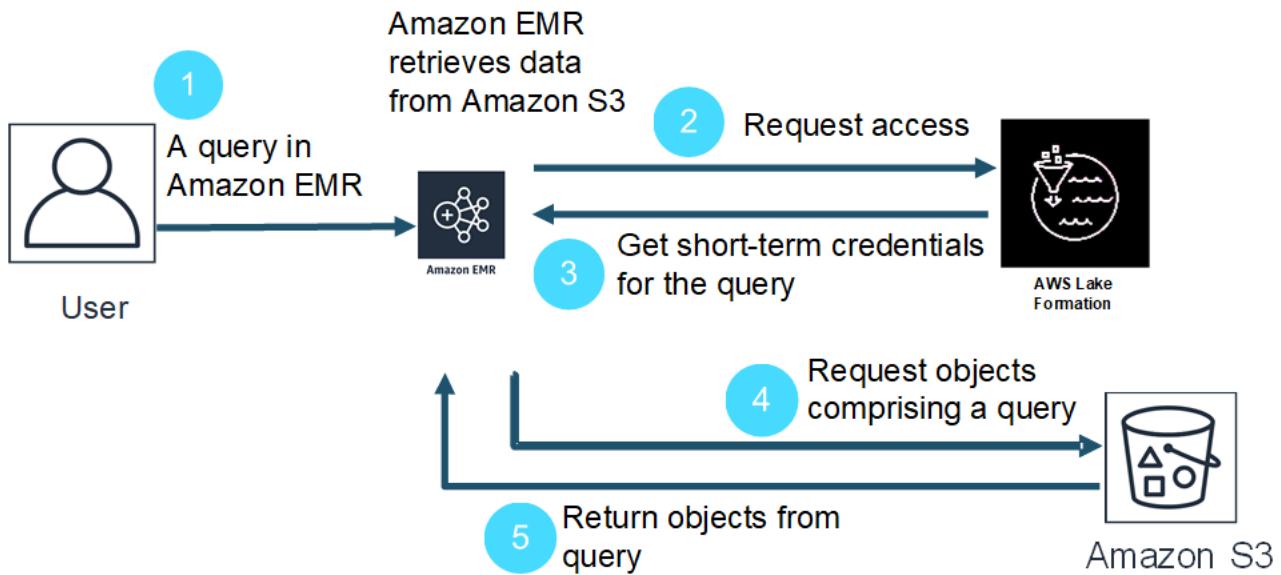
可以存取 Lake Formation 政策所保護的資源，並在 Amazon EMR 中執行查詢的實體。委託人可以是 AWS Identity and Access Management (IAM) 使用者或角色，或由其 SAML 身分供應商 (IdP) 識別的聯合身分使用者。

在 Lake Formation 中存取資料的運作方式

Lake Formation 提供 Amazon EMR 等服務的臨時登入資料來允許存取資料。此程序稱為登入資料販售程序。如需詳細資訊，請參閱 [AWS Lake Formation](#)。

當您對受 Lake Formation 安全政策保護的資料執行查詢時，Amazon EMR 會向 AWS Lake Formation 請求臨時登入資料以存取 Amazon S3 中所存放的資料。

以下是授予資料存取權的方式：



1. 您可以使用 AWS Lake Formation 政策來設定和控制使用者對資源的存取。您可以使用 Lake Formation 主控台內的一組授予和撤銷許可來建立政策。例如，您可以授予對資料庫或資料表的存取。也可以將欄層級許可授予使用者。您可以直接在 Lake Formation 中指定資料表和資料欄的許可，而不是為 Amazon S3 儲存貯體和物件指定它們。如需詳細資訊，請參閱 [Lake Formation 許可](#)。
2. 當委託人嘗試在 Amazon EMR 中對來自 Lake Formation 的資料執行查詢時，Amazon EMR 會向 AWS Lake Formation 請求用於存取資料的臨時登入資料。
3. Lake Formation 會傳回臨時登入資料，以允許資料存取。
4. Amazon EMR 會傳送查詢請求，以從 Amazon S3 取得資料。
5. Amazon EMR 會根據 Lake Formation 中所定義的使用者許可來篩選並傳回結果。

Amazon EMR 元件

Amazon EMR 使用下列元件來啟用 Lake Formation 的精細定義存取控制：

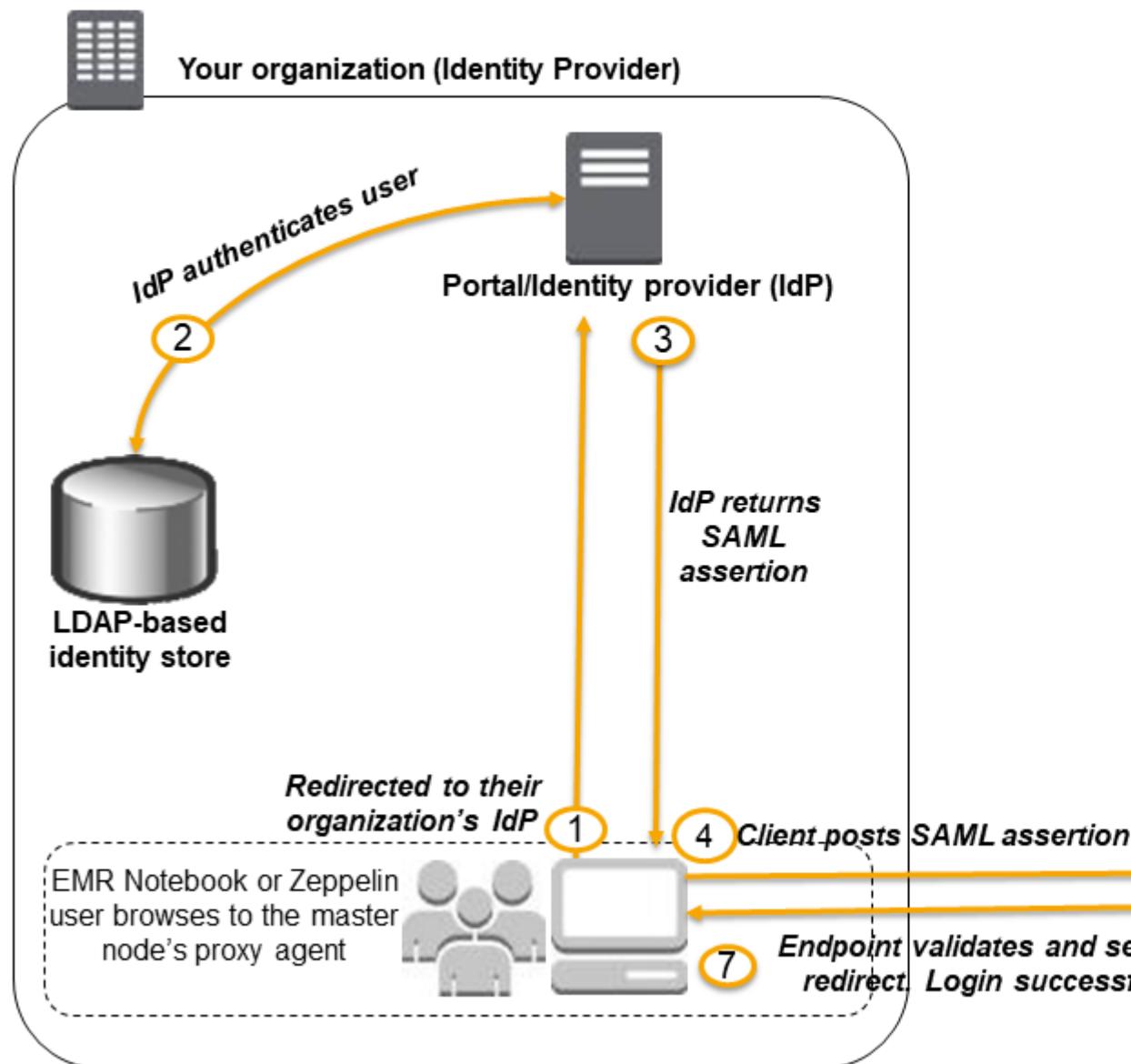
- Proxy agent (Proxy 代理程式) – Proxy 代理程式以 Apache Knox 為基礎。它會從使用者收到 SAML 驗證的請求，並將 SAML 宣告轉換為臨時登入資料。它也會將臨時登入資料存放在秘密代理程式中。Proxy 代理程式會以 `knox` 系統使用者的身分在主節點上執行，並將日誌寫入 `/var/log/knox` 目錄。
- 密碼代理程式 – 密碼代理程式可安全地儲存密碼並將密碼分發到其他 EMR 元件或應用程式。密碼可以包含臨時使用者登入資料、加密金鑰或 Kerberos 票證。密碼代理程式會在叢集中的每個節點上執行，並使用 Lake Formation 和 AWS Glue API 摘取臨時登入資料和 AWS Glue Data Catalog 中繼資料。密碼代理程式會以 `emrsecretagent` 使用者身分執行，並將日誌寫入 `/emr/secretagent/log` 目錄。此程序倚賴一組特定的 `iptables` 規則來運作。請務必確保 `iptables` 不會停用，而且如果您自訂 `iptables` 組態，則必須保留 `nat` 資料表規則並保持不變。
- 記錄伺服器 – 記錄伺服器接收存取資料的請求。然後，它會根據由密碼代理程式分發的臨時登入資料和資料表存取控制政策來授權請求。記錄伺服器會從 Amazon S3 讀取資料，並傳回使用者獲授權存取的資料欄層級資料。記錄伺服器會以 `emr_record_server` 使用者身分在叢集中的每個節點上執行，並將日誌寫入 `/var/log/emr-record-server` 目錄。

Note

Spark SQL 已與這些元件整合，允許 Spark SQL 任務能夠讀取和處理受到 Lake Formation 政策保護的資料。

啟用 SAML 的單一登入和精細存取控制架構

下圖說明使用 Lake Formation 和 Amazon EMR 啟用 SAML 的單一登入和精細存取控制架構。



1. 未驗證的使用者使用 Proxy 代理程式來存取 EMR notebooks 或 Zeppelin。系統會將使用者重新導向到您組織的身分供應商 (IdP) 登入頁面。
2. IdP 可驗證使用者在您組織中的身分。

3. IdP 會產生一個 SAML 身分驗證回應，其中包括辨識使用者身分的聲明以及使用者的相關屬性。
4. 用戶端瀏覽器會將 SAML 嘴銳發佈到 Proxy 代理程式。
5. Proxy 代理程式會代表使用者向 AWS Lake Formation 請求使用者特定的臨時安全登入資料。臨時安全登入資料會傳回至 Proxy 代理程式。
6. Proxy 代理程式會將使用者特定的臨時安全登入資料儲存在密碼代理程式中。密碼代理程式會將臨時使用者登入資料傳送到核心節點和任務節點中的密碼代理程式。
7. Proxy 代理程式可讓使用者成功登入。
8. 當使用者使用 EMR notebooks 或 Zeppelin 執行 Spark 任務時，記錄伺服器會呼叫密碼代理程式以取得臨時使用者登入資料。
9. 記錄伺服器會根據 Lake Formation 中定義的政策，從 Amazon S3 讀取和篩選資料。

從使用者的觀點來看，此程序是以透明的方式進行。使用者透過瀏覽器在您組織的身分驗證頁面開始操作，在 EMR notebooks 或 Zeppelin 結束操作，無需提供任何 AWS 登入資料。

支援的應用程式和功能

支援的應用程式

Amazon EMR 和 AWS Lake Formation 之間的整合支援以下應用程式：

- Apache Spark
- Apache Zeppelin
- Amazon EMR notebooks

Important

目前不支援其他應用程式。為確保叢集的安全性，請勿安裝此清單以外的其他應用程式。

支援的功能

以下的 Amazon EMR 功能可與 EMR 和 Lake Formation 搭配使用：

- 靜態和傳輸中加密
- 使用叢集專用 KDC 的 Kerberos 身分驗證
- 執行個體群組、執行個體機群和 Spot 執行個體
- 在執行中叢集內重新設定應用程式

以下 EMR 功能目前不適用於 Lake Formation 整合：

- 步驟
- 多個主節點
- EMRFS 一致檢視
- 使用客戶提供加密金鑰的 EMRFS CSE-C 和 SSE-C

限制

使用 Amazon EMR 搭配 AWS Lake Formation 時，請考慮下列限制：

- 在 Lake Formation 啟用的叢集中，Spark SQL 只能從 AWS Glue Data Catalog 管理的資料讀取，而且無法存取 AWS Glue 或 Lake Formation 之外管理的資料。如果在叢集部署期間選擇的其他 AWS 服務的 IAM 角色具有允許叢集存取這些資料來源的政策，則可以使用非 Spark SQL 操作來存取來自其他來源的資料。

- 例如，除了一組 Lake Formation 資料表之外，您可能也希望 Spark 任務存取兩個 Amazon S3 儲存貯體和 Amazon DynamoDB 資料表。在此情況下，您可以建立能存取兩個 Amazon S3 儲存貯體和 Amazon DynamoDB 資料表的角色，並在啟動叢集時將其用於 IAM role for other AWS services。
- Spark 任務提交必須透過 EMR notebooks、Zeppelin 或 Livy 完成。透過 spark-submit 提交的 Spark 任務目前無法用於 Lake Formation。
- Spark SQL 只能從 Lake Formation 資料表讀取。目前不支援使用 Spark SQL 寫入資料表或在 Lake Formation 中建立新資料表。
- 目前不支援使用 Spark SQL 存取使用 Hive Map 資料類型的 Lake Formation 資料表。
- 使用 Spark 存取以單欄格式儲存的資料時，不支援述詞下推和向量讀取等效能最佳化。倚賴這些最佳化的那些 Spark SQL 應用程式會在搭配 Lake Formation 使用時看到效能降低。
- 目前沒有集中登出可供 Amazon EMR notebooks 和 Zeppelin 使用。
- 使用 Spark SQL 存取 Lake Formation 保護的資料時，資料存取的 AWS CloudTrail 項目只包含與 Amazon EMR 叢集關聯的 IAM 角色名稱。他們不包含使用 notebook 的聯合身分使用者。
- 使用 Lake Formation 的此版本不支援使用 Spark 的備援至 HDFS 統計收集功能。此功能的 spark.sql.statistics.fallBackToHdfs 屬性預設為停用。手動啟用此屬性時，此功能無法運作。
- 目前不支援查詢包含 Amazon S3 中不同資料表路徑下分區的資料表。
- 請務必了解，Lake Formation 資料欄層級授權會阻止使用者存取使用者無法存取的資料欄中的資料。不過，在某些情況下，使用者可以存取描述資料表中所有資料欄的中繼資料，包括使用者無法存取的資料欄。此資料欄中繼資料會儲存在資料表的資料表屬性中，這些資料表使用 Avro 儲存格式或使用自訂序列化程式/還原序列化程式 (SerDe)，其中資料表結構描述與 SerDe 定義一起在資料表屬性中定義。當您使用 Amazon EMR 和 Lake Formation 時，我們建議您檢閱要保護之資料表的資料表屬性內容，並盡可能限制資料表屬性中所儲存的資訊，以防止使用者看到任何敏感中繼資料。

開始之前

使用 AWS Lake Formation 啟動 Amazon EMR 叢集之前，請先完成下列事前準備：

- 設定 AWS IAM 角色和 IdP 供應商，以啟用以 SAML 2.0 為基礎的聯合。
- 設定 Amazon EMR 安全功能。

主題

- [Lake Formation 的 IAM 角色概觀 \(p. 219\)](#)
- [設定 IdP 和 Lake Formation 之間的信任關係 \(p. 221\)](#)
- [SAML 支援的第三方供應商 \(p. 223\)](#)
- [設定 EMR 安全功能 \(p. 224\)](#)

Lake Formation 的 IAM 角色概觀

Amazon EMR 和 AWS Lake Formation 之間的整合倚賴三個關鍵角色：適用於 Lake Formation 的 IAM 角色、AWS 服務的 IAM 角色，和 Amazon EMR 的 EC2 執行個體描述檔。本節提供這些角色以及您需要為每個角色包含之政策的概觀。

如需如何設定 Lake Formation 角色的詳細資訊，請參閱 [設定 IdP 和 Lake Formation 之間的信任關係 \(p. 221\)](#)。

Lake Formation 的 IAM 角色

Lake Formation 的 IAM 角色定義了使用者透過 IdP 登入的權限，以及可擔任此角色的身分供應商。角色的 Maximum CLI/API session duration 定義存取 EMR Notebooks 和 Apache Zeppelin 的工作階段逾時。

- 必須使用下列許可政策來建立此角色。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "lakeformation:GetDataAccess",  
                "lakeformation:GetMetadataAccess",  
                "glue:GetUnfiltered*",  
                "glue:GetTable",  
                "glue:GetTables",  
                "glue:GetDatabase",  
                "glue:GetDatabases",  
                "glue:GetUserDefinedFunction",  
                "glue:GetUserDefinedFunctions"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Note

請勿授予此角色存取 AWS Glue 所管理之任何 Amazon S3 儲存體的許可。聯合身分使用者應該使用 Spark SQL 透過 Lake Formation 存取資料，且不應透過 Amazon S3 直接存取資料。

- 該角色還必須包含下列信任政策，允許您的 IAM 身分供應商擔任該角色。使用您的 AWS 帳戶 ID 取代 *accountID*。使用 IAM 身分供應商的名稱取代 *IAM_identity_provider_name*。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Federated": "arn:aws:iam::account-id:saml-provider/IAM_identity_provider_name"  
            },  
            "Action": "sts:AssumeRoleWithSAML"  
        },  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "glue.amazonaws.com",  
                    "lakeformation.amazonaws.com"  
                ]  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

AWS 服務的 IAM 角色

AWS 服務的 IAM 角色定義 Amazon EMR 叢集在存取非 AWS Lake Formation 服務時擁有的許可。例如，如果叢集上執行的任務需要存取 Amazon DynamoDB 或任何其他 AWS 服務，AWS 服務的 IAM 角色必須包含存取這些服務所需的政策。當您為此角色設定政策時，請確定角色沒有下列 API 操作的存取權：

- 任何 AWS Glue API 操作。
- 任何 AWS Lake Formation API 操作。

- 任何 AWS Security Token Service (STS) AssumeRole 操作。
- 對 AWS Glue 所管理儲存貯體的任何 Amazon S3 存取。叢集應使用 Spark SQL 透過 Lake Formation 存取資料，且不應透過 Amazon S3 直接存取資料。

EC2 執行個體描述檔

EC2 執行個體描述檔是一種特殊類型的服務角色，可定義 EMR 叢集與 Lake Formation 和其他 AWS 服務互動的許可。您可以在啟動叢集時使用 `EMR_EC2_DefaultRole`，或選擇使用自訂的 EC2 執行個體描述檔。在這兩種情況下，以下政策必須新增到角色，包括參考 Lake Formation 的 IAM 角色和 AWS 服務角色的 IAM 角色。使用您的 AWS 帳戶 ID 取代 `accountID`。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "arn:aws:iam::account-id:role/IAM_Role_For_Lake_Formation"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "sts:AssumeRole",  
            "Resource": "arn:aws:iam::account-id:role/IAM_Role_for_AWS_Services"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "lakeformation:GetTemporaryUserCredentialsWithSAML",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:GetRole",  
            "Resource": "arn:aws:iam::*:role/*"  
        }  
    ]  
}
```

如需詳細資訊，請參閱叢集 EC2 執行個體的服務角色 (EC2 執行個體描述檔) 和自訂 IAM 角色。

設定 IdP 和 Lake Formation 之間的信任關係

若要在組織的身分供應商 (IdP) 和 AWS 之間建立信任關係，您必須執行以下操作：

- 在 IdP 和 AWS 之間新增依賴方信任，以告知您的 IdP 有關服務供應商的 AWS。
- 為 AWS IAM 中的 SAML 存取建立 IAM 身分供應商和角色，以告知 AWS 有關您的外部 IdP。

設定此信任關係

1. 向您的 IdP 註冊 AWS。向 IdP 註冊 AWS 的程序取決於您使用的 IdP。如需如何針對 Auth0、Microsoft Active Directory Federation Services (AD FS) 和 Okta 執行此作業的詳細資訊，請參閱 [SAML 支援的第三方供應商 \(p. 223\)](#)。
2. 使用您的 IdP 產生中繼資料 XML 檔案，該檔案可將您的 IdP 描述為 AWS 中的 IAM 身分供應商。它必須包括發佈者名稱、建立日期、過期日期以及 AWS 可用來驗證來自您組織的身分驗證回應 (聲明) 的金鑰。每個 IdP 都有特定的方式能簡單匯出此中繼資料。如需詳細資訊，請參閱您的 IdP 文件。

您必須將中繼資料 XML 檔案上傳至 Amazon S3 儲存貯體。當您啟動與 Lake Formation 整合的叢集時，需要指定 S3 儲存貯體的路徑。

3. 在 IAM 主控台中，您可以建立一個 SAML 身分供應商實體。
 - a. 登入 AWS 管理主控台，開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
 - b. 在導覽窗格中，選擇 Identity Providers (身分供應商)、Create Provider (建立供應商)。
 - c. 針對 Provider Type (供應商類型)，選擇 Choose a provider type (選擇供應商類型)、SAML。
 - d. 輸入身分供應商的名稱。
 - e. 針對 Metadata Document (中繼資料文件)，按一下 Choose File (選擇檔案)，指定您在先前步驟從 IdP 下載的 SAML 中繼資料文件，然後選擇 Open (開啟)。
 - f. 確認您提供的資訊，然後按一下 Create (建立)。
4. 在 IAM 主控台中，建立聯合身分的 IAM 角色。
 - a. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)、Create role (建立角色)。
 - b. 選擇 SAML 2.0 federation (SAML 2.0 聯合身分) 角色類型。
 - c. 針對 SAML Provider (SAML 供應商)，選擇您角色的供應商。
 - d. 選擇 Allow programmatic and AWS Management Console access (允許程式設計和 AWS Management Console 存取) 以建立可以透過程式設計方式從主控台擔任角色。
 - e. 檢閱您的 SAML 2.0 信任資訊，然後選擇 Next: Permissions (下一步：許可)。
 - f. 根據 [Lake Formation 的 IAM 角色概觀 \(p. 219\)](#) 中的範例，為角色建立許可政策。
 - g. 選擇 Next: Tags (下一步：標籤)。
 - h. 選擇 Next: Review (下一步：檢閱)。
 - i. 針對 Role name (角色名稱)，輸入角色名稱。角色名稱在您的 AWS 帳戶內必須是獨一無二的。
 - j. 檢閱角色，然後選擇 Create role (建立角色)。
 - k. 按一下 Roles (角色) 標籤，搜尋在上一個步驟建立的角色名稱。
 - l. 選擇 Trust relationships (信任關係)，然後選取 Edit trust relationship (編輯信任關係)。
 - m. 使用 [Lake Formation 的 IAM 角色概觀 \(p. 219\)](#) 一節中指定之 Lake Formation 信任政策的 IAM 角色覆寫現有的政策文件。然後，按一下 Update Trust Relationship (更新信任關係)。
5. 在您組織的 IdP 中，您必須設定 SAML 聲明，將組織中的使用者映射到剛建立的 Lake Formation 的身分供應商和 IAM 角色。您可以透過設定下表所示的三個屬性元素來執行此作業。
 - 使用您的 AWS 帳戶 ID 取代 *accountID*。
 - 以您建立的 Lake Formation 的 IAM 角色名稱取代 *IAM_Role_For_Lake_Formation*。
 - 以您在先前步驟中建立的 IAM 身分供應商名稱取代 *IAM_identity_provider_name*。
 - 以用於儲存組織中定義之使用者名稱的屬性名稱取代 *user_alias*。

屬性元素	值
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: <i>account-id</i> :role/ <i>IAM_Role_For_Lake_Formation</i> ,arn:aws:iam:: <i>account-id</i> :saml-provider/ <i>IAM_identity_provider_name</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	<i>user_alias</i>
https://lakeformation.amazon.com/SAML/Attributes/Username	<i>user_alias</i>

執行映射的確切步驟取決於您使用的 IdP。如需詳細資訊，請參閱下一節 [SAML 支援的第三方供應商 \(p. 223\)](#)。

如需詳細資訊，請參閱[為身分驗證回應配置 SAML 聲明](#)。

SAML 支援的第三方供應商

Amazon EMR 與 AWS Lake Formation 之間的整合支援與下列第三方供應商的 SAML 2.0 聯合身分：Microsoft Active Directory Federation Services (AD FS)、Auth0 和 Okta。以下章節提供的資訊可協助您設定這些 IdP，以與 AWS Lake Formation 聯合身分工作。

Auth0

[Auth0 中的 AWS 整合](#) – Auth0 文件網站上的這個頁面說明如何使用 AWS Management Console 設定單一登入 (SSO)，也包含 JavaScript 範例。

若要啟用 Lake Formation 的聯合身分存取，請在 Auth0 文件中自訂下列步驟：

- 提供應用程式回呼 URL 時，請提供暫時 URL，如下列範例所示。啟動叢集後，使用主節點的實際 DNS 名稱來更新 *public-dns*。

```
https://public-dns:8442/gateway/knoxss0/api/v1/websso?  
pac4jCallback=true&client_name=SAML2Client
```

- 設定 SAML 時，將以下 SAML 組態程式碼貼到 Settings (設定)。

```
{  
    "audience": "urn:amazon:webservices",  
    "mappings": {  
        "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",  
        "name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"  
    },  
    "createUpnClaim": false,  
    "passthroughClaimsWithNoMapping": false,  
    "mapUnknownClaimsAsIs": false,  
    "mapIdentities": false,  
    "nameIdentifierFormat": "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",  
    "nameIdentifierProbes": [  
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"  
    ]  
}
```

- 將 AWS 角色映射至使用者時，請使用下列程式碼建立規則。以您建立的 Lake Formation 的 IAM 角色名稱取代 *IAM_Role_For_Lake_Formation*。以您為 Auth0 建立的 IAM 身分供應商名稱取代 *IAM_identity_provider_name*。

```
function (user, context, callback) {  
    user.awsRole = 'arn:aws:iam::account-id:role/IAM_Role_For_Lake_Formation,arn:aws:iam::account-id:saml-provider/IAM_identity_provider_name';  
    // the username must not contain "@" - as it is not a valid Linux username  
    user.glueUser = user.name.replace(/@.*/, '');  
  
    context.samlConfiguration.mappings = {  
        'https://aws.amazon.com/SAML/Attributes/Role': 'awsRole',  
        'https://aws.amazon.com/SAML/Attributes/RoleSessionName': 'glueUser',  
        'https://lakeformation.amazonaws.com/SAML/Attributes/Username': 'glueUser'  
    };  
  
    callback(null, user, context);  
}
```

Microsoft Active Directory Federation Services (AD FS)

[AWS Federated Authentication with Active Directory Federation Services \(AD FS\)](#) – AWS 安全部落格上的這篇文章說明如何設定 AD FS 並啟用與 AWS 的 SAML 聯合。

若要啟用 Lake Formation 的聯合身分存取，請自訂以下步驟：

- 若要新增依賴方信任，請手動輸入依賴方的相關資料，而不是從現有 URL 匯入中繼資料。選取 Permit all users to access this relying party (允許所有使用者存取此依賴方) 選項。針對端點信任的 URL，提供暫時 URL，如以下範例所示。啟動叢集後，使用主節點的實際 DNS 名稱來更新 *public-dns*。

```
https://public-dns:8442/gateway/knoxss0/api/v1/websso?  
pac4jCallback=true&client_name=SAML2Client
```

- 在編輯申請發行政策的步驟中，根據 [設定 IdP 和 Lake Formation 之間的信任關係 \(p. 221\)](#) 中的屬性元素值自訂 NameId、RoleSessionName 和 Role 這三個規則。

Okta

[在 Okta 中設定 SAML 應用程式](#) – 從 Okta 支援網站上的這個頁面，您可以藉由提供依賴方的中繼資料來了解如何設定 Okta。

若要啟用 Lake Formation 的聯合身分存取，請自訂以下步驟：

- 設定 SAML 時，在 Single sign-on URL (單一登入 URL) 使用臨時 URL，如以下範例所示。啟動叢集後，使用主節點的實際 DNS 名稱來更新 *public-dns*。

```
https://public-dns:8442/gateway/knoxss0/api/v1/websso?  
pac4jCallback=true&client_name=SAML2Client
```

- 在 Audience URI (SP 實體 ID) 方塊中，填寫 `urn:amazon:webservices`。
- 在 Attribute Statements (屬性陳述式) 區段中，新增三個屬性陳述式，如下列程序所示。以您建立的 Lake Formation 的 IAM 角色名稱取代 *IAM_Role_For_Lake_Formation*。以您在先前步驟中建立的 IAM 身分供應商名稱取代 *IAM_identity_provider_name*。以用於儲存組織中定義之使用者名稱的屬性名稱取代 *user_alias*。

1. 名稱：<https://aws.amazon.com/SAML/Attributes/Role>

值：`arn:aws:iam::account-
id:role/IAM_Role_For_Lake_Formation,arn:aws:iam::account-id:saml-
provider/IAM_identity_provider_name`

2. 名稱：<https://aws.amazon.com/SAML/Attributes/RoleSessionName>

值：`user_alias`

3. 名稱：<https://glue.amazon.com/SAML/Attributes/UserName>

值：`user_alias`

設定 EMR 安全功能

為確保 Amazon EMR 已與 AWS Lake Formation 安全地整合，請設定下列 EMR 安全功能：

- 使用叢集專用 KDC 啟用 Kerberos 身分驗證。如需詳細資訊，請參閱[使用 Kerberos 身分驗證](#)。
- 設定您的 Amazon EC2 安全群組或 Amazon VPC 網路存取控制清單 (ACL)，以允許從使用者的桌面存取 Proxy 代理程式 (連接埠 8442)。如需詳細資訊，請參閱[使用安全群組控制網路流量](#)。
- (選用) 啟用傳輸中或靜態加密。如需詳細資訊，請參閱《Amazon EMR Management Guide》中的[加密選項](#)。

- (選用) 建立 Proxy 代理程式的自訂 Transport Layer Security (TLS) 金鑰對。如需詳細資訊，請參閱 [自訂 Proxy 代理程式憑證 \(p. 228\)](#)。

如需詳細資訊，請參閱 [Amazon EMR中的安全性](#)。

使用 Lake Formation 啟動 Amazon EMR 叢集

本節提供有關如何啟動與 Lake Formation 整合的 Amazon EMR 叢集的資訊。還說明如何更新 IdP 中的單一登入 URL，如何將 notebooks 搭配 Lake Formation 使用，以及如何自訂 Proxy 代理程式憑證。

如需疑難排解常見問題的詳細資訊，請參閱 Amazon EMR Management Guide 中的[Lake Formation 叢集疑難排解](#)。

主題

- [使用主控台啟動含 Lake Formation 的 Amazon EMR 叢集 \(p. 225\)](#)
- [使用 CLI 啟動與 Lake Formation 整合的 Amazon EMR 叢集 \(p. 225\)](#)
- [在 IdP 中更新回呼或單一登入 URL \(p. 227\)](#)
- [搭配 Lake Formation 使用 Notebooks \(p. 227\)](#)
- [自訂 Proxy 代理程式憑證 \(p. 228\)](#)

使用主控台啟動含 Lake Formation 的 Amazon EMR 叢集

1. 建立指定 AWS Lake Formation 整合選項的安全組態：

1. 在 Amazon EMR 主控台中，選擇 Security configurations (安全組態)、Create (建立)。
2. 輸入安全組態的 Name (名稱)。您建立叢集時會使用此名稱來指定安全組態。
3. 在 AWS Lake Formation 整合下方，選取 Enable fine-grained access control managed by AWS Lake Formation (啟用由 AWS Lake Formation 管理的精細存取控制)。
4. 選取要套用的 AWS Lake Formation IAM 角色。

Note

如需詳細資訊，請參閱 [Lake Formation 的 IAM 角色概觀 \(p. 219\)](#)。

5. 選取要套用的其他 AWS 服務的 IAM 角色。
6. 指定中繼資料所在的 S3 路徑，上傳您的身分供應商 (IdP) 中繼資料。

Note

如需詳細資訊，請參閱 [設定 IdP 和 Lake Formation 之間的信任關係 \(p. 221\)](#)。

7. 適當地設定其他的安全組態選項，然後選擇 Create (建立)。您必須使用叢集專用 KDC 啟用 Kerberos 身分驗證。如需詳細資訊，請參閱 [設定 EMR 安全功能 \(p. 224\)](#)。
2. 使用您在上一個步驟中指定的安全組態來啟動叢集。如需詳細資訊，請參閱 [指定叢集的安全組態](#)。

使用 CLI 啟動與 Lake Formation 整合的 Amazon EMR 叢集

下列程序示範如何使用與 AWS Lake Formation 整合的 Zeppelin 啟動 Amazon EMR 叢集。

1. 使用下列內容建立安全組態的 `security-configuration.json` 檔案。
 - 指定在 S3 中上傳之 IdP 中繼資料檔案的完整路徑。
 - 使用您的 AWS 帳戶 ID 取代 `accountID`。
 - 指定 `TicketLifetimeInHours` 的值，以判斷由 KDC 發行的 Kerberos 票證的有效期間。

```
{  
    "LakeFormationConfiguration": {  
        "IdpMetadataS3Path": "s3://mybucket/myfolder/idpmetadata.xml",  
        "EmrRoleForUsersARN": "arn:aws:iam::account-id:role/IAM_Role_For_AWS_Services",  
        "LakeFormationRoleForSAMLPrincipalARN": "arn:aws:iam::account-  
id:role/IAM_Role_For_Lake_Formation"  
    },  
    "AuthenticationConfiguration": {  
        "KerberosConfiguration": {  
            "Provider": "ClusterDedicatedKdc",  
            "ClusterDedicatedKdcConfiguration": {  
                "TicketLifetimeInHours": 24  
            }  
        }  
    }  
}
```

2. 執行以下命令來建立安全組態。

```
aws emr create-security-configuration \  
--security-configuration file://./security-configuration.json \  
--name security-configuration
```

3. 建立設定 Hive 中繼存放區的 configurations.json 檔案。

```
[  
    {  
        "Classification": "spark-hive-site",  
        "Properties": {  
            "hive.metastore.glue.catalogid": "account-id"  
        }  
    }  
]
```

4. 執行下列命令，以啟動 Amazon EMR 叢集。

- 以您的子網路 ID 取代 `subnet-00xxxxxxxxxxxxxx11`。
- 以此叢集的 EC2 金鑰對名稱取代 `EC2_KEY_PAIR`。EC2 金鑰對是選用的，且只有在您想要使用 SSH 存取叢集時才需要。
- 以您的叢集名稱取代 `cluster-name`。

```
aws emr create-cluster --region us-east-1 \  
--release-label emr-5.26.0 \  
--use-default-roles \  
--instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.xlarge \  
InstanceGroupType=CORE,InstanceCount=1,InstanceType=m4.xlarge \  
--applications Name=Zeppelin Name=Livy \  
--kerberos-attributes Realm=EC2.INTERNAL,KdcAdminPassword=MyClusterKDCAdminPassword \  
--configurations file://configurations.json \  
--ec2-attributes KeyName=EC2_KEY_PAIR,SubnetId=subnet-00xxxxxxxxxxxxxx11 \  
--security-configuration security-configuration \  
--name cluster-name
```

在 IdP 中更新回呼或單一登入 URL

1. 使用主控台或 CLI 找出叢集中主節點和主執行個體 ID 的公有 IP 地址。
2. 在您的 IdP 帳戶中設定回呼 URL：
 - 使用 AD FS 做為 IDP 時，請完成以下步驟：
 1. 從 AD FS 管理主控台，進入 Relying Party Trusts (依賴方信任)。
 2. 以滑鼠右鍵按一下回覆方信任的顯示名稱，然後選擇 Properties (屬性)。
 3. 在 Properties (屬性) 視窗中，選擇 Endpoints (端點) 標籤。
 4. 選取您先前提供的臨時 URL，然後選擇 edit (編輯)。
 5. 在 Edit Endpoint (編輯端點) 視窗中，使用您主節點的正確 DNS 名稱更新信任的 URL。
 6. 在 Add an Endpoint (新增端點) 視窗中，在 Trusted URL (信任的 URL) 方塊中填入您的主節點公有 DNS。例如：

```
https://ec2-11-111-11-111.compute-1.amazonaws.com:8442/gateway/knoxss/api/v1/webss?pac4jCallback=true&client_name=SAML2Client
```

 - 7. 選擇 OK (確定)。
- 使用 Auth0 做為您的 IdP 時，請完成以下步驟：
 1. 前往 https://auth0.com/ 並登入。
 2. 在左側面板中，選擇 Applications (應用程式)。
 3. 選取您先前建立的應用程式。
 4. 在 Settings (設定) 標籤上，使用您的主節點公有 DNS 更新 Allowed Callback URL (允許的回呼 URL)。
- 使用 Okta 做為您的 IdP 時，請完成以下步驟：
 1. 前往 https://developer.okta.com/ 並登入。
 2. 在右上角，選擇 Admin (管理員)，然後選擇 Applications (應用程式) 標籤。
 3. 選取應用程式的名稱。
 4. 在應用程式的 General (一般) 標籤，選擇 SAML Settings (SAML 設定)，然後選擇 Edit (編輯)。
 5. 在 Configure SAML (設定 SAML) 標籤上，使用主節點公有 DNS 更新 Single-sign on URL (單一登入 URL)。

搭配 Lake Formation 使用 Notebooks

Apache Zeppelin 和 EMR Notebooks 都與 Lake Formation 整合，只要建立 EMR 叢集與 Lake Formation 的整合，即可使用。

若要存取這兩個筆記本應用程式，您必須先確定叢集的 EC2 安全群組或 VPC 網路存取控制清單 (ACL) 已設定為允許從桌面存取 Proxy 代理程式 (連接埠 8442)。

Note

EMR 叢集上的 Proxy 代理程式預設使用自我簽署的 Transport Layer Security (TLS) 憑證，您的瀏覽器將提示您接受憑證再繼續。如果您想要使用 Proxy 代理程式的自訂憑證，請參閱「自訂 Proxy 代理程式憑證」一節。

Apache Zeppelin

若要存取 Apache Zeppelin，請使用 EMR 主控台從叢集的 Summary (摘要) 標籤中找到 *Master public DNS (#### DNS)*。使用您的瀏覽器，導覽至 <https://MasterPublicDNS:8442/gateway/default/zeppelin/>。確認 URL 結尾包含斜線。

一旦接受 Proxy 代理程式的憑證，您的瀏覽器會將您重新導向至身分供應商 (IdP) 進行身分驗證。一旦通過身分驗證，系統會將您重新導向至 Zeppelin。

建立您的第一個 Zeppelin Notebook

若要開始使用，請選取 Notebook (筆記本)、Create new note (建立新備註) 來建立新的筆記本。為您的筆記本命名，並使用預設的 livy 解譯器。

若要查看 Lake Formation 資料庫清單，請使用下列 Spark SQL 命令。

```
spark.sql("show databases").show()
```

若要查詢特定的 Lake Formation 資料表，請使用下列 Spark SQL 命令。以 Lake Formation 中的實際資料庫和資料表取代 `database.table`：

```
spark.sql("SELECT * FROM database.table limit 10").show()
```

EMR Notebooks

EMR notebooks 可以使用 Amazon EMR 主控台建立，並搭配與 Lake Formation 整合的現有 EMR 叢集使用。

建立 EMR notebook

1. 在 <https://console.aws.amazon.com/elasticmapreduce/> 開啟 Amazon EMR 主控台。
2. 選擇 Notebooks (筆記本)、Create notebook (建立筆記本)。
3. 輸入 Notebook name (筆記本名稱) 和選填的 Notebook description (筆記本說明)。
4. 選取 Choose an existing cluster (選擇現有叢集)，然後選擇 Choose (選擇)。
5. 選取與 Lake Formation 整合的現有 EMR 叢集。
6. 選取 Create notebook (建立筆記本) 來建立筆記本。

建立筆記本之後，請選取筆記本，然後按一下 Open (開啟)。系統會將您重新導向至 Amazon EMR 叢集上的 Proxy 代理程式。一旦您接受 Proxy 代理程式的憑證，您的瀏覽器會將您重新導向至身分供應商 (IdP) 進行身分驗證。一旦通過身分驗證，系統會將您重新導向至 EMR notebook。

如需詳細資訊，請參閱《Amazon EMR Management Guide》中的[使用 Amazon EMR Notebooks](#)。

自訂 Proxy 代理程式憑證

Proxy 代理程式預設使用自我簽署的 Transport Layer Security (TLS) 憑證。若要對 Proxy 代理程式使用自訂憑證，您必須先從您的憑證授權單位取得憑證、憑證鏈和私有金鑰。有了這些項目，便能使用 PKCS12 檔案保護金鑰材料，以便可以將其匯入 Proxy 代理程式的金鑰存放區。Proxy 代理程式是以 Apache Knox 為基礎。您可以使用下列步驟用您的自訂憑證取代預設憑證。

在下列步驟中，將 `MasterPublicDNS` 取代為叢集詳細資訊窗格的 Summary (摘要) 標籤上 Master public DNS (主要公有 DNS) 顯示的值。例如，`ec2-11-222-33-44.compute-1.amazonaws.com`。

1. 若要從憑證、憑證鏈和私有金鑰建立 PKCS12 檔案，請在已安裝憑證檔案和 openssl 的主機上執行以下命令。

```
openssl pkcs12 -export -out proxy_agent_certificate.pfx -inkey private.key -  
in certificate.cer -certfile certchain.cer
```

2. 將 proxy_agent_certificate.pfx 檔案複製到叢集主節點上的 /home/hadoop 目錄。

```
scp -i EC2KeyPair.pem proxy_agent_certificate.pfx hadoop@MasterPublicDNS:/home/hadoop
```

3. SSH 連線到叢集的主節點。

```
ssh -i EC2KeyPair.pem hadoop@MasterPublicDNS
```

4. 使用下列命令尋找叢集專屬的主金鑰。

```
less /etc/knox/conf/gateway-site.xml
```

找出 *gateway.master.secret* 屬性，並複製 value 標籤的內容，因為後續步驟會用到它。

5. 使用下列命令，建立現有 Proxy 代理程式金鑰存放區的備份複本。

```
sudo -s
cd /mnt/var/lib/knox/data/security keystores
mkdir backups
mv gateway.jks __gateway-credentials.jceks backups/
```

6. 使用下列命令，將您的自訂憑證匯入新的金鑰存放區。

```
sudo -s
cd /mnt/var/lib/knox/data/security keystores
keytool -importkeystore \
-srckeystore /home/hadoop/proxy_agent_certificate.pfx \
-srcstoretype pkcs12 -destkeystore gateway.jks \
-deststoretype jks \
-srcalias 1 \
-destalias gateway-identity
```

當系統提示 Enter destination keystore password 時，使用 gateway-site.xml 檔案中的 Knox 主要密碼。

使用下列命令，確認 knox 使用者擁有新建立的 gateway.jks 檔案。

```
chown knox:knox gateway.jks
```

如果您的私有金鑰受密碼保護，請確保 Knox 知道該密碼。

```
sudo -u knox bash
cd /usr/lib/knox
bin/knoxcli.sh create-cert create-alias gateway-identity-passphrase
```

出現提示時，輸入保護您私有金鑰的密碼。

7. 使用以下命令重新啟動 Knox。

```
sudo -u knox bash
cd /usr/lib/knox
bin/gateway.sh stop
```

Knox 應該會自動重新啟動，您可以透過檢視 /var/log/knox/gateway.log 來查看 Knox 的狀態。

8. 為確保 Proxy 代理程式會使用新的憑證，請導覽至 Apache Zeppelin <https://MasterPublicDNS:8442/gateway/default/zeppelin/>。您可以使用瀏覽器來檢查憑證，以確保它是您的自訂憑證。

使用安全群組控制網路流量

安全群組就像是您叢集中 EC2 執行個體的虛擬防火牆，可用來控管傳入及傳出的流量。每個安全群組都具有一組控管傳入流量的規則，以及另一組控管傳出流量的規則。如需詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [適用於 Linux 執行個體的 Amazon EC2 安全群組](#)。

您可以使用兩種類別的安全群組來搭配 Amazon EMR：Amazon EMR 受管安全群組 和 額外的安全群組。

每個叢集都有與其相關聯的受管安全群組。您可以使用預設的受管安全群組，或指定自訂的受管安全群組。無論是哪一個選項，Amazon EMR 都會自動將規則新增到受管安全群組，叢集需要這些安全群組，來在叢集執行個體和 AWS 服務之間進行通訊。

額外的安全群組為選用。您可以在受管的安全群組之外，再指定這些群組，來量身打造對叢集執行個體的存取機制。額外的安全群組只包含您自己定義的規則。Amazon EMR 不會修改這些規則。

Amazon EMR 在受管安全群組中建立的規則，允許叢集在內部元件之間進行通訊。若要允許使用者和應用程式從叢集的外部來存取叢集，您可以編輯受管安全群組中的規則、建立包含額外規則的其他安全群組，或是同時執行這兩項動作。

Important

編輯受管安全群組中的規則，可能會有未預期的後果。您可能會在無意中封鎖叢集正常運作所需的流量，而且因為無法連線到節點而造成錯誤。請在建置之前仔細的規劃和測試安全群組狀態。

Warning

系統會使用可允許在連接埠 22 上來自所有來源 (IPv4 0.0.0.0/0) 之傳入流量的規則，來預先設定適用於公有子網路中主執行個體的預設 EMR 受管安全群組 `ElasticMapReduce-master`。這麼做可簡化 SSH 用戶端到主節點的初始連接。我們強烈建議您編輯此傳入規則，來限制只接收來自信任來源的流量或指定會限制存取的自訂安全群組。如需詳細資訊，請參閱 [使用 Amazon EMR 受管安全群組 \(p. 231\)](#)。

您可以在建立叢集時指定安全群組。當叢集正在執行時，規則無法新增到叢集或叢集執行個體，但您可以針對現有安全群組的規則，進行編輯、新增和移除。規則一旦儲存就會生效。

依預設，安全群組受到限制。除非已新增允許流量的規則，否則流量將會遭到拒絕。如果有一個以上的規則套用到相同的流量和相同的來源，則會套用最寬鬆的規則。例如，如果您的規則可允許從 IP 地址 192.0.2.12/32 進行 SSH 連線，而另一個規則允許從 192.0.2.0/24 的範圍存取所有的 TCP 流量，則允許從包含 192.0.2.12 的地址範圍，來存取所有 TCP 流量的規則，將會具有優先性。在這種情況中，位於 192.0.2.12 的用戶端，可能有擁有比您預期更多的存取權限。

在編輯安全群組規則時請務必小心。新增規則時，請務必只針對必要的通訊協定和連接埠，允許來自受信任用戶端的流量。我們不建議允許公有存取的傳入規則，也就是來自指定為 IPv4 0.0.0.0/0 或 IPv6::/0 之來源的流量。如果規則允許任何您未新增到例外清單連接埠上的公有存取，則您可以在每個區域中 Amazon EMR 設定封鎖公開存取，以防止建立叢集。根據預設，SSH 的連接埠 22 列於例外清單中。對於 2019 年 7 月之後建立的 AWS 帳戶，Amazon EMR 封鎖公開存取預設為開啟。對於 2019 年 7 月之前建立叢集的 AWS 帳戶，Amazon EMR 封鎖公開存取預設為關閉。如需詳細資訊，請參閱 [使用 Amazon EMR 封鎖公開存取 \(p. 238\)](#)。

主題

- [使用 Amazon EMR 受管安全群組 \(p. 231\)](#)
- [使用額外的安全群組 \(p. 235\)](#)
- [指定 Amazon EMR 受管安全群組和額外的安全群組 \(p. 235\)](#)
- [為 EMR 筆記本指定 EC2 安全群組 \(p. 236\)](#)
- [使用 Amazon EMR 封鎖公開存取 \(p. 238\)](#)

使用 Amazon EMR 受管安全群組

不同的受管安全群組，會和主執行個體及叢集中的核心與任務執行個體相關聯。當您在私有子網路中建立叢集時，會需要額外的受管安全群組以存取服務。關於您網路組態的受管安全群組角色，詳細資訊請參閱 [Amazon VPC 選項 \(p. 96\)](#)。

當您指定叢集的受管安全群組時，您必須針對所有的受管安全群組，使用相同類型的安全群組（預設或自訂）。例如，您不能指定主執行個體的自訂安全群組，然後不指定核心執行個體與任務執行個體的自訂安全群組。

如果使用預設的受管安全群組，則不需要在建立叢集時指定這些群組。Amazon EMR 會自動使用預設值。此外，如果預設群組不存在於叢集的 VPC 中，Amazon EMR 會建立這些群組。如果您明確指定尚未存在的群組，Amazon EMR 也會加以建立。

您可以在建立叢集之後，編輯受管安全群組中的規則。當您建立新的叢集時，Amazon EMR 會針對您所指定的受管安全群組，檢查其中的規則，然後在先前可能已經新增的規則之外，再建立新叢集所需任何遺漏的規則。除非明確說明，否則預設 EMR 受管安全群組的每個規則也會新增到您指定的自訂 EMR 受管安全群組。

預設的受管安全群組如下：

- ElasticMapReduce-master

如需此安全群組中的規則，請參閱 [適用於主執行個體的 Amazon EMR 受管安全群組 \(公有子網路\) \(p. 231\)](#)。

- ElasticMapReduce-slave

如需此安全群組中的規則，請參閱 [適用於核心執行個體和執行個體的 Amazon EMR 受管安全群組 \(公有子網路\) \(p. 233\)](#)。

- ElasticMapReduce-Master-Private

如需此安全群組中的規則，請參閱 [適用於主執行個體的 Amazon EMR 受管安全群組 \(私有子網路\) \(p. 233\)](#)。

- ElasticMapReduce-Slave-Private

如需此安全群組中的規則，請參閱 [適用於核心執行個體和執行個體的 Amazon EMR 受管安全群組 \(私有子網路\) \(p. 234\)](#)。

- ElasticMapReduce-ServiceAccess

如需此安全群組中的規則，請參閱 [用來存取服務 \(私有子網路\) 的 Amazon EMR 受管安全群組 \(p. 234\)](#)。

適用於主執行個體的 Amazon EMR 受管安全群組 (公有子網路)

公有子網路中主執行個體的預設受管安全群組，具有 ElasticMapReduce-master (ElasticMapReduce-master) 的 Group Name (群組名稱)。如果預設受管安全群組有下列規定，Amazon EMR 也會在您指定自訂受管安全群組時新增相同規定。

類型	通訊協定	連接埠範圍	來源	詳細資訊
傳入規則				
所有 ICMP-IPv4	全部	無	受管安全群組的群組 ID (適用於主執行個體)	這些自反規則，會允許與指定安全群組相關的任何執行個體，所傳入的流量。針對多個叢集使用預設的 ElasticMapReduce-master，可讓這些叢集

類型	通訊協定	連接埠範圍	來源	詳細資訊
所有 TCP	TCP	全部	體)。也就是包含規則的同一個安全群組。	的核心節點和任務節點，透過 ICMP 或任何 TCP 或 UDP 連接埠，來與彼此進行通訊。指定自訂的受管安全群組，來限制跨叢集存取。
所有 UDP	UDP	全部		
所有 ICMP-IPV4	全部	無	受管安全群組的群組 ID (針對核心節點和任務節點所指定)。	即使執行個體位於不同的叢集中，這些規則也可針對與指定安全群組相關聯的任何核心執行個體和任務執行個體，允許所有的傳入的 ICMP 流量，以及從這些執行個體透過任何 TCP 或 UDP 連接埠傳送的流量。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		
自訂	TCP	8443	各種 Amazon IP 地址範圍	這些規則可讓叢集管理程式和主節點進行通訊。
SSH	TCP	22	0.0.0.0/0	<p>允許來自任何來源的傳入 SSH 連接。</p> <p>Warning</p> <p>我們強烈建議您編輯此傳入規則，來限制只接收來自信任來源的流量。或者，指定要限制存取的自訂 EMR 受管安全群組。如需詳細資訊，請參閱 移除對 SSH 公有存取的程序 (p. 232)。</p>

針對 ElasticMapReduce-master 安全群組來移除可允許使用 SSH 進行公用存取的傳入規則

下列程序假設 ElasticMapReduce-master 安全群組先前未曾經過編輯。此外，若要編輯安全群組，您還必須以根使用者身分或可讓您管理叢集所在 VPC 之安全群組的 IAM 委託人身分，來登入 AWS。如需詳細資訊，請參閱 IAM User Guide 中的「[變更 IAM 使用者的許可](#)」和允許管理 EC2 安全群組的「[範例政策](#)」。

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Clusters (叢集)。
3. 選擇叢集的 Name (名稱)。
4. 在 Security and access (安全性與存取) 中，選擇 Security groups for Master (主叢集的安全群組) 連結。
5. 從清單中選擇 ElasticMapReduce-master (ElasticMapReduce-master)。
6. 選擇 Inbound (傳入)、Edit (編輯)。
7. 尋找具有下列設定的規則，然後選擇 x 圖示來刪除該規則：
 - 類型
 - 連接埠
 - 來源

SSH
22
自訂 0.0.0.0/0
8. 向下捲動到規則清單底部，然後選擇 Add Rule (新增規則)。

9. 針對 Type (類型) , 選擇 SSH (SSH)。

這會自動輸入 TCP 作為 Protocol (通訊協定) , 並輸入 22 作為 Port Range (連接埠範圍)。

10. 針對來源 , 選擇 My IP (我的 IP)。

這會自動將您用戶端電腦的 IP 地址 , 新增為來源地址。或者 , 您可以新增各種 Custom (自訂) 的受信任用戶端 IP 地址 , 然後選擇 Add rule (新增規則) , 來為其他的用戶端建立額外的規則。在許多的網路環境中 , IP 地址是動態分配的 , 因此您可能會需要定期編輯安全群組規則 , 來更新受信任用戶端的 IP 地址。

11. 選擇 Save (儲存)。

12. (選擇性) 從清單中選擇 ElasticMapReduce-slave (ElasticMapReduce-slave) , 並重複上述的步驟 , 以允許 SSH 用戶端從受信任的用戶端存取核心節點和任務節點。

適用於核心執行個體和執行個體的 Amazon EMR 受管安全群組 (公有子網路)

在公有子網路中 , 適用於核心執行個體和任務執行個體的預設受管安全群組 , 具有 ElasticMapReduce-slave (ElasticMapReduce-slave) 的 Group Name (群組名稱)。如果預設受管安全群組有下列規定 , Amazon EMR 也會在您指定自訂受管安全群組時新增相同規定。

類型	通訊協定	連接埠範圍	來源	詳細資訊
傳入規則				
所有 ICMP-IPv4	全部	無	受管安全群組的群組 ID (適用於核心執行個體和任務執行個體)。也就是包含規則的同一個安全群組。	這些自反規則 , 會允許與指定安全群組相關的任何執行個體 , 所傳入的流量。針對多個叢集使用預設的 ElasticMapReduce-slave , 可讓這些叢集的核心執行個體和任務執行個體 , 透過 ICMP 或任何 TCP 或 UDP 連接埠 , 來與彼此進行通訊。指定自訂的受管安全群組 , 來限制跨叢集存取。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		
所有 ICMP-IPv4	全部	無	受管安全群組的群組 ID (適用於主執行個體)。	即使執行個體位於不同的叢集中 , 這些規則也可針對與指定安全群組相關聯的任何主執行個體 , 允許所有的傳入的 ICMP 流量 , 以及從這些執行個體透過任何 TCP 或 UDP 連接埠傳送的流量。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		

適用於主執行個體的 Amazon EMR 受管安全群組 (私有子網路)

私有子網路中主執行個體的預設受管安全群組 , 具有 ElasticMapReduce-Master-Private (ElasticMapReduce-Master-Private) 的 Group Name (群組名稱)。如果預設受管安全群組有下列規定 , Amazon EMR 也會在您指定自訂受管安全群組時新增相同規定。

類型	通訊協定	連接埠範圍	來源	詳細資訊
傳入規則				
所有 ICMP-IPv4	全部	無	受管安全群組的群組 ID (適用於主執行個體)	這些自反規則 , 會允許與指定安全群組相關的任何執行個體 , 所傳入的流量 , 而且可從私

類型	通訊協定	連接埠範圍	來源	詳細資訊
所有 TCP	TCP	全部	體)。也就是包含規則的同一個安全群組。	有子網路中存取。針對多個叢集使用預設的 ElasticMapReduce-Master-Private，可讓這些叢集的核心節點和任務節點，透過 ICMP 或任何 TCP 或 UDP 連接埠，來與彼此進行通訊。指定自訂的受管安全群組，來限制跨叢集存取。
所有 UDP	UDP	全部		
所有 ICMP-IPV4	全部	無	受管安全群組的群組 ID (適用於核心節點和任務節點)。	即使執行個體位於不同的叢集中，這些規則也可針對與指定安全群組相關聯的任何核心執行個體和任務執行個體 (可從私有子網路與其連線)，允許所有的傳入的 ICMP 流量，以及從這些執行個體透過任何 TCP 或 UDP 連接埠傳送的流量。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		
HTTPS (8443)	TCP	8443	受管安全群組的群組 ID，用來在私有子網路中存取服務。	此規則可允許叢集管理程式與主節點進行通訊。

適用於核心執行個體和執行個體的 Amazon EMR 受管安全群組 (私有子網路)

在私有子網路中，適用於核心執行個體和任務執行個體的預設受管安全群組，具有 ElasticMapReduce-Slave-Private (ElasticMapReduce-Slave-Private) 的 Group Name (群組名稱)。如果預設受管安全群組有下列規定，Amazon EMR 也會在您指定自訂受管安全群組時新增相同規定。

類型	通訊協定	連接埠範圍	來源	詳細資訊
傳入規則				
所有 ICMP-IPV4	全部	無	受管安全群組的群組 ID (適用於核心執行個體和任務執行個體)。	這些自反規則，會允許與指定安全群組相關的任何執行個體，所傳入的流量。針對多個叢集使用預設的 ElasticMapReduce-slave，可讓這些叢集的核心執行個體和任務執行個體，透過 ICMP 或任何 TCP 或 UDP 連接埠，來與彼此進行通訊。指定自訂的受管安全群組，來限制跨叢集存取。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		
所有 ICMP-IPV4	全部	無	受管安全群組的群組 ID (適用於主執行個體)。	即使執行個體位於不同的叢集中，這些規則也可針對與指定安全群組相關聯的任何主執行個體，允許所有的傳入的 ICMP 流量，以及從這些執行個體透過任何 TCP 或 UDP 連接埠傳送的流量。
所有 TCP	TCP	全部		
所有 UDP	UDP	全部		
HTTPS (8443)	TCP	8443	受管安全群組的群組 ID，用來在私有子網路中存取服務。	此規則可允許叢集管理程式和核心節點與任務節點進行通訊。

用來存取服務 (私有子網路) 的 Amazon EMR 受管安全群組

私有子網路中用來存取服務的預設受管安全群組，具有 ElasticMapReduce-ServiceAccess (ElasticMapReduce-ServiceAccess) 的 Group Name (群組名稱)。該群組不具有傳入與傳出規則，來允許透

過 HTTPS (連接埠 8443) , 將流量傳送到私有子網路中的其他受管安全群組。這些規則可讓叢集管理程式和主節點、核心和任務節點進行通訊。如果您指定自訂的安全群組，會新增相同的規則。

使用額外的安全群組

無論您是使用預設的受管安全群組，或指定自訂的受管安全群組，都可以使用額外的安全群組。額外的安全群組可提供彈性，讓您量身打造叢集之間的存取，以及從外部用戶端、資源和應用程式進行的存取。

以下列的情境為例。您擁有需要互相進行通訊的多個叢集，但您只想針對特定的部分叢集，允許傳入的 SSH 存取主執行個體。若要這麼做，您可以針對叢集使用同一組受管安全群組。然後，建立額外的安全群組，以允許從受信任用戶端的傳入 SSH 存取，並且為子集中每個叢集的主執行個體，指定額外的安全群組。

您可以針對主執行個體、核心執行個體與任務執行個體及服務存取 (在私有子網路中)，各指定最多四個額外的安全群組。如有必要，您可以針對主執行個體、核心執行個體與任務執行個體及服務存取，指定同樣的額外安全群組。您帳戶中安全群組與規則的數目上限，會受到帳戶的限制。如需詳細資訊，請參閱 Amazon VPC User Guide 中的[安全群組限制](#)。

指定 Amazon EMR 受管安全群組和額外的安全群組

您可以利用 AWS Management Console、AWS CLI 或 EMR API 來指定安全群組。如果您未指定安全群組，Amazon EMR 會建立預設的安全群組。指定額外的安全群組為選用功能。您可以針對主執行個體、核心執行個體與任務執行個體及服務存取 (僅限私有子網路)，指定額外的安全群組。

使用主控台來指定安全群組

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集) , Go to advanced options (前往進階選項)。
3. 為您的叢集選取選項，直到進入 Step 4: Security (步驟 4：安全性)。
4. 選取 EC2 Security Groups (EC2 安全群組) 來展開此區段。

在 EMR managed security groups (EMR 受管安全群組) 中，預設會選取預設的受管安全群組。如果在 VPC 中，不存在適用於 Master (主要)、Core & Task (核心與任務) 或 Service Access (服務存取) (僅限私有子網路) 的預設受管安全群組，則在關聯的安全群組名稱前方，會顯示 Create (建立)。

5. 如果您使用自訂的受管安全群組，請從 EMR managed security groups (EMR 受管安全群組) 清單中選擇。

如果您選取自訂的受管安全群組，會出現訊息，通知您選擇其他執行個體的自訂安全群組。您可以針對叢集使用自訂的或唯一的預設受管安全群組。

6. 或者，您可以在 Additional security groups (額外的安全群組) 中，選擇鉛筆圖示、從清單中選取最多四個安全群組，然後選擇 Assign security groups (指派安全群組)。根據需要，各針對 Master (主要)、Core & Task (核心與任務) 和 Service Access (服務存取)，重複前述的動作。
7. 選擇 Create Cluster (建立叢集)。

使用 AWS CLI 來指定安全群組

若要使用 AWS CLI 來指定安全群組，您可以使用 `create-cluster` 指令搭配 `--ec2-attributes` 選項的下列參數：

參數	描述
<code>EmrManagedMasterSecurityGroup</code>	使用此參數來為主執行個體指定自訂的受管安全群組。如果指定此參數，也必須指定 <code>EmrManagedSlaveSecurityGroup</code> 。

參數	描述
	如果是私有子網路中的叢集，還必須指定 <code>ServiceAccessSecurityGroup</code> 。
<code>EmrManagedSlaveSecurityGroup</code>	使用此參數來為核心執行個體與任務執行個體，指定自訂的受管安全群組。如果指定此參數，也必須指定 <code>EmrManagedMasterSecurityGroup</code> 。如果是私有子網路中的叢集，還必須指定 <code>ServiceAccessSecurityGroup</code> 。
<code>ServiceAccessSecurityGroup</code>	使用此參數來指定自訂受管安全群組受管的服務存取，這只適用於私有子網路中的叢集。如果指定此參數，也必須指定 <code>EmrManagedMasterSecurityGroup</code> 。
<code>AdditionalMasterSecurityGroups</code>	使用此參數來為主執行個體指定最多四個額外的受管安全群組。
<code>AdditionalSlaveSecurityGroups</code>	使用此參數來為核心執行個體和任務執行個體，指定最多四個額外的受管安全群組。

Example — 指定自訂的 Amazon EMR 受管安全群組和額外安全群組

下列範例為私有子網路中的叢集，指定自訂的 Amazon EMR 受管安全群組、為主執行個體指定多個額外的安全群組，以及為核心執行個體和任務執行個體指定一個額外的安全群組。

Note

將 Linux 的行接續字元 (\) 包含在內，以提升可讀性。這些字元可以移除或在 Linux 命令中使用。用於 Windows 時，請將其移除或以插入號 (^) 取代。

```
aws emr create-cluster --name "ClusterCustomManagedAndAdditionalSGs" \
--release-label emr-emr-5.28.0 --applications Name=Hue Name=Hive \
Name=Pig --use-default-roles --ec2-attributes \
SubnetIds=subnet-xxxxxxxxxxxx,KeyName=myKey, \
ServiceAccessSecurityGroup=sg-xxxxxxxxxxxx, \
EmrManagedMasterSecurityGroup=sg-xxxxxxxxxxxx, \
EmrManagedSlaveSecurityGroup=sg-xxxxxxxxxxxx, \
AdditionalMasterSecurityGroups=['sg-xxxxxxxxxxxx', \
'sg-xxxxxxxxxxxx', 'sg-xxxxxxxxxxxx'], \
AdditionalSlaveSecurityGroups=sg-xxxxxxxxxxxx \
--instance-type m5.xlarge
```

如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [create-cluster](#)。

為 EMR 筆記本指定 EC2 安全群組

當您建立 EMR 筆記本 時，可使用兩個安全群組，在使用筆記本編輯器時，控管 EMR 筆記本 與 Amazon EMR 叢集之間的網路流量。預設的安全群組具有最低要求的規則，只針對 EMR 筆記本 服務和筆記本所連接的叢集，允許這兩者之間的網路流量。

EMR 筆記本 會使用 [Apache Livy](#)，利用 TCP 連接埠 18888，透過代理程式來和叢集進行通訊。藉由建立自訂的安全群組，以及根據您環境量身打造的規則，您可以限制網路流量，只允許筆記本的子集可以在特定叢集上的筆記本編輯器中，來執行程式碼。除了叢集的安全群組之外，也會使用這些安全群組。如需詳細資訊，請參閱 Amazon EMR Management Guide 與 [為 EMR 筆記本指定 EC2 安全群組 \(p. 236\)](#) 中的 [使用安全群組來控管網路流量](#)。

主執行個體預設的 EC2 安全群組

除了叢集適用於主執行個體的安全群組之外，主執行個體適用的預設 EC2 安全群組，也和主執行個體具有關聯。

群組名稱：ElasticMapReduceEditors-Livy (ElasticMapReduceEditors-Livy)

規則

- 傳入

允許從 EMR 筆記本 預設 EC2 安全群組中的任何資源，透過 TCP 連接埠 18888 傳送

- 傳出

無

EMR Notebooks 的預設 EC2 安全群組

EMR 筆記本 的預設 EC2 安全群組，會和指派給任何 EMR 筆記本 的筆記本編輯器具有關聯。

群組名稱：ElasticMapReduceEditors-Editor (ElasticMapReduceEditors-Editor)

規則

- 傳入

無

- 傳出

允許透過 TCP 連接埠 18888，傳送至 EMR 筆記本 預設 EC2 安全群組中的任何資源。

建立筆記本與 Git 儲存庫的關聯性時，EMR Notebooks 的自訂 EC2 安全群組

若要將 Git 儲存庫連結到筆記本，EMR 筆記本的安全群組必須包含傳出規則，讓筆記本能夠透過叢集將流量路由傳送到網際網路。建議您針對此用途建立新的安全群組。更新預設 ElasticMapReduceEditors-Editor 安全群組時，可將相同的傳出規則提供給已連接到此安全群組的其他筆記本。

規則

- 傳入

無

- 傳出

允許筆記本透過叢集將流量路由到網際網路，如下列範例所示：

類型	通訊協定	連接埠範圍	目的地
自訂 TCP 規則	TCP	18888	SG-
自訂 TCP 規則	TCP	8998	SG-
HTTPS	TCP	443	0.0.0.0/0

使用 Amazon EMR 封鎖公開存取

當任何安全群組與具有規則（允許來自連接埠上 IPv4 0.0.0.0/0 or IPv6 ::/0 (公開存取) 的傳入流量）的叢集相關聯時，Amazon EMR 封鎖公開存取會防止叢集啟動，除非連接埠已被指定為例外。連接埠 22 預設為例外。您可以設定例外狀況，以允許連接埠或連接埠範圍的公有存取。此外，您可以啟用或停用封鎖公開存取。建議您啟用此功能。

您 AWS 帳戶中每個 AWS 區域已啟用且設定封鎖公開存取。換言之，每個區域都有封鎖公開存取組態，適用於您帳戶在該區域中建立的所有叢集。

設定封鎖公開存取

您可以使用 AWS Management Console、AWS CLI 和 Amazon EMR API 啟用和停用封鎖公開存取設定。設定會依據各個區域套用到您的帳戶。

使用 AWS Management Console 設定封鎖公開存取

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 在導覽列上，確定已選取您要設定的 Region (區域)。
3. 選擇 封鎖公開存取。
4. 在 Block public access settings (封鎖公開存取設定) 下，完成以下步驟。

若要...	執行此作業...
開啟或關閉封鎖公開存取	選擇 Change (變更)，選擇 On (開啟) 或 Off (關閉)，然後選擇核取記號來確認。
編輯例外清單中的連接埠	<ol style="list-style-type: none">1. 在 Exceptions (例外狀況) 下，選擇 Edit (編輯)。2. 若要將連接埠新增至例外清單，請選擇 Add a port range (新增連接埠範圍)，然後輸入新的連接埠或連接埠範圍。針對每個新增的連接埠或連接埠範圍重複此步驟。3. 若要移除連接埠或連接埠範圍，請選擇在 Port range (連接埠範圍) 清單旁的 x。4. 選擇 Save Changes (儲存變更)。

使用 AWS CLI 設定封鎖公開存取

使用 `aws emr put-block-public-access-configuration` 指令來設定封鎖公開存取，如下列範例所示。

若要...	執行此作業...
開啟封鎖公開存取	<p>如下列範例所示，設定 <code>BlockPublicSecurityGroupRules</code> 到 <code>true</code>。若要讓叢集啟動，任何與叢集相關聯的安全群組都可以有允許公開存取的傳入規則。</p> <pre>aws emr put-block-public-access-configuration --block-public-access-configuration BlockPublicSecurityGroupRules=true</pre>

若要...	執行此作業...
關閉封鎖公開存取	<p>如下列範例所示，設定 BlockPublicSecurityGroupRules 到 false。與叢集相關聯的安全群組可以擁有允許任何連接埠上公有存取的傳入規則。我們不建議使用此組態。</p> <pre>aws emr put-block-public-access-configuration --block-public-access-configuration BlockPublicSecurityGroupRules=false</pre>
開啟封鎖公開存取，並將連接埠指定為例外狀況	<p>下列範例開啟封鎖公開存取，並將連接埠 22 和連接埠 100-101 指定為例外狀況。這可以讓叢集建立相關聯的安全群組具有允許連接埠 22、連接埠 100 或連接埠 101 公開存取的傳入規則。</p> <pre>aws emr put-block-public-access-configuration --block-public-access-configuration '{ "BlockPublicSecurityGroupRules": true, "PermittedPublicSecurityGroupRuleRanges": [{ "MinRange": 22, "MaxRange": 22 }, { "MinRange": 100, "MaxRange": 101 }] }'</pre>

Amazon EMR 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 Amazon EMR 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱[合規計劃內的 AWS 服務](#)。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱[在 AWS Artifact 中下載報告](#)。

您使用 Amazon EMR 的合規責任，取決於資料的機密性、您公司的合規目標及適用法律和法規。若您使用的 Amazon EMR 必須遵循特定標準（如 HIPAA、PCI 或 FedRAMP），AWS 會提供資源予以協助：

- [安全與合規快速入門指南](#) – 這些部署指南討論在 AWS 上部署以安全及合規為重心之基準環境的架構考量和步驟。
- [HIPAA 安全與合規架構白皮書](#) – 本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- [AWS 合規資源](#) – 這組手冊和指南可能適用於您的產業和位置。
- [AWS Config](#) – 此 AWS 服務可評定資源組態與內部實務、業界準則和法規的合規狀態。
- [AWS Security Hub](#) – 此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

Amazon EMR 中的彈性

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠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、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域與可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施，Amazon EMR 還提供數種功能，可協助支援資料的彈性和備份需求。

- 透過 EMRFS 整合 Amazon S3
- 支援多個主節點

Amazon EMR 中的基礎設施安全

Amazon EMR 為受管服務，受到 [Amazon Web Services：安全程序概觀](#)白皮書所述的 AWS 全球網路安全程序所保護。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon EMR。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。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 委託人相關聯的私密存取金鑰來簽署。或者，您可以使用 [AWS Security Token Service \(AWS STS\)](#) 來產生暫時安全登入資料來簽署請求。

管理叢集

啟動叢集之後，您可以加以監控和管理。Amazon EMR 提供多種工具，可用來連接和控制您的叢集。

主題

- [查看和監控叢集 \(p. 241\)](#)
- [連接叢集 \(p. 276\)](#)
- [終止叢集 \(p. 288\)](#)
- [調整叢集資源規模 \(p. 290\)](#)
- [使用主控台複製叢集 \(p. 304\)](#)
- [將工作提交到叢集 \(p. 305\)](#)
- [使用 AWS Data Pipeline 自動化再次出現的叢集 \(p. 309\)](#)

查看和監控叢集

Amazon EMR 提供您可以使用的多種工具來蒐集叢集的相關資訊。您可以從主控台、CLI 或以程式設計的方式存取叢集的相關資訊。Hadoop 的 Web 界面和日誌檔的標準在主節點上可供使用。您也可以使用 CloudWatch 和 Ganglia 等監控服務，來追蹤叢集的效能。

主題

- [查看叢集狀態和詳細資訊 \(p. 241\)](#)
- [增強型步驟偵錯 \(p. 246\)](#)
- [查看應用程式歷史記錄 \(p. 247\)](#)
- [檢視日誌檔 \(p. 250\)](#)
- [檢視 Amazon EC2 中的叢集執行個體 \(p. 254\)](#)
- [CloudWatch 事件與指標 \(p. 254\)](#)
- [使用 Ganglia 檢視叢集應用程式指標 \(p. 274\)](#)
- [在 AWS CloudTrail 中記錄 Amazon EMR API 呼叫 \(p. 274\)](#)

查看叢集狀態和詳細資訊

建立叢集後，您可以監控叢集的狀態，也可以取得叢集執行狀況和可能發生過的錯誤的詳細資訊，即使叢集已經終止也無妨。Amazon EMR 會將終止叢集的中繼資料保留兩個月以供參考使用，之後才會將其刪除。應用程式歷史記錄則會從記錄開始的時間起算，保留一週，無論叢集是在運作中抑或已終止。您無法刪除叢集歷程記錄中的叢集，但在使用 AWS Management Console 時可使用 Filter (篩選條件)，而使用 AWS CLI 時則可透過選項搭配 `list-clusters` 命令，藉以聚焦在您所關注的叢集上。

使用 AWS Management Console 檢視叢集狀態

Amazon EMR 主控台的 Clusters List (叢集清單) 會列出您帳戶和 AWS 區域內的所有叢集，包括已終止的叢集。該清單顯示了每個叢集的以下內容：Name (名稱) 及 ID、Status (狀態)、Creation time (建立時間)，叢集執行的 Elapsed time (經過時間)，與叢集中所有 EC2 執行個體已累積的 Normalized instance hours (執行

個體時數標準化)。這份清單就是用來監控叢集狀態的起點。它的設計用意是要讓使用者深入探索各個叢集的詳細資訊，以供分析和疑難排解。

檢視叢集資訊的簡略版摘要

- 選取 Name (名稱) 下方叢集連結旁的向下箭頭。

如此即會展開叢集列，提供更多叢集、硬體、步驟、引導操作的相關資訊。使用此區段的連結即可深入探索各項規格。舉例而言，按一下 Steps (步驟) 下方的連結，即可存取步驟日誌檔，也可以查看步驟相關的 JAR，進一步深究該步驟的任務和任務，也可以存取日誌檔。

The screenshot shows the Amazon EMR console interface. At the top, there's a filter bar with 'All clusters' selected, showing '100 clusters loaded'. Below it is a table with columns: Name, ID, Status, Creation time (UTC-7), Elapsed time, and Normalized instances. One row is highlighted for 'Word count' with ID 'j-3HXR4JT224DZZ', showing 'Terminated' status and 'All steps completed'. A tooltip for 'View all interactive jobs' is visible over the 'Steps' column. To the right of the main table, there's a sidebar with sections for 'Summary', 'Master public DNS', 'Termination protection', 'Tags', and 'Hardware'. Under 'Hardware', it lists 'Master: Terminated 1 m1.small', 'Core: Terminated 2 m1.small', and 'Task: --'. On the far right, there's a section for 'Bootstrap Actions' with a note 'No bootstrap actions available'.

深入檢視叢集狀態

- 選擇 Name (名稱) 下方的叢集連結，即可開啟該叢集的叢集詳細資訊頁面。各個標籤可以檢視下段所述的各項資訊。

各標籤分別提供下列資訊：

This screenshot shows the 'Summary' tab of a cluster detail page. It includes tabs for Summary, Application history, Monitoring, Hardware, Events, Steps, Configurations, and Bootstrap actions. The Summary tab displays basic cluster information: ID (j-162692D2BOSWL), Creation date (2017-09-07 13:42 UTC-7), Elapsed time (10 days), Auto-terminate (No), and Termination protection (Change). It also shows network details like Availability zone (us-east-1b), Subnet ID (us-east-1b), and EC2 instance profile (EMR_E2C_DefaultRole). Security details include Key name (MyKeyPair), EC2 instance profile (EMR_E2C_DefaultRole), and EC2 instance role (EMR_DefaultRole). It also lists security groups for master (ElasticMapReduce-Master) and core (ElasticMapReduce-Core & Task).

Tab	資訊
摘要	此索引標籤可檢視叢集組態的基本資訊，例如至主節點的 SSH 連線所用的 URL、叢集建立時 Amazon EMR 所安裝的開放原始碼應用程式、存放於 Amazon S3 內的日誌、用於建立叢集的 Amazon EMR 版本等。
應用程式歷程記錄	此標籤可檢視 YARN 應用程式的詳細資訊。若為 Spark 任務，您可以深入探索任務、階段、執行狀況的可用資訊。如需更多詳細資訊，請參閱 查看應用程式歷史記錄 (p. 247) 。
監控	此標籤可查看多種圖表，圖表中會顯示出您所指定的時段中叢集操作的關鍵指標。可檢視叢集層級和節點層級的資料，以及 I/O 和資料儲存體的相關資訊。
硬體	使用此標籤可檢視叢集中節點的相關資訊，包括 EC2 執行個體 ID、DNS 名稱、IP 地址等。

Tab	資訊
活動	此標籤可檢視叢集的事件日誌。如需更多詳細資訊，請參閱 監控 CloudWatch Events (p. 255) 。
步驟	使用此標籤可查看您提交之步驟的狀態和存取日誌檔。如需步驟的詳細資訊，請參閱 使用 CLI 和主控台來使用步驟 (p. 305) 。
組態	此標籤可檢視套用自該叢集的任何自訂組態。如需組態分態的詳細資訊，請參閱 Amazon EMR Release Guide 中的 設定應用程式 。
引導操作	此標籤可檢視叢集啟動時所執行的任何引導操作的狀態。引導操作是供自訂軟體安裝和進階組態之用。如需更多詳細資訊，請參閱 建立引導操作來安裝其他軟體 (p. 86) 。

使用 AWS CLI 檢視叢集狀態

以下範例示範了如何使用 AWS CLI 摳取叢集的詳細資訊。如需可用命令的詳細資訊，請參閱 [Amazon EMR 之 AWS CLI 命令列參考](#)。您可以使用 `describe-cluster` 命令檢視叢集層級的詳細資訊，包括狀態、軟硬體組態、VPC 設定、引導操作、執行個體群組等。以下範例示範 `describe-cluster` 命令的使用方式，後續還會提供 `list-clusters` 命令的範例。

Example 檢視叢集狀態

若要使用 `describe-cluster` 命令，則需要有叢集 ID。此範例所示範的是用於取得在特定時間範圍內建立的叢集清單，再使用其中一個回傳的叢集 ID 來列出更多個別叢集狀態的資訊。

以下命令描述的是叢集 `j-1K48XXXXXXHCB`，請改為您的叢集 ID。

```
aws emr describe-cluster --cluster-id j-1K48XXXXXXHCB
```

您命令的輸出會類似如下：

```
{
    "Cluster": {
        "Status": {
            "Timeline": {
                "ReadyDateTime": 1438281058.061,
                "CreationDateTime": 1438280702.498
            },
            "State": "WAITING",
            "StateChangeReason": {
                "Message": "Waiting for steps to run"
            }
        },
        "Ec2InstanceAttributes": {
            "EmrManagedMasterSecurityGroup": "sg-cXXXXXX0",
            "IamInstanceProfile": "EMR_EC2_DefaultRole",
            "Ec2KeyName": "myKey",
            "Ec2AvailabilityZone": "us-east-1c",
            "EmrManagedSlaveSecurityGroup": "sg-example"
        },
        "Name": "Development Cluster",
        "ServiceRole": "EMR_DefaultRole",
        "Tags": []
    }
}
```

```

    "TerminationProtected": false,
    "ReleaseLabel": "emr-4.0.0",
    "NormalizedInstanceHours": 16,
    "InstanceGroups": [
        {
            "RequestedInstanceCount": 1,
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1438281058.101,
                    "CreationDateTime": 1438280702.499
                },
                "State": "RUNNING",
                "StateChangeReason": {
                    "Message": ""
                }
            },
            "Name": "CORE",
            "InstanceGroupType": "CORE",
            "Id": "ig-2EEXAMPLEXXP",
            "Configurations": [],
            "InstanceType": "m5.xlarge",
            "Market": "ON_DEMAND",
            "RunningInstanceCount": 1
        },
        {
            "RequestedInstanceCount": 1,
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1438281023.879,
                    "CreationDateTime": 1438280702.499
                },
                "State": "RUNNING",
                "StateChangeReason": {
                    "Message": ""
                }
            },
            "Name": "MASTER",
            "InstanceGroupType": "MASTER",
            "Id": "ig-2A1234567XP",
            "Configurations": [],
            "InstanceType": "m5.xlarge",
            "Market": "ON_DEMAND",
            "RunningInstanceCount": 1
        }
    ],
    "Applications": [
        {
            "Version": "1.0.0",
            "Name": "Hive"
        },
        {
            "Version": "2.6.0",
            "Name": "Hadoop"
        },
        {
            "Version": "0.14.0",
            "Name": "Pig"
        },
        {
            "Version": "1.4.1",
            "Name": "Spark"
        }
    ],
    "BootstrapActions": [],
    "MasterPublicDnsName": "ec2-X-X-X-X.compute-1.amazonaws.com",
    "AutoTerminate": false,

```

```
"Id": "j-jobFlowID",
"Configurations": [
    {
        "Properties": {
            "hadoop.security.groups.cache.secs": "250"
        },
        "Classification": "core-site"
    },
    {
        "Properties": {
            "mapreduce.tasktracker.reduce.tasks.maximum": "5",
            "mapred.tasktracker.map.tasks.maximum": "2",
            "mapreduce.map.sort.spill.percent": "90"
        },
        "Classification": "mapred-site"
    },
    {
        "Properties": {
            "hive.join.emit.interval": "1000",
            "hive.merge.mapfiles": "true"
        },
        "Classification": "hive-site"
    }
]
```

Example 按建立日期列出叢集

若要擷取在指定日期範圍內建立的叢集，請使用 `list-clusters` 命令搭配 `--created-after` 及 `--created-before` 參數。

以下命令會列出 2014 年 10 月 9 日到 2014 年 10 月 12 日之間建立的所有叢集。

```
aws emr list-clusters --created-after 2014-10-09T00:12:00 --created-before 2014-10-12T00:12:00
```

Example 按狀態列出叢集

若要按狀態列出叢集，請使用 `list-clusters` 命令搭配 `--cluster-states` 參數。有效的叢集狀態包括：
STARTING、BOOTSTRAPPING、RUNNING、WAITING、TERMINATING、TERMINATED、TERMINATED_WITH_ERRORS

```
aws emr list-clusters --cluster-states TERMINATED
```

您也可以使用以下捷徑參數列出所有處在指定狀態下的叢集：

- `--active` 會篩選出處於 STARTING、BOOTSTRAPPING、RUNNING、WAITING 或 TERMINATING 狀態下的叢集。
- `--terminated` 會篩選出處於 TERMINATED 狀態的叢集。
- `--failed` 參數會篩選出處於 TERMINATED_WITH_ERRORS 狀態的叢集。

以下命令會傳回相同的結果。

```
aws emr list-clusters --cluster-states TERMINATED
```

```
aws emr list-clusters --terminated
```

增強型步驟偵錯

如果 Amazon EMR 步驟失敗，而您使用包含 AMI 5.x 或更新版本的步驟 API 操作，提交了工作，則 Amazon EMR 可以在某些情況中，找出和傳回步驟失敗的根本原因，以及相關日誌檔的名稱，並透過 API 追蹤部分應用程式堆疊。例如，您可以識別以下失敗：

- 常見 Hadoop 錯誤 (例如輸出目錄已存在，輸入目錄不存在，或應用程式將記憶體用盡)。
- Java 錯誤 (例如使用不相容的 Java 版本來編譯應用程式，或應用程式透過找不到的主要類別來執行)。
- 存取在 Amazon S3 中存放之物件的問題。

您可以使用 [DescribeStep](#) 和 [ListSteps](#) API 操作來獲得此資訊。[StepSummary](#) 的 [FailureDetails](#) 欄位 (由這些操作所傳回)。若要存取 FailureDetails 資訊，請使用 AWS CLI、主控台或 AWS 開發套件。

使用 AWS 主控台檢視失敗的詳細資訊

- Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
- 選擇 Cluster List (叢集清單)，然後選取叢集。
- 選取每個步驟旁的箭頭圖示，來檢視更多詳細資訊。

如果步驟失敗且 Amazon EMR 可以識別根本原因的，請參閱故障的詳細資訊。

ID	Name	Status
s-IVXTXADABLBE	WordCount	Failed

Status: FAILED
Reason: Output directory already exists.
Log File: s3://aws-logs-us-east-1/elasticmapreduce/j-MQG1MTOTJ7HM/steps/s-IVXTXADABLBE/stderr.gz ⓘ
Details: org.apache.hadoop.mapred.FileAlreadyExistsException: Output directory s3://bucket/output already exists
JAR location: s3://bucket/hadoop-mapreduce-examples-2.7.2-amzn-1.jar
Main class: None
Arguments: wordcount s3://bucket/input/hello.txt s3://bucket/output
Action on failure: Continue

ID	Name	Status
s-3R6M87MQTDGPS	WordCount	Failed
s-43HPMI46PES7	Custom JAR	Failed
s-21EQLTWWIUTUV	Setup hadoop debugging	Completed

使用 AWS CLI 檢視失敗的詳細資訊

- 若要取得使用 AWS CLI 的步驟失敗詳細資訊，請使用 `describe-step` 命令。

```
aws emr describe-step --cluster-id j-1K48XXXXXXHCB --step-id s-3QM0XXXXXM1W
```

輸出格式應類似以下內容：

```
{  
  "Step": {  
    "Status": {  
      "FailureDetails": {  
        "Reason": "Output directory already exists.",  
        "LogFile": "s3://aws-logs-us-east-1/elasticmapreduce/j-MQG1MTOTJ7HM/steps/s-IVXTXADABLBE/stderr.gz",  
        "Details": "org.apache.hadoop.mapred.FileAlreadyExistsException: Output directory s3://bucket/output already exists",  
        "JARLocation": "s3://bucket/hadoop-mapreduce-examples-2.7.2-amzn-1.jar",  
        "MainClass": "None",  
        "Arguments": "wordcount s3://bucket/input/hello.txt s3://bucket/output",  
        "ActionOnFailure": "Continue"  
      }  
    }  
  }  
}
```

```
"LogFile": "s3://myBucket/logs/j-1K48XXXXXXHCB/steps/s-3QM0XXXXXM1W/stderr.gz",
"Message": "org.apache.hadoop.mapred.FileAlreadyExistsException: Output
directory s3://myBucket/logs/beta already exists",
"Reason": "Output directory already exists."
},
"Timeline": {
"EndDate": 1469034209.143,
"CreationDate": 1469033847.105,
"Start": 1469034202.881
},
"State": "FAILED",
"StateChangeReason": {}
},
"Config": {
"Args": [
"wordcount",
"s3://myBucket/input/input.txt",
"s3://myBucket/logs/beta"
],
"Jar": "s3://myBucket/jars/hadoop-mapreduce-examples-2.7.2-amzn-1.jar",
"Properties": {}
},
"Id": "s-3QM0XXXXXM1W",
"ActionOnFailure": "CONTINUE",
"Name": "ExampleJob"
}
}
```

查看應用程式歷史記錄

您可以使用主控台之叢集詳細資訊頁面的 Application history (應用程式歷程記錄) 索引標籤，檢視 Spark 和 YARN 應用程式詳細資訊。Amazon EMR 應用程式歷程記錄可讓您針對使用中的任務和任務歷程記錄輕鬆進行疑難排解和分析。

Application history (應用程式歷程記錄) 索引標籤提供兩種檢視選項：

- 從主控台存取 Spark 歷程記錄伺服器 UI – 透過 Amazon EMR 5.25.0 版或更新版本，您可以選擇連結以存取 Spark 歷程記錄伺服器 UI，而不需要透過 SSH 連線設定 Web Proxy。Spark 歷程記錄伺服器 UI 可提供排程器階段和任務的相關詳細資訊、RDD 大小和記憶體使用量、環境資訊，以及執行中執行程式的相關資訊。
- 檢視應用程式歷程記錄摘要 – 透過 Amazon EMR 5.8.0 版或更新版本，您可以在 EMR 主控台中檢視應用程式歷程記錄摘要，包括階段任務和執行程式的關鍵指標。應用程式歷程記錄摘要適用於所有 YARN 應用程式。系統會提供 Spark 應用程式的其他詳細資訊，但這些詳細資訊僅為透過 Spark 歷程記錄伺服器 UI 取得的資訊子集。

主題

- [從主控台存取 Spark 歷程記錄伺服器 UI \(p. 247\)](#)
- [檢視應用程式歷程記錄摘要 \(p. 249\)](#)

從主控台存取 Spark 歷程記錄伺服器 UI

透過 Amazon EMR 5.25.0 版和更新版本，您可以從叢集 Summary (摘要) 頁面或主控台的 Application history (應用程式歷程記錄) 索引標籤連結到 Spark 歷程記錄伺服器 UI，而不需要透過 SSH 連線設定 Web Proxy。從主控台存取 Spark 歷程記錄伺服器 UI 具有以下優點：

- 您可以檢視 Spark 執行歷程記錄的詳細資訊並存取相關日誌檔案，藉此針對使用中的任務和任務歷程記錄快速進行分析和疑難排解。

- 即使叢集終止後，您仍可存取 Spark 歷程記錄並進行偵錯。這些日誌適用於使用中的叢集，且會在叢集終止後保留 30 天。

若是使用叢集的私有子網路，則您務必要在私有子網路的 Amazon S3 政策資源清單中加入 "`arn:aws:s3:::prod.MyRegion.appinfo.src/*`"。如需詳細資訊，請參閱[私有子網路的 Amazon S3 政策下限](#)。

若要從 Spark 歷程記錄伺服器 UI 存取 YARN 容器日誌，您必須啟用叢集的 Amazon S3 記錄功能。如需詳細資訊，請參閱[設定叢集記錄和偵錯](#)。

事件日誌收集

Amazon EMR 會將 Spark 事件日誌收集到 EMR 系統儲存貯體，以便使用者從主控台存取 Spark 歷程記錄伺服器 UI。事件日誌的靜態加密是使用伺服器端的加密搭配 Amazon S3 受管金鑰 (SSE-S3)。如果基於隱私考量而需要停用此功能，您可以在建立叢集時使用引導指令碼來停止協助程式，如下列範例所示。

```
aws emr create-cluster --name "Stop SparkUI Support" --release-label emr-5.28.0
--applications Name=Hadoop Name=Spark --ec2-attributes KeyName=keyname
--instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m3.xlarge
  InstanceGroupType=CORE,InstanceCount=1,InstanceType=m3.xlarge
  InstanceGroupType=TASK,InstanceCount=1,InstanceType=m3.xlarge
--use-default-roles --bootstrap-actions Path=s3://elasticmapreduce/bootstrap-actions/
run-if,Args=[ "instance.isMaster=true","echo Stop Spark UI | sudo tee /etc/apppusher/run-
apppusher" ]
```

執行此引導指令碼後，Amazon EMR 不會將任何 Spark 事件日誌收集到 EMR 系統儲存貯體。Application history (應用程式歷程記錄) 索引標籤不會顯示任何應用程式歷程記錄資訊，而且您將無法從主控台存取 Spark 歷程記錄伺服器 UI。

考量事項與限制

這項功能目前具有下列限制：

- 從主控台存取 Spark 歷程記錄伺服器 UI 目前不適用於具有多個主節點的 EMR 叢集，或與 AWS Lake Formation 整合的 EMR 叢集。
- 若要從主控台存取 Spark 歷程記錄伺服器 UI，您必須具備 EMR 的 ListSteps 動作權限。如果您拒絕 IAM 委託人對此動作的權限，大約需要五分鐘來傳播權限變更。
- 如果您在正在執行的叢集中重新設定 Spark 應用程式，將無法透過 Spark 歷程記錄伺服器 UI 取得應用程式歷程記錄。
- 針對每個 AWS 帳戶，使用中 Spark 歷程記錄伺服器 UI 的數量不得超過 50 個。
- 在美國東部 (維吉尼亞北部和俄亥俄)、美國西部 (加利佛尼亞北部和奧勒岡)、加拿大 (中部)、歐洲 (法蘭克福、愛爾蘭和倫敦) 以及亞太區域 (孟買、首爾、新加坡、雪梨和東京) 等區域，您可以從主控台存取 Spark 歷程記錄伺服器 UI。

透過 Spark 歷程記錄伺服器 UI 存取應用程式歷程記錄

在 Application history (應用程式歷程記錄) 索引標籤或 Amazon EMR 主控台之叢集的叢集 Summary (摘要) 頁面上，選擇 Spark history server UI (Spark 歷程記錄伺服器 UI) 連結。

[Summary](#) [Application history](#) [Monitoring](#) [Hardware](#) [Configurations](#) [Events](#) [Steps](#) [Bootstrap actions](#)

Amazon EMR collects information from YARN applications on your cluster and keeps historical information after applications have completed.

Spark history server UI



Use the Spark history server UI to view scheduler stages and tasks, RDD sizes and memory usage, environmental information and information about the running executors. Available on running clusters or for up to 30 days for terminated clusters. [Learn more](#)

Spark history server UI (SSH tunneling not required)

Spark 歷程記錄伺服器 UI 會在新的瀏覽器分頁中開啟。如果您是透過 SSH 連線設定 Web Proxy，此 Web 界面會顯示與開放原始碼 Spark 歷程記錄伺服器 UI 相同的資訊。如需詳細資訊，請參閱[監控和檢測](#)。

您可以透過 Spark 歷程記錄伺服器 UI 上的連結檢視 YARN 容器日誌。

Note

若要從 Spark 歷程記錄伺服器 UI 存取 YARN 容器日誌，您必須啟用叢集的 Amazon S3 記錄功能。若未啟用日誌功能，則無法使用 YARN 容器日誌的連結。

檢視應用程式歷程記錄摘要

透過 Amazon EMR 5.8.0 版和更新版本，您可以從 Amazon EMR 主控台的 Application history (應用程式歷程記錄) 索引標籤檢視應用程式歷程記錄摘要。在應用程式完成後，Amazon EMR 會將應用程式歷程記錄摘要保留七天。

以下步驟示範如何使用叢集詳細資訊頁面上的 Application history (應用程式歷程記錄)，深入探索 Spark 或 YARN 應用程式的任務詳細資訊。若要檢視叢集詳細資訊，請從 Clusters (叢集) 清單選取叢集 Name (名稱)。若要檢視 YARN 容器日誌的相關資訊，您必須啟用叢集的日誌功能。如需詳細資訊，請參閱[設定叢集記錄和偵錯](#)。針對 Spark 應用程式歷程記錄，摘要表格提供的資訊僅為透過 Spark 歷程記錄伺服器 UI 取得的資訊子集。

在下列 Application history (應用程式歷程記錄) 索引標籤範例中，展開的兩列顯示了兩個不同 Spark 應用程式的診斷摘要資訊，而 Application ID (應用程式 ID) 已選取，可檢視進一步的應用程式詳細資訊。

Application ID	Type	Action	Status	Start time (UTC-7)	Duration	Finish time (UTC-7)	User
application_1505786029486_0006	Spark	spark-wordcount.py	Failed	2017-09-18 18:58 (UTC-7)	22 s	2017-09-18 18:58 (UTC-7)	hadoop
application_1505786029486_0005	Spark	spark-wordcount.py	Failed	2017-09-18 18:57 (UTC-7)	23 s	2017-09-18 18:58 (UTC-7)	hadoop
application_1505786029486_0004	Spark	spark-wordcount.py	Failed	2017-09-18 18:57 (UTC-7)	22 s	2017-09-18 18:57 (UTC-7)	hadoop
application_1505786029486_0002	Spark	spark-wordcount.py	Failed	2017-09-18 18:57 (UTC-7)	23 s	2017-09-18 18:57 (UTC-7)	hadoop
Diagnostics: User application exited with status 1							
application_1505786029486_0001	Spark	spark-wordcount.py	Succeeded	2017-09-18 18:56 (UTC-7)	29 s	2017-09-18 18:57 (UTC-7)	hadoop
Diagnostics: Succeeded							

在 YARN application (YARN 應用程式) 的 Jobs (任務) 索引標籤中，選取「Job 0」(任務 0) 的「Description」(敘述)，以查看任務 0 的詳細資訊：

Job ID	Status	Description	Submitted (UTC-7)	Duration	Stages succeeded / total	Tasks succeeded / total
0	Succeeded	saveAsTextFile at NativeMethodAccessorsImpl.java:0	2017-09-18 18:57 (UTC-7)	15 s	2 / 2	4 / 4

在 Job 0 (任務 0) 的詳細資訊頁面，展開了個別任務階段的資訊，而 Stage 1 (階段 1) 的「Description」(敘述) 已選取，可查看階段 1 的詳細資訊。

Cluster: Holmes **Waiting** Cluster ready after last step failed.

Summary Application history Monitoring Hardware Events Steps Configurations Bootstrap actions

Application history > application_1505786029486_0001 (Spark) C

Jobs Stages Executors

Jobs > Job 0

Status: Succeeded

Completed stages: 2

Stages (2)

Stage ID	Status	Description	Submitted (UTC-7)	Duration	Tasks succeeded / total	Input	Output	Shuffle read	Shuffle write
1	Complete	saveAsTextFile at NativeMethodAccessormpl.java:0	2017-09-18 18:57 (UTC-7)	0.5 s	2 / 2	1.4 kB	2.0 kB		

0 Complete reduceByKey at spark-wordcount.py:10 2017-09-18 18:57 (UTC-7) 6 s 2 / 2 1.6 kB 2.0 kB

在 Stage 1 (階段 1) 詳細資訊頁面，可看見階段任務和執行器的重要指標，也可以透過各個連結檢視任務和執行器的記錄。

Summary Application history Monitoring Hardware Events Steps Configurations Bootstrap actions

Application history > application_1505786029486_0001 (Spark) C

Jobs Stages Executors

Jobs > Job 0 > Stage 1 (attempt 0)

Total time across all tasks: 0.7 s

Locality level summary: Node local: 2

Output (size / records): 1.4 kB / 101

Shuffle read (size / records): 2.0 kB / 12

Summary metrics for 2 completed tasks

Metric	Min	25th percentile	Median	75th percentile	Max
Duration	0.4 s	0.4 s	0.4 s	0.4 s	0.4 s
GC time	8 ms	8 ms	8 ms	8 ms	8 ms
Output (size / records)	680.0 B / 46	680.0 B / 46	779.0 B / 55	779.0 B / 55	779.0 B / 55
Result serialization time	1 ms	1 ms	1 ms	1 ms	1 ms
Shuffle read (size / records)	914.0 B / 6	914.0 B / 6	1.1 kB / 6	1.1 kB / 6	1.1 kB / 6
Shuffle remote reads	0.0 B	0.0 B	0.0 B	0.0 B	0.0 B
Task deserialization time	64 ms	64 ms	65 ms	65 ms	65 ms

Aggregated metrics by executor (1)

Executor ID	Address	Task time	Total tasks	Failed tasks	Succeeded tasks	Output	Shuffle read	Blacklisted
1	ip-10-218-185-134.ec2.internal:34689	0.9 s	4	0	2	1.4 kB	2.0 kB	

Tasks (2)

ID	Attempt	Status	Locality level	Executor ID / Host	Launch time (UTC-7)	Duration	Task deserialization time	GC time	Result serialization time	Output size /records	Shuffle read size /records	Shuffle remote reads	Errors
2	0	Succeeded	Node local	1 / ip-10-218-185-134.ec2.internal	2017-09-18 18:57 (UTC-7)	0.4 s	64 ms	8 ms	1 ms	779.0 B / 55	1.1 kB / 6	0.0 B	
3	0	Succeeded	Node local	1 / ip-10-218-185-134.ec2.internal	2017-09-18 18:57 (UTC-7)	0.4 s	65 ms	8 ms	1 ms	680.0 B / 46	914.0 B / 6	0.0 B	

檢視日誌檔

Amazon EMR 和 Hadoop 都會產生回報叢集狀態的日誌檔。根據預設，這些狀態會寫入主節點的 /mnt/var/log/ 目錄中。根據您設定叢集的方式而定，當您啟動叢集，這些日誌也可能會封存至 Amazon S3，並且可透過圖形偵錯工具檢視。

寫入主節點的日誌類型有許多種。Amazon EMR 會撰寫步驟、引導操作和執行個體狀態日誌。Apache Hadoop 會撰寫日誌來回報任務、任務和任務嘗試的處理情形。Hadoop 也會記錄其協助程式的日誌。如需 Hadoop 所撰寫日誌的詳細資訊，請前往 <http://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-common/ClusterSetup.html>。

主題

- [檢視主節點上的日誌檔 \(p. 251\)](#)

- 檢視封存到 Amazon S3 的日誌檔 (p. 252)
- 在除錯工具中檢視日誌檔 (p. 253)

檢視主節點上的日誌檔

下表列出可在主節點上找到的一些日誌檔。

位置	描述
/mnt/var/log/bootstrap-actions	在處理引導操作期間撰寫的日誌。
/mnt/var/log/hadoop-state-pusher	Hadoop 狀態推送器程序撰寫的日誌。
/mnt/var/log/instance-controller (Amazon EMR 4.6.0 和舊版)	執行個體控制器日誌。
/emr/instance-controller (Amazon EMR 4.7.0 和更新版本)	
/mnt/var/log/instance-state	執行個體狀態日誌。這些日誌包含有關節點的 CPU、記憶體狀態和廢棄項目收集器執行緒的資訊。
/mnt/var/log/service-nanny (Amazon EMR 4.6.0 和舊版)	service nanny 程序撰寫的日誌。
/emr/service-nanny (Amazon EMR 4.7.0 和更新版本)	
/mnt/var/log/ <i>application</i>	應用程式專屬日誌，例如 Hadoop、Spark 或 Hive。
/mnt/var/log/hadoop/steps/ <i>N</i>	步驟日誌，包含處理步驟的相關資訊。 <i>N</i> 的值表示 Amazon EMR 指派的 stepId。例如，叢集有兩個步驟：s-1234ABCDEFGH 和 s-5678IJKLMNOP。第一個步驟位於 /mnt/var/log/hadoop/steps/s-1234ABCDEFGH/ 中，第二個步驟位於 /mnt/var/log/hadoop/steps/s-5678IJKLMNOP/ 中。 Amazon EMR 寫入的步驟日誌如下。 <ul style="list-style-type: none">controller — 處理步驟的相關資訊。如果您的步驟在載入時失敗，可以在這個日誌中找到堆疊追蹤。syslog — 描述步驟中 Hadoop 工作的執行。stderr — Hadoop 處理步驟時的標準錯誤通道。stdout — Hadoop 處理步驟時的標準輸出通道。

檢視主節點上的日誌檔

1. 使用 SSH 連接到主節點，如 [使用 SSH 連接至主節點 \(p. 277\)](#) 中所述。
2. 導覽至包含您要檢視的日誌檔資訊的目錄。上表提供可用的日誌檔類型清單，以及這些日誌檔的所在位置。以下範例說明導覽至 ID 為 s-1234ABCDEFGH 之步驟日誌的命令。

```
cd /mnt/var/log/hadoop/steps/s-1234ABCDEFGH/
```

3. 使用您選擇的檔案檢視器來檢視日誌檔。以下範例使用 Linux less 命令來檢視 controller 日誌檔。

```
less controller
```

檢視封存到 Amazon S3 的日誌檔

根據預設，使用主控台啟動的 Amazon EMR 叢集會自動將日誌檔封存到 Amazon S3。您可以指定自己的日誌路徑，也可以讓主控台自動產生日誌路徑。若是使用 CLI 或 API 啟動叢集，您必須手動設定 Amazon S3 日誌封存。

當 Amazon EMR 設定為將日誌檔封存到 Amazon S3，會將檔案存放到 S3 中您所指定的位置，位於 */JobFlowId/* 資料夾，其中 *JobFlowId* 是叢集識別符。

下表列出可在 Amazon S3 上找到的一些日誌檔。

位置	敘述
<i>/JobFlowId/node/</i>	節點日誌，包括節點的引導操作、執行個體狀態和應用程式日誌。每個節點的日誌都會存放在以該節點的 EC2 執行個體識別符標示的資料夾中。
<i>/JobFlowId/node/instanceId/application</i>	每個應用程式或與應用程式相關聯的協助程式所建立的日誌。例如，Hive 伺服器日誌位於 <i>JobFlowId/node/instanceId/hive/hive-server.log</i> 。
<i>/JobFlowId/steps/N/</i>	步驟日誌，包含處理步驟的相關資訊。 <i>N</i> 的值表示 Amazon EMR 指派的 stepId。例如，叢集有兩個步驟： <i>s-1234ABCDEFGH</i> 和 <i>s-5678IJKLMNOP</i> 。第一個步驟位於 <i>/mnt/var/log/hadoop/steps/s-1234ABCDEFGH/</i> 中，第二個步驟位於 <i>/mnt/var/log/hadoop/steps/s-5678IJKLMNOP/</i> 中。 Amazon EMR 寫入的步驟日誌如下。 <ul style="list-style-type: none">controller — 處理步驟的相關資訊。如果您的步驟在載入時失敗，可以在這個日誌中找到堆疊追蹤。syslog — 描述步驟中 Hadoop 工作的執行。stderr — Hadoop 處理步驟時的標準錯誤通道。stdout — Hadoop 處理步驟時的標準輸出通道。
<i>/JobFlowId/containers</i>	應用程式容器日誌。每個 YARN 應用程式的日誌都會存放在這些位置。

使用主控台檢視封存至 Amazon S3 的日誌檔

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. 當您設定叢集將日誌檔封存在 Amazon S3 中時，開啟指定的 S3 儲存貯體。

3. 導覽至包含所要顯示資訊的日誌檔。上表提供可用的日誌檔類型清單，以及這些日誌檔的所在位置。
4. 按兩下日誌檔，即可在瀏覽器中檢視日誌檔。

如果您不想在 Amazon S3 主控台中檢視日誌檔，可使用 Firefox Web 瀏覽器的 Amazon S3 Organizer 外掛程式這類工具，從 Amazon S3 將檔案下載到您的本機機器上，或撰寫應用程式以從 Amazon S3 摘取物件。如需詳細資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的[取得物件](#)。

在除錯工具中檢視日誌檔

Amazon EMR 不會自動啟用除錯工具。您必須在啟動叢集時設定。

使用主控台檢視叢集日誌

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 從 Cluster List (叢集清單) 頁面選擇欲檢視叢集旁的詳細資訊圖示。

您會前往 Cluster Details (叢集詳細資訊) 頁面。在 Steps (步驟) 部分，各步驟右側的連結會顯示步驟可用的各種日誌類型。這些步驟是由 Amazon EMR 產生。

3. 要檢視與特定步驟關聯的 Hadoop 工作清單，請選擇步驟右側的 View Jobs (檢視工作) 連結。
4. 要檢視與特定工作關聯的 Hadoop 任務清單，請選擇工作右側的 View Tasks (檢視任務) 連結。

Job	State	Start time local time (UTC-8)	Actions
job_201311042101_0001	COMPLETED	2013-11-04 13:03:21	View tasks

5. 要檢視特定任務試圖完成工作而執行的嘗試清單，請選擇任務右側的 View Attempts (檢視嘗試) 連結。

Task	Type	State	Start time local time (UTC-8)	Actions
r_000002	reduce	COMPLETED	2013-11-04 13:05:26	View attempts
r_000001	reduce	COMPLETED	2013-11-04 13:04:17	View attempts
r_000000	reduce	COMPLETED	2013-11-04 13:04:15	View attempts
m_000012	map	COMPLETED	2013-11-04 13:05:08	View attempts

6. 要檢視任務嘗試所產生的日誌，請選擇任務嘗試右側的 stderr、stdout 和 syslog 連結。

Attempt	Type	State	Log files
0	reduce	SUCCEEDED	controller* syslog stderr stdout

在 Amazon EMR 將日誌檔上傳至您於 Amazon S3 的儲存貯體後，除錯工具就會顯示日誌檔的連結。由於日誌檔每 5 分鐘就會上傳到 Amazon S3 一次，因此步驟完成後，可能還需要幾分鐘時間日誌檔上傳才會完成。

Amazon EMR 會定期更新除錯工具中 Hadoop 任務、任務和任務嘗試的狀態。您可以按一下除錯窗格中的 Refresh List (重新整理清單)，以取得這些項目的最新狀態。

檢視 Amazon EC2 中的叢集執行個體

為了協助資源的管理，Amazon EC2 允許您以標籤的形式為資源指派中繼資料。各個 Amazon EC2 標籤均是由金鑰與值所組成。標籤可讓您以不同的方式分類您的 Amazon EC2 資源：例如可依據目的、擁有者或環境來分類。

您可以根據標籤來搜尋和篩選資源。使用您的 AWS 帳戶指派的標籤僅供您使用。其他共用資源的帳戶並無法查看您的標籤。

Amazon EMR 會在啟用 EC2 執行個體時，以金鑰值對自動為各個 EC2 執行個體加上標籤，可用於識別執行個體所屬的叢集和執行個體群組。如此即可輕鬆地篩選要顯示的 EC2 執行個體，例如僅顯示屬於特定叢集的執行個體，或是顯示目前任務執行個體群組中執行的所有執行個體。若您同時執行多個叢集，或是要管理大量的 EC2 執行個體，這個功能就格外有用。

以下為 Amazon EMR 指派的預先定義好的金鑰值對：

金鑰	數值
aws:elasticmapreduce:job-flow-id	<job-flow-identifier>
aws:elasticmapreduce:instance-group-role	<group-role>

這類值可按下列方式進一步定義：

- <job-flow-identifier> 為佈建執行個體的叢集 ID。會以 j-XXXXXXXXXXXXXX 格式顯示。
- <group-role> 是下列其中一種值：master、core 或 task。上述幾個值分別對應至主要執行個體群組、核心執行個體群組和任務執行個體群組。

您可以檢視和篩選 Amazon EMR 所加的標籤。如需詳細資訊，請參閱 [Amazon EC2 User Guide for Linux Instances](#) 中的 [使用標籤](#)。由於 Amazon EMR 所設的標為系統標籤，無法編輯或刪除，顯示和篩選標籤的區段是最為重要的。

Note

Amazon EMR 會在 EC2 執行個體狀態更新為執行中的時候，為 EC2 執行個體加上標籤。若 EC2 執行個體的佈建時間和狀態設為執行中的時間有所落差，Amazon EMR 所設的標籤會等到執行個體開始執行後才會顯示。若看不標籤，請稍待幾分鐘並重新整理畫面。

CloudWatch 事件與指標

您可以使用事件和指標以追蹤 Amazon EMR 叢集的活動和運作狀態，在 Amazon EMR 主控台快速為單一叢集檢視事件和指標，以及在區域中為所有叢集檢視事件。當 Amazon EMR 產生符合您指定模式的事件，您可以使用 CloudWatch Events 定義欲採取的動作，也可以使用 CloudWatch 監控指標。

活動有助於監控叢集中特定發生事件—例如，當叢集開始執行時變更狀態。指標有助於監控特定的數值—例如，HDFS 在叢集中所使用的可用磁碟空間百分比。

如需 CloudWatch Events 的詳細資訊，請參閱 [Amazon CloudWatch Events User Guide](#)。如需 CloudWatch 指標的詳細資訊，請參閱 [Amazon CloudWatch User Guide](#) 中的 [使用 Amazon CloudWatch 指標](#) 和 [建立 Amazon CloudWatch 訊息](#)。

主題

- [監控 CloudWatch Events \(p. 255\)](#)
- [使用 CloudWatch 監控指標 \(p. 262\)](#)

監控 CloudWatch Events

Amazon EMR 會追蹤事件，並保留相關資料，而保留時間最多為七天。在叢集狀態、執行個體群組、自動擴展政策和步驟變更時，會造成被記錄的事件。每個事件的資訊，如事件發生的日期和時間，以及有關事件進一步的詳細資訊，例如受到影響的叢集或執行個體群組。

下表會列出 Amazon EMR 事件，以及該事件的狀態或狀態變更、該事件嚴重性以及事件訊息。每個事件表示做為自動傳送到事件串流的 JSON 物件。JSON 物件包含有關該事件進一步的詳細資訊。當您使用 CloudWatch Events 為事件處理設定規則時，JSON 物件尤其重要，因為規則要試圖符合 JSON 物件中的模式。如需詳細資訊，請參閱 Amazon CloudWatch Events User Guide 中的[事件和事件模式](#)和 [Amazon EMR 事件](#)。

叢集事件

狀態或狀態變更	嚴重性	訊息
STARTING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 是在 <i>Time</i> 請求並建立。
STARTING	INFO	<p>Note</p> <p>僅適用於具有 VPC 內部選擇的執行個體機群組態和多個子網路的叢集。</p> <p>Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 是在可用區域 (<i>AvailabilityZoneID</i>) 之 VPC (<i>VPCName</i>) 中的子網路 (<i>SubnetName</i>) 建立，並從指定 VPC 選項中選擇。</p>
STARTING	INFO	<p>Note</p> <p>僅適用於具有 EC2-Classic 內部選擇的執行個體機群組態和多個可用區域的叢集。</p> <p>Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 是在可用區域 (<i>AvailabilityZoneID</i>) 中建立，並從指定可用區域選項中選擇。</p>
RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 開始在 <i>Time</i> 執行步驟。
WAITING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 是在 <i>Time</i> 建立並可供使用。

狀態或狀態變更	嚴重性	訊息
		<p>—或—</p> <p>Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 已在 <i>Time</i> 完成執行所有待定步驟。</p> <p>Note</p> <p>處於 WAITING 狀態的叢集可能仍在處理任務。</p>
TERMINATED	<p>嚴重程度依狀態更改原因而定，如下所示：</p> <ul style="list-style-type: none"> CRITICAL 若該叢集因以下任何狀態變更原因而終止：INTERNAL_ERROR、VALIDATION_ERROR、INSTANCE_FAILURE、BOOTSTRAP_FAILURE 或 STEP_FAILURE。 INFO 若該叢集因以下任何狀態變更原因而終止：USER_REQUEST 或 ALL_STEPS_COMPLETED。 	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 已在 <i>Time</i> 因為 <i>StateChangeReason:Code</i> 而終止。
TERMINATED_WITH_ERRORS	CRITICAL	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 已在 <i>Time</i> 因為 <i>StateChangeReason:Code</i> 導致錯誤而終止。

執行個體機群事件

Note

執行個體佇列組態只能在 Amazon EMR 發行版本 4.8.0 及更新版本中使用，不含 5.0.0 及 5.0.3。

狀態或狀態變更	嚴重性	訊息
從 PROVISIONING 到 WAITING	INFO	<p>於 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 佈建已完成。佈建於 <i>Time</i> 開始並花費 <i>Num</i> 分鐘。執行個體機群現在有 <i>Num</i> 的隨需容量和 <i>Num</i> 的 Spot 容量。目標隨需容量為 <i>Num</i>，而目標 Spot 容量為 <i>Num</i>。</p>
從 WAITING 到 RESIZING	INFO	<p>Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的 <i>InstanceFleetID</i> 執行個體機群的規模調整在 <i>Time</i> 開始。執行個體機群正在從 <i>Num</i> 的隨需容量重新調整為 <i>Num</i> 的目標，並從 <i>Num</i> 的 Spot 容量調整為 <i>Num</i> 的目標。</p>

狀態或狀態變更	嚴重性	訊息
從 RESIZING 到 WAITING	INFO	於 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 規模調整操作已完成。規模調整於 <i>Time</i> 開始並花費 <i>Num</i> 分鐘。執行個體機群現在有 <i>Num</i> 的隨需容量和 <i>Num</i> 的 Spot 容量。目標隨需容量為 <i>Num</i> 而目標 Spot 容量為 <i>Num</i> 。
從 RESIZING 到 WAITING	WARN	於 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 規模調整操作已逾時且停止。規模調整於 <i>Time</i> 開始並於 <i>Num</i> 分鐘後停止。執行個體機群現在有 <i>Num</i> 的隨需容量和 <i>Num</i> 的 Spot 容量。目標隨需容量為 <i>Num</i> 而目標 Spot 容量為 <i>Num</i> 。
ARRESTED	ERROR	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 在 <i>Time</i> 遭阻擋，原因如下： <i>ReasonDesc</i> 。
RESIZING	WARNING	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 規模調整操作由於以下原因遭凍結： <i>ReasonDesc</i> 。
WAITING 或 RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體機群 <i>InstanceFleetID</i> 規模調整已由 <i>Entity</i> 在 <i>Time</i> 啟動。

執行個體群組事件

狀態或狀態變更	嚴重性	訊息
從 RESIZING 到 RUNNING	INFO	於 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 的執行個體群組 <i>InstanceGroupID</i> 規模調整操作已完成。這現在有 <i>Num</i> 的執行個體計數。規模調整於 <i>Time</i> 開始並花費 <i>Num</i> 分鐘完成。
從 RUNNING 到 RESIZING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> 規模調

狀態或狀態變更	嚴重性	訊息
		整於 <i>Time</i> 開始。這是從執行個體計數 <i>Num</i> 到 <i>Num</i> 來調整規模。
ARRESTED	ERROR	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> 在 <i>Time</i> 遭阻擋，原因如下： <i>ReasonDesc</i> 。
RESIZING	WARNING	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> 規模調整操作由於以下原因遭到凍結： <i>ReasonDesc</i> 。
WAITING 或 RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> 規模調整已由 <i>Entity</i> 於 <i>Time</i> 啟動。

Note

對於 Amazon EMR 5.21.0 版和更新版本，您可以覆寫叢集組態，並且為執行中叢集的每個執行個體群組，指定額外組態分類。您可以使用 Amazon EMR 主控台、AWS Command Line Interface (AWS CLI) 或 AWS 開發套件來這樣做。如需詳細資訊，請參閱[為執行中叢集的執行個體群組提供組態](#)。

下表會列出重新設定操作的 Amazon EMR 事件，以及該事件的狀態或狀態變更、該事件嚴重性以及事件訊息。

狀態或狀態變更	嚴重性	訊息
RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupID</i> 的重新設定是由使用者於 <i>Time</i> 起啟。要求的組態版本是 <i>Num</i> 。
從 RECONFIGURING 到 RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupID</i> 的重新設定操作已完成。重新設定於 <i>Time</i> 開始並花費 <i>Num</i> 分鐘完成。目前的組態版本為 <i>Num</i> 。
從 RUNNING 到 RECONFIGURING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupID</i> 的重新設定於 <i>Time</i> 開始。這將版本編號從 <i>Num</i> 設定為版本編號 <i>Num</i> 。
RESIZING	INFO	將 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupID</i> 重新設定為組態版本 <i>Num</i> 的操作於 <i>Time</i> 暫

狀態或狀態變更	嚴重性	訊息
		時封鎖，因為執行個體群組處於 <i>State</i> 。
RECONFIGURING	INFO	將 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupId</i> 大小重新調整為執行個體計數 <i>Num</i> 的操作於 <i>Time</i> 暫時封鎖，因為執行個體群組處於 <i>State</i> 。
RECONFIGURING	WARNING	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupId</i> 的重新設定操作於 <i>Time</i> 失敗，並經歷了 <i>Num</i> 分鐘而失敗。失敗的組態版本為 <i>Num</i> 。
RECONFIGURING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupId</i> 的組態會於 <i>Time</i> 還原為先前的成功版本號碼 <i>Num</i> 。新的組態版本為 <i>Num</i> 。
從 RECONFIGURING 到 RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupId</i> 的組態已經於 <i>Time</i> 成功還原為先前的成功版本 <i>Num</i> 。新的組態版本為 <i>Num</i> 。
從 RECONFIGURING 到 ARRESTED	CRITICAL	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中執行個體群組 <i>InstanceGroupId</i> 無法於 <i>Time</i> 還原為先前的成功版本 <i>Num</i> 。

自動調整規模政策事件

狀態或狀態變更	嚴重性	訊息
PENDING	INFO	Auto Scaling 政策已在 <i>Time</i> 新增到 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupId</i> 。該政策正在等待附件。 —或— Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupId</i> Auto Scaling 政策，已於 <i>Time</i> 更新。該政策正在等待附件。

狀態或狀態變更	嚴重性	訊息
ATTACHED	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> Auto Scaling 政策，已於 <i>Time</i> 連接。
DETACHED	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> Auto Scaling 政策，已於 <i>Time</i> 分離。
FAILED	ERROR	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> Auto Scaling 政策無法連接，已於 <i>Time</i> 失敗。 —或— Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的執行個體群組 <i>InstanceGroupID</i> Auto Scaling 政策無法分離，已於 <i>Time</i> 失敗。

步驟事件

狀態或狀態變更	嚴重性	訊息
PENDING	INFO	步驟 <i>StepID</i> (<i>StepName</i>) 已在 <i>Time</i> 新增到 Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>)，且正在等待執行。
CANCEL_PENDING	WARN	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的步驟 <i>StepID</i> (<i>StepName</i>) 已在 <i>Time</i> 取消，且正在等待取消。
RUNNING	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的步驟 <i>StepID</i> (<i>StepName</i>) 已在 <i>Time</i> 開始執行。
COMPLETED	INFO	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的步驟 <i>StepID</i> (<i>StepName</i>) 已在 <i>Time</i> 完成執行。步驟於 <i>Time</i> 開始執行並花費 <i>Num</i> 分鐘完成。
CANCELLED	WARN	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的叢集步驟 <i>StepID</i> (<i>StepName</i>) 的取消請求已在 <i>Time</i> 成功，該步驟現已取消。

狀態或狀態變更	嚴重性	訊息
FAILED	ERROR	Amazon EMR 叢集 <i>ClusterId</i> (<i>ClusterName</i>) 中的步驟 <i>StepID</i> (<i>StepName</i>) 已在 <i>Time</i> 失敗。

使用 Amazon EMR 主控台檢視事件

對於每個叢集，您可以在詳細資訊窗格中查看簡單的事件清單，該清單以遞減順序列出出現的事件。您也可以以遞減順序檢視區域中全部叢集所出現的所有事件。

Note

如果您不希望使用者查看區域的所有叢集事件，請為 "Effect": "Deny" 動作新增拒絕許可 (elasticmapreduce:ViewEventsFromAllClustersInConsole) 描述到連接至使用者的政策。

在區域中查看所有叢集事件

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Events (事件)。

查看特定叢集事件

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Cluster List (叢集清單)，選取一個叢集，然後選擇 View details (查看詳細資訊)。
3. 在叢集詳細資訊窗格中選擇 Events (事件)。

The screenshot shows the Amazon EMR console interface. On the left, there's a navigation sidebar with options like 'Cluster List', 'Security configurations', 'VPC subnets', and 'Help'. The main area is titled 'Cluster: JeffGoliAutoScale' and shows 'Waiting' status. It includes sections for 'Connections', 'Summary' (with cluster ID, creation date, and termination protection), 'Configuration Details' (with release label, distribution, and applications), 'Network and Hardware' (with subnet ID, master and core instance counts, and task count), and 'Security and Access' (with key name, EC2 instance profile, EMR role, auto scaling role, and security group information). At the bottom of the main area, there are tabs for 'Monitoring', 'Hardware', 'Steps', 'Configurations', and 'Events'. The 'Events' tab is highlighted with a red box. Below it, a table lists two events:

Time	Event Description	Resource ID	Resource Type	Event Type	Severity	Full Date & Time
Dec 14 02:15 PM	The resize for your Amazon EMR cluster j-3CHYFADDOE0DM (JeffGoliAutoScale) is complete and instance group ip-140CC09M5A2T1Z has an active instance count of 1. The resize was initiated at 2016-12-14 20:34 UTC and took 101 minutes to complete.	ip-140CC09M5A2T1Z	Instance Group	Instance Group State Change	info	December 14, 2016 at 02:15:55 PM (UTC-8)
Dec 14 12:35 PM	A resize for your Amazon EMR cluster j-3CHYFADDOE0DM (JeffGoliAutoScale) was started at 2016-12-14 20:34 UTC. Instance group ip-140CC09M5A2T1Z RESIZING from instance count of 2 to 1.	ip-140CC09M5A2T1Z	Instance Group	Instance Group State Change	info	December 14, 2016 at 12:35:17 PM (UTC-8)

使用 CloudWatch 為 Amazon EMR 事件建立規則

Amazon EMR 會自動將事件傳送至 CloudWatch 事件串流。您可以根據指定模式建立符合事件的規則，並轉傳該事件至目標以採取動作，例如傳送一封電子郵件通知。模式與事件 JSON 物件相符合。如需 Amazon EMR 事件詳細資訊，請參閱 Amazon CloudWatch Events User Guide 中的 [Amazon EMR 事件](#)。

如需設定 CloudWatch 事件規則的詳細資訊，請參閱[建立由事件觸發的 CloudWatch 規則](#)。

使用 CloudWatch 監控指標

指標會每五分鐘更新一次，自動收集並推送到每個 EMR 叢集的 CloudWatch。此間隔無法設定。在 CloudWatch 中報告的 Amazon EMR 指標不需付費。指標將封存兩週，之後便會捨棄資料。

如何使用 Amazon EMR 指標？

Amazon EMR 回報的指標可提供資訊，您可透過不同方式加以分析。下表說明一些常見的指標用法。這些是協助您開始的建議，而不是完整清單。如需由 Amazon EMR 回報的完整指標清單，請參閱 [在 CloudWatch 中由 Amazon EMR 報告的指標 \(p. 265\)](#)。

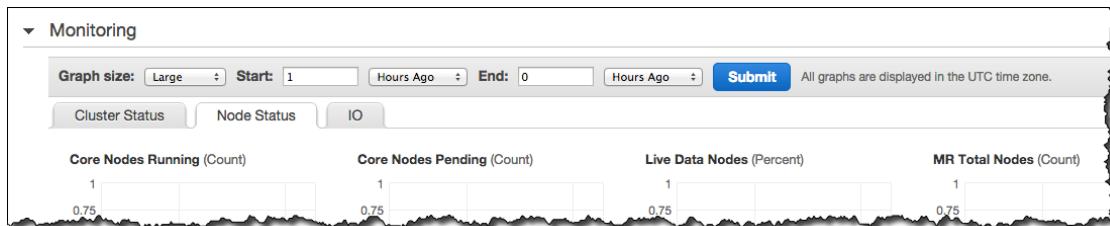
運作方式？	相關指標
追蹤我的叢集進度	查看 RunningMapTasks、RemainingMapTasks、RunningReduceTasks 和 RemainingReduceTasks 指標。
偵測閒置叢集	IsIdle 指標會追蹤叢集是否處於活動狀態，而非目前正在執行的任務。當叢集已閒置一段指定時間（例如 30 分鐘）時，您可以設置警示以將其觸發。
偵測節點何時耗盡儲存空間	HDFSUtilization 指標為目前已使用的磁碟空間百分比。如果這超出了應用程式可接受的水準，例如已使用 80% 的容量，則您可能需要調整叢集規模，並添加更多的核心節點。

存取 CloudWatch 指標

存取 Amazon EMR 推送至 CloudWatch 之指標的方法有很多種。您可以透過 Amazon EMR 主控台或 CloudWatch 主控台檢視，或使用 CloudWatch CLI 或 CloudWatch API 撈取。以下程序旨在說明如何使用這些多種工具來存取指標。

在 Amazon EMR 主控台檢視指標

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 要檢視叢集指標，請選擇一個叢集以顯示 Summary (摘要) 窗格。
3. 選擇 Monitoring (監控) 以檢視該叢集的相關資訊。選擇任何一個名稱為 Cluster Status (叢集狀態)、Map/Reduce (對應/降低)、Node Status (節點狀態)、IO 或 HBase 之索引標籤，以載入叢集的進度和運作狀態報告。
4. 選擇要檢視的指標後，您可以選擇圖表大小。編輯 Start (開始) 和 End (結束) 欄位來篩選特定時間範圍內的指標。



在 CloudWatch 主控台檢視指標

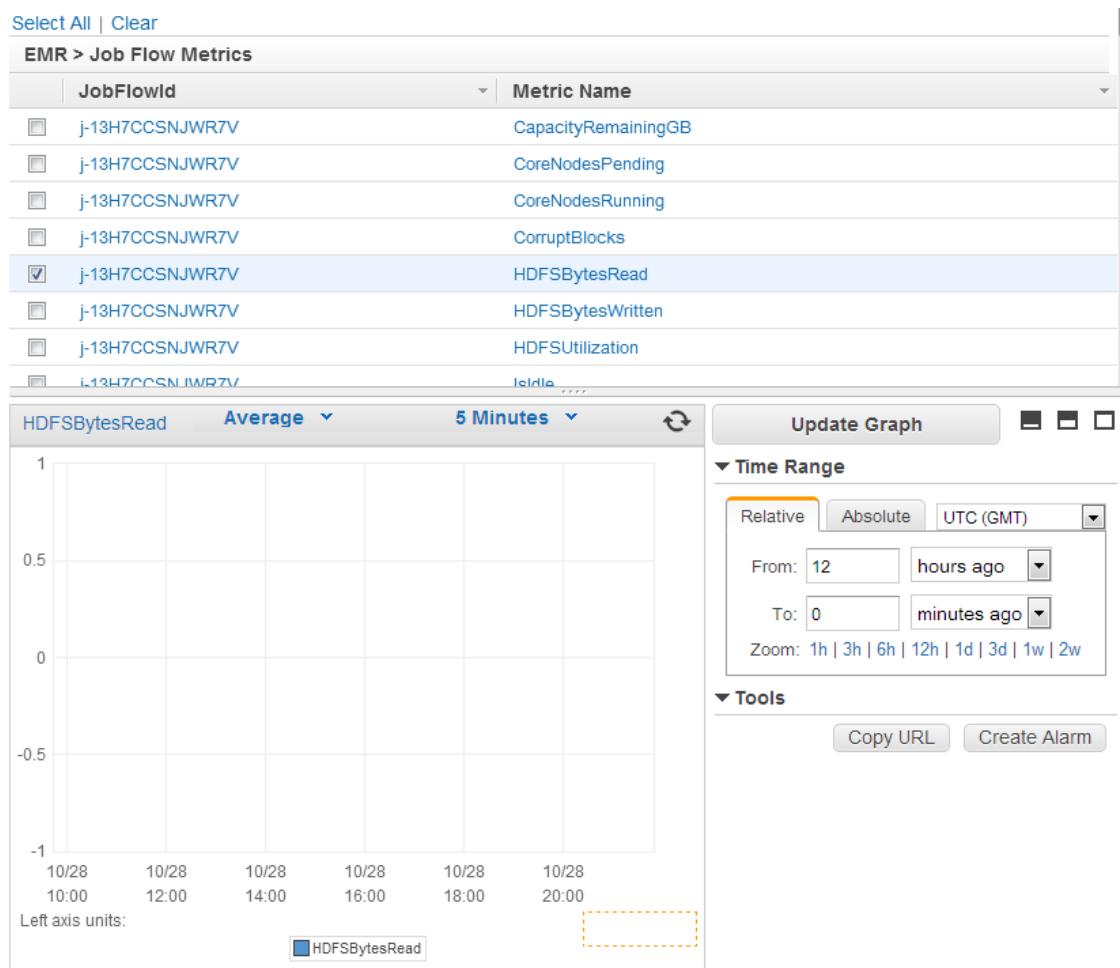
1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. 在導覽窗格中，選擇 EMR (EMR)。
3. 向下捲動到指標以製作圖形。您可以在叢集搜尋叢集識別符以進行監控。

The screenshot shows the CloudWatch Metrics interface. On the left, a navigation pane lists various services: Dashboard, Alarms, ALARM (0), INSUFFICIENT (4), OK (0), Billing, Metrics (selected), Selected Metrics, DynamoDB, EBS, EC2, EMR (selected), RDS, and Redshift. The main area is titled 'EMR Metrics' and displays a list of metrics for a specific job flow. The title bar includes 'Browse Metrics', a search bar, and a close button. A message at the top says 'Showing the first 200 matching metrics. 4 additional metrics not listed for EMR Metrics'. Below this is a 'Select All | Clear' link. The metric list is titled 'EMR > Job Flow Metrics' and has columns for 'JobFlowId' and 'Metric Name'. The data table contains 20 rows of metric names, such as CapacityRemainingGB, CoreNodesPending, CoreNodesRunning, CorruptBlocks, HDFSBytesRead, HDFSBytesWritten, HDFSUtilization, Idle, JobsFailed, JobsRunning, LiveDataNodes, LiveTaskTrackers, MapSlotsOpen, and MissingBlocks.

JobFlowId	Metric Name
j-13H7CCSNJWR7V	CapacityRemainingGB
j-13H7CCSNJWR7V	CoreNodesPending
j-13H7CCSNJWR7V	CoreNodesRunning
j-13H7CCSNJWR7V	CorruptBlocks
j-13H7CCSNJWR7V	HDFSBytesRead
j-13H7CCSNJWR7V	HDFSBytesWritten
j-13H7CCSNJWR7V	HDFSUtilization
j-13H7CCSNJWR7V	Idle
j-13H7CCSNJWR7V	JobsFailed
j-13H7CCSNJWR7V	JobsRunning
j-13H7CCSNJWR7V	LiveDataNodes
j-13H7CCSNJWR7V	LiveTaskTrackers
j-13H7CCSNJWR7V	MapSlotsOpen
i-13H7CCSNJWR7V	MissingBlocks

4. 開啟一個指標以顯示圖形。



從 CloudWatch CLI 存取指標

- 呼叫 `mon-get-stats`。如需詳細資訊，請參閱 [Amazon CloudWatch User Guide](#)。

從 CloudWatch API 存取指標

- 呼叫 `GetMetricStatistics`。如需更多詳細資訊，請參閱 [Amazon CloudWatch API Reference](#)。

在指標上設定警示

Amazon EMR 會推送指標至 CloudWatch，這表示您可以使用 CloudWatch 在您的 Amazon EMR 指標上設定警示。例如，您可以在 CloudWatch 中設定警示，在每當 HDFS 使用率超過 80% 的時候，傳送電子郵件給您。

以下主題給您如何使用 CloudWatch 設定警示的高階概觀。如需詳細說明，請參閱 [Amazon CloudWatch User Guide](#) 中的 [建立或編輯 CloudWatch 警示](#)。

使用 CloudWatch 主控台設定警示

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. 選擇Create Alarm (建立警示)。這會啟動 Create Alarm Wizard (建立警示精靈)。

3. 選擇 EMR Metrics (EMR 指標) 並捲動檢視 Amazon EMR 指標，以找到您要設定警報的指標。要在此對話方塊中僅顯示 Amazon EMR 指標的簡單方法是搜尋叢集的叢集識別符。選取要建立警報的指標，然後選擇 Next (下一步)。
4. 填入指標的 Name (名稱)、Description (描述)、Threshold (閾值) 和 Time (時間) 值。
5. 如果您希望 CloudWatch 在達到警報狀態時傳送電子郵件給您，請在 Whenever this alarm: (每當此警報：) 欄位中選擇 State is ALARM (狀態為警報)。在 Send notification to: (傳送通知至：)，選取現有 SNS 主題。如果您選擇 Create topic (建立主題)，即可為新電子郵件訂閱清單設定名稱和電子郵件地址。此清單會儲存並顯示在欄位中供未來警報使用。

Note

如果您使用 Create topic (建立主題) 來建立新的 Amazon SNS 主題，電子郵件地址必須先經過驗證才會接收通知。電子郵件只有在警報進入警報狀態時才會傳送。如果此警報狀態在驗證電子郵件地址之前發生變更，就不會收到通知。

6. 此時，Define Alarm (定義警報) 畫面會提供您機會檢閱您將建立的警報。選擇 Create Alarm (建立警報)。

Note

如需使用 CloudWatch 主控台設定警報的詳細資訊，請參閱 Amazon CloudWatch User Guide 中的[建立傳送電子郵件的警報](#)。

使用 CloudWatch API 設定警報

- 呼叫 [mon-put-metric-alarm](#)。如需詳細資訊，請參閱 [Amazon CloudWatch User Guide](#)。

使用 CloudWatch API 設定警報

- 呼叫 [PutMetricAlarm](#)。如需更多詳細資訊，請參閱 [Amazon CloudWatch API Reference](#)

在 CloudWatch 中由 Amazon EMR 報告的指標

以下表格列出 Amazon EMR 在主控台報告並推送到 CloudWatch 的指標。

Amazon EMR 個指標

Amazon EMR 為數個指標傳送資料至 CloudWatch。所有 Amazon EMR 叢集將自動以五分鐘間隔傳送指標。指標將封存兩週，之後即會捨棄資料。

AWS/ElasticMapReduce 命名空間包含下列指標。

Note

Amazon EMR 會從 cluster 提取指標。如果 cluster 無法連接，除非 cluster 再次可用，否則不會報告指標。

以下指標可用於執行 Hadoop 2.x 版本的叢集。

指標	描述
叢集狀態	
IsIdle	指出cluster不再執行工作，但仍然存活並產生費用。如果未執行任何任務，而且未執行任何工作，則會設為 1，否則設為 0。此值會以五分鐘的間隔進行檢查，而值 1 指出cluster只在檢查時為閒置，而不是整個五分鐘都閒置。為了避免誤判，此值已為 1 且持

指標	描述
	<p>續多個連續 5 分鐘檢查時，您應該發出警示。例如，如果此值已為 1 且持續 30 分鐘（含）以上，則您可以對此值發出警示。</p> <p>使用案例：監控 cluster 效能</p> <p>單位：布林值</p>
ContainerAllocated	<p>ResourceManager 所配置的資源容器數目。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
ContainerReserved	<p>保留容器數目。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
ContainerPending	<p>佇列中尚未配置的容器數目。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
ContainerPendingRatio	<p>擱置中容器與已配置容器的比率 (ContainerPendingRatio = ContainerPending / ContainerAllocated)。如果 ContainerAllocated = 0，則 ContainerPendingRatio = ContainerPending。ContainerPendingRatio 的值代表數字，而不是百分比。此值適用於根據容器配置行為來調整叢集資源。</p> <p>單位：計數</p>
AppsCompleted	<p>提交給已完成 YARN 的應用程式數目。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
AppsFailed	<p>提交給無法完成之 YARN 的應用程式數目。</p> <p>使用案例：監控 cluster 進度、監控 cluster 運作狀態</p> <p>單位：計數</p>
AppsKilled	<p>提交給已刪除 YARN 的應用程式數目。</p> <p>使用案例：監控 cluster 進度、監控 cluster 運作狀態</p> <p>單位：計數</p>
AppsPending	<p>提交給處於擱置中狀態之 YARN 的應用程式數目。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>

指標	描述
AppsRunning	<p>提交給執行中 YARN 的應用程式數目。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
AppsSubmitted	<p>提交給 YARN 的應用程式數目。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
節點狀態	
CoreNodesRunning	<p>運作中核心節點數目。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
CoreNodesPending	<p>等待進行指派的核心節點數目。所有要求的核心節點可能都無法立即可用；此指標報告擱置中要求。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
LiveDataNodes	<p>將接收來自 Hadoop 之工作的資料節點百分比。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：百分比</p>
MRTotalNodes	<p>目前可供 MapReduce 工作使用的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.TotalNodes</code>。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
MRActiveNodes	<p>目前執行 MapReduce 任務或工作的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.NoOfActiveNodes</code>。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
MRLostNodes	<p>配置給已標記為 LOST 狀態之 MapReduce 的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.NoOfLostNodes</code>。</p> <p>使用案例：監控 cluster 運作狀態、監控 cluster 進度</p> <p>單位：計數</p>

指標	描述
MRUnhealthyNodes	<p>可供標記為 UNHEALTHY 狀態之 MapReduce 工作使用的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.NoOfUnhealthyNodes</code>。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
MRDecommissionedNodes	<p>配置給已標記為 DECOMMISSIONED 狀態之 MapReduce 應用程式的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.NoOfDecommissionedNodes</code>。</p> <p>使用案例：監控 cluster 運作狀態、監控 cluster 進度</p> <p>單位：計數</p>
MRRebootedNodes	<p>可供已重新啟動與標記為 REBOOTED 狀態之 MapReduce 使用的節點數目。相當於 YARN 指標 <code>mapred.resourcemanager.NoOfRebootedNodes</code>。</p> <p>使用案例：監控 cluster 運作狀態、監控 cluster 進度</p> <p>單位：計數</p>
MultiMasterInstanceGroupNodesRunning	<p>執行中主節點的數量。</p> <p>使用案例：監控主節點故障情形和替換狀況</p> <p>單位：計數</p>
MultiMasterInstanceGroupNodesRunningOverRequested	<p>超過所請求主節點執行個體計數的主節點百分比。</p> <p>使用案例：監控主節點故障情形和替換狀況</p> <p>單位：百分比</p>
MultiMasterInstanceGroupNodesRequested	<p>請求的主節點數量。</p> <p>使用案例：監控主節點故障情形和替換狀況</p> <p>單位：計數</p>
IO	
S3BytesWritten	<p>寫入至 Amazon S3 的位元組數目。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
S3BytesRead	<p>讀取自 Amazon S3 的位元組數目。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>

指標	描述
HDFSUtilization	<p>目前使用中 HDFS 儲存體百分比。</p> <p>使用案例：分析 cluster 效能</p> <p>單位：百分比</p>
HDFSBytesRead	<p>讀取自 HDFS 的位元組數目。此指標只會彙整 MapReduce 工作，並不適用於 EMR 上的其他工作負載。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
HDFSBytesWritten	<p>寫入至 HDFS 的位元組數目。此指標只會彙整 MapReduce 工作，並不適用於 EMR 上的其他工作負載。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
MissingBlocks	<p>HDFS 在其中沒有複本的區塊數目。這些可能是毀損區塊。</p> <p>使用案例：監控 cluster 運作狀態</p> <p>單位：計數</p>
CorruptBlocks	<p>HDFS 報告為毀損的區塊數目。</p> <p>使用案例：監控 cluster 運作狀態</p> <p>單位：計數</p>
TotalLoad	<p>並行資料傳送總次數。</p> <p>使用案例：監控 cluster 運作狀態</p> <p>單位：計數</p>
MemoryTotalMB	<p>叢集中的總記憶體量。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
MemoryReservedMB	<p>保留記憶體數量。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>
MemoryAvailableMB	<p>可供配置的記憶體數量。</p> <p>使用案例：監控 cluster 進度</p> <p>單位：計數</p>

指標	描述
YARNMemoryAvailablePercentage	可供 YARN 使用的剩餘記憶體百分比 (YARNMemoryAvailablePercentage = MemoryAvailableMB / MemoryTotalMB)。此值適用於根據 YARN 記憶體用量來調整叢集資源。
MemoryAllocatedMB	已配置給叢集的記憶體數量。 使用案例：監控 cluster 進度 單位：計數
PendingDeletionBlocks	標記進行刪除的區塊數目。 使用案例：監控 cluster 進度、監控 cluster 運作狀態 單位：計數
UnderReplicatedBlocks	需要複寫一或多次的區塊數目。 使用案例：監控 cluster 進度、監控 cluster 運作狀態 單位：計數
DfsPendingReplicationBlocks	區塊複寫狀態：正在複寫的區塊、複寫要求存留期，以及失敗的複寫要求。 使用案例：監控 cluster 進度、監控 cluster 運作狀態 單位：計數
CapacityRemainingGB	剩餘 HDFS 磁碟容量的數量。 使用案例：監控 cluster 進度、監控 cluster 運作狀態 單位：計數
HBase	
HbaseBackupFailed	最後一個備份是否失敗。根據預設，這設為 0，並在先前的備份嘗試失敗時更新為 1。只會針對 HBase cluster 報告此指標。 使用案例：監控 HBase 備份 單位：計數
MostRecentBackupDuration	先前完成備份所需要的時間量。不論最後一個已完成的備份成功還是失敗，都會設定此指標。正在進行備份時，此指標會傳回備份開始之後的分鐘數。只會針對 HBase cluster 報告此指標。 使用案例：監控 HBase 備份 單位：分鐘
TimeSinceLastSuccessfulBackup	在叢集上開始最後一個成功 HBase 備份之後所經歷的分鐘數。只會針對 HBase cluster 報告此指標。 使用案例：監控 HBase 備份 單位：分鐘

下列是 Hadoop 1 指標：

指標	描述
叢集狀態	
Idle	<p>指出cluster不再執行工作，但仍然存活並產生費用。如果未執行任何任務，而且未執行任何工作，則會設為 1，否則設為 0。此值會以五分鐘的間隔進行檢查，而值 1 指出cluster只在檢查時為閒置，而不是整個五分鐘都閒置。為了避免誤判，此值已為 1 且持續多個連續 5 分鐘檢查時，您應該發出警報。例如，如果此值已為 1 且持續 30 分鐘(含)以上，則您可以對此值發出警報。</p> <p>使用案例：監控cluster效能</p> <p>單位：布林值</p>
JobsRunning	<p>叢集中目前正在執行的工作數目。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
JobsFailed	<p>叢集中失敗的工作數目。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
對應/降低	
MapTasksRunning	<p>每個工作的執行中對應任務數目。如果您已安裝排程器，並且有多個工作正在執行，則會產生多個圖形。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
MapTasksRemaining	<p>每個工作的剩餘對應任務數目。如果您已安裝排程器，並且有多個工作正在執行，則會產生多個圖形。剩餘對應任務就是未處於下列任何狀態的任務：執行中、已刪除或已完成。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
MapSlotsOpen	<p>未使用的對應任務容量。這計算為指定叢集的對應任務數目上限，小於目前在該叢集中執行的對應任務總數。</p> <p>使用案例：分析cluster效能</p> <p>單位：計數</p>
RemainingMapTasksPerSlot	<p>剩餘對應任務總數與叢集中可用對應槽總數的比率。</p> <p>使用案例：分析cluster效能</p> <p>單位：比率</p>
ReduceTasksRunning	<p>每個工作的執行中降低任務數目。如果您已安裝排程器，並且有多個工作正在執行，則會產生多個圖形。</p>

指標	描述
	<p>使用案例：監控cluster進度</p> <p>單位：計數</p>
ReduceTasksRemaining	<p>每個工作的剩餘降低任務數目。如果您已安裝排程器，並且有多個工作正在執行，則會產生多個圖形。</p> <p>使用案例：監控cluster進度</p> <p>單位：計數</p>
ReduceSlotsOpen	<p>未使用的降低任務容量。這計算為指定叢集的降低任務容量上限，小於目前在該叢集中執行的降低任務總數。</p> <p>使用案例：分析cluster效能</p> <p>單位：計數</p>
節點狀態	
CoreNodesRunning	<p>運作中核心節點數目。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
CoreNodesPending	<p>等待進行指派的核心節點數目。所有要求的核心節點可能都無法立即可用；此指標報告擱置中要求。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
LiveDataNodes	<p>將接收來自 Hadoop 之工作的資料節點百分比。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：百分比</p>
TaskNodesRunning	<p>運作中任務節點數目。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>
TaskNodesPending	<p>等待指派的任務節點數目。所有要求的任務節點可能都無法立即可用；此指標報告擱置中要求。只有在對應的執行個體群組存在時，才會報告此指標的資料點。</p> <p>使用案例：監控cluster運作狀態</p> <p>單位：計數</p>

指標	描述
LiveTaskTrackers	<p>運作中任務追蹤器百分比。</p> <p>使用案例：監控 cluster 運作狀態</p> <p>單位：百分比</p>
IO	
S3BytesWritten	<p>寫入至 Amazon S3 的位元組數目。此指標只會彙整 MapReduce 工作，並不適用於 EMR 上的其他工作負載。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
S3BytesRead	<p>讀取自 Amazon S3 的位元組數目。此指標只會彙整 MapReduce 工作，並不適用於 EMR 上的其他工作負載。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
HDFSUtilization	<p>目前使用中 HDFS 儲存體百分比。</p> <p>使用案例：分析 cluster 效能</p> <p>單位：百分比</p>
HDFSBytesRead	<p>讀取自 HDFS 的位元組數目。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
HDFSBytesWritten	<p>寫入至 HDFS 的位元組數目。</p> <p>使用案例：分析 cluster 效能、監控 cluster 進度</p> <p>單位：計數</p>
MissingBlocks	<p>HDFS 在其中沒有複本的區塊數目。這些可能是毀損區塊。</p> <p>使用案例：監控 cluster 運作狀態</p> <p>單位：計數</p>
TotalLoad	<p>叢集中所有 DataNodes 所報告的目前讀取者與寫入者總數。</p> <p>使用案例：診斷高 I/O 可能造成工作執行效能不佳的程度。執行 DataNode 協助程式的工作者節點也必須執行對應與降低任務。一段時間持續具有高 TotalLoad 值，可能表示高 I/O 或為效能不佳的影響因素。此值偶而爆增為正常現象，不一定表示發生問題。</p> <p>單位：計數</p>
HBase	

指標	描述
BackupFailed	<p>最後一個備份是否失敗。根據預設，這設為 0，並在先前的備份嘗試失敗時更新為 1。只會針對 HBase cluster 報告此指標。</p> <p>使用案例：監控 HBase 備份</p> <p>單位：計數</p>
MostRecentBackupDuration	<p>先前完成備份所需要的時間量。不論最後一個已完成的備份成功還是失敗，都會設定此指標。正在進行備份時，此指標會傳回備份開始之後的分鐘數。只會針對 HBase cluster 報告此指標。</p> <p>使用案例：監控 HBase 備份</p> <p>單位：分鐘</p>
TimeSinceLastSuccessfulBackup	<p>在叢集上開始最後一個成功 HBase 備份之後所經歷的分鐘數。只會針對 HBase cluster 報告此指標。</p> <p>使用案例：監控 HBase 備份</p> <p>單位：分鐘</p>

Amazon EMR 指標的維度

Amazon EMR 資料可在下表中使用任何維度進行篩選。

維度	描述
JobFlowId	與 cluster ID 相同，為叢集的唯一識別符，格式為 j-xxxxxxxxxxxxxx。在 Amazon EMR 主控台中按一下 cluster 即可找到此值。
JobId	cluster 中的工作的識別符。您可以使用其篩選 cluster 傳回的指標，最深可以篩選適用於 cluster 內單一任務的指標。JobId，格式為 job_XXXXXXXXXXXX_XXXX。

使用 Ganglia 檢視叢集應用程式指標

Ganglia 隨 Amazon EMR 4.2 版及更新版本提供。Ganglia 是開放原始碼專案，是一種可擴展的分散式系統，設計來監控叢集和網格，同時將對效能的影響降至最低。當您在叢集上啟用 Ganglia 時，您可以產生報告並查看整個叢集的效能，並檢查個別節點執行個體的效能。Ganglia 也會設定為擷取和視覺化 Hadoop 和 Spark 指標。如需詳細資訊，請參閱 Amazon EMR Release Guide 中的 [Ganglia](#)。

在 AWS CloudTrail 中記錄 Amazon EMR API 呼叫

Amazon EMR 已與 AWS CloudTrail 服務整合，此服務會記錄使用者、角色或 Amazon EMR 中 AWS 服務所採取的動作。CloudTrail 會擷取 Amazon EMR 的所有 API 呼叫當做事件。擷取的呼叫包括從 Amazon EMR 主控台的呼叫，以及對 Amazon EMR API 操作的程式碼呼叫。如果您建立追蹤記錄，就可以持續將 CloudTrail 事件傳送至 Amazon S3 儲存貯體，包括 Amazon EMR 的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。使用由 CloudTrail 收集的資訊，您就可以判斷送至 Amazon EMR 的請求、提出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail User Guide](#)。

CloudTrail 中的 Amazon EMR 資訊

當您建立帳戶時，系統會在您的 AWS 帳戶中啟用 CloudTrail。當 Amazon EMR 中發生活動，該活動會記錄在 CloudTrail 事件中，其他 AWS 服務事件則記錄於 Event history (事件歷程記錄)。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱[使用 CloudTrail 事件歷程記錄檢視事件](#)。

若要持續記錄 AWS 帳戶中的事件（包括 Amazon EMR 事件），請建立追蹤記錄。追蹤記錄可讓 CloudTrail 將日誌檔案交付到 Amazon S3 儲存貯體。依預設，當您在主控台建立追蹤時，該追蹤會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 Amazon EMR 動作，並記錄在 [Amazon EMR API Reference](#) 中。例如，對 RunJobFlow、ListCluster、DescribeCluster 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或記錄項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail 使用者身分元素](#)。

範例：Amazon EMR 日誌檔案項目

追蹤記錄是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。事件代表從任何來源的單一請求，並包含有關請求的動作、動作的日期和時間、請求參數等資訊。CloudTrail 日誌檔不是公有 API 呼叫的排序堆疊追蹤記錄，因此不會現以任何特定順序顯示。

以下範例為示範 RunJobFlow (RunJobFlow) 動作的 CloudTrail 日誌項目。

```
{  
  "Records": [  
    {  
      "eventVersion": "1.01",  
      "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "EX_PRINCIPAL_ID",  
        "arn": "arn:aws:iam::123456789012:user/temporary-user-xx-7M",  
        "accountId": "123456789012",  
        "userName": "temporary-user-xx-7M"  
      },  
      "eventTime": "2018-03-31T17:59:21Z",  
      "eventSource": "elasticmapreduce.amazonaws.com",  
      "eventName": "RunJobFlow",  
      "awsRegion": "us-east-1",  
      "version": "1.01",  
      "invocationType": "Programmatic",  
      "recipientAccountId": "123456789012",  
      "resources": [{}],  
      "sourceIPAddress": "123.45.67.89",  
      "awsPartition": "aws",  
      "requestParameters": {}  
    }  
  ]  
}
```

```
"awsRegion":"us-west-2",
"sourceIPAddress":"192.0.2.1",
"userAgent":"aws-sdk-java/unknown-version Linux/xx Java_HotSpot(TM)_64-
Bit_Server_VM/xx",
"requestParameters":{
    "tags":[
        {
            "value":"prod",
            "key":"domain"
        },
        {
            "value":"us-west-2",
            "key":"realm"
        },
        {
            "value":"VERIFICATION",
            "key":"executionType"
        }
    ],
    "instances":{
        "slaveInstanceType":"m5.xlarge",
        "ec2KeyName":"emr-integtest",
        "instanceCount":1,
        "masterInstanceType":"m5.xlarge",
        "keepJobFlowAliveWhenNoSteps":true,
        "terminationProtected":false
    },
    "visibleToAllUsers":false,
    "name":"MyCluster",
    "ReleaseLabel":"emr-5.16.0"
},
"responseElements":{
    "jobFlowId":"j-2WDJCGEG4E6AJ"
},
"requestID":"2f482daf-b8fe-11e3-89e7-75a3d0e071c5",
"eventID":"b348a38d-f744-4097-8b2a-e68c9b424698"
},
...additional entries
]
}
```

連接叢集

執行 Amazon EMR 叢集時，通常您只需執行應用程式來分析資料，然後從 Amazon S3 儲存貯體收集輸出。或者，您可能要在叢集執行時與主節點互動。例如，您可能想要連接到主節點執行互動式查詢、檢查日誌檔、偵錯叢集、使用在主節點上執行的應用程式上（例如 Ganglia）監控效能問題，以此類推。以下區段說明您可以用來連接到主節點的技術。

在 EMR 叢集中，主節點是 Amazon EC2 執行個體，其會協調以任務和核心節點的形式執行的 EC2 執行個體。主節點會公開您可以用來連接到其中的公有 DNS 名稱。根據預設，Amazon EMR 會建立主節點、核心和任務節點的安全群組規則，以判斷您如何存取節點。

Note

您可以在叢集執行時連接到主節點。叢集終止時，做為主節點活動的 EC2 執行個體會終止，且不再可用。若要連接到主節點，您還必須對叢集進行驗證。您可以在啟動叢集時使用 Kerberos 進行驗證，或者指定 Amazon EC2 金鑰對私有金鑰。如需有關設定 Kerberos 然後連線的詳細資訊，請參閱 [使用 Kerberos 身份驗證 \(p. 190\)](#)。當您從主控台啟動叢集，系統會於 Create Cluster (建立叢集) 頁面的 Security and Access (安全和存取) 區段指定 Amazon EC2 金鑰對私密金鑰。

在預設情況下，ElasticMapReduce 主安全群組不允許傳入 SSH 存取。您可能需要新增傳入規則，以從您想要進行存取的來源允許 SSH 存取 (TCP 連接埠 22)。如需修改安全群組規則的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的[新增規則至安全群組](#)。

Important

請勿在 ElasticMapReduce 主安全群組修改剩餘的規則。修改這些規則可能會干擾叢集的操作。

主題

- [使用 SSH 連接至主節點 \(p. 277\)](#)
- [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)

使用 SSH 連接至主節點

Secure Shell (SSH) 是一種網路協定，您可用來建立對遠端電腦的安全連線。建立連線後，本機電腦上的終端機就會像在遠端電腦上執行一樣。您在本機發出的命令會在遠端電腦上執行，而且從遠端電腦的命令輸出會出現在您的終端機視窗。

當您使用 SSH 搭配 AWS，您所連接的是 EC2 執行個體，這是在雲端中執行的虛擬伺服器。使用 Amazon EMR 時，最常見的 SSH 用法是連接到 EC2 執行個體，並以叢集的主節點的形式活動。

使用 SSH 連接到主節點可讓您監控叢集並與其互動。您可以在主節點上發出 Linux 命令、以互動方式執行應用程式（如 Hive 和 Pig）、瀏覽目錄、閱讀日誌檔，以此類推。您也可以在 SSH 連線中建立一個通道來檢視主節點上託管的 Web 界面。如需更多詳細資訊，請參閱[檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

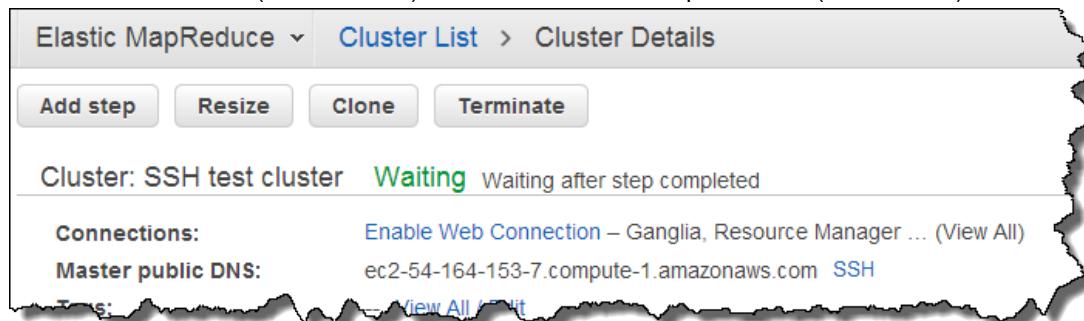
若要使用 SSH 連接到主節點，您需要主節點的公有 DNS 名稱。此外，關聯到主節點的安全群組必須擁有傳入規則，以允許來自包含 SSH 連線起源用戶端之來源的 SSH (TCP 連接埠 22) 流量。您可能需要新增規則來允許來自您用戶端的 SSH 連接。如需修改安全群組規則的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的[使用安全群組控制網路流量 \(p. 230\)](#)和[新增規則至安全群組](#)。

擷取主節點的公有 DNS 名稱

您可以使用 Amazon EMR 主控台和 AWS CLI 擷取主公有 DNS 名稱。

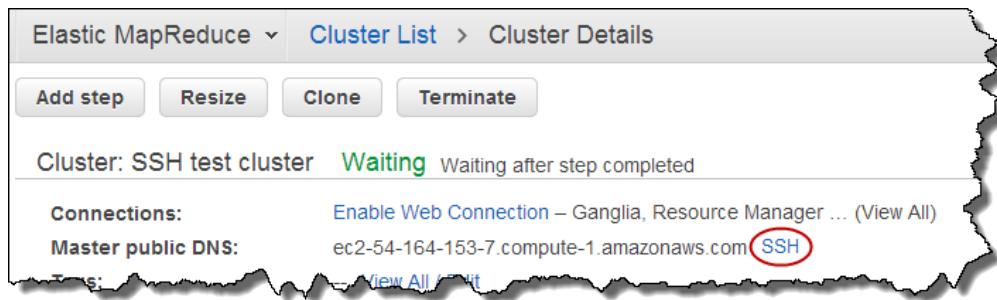
若要使用 Amazon EMR 主控台擷取主節點的公有 DNS 名稱

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 在 Cluster List (叢集清單) 頁面中，選取您叢集的連結。
3. 請注意 Cluster Details (叢集詳細資訊) 頁面頂部顯示的 Master public DNS (主公有 DNS) 值。



Note

您也可以選擇主公有 DNS 名稱旁邊的 SSH 連結以指示使用主節點來建立 SSH 連線。



若要使用 AWS CLI 撈取主節點的公有 DNS 名稱

1. 若要檢視叢集識別碼，請輸入如下命令。

```
aws emr list-clusters
```

輸出會列出叢集 (包括叢集 ID)。請注意，叢集 ID 表示您正連接至其中的叢集。

```
"Status": {  
    "Timeline": {  
        "ReadyDateTime": 1408040782.374,  
        "CreationDateTime": 1408040501.213  
    },  
    "State": "WAITING",  
    "StateChangeReason": {  
        "Message": "Waiting after step completed"  
    }  
},  
"NormalizedInstanceHours": 4,  
"Id": "j-2AL4XXXXXX5T9",  
"Name": "My cluster"
```

2. 若要列出叢集執行個體 (包括叢集的主公有 DNS 名稱)，請輸入以下其中一個命令。使用之前命令傳回的叢集 ID 取代 **j-2AL4XXXXXX5T9**。

```
aws emr list-instances --cluster-id j-2AL4XXXXXX5T9
```

或者：

```
aws emr describe-cluster --cluster-id j-2AL4XXXXXX5T9
```

輸出會列出叢集執行個體 (包括 DNS 名稱和 IP 地址)。請記下 PublicDnsName 的值。

```
"Status": {  
    "Timeline": {  
        "ReadyDateTime": 1408040779.263,  
        "CreationDateTime": 1408040515.535  
    },  
    "State": "RUNNING",  
    "StateChangeReason": {}  
},  
"Ec2InstanceId": "i-e89b45e7",  
"PublicDnsName": "ec2-###-##-##-##.us-west-2.compute.amazonaws.com"  
"PrivateDnsName": "ip-###-##-##-##.us-west-2.compute.internal",
```

```
"PublicIpAddress": "##.###.##.##",
"Id": "ci-12XXXXXXXXFMH",
"PrivateIpAddress": "##.##.##.##"
```

如需詳細資訊，請參閱 AWS CLI 中的 Amazon EMR 命令。

在 Linux、Unix 和 Mac OS X 使用 SSH 和 Amazon EC2 私密金鑰連接到主節點

若要建立透過私有金鑰檔案驗證的 SSH 連線，您需要在啟動叢集時指定 Amazon EC2 金鑰對私有金鑰。若您從主控台啟動叢集，系統會在 Create Cluster (建立叢集) 頁面的 Security and Access (安全和存取) 區段指定 Amazon EC2 金鑰對私密金鑰。如需存取金鑰對的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2 金鑰對](#)。

根據預設，您的 Linux 電腦很可能包含 SSH 用戶端。例如，大多數的 Linux、Unix 和 macOS 作業系統都會安裝 OpenSSH。您可以藉由在命令列鍵入 ssh 來檢查 SSH 用戶端。若您的電腦無法識別該命令，請安裝 SSH 用戶端以連線到主節點。OpenSSH 專案提供 SSH 工具完整套件的免費實作。如需詳細資訊，請參閱 [OpenSSH 網站](#)。

以下說明示範開立 SSH 連接到在 Linux、Unix 和 Mac OS X 的 Amazon EMR 主節點。

若要設定金鑰對私有金鑰檔案權限

在可以使用您的 Amazon EC2 金鑰對私密金鑰來建立 SSH 連線前，您必須設定 .pem 檔案的權限，讓唯一的金鑰擁有者有權限存取檔案。使用終端機或 AWS CLI 建立 SSH 連線需要進行此操作。

1. 尋找您的 .pem 檔案。這些說明假設檔案名為 mykeypair.pem 且存放在目前的使用者主目錄中。
2. 輸入以下命令來設定權限。使用您金鑰對私密金鑰檔案的位置和檔案名稱來取代 `~/mykeypair.pem`。

```
chmod 400 ~/mykeypair.pem
```

如果您沒有設定 .pem 檔案的許可，您將會收到錯誤，告知您金鑰檔案未受保護且金鑰會遭到拒絕。若要連接，您只需在第一次使用金鑰對私有金鑰檔案時設定其許可。

若要使用終端機連接到主節點

1. 開啟終端機視窗。在 Mac OS X 上，選擇 Applications (應用程式) > Utilities (公用程式) > Terminal (終端機)。在其他 Linux 分佈，通常可於 Applications (應用程式) > Accessories (附屬應用程式) > Terminal (終端機) 找到終端機。
2. 欲建立連接至主節點的連線，請輸入下列命令。以叢集的主公有 DNS 名稱取代 `ec2-###-##-##-##.compute-1.amazonaws.com` 並以 .pem 檔案的位置和檔案名稱取代 `~/mykeypair.pem`。

```
ssh hadoop@ec2-###-##-##-##.compute-1.amazonaws.com -i ~/mykeypair.pem
```

Important

您必須在連接到 Amazon EMR 主節點時使用登入名稱 hadoop，否則，您可能會看到與 Server refused our key 類似的錯誤。

3. 警告說明系統無法驗證您要在連接之主機的真實性。輸入 yes 以繼續。
4. 當您完成處理主節點時，輸入下列命令來關閉 SSH 連線。

```
exit
```

使用 AWS CLI 連接至主節點

您可以在 Windows 和 Linux、Unix 和 Mac OS X 使用 AWS CLI 建立至主節點的 SSH 連線，無論平台為何，您需要主節點的公有 DNS 名稱和 Amazon EC2 金鑰對私密金鑰。如果您在 Linux、Unix 或 Mac OS X 上使用的是 AWS CLI，您還必須設定私密金鑰 (.pem 或 .ppk) 檔案的許可，如 [若要設定金鑰對私有金鑰檔案權限 \(p. 279\)](#) 中所示。

若要使用 AWS CLI 連接至主節點

1. 若要擷取叢集識別符，輸入：

```
aws emr list-clusters
```

輸出會列出叢集 (包括叢集 ID)。請注意，叢集 ID 表示您正連接至其中的叢集。

```
"Status": {  
    "Timeline": {  
        "ReadyDateTime": 1408040782.374,  
        "CreationDateTime": 1408040501.213  
    },  
    "State": "WAITING",  
    "StateChangeReason": {  
        "Message": "Waiting after step completed"  
    }  
},  
"NormalizedInstanceHours": 4,  
"Id": "j-2AL4XXXXXX5T9",  
"Name": "AWS CLI cluster"
```

2. 輸入下列命令以開啟對主節點的 SSH 連線。在下列範例中，使用叢集 ID 來取代 **j-2AL4XXXXXX5T9** 並使用您 .pem 檔案 (若是 Linux、Unix 和 Mac OS X) 或 .ppk 檔案 (若是 Windows) 的位置和檔名來取代 **~/mykeypair.key**。

```
aws emr ssh --cluster-id j-2AL4XXXXXX5T9 --key-pair-file ~/mykeypair.key
```

3. 當您完成處理主節點時，關閉 AWS CLI 視窗。

如需詳細資訊，請參閱 [AWS CLI 中的 Amazon EMR 命令](#)。

使用 Windows 上的 SSH 來連接至主節點

Windows 使用者可以使用 SSH 用戶端 (例如 PuTTY) 來連接到主節點。連接到 Amazon EMR 主節點前，您應該下載並安裝 PuTTY 和 PuTTYgen。您可以從 [PuTTY 下載頁面](#) 下載這些工具。

PuTTY 原生並不支援 Amazon EC2 產生的金鑰對私密金鑰檔案格式 (.pem)。您要使用 PuTTYgen 將您的私密金鑰轉換為 PuTTY 所需的格式 (.ppk)。您必須將金鑰轉換為此格式 (.ppk)，再嘗試使用 PuTTY 連接至主節點。

如需轉換金鑰對的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [使用 PuTTYgen 轉換私密金鑰](#)。

若要使用 PuTTY 連接至主節點

1. 開啟 **putty.exe**。您也可以從 Windows 程式清單啟動 PuTTY。
2. 必要時，選擇 Category (類別) 清單中的 Session (工作階段)。
3. 對於 Host Name (or IP address) (主機名稱 (或 IP 地址))，輸入 **hadoop@MasterPublicDNS**。例如：**hadoop@ec2-###-##-##-##.compute-1.amazonaws.com**。

4. 在 Category (類別) 清單中選擇 Connection > SSH (連線 > SSH)、Auth。
5. 針對 Private key file for authentication (要身份驗證的私密金鑰檔案)，選擇 Browse (瀏覽) 並選取您產生的 .ppk 檔案。
6. 選擇 Open (開啟)，接著選擇 Yes (是) 以關閉 PuTTY 安全提醒。

Important

登入主節點類型時，如果系統提示您輸入使用者名稱，則輸入 hadoop。

7. 當您完成處理主節點時，可以關閉 PuTTY 來關閉 SSH 連線。

Note

為避免 SSH 連線逾時，您可以選擇 Category (類別) 清單中的 Connection (連線) 並選取選項 Enable TCP_keepalives (啟用 TCP_keepalives)。如果您在 PuTTY 中有作用中的 SSH 工作階段，您可以開啟 PuTTY 標題列的內容 (按一下滑鼠右鍵) 並選擇 Change Settings (變更設定) 以變更設定。

檢視 Amazon EMR 叢集上託管的 Web 界面

Hadoop 和您在 Amazon EMR 叢集安裝的其他應用程式會將使用者界面發佈為網站，並託管於主節點。基於安全考量，當使用 EMR 管理的安全群組，這些網站只在主節點的本機 Web 伺服器上可供使用，因此您需要連接到主節點以進行檢視。如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。Hadoop 也發行使用者界面做為網站，並在核心節點和任務節點上託管。這些網站也僅適用於本機 Web 伺服器的節點。

Warning

您可以設定自訂安全群組，以允許傳入存取這些 Web 界面。請注意，您允許輸入流量的任何連接埠代表潛在安全漏洞。請詳閱自訂安全群組，以確保您將漏洞數量降至最低。如需更多詳細資訊，請參閱 [使用安全群組控制網路流量 \(p. 230\)](#)。

下表列出可在叢集執行個體上檢視的 Web 界面。這些 Hadoop 界面可適用於所有叢集。針對主執行個體界面，以 EMR 主控台之叢集 Summary (摘要) 索引標籤所列的 Master public DNS (主公有 DNS) 取代 *master-public-dns-name*。針對核心和任務執行個體界面，以執行個體列出的 Public DNS name (公有 DNS 名稱) 取代 *coretask-public-dns-name*。若要尋找執行個體的 Public DNS name (公有 DNS 名稱)，請至 EMR 主控台從清單選擇叢集，選擇 Hardware (硬體) 索引標籤，選擇包含您想要連接之執行個體的執行個體群組 ID，接著記下執行個體列出的 Public DNS name (公有 DNS 名稱)。

Important

若要存取 Web 界面，您必須編輯與主執行個體和核心執行個體關聯的安全群組，使其具有傳入規則以允許來自信任用戶端的 SSH 流量 (連接埠 22)，例如您電腦的 IP 地址。如需修改安全群組規則的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [新增規則至安全群組](#)。

界面的名稱	URI
YARN ResourceManager	http://<i>master-public-dns-name</i>:8088/
YARN NodeManager	http://<i>coretask-public-dns-name</i>:8042/
Hadoop HDFS NameNode	http://<i>master-public-dns-name</i>:50070/
Hadoop HDFS DataNode	http://<i>coretask-public-dns-name</i>:50075/
Spark HistoryServer	http://<i>master-public-dns-name</i>:18080/
Zeppelin	http://<i>master-public-dns-name</i>:8890/
Hue	http://<i>master-public-dns-name</i>:8888/

界面的名稱	URI
Ganglia	http://<i>master-public-dns-name</i>/ganglia/
HBase	http://<i>master-public-dns-name</i>:16010/
JupyterHub	https://<i>master-public-dns-name</i>:9443/

由於有多種應用程式特定界面可用於主節點，而不可用於核心和任務節點，此文件中的指示是專屬於 Amazon EMR 主節點。在核心和任務節點上存取 Web 界面，可以透過與您在主節點上存取 Web 界面的相同方式完成。

有多種可以在主節點上存取 Web 界面的方法。使用 SSH 連接到主節點並使用以文字為基礎的瀏覽器 (Lynx)，以查看在 SSH 用戶端中網站的最簡單和快的方法。不過，Lynx 是以文字為基礎的瀏覽器，其使用者介面有無法顯示圖形的限制。以下範例說明如何使用 Lynx (Lynx URL 也會在您使用 SSH 登入主節點時提供) 開啟 Hadoop ResourceManager 界面。

```
lynx http://ip-###-##-##-##.us-west-2.compute.internal:8088/
```

有兩種剩餘的選項，讓您在提供完整瀏覽器功能的主節點存取 Web 界面。選擇下列其中一項：

- 選項 1 (建議較技術導向的使用者使用)：使用 SSH 用戶端來連接到主節點、設定含本機連接埠轉寄的 SSH 通道，並使用網際網路瀏覽器以開啟在主節點上託管的 Web 界面。這個方法可讓您設定 Web 界面存取，而不需使用 SOCKS 代理。
- 選項 2 (建議新使用者使用)：使用 SSH 用戶端連接到主節點、設定含動態連接埠轉送的 SSH 通道，並設定網際網路瀏覽器以使用附加元件 (例如 FoxyProxy 或 SwitchySharp) 來管理 SOCKS 代理設定。這個方法可讓您根據文字模式自動篩選 URL，並將代理設定限制為與主節點 DNS 名稱的形式相符的網域。當您在主節點上託管的檢視網站和這些網際網路上的檢視網站切換時，瀏覽器附加元件會自動處理 Proxy 的開啟和關閉。如需有關如何設定 FoxyProxy for Firefox 和 Google Chrome 的詳細資訊，請參閱[第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站 \(p. 285\)](#)。

主題

- [選項 1：使用本機連接埠轉送將 SSH 通道設定為主節點 \(p. 282\)](#)
- [第 1 部分選項 2：使用動態連接埠轉送將 SSH 通道設定為主節點 \(p. 283\)](#)
- [第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站 \(p. 285\)](#)
- [使用主控台在主節點上存取 Web 界面 \(p. 287\)](#)

選項 1：使用本機連接埠轉送將 SSH 通道設定為主節點

要連接到主節點上的本機 Web 伺服器，您會在電腦和主節點之間的建立一個 SSH 通道。這就是所謂的連接埠轉送。如果您不想使用 SOCKS 代理，您可以使用本機連接埠轉送設定一個到主節點的 SSH 通道。使用本機連接埠轉送，您需要指定未使用的本機連接埠，其會用來將流量轉送至主節點本機 Web 伺服器上的特定遠端連接埠。

使用本機連接埠轉送設定一個 SSH 通道需要主節點的公有 DNS 名稱和金鑰對私有金鑰檔案。如需尋找主公有 DNS 名稱的詳細資訊，請參閱[若要使用 Amazon EMR 主控台擷取主節點的公有 DNS 名稱 \(p. 277\)](#)。如需存取金鑰對的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [Amazon EC2 金鑰對](#)。如需您想要在主節點上檢視之網站的詳細資訊，請參閱[檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

使用本機連接埠轉送在 Linux、Unix 和 Mac OS X 將 SSH 通道設定為主節點

若要使用本機連接埠轉送在終端機中設定一個 SSH 通道

1. 開啟終端機視窗。在 Mac OS X 上，選擇 Applications (應用程式) > Utilities (公用程式) > Terminal (終端機)。在其他 Linux 分佈，通常可於 Applications (應用程式) > Accessories (附屬應用程式) > Terminal (終端機) 找到終端機。
2. 輸入下列命令以在本機電腦上開啟一個 SSH 通道。此命令透過在本機連接埠 8157 (隨機選擇，未使用的本機連接埠) 上將流量轉送至在主節點本機 Web 伺服器上的連接埠 8088 來存取 ResourceManager Web 界面。在命令中，以 .pem 檔案的位置和檔案名稱取代 `~/mykeypair.pem` 並以叢集的主公有 DNS 名稱取代 `ec2-###-##-##-##.compute-1.amazonaws.com`。

```
ssh -i ~/mykeypair.pem -N -L 8157:ec2-###-##-##-##.compute-1.amazonaws.com:8088
hadoop@ec2-###-##-##-##.compute-1.amazonaws.com
```

發出此命令後，終端會保持開啟，且不會傳回回應。

Note

`-L` 表示使用本機連接埠轉送，其可讓您指定本機連接埠，以便用於轉送資料以識別在主節點本機 Web 伺服器上的遠端連接埠。

3. 若要在瀏覽器中開啟 ResourceManager Web 界面，請在地址列輸入：`http://localhost:8157/`。
4. 當您在主節點完成 Web 界面的處理時，請關閉終端機視窗。

第 1 部分選項 2：使用動態連接埠轉送將 SSH 通道設定為主節點

要連接到主節點上的本機 Web 伺服器，您會在電腦和主節點之間的建立一個 SSH 通道。這就是所謂的連接埠轉送。如果您使用動態連接埠轉送建立您的 SSH 通道，所有路由到指定未使用的本機連接埠流量會轉送到主節點上的本機 Web 伺服器。這會建立一個 SOCKS 代理。然後，您可以設定您的網際網路瀏覽器使用附加元件 (例如 FoxyProxy 或 SwitchySharp) 來管理您的 SOCKS 代理設定。使用代理管理附加元件可讓您根據文字模式，自動篩選 URL 並將代理設定限制為與主節點 DNS 名稱之形式相符的網域。當您 在主節點上託管的檢視網站和這些網際網路上的檢視網站切換時，瀏覽器附加元件會自動處理 Proxy 的開啟和關閉。

開始之前，您需要主節點的公有 DNS 名稱和您的金鑰對私有金鑰檔案。如需尋找主公有 DNS 名稱的詳細資訊，請參閱 [若要使用 Amazon EMR 主控台擷取主節點的公有 DNS 名稱 \(p. 277\)](#)。如需存取金鑰對的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 Amazon EC2 金鑰對。如需您想要在主節點上檢視之網站的詳細資訊，請參閱 [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

使用動態連接埠轉送，在 Linux、Unix 和 Mac OS X 將 SSH 通道設定為主節點

若要使用動態連接埠轉送，在 Linux、Unix 和 Mac OS X 設定 SSH 通道

1. 開啟終端機視窗。在 Mac OS X 上，選擇 Applications (應用程式) > Utilities (公用程式) > Terminal (終端機)。在其他 Linux 分佈，通常可於 Applications (應用程式) > Accessories (附屬應用程式) > Terminal (終端機) 找到終端機。
2. 輸入下列命令以在本機電腦上開啟一個 SSH 通道。以 .pem 檔案的位置和檔案名稱取代 `~/mykeypair.pem`，以未使用的本機連接埠號碼取代 `8157`，並以叢集的主公有 DNS 名稱取代 `ec2-###-##-##-##.compute-1.amazonaws.com`。

```
ssh -i ~/mykeypair.pem -N -D 8157 hadoop@ec2-###-##-##-##.compute-1.amazonaws.com
```

發出此命令後，終端會保持開啟，且不會傳回回應。

Note

-D 表示使用動態連接埠轉送，其可讓您指定本機連接埠，以便用於將資料轉送至主節點本機 Web 伺服器上的所有遠端連接埠。動態連接埠轉送會在命令中指定的連接埠上建立本機 SOCKS 代理接聽。

3. 通道在作用中後，為您的瀏覽器設定 SOCKS 代理。如需更多詳細資訊，請參閱 [第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站 \(p. 285\)](#)。
4. 當您在主節點完成 Web 界面的處理時，請關閉終端機視窗。

使用動態連接埠轉送搭配 AWS CLI 來設定 SSH 通道

您可以使用 AWS CLI 在 Windows 和 Linux、Unix 和 Mac OS X 上建立一個 SSH 連線與主節點。如果您在 Linux、Unix 或 Mac OS X 上使用 AWS CLI，您必須在 .pem 檔案上設定權限，如 [若要設定金鑰對私有金鑰檔案權限 \(p. 279\)](#) 中所示。如果您在 Windows 上使用 AWS CLI，則 PuTTY 必須顯示在路徑環境變數中，否則您可能會收到錯誤，例如 OpenSSH or PuTTY not available (OpenSSH 或 PuTTY 不可用)。

若要使用動態連接埠轉送搭配 AWS CLI 來設定 SSH 通道

1. 建立 SSH 連線與主節點，如 [使用 AWS CLI 連接至主節點 \(p. 280\)](#) 中所示。
2. 若要擷取叢集識別符，輸入：

```
aws emr list-clusters
```

輸出會列出叢集 (包括叢集 ID)。請注意，叢集 ID 表示您正連接至其中的叢集。

```
"Status": {  
    "Timeline": {  
        "ReadyDateTime": 1408040782.374,  
        "CreationDateTime": 1408040501.213  
    },  
    "State": "WAITING",  
    "StateChangeReason": {  
        "Message": "Waiting after step completed"  
    }  
},  
"NormalizedInstanceHours": 4,  
"Id": "j-2AL4XXXXXX5T9",  
"Name": "AWS CLI cluster"
```

3. 使用動態連接埠轉送來建立開啟至主節點的 SSH 通道，請輸入下列命令。在下列範例中，使用叢集 ID 來取代 **j-2AL4XXXXXX5T9** 並使用您 .pem 檔案 (若是 Linux、Unix 和 Mac OS X) 或 .ppk 檔案 (若是 Windows) 的位置和檔名來取代 **~/mykeypair.key**。

```
aws emr socks --cluster-id j-2AL4XXXXXX5T9 --key-pair-file ~/mykeypair.key
```

Note

socks 命令會在本機連接埠 8157 上自動設定動態連接埠轉送。目前，此設定無法修改。

4. 通道在作用中後，為您的瀏覽器設定 SOCKS 代理。如需更多詳細資訊，請參閱 [第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站 \(p. 285\)](#)。
5. 當您在主節點完成 Web 界面的處理時，請關閉 AWS CLI 視窗。

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用動態連接埠轉送在 Windows 上將 SSH 通道設定為主節點

Windows 使用者可以使用 SSH 用戶端 (例如 PuTTY) 來對主節點建立 SSH 通道。連接到 Amazon EMR 主節點前，您應該下載並安裝 PuTTY 和 PuTTYgen。您可以從 [PuTTY 下載頁面](#) 下載這些工具。

PuTTY 原生並不支援 Amazon EC2 產生的金鑰對私密金鑰檔案格式 (.pem)。您要使用 PuTTYgen 將您的私密金鑰轉換為 PuTTY 所需的格式 (.ppk)。您必須將金鑰轉換為此格式 (.ppk)，再嘗試使用 PuTTY 連接至主節點。

如需轉換金鑰對的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的 [使用 PuTTYgen 轉換私密金鑰](#)。

若要使用動態連接埠轉送在 Windows 上設定 SSH 通道

- 按兩下 `putty.exe` 以啟動 PuTTY。您也可以從 Windows 程式清單啟動 PuTTY。

Note

如果您已有作用中的 SSH 工作階段和主節點，您可以在 PuTTY 標題列按一下滑鼠右鍵並選擇 Change Settings (變更設定) 來新增通道。

- 必要時，選擇 Category (類別) 清單中的 Session (工作階段)。
- 在 Host Name (主機名稱) 欄位，輸入 `hadoop@MasterPublicDNS`。例如：`hadoop@ec2-###-##-##-##.compute-1.amazonaws.com`。
- 在 Category (類別) 清單中，展開 Connection > SSH (連線 > SSH)，然後選擇 Auth。
- 針對 Private key file for authentication (要身份驗證的私密金鑰檔案)，選擇 Browse (瀏覽) 並選取您產生的 .ppk 檔案。

Note

PuTTY 原生並不支援 Amazon EC2 產生的金鑰對私密金鑰檔案格式 (.pem)。您要使用 PuTTYgen 將您的私密金鑰轉換為 PuTTY 所需的格式 (.ppk)。您必須將金鑰轉換為此格式 (.ppk)，再嘗試使用 PuTTY 連接至主節點。

- 在 Category (類別) 清單中，展開 Connection > SSH (連線 > SSH)，然後選擇 Tunnels (通道)。
- 在 Source port (來源連接埠) 欄位中，輸入 8157 (未使用的本機連接埠)。
- 將 Destination (目的地) 欄位保留空白。
- 選取 Dynamic (動態) 與 Auto (自動) 選項。
- 選擇 Add (新增) 和 Open (開啟)。
- 選擇 Yes (是) 關閉 PuTTY 安全提醒。

Important

登入主節點類型時，如果系統提示您輸入使用者名稱，則輸入 `hadoop`。

- 通道在作用中後，為您的瀏覽器設定 SOCKS 代理。如需更多詳細資訊，請參閱 [第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站 \(p. 285\)](#)。
- 當您 在主節點完成 Web 界面的處理時，請關閉 PuTTY 視窗。

第 2 部分選項 2：設定代理設定，以查看主節點上託管的網站

如果您使用 SSH 通道搭配動態連接埠轉送，您必須使用 SOCKS 代理管理附加元件，以控制在瀏覽器中的代理設定。使用 SOCKS 代理管理工具可讓您根據文字模式自動篩選 URL，並將代理設定限制為與主節點公有 DNS 名稱之形式相符的網域。當您在主節點上託管的檢視網站和這些網際網路上的檢視網站切換時，瀏覽器附加元件會自動處理 Proxy 的開啟和關閉。若要管理代理設定，將您的瀏覽器設定為使用附加元件 (例如 FoxyProxy 或 SwitchySharp)。

如需建立 SSH 通道的詳細資訊，請參閱 [第 1 部分選項 2：使用動態連接埠轉送將 SSH 通道設定為主節點 \(p. 283\)](#)。如需這些可用 Web 介面的詳細資訊，請參閱 [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

以下範例示範使用 Google Chrome 的 FoxyProxy 組態。範例中從組態檔案載入的相關設定如下：

- Host or IP Address (主機或 IP 地址)—在範例中此設定為 localhost，而連接埠設為 8157。您應該將此連接埠設定為您使用 [第 1 部分選項 2：使用動態連接埠轉送將 SSH 通道設定為主節點 \(p. 283\)](#) 中主節點來建立 SSH 通道的本機連接埠號碼。此連接埠也必須與在 PuTTY 使用的連接埠編號或您用於連接的其他終端機模擬器相符。
- SOCKS v5 (SOCKS v5) 組態已指定。
- 未指定登入資料。
- URL Patterns (URL 模式)

以下 URL 模式已加入允許清單並使用萬用字元模式類型加以指定：

- *ec2*.amazonaws.com* 與 *10*.amazonaws.com* 模式會與美國區域的叢集公有 DNS 名稱相符。
- 而 *ec2*.compute* 和 *10*.compute* 模式則會與所有其他區域的叢集公有 DNS 名稱相符。
- 10.* (10.*) 模式提供對 Hadoop 中 JobTracker 日誌檔案的存取。如果此篩選條件與網路存取計畫衝突，請進行更改。

設定 FoxyProxy for Google Chrome

您可以設定 FoxyProxy for Google Chrome、Mozilla Firefox 和 Microsoft Internet Explorer。FoxyProxy 提供一組代理管理工具，可讓您將代理伺服器用於與對應到 Amazon EMR 叢集中 Amazon EC2 執行個體使用之網域之模式相符的 URL。

若要使用 Google Chrome 安裝和設定 FoxyProxy

1. 請參閱 <https://chrome.google.com/webstore/search/foxy%20proxy> 並依照連結和指示，以將 FoxyProxy 新增到 Chrome。
2. 使用文字編輯器，並建立名為 foxyproxy-settings.xml 的檔案，內含下列內容：

```
<?xml version="1.0" encoding="UTF-8"?>
<foxyproxy>
  <proxies>
    <proxy name="emr-socks-proxy" id="2322596116" notes="" fromSubscription="false"
enabled="true" mode="manual" selectedTabIndex="2" lastresort="false"
animatedIcons="true" includeInCycle="true" color="#0055E5" proxyDNS="true"
noInternalIPs="false" autoconfMode="pac" clearCacheBeforeUse="false"
disableCache="false" clearCookiesBeforeUse="false" rejectCookies="false">
      <matches>
        <match enabled="true" name="*ec2*.amazonaws.com*"
pattern="*ec2*.amazonaws.com*" isRegEx="false" isBlackList="false" isMultiLine="false"
caseSensitive="false" fromSubscription="false" />
        <match enabled="true" name="*ec2*.compute*" pattern="*ec2*.compute*"
isRegEx="false" isBlackList="false" isMultiLine="false" caseSensitive="false"
fromSubscription="false" />
        <match enabled="true" name="10.*" pattern="http://10.*"
isRegEx="false" isBlackList="false" isMultiLine="false" caseSensitive="false"
fromSubscription="false" />
        <match enabled="true" name="*10*.amazonaws.com*"
pattern="*10*.amazonaws.com*" isRegEx="false" isBlackList="false" isMultiLine="false"
caseSensitive="false" fromSubscription="false" />
        <match enabled="true" name="*10*.compute*" pattern="*10*.compute*"
isRegEx="false" isBlackList="false" isMultiLine="false" caseSensitive="false"
fromSubscription="false" />
        <match enabled="true" name="*.compute.internal*"
pattern="*.compute.internal*" isRegEx="false" isBlackList="false" isMultiLine="false"
caseSensitive="false" fromSubscription="false"/>
      </matches>
    </proxy>
  </proxies>
</foxyproxy>
```

```
<match enabled="true" name=".ec2.internal*" pattern=".ec2.internal*"
isRegEx="false" isBlackList="false" isMultiLine="false" caseSensitive="false"
fromSubscription="false"/>
</matches>
<manualconf host="localhost" port="8157" socksversion="5" isSocks="true"
username="" password="" domain="" />
</proxy>
</proxies>
</foxyproxy>
```

3. 在 Chrome 管理擴展 (請前往 chrome://extensions)。
4. 針對 FoxyProxy Standard，選擇 Options (選項)。
5. 在 FoxyProxy 頁面，選擇 Import/Export (匯入/匯出)。
6. 在 Import/Export (匯入/匯出) 頁面，選擇 Choose File (選擇檔案)，然後瀏覽到您建立的 foxyproxy-settings.xml 檔案的位置，選取檔案，接著選擇 Open (開啟)。
7. 在系統提示要覆寫現有的設定時，選擇 Replace (取代)。
8. 對於 Proxy mode (代理模式)，選擇 Use proxies based on their predefined patterns and priorities (根據預先定義模式和優先順序使用代理伺服器)。
9. 若要在瀏覽器中的地址列中開啟 Web 界面，輸入 *master-public-dns*，接著輸入連接埠號碼或 URL。

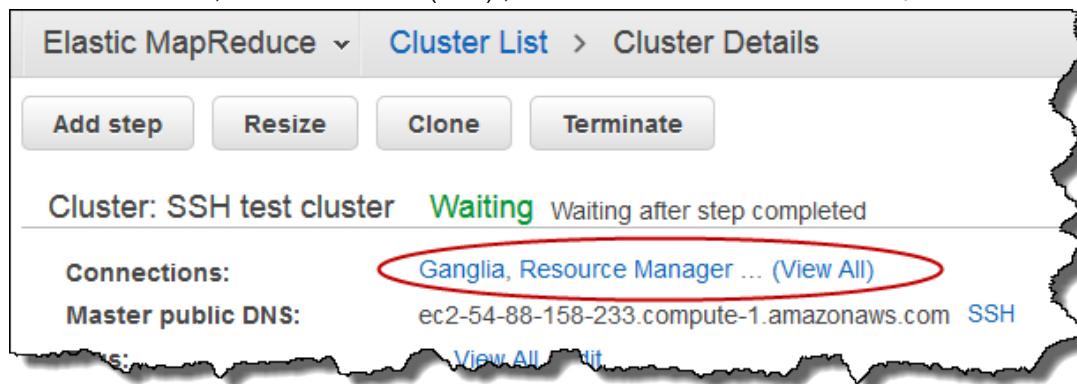
如需主節點的 Web 介面完整清單，請參閱[檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

使用主控台在主節點上存取 Web 界面

如果您已使用動態連接埠轉送搭配 Amazon EMR 主節點的已設定 SSH 通道，您可以使用主控台來開啟 Web 界面。

若要使用主控台開啟 Web 界面

1. 確定您已經建立 SSH 通道與主節點，而且您為瀏覽器設定代理管理附加元件。
2. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
3. 在 Cluster List (叢集清單) 頁面，選擇您叢集的連結。
4. 在叢集詳細資訊中，對於 Connections (連線)，選擇您要在瀏覽器中開啟的 Web 界面。



5. 或者，選擇 View All (查看所有) 連結以對叢集主節點上所有可用的 Web 界面顯示連結。選擇連結會在瀏覽器中開啟界面。

Web Interfaces Hosted on this Cluster

Hadoop, Ganglia, and other applications publish user interfaces as websites hosted on the master node. For security reasons, these websites are only available on the master node's local webserver (<http://localhost>) and are not published on the Internet.

Note
For the below links to work properly an SSH tunnel must be open and your browser configured to use the proxy for Amazon EC2 URLs.

The following table lists web interfaces you can view on the master node:

Interface	URI
Resource Manager	http://ec2-54-164-54-29.compute-1.amazonaws.com:9026/
HDFS Name Node	http://ec2-54-164-54-29.compute-1.amazonaws.com:9101/

The following table lists web interfaces you can view on the slave nodes:

Interface	URI
Node Manager	http://ec2-000-000-000-000.compute-1.amazonaws.com:9035/
HDFS Data Node	http://ec2-000-000-000-000.compute-1.amazonaws.com:9102/

如果您沒有與主節點開啟的 SSH 通道，請選擇 Enable Web Connection (啟用 Web 連線) 以指示建立通道。

Elastic MapReduce ▾ Cluster List > Cluster Details

Add step Resize Clone Terminate

Cluster: SSH test cluster Waiting Waiting after step completed

Connections: [Enable Web Connection](#) – Ganglia, Resource Manager ... (View All)

Master public DNS: ec2-54-88-158-233.compute-1.amazonaws.com SSH

Tags: – [View All / Edit](#)

Note

如果您已使用本機連接埠轉送設定一個 SSH 通道，則 Amazon EMR 主控台不會偵測連線。

終止叢集

本節說明終止叢集的方法。如需啟用終止保護和自動終止叢集的詳細資訊，請參閱 [控制叢集終止 \(p. 73\)](#)。您可以在終止狀態為 STARTING、RUNNING 或 WAITING 的叢集。狀態為 WAITING 的叢集必須終止，否則其無限期地執行，會對您的帳戶產生費用。您可以將無法離開 STARTING 狀態或無法完成步驟的叢集加以終止。

如果您正在終止的叢集已設定終止保護，您必須停用終止保護，才能終止叢集。您可以使用主控台、AWS CLI 或者以程式設計方式使用 `TerminateJobFlows` API 終止叢集。

依據叢集組態的不同，叢集可能需要 5-20 分鐘時間才會完成終止並釋出配置資源 (例如 EC2 執行個體)。

使用主控台終止叢集

您可以使用 Amazon EMR 主控台來終止一或多個叢集。主控台中終止叢集的步驟會因終止保護是否開啟或關閉而有所不同。若要終止保護的叢集，您必須先停用終止保護。

若要將終止保護為關閉的叢集加以終止

1. Sign in to the AWS Management Console and open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選取要終止的叢集。您可以選取多個叢集並將它們同時終止。
3. 選擇 Terminate (終止)。
4. 出現提示時，選擇 Terminate (終止)。

Amazon EMR 會在叢集中終止執行個體，並阻止節省日誌資料。

若要將終止保護為開啟的叢集加以終止

1. Sign in to the AWS Management Console and open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 在 Cluster List (叢集清單) 頁面中，選取您要終止的叢集。您可以選取多個叢集並將它們同時終止。
3. 選擇 Terminate (終止)。
4. 當出現提示，選擇 Change (變更) 關閉終止保護。如果您選取的是多個叢集，請選擇 Turn off all (全部關閉) 一次停用對所有叢集的終止保護。
5. 在 Terminate clusters (終止叢集) 對話方塊，對於 Termination Protection (終止保護)，請選擇 Off (關閉)，然後按一下檢查標記以進行確認。
6. 按一下 Terminate (終止)。

Amazon EMR 會在叢集中終止執行個體，並阻止節省日誌資料。

使用 AWS CLI 終止叢集

欲使用 AWS CLI 來終止未受保護的叢集

若要使用 AWS CLI 終止未受保護的叢集，請使用 terminate-clusters 子指令與 --cluster-ids 參數。

- 輸入下列命令以終止單一叢集，並使用叢集 ID 取代 **j-3KVXXXXXXX7UG**。

```
aws emr terminate-clusters --cluster-ids j-3KVXXXXXXX7UG
```

若要終止多個叢集，請輸入下列命令，並使用叢集 ID 取代 **j-3KVXXXXXXX7UG** 和 **j-WJ2XXXXXXX8EU**。

```
aws emr terminate-clusters --cluster-ids j-3KVXXXXXXX7UG j-WJ2XXXXXXX8EU
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

欲使用 AWS CLI 來終止受保護的叢集

若要使用 AWS CLI 終止受保護叢集，請先使用 modify-cluster-attributes 子指令與 --no-termination-protected 參數停用終止保護。然後，使用 terminate-clusters 子指令和 --cluster-ids 參數來進行終止。

1. 輸入下列命令停用終止保護，並使用叢集 ID 取代 **j-3KVTXXXXXX7UG**。

```
aws emr modify-cluster-attributes --cluster-id j-3KVTXXXXXX7UG --no-termination-protected
```

2. 若要終止叢集，輸入下列命令，並使用叢集 ID 取代 *j-3KVXXXXXXX7UG*。

```
aws emr terminate-clusters --cluster-ids j-3KVXXXXXXX7UG
```

若要終止多個叢集，請輸入下列命令，並使用叢集 ID 取代 *j-3KVXXXXXXX7UG* 和 *j-WJ2XXXXXX8EU*。

```
aws emr terminate-clusters --cluster-ids j-3KVXXXXXXX7UG j-WJ2XXXXXX8EU
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用 API 終止叢集

`TerminateJobFlows` 操作會結束步驟處理，將任何日誌資料從 Amazon EC2 上傳至 Amazon S3 (如有設定)，並終止 Hadoop 叢集。如果您在 `KeepJobAliveWhenNoSteps` 請求中將 `False` 設為 `RunJobFlows`，叢集會自動終止。

您可以使用此動作來依叢集 ID 終止單一叢集或叢集清單。

如需 `TerminateJobFlows` 唯一輸入參數的詳細資訊，請參閱 [TerminateJobFlows](#)。如需一般請求參數的詳細資訊，請參閱 [常見的請求參數](#)。

調整叢集資源規模

您可以自動或手動調整提供給 EMR 叢集使用的 Amazon EC2 執行個體數量以應對不同需求的工作負載。以下是可用的選項：

- 使用 Amazon EMR 4.x 版和更新版本，在首次建立核心執行個體群組和任務執行個體群組時或在叢集執行後，即可將其設定為自動調整規模。Amazon EMR 會自動根據您指定的規則設定 Auto Scaling 參數，接著根據 CloudWatch 指標新增和移除執行個體。
- 您可以手動新增或移除 Amazon EC2 執行個體，藉此調整核心執行個體群組和任務執行個體群組。
- 可將任務執行個體群組新增至叢集。

僅有在首次設定執行個體群組時，才能指定 Amazon EC2 執行個體的類型，因此 Amazon EC2 執行個體類型只能以新增任務的方式變更。使用 Amazon EMR 5.1.0 版或更新版本時，您可以指定自叢集移出的 Amazon EC2 執行個體是否要在執行個體該小時的範圍內終止，或是要在 Amazon EC2 執行個體上的任務完成時終止，此設定會套用到整個叢集上。如需詳細資訊，請參閱 [縮小叢集 \(p. 303\)](#)。

在決定選用本節所介紹的規模調整方式前，需先認識一些重要概念。首先要了解的是節點類型在 EMR 叢集中的功用，以及如何運用執行個體群組管理節點。如需節點類型功能的詳細資訊，請參閱 [什麼是 Amazon EMR？](#)，而如需執行個體群組的詳細資訊，請參閱 [執行個體群組](#)。也請根據工作負載的性質制定策略，將叢集資源調整為適當的規模。如需詳細資訊，請參閱 [叢集組態指導方針](#)。

Note

EMR 叢集中主要執行個體群組一律由單一節點或三個主節點組成，因此無法在您初次設定完畢後進行擴展。您要以核心執行個體群組和任務執行個體群組來調整叢集的規模。叢集可以只有主節點，而完全沒有核心或任務節點。您在建立叢集時必須至少有一個核心節點，以便調整叢集的規模。換言之，單一節點叢集無法調整大小。

重新設定執行個體群組與調整其大小無法同時發生。如果在調整執行個體群組大小時起啟重新設定，則直到執行個體群組完成大小調整後，才能開始重新設定，反之亦然。

主題

- 於 Amazon EMR 使用自動調整規模 (p. 291)
- 手動調整執行中的叢集規模 (p. 298)
- 縮小叢集 (p. 303)

於 Amazon EMR 使用自動調整規模

Amazon EMR 4.0 版及更新版本具有自動調整規模功能，可根據 CloudWatch 指標或是您在 擴展政策 中所指定的其他參數，以程式設計方式向外擴展或向內擴展核心節點和任務節點。使用執行個體群組設定時可自動調整規模，但在使用執行個體機群時即無法自動調整。如需執行個體群組和執行個體機群的詳細資訊，請參閱 [使用執行個體機群或統一執行個體群組建立叢集 \(p. 104\)](#)。

Note

若要在 Amazon EMR 中使用自動調整規模功能，您必須在建立叢集時保留 `VisibleToAllUsers` 參數的預設設定 `true`。如需詳細資訊，請參閱 [SetVisibleToAllUsers](#)。

擴展政策屬於執行個體群組設定的一部分。您可以在初次設定執行個體群組時指定政策，或是修改既有叢集中的執行個體群組，即使執行個體群組處於使用中的狀態也無妨。除了主要執行個體群組織外，每個叢集中的執行個體群組均能擁有屬於自己的擴展政策，包含橫向擴展和縮減規則。橫向擴充和縮減的規則可分開設定，每項規則均有不同的參數。

您可使用 AWS Management Console、AWS CLI 或 Amazon EMR API 設定擴展政策。使用 AWS CLI 或 Amazon EMR API 時，要以 JSON 格式指定擴展政策。此外，使用 AWS CLI 或 Amazon EMR API 時，可指定自訂的 CloudWatch 指標。使用 AWS Management Console 時無法選擇自訂指標。初次使用主控台建立擴展政策時，系統會預先設定好多數應用程式適用的預設政策，以協助您開始使用。這些預設規則均可刪除或修改。

即使自動調整規模可在不停機的狀態下調整 EMR 叢集容量，仍應考量基準工作負載需求並妥善規劃您的節點和執行個體群組設定。如需詳細資訊，請參閱 [叢集組態指導方針](#)。

Note

對於大多數的工作負載而言，最好橫向縮減和橫向擴充兩方規則均要設定，以達到最佳的資源使用效果。若設定規則時少了其中一項，即代表必須在擴展活動後再手動重新調整執行個體的數量。換言之，如此設定的是「單向」的自動橫向擴展或縮減政策，且需手動重新設定。

建立自動調整規模的 IAM 角色

Amazon EMR 中的自動調整規模功能需要具有許可的 IAM 角色，方可在觸發擴展活動時新增和終止執行個體。預設角色 `EMR_AutoScaling_DefaultRole` 已設定好合適的角色政策和信任政策，可用於此目的。首次使用 AWS Management Console 以擴展政策建立叢集時，Amazon EMR 會建立預設的角色，並附加上預設的受管政策 `AmazonElasticMapReduceforAutoScalingRole` 以獲得許可。

使用 AWS CLI 建立含有自動調整規模政策的叢集時，必須先確保預設的 IAM 角色是否存在，或者是否具有自訂的 IAM 角色，且需附有能夠提供適當許可的政策。若要建立預設角色，可在建立叢集前先執行 `create-default-roles` 命令。也可以在建立叢集時指定 `--auto-scaling-role` `EMR_AutoScaling_DefaultRole` 選項。或者可以建議自訂的自動調整規模角色，再於建立叢集時指定該角色，例如 `--auto-scaling-role` `MyEMRAutoScalingRole`。若您替 Amazon EMR 建立的自訂的自動擴展角色，建議您根據受管政策替您的自訂角色建立基本的許可政策。如需更多詳細資訊，請參閱 [將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。

了解自動調整規模規則

當橫向擴充規則觸發執行個體群組的擴展活動時，會根據您的規則，將 Amazon EC2 執行個體新增至執行個體群組中。待 Amazon EC2 執行個體進入 `InService` 狀態後，Apache Spark 及 Apache Hive 這類應用程式即可使用新節點。您也可以設定橫向縮減規則，用於終止執行個體和移除節點。如需可自動調整規模的 Amazon EC2 執行個體詳細資訊，請參閱 Amazon EC2 Auto Scaling User Guide 中的 [Auto Scaling 生命週期](#)。

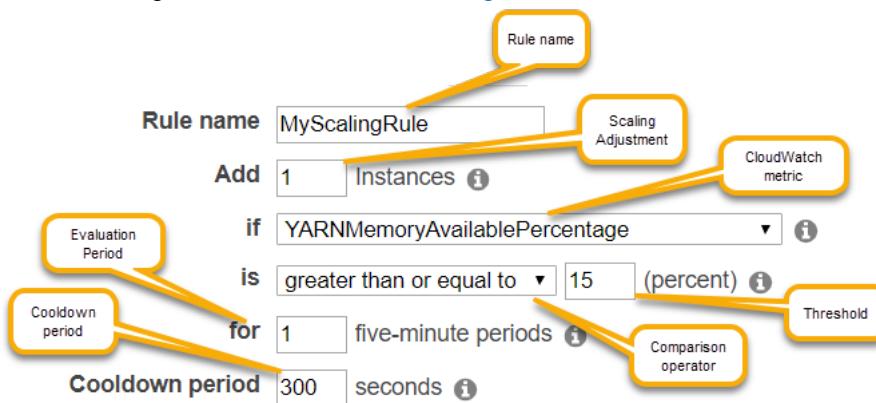
您可以設定叢集終止 Amazon EC2 執行個體的方式。可選擇要在 Amazon EC2 執行個體每小時計價的範圍內終止執行個體，還是在任務完成時再終止。此設定會套用至自動調整規模和手動重新調整兩邊的操作上。如需此組態的詳細資訊，請參閱「[縮小叢集 \(p. 303\)](#)」。

以下是政策中每條規則用於決定自動調整規模行為的參數。

Note

此處所列的參數是根據 Amazon EMR 的 AWS Management Console。使用 AWS CLI 或 Amazon EMR API 時，會有更多進階設定選項可供使用。如需進階選項的詳細資訊，請參閱 Amazon EMR API Reference 中的 [SimpleScalingPolicyConfiguration](#)。

- 執行個體上限與執行個體下限。Maximum instances (執行個體上限) 這項限制所指定的是可在執行個體群組中存在的 Amazon EC2 執行個體最大數量，會套用至所有向外擴展規則。同樣地，Minimum instances (執行個體下限) 限制指定了 Amazon EC2 執行個體的最小數量，也會套用至所有向內擴展規則。
- Rule name (規則名稱)，在政策內必須是唯一的。
- scaling adjustment (規模調整) 會決定受到規則觸發的擴展活動所要新增 (向外擴展規則) 或終止 (向內擴展規則) 的 EC2 執行個體數量。
- CloudWatch metric (CloudWatch 指標)，用於監看警示條件。
- comparison operator (比較運算子)，用於將 CloudWatch 指標與 Threshold (閾值) 的值進行比較，判定觸發的條件。
- evaluation period (評估時間)，以五分鐘為單位遞增，CloudWatch 指標必須在此段時間內處於觸發條件之下，才會觸發擴展活動。
- Cooldown period (冷卻時間) 會決定在某條規則觸發擴展活動後，需經過多久才可開始下一次的觸發活動，不論活動是由哪一條規則觸發。當執行個體群組結束了擴展活動，且達到了後期擴展狀態，冷卻時間會提供機會給可能觸發後續擴展活動的 CloudWatch 指標，以使之穩定。如需詳細資訊，請參閱 Amazon EC2 Auto Scaling User Guide 中的 [Auto Scaling 冷卻](#)。



使用 AWS Management Console 設定自動調整規模

當您建立叢集時，會使用進階叢集設定選項來設定執行個體群組的規模調整政策。您也可以在既有叢集的 Hardware (硬體) 設定中修改執行個體群組，藉此建立或修改服務中的執行個體群組的擴展政策。

1. 若您要建立叢集，請在 Amazon EMR 主控台選擇 Create Cluster (建立叢集)，選取 Go to advanced options (前往進階選項)，選擇 Step 1: Software and Steps (步驟 1：軟體和步驟) 的選項，接著前往 Step 2: Hardware Configuration (步驟 2：硬體組態)。

—或—

若您要修改執行中叢集內的執行個體群組，請在叢集清單中選取您的叢集，再展開 Hardware (硬體) 區段。

2. 請按一下您要設定的執行個體群組 Auto Scaling 欄位上的鉛筆圖示。若已經為該執行個體群組設定了自動調整規模政策，Maximum instances (執行個體上限) 和 Minimum instances (執行個體下限) 的數量會出現在此欄中，若未設定則會顯示 Not enabled (未啟用)。
會開啟 Auto Scaling 規則畫面。系統會預設選取 Scale out (向外擴展) 和 Scale in (向內擴展)，且會先設定好預設規則，採用適合大多數應用程式的設定。
3. 請輸入您希望執行個體群組在向外擴展完畢後的 Maximum instances (執行個體上限)，以及在向內擴展後的 Minimum instances (執行個體下限)。
4. 請按一下鉛筆圖示以編輯規則參數，按一下 X 可從政策中移除該條規則，按一下 Add rule (新增規則) 則可增加更多規則。
5. 按本主題之前的說明，選擇規則參數。如需 Amazon EMR 可用的 CloudWatch 指標之說明，請參閱 Amazon CloudWatch User Guide 中的 [Amazon EMR 指標與維度](#)。

使用 AWS CLI 設定自動調整規模

建立叢集和執行個體群組時，您可以使用 Amazon EMR 的 AWS CLI 命令設定自動調整規模功能。可使用速記語法來指定相關命令中內嵌的 JSON 組態，或是以含有組態 JSON 的檔案做為參照。您也可以將自動調整規模的政策套用到既有的執行個體群組上，並移除先前套用的自動調整規模政策。此外還能從執行中的叢集上擷取調整規模政策組態的詳細資訊。

Important

建立具有自動調整規模政策的叢集時，必須使用 `--auto-scaling-role MyAutoScalingRole` 命令指定自動調整規模所用的 IAM 角色。預設角色為 `EMR_AutoScaling_DefaultRole`，可由 `create-default-roles` 命令建立。該角色只能在建立叢集時新增，且無法新增至既有的叢集。

如需設定自動調整規模政策時可用的參數說明，請參閱 Amazon EMR API Reference 中的 [PutAutoScalingPolicy](#)。

建立內含套用至執行個體群組之自動調整規模政策的叢集

也可以在 `--instance-groups` 命令的 `aws emr create-cluster` 選項中指定自動調整規模的設定。以下範例所說明的建立叢集命令中，是以內嵌方式提供核心執行個體群組的自動調整規模政策。此命令所建立的調整規模設定，等同於使用 Amazon EMR 之 AWS Management Console 時出現的預設向外擴展政策。為了簡潔之故，不會顯示縮減政策。不建議建立不含縮減規則的横向擴展規則。

```
aws emr create-cluster --release-label emr-5.2.0 --service-role EMR_DefaultRole --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole --auto-scaling-role EMR_AutoScaling_DefaultRole --instance-groups 'Name=MyMasterIG,InstanceGroupType=MASTER,InstanceType=m5.xlarge,InstanceCount=1' 'Name=MyCoreIG,InstanceGroupType=CORE,InstanceType=m5.xlarge,InstanceCount=2,AutoScalingPolicy={Constraints=[{scale-out,Description=Replicates the default scale-out rule in the console.},Action={SimpleScalingPolicyConfiguration={AdjustmentType=CHANGE_IN_CAPACITY,ScalingAdjustmentType=CHANGE_IN_CAPACITY,ElasticMapReduce,Period=300,Statistic=AVERAGE,Threshold=15,Unit=PERCENT,Dimensions=[{Key=JobFlowId,Value=your-job-flow-id}],MetricName=CPUUtilization}],MinCapacity=2,MaxCapacity=2,DesiredCapacity=2,Status=ENABLED}}'
```

以下命令所顯示的是，使用命令列將自動調整規模政策的定義當做執行個體群組組態檔案 (名稱為 `instancegroupconfig.json`) 的一部分，以此方式來提供該定義。

```
aws emr create-cluster --release-label emr-5.2.0 --service-role EMR_DefaultRole --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole --instance-groups file://your/path/to/instancegroupconfig.json --auto-scaling-role EMR_AutoScaling_DefaultRole
```

組態檔案的內容如下所示：

```
[  
{  
    "InstanceCount": 1,  
    "Name": "MyMasterIG",  
    "InstanceGroupType": "MASTER",  
    "InstanceType": "m5.xlarge"  
},  
{  
    "InstanceCount": 2,  
    "Name": "MyCoreIG",  
    "InstanceGroupType": "CORE",  
    "InstanceType": "m5.xlarge",  
    "AutoScalingPolicy":  
    {  
        "Constraints":  
        {  
            "MinCapacity": 2,  
            "MaxCapacity": 10  
        },  
        "Rules":  
        [  
            {  
                "Name": "Default-scale-out",  
                "Description": "Replicates the default scale-out rule in the console for YARN  
memory.",  
                "Action":{  
                    "SimpleScalingPolicyConfiguration":{  
                        "AdjustmentType": "CHANGE_IN_CAPACITY",  
                        "ScalingAdjustment": 1,  
                        "CoolDown": 300  
                    }  
                },  
                "Trigger":{  
                    "CloudWatchAlarmDefinition":{  
                        "ComparisonOperator": "LESS_THAN",  
                        "EvaluationPeriods": 1,  
                        "MetricName": "YARNMemoryAvailablePercentage",  
                        "Namespace": "AWS/ElasticMapReduce",  
                        "Period": 300,  
                        "Threshold": 15,  
                        "Statistic": "AVERAGE",  
                        "Unit": "PERCENT",  
                        "Dimensions": [  
                            {  
                                "Key" : "JobFlowId",  
                                "Value" : "${emr.clusterId}"  
                            }  
                        ]  
                    }  
                }  
            }  
        ]  
    }  
}]
```

將含有自動調整規模政策的執行個體群組新增至叢集內

可以使用 `--instance-groups` 選項搭配 `add-instance-groups` 命令來指定擴展政策組態，方式與使用 `create-cluster` 時相同。以下範例參考的是 JSON 檔案 `instancegroupconfig.json`，搭配執行個體群組的組態。

```
aws emr add-instance-groups --cluster-id j-1EKZ3TYEVF1S2 --instance-groups file://your/path/to/instancegroupconfig.json
```

將自動調整規模政策套用到既有的執行個體群組上，或修改所套用的政策

請使用 `aws emr put-auto-scaling-policy` 指定將自動調整規模政策套用到既有的執行個體群組上。該執行個體群組必須屬於某個使用自動調整規模 IAM 角色的叢集。以下範例參考的是 JSON 檔案 `autoscaleconfig.json`，該檔案指定了自動調整規模政策的組態。

```
aws emr put-auto-scaling-policy --cluster-id j-1EKZ3TYEVF1S2 --instance-group-id ig-3PLUZBA6WLS07 --auto-scaling-policy file://your/path/to/autoscaleconfig.json
```

`autoscaleconfig.json` 檔案的內容所定義的橫向擴展規則與上個範例相同，如下所示。

```
[{
  "AutoScalingPolicy": {
    "Constraints": {
      "MinCapacity": 2,
      "MaxCapacity": 10
    },
    "Rules": [
      {
        "Name": "Default-scale-out",
        "Description": "Replicates the default scale-out rule in the console for YARN memory.",
        "Action": {
          "SimpleScalingPolicyConfiguration": {
            "AdjustmentType": "CHANGE_IN_CAPACITY",
            "ScalingAdjustment": 1,
            "CoolDown": 300
          }
        },
        "Trigger": {
          "CloudWatchAlarmDefinition": {
            "ComparisonOperator": "LESS_THAN",
            "EvaluationPeriods": 1,
            "MetricName": "YARNMemoryAvailablePercentage",
            "Namespace": "AWS/ElasticMapReduce",
            "Period": 300,
            "Threshold": 15,
            "Statistic": "AVERAGE",
            "Unit": "PERCENT",
            "Dimensions": [
              {
                "Key": "JobFlowId",
                "Value": "${emr.clusterId}"
              }
            ]
          }
        }
      }
    ]
  }
}]
```

將自動調整規模政策自執行個體群組中移除

```
aws emr remove-auto-scaling-policy --cluster-id j-1EKZ3TYEVF1S2 --instance-group-id ig-3PLUZBA6WLS07
```

擷取自動調整規模政策的組態

`describe-cluster` 命令會擷取 InstanceGroup 區塊中的政策組態。舉例而言，以下命令會擷取叢集 ID 為 `j-1CWOHP4PI30VJ` 的叢集的組態。

```
aws emr describe-cluster --cluster-id j-1CWOHP4PI30VJ
```

該命令會產生以下的輸出範例。

```
{  
    "Cluster": {  
        "Configurations": [],  
        "Id": "j-1CWOHP4PI30VJ",  
        "NormalizedInstanceHours": 48,  
        "Name": "Auto Scaling Cluster",  
        "ReleaseLabel": "emr-5.2.0",  
        "ServiceRole": "EMR_DefaultRole",  
        "AutoTerminate": false,  
        "TerminationProtected": true,  
        "MasterPublicDnsName": "ec2-54-167-31-38.compute-1.amazonaws.com",  
        "LogUri": "s3n://aws-logs-232939870606-us-east-1/elasticmapreduce/",  
        "Ec2InstanceAttributes": {  
            "Ec2KeyName": "performance",  
            "AdditionalMasterSecurityGroups": [],  
            "AdditionalSlaveSecurityGroups": [],  
            "EmrManagedSlaveSecurityGroup": "sg-09fc9362",  
            "Ec2AvailabilityZone": "us-east-1d",  
            "EmrManagedMasterSecurityGroup": "sg-0bfc9360",  
            "IamInstanceProfile": "EMR_EC2_DefaultRole"  
        },  
        "Applications": [  
            {  
                "Name": "Hadoop",  
                "Version": "2.7.3"  
            }  
        ],  
        "InstanceGroups": [  
            {  
                "AutoScalingPolicy": {  
                    "Status": {  
                        "State": "ATTACHED",  
                        "StateChangeReason": {  
                            "Message": ""  
                        }  
                    },  
                    "Constraints": {  
                        "MaxCapacity": 10,  
                        "MinCapacity": 2  
                    },  
                    "Rules": [  
                        {  
                            "Name": "Default-scale-out",  
                            "Trigger": {  
                                "CloudWatchAlarmDefinition": {  
                                    "MetricName": "YARNMemoryAvailablePercentage",  
                                    "Unit": "PERCENT",  
                                    "Namespace": "AWS/ElasticMapReduce",  
                                    "Threshold": 15,  
                                    "Dimensions": [  
                                        {  
                                            "Key": "JobFlowId",  
                                            "Value": "j-1CWOHP4PI30VJ"  
                                        }  
                                    ]  
                                }  
                            }  
                        }  
                    ]  
                }  
            }  
        ]  
    }  
}
```

```
        "Value": "j-1CWOHP4PI30VJ"
    }
],
"EvaluationPeriods": 1,
"Period": 300,
"ComparisonOperator": "LESS_THAN",
"Statistic": "AVERAGE"
}
},
"Description": "",
"Action": {
    "SimpleScalingPolicyConfiguration": {
        "CoolDown": 300,
        "AdjustmentType": "CHANGE_IN_CAPACITY",
        "ScalingAdjustment": 1
    }
}
},
{
    "Name": "Default-scale-in",
    "Trigger": {
        "CloudWatchAlarmDefinition": {
            "MetricName": "YARNMemoryAvailablePercentage",
            "Unit": "PERCENT",
            "Namespace": "AWS/ElasticMapReduce",
            "Threshold": 75,
            "Dimensions": [
                {
                    "Key": "JobFlowId",
                    "Value": "j-1CWOHP4PI30VJ"
                }
            ],
            "EvaluationPeriods": 1,
            "Period": 300,
            "ComparisonOperator": "GREATER_THAN",
            "Statistic": "AVERAGE"
        }
    },
    "Description": "",
    "Action": {
        "SimpleScalingPolicyConfiguration": {
            "CoolDown": 300,
            "AdjustmentType": "CHANGE_IN_CAPACITY",
            "ScalingAdjustment": -1
        }
    }
}
]
},
"Configurations": [],
"InstanceType": "m5.xlarge",
"Market": "ON_DEMAND",
"Name": "Core - 2",
"ShrinkPolicy": {},
"Status": {
    "Timeline": {
        "CreationDateTime": 1479413437.342,
        "ReadyDateTime": 1479413864.615
    },
    "State": "RUNNING",
    "StateChangeReason": {
        "Message": ""
    }
},
"RunningInstanceCount": 2,
"Id": "ig-3M16XBE8C3PH1",
```

```
        "InstanceGroupType": "CORE",
        "RequestedInstanceCount": 2,
        "EbsBlockDevices": []
    },
    {
        "Configurations": [],
        "Id": "ig-OP62I28NSE8M",
        "InstanceGroupType": "MASTER",
        "InstanceType": "m5.xlarge",
        "Market": "ON_DEMAND",
        "Name": "Master - 1",
        "ShrinkPolicy": {},
        "EbsBlockDevices": [],
        "RequestedInstanceCount": 1,
        "Status": {
            "Timeline": {
                "CreationDateTime": 1479413437.342,
                "ReadyDateTime": 1479413752.088
            },
            "State": "RUNNING",
            "StateChangeReason": {
                "Message": ""
            }
        },
        "RunningInstanceCount": 1
    }
],
"AutoScalingRole": "EMR_AutoScaling_DefaultRole",
"Tags": [],
"BootstrapActions": [],
"Status": {
    "Timeline": {
        "CreationDateTime": 1479413437.339,
        "ReadyDateTime": 1479413863.666
    },
    "State": "WAITING",
    "StateChangeReason": {
        "Message": "Cluster ready after last step completed."
    }
}
}
```

手動調整執行中的叢集規模

您可使用 AWS Management Console、AWS CLI 或 Amazon EMR API，將執行個體新增到執行中叢集的核心及任務執行個體群組以及執行個體機群內，或是從中移出。若叢集使用的是執行個體群組，您要明確地變更執行個體數量。若叢集使用的是執行個體機群，您可以將目標單位變更為隨需執行個體和 Spot 執行個體。接著執行個體機群會新增和移除執行個體，以符合新目標。如需更多詳細資訊，請參閱 [執行個體機群選項 \(p. 105\)](#)。只要執行個體可供使用，應用程式便可使用新佈建的 Amazon EC2 執行個體來代管節點。當執行個體遭移除時，Amazon EMR 會以不會對工作造成干擾的方式來終止任務，並避免資料遺失。如需更多詳細資訊，請參閱 [於任務完成時終止 \(p. 303\)](#)。

使用主控台調整叢集規模

可使用 Amazon EMR 主控台調整執行中叢集的大小。

使用主控台變更既有執行中叢集的執行個體數量

1. 在 Cluster List (叢集清單) 頁面上，選擇要調整規模的叢集。

2. 在 Cluster Details (叢集詳細資訊) 頁面，選擇 Hardware (硬體)。
3. 如果您的叢集使用的是執行個體群組，請在想要調整的執行個體群組的 Instance count (執行個體計數) 一欄中，選擇 Resize (調整)，並輸入新的執行個體數量，再選擇綠色勾號。

ID	Status	Node type & name	Instance type	Instance count
MASTER	Running	Master - 1	m3.xlarge 8 vCore, 15 GiB memory, 80 SSD GB storage EBS Storage: none	1 Instances
CORE	Running	Core - 2	m3.xlarge 8 vCore, 15 GiB memory, 80 SSD GB storage EBS Storage: none	1 Instances
TASK	Running	Task - 3	m3.xlarge 8 vCore, 15 GiB memory, 80 SSD GB storage EBS Storage: none	1 Instances

-OR-

若您的叢集使用的是執行個體機群，請選擇 Provisioned capacity (佈建容量) 一欄內的 Resize (調整)，在 On-demand units (隨需單位) 和 Spot units (Spot 單位) 中輸入新值，再選擇 Resize (調整)。

ID	Status	Node type & name	Fleet instance types	Provisioned capacity	Advanced Spot
MASTER	Running	Master - 1	m4.large 4 vCore, 8 GiB memory, EBS only storage EBS Storage: 32 GiB Maximum Spot price: 100 % of On-demand price Each instance counts as 1 units	1 On-demand units 0 Spot units 1 Total units	Defined duration None
CORE	Running (2 On Demand Requested)	Core - 2	m4.large 4 vCore, 8 GiB memory, EBS only storage EBS Storage: 32 GiB Maximum Spot price: 100 % of On-demand price Each instance counts as 4 units	4 On-demand units 4 Spot units 8 Total units	Provisioning time After 60 minutes Instances

變更節點數量時，執行個體群組的 Status (狀態) 也會更新。提出的變更完成時，Status (狀態) 為 Running (執行中)。

使用 AWS CLI 調整叢集規模

可使用 AWS CLI 調整執行中叢集的大小。您可以增加或減少任務節點的數量，並可增加執行中叢集的核心節點數量。也可以使用 AWS CLI 或 API 終止核心執行個體群組內的執行個體。此動作請務必謹慎進行。終止核心執行個體群組中的執行個體，會導致資料遺失的風險，且不會自動替換執行個體。

除了調整核心和任務群組的規模外，也可以使用 AWS CLI，將一個或更多個執行個體群組新增至執行中的叢集。

使用 AWS CLI 變更執行個體數量以調整叢集規模

您可以使用 AWS CLI `modify-instance-groups` 子命令搭配 `InstanceCount` 參數新增執行個體到核心群組或任務群組中，並從任務群組中移除執行個體。若要將執行個體新增至核心群組或任務群組，請提高 `InstanceCount`。若要減少任務群組中執行個體的數量，則降低 `InstanceCount`。將任務群組中執行個體的數量變更為 0，即會移除所有執行個體，但不會移除執行個體群組。

- 若要將任務執行個體群組的執行個體數量從 3 增加為 4，請輸入以下命令，並將 `ig-31JXXXXXXBTO` 替換為執行個體群組的 ID。

```
aws emr modify-instance-groups --instance-groups  
  InstanceGroupId=ig-31JXXXXXXBTO, InstanceCount=4
```

若要取得 `InstanceGroupId`，請使用 `describe-cluster` 子命令。在名為 `Cluster` 的 JSON 物件的輸出結果中，含有各個執行個體群組的 ID。若要使用此命令，您需要叢集 ID (可使用 `aws emr list-clusters` 命令或使用主控台取得)。若要取得執行個體群組 ID，請輸入以下命令，並將 `j-2AXXXXXXGAPLF` 改為叢集 ID。

```
aws emr describe-cluster --cluster-id j-2AXXXXXXGAPLF
```

使用 AWS CLI 時，您也可以藉由 `--modify-instance-groups` 子命令終止核心執行個體群組中的執行個體。

Warning

指定 `EC2InstanceIdsToTerminate` 時請務必小心謹慎。不論在執行個體上執行的應用程式處於何種狀態，執行個體都會立即終止，且不會自動更換執行個體。無論叢集的 Scale down behavior (縮減規模行為) 設定為何，均會如此。以此種方式終止執行個體，可能會導致資料損失，叢集也可能會出現意料外的行為。

若要終止特定的執行個體，則需要執行個體群組 ID (由 `aws emr describe-cluster --cluster-id` 子命令傳回) 和執行個體 ID (由 `aws emr list-instances --cluster-id` 子命令傳回)，請輸入以下命令並將 `ig-6RXXXXXX07SA` 改為執行個體群組 ID，`i-f9XXXXf2` 改為執行個體 ID。

```
aws emr modify-instance-groups --instance-groups  
  InstanceGroupId=ig-6RXXXXXX07SA, EC2InstanceIdsToTerminate=i-f9XXXXf2
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用 AWS CLI 新增任務執行個體群組以調整叢集規模

使用 AWS CLI 時，可以使用 `--add-instance-groups` 子命令，將 1 – 48 個任務執行個體群組新增至叢集。任務執行個體群組僅能新增到內有主要執行個體群組和核心執行個體群組的叢集內。使用 AWS CLI 時，每使用一次 `--add-instance-groups` 子命令最多可新增五個任務執行個體群組。

- 若要在叢集中新增單個任務執行個體群組，請輸入以下命令，並將 `j-JXBXXXXXX37R` 改為叢集 ID。

```
aws emr add-instance-groups --cluster-id j-JXBXXXXXX37R --instance-groups  
  InstanceCount=6,InstanceGroupType=task,InstanceType=m5.xlarge
```

2. 若要在叢集中新增多個任務執行個體群組，請輸入以下命令，並將 **j-JXBXXXXXX37R** 改為叢集 ID。一個命令最多可新增五個任務執行個體群組。

```
aws emr add-instance-groups --cluster-id j-JXBXXXXXX37R --instance-groups  
  InstanceCount=6,InstanceGroupType=task,InstanceType=m5.xlarge  
  InstanceCount=10,InstanceGroupType=task,InstanceType=m5.xlarge
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

中斷調整規模

若使用的是 Amazon EMR 4.1.0 版或更新版本，您可以在執行既有調整規模的操作途中，再次提出調整規模的請求。此外您也可以停止先前提出的調整規模請求，或是提交新的請求來覆寫上一次的請求，而不需等待操作進行完畢。也可以透過主控台停止既有的調整規模操作，或使用 `ModifyInstanceGroups` API 呼叫，將目前的數量做為叢集的目標數量。

以下螢幕截圖顯示的是正在調整規模的任務執行個體群組，選擇 Stop (停止) 即可停止調整規模。



使用 AWS CLI 中斷調整規模

您可以使用 AWS CLI，透過 `modify-instance-groups` 子命令停止調整規模。假設您的執行個體群組中有六個執行個體，而您想將數量新增到 10。您稍後決定要取消此請求：

- 最初的請求：

```
aws emr modify-instance-groups --instance-groups  
  InstanceGroupId=ig-myInstanceId,InstanceCount=10
```

停止第一個請求的第二個請求：

```
aws emr modify-instance-groups --instance-groups  
  InstanceGroupId=ig-myInstanceId,InstanceCount=6
```

Note

由於此程序並非同步進行，您可以看到執行後續請求之前 API 請求的執行個體變更數量。若是縮減的情況，則節點尚可能還有工作在執行，執行個體群組會等到節點工作完成後再進行縮減。

阻擋狀態

若執行個體群組在嘗試啟動新的叢集節點時，發生太多錯誤，即會進入阻擋狀態。舉例而言，若新節點執行引導操作時失敗，執行個體群組便會進入 ARRESTED (阻擋) 狀態，而不會繼續佈建新節點。在您解決根本的問題後，請重設叢集執行個體的所需數量，執行個體群組便會重新開始分配節點。修改執行個體群組的動作會命令 Amazon EMR 嘗試再度佈建節點。執行中的節點不會重新啟動或遭到終止。

在 AWS CLI 中，`list-instances` 子命令會傳回所有執行個體和其狀態，`describe-cluster` 亦是如此。若 Amazon EMR 偵測到執行個體群組出現錯誤，其會將群組的狀態變更為 ARRESTED。

使用 AWS CLI 重設在 ARRESTED (阻擋) 狀態下的叢集

請輸入 `describe-cluster` 子命令和 `--cluster-id` 參數，以檢視叢集中執行個體的狀態。

- 若要檢視叢集中所有執行個體和執行個體群組的資訊，請輸入以下命令，並將 `j-3KVXXXXXXXXY7UG` 改為叢集 ID。

```
aws emr describe-cluster --cluster-id j-3KVXXXXXXXXY7UG
```

輸出結果會顯示您的執行個體群組和執行個體的狀態：

```
{  
    "Cluster": {  
        "Status": {  
            "Timeline": {  
                "ReadyDateTime": 1413187781.245,  
                "CreationDateTime": 1413187405.356  
            },  
            "State": "WAITING",  
            "StateChangeReason": {  
                "Message": "Waiting after step completed"  
            }  
        },  
        "Ec2InstanceAttributes": {  
            "Ec2AvailabilityZone": "us-west-2b"  
        },  
        "Name": "Development Cluster",  
        "Tags": [],  
        "TerminationProtected": false,  
        "RunningAmiVersion": "3.2.1",  
        "NormalizedInstanceHours": 16,  
        "InstanceGroups": [  
            {  
                "RequestedInstanceCount": 1,  
                "Status": {  
                    "Timeline": {  
                        "ReadyDateTime": 1413187775.749,  
                        "CreationDateTime": 1413187405.357  
                    },  
                    "State": "RUNNING",  
                    "StateChangeReason": {  
                        "Message": ""  
                    }  
                },  
                "Name": "MASTER",  
                "InstanceGroupType": "MASTER",  
                "InstanceType": "m5.xlarge",  
                "Id": "ig-3ETXXXXXXFYV8",  
                "Market": "ON_DEMAND",  
                "RunningInstanceCount": 1  
            },  
            {  
                "RequestedInstanceCount": 1,  
                "Status": {  
                    "Timeline": {  
                        "ReadyDateTime": 1413187781.301,  
                        "CreationDateTime": 1413187405.357  
                    },  
                    "State": "RUNNING",  
                    "StateChangeReason": {  
                        "Message": ""  
                    }  
                },  
                "Name": "CORE",  
                "InstanceGroupType": "CORE",  
                "InstanceType": "m5.xlarge",  
                "Id": "ig-3ETXXXXXXFYV9",  
                "Market": "ON_DEMAND",  
                "RunningInstanceCount": 1  
            }  
        ]  
    }  
}
```

```
"Name": "CORE",
"InstanceGroupType": "CORE",
"InstanceType": "m5.xlarge",
"Id": "ig-3SUXXXXXXXQ9ZM",
"Market": "ON_DEMAND",
"RunningInstanceCount": 1
}
...
}
```

若要檢視特定執行個體群組的資訊，請輸入 `list-instances` 子命令和 `--cluster-id` 及 `--instance-group-types` 的參數。您可以檢視 MASTER、CORE、TASK 群組的資訊。

```
aws emr list-instances --cluster-id j-3KVXXXXXXY7UG --instance-group-types "CORE"
```

請使用 `modify-instance-groups` 子命令搭配 `--instance-groups` 參數來重設 ARRESTED 狀態下的叢集。`describe-cluster` 子命令會傳回執行個體群組的 ID。

```
aws emr modify-instance-groups --instance-groups
InstanceId=ig-3SUXXXXXXXQ9ZM,InstanceCount=3
```

縮小叢集

Amazon EMR 5.1.0 版和更新版本中，有兩種縮減行為的選項：於執行個體每小時 Amazon EC2 計價範圍內終止，或於任務完成時終止。自 Amazon EMR 5.10.0 版開始，因為在 Amazon EC2 內引進了每秒計費的功能，已淘汰在執行個體每小時範圍內終止的設定。若版本中有在執行個體每小時範圍內終止的選項，也不建議指定該選項。

Warning

若您是使用 AWS CLI 提出 `modify-instance-groups` 和 `EC2InstanceIdsToTerminate`，這類執行個體會立即終止，不會考量到此類設定，也不會受其上執行的應用程式狀態影響。以此種方式終止執行個體，可能會導致資料損失，叢集也可能會出現意料外的行為。

若指定在任務完成時終止，Amazon EMR 會封鎖並耗盡節點上的任務，再終止 Amazon EC2 執行個體。不論指定的是哪一種行為，若可能導致 HDFS 損壞，Amazon EMR 都不會終止核心執行個體群組中的 Amazon EC2 執行個體。

於任務完成時終止

Amazon EMR 可以在不影響工作負載的情況下，將您的叢集縮小。在調整期間，Amazon EMR 會逐漸將核心和任務節點上的 YARN、HDFS 以及其他協助程式淘汰，而不會導致資料遺失或中斷工作進行。Amazon EMR 僅會在指派給執行個體群組的工作已完成且處於閒置狀態時，再將執行個體群組縮小。若是要將 YARN NodeManager 除役，您可以手動調整節點等待除役的時間。

可使用 `yarn-site` 組態分類內的屬性來加以設定。若使用的是 Amazon EMR 5.12.0 版或更新版本，請指定 `yarn.resourcemanager.nodemanager-graceful-decommission-timeout-secs` 屬性。若使用的是更早期的 Amazon EMR 版本，請指定 `yarn.resourcemanager.decommissioning.timeout` 屬性。

若在除役逾時時間過去後，仍有執行中的 YARN 應用程式，則節點會遭到強制除役，而 YARN 會將受影響的容器重新安排到其他節點上。預設值為 3600 秒 (1 小時)。您可以將逾時時間隨意設為較高的值，強迫等待較長時間再逐漸縮減。如需詳細資訊，請參閱 Apache Hadoop 文件中的 [Graceful Decommission of YARN Nodes](#)。

任務節點群組

Amazon EMR 會以智慧方式挑選並未執行與任何步驟或應用程式相關任務的執行個體，並先從叢集中移除。若叢集中所有執行個體均在使用中，Amazon EMR 會等待指定執行個體上的任務完成，再從叢集中將其移除。預設等待時間為 1 小時，此值可於設定 `yarn.resourcemanager.decommissioning.timeout` 變更。Amazon EMR 會動態使用新設定。您可以將之隨意設定為較大的數量，已確保在縮減叢集時不會終止任何任務。

核心節點群組

在核心節點上，YARN NodeManager 和 HDFS DataNode 協助程式都必須先除役，執行個體群組才能縮減。若為 YARN，逐漸縮減的方式可確保標示為等待除役的節點僅會在沒有等待中或未完成的容器或應用程式時，才會轉移為 DECOMMISSIONED 狀態。若開始除役時，節點上就沒有正在執行的容器，則除役工作會立即完成。

若為 HDFS，逐漸縮減的方式可確保 HDFS 有足夠的目標容量，可容納所有既有的區塊。若目標的容量不足，則僅有部分的核心執行個體能夠除役，讓剩下的節點可處理存在於 HDFS 的資料。請確保有更多 HDFS 容量，以供未來除役使用。您也可以在縮減執行個體群組前，先將寫入 I/O 降至最低，因為寫入可能會延遲到調整規模操作的完成時間。

另一個限制是預設的複寫因素，`/etc/hadoop/conf/hdfs-site` 中的 `dfs.replication`。Amazon EMR 會根據叢集中執行個體的數量來設定該值：1 到 3 個執行個體為 1，4 到 9 個執行個體為 2，超過 10 個以上的執行個體為 3。逐漸縮減功能並不允許將核心節點縮減至低於 HDFS 複寫因素，這是為了避免 HDFS 由於複寫不足而無法關閉檔案。若要避開此限制，您必須降低複寫因素，並重新啟動 NameNode 協助程式。

設定 Amazon EMR 的縮減行為

Note

此設定功能僅適用於 Amazon EMR 5.1.0 版或更新版本。

您可以使用 AWS Management Console、AWS CLI 或 Amazon EMR API 在建立叢集時設定縮減行為。使用 AWS Management Console 設定縮減需在使用 Advanced options (進階選項) 設定叢集時，於 Step 3: General Cluster Settings (步驟 3：一般叢集設定) 的畫面設定。

Create Cluster - Advanced Options [Go to quick options](#)

Step 1: Software and Steps

Step 2: Hardware

Step 3: General Cluster Settings

Step 4: Security

General Options

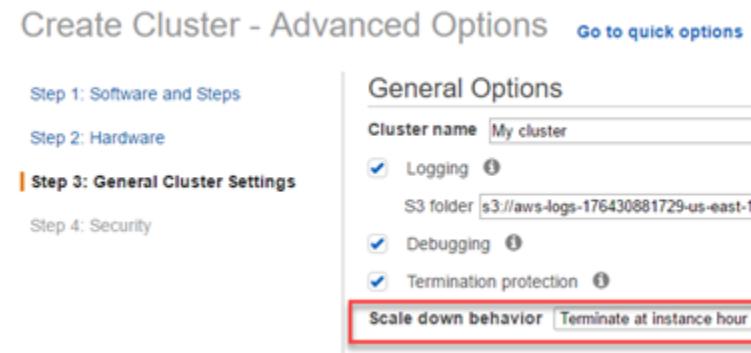
Cluster name: My cluster

Logging: S3 folder: s3://aws-logs-176430881729-us-east-1/elasticmapreduce/

Debugging

Termination protection

Scale down behavior: **Terminate at instance hour**



使用 AWS CLI 建立叢集時，請以 `--ScaleDownBehavior` 選項指定 `TERMINATE_AT_INSTANCE_HOUR` 或 `TERMINATE_AT_TASK_COMPLETION`。

使用主控台複製叢集

您可以使用 Amazon EMR 主控台來複製叢集，其會製作原始叢集之組態的複本，以用來做為新叢集的基礎。

使用主控台複製叢集

1. 在 Cluster List (叢集清單) 頁面上，按一下要複製的叢集。
2. 在 Cluster Details (叢集詳細資訊) 頁面頂端，按一下 Clone (複製)。

在對話方塊中，選擇 Yes (是)，以納入複製叢集中來自原始叢集的步驟。選擇 No (否) 以複製原始叢集的組態，而不包括任何步驟。

Note

對於使用 AMI 3.1.1 和更高版本 (Hadoop 2.x) 或 AMI 2.4.8 和更高版本 (Hadoop 1.x) 建立的叢集，如果您複製叢集並包含步驟，所有系統步驟 (例如設定 Hive) 會連同使用者提交的步驟一起複製，總數最多 1,000 個。不再顯示在主控台步驟歷史記錄的任何舊步驟皆無法複製。對於舊 AMI，只可複製 256 個步驟 (包括系統步驟)。如需更多詳細資訊，請參閱 [將工作提交到叢集 \(p. 305\)](#)。

3. Create Cluster (建立叢集) 頁面會顯示原始叢集組態的複本。檢閱組態，進行任何必要的變更，然後按一下 Create Cluster (建立叢集)。

將工作提交到叢集

本節說明將工作提交到 Amazon EMR 叢集的方法。您可以透過新增步驟或以互動方式將 Hadoop 任務提交到主節點來將工作提交至叢集。叢集中允許的 PENDING 和 ACTIVE 步驟的上限數為 256。即使您在叢集上有 256 個執行的作用中步驟，您可以互動方式將任務提交至主節點上。在長執行生命週期的叢集中您可以提交不受限的步驟數，但在給定時間僅 256 個步驟可以是 ACTIVE 或 PENDING。

主題

- [使用 CLI 和主控台來使用步驟 \(p. 305\)](#)
- [以互動方式提交 Hadoop 任務 \(p. 307\)](#)
- [在叢集中新增 256 個以上的步驟 \(p. 309\)](#)

使用 CLI 和主控台來使用步驟

您可以使用 AWS Management Console、AWS CLI 或 Amazon EMR API 將步驟新增至叢集。叢集中允許的 PENDING and ACTIVE 步驟數上限是 256，其中包含系統步驟，例如安裝 Pig、安裝 Hive、安裝 HBase 和設定 debugging。在長執行生命週期的叢集中您可以提交不受限的步驟數，但在給定時間僅 256 個步驟可以是 ACTIVE 或 PENDING。您可以透過 EMR 版本 4.8.0 和更新版本 (除了版本 5.0.0)，使用 AWS Management Console、AWS CLI 或 Amazon EMR API 來取消 PENDING 的步驟。

在叢集中新增步驟

您可以使用 AWS CLI、Amazon EMR 軟體開發套件或 AWS Management Console 將步驟新增至叢集。您可以使用 AWS Management Console，在建立叢集時，在叢集中新增步驟。您也可以將步驟新增至長時間執行的叢集，也就是說，已停用自動終止選項的叢集。

使用主控台新增步驟

無論您是在叢集建立期間新增步驟，或將步驟新增至叢集，程序會與以下程序類似。

使用 AWS Management Console 將步驟新增至執行中的叢集

1. 在 [Amazon EMR 主控台](#)，於 Cluster List (叢集清單) 頁面，按一下叢集的連結。
2. 在 Cluster Details (叢集詳細資訊) 頁面，展開 Steps (步驟) 區段，然後按一下 Add step (新增步驟)。
3. 在 Add Step (新增步驟) 對話方塊中的欄位中輸入適當的值，然後按一下 Add (新增)。根據步驟類型而定，選項會有所不同。

使用 AWS CLI 新增步驟

以下程序示範使用 AWS CLI 將步驟新增到新建立的叢集與執行中叢集。在這兩種範例中，會使用 `--steps` 子指令來在叢集中新增步驟。

在叢集建立期間新增步驟

- 輸入下列命令來建立叢集並新增 Pig 步驟。使用 EC2 金鑰對的名稱來取代 `myKey`，並使用 Amazon S3 儲存貯體的名稱來取代 `mybucket`。
 - Linux、UNIX 及 Mac OS X 使用者：

```
aws emr create-cluster --name "Test cluster" --ami-version 2.4 --applications
  Name=Hive Name=Pig \
  --use-default-roles --ec2-attributes KeyName=myKey \
  --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m5.xlarge \
  InstanceGroupType=CORE,InstanceCount=2,InstanceType=m5.xlarge \
  --steps Type=PIG,Name="Pig Program",ActionOnFailure=CONTINUE,Args=[-f,s3://mybucket/
  scripts/pigscript.pig,-p,INPUT=s3://mybucket/inputdata/, -p,OUTPUT=s3://mybucket/
  outputdata/, $INPUT=s3://mybucket/inputdata/, $OUTPUT=s3://mybucket/outputdata/]
```

- Windows 使用者：

```
aws emr create-cluster --name "Test cluster" --ami-version 2.4 --applications
  Name=Hive Name=Pig --use-default-roles --ec2-attributes KeyName=myKey --
  instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m5.xlarge
  InstanceGroupType=CORE,InstanceCount=2,InstanceType=m5.xlarge --steps
  Type=PIG,Name="Pig Program",ActionOnFailure=CONTINUE,Args=[-f,s3://mybucket/
  scripts/pigscript.pig,-p,INPUT=s3://mybucket/inputdata/, -p,OUTPUT=s3://mybucket/
  outputdata/, $INPUT=s3://mybucket/inputdata/, $OUTPUT=s3://mybucket/outputdata/]
```

Note

引數變更清單會根據步驟類型而有所不同。

輸出與下列輸出類似：

```
{  
  "ClusterId": "j-2AXXXXXXGAPLF"  
}
```

將步驟新增至執行中叢集

- 輸入下列命令來將步驟新增至執行中的叢集。請將 `j-2AXXXXXXGAPLF` 替換為您的叢集 ID，並將 `mybucket` 替換為您的 Amazon S3 儲存貯體名稱。

```
aws emr add-steps --cluster-id j-2AXXXXXXGAPLF --steps Type=PIG,Name="Pig
  Program",Args=[-f,s3://mybucket/scripts/pigscript.pig,-p,INPUT=s3://
  mybucket/inputdata/, -p,OUTPUT=s3://mybucket/outputdata/, $INPUT=s3://mybucket/
  inputdata/, $OUTPUT=s3://mybucket/outputdata/]
```

輸出是與下列項目類似的步驟識別碼：

```
{  
  "StepIds": [  
    "s-Y9XXXXXXAPMD"  
  ]
```

}

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

檢視步驟

您可以檢視的步驟記錄 (無論狀態為何) 總數量是 1,000 個。此總計包含使用者提交和系統步驟。當使用者提交步驟的狀態變更為 COMPLETED 或 FAILED，您可以將其他使用者提交步驟新增到叢集，直到達到 1,000 個步驟的限制。已將 1,000 個步驟新增到叢集，提交額外步驟會導致舊使用者提交步驟記錄遭到移除。不會將這些記錄從日誌檔移除。系統會將這些記錄從主控台顯示中移除，它們也不會在您使用 CLI 或 API 來擷取叢集資訊時出現。系統步驟記錄永遠不會被移除。

您可以檢視的步驟資訊取決於用於擷取叢集資訊的機制。下表顯示每個可用選項傳回的步驟資訊。

選項	DescribeJobFlow 或 --describe --jobflow	ListSteps 或 list-steps
SDK	256 個步驟	1,000 個步驟
Amazon EMR CLI	256 個步驟	不適用
AWS CLI	不適用	1,000 個步驟
API	256 個步驟	1,000 個步驟

取消待定步驟

您可以使用 AWS Management Console、AWS CLI 或 Amazon EMR API 取消步驟。您只能取消 PENDING 的步驟。

使用 AWS Management Console 取消步驟

1. 在 [Amazon EMR 主控台](#) 的 Cluster List (叢集清單) 頁面上，選擇叢集的連結。
2. 在 Cluster Details (叢集詳細資料) 頁面上，展開 Steps (步驟) 區段。
3. 針對您想要取消的每個步驟，從 Steps (步驟) 選取 Cancel step (取消步驟)，接著確認您是否要取消步驟。

使用 AWS CLI 取消步驟

- 使用 aws emr cancel-steps 命令，指定要取消的叢集和步驟。以下範例示範取消兩個步驟的 AWS CLI 命令。

```
aws emr cancel-steps --cluster-id j-2QUAJ7T3OTEI8 --step-ids s-3M8DKCZYYN1QE, s-3M8DKCZYYN1QE
```

以互動方式提交 Hadoop 任務

除了在叢集中新增步驟，您可以使用 SSH 用戶端或 AWS CLI 來連接主節點並以互動方式來提交 Hadoop 任務。例如，您可以使用 PuTTY 來建立內含主節點的 SSH 連接和提交互動式 Hive 查詢 (其會編譯成一或多個 Hadoop 任務)。

您可以透過建立對主節點的 SSH 連接 (使用 SSH 用戶端，例如 PuTTY 或 OpenSSH) 或使用 AWS CLI 中的 ssh 子指令，來以互動方式提交 Hadoop 任務。即使您在叢集上有 256 個執行的作用中步驟，您可以互動方式將任務提交至主節點上。不過，請注意，與以互動方式提交之任務相關聯的日誌記錄會包含在目前執行中步驟之控制器日誌的「步驟建立任務」區段。如需更多步驟日誌的資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

以下範例示範以互動方式將 Hadoop 任務和 Hive 任務提交至主節點。其他程式設計架構之提交任務的程序 (例如 Pig) 與這些範例是相類似的。

使用 AWS CLI 以互動方式提交 Hadoop 任務

- 您可以在 CLI 命令中建立 SSH 連接 (使用 ssh 子命令)，藉由 AWS CLI 以互動的方式提交 Hadoop 任務。若要將 JAR 檔案從本機 Windows 機器複製到主節點的檔案系統，請輸入下列命令。使用叢集 ID 取代 **j-2A6HXXXXXXL7J**，使用金鑰對檔案的名稱取代 **mykey.ppk**，並使用 JAR 檔案的名稱取代 **myjar.jar**。

```
aws emr put --cluster-id j-2A6HXXXXXXL7J --key-pair-file "C:\Users\username\Desktop\Keys\mykey.ppk" --src "C:\Users\username\myjar.jar"
```

若要建立 SSH 連線並提交 Hadoop 任務 **myjar.jar**，請輸入下列命令。

```
aws emr ssh --cluster-id j-2A6HXXXXXXL7J --key-pair-file "C:\Users\username\Desktop\Keys\mykey.ppk" --command "hadoop jar myjar.jar"
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

使用 AWS CLI 以互動方式提交 Hive 任務

除了透過 JAR 檔案將任務提交到主節點上，您可以透過與在主節點上執行的其中一個 Hadoop 程式設計架構互動來提交任務。例如，您可以互動方式在命令列提交 Hive 查詢或 Pig 轉換，或者您可以將指令碼提交到叢集以進行處理。系統會將您的命令或指令碼編譯成一或多個 Hadoop 任務。

下列程序示範使用 AWS CLI 來執行 Hive 指令碼。

- 如果未將 Hive 安裝在叢集，請輸入下列命令來加以安裝。使用叢集 ID 來取代 **j-2A6HXXXXXXL7J**。

```
aws emr install-applications --cluster-id j-2A6HXXXXXXL7J --apps Name=Hive
```

- 建立包含要執行之查詢或命令的 Hive 指令碼檔案。以下名為 **my-hive.q** 的範例指令碼會建立兩個表格 (**aTable** 以及 **anotherTable**)，並會將 **aTable** 的內容複製到 **anotherTable** 以取代所有資料。

```
---- sample Hive script file: my-hive.q ----
create table aTable (aColumn string);
create table anotherTable like aTable;
insert overwrite table anotherTable select * from aTable
```

- 輸入下列命令來使用 ssh 子指令從命令列執行指令碼。

若要從 Windows 機器將 **my-hive.q** 複製到您的叢集，請輸入下列命令。使用叢集 ID 取代 **j-2A6HXXXXXXL7J**，並使用金鑰對檔案的名稱來取代 **mykey.ppk**。

```
aws emr put --cluster-id j-2A6HXXXXXXL7J --key-pair-file "C:\Users\username\Desktop\Keys\mykey.ppk" --src "C:\Users\username\my-hive.q"
```

若要建立 SSH 連線並提交 Hive 指定碼 **my-hive.q**，請輸入下列命令。

```
aws emr ssh --cluster-id j-2A6HXXXXXXL7J --key-pair-file "C:\Users\username\Desktop\Keys\mykey.ppk" --command "hive -f my-hive.q"
```

如需在 AWS CLI 中使用 Amazon EMR 命令的詳細資訊，請參閱 <https://docs.aws.amazon.com/cli/latest/reference/emr>。

在叢集中新增 256 個以上的步驟

從 AMI 3.1.1 (Hadoop 2.x) 和 AMI 2.4.8 (Hadoop 1.x) 開始，您可以在長時間執行的叢集中提交不限數量的步驟，但在給定時間只有 256 個步驟可以是作用中或待定。對於較舊的 AMI 版本，叢集可處理的步驟總數量限制為 256 個（包括系統步驟，例如安裝 Hive 和安裝 Pig）。如需更多詳細資訊，請參閱 [將工作提交到叢集 \(p. 305\)](#)。

在早於 3.1.1 和早於 2.4.8 AMI 中您可以使用多種方法來克服 256 個步驟的限制：

- 透過每個步驟將多個任務提交至 Hadoop。您無法在早於 3.1.1 和早於 2.4.8 AMI 中使用無限制的步驟，但如果需要大於 256 個固定數量的步驟，這是最簡單的解決方案。
- 寫入在長時間執行叢集上的叢集中執行之工作流程計畫，並將任務提交到 Hadoop。您可以讓工作流程計畫執行以下動作：
 - 接聽 Amazon SQS 佇列以接收要執行之新步驟的相關資訊。
 - 定期檢查 Amazon S3 儲存貯體是否有包含要執行之新步驟相關資訊的檔案。
- 寫入在 Amazon EMR 外 EC2 執行個體上執行的工作流程計畫，並使用 SSH 將任務提交到長時間執行的叢集。
- 透過 SSH 連接到長時間執行的叢集並使用 Hadoop API 提交 Hadoop 任務。如需詳細資訊，請參閱 <http://hadoop.apache.org/docs/current/api/org/apache/hadoop/mapred/JobClient.html>。
- 使用 SSH 用戶端（例如 PuTTY 或 OpenSSH）連接到主節點和手動將任務提交到叢集，或在 AWS CLI 中使用 ssh 子命令以同時連接並提交任務。如需使用主節點建立 SSH 連線的詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。如需以互動方式提供 Hadoop 任務的詳細資訊，請參閱 [以互動方式提交 Hadoop 任務 \(p. 307\)](#)。

使用 AWS Data Pipeline 自動化再次出現的叢集

AWS Data Pipeline 是一項服務，可自動化資料的移動和轉換。您可以使用它來排定將輸入資料移動到 Amazon S3 的時程和排定啟動叢集來處理該資料的時程。例如，假設您有一個記錄流量日誌的 Web 伺服器。如果您想要執行週叢集，以分析每週的流量資料，可以使用 AWS Data Pipeline 來將這些叢集排程。AWS Data Pipeline 是一種資料導向的工作流程，因此某個任務（啟動叢集）可以和另一個任務（將輸入資料移到 Amazon S3）相依。它還具有強大的重試功能。

如需關於 AWS Data Pipeline 的詳細資訊，請參閱 [AWS Data Pipeline Developer Guide](#)，尤其是有關於 Amazon EMR 的教學課程：

- [教學課程：啟動 Amazon EMR 任務流程](#)
- [入門：使用 AWS Data Pipeline、Amazon EMR 和 Hive 來處理 Web 日誌](#)
- [教學課程：使用 AWS Data Pipeline 的 Amazon DynamoDB 匯入和匯出](#)

故障診斷叢集

由 Amazon EMR 託管的叢集是由數種類型的開放原始碼軟體、自訂應用程式碼和 Amazon Web Services 所組成，並在複雜的生態系統中執行。在這些部分中的任何問題，都可能導致該叢集失敗或需要比預期更長的時間來完成。下列主題將協助您找出叢集中的錯誤，並提供您建議的修正方法。

主題

- [哪些工具適用於故障診斷？\(p. 310\)](#)
- [檢視和重新啟動 Amazon EMR 和應用程式程序 \(常駐程式\) \(p. 311\)](#)
- [對失敗的叢集進行故障排除 \(p. 313\)](#)
- [故障診斷執行緩慢的叢集 \(p. 316\)](#)
- [Amazon EMR 中的常見錯誤 \(p. 321\)](#)
- [故障診斷 Lake Formation 叢集 \(Beta 版\) \(p. 335\)](#)

開發新的 Hadoop 應用程式時，我們建議您啟用除錯，並且處理一個小型但具代表性的資料子集以測試應用程式。您也可以逐步執行應用程式以分別測試各個步驟。如需詳細資訊，請參閱「[設定叢集記錄和除錯 \(p. 118\)](#)」與「[步驟 5：逐步測試叢集 \(p. 315\)](#)」。

哪些工具適用於故障診斷？

您可使用多種工具來蒐集叢集的相關資訊，以協助判斷發生的錯誤。部分工具在您啟動叢集時需要初始化；其他則是每個叢集都已備妥的工具。

主題

- [顯示叢集詳細資訊的工具 \(p. 310\)](#)
- [檢視日誌檔的工具 \(p. 311\)](#)
- [監控叢集效能的工具 \(p. 311\)](#)

顯示叢集詳細資訊的工具

您可以使用 AWS Management Console、AWS CLI 或 EMR API 來擷取 EMR 叢集和執行工作的詳細資訊。如需使用 AWS Management Console 和 AWS CLI 的詳細資訊，請參閱 [查看叢集狀態和詳細資訊 \(p. 241\)](#)。

Amazon EMR 主控台詳細資訊窗格

在 Amazon EMR 主控台上的 Clusters (叢集) 清單中，您可以查看在您的帳戶和區域中每個叢集狀態的高階資訊。此清單會顯示您在過去兩個月已啟動的所有叢集 (無論是有效或終止)。從 Clusters (叢集) 清單中，您可以選擇叢集 Name (名稱) 來查看叢集詳細資訊。此資訊分為不同類別，讓您可以輕鬆導覽。

叢集詳細資訊頁面中的 Application history (應用程式歷史記錄) 特別有助於故障診斷。其提供 YARN 應用程式的狀態，針對部分應用程式 (像是 Spark)，您可以深入不同的指標和面向 (例如工作、階段和執行者)。如需更多詳細資訊，請參閱 [查看應用程式歷史記錄 \(p. 247\)](#)。這項功能僅能在 Amazon EMR 版本 5.8.0 及更新版本中使用。

Amazon EMR 命令列界面

您可以使用 --describe 引數從 CLI 中尋找叢集的詳細資訊。

Amazon EMR API

您可以使用 `DescribeJobFlows` 動作從 API 中尋找叢集的詳細資訊。

檢視日誌檔的工具

叢集執行時，Amazon EMR 和 Hadoop 會同時產生日誌檔。您可以從多種不同的工具存取這些日誌檔案，這取決於您在啟動叢集時指定的組態而定。如需更多詳細資訊，請參閱 [設定叢集記錄和除錯 \(p. 118\)](#)。

在主節點的日誌檔

每個叢集會將日誌檔案到發佈到主節點上的 `/mnt/var/log/` 目錄。這些日誌檔只可在叢集執行時可供使用。

封存到 Amazon S3 的日誌檔

如果您啟動叢集，並指定 Amazon S3 日誌路徑，叢集會以 5 分鐘的間隔，將存放在主節點上 `/mnt/var/log/` 的日誌檔複製到 Amazon S3。這可確保即使叢集終止，您仍有權存取日誌檔。由於系統以 5 分鐘的間隔封存一次檔案，最後幾分鐘突然終止的叢集可能會無法提供使用。

監控叢集效能的工具

Amazon EMR 提供多種工具來監控您叢集的效能。

Hadoop Web 界面

每個叢集會在包含叢集資訊的主節點上發佈一組 Web 界面。您可以使用 SSH 通道連接主節點上的 web 頁面，以存取這些網頁。如需更多詳細資訊，請參閱 [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

CloudWatch 個指標

每個叢集會向 CloudWatch 報告指標。CloudWatch 是一項追蹤指標的 Web 服務，可用來設定對這些指標的警示。如需更多詳細資訊，請參閱 [使用 CloudWatch 監控指標 \(p. 262\)](#)。

檢視和重新啟動 Amazon EMR 和應用程式程序 (常駐程式)

當您對叢集進行疑難排解時，您可能需要列出執行中的程序。您也可能會發現在某些情況下（例如，在您分析日誌檔和錯誤訊息後並變更組態或向特定處理通知問題後）停止或重新啟動程序很有用。

在叢集上執行的程序有兩種類型：Amazon EMR 程序（例如，執行個體控制器和日誌推送器）和與叢集上安裝的應用程式相關的程序（例如，`hadoop-hdfs-namenode` 和 `hadoop-yarn-resourcemanager`）。

若要直接在叢集上使用程序，您可以連接到主節點。如需更多詳細資訊，請參閱 [連接叢集 \(p. 276\)](#)。

檢視執行中的程序

如果您使用的是 Amazon EMR 4.x 版或更新版本，應用程式版本是使用根據 Apache Bigtop 的系統來封裝，如此這些應用程式會透過 `.conf` 指令碼在 `upstart init` 系統下進行設定。另一方面，已使用 SysV (`init.d` 程序檔) 設定 Amazon EMR 程序，該指定檔可與 `upstart` 回溯相容。

若要查看執行中 Amazon EMR 程序的清單

- 輸入下列命令 (不含 \$，其會表示 Linux 命令提示)：

```
$ ls /etc/init.d/
```

該命令會傳回類似以下範例的執行中 Amazon EMR 程序清單：

acpid	cloud-init-local	instance-controller	ntpd
-------	------------------	---------------------	------

要查看與應用程式版本相關的程序清單

- 輸入以下命令：

```
$ ls /etc/init/
```

該命令會傳回類似以下範例的執行中應用程式程序清單：

control-alt-delete.conf	hadoop-yarn-resourcemanager.conf	hive-
metastore.conf		

重新啟動程序

在您判斷執行中的是哪些程序後，必要時，您可以先停止它們然後再予以重新啟動。啟動和停止服務的方式取決於無論其是否是 Amazon EMR 服務或與應用程式相關聯的服務。

若要重新啟動與應用程式版本關聯的程序

- 輸入以下命令來停止程序，使用以上程序中 *processname* 命令傳回的程序名稱來取代 ls：

```
$ sudo /etc/init.d/processname stop
```

例如：sudo /etc/init.d/hadoop-hdfs-namenode stop。

- 輸入以下命令來重新啟動程序：

```
$ sudo /etc/init.d/processname start
```

例如，sudo /etc/init.d/hadoop-hdfs-namenode start。

若要重新啟動 Amazon EMR 程序

- 輸入以下命令來停止程序，使用以上程序中 *processname* 命令傳回的程序名稱來取代 ls：

```
$ sudo /sbin/stop processname
```

例如，sudo /sbin/stop instance-controller。

- 輸入以下命令來重新啟動程序：

```
$ sudo sbin/start processname
```

例如，`sudo sbin/start instance-controller`。

Note

`sbin/start`, `stop` 和 `restart` 命令是 `/sbin/initctl` 的符號連結。如需 `initctl` 的更多資訊，請在命令提示字元輸入 `man initctl` 以參閱 `initctl man` 頁面。

對失敗的叢集進行故障排除

本節將逐步引導您對失敗的叢集進行故障排除。這表示，叢集終止並出現錯誤代碼。如果叢集仍在執行，但需要很長的時間才能傳回結果，則另請參閱 [故障診斷執行緩慢的叢集 \(p. 316\)](#)。

主題

- [步驟 1：收集有關問題的資料 \(p. 313\)](#)
- [步驟 2：檢查環境 \(p. 313\)](#)
- [步驟 3：查看最後狀態變更 \(p. 314\)](#)
- [步驟 4：檢查日誌檔 \(p. 315\)](#)
- [步驟 5：逐步測試叢集 \(p. 315\)](#)

步驟 1：收集有關問題的資料

叢集故障診斷的第一步驟是收集資訊，包括發生的錯誤與叢集的目前狀態及組態。此資訊會用於下列步驟，以確認或排除問題的可能原因。

定義問題

首先，要對問題有清楚的定義。您可以問自己：

- 我預期會發生什麼？結果發生了什麼？
- 這個問題最早是何時發生的？從那之後發生的頻率？
- 有任何事改變了我設定或執行叢集的方式嗎？

叢集詳細資訊

以下的叢集詳細資訊可協助您追蹤問題。如需收集此資訊之方式的詳細資訊，請參閱 [查看叢集狀態和詳細資訊 \(p. 241\)](#)。

- 叢集的識別符(也稱為任務流程識別符。)
- 叢集啟動的區域和可用區域。
- 叢集的狀態，包括上次狀態變更的詳細資訊。
- 主節點、核心節點和任務節點指定的 EC2 執行個體類型和編號。

步驟 2：檢查環境

Amazon EMR 是做為 Web 服務和開放原始碼軟體生態系統的一部分運作。影響這些相依性的一切都會連帶衝擊 Amazon EMR 的效能。

主題

- 檢查是否發生服務中斷 (p. 314)
- 檢查用量範圍 (p. 314)
- 檢查發行版本 (p. 314)
- 檢查 Amazon VPC 子網路組態 (p. 314)

檢查是否發生服務中斷

Amazon EMR 會在內部使用數種 Amazon Web Services。這包括在 Amazon EC2 上執行虛擬伺服器，在 Amazon S3 上存放資料和指令碼，在 Amazon SimpleDB 中建立日誌檔案索引，以及向 CloudWatch 報告各項指標。干擾這些服務的事件非常罕見 — 但是如果發生 — 就會在 Amazon EMR 中造成問題。

在您繼續之前，請參閱[服務運作狀態儀表板](#)。請檢查您啟動叢集的區域，以確認上述服務是否出現干擾事件。

檢查用量範圍

如果您啟動大型叢集、同時啟動許多叢集，或您是與其他使用者共用一個 AWS 帳戶的 IAM 使用者，叢集可能會因為您超出了 AWS Service Limit 而無法啟動。

Amazon EC2 會將在單一 AWS 區域運行的虛擬伺服器執行個體數量限制在 20 個隨需執行個體或預留執行個體。如果您在超過 20 個節點啟動叢集，或啟動叢集時造成在您 AWS 帳戶中作用的 EC2 執行個體總數超過 20 個，叢集可能會無法啟動其所需的全部 EC2 執行個體，也有可能啟動失敗。發生此情況時，Amazon EMR 會傳回 EC2 QUOTA EXCEEDED 錯誤。您可以提交[請求增加 Amazon EC2 執行個體限制](#)應用程式，請求 AWS 增加您能夠在帳戶中執行的 EC2 執行個體數量。

另一個可能造成您超出用量限制的狀況，是叢集在終止和釋出所有資源時發生延遲。依據其組態，叢集可能需要 5-20 分鐘時間才會完全終止並釋出配置資源。如果您在嘗試啟動叢集時得到 EC2 QUOTA EXCEEDED 錯誤，原因可能是剛終止的叢集尚未釋出資源。此情況下，您可以[請求增加 Amazon EC2 配額](#)，或等待二十分鐘再重新啟動叢集。

Amazon S3 將每個帳戶可建立儲存貯體的數量限制在 100 個。如果叢集建立的新儲存貯體超過此限制，就無法建立儲存貯體，而且可能導致叢集無法啟動。

檢查發行版本

將您用於啟動叢集的發行標籤與最新的 Amazon EMR 版本進行比較。Amazon EMR 的每個版本都會有所改善，例如新的應用程式、新功能、修補程式和錯誤修正。影響叢集的問題可能已經在最新的發行版本中獲得解決。如果可以，請使用最新的版本重新執行 cluster。

檢查 Amazon VPC 子網路組態

如果您的叢集在 Amazon VPC 子網路中啟動，則子網路必須依照[設定網路 \(p. 95\)](#)所述進行設定。此外，請確認您啟動叢集的子網路擁有足夠的可用彈性 IP 地址以指派給叢集每個節點。

步驟 3：查看最後狀態變更

最後狀態變更可提供相關資訊，有助於了解叢集最後一次變更狀態時發生了什麼狀況。通常提供的資訊可告訴您，發生什麼樣的錯誤導致叢集狀態變更為 FAILED。例如，如果您啟動串流叢集並指定已存在 Amazon S3 中的輸出位置，則叢集將會失敗並出現最後狀態變更「串流輸出目錄已存在」。

您可以在主控台上檢視叢集的詳細資料窗格、從 CLI 使用 list-steps 或 describe-cluster 引數，或從 API 使用 DescribeCluster 和 ListSteps 動作來尋找最後狀態變更值。如需更多詳細資訊，請參閱[查看叢集狀態和詳細資訊 \(p. 241\)](#)。

步驟 4：檢查日誌檔

下個步驟是檢查日誌檔，找出錯誤代碼或是其他關於叢集所遭遇問題的資訊。關於可用的日誌檔案，到何處尋找以及如何檢視，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您可能需要一些調查才能確認情況。Hadoop 會在叢集中多個節點執行任務嘗試的工作作業。Amazon EMR 可啟動推測式任務嘗試，終止其他未先完成的任務嘗試。這會產生大量活動，並在發生時記錄至 controller、stderr 和 syslog 日誌檔案。此外，雖然多重任務嘗試是同時執行，但日誌檔案可透過線性方式顯示結果。

首先，檢查引導操作日誌是否有叢集啟動期間發生的錯誤或未預期的組態變更。接下來，查看步驟日誌，找出依步驟啟動的 Hadoop 工作之錯誤。檢查 Hadoop 工作日誌，找出失敗的任務嘗試。任務嘗試日誌會包含造成任務嘗試失敗的詳細資訊。

以下部分說明如何使用多種日誌檔找出叢集中的錯誤。

檢查引導操作日誌

引導操作啟動後會在叢集執行指令碼。引導操作常用於在叢集安裝其他軟體，或是改變預設值的組態設定。查看日誌能讓您深入了解在叢集設定期間發生的錯誤，以及可能影響效能的組態設定變更。

檢查步驟日誌

步驟日誌有四種類型。

- controller—包含由 Amazon EMR (Amazon EMR) 產生的檔案，會在嘗試執行步驟而遭遇錯誤時出現。如果您的步驟在載入時失敗，可以在這個日誌中找到堆疊追蹤。此處通常會描述載入或存取應用程式時的錯誤，以及缺少映射器檔案的錯誤。
- stderr—包含在處理步驟時發生的錯誤訊息。此處通常描述應用程式載入錯誤。此日誌有時會包含堆疊追蹤。
- stdout—包含由映射器和縮減器可執行檔產生的狀態。此處通常描述應用程式載入錯誤。此日誌有時會包含應用程式錯誤訊息。
- syslog—包含來自非 Amazon 軟體的日誌，例如 Apache 和 Hadoop。此處通常會描述串流錯誤。

您可檢查 stderr 找出明顯的錯誤。如果 stderr 顯示出簡短的錯誤清單，此步驟會迅速停止並擲出錯誤。最常出現的原因是在叢集中執行的映射器和縮減器應用程式發生了錯誤。

請檢查 controller 和 syslog 的最後幾行是否有錯誤或失敗的通知。請注意任何關於作業失敗的通知，尤其是顯示「Job Failed」時。

檢查任務嘗試日誌

如果先前的步驟日誌分析發現了一個或多個失敗的工作，請調查相應工作嘗試的日誌以獲得更詳細的錯誤資訊。

步驟 5：逐步測試叢集

當您嘗試追蹤錯誤來源時，有一項實用的技術就是重新啟動叢集並逐一提交步驟。這可讓您先查看每個步驟的結果，然後再處理下一個步驟，如此就有機會更正並重新執行失敗的步驟。另一項好處在於，您只需載入輸入資料一次。

逐步測試叢集

1. 啓動新叢集，同時啟用持續作用和終止保護功能。持續作用功能可讓叢集在完成所有待處理步驟之後保持執行狀態。終止保護功能可防止叢集在發生錯誤時關閉。如需更多詳細資訊，請參閱 [設定叢集自動終止或繼續 \(p. 74\)](#) 及 [使用終止保護 \(p. 75\)](#)。

2. 提交步驟至叢集。如需更多詳細資訊，請參閱 [將工作提交到叢集 \(p. 305\)](#)。
3. 當步驟完成處理時，查看步驟日誌檔中是否有錯誤。如需更多詳細資訊，請參閱 [步驟 4：檢查日誌檔 \(p. 315\)](#)。尋找這些日誌檔最快的方式，就是連接到主節點並於該處檢視日誌檔。步驟日誌檔會在步驟執行一段時間、完成或失敗後才產生。
4. 如果步驟成功且未產生錯誤，請執行下一個步驟。如果發生錯誤，請調查日誌檔中的錯誤。如果是程式碼發生錯誤，請進行更正並重新執行步驟。繼續執行，直到所有步驟都執行且沒有錯誤。
5. 當您完成叢集偵錯且想要將其終止時，必須手動將它終止。在叢集啟動並啟用終止保護功能的情況下，您就必須這樣做。如需更多詳細資訊，請參閱 [使用終止保護 \(p. 75\)](#)。

故障診斷執行緩慢的叢集

此區段逐步引導您在叢集仍然執行，但需要很長的時間來傳回結果時故障排除的程序。如需有關在叢集終止且內含錯誤碼時該執行什麼動作的詳細資訊，請參閱 [對失敗的叢集進行故障排除 \(p. 313\)](#)

Amazon EMR 可讓您在叢集中指定執行個體的數量和類型。這些規格是影響您資料處理完成速度的主要方式。您可以考慮是其中一點是重新執行叢集，而這次指定內含更多資源的 EC2 執行個體，或指定叢集中較大的執行個體數目。如需更多詳細資訊，請參閱 [設定叢集硬體和聯網 \(p. 89\)](#)。

下列主題會逐步引導您辨識導致叢集執行緩慢之替代方案的程序。

主題

- [步驟 1：收集有關問題的資料 \(p. 316\)](#)
- [步驟 2：檢查環境 \(p. 317\)](#)
- [步驟 3：檢查日誌檔 \(p. 317\)](#)
- [步驟 4：檢查叢集和執行個體運作狀態 \(p. 318\)](#)
- [步驟 5：檢查遭阻擋的群組 \(p. 319\)](#)
- [步驟 6：檢閱組態設定 \(p. 320\)](#)
- [步驟 7：檢查輸入資料 \(p. 321\)](#)

步驟 1：收集有關問題的資料

叢集故障診斷的第一步驟是收集資訊，包括發生的錯誤與叢集的目前狀態及組態。此資訊會用於下列步驟，以確認或排除問題的可能原因。

定義問題

首先，要對問題有清楚的定義。您可以問自己：

- 我預期會發生什麼？結果發生了什麼？
- 這個問題最早是何時發生的？從那之後發生的頻率？
- 有任何事改變了我設定或執行叢集的方式嗎？

叢集詳細資訊

以下的叢集詳細資訊可協助您追蹤問題。如需收集此資訊之方式的詳細資訊，請參閱 [查看叢集狀態和詳細資訊 \(p. 241\)](#)。

- 叢集的識別符(也稱為任務流程識別符。)
- 叢集啟動的區域和可用區域。

- 叢集的狀態，包括上次狀態變更的詳細資訊。
- 主節點、核心節點和任務節點指定的 EC2 執行個體類型和編號。

步驟 2：檢查環境

主題

- [檢查是否發生服務中斷 \(p. 317\)](#)
- [檢查用量範圍 \(p. 317\)](#)
- [檢查 Amazon VPC 子網路組態 \(p. 317\)](#)
- [重新啟動叢集 \(p. 317\)](#)

檢查是否發生服務中斷

Amazon EMR 會在內部使用數種 Amazon Web Services。這包括在 Amazon EC2 上執行虛擬伺服器，在 Amazon S3 上存放資料和指令碼，在 Amazon SimpleDB 中建立日誌檔案索引，以及向 CloudWatch 報告各項指標。干擾這些服務的事件非常罕見 — 但是如果發生 — 就會在 Amazon EMR 中造成問題。

在您繼續之前，請參閱[服務運作狀態儀表板](#)。請檢查您啟動叢集的區域，以確認上述服務是否出現干擾事件。

檢查用量範圍

如果您啟動大型叢集、同時啟動許多叢集，或您是與其他使用者共用一個 AWS 帳戶的 IAM 使用者，叢集可能會因為您超出了 AWS Service Limit 而無法啟動。

Amazon EC2 會將在單一 AWS 區域運行的虛擬伺服器執行個體數量限制在 20 個隨需執行個體或預留執行個體。如果您在超過 20 個節點啟動叢集，或啟動叢集時造成在您 AWS 帳戶中作用的 EC2 執行個體總數超過 20 個，叢集可能會無法啟動其所需的全部 EC2 執行個體，也有可能啟動失敗。發生此情況時，Amazon EMR 會傳回 `EC2 QUOTA EXCEEDED` 錯誤。您可以提交[請求增加 Amazon EC2 執行個體限制](#)應用程式，請求 AWS 增加您能夠在帳戶中執行的 EC2 執行個體數量。

另一個可能造成您超出用量限制的狀況，是叢集在終止和釋出所有資源時發生延遲。依據其組態，叢集可能需要 5-20 分鐘時間才會完全終止並釋出配置資源。如果您在嘗試啟動叢集時得到 `EC2 QUOTA EXCEEDED` 錯誤，原因可能是剛終止的叢集尚未釋出資源。此情況下，您可以[請求增加 Amazon EC2 配額](#)，或等待二十分鐘再重新啟動叢集。

Amazon S3 將每個帳戶可建立儲存貯體的數量限制在 100 個。如果叢集建立的新儲存貯體超過此限制，就無法建立儲存貯體，而且可能導致叢集無法啟動。

檢查 Amazon VPC 子網路組態

如果您的叢集在 Amazon VPC 子網路中啟動，則子網路必須依照 [設定網路 \(p. 95\)](#) 所述進行設定。此外，請確認您啟動叢集的子網路擁有足夠的可用彈性 IP 地址以指派給叢集每個節點。

重新啟動叢集

處理時的速度降低可能是因為暫時性的狀況。考慮終止和重新啟動叢集，看看效能是否改善。

步驟 3：檢查日誌檔

下個步驟是檢查日誌檔，找出錯誤代碼或是其他關於叢集所遭遇問題的資訊。關於可用的日誌檔案，到何處尋找以及如何檢視，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您可能需要一些調查才能確認情況。Hadoop 會在叢集中多個節點執行任務嘗試的工作作業。Amazon EMR 可啟動推測式任務嘗試，終止其他未完成的任務嘗試。這會產生大量活動，並在發生時記錄至 controller、stderr 和 syslog 日誌檔案。此外，雖然多重任務嘗試是同時執行，但日誌檔案可透過線性方式顯示結果。

首先，檢查引導操作日誌是否有叢集啟動期間發生的錯誤或未預期的組態變更。接下來，查看步驟日誌，找出依步驟啟動的 Hadoop 工作之錯誤。檢查 Hadoop 工作日誌，找出失敗的任務嘗試。任務嘗試日誌會包含造成任務嘗試失敗的詳細資訊。

以下部分說明如何使用多種日誌檔找出叢集中的錯誤。

檢查引導操作日誌

引導操作啟動後會在叢集執行指令碼。引導操作常用於在叢集安裝其他軟體，或是改變預設值的組態設定。查看日誌能讓您深入了解在叢集設定期間發生的錯誤，以及可能影響效能的組態設定變更。

檢查步驟日誌

步驟日誌有四種類型。

- controller—包含由 Amazon EMR (Amazon EMR) 產生的檔案，會在嘗試執行步驟而遭遇錯誤時出現。如果您的步驟在載入時失敗，可以在這個日誌中找到堆疊追蹤。此處通常會描述載入或存取應用程式時的錯誤，以及缺少映射器檔案的錯誤。
- stderr—包含在處理步驟時發生的錯誤訊息。此處通常描述應用程式載入錯誤。此日誌有時會包含堆疊追蹤。
- stdout—包含由映射器和縮減器可執行檔產生的狀態。此處通常描述應用程式載入錯誤。此日誌有時會包含應用程式錯誤訊息。
- syslog—包含來自非 Amazon 軟體的日誌，例如 Apache 和 Hadoop。此處通常會描述串流錯誤。

您可檢查 stderr 找出明顯的錯誤。如果 stderr 顯示出簡短的錯誤清單，此步驟會迅速停止並擲出錯誤。最常出現的原因是在叢集中執行的映射器和縮減器應用程式發生了錯誤。

請檢查 controller 和 syslog 的最後幾行是否有錯誤或失敗的通知。請注意任何關於作業失敗的通知，尤其是顯示「Job Failed」時。

檢查任務嘗試日誌

如果先前的步驟日誌分析發現了一個或多個失敗的工作，請調查相應工作嘗試的日誌以獲得更詳細的錯誤資訊。

檢查 Hadoop 協助程式日誌

在極少數情況下，Hadoop 可能會執行失敗。要確認是否為此情況，您必須查看 Hadoop 日誌。日誌位於各節點上的 /var/log/hadoop/，。

您可以使用 JobTracker 日誌將失敗的任務嘗試對應至其執行的節點。知道與任務嘗試關聯的節點後，您就能檢查該節點的 EC2 執行個體運作狀態以確認是否有任何問題，例如 CPU 或記憶體不足。

步驟 4：檢查叢集和執行個體運作狀態

Amazon EMR 叢集是由在 Amazon EC2 執行個體上執行的節點所組成。如果那些執行個體受限於資源（例如，CPU 或記憶體用盡）、發生網路連線問題，或是終止，則叢集處理速度會降低。

叢集中的節點類型有三種：

- master node (主節點) — 管理叢集。如果發生效能問題，整個叢集都會受到影響。
- core nodes (核心節點) — 處理映射縮減的任務，並保留 Hadoop 分散式檔案系統 (HDFS)。如果其中一個節點發生效能問題，它可以讓 HDFS 操作以及映射縮減處理速度慢下來。您可以將額外的核心節點新增到叢集以提升效能，但不可以移除核心節點。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#)。
- task nodes (任務節點) — 處理映射縮減任務。這些是純粹的運算資源而不會存放資料。您可以將任務節點新增到叢集以加速效能，或移除不需要的任務節點。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#)。

當您查看叢集的運作狀態時，您也該同時查看叢集的整體效能，以及個別執行個體的效能。有多種工具可供您使用：

使用 CloudWatch 檢查叢集運作狀態

每個 Amazon EMR 叢集都會向 CloudWatch 報告指標。這些指標提供有關叢集的摘要效能資訊，例如總負載、HDFS 使用率、執行中任務、剩餘的任務、損毀區塊等等。查看 CloudWatch 指標可讓您深入了解叢集的目前狀況，並讓您在處理時了解執行速度緩慢的原因。除了使用 CloudWatch 來分析現有的效能問題，您可以設定提醒，此會讓 CloudWatch 在未來發生效能問題時進行提醒。如需更多詳細資訊，請參閱 [使用 CloudWatch 監控指標 \(p. 262\)](#)。

檢查任務狀態和 HDFS 運作狀態

使用叢集詳細資訊頁面上的 Application history (應用程式歷史記錄)，以檢視 YARN 應用程式的詳細資訊。對於特定的應用程式，您可以深入了解進一步詳細資訊和直接存取日誌。此方式特別適用於 Spark 應用程式。如需更多詳細資訊，請參閱 [查看應用程式歷史記錄 \(p. 247\)](#)。

Hadoop 提供一系列的 Web 介面，您可使用這些介面來檢視資訊。如需如何存取這些 web 介面的詳細資訊，請參閱 [檢視 Amazon EMR 叢集上託管的 Web 界面 \(p. 281\)](#)。

- JobTracker — 提供有關叢集處理之任務的進度。您可以使用此介面來識別任務變為停滯的時間。
- HDFS NameNode — 提供 HDFS 使用率和在每個節點上可用空間之百分比的相關資訊。您可以使用此介面來識別 HDFS 成為受資源限定的時間，且需要額外的容量。
- TaskTracker — 提供有關叢集處理之任務的作業。您可以使用此介面來識別作業變為停滯的時間。

使用 Amazon EC2 檢查執行個體運作狀態

在叢集中尋找執行個體相關狀態資訊的另一個方式是使用 Amazon EC2 主控台。因為叢集中的每個節點是在 EC2 執行個體上執行，您可以使用 Amazon EC2 提供的工具來檢查他們的狀態。如需更多詳細資訊，請參閱 [檢視 Amazon EC2 中的叢集執行個體 \(p. 254\)](#)。

步驟 5：檢查遭阻擋的群組

執行個體群組在嘗試啟動節點時，因為遇到太多錯誤而遭阻擋。舉例而言，若新節點執行引導操作時不斷失敗，執行個體群組在一段時間後便會進入 ARRESTED 狀態，而不會繼續嘗試佈建新節點。

若發生以下事項，節點即可容錯移轉：

- Hadoop 或叢集因某些原因中斷，並不會接受新節點進入叢集
- 引導操作在新節點上失敗
- 節點的運作不正常且無法使用 Hadoop 來簽入

如果執行個體群組的狀態是 ARRESTED，且叢集狀態是 WAITING，您可以新增叢集步驟來重設所需的核心和任務節點數。新增步驟會恢復叢集的處理步驟，然後執行個體群組的狀態會回到 RUNNING。

如需有關如何針對狀態為遭阻擋的叢集進行重設的詳細資訊，請參閱 [阻擋狀態 \(p. 301\)](#)。

步驟 6：檢閱組態設定

組態設定會指定叢集執行方式的詳細資訊，例如重試任務的次數，以及可用於排序的記憶體量。當您使用 Amazon EMR 啟動叢集，除了標準 Hadoop 組態設定，還有 Amazon EMR 特定的設定。組態設定是存放在叢集的主節點。您可以檢查組態設定，以確保叢集擁有為了可有效執行而所需的資源。

Amazon EMR 會定義預設的 Hadoop 組態設定，其會使用此設定來啟動叢集。這些值是根據您為叢集指定的 AMI 和執行個體類型而定。您可以使用引導操作或透過在任務執行參數中指定新的值來從預設值修改組態設定。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#)。若要判斷引導操作是否已變更組態設定，請檢查引導操作日誌。

Amazon EMR 會記錄用來執行每個任務的 Hadoop 設定。日誌資料會存放在主節點的 `/mnt/var/log/hadoop/history/` 目錄下名為 `job_job-id_conf.xml` 的檔案中，其中任務的識別符會取代 `job-id`。如果您已啟用日誌存檔，系統會將此資料複製到在 `logs/date/jobflow-id/jobs` 資料夾的 Amazon S3 中，其中 `date` 是任務執行的日期而 `jobflow-id` 是叢集識別符。

以下 Hadoop 任務組態設定特別適用於研究效能問題。如需 Hadoop 組態設定以及這些設定如何影響 Hadoop 行為的詳細資訊，請移至 <http://hadoop.apache.org/docs/>。

組態設定	敘述
<code>dfs.replication</code>	要將單一區塊（例如硬碟區塊）複製到其中的 HDFS 節點數，以產生類似 RAID 的環境。決定 HDFS 節點的數量，其中包含區塊複本。
<code>io.sort.mb</code>	可用於排序的記憶體總數。這個值應該是 10 乘以 <code>io.sort.factor</code> 。此設定還可用於計算任務節點所用的記憶體總數，方法是將 <code>io.sort.mb</code> 乘以 <code>mapred.tasktracker.ap.tasks.maximum</code> 來計算而得。
<code>io.sort.spill.percent</code>	此值會在排序時用到，在該時間點會開始使用磁碟，因為配置的排序記憶體即將用盡。
<code>mapred.child.java.opts</code>	已廢除。改用 <code>mapred.map.child.java.opts</code> 和 <code>mapred.reduce.child.java.opts</code> 。TaskTracker 在為要在其中執行任務啟動 JVM 時使用的 Java 選項。設定最大記憶體大小的常見參數為「 <code>-Xmx</code> 」。
<code>mapred.map.child.java.opts</code>	TaskTracker 在為要在其中執行映射啟動 JVM 時使用的 Java 選項。設定最大記憶體堆積大小的常見參數為「 <code>-Xmx</code> 」。
<code>mapred.map.tasks.speculative.execution</code>	決定相同任務的映射任務嘗試是否會平行啟動。
<code>mapred.reduce.tasks.speculative.execution</code>	決定相同任務的縮減任務嘗試是否會平行啟動。
<code>mapred.map.max.attempts</code>	映射任務可以嘗試的次數上限。如果所有次數皆失敗，那麼會將映射任務標示為失敗。
<code>mapred.reduce.child.java.opts</code>	TaskTracker 在為要在其中執行縮減啟動 JVM 時使用的 Java 選項。設定最大記憶體堆積大小的常見參數為「 <code>-Xmx</code> 」。
<code>mapred.reduce.max.attempts</code>	縮減任務可以嘗試的次數上限。如果所有次數皆失敗，那麼會將縮減任務標示為失敗。
<code>mapred.reduce.slowstart.completed.maps</code>	在嘗試縮減任務前應完成的映射任務數。等待時間不足可能會在嘗試時導致「擷取失敗太多次」錯誤。

組態設定	敘述
mapred.reuse.jvm.num.tasks	任務會在單一 JVM 中執行。指定可能重複使用相同 JVM 的任務數。
mapred.tasktracker.map.tasks.maximum	映射期間每一任務節點可平行執行的最大任務數。
mapred.tasktracker.reduce.tasks.maximum	縮減期間每一任務節點可平行執行的最大任務數。

如果叢集任務需要使用大量記憶體，您可以讓每個核心節點使用較少的任務，並降低任務追蹤器堆積大小來增強效能。

步驟 7：檢查輸入資料

查看輸入資料。確認資料在索引鍵值間是否平均分配？如果您的資料分布明顯集中於一或幾個索引鍵值，系統可能會將處理負載映射到少量的節點，而其他節點會處於閒置的狀態。分布不平均的工作可能會導致處理時間變慢。

分佈不平衡的資料集範例會依字母排序單字來執行叢集，但會讓僅包含一個單字的資料集從字母「a」開始。當對工作進行映射，處理以「a」為開頭值的節點可能會過度負載，而處理以其他字母為開頭單字的節點則會閒置。

Amazon EMR 中的常見錯誤

叢集失敗或處理資料速度緩慢可能有許多原因。以下區段列出最常見的問題和修復建議。

主題

- [輸入和輸出錯誤 \(p. 321\)](#)
- [許可錯誤 \(p. 323\)](#)
- [資源錯誤 \(p. 324\)](#)
- [串流叢集錯誤 \(p. 330\)](#)
- [自訂 JAR 叢集錯誤 \(p. 331\)](#)
- [Hive 叢集錯誤 \(p. 331\)](#)
- [VPC 錯誤 \(p. 332\)](#)
- [AWS GovCloud \(US-West\) 錯誤 \(p. 335\)](#)
- [其他問題 \(p. 335\)](#)

輸入和輸出錯誤

以下是在叢集輸入和輸出操作時常見的錯誤。

主題

- [Amazon Simple Storage Service \(Amazon S3\) 的路徑是否有至少三個斜線？ \(p. 322\)](#)
- [您是否想要嘗試以遞迴的方式周遊輸入目錄？ \(p. 322\)](#)
- [您的輸出目錄是否已存在？ \(p. 322\)](#)
- [您是否想要嘗試使用 HTTP URL 來指定資源？ \(p. 322\)](#)
- [您是否使用無效名稱格式來參照 Amazon S3 儲存貯體？ \(p. 322\)](#)

- 您在 Amazon S3 之間來回載入資料時是否遇到困難？(p. 322)

Amazon Simple Storage Service (Amazon S3) 的路徑是否有至少三個斜線？

指定 Amazon S3 儲存貯體時，您必須在 URL 結尾包含終止斜線。例如，與其以「`s3n://aws-s3-bucket1`」的形式來參考儲存貯體，您應該使用「`s3n://aws-s3-bucket1/`」，否則在大部分情況下，Hadoop 會將您的叢集視為失敗。

您是否想要嘗試以遞迴的方式周遊輸入目錄？

Hadoop 不會以遞迴的方式搜尋檔案的輸入目錄。如果您的目錄結構是 `/corpus/01/01.txt`、`/corpus/01/02.txt`、`/corpus/02/01.txt` 等等，而且您對於叢集指定 `/corpus/` 做為輸入參數，則 Hadoop 會找不到該輸入檔，因為 `/corpus/` 目錄是空的，而且 Hadoop 不會檢查子目錄的內容。同樣地，Hadoop 不會以遞迴的方式檢查 Amazon S3 儲存貯體的子目錄。

輸入檔案必須直接在輸入目錄中或您指定的 Amazon S3 儲存貯體，而不是在子目錄中。

您的輸出目錄是否已存在？

如果您指定的輸出路徑已存在，在大部分情況下，Hadoop 叢集將叢集視為失敗。這表示如果您執行叢集一次，然後使用完全相同的參數重新執行一次，很可能第一次會成功，但在第一次執行後就不再能夠運作，因為該輸出路徑已存在且會導致連續執行失敗。

您是否想要嘗試使用 HTTP URL 來指定資源？

Hadoop 不接受使用 `http://` 字首的資源位置。您不能使用 HTTP URL 來參考資源。例如，使用 `http://mysite/myjar.jar` 做為 JAR 參數的傳遞會導致叢集失敗。

您是否使用無效名稱格式來參照 Amazon S3 儲存貯體？

如果您嘗試使用儲存貯體名稱（例如「`aws-s3-bucket1.1`」）搭配 Amazon EMR，您的叢集將會失敗，因為 Amazon EMR 需要儲存貯體名稱是有效的 RFC 2396 主機名稱；名稱結尾不得是數字。此外，由於 Hadoop 的要求，與 Amazon EMR 搭配使用的 Amazon S3 儲存貯體名稱必須僅包含小寫字母、數字、句點(.) 和連字號(-)。如需如何格式化 Amazon S3 儲存貯體的更多相關資訊，請參閱 Amazon Simple Storage Service Developer Guide 中的 [儲存貯體限制](#)。

您在 Amazon S3 之間來回載入資料時是否遇到困難？

Amazon S3 是 Amazon EMR 最熱門的輸入和輸出來源。一般錯誤是將 Amazon S3 視為一般檔案系統。您在執行叢集時，需要考量 Amazon S3 和檔案系統之間的差異。

- 如果在 Amazon S3 中發生內部錯誤，您的應用程式需要從容地處理此問題和重新嘗試操作。
- 如果對 Amazon S3 的呼叫需時太久，您的應用程式可能需要降低它呼叫 Amazon S3 的頻率。
- 列出 Amazon S3 儲存貯體中的所有物件是一種昂貴的呼叫。您的應用程式應將此類操作的執行次數降到最低。

有多種方法可改善叢集與 Amazon S3 互動的方式。

- 使用 Amazon EMR 的最新版本來啟動您的叢集。
- 使用 S3DistCp 將物件傳入和傳出 Amazon S3。S3DistCp 實作錯誤處理、重試和退避來符合 Amazon S3 的需求。如需詳細資訊，請參閱 [使用 S3DistCp 的分散式複製](#)。

- 設計您的應用程式，並保持最終一致性。在叢集執行中時使用中繼資料儲存體的 HDFS，而 Amazon S3 僅會輸出初始資料並輸出最終結果。
- 如果您的叢集每秒會將 200 個或多個交易遞交至 Amazon S3，請[聯絡支援](#)以準備讓儲存貯體獲得每秒更佳的交易，請考慮使用[Amazon S3 效能秘訣和技巧](#)中所述的金鑰分割區策略。
- 將 Hadoop 組態設定 `io.file.buffer.size` 設定為 65536。這可讓 Hadoop 花費較少的時間來搜尋 Amazon S3 物件。
- 如果您的叢集不斷發生 Amazon S3 並行問題，請考量停用 Hadoop 推測性執行功能。您可透過 `mapred.map.tasks.speculative.execution` 及 `mapred.reduce.tasks.speculative.execution` 組態設定來執行此操作。在針對緩慢叢集進行故障排除時也很有用。
- 如果您執行的是 Hive 叢集，請參閱 [您在 Amazon S3 與 Hive 之間來回載入資料時是否遇到困難？\(p. 332\)](#)。

如需更多資訊，請參閱 Amazon Simple Storage Service Developer Guide中的 [Amazon S3 錯誤最佳實務](#)。

許可錯誤

以下為使用許可或登入資料時的一些常見的錯誤。

主題

- [您是否將正確的登入資料傳遞到 SSH？\(p. 323\)](#)
- [如果您使用的是 IAM，您是否已設定適當的 Amazon EC2 政策設定？\(p. 324\)](#)

您是否將正確的登入資料傳遞到 SSH？

如果您無法使用 SSH 連接到主節點，很可能是因為您的安全登入資料有問題。

首先，檢查包含 SSH 金鑰的 .pem 檔案是否有適當的許可。您可以使用 chmod 來變更 .pem 檔案的許可，如下所示，其中請使用您自己的 .pem 檔案名稱來取代 mykey.pem。

```
chmod og-rwx mykey.pem
```

第二種可能性是，您使用的不是建立叢集時所指定的金鑰對。如果您建立的是多個金鑰對，作法會簡單得多。檢查 Amazon EMR 主控台中的叢集詳細資訊（或使用 CLI 中的 `--describe` 選項），確認是否有在叢集建立時所指定的金鑰對名稱。

在驗證您使用的是正確的金鑰對，且 .pem 檔案的許可設定是正確的，您可以使用以下命令來使用 SSH 連接到主節點，其中您會使用 .pem 檔案的名稱來取代 mykey.pem，並使用主節點公有 DNS 名稱（可透過 CLI 中的 `--describe` 選項或透過 Amazon EMR 主控台來取得。）來取代 `hadoop@ec2-01-001-001-1.compute-1.amazonaws.com`。

Important

您必須在連接到 Amazon EMR 叢集節點時使用登入名稱 `hadoop`，否則，可能會發生與 `Server refused our key` 類似的錯誤。

```
ssh -i mykey.pem hadoop@ec2-01-001-001-1.compute-1.amazonaws.com
```

如需更多詳細資訊，請參閱 [使用 SSH 連接至主節點 \(p. 277\)](#)。

如果您使用的是 IAM，您是否已設定適當的 Amazon EC2 政策設定？

由於 Amazon EMR 使用 EC2 執行個體做為節點，Amazon EMR 的 IAM 使用者還必須具備特定 Amazon EC2 政策集，Amazon EMR 才能夠代表 IAM 使用者管理那些執行個體。如果您沒有設定所需的許可，Amazon EMR 會傳回錯誤："User account is not authorized to call EC2."（「使用者帳戶無權呼叫 EC2。」）

如需更多有關 IAM 帳戶需要設定以執行 Amazon EMR 之 Amazon EC2 政策的詳細資訊，請參閱 [Amazon EMR 如何搭配 IAM 運作 \(p. 154\)](#)。

資源錯誤

以下錯誤通常肇因為叢集上的限制資源。

主題

- [叢集由於 NO_SLAVE_LEFT 和叢集節點 FAILED_BY_MASTER 而終止 \(p. 324\)](#)
- [無法複寫區塊，僅能設法複寫到零節點。 \(p. 326\)](#)
- [超過 EC2 配額 \(p. 326\)](#)
- [太多擷取失敗 \(p. 326\)](#)
- [檔案只能複製到 0 個節點，而不是 1 個 \(p. 327\)](#)
- [列入封鎖清單的節點 \(p. 328\)](#)
- [調節錯誤 \(p. 328\)](#)
- [不支援的執行個體類型 \(p. 329\)](#)
- [EC2 容量已滿 \(p. 329\)](#)

叢集由於 NO_SLAVE_LEFT 和叢集節點 FAILED_BY_MASTER 而終止

通常會發生這種情況，是因為終止保護已停用，而且所有核心節點超過 `yarn-site.xml` 檔案相對應的 `yarn-site` 組態分類之中使用率閾值上限所指定的磁碟儲存容量。此值預設為 90%。核心節點的磁碟使用率超過使用率閾值時，YARN NodeManager 運作狀態服務會報告節點為 UNHEALTHY。在此狀態中，Amazon EMR 會將節點列入封鎖清單，而不會對其分配 YARN 容器。如果節點維持運作狀態不佳的狀態持續 45 分鐘，Amazon EMR 會將終止的相關聯 Amazon EC2 執行個體標記為 FAILED_BY_MASTER。核心節點相關聯的所有 Amazon EC2 執行個體均已標示為終止時，叢集會以 NO_SLAVE_LEFT 狀態終止，因為沒有資源可執行任務。

一個核心節點超出磁碟使用率可能會導致連鎖反應。如果單一節點由於 HDFS 超出磁碟使用率閾值，則其他節點也可能已接近閾值。第一個節點超出磁碟使用率閾值，因此 Amazon EMR 將其列入黑名單。這會對於其餘節點增加磁碟使用率的負擔，因為其餘節點會開始複製在列入黑名單的節點上彼此之間缺少的 HDFS 資料。每個節點接著都會以類似的方式變成 UNHEALTHY，叢集最終會終止。

最佳實務與建議

設定叢集硬體的足夠儲存

您建立叢集時，請確保有足夠的核心節點，而且每個產品都擁有對於 HDFS 充足的執行個體存放區和 EBS 儲存磁碟區。如需更多詳細資訊，請參閱 [計算叢集的必要 HDFS 容量 \(p. 117\)](#)。您也可以手動或使用自動擴展將核心執行個體新增到現有的執行個體群組。新的執行個體具有與執行個體群組中的其他執行個體相同的儲存體組態。如需更多詳細資訊，請參閱 [調整叢集資源規模 \(p. 290\)](#)。

啟用終止保護

啟用終止保護。如此一來，如果某個核心節點被列入黑名單，您可以使用 SSH 連接到相關聯的 Amazon EC2 執行個體，以進行故障診斷並恢復資料。如果您啟用終止保護，請注意 Amazon EMR 不會以新的執行個體取代 Amazon EC2 執行個體。如需更多詳細資訊，請參閱 [使用終止保護 \(p. 75\)](#)。

對於 MRUnhealthyNodes CloudWatch 指標建立警示

這個指標會報告呈報 UNHEALTHY 狀態的節點數量。這是相當於 YARN 指標 `mapred.resourcemanager.NoOfUnhealthyNodes`。您可以設定此警示的通知在達到 45 分鐘逾前告知您運作狀態不佳的節點。如需更多詳細資訊，請參閱 [使用 CloudWatch 監控指標 \(p. 262\)](#)。

使用 yarn-site 調整設定

您可以根據您的應用程式需求調整下列節點。例如，對於節點報告 UNHEALTHY 的情況，您可能想要增加 `yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage` 的值來提高磁碟使用率閾值。

您可以在使用 `yarn-site` 組態分類建立叢集時設定這些值。如需詳細資訊，請參閱《Amazon EMR Release Guide》中的[設定應用程式](#)。您也可以使用 SSH 連接到與核心節點相關聯的 Amazon EC2 執行個體，然後使用文字編輯器在 `/etc/hadoop/conf.empty/yarn-site.xml` 中新增值。變更後，您必須重新啟動 Hadoop-yarn-nodemanager，如下所示。

Important

您重新啟動 NodeManager 服務時，除非在您建立叢集時

`yarn.nodemanager.recovery.enabled` 是使用 `yarn-site` 組態分類的設定為 `true`，否則會終止作用中的 YARN 容器。您也必須使用 `yarn.nodemanager.recovery.dir` 屬性指定目錄來存放容器狀態。

```
sudo /sbin/stop hadoop-yarn-nodemanager
sudo /sbin/start hadoop-yarn-nodemanager
```

如需目前 `yarn-site` 屬性和預設值的詳細資訊，請參閱 Apache Hadoop 文件中的 [YARN 預設設定](#)。

屬性	預設值	敘述
<code>yarn.nodemanager.disk-health-checker.interval-ms</code>	120000	磁碟執行運作狀態檢查的頻率 (以秒為單位)。
<code>yarn.nodemanager.disk-health-checker.min-healthy-disks</code>	0.25	NodeManager 啟動新的容器時必須達到的最低正常運作磁碟數量。這對應於 <code>yarn.nodemanager.local-dirs</code> (預設為 Amazon EMR 中的 <code>/mnt/yarn</code>) 和 <code>yarn.nodemanager.log-dirs</code> (預設為 <code>/var/log/hadoop-yarn/containers</code> ，這會透過符號連結來連結到 Amazon EMR 中的 <code>mnt/var/log/hadoop-yarn/containers</code>)。
<code>yarn.nodemanager.disk-health-checker.max-disk-utilization-per-disk-percentage</code>	90.0	磁碟標示為錯誤之前允許的磁碟空間使用率百分比上限。值可介於 0.0 到 100.0 之間。如果值大於或等於 100，NodeManager 會檢查整個磁碟。這適用於 <code>yarn.nodemanager.local-dirs</code>

屬性	預設值	敘述
		和 <code>yarn.nodemanager.log-dirs</code> 。
<code>yarn.nodemanager.disk-health-checker.min-free-space-per-disk-mb</code>	0	磁碟提供的空間下限。這適用於 <code>yarn-nodemanager.local-dirs</code> 和 <code>yarn.nodemanager.log-dirs</code> 。

無法複寫區塊，僅能設法複寫到零節點。

「Cannot replicate block, only managed to replicate to zero nodes.」(無法複寫區塊，僅能設法複寫到零節點。) 的錯誤通常發生在叢集沒有足夠 HDFS 儲存體時。當您在叢集中產生的資料量超過可存放在 HDFS 中的資料量時會發生此錯誤。您僅會在該叢集執行時看到此錯誤，因為當該任務終止時，它將會釋放該任務所使用的 HDFS 空間。

叢集可使用的 HDFS 空間數量，將依用作核心節點的 Amazon EC2 執行個體類型數量而定。任務節點並不適用於 HDFS 儲存體。在每個 Amazon EC2 執行個體上的所有磁碟空間，包括連接至 EBS 儲存體的磁碟，都可供 HDFS 使用。關於每一個 EC2 執行個體類型區域儲存量的詳細資訊，請參閱 Amazon EC2 User Guide for Linux Instances 中的[執行個體類型與系列](#)。

影響 HDFS 空間可用量的另一個因素是複寫因素，它是存放在 HDFS 中用於備援的每個資料區塊的複本數量。複寫因素依叢集中的節點數量而增加：對於有 10 個或更多節點的叢集，每個資料區塊有 3 個複本，有 4 到 9 個節點的叢集，每個區塊有 2 個複本，有 3 個或更少節點的叢集，有 1 個副本(無備援)。總可用 HDFS 空間除以複寫因素。在某些情況，例如節點數量從 9 增加為 10 的時候，增加的複寫因素可確實導致可用 HDFS 空間減少。

例如，一個擁有 10 個 m1.large 類型核心節點叢集，會有可供 HDFS 使用的 2833 GB 空間 ((10 個節點 X 每個節點 850 GB) 除以 3 個複寫因素)。

若您的叢集超出 HDFS 可用空間量，您可新增額外核心節點至您的叢集，或使用資料壓縮以建立更多 HDFS 空間。若您的叢集是能夠停止與重新啟動的，您可考慮使用較大的 Amazon EC2 執行個體類型核心節點。或者您也可以考慮調整複寫因素。但請注意，減少複寫因素便會減少 HDFS 資料備援，以及您從遺失或毀損的 HDFS 區塊中復原的叢集能力。

超過 EC2 配額

如果您看到了 EC2 QUOTA EXCEEDED 訊息，這可能有數個原因。依據其組態的不同，之前的叢集可能需要 5-20 分鐘時間才會終止並釋出配置資源。如果您在嘗試啟動叢集時收到了 EC2 QUOTA EXCEEDED 錯誤，原因可能是剛終止的叢集尚未釋出資源。此訊息也可能是因為執行個體群組，或執行個體機群大小調整為大於該帳戶目前執行個體配額的目標大小所導致。這可以透過自動調整規模來手動或自動進行。

請考量下列選項來解決這個問題：

- [建立支援案例](#)以申請提高配額。
- 如果一個或多個正在執行的叢集未達到容量，請調整執行個體群組的大小，或降低執行個體機群中的目標容量以執行叢集。
- 以較少的 EC2 執行個體或減少的目標容量來建立叢集。

太多擷取失敗

在步驟中或任務嘗試日誌中出現「Too many fetch-failures (太多擷取失敗)」或「Error reading task output (讀取任務輸出時出錯)」錯誤訊息，代表正在執行的任務是依據另一個任務的輸出。當降低任務排入執行佇列，並需要輸出一個或多個映射任務且輸出尚不可用時，通常會發生這種情況。

有幾個可能導致輸出不可用的原因：

- 該必要任務仍正在處理中。這通常是映射任務。
- 若該資料位於不同的執行個體，由於網路連線不佳，資料可能無法使用。
- 若 HDFS 已用於擷取輸出，則 HDFS 可能存在問題。

造成此錯誤最普遍的原因，是因為之前的任務尚在進行。如果減少任務首次嘗試執行時發生錯誤，則這種情況尤其可能發生。您可以透過檢視回傳錯誤的叢集步驟 syslog 日誌，來確認是否屬於此種狀況。若該 syslog 同時顯示映射與進行中的減少任務，這表示該減少階段已開始，同時有映射任務尚未完成。

在日誌中應注意查看的是達到 100%，且隨後降至較低數值的映射進行百分率。當映射百分比達 100% 時，並不表示所有映射任務已完成。那僅代表 Hadoop 正在執行所有的映射任務。若此數值降至 100% 以下，則代表映射任務已失敗，依據組態狀況，Hadoop 可能會嘗試重新排程任務。若在日誌中該對應百分比維持在 100%，請檢視 CloudWatch 指標，特別是 RunningMapTasks，以檢查該對應任務是否仍在進行。您也可在主節點上使用 Hadoop web 介面找到此訊息。

若您正看到此問題，您可以嘗試一些方法：

- 引導該減少階段在開始之前等久一點。您可透過改變 Hadoop 組態設定 mapred.reduce.slowstart.completed.maps 至較長時間以達成此目的。如需更多詳細資訊，請參閱 [建立引導操作來安裝其他軟體 \(p. 86\)](#)。
- 讓縮減器計數符合該叢集的總縮減器功能。您可透過調整該任務 Hadoop 組態設定 mapred.reduce.tasks 以達成此目的。
- 使用組合器類型代碼將需要擷取的輸出量降至最小。
- 檢查該 Amazon EC2 服務並沒有會影響叢集網路效能的問題。您可使用 [運作狀態儀表板](#) 做到這點。
- 檢視您叢集中的執行個體 CPU 與記憶體資源，以確認您的資料處理尚未對您的節點造成過大負擔。如需更多詳細資訊，請參閱 [設定叢集硬體和聯網 \(p. 89\)](#)。
- 檢查您 Amazon EMR 叢集中使用的 Amazon Machine Image (AMI) 版本。若該版本介於 2.3.0 至 2.4.4，請更新至最新版本。特定範圍內 AMI 版本使用的 Jetty 版本，可能會造成無法從映射階段接收輸出。當縮減器無法從映射階段取得輸出時，將出現擷取錯誤。

Jetty 是一個開放原始碼 HTTP 伺服器，以用來在 Hadoop 叢集中進行機器間的通訊。

檔案只能複製到 0 個節點，而不是 1 個

當檔案被寫入至 HDFS 時，它即被複寫至多個核心節點。當您看到此錯誤時，即代表 NameNode 協助程式沒有任何可用的 DataNode 執行個體將資料寫入至 HDFS。意即並未發生區塊複寫。這錯誤可能是由於多個問題所致：

- 該 HDFS 檔案系統可能已將空間用盡。這是最可能的原因。
- DataNode 執行個體在任務執行時可能不可用。
- DataNode 執行個體可能已被封鎖與主節點通訊。
- 在核心執行個體群組中的執行個體可能無法使用。
- 可能遭失權限。例如，JobTracker 協助程式可能沒有建立任務追蹤器資訊的許可。
- DataNode 執行個體保留的空間設定可能不足。透過檢查 dfs.datanode.du.reserved 組態設定來檢查是否屬於這種情況。

欲檢查此問題是否為在磁碟空間外執行的 HDFS 所致，請查看 CloudWatch 中的 HDFSUtilization 指標。若此數值過高，您可新增額外核心節點至該叢集。若您認為可能有一個叢集已經用盡 HDFS 磁碟空間，您可在 CloudWatch 中設定警報，以在 HDFSUtilization 數值超出特定層級時提醒您。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#) 及 [使用 CloudWatch 監控指標 \(p. 262\)](#)。

若 HDFS 空間用盡並非問題，檢查 DataNode 日誌、NameNode 日誌與網路連線，以了解可能阻止 HDFS 複製資料的其他問題。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

列入封鎖清單的節點

NodeManager 協助程式負責於核心節點和任務節點啟動和管理容器。該容器是由主節點上執行的 ResourceManager 協助程式分配給 NodeManager 協助程式。ResourceManager 透過活動訊號監控 NodeManager 節點。

在幾種情況下，ResourceManager 協助程式會將 NodeManager 節點列入封鎖清單，將其從可用於處理任務的節點集區中刪除：

- 若該 NodeManager 節點尚未在過去 10 分鐘 (6 萬毫秒) 內傳送活動訊號至 ResourceManager 協助程式。可使用 `yarn.nm.liveness-monitor.expiry-interval-ms` 組態以設定此期間。如需變更 Yarn 組態設定的詳細資訊，請參閱 Amazon EMR Release Guide 中[設定應用程式](#)的相關文章。
- NodeManager 檢查由 `yarn.nodemanager.local-dirs` 和 `yarn.nodemanager.log-dirs` 所決定的磁碟運作狀態。此檢查包含權限和可用磁碟空間 (< 90%)。如果某個磁碟未通過檢查，該 NodeManager 將停止使用該特定磁碟，但仍會回報該節點的運作狀態良好。如果多個磁碟未通過檢查，該節點會回報為運作狀態不佳至 ResourceManager，且新的容器不會指派給該節點。

若出現超過三個以上的失敗任務，該應用程式主控也可將 NodeManager 節點列入封鎖清單。您可以使用 `mapreduce.job.maxtaskfailures.per.tracker` 組態參數將此變更為較高數值。您可能變更的其他組態設定，控制了在將任務標記為失敗之前嘗試執行任務的次數：`mapreduce.map.max.attempts` 用於對應任務和 `mapreduce.reduce.maxattempts` 用於減少任務。如需變更組態設定的詳細資訊，請參閱 Amazon EMR Release Guide 中[設定應用程式](#)的相關文章。

調節錯誤

因為另一個服務已調節該活動，導致 Amazon EMR 無法完成請求時，會出現「Throttled from [Amazon EC2](#) while launching cluster」(在啟動叢集時從 [Amazon EC2](#) 調節) 和「Failed to provision instances due to throttling from [Amazon EC2](#)」(由於從 [Amazon EC2](#) 進行調節而無法佈建執行個體) 的錯誤。Amazon EC2 是調節錯誤最常見的來源，但其他服務也可能是調節錯誤的原因。[AWS 服務限制](#)適用於每個區域以提高效能，而調節錯誤表示您已超出該區域中帳戶的服務限制。

可能原因

Amazon EC2 調節錯誤最常見的來源，就是大量叢集執行個體的啟動，造成您的 EC2 執行個體服務超出限制。叢集執行個體可能會因為下列原因而啟動：

- 新叢集的建立。
- 手動調整叢集規模。如需更多詳細資訊，請參閱 [手動調整執行中的叢集規模 \(p. 298\)](#)。
- 因為自動擴展規則，導致叢集中的執行個體群組新增執行個體 (向外擴展)。如需更多詳細資訊，請參閱 [了解自動調整規模規則 \(p. 291\)](#)。
- 叢集中的執行個體機群新增執行個體，以滿足增加的目標容量。如需更多詳細資訊，請參閱 [設定執行個體機群 \(p. 105\)](#)。

也有可能是因為向 Amazon EC2 進行的 API 請求頻率或類型導致調節錯誤。有關 Amazon EC2 如何調節 API 請求的詳細資訊，請參閱 Amazon EC2 API Reference 中的 [查詢 API 請求率](#)。

解決方案

請考量下列解決方案：

- [建立支援案例](#)以申請 Service limit increase (提高服務限制)。
- 如果您的叢集按照相同的排程啟動 (例如，在每小時的一開始)，請考慮大量的開始時間。

- 如果您有針對尖峰需求設定大小的叢集，並且定期擁有執行個體容量，請考慮指定自動擴展以隨需新增和移除執行個體。如此便能更有效地使用執行個體，並根據需求設定檔，可以在帳戶的指定時間請求更多的執行個體。如需更多詳細資訊，請參閱 [於 Amazon EMR 使用自動調整規模 \(p. 291\)](#)。

不支援的執行個體類型

如果您建立了一個叢集，而該叢集失敗並顯示錯誤訊息「The requested instance type *InstanceType* is not supported in the requested Availability Zone」(要求的可用區域中不支援所要求的執行個體類型 *InstanceType*)，這表示您已建立了叢集，並為一個或多個執行個體群組 (這些群組在叢集建立的區域和可用區域中不受 Amazon EMR 支援) 指定了執行個體類型。Amazon EMR 可能支援區域內一個可用區域的執行個體類型，而不支援另一個。您為叢集選擇的子網路決定了區域內的可用區域。

解決方案

在您使用 Amazon EMR 主控台建立叢集時，執行個體清單會自動限制為可用的執行個體類型，因此當您使用 AWS CLI 或 Amazon EMR API 以編寫程式的方式建立叢集時，通常會發生此錯誤。

區域和可用區域支援的 Amazon EMR 執行個體類型整合清單尚不可用，因此任何解決方案的第一步，是判斷在所需的可用區域中是否有所需的執行個體類型可用。

使用 Amazon EMR 管理主控台判定可用區域中可用的執行個體類型

1. Open the Amazon EMR console at <https://console.aws.amazon.com/elasticmapreduce/>.
2. 選擇 Create cluster (建立叢集)，Go to advanced options (前往進階選項)。
3. 選擇 Next (下一步) 以檢視 Hardware Configuration (硬體組態) 選項。
4. 選擇 Network (網路)，然後叢集的 EC2 Subnet (EC2 子網路)。
5. 在 Instance type (執行個體類型) 下任何的 Master (主節點)、Core (核心) 或 Task (任務) Node types (節點類型) 選擇預設執行個體類型旁的鉛筆圖示。
6. 與您選擇的 EC2 Subnet (EC2 子網路) 關聯的區域和可用區域中可用的執行個體類型清單會顯示。
7. 您可以繼續建立叢集，或選擇 Cancel (取消)，選擇不同的 Network (網路) 和 EC2 Subnet (EC2 子網路)，並重複上一個步驟。

使用 AWS CLI 判定可用區域中可用的執行個體類型

- 使用 `ec2 run-instances` 命令搭配 `--dry-run` 選項。在下方的範例中，將您要使用的執行個體類型取代 `m5.xlarge`、以該執行個體類型關聯的 AMI 取代 `ami-035be7bafff33b6b6`，並以可用區域中您要查詢的子網路取代 `subnet-12ab3c45`。

```
aws ec2 run-instances --instance-type m5.xlarge --dry-run --image-id ami-035be7bafff33b6b6 --subnet-id subnet-12ab3c45
```

在您決定可用的執行個體類型後，您便可執行任何以下的操作：

- 在同一個區域和 EC2 子網路中建立叢集，並選擇與初始選擇具備類似功能的不同執行個體類型。如需支援的執行個體類型清單，請參閱 [支援的執行個體類型 \(p. 91\)](#)。如需比較 EC2 執行個體類型的功能，請參閱 [Amazon EC2 執行個體類型](#)。
- 在可用區域中選擇叢集的子網路，該可用區域的執行個體類型為可用且受 Amazon EMR 支援。

EC2 容量已滿

建立叢集或將執行個體新增到叢集時，會出現「EC2 is out of capacity for *InstanceType*」(*InstanceType* 的 EC2 容量已滿) 錯誤，並且由於需求而導致區域或可用區域中不再存在該 EC2 執行個體類型。您為叢集選擇的子網路決定了可用區域。

如果要建立叢集，您可以指定具有類似功能的其他執行個體類型，或在其他區域中建立叢集，或在可用區域中選擇所需執行個體類型可用的子網路。

如果將執行個體新增到正在執行的叢集，您可以修改執行個體群組組態或執行個體機群組態，以新增具有類似功能的可用執行個體類型。如需支援的執行個體類型清單，請參閱 [支援的執行個體類型 \(p. 91\)](#)。如需比較 EC2 執行個體類型的功能，請參閱 [Amazon EC2 執行個體類型](#)。您也可以終止叢集並在執行個體類型可用的區域和可用區域中重新建立叢集。

串流叢集錯誤

您通常可以在 `syslog` 檔案中發現串流錯誤的原因。從 Steps (步驟) 窗格即可連結至該訊息。

以下是串流叢集常見的錯誤。

主題

- [傳送至映射器的資料格式是否錯誤？ \(p. 330\)](#)
- [您的指令碼是否逾時？ \(p. 330\)](#)
- [您是否使用無效串流引數來進行傳遞？ \(p. 330\)](#)
- [您的指令碼結束時是否有發生錯誤？ \(p. 331\)](#)

傳送至映射器的資料格式是否錯誤？

如果是這種情況，請尋找在任務嘗試日誌的失敗任務嘗試中 `syslog` 檔案中的錯誤訊息。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您的指令碼是否逾時？

映射器或縮減器指令碼的預設逾時為 600 秒。如果您的指令碼所耗時間超過此值，任務嘗試將會失敗。您可以透過檢查在任務嘗試日誌的失敗任務嘗試中的 `syslog` 檔案來確認是否為此狀況。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您可以透過為 `mapred.task.timeout` 組態設定設定新的值來變更時間限制。此設定會指定一個毫秒數，若一個任務在經該時間後沒有讀取輸入、寫入輸出、或更新其狀態字串，Amazon EMR 便會終止該任務。您可以透過傳遞額外的串流引數 `-jobconf mapred.task.timeout=800000` 來更新這個值。

您是否使用無效串流引數來進行傳遞？

Hadoop 串流僅支援以下引數。如果您是使用如下所示以外的引數來進行傳遞，叢集將會失敗。

```
-blockAutoGenerateCacheFiles
-cacheArchive
-cacheFile
-cmdenv
-combiner
-debug
-input
-inputformat
-inputreader
-jobconf
-mapper
-numReduceTasks
-output
-outputformat
-partitioner
-reducer
```

-verbose

此外，Hadoop 串流只能辨識使用 Java 語法（也就是以單一連字號為開頭）傳遞的引數。如果您使用以雙連字號為開頭的引數來進行傳遞，叢集將會失敗。

您的指令碼結束時是否有發生錯誤？

如果您的映射器或縮減器指令碼結束時出現錯誤，您可以找到在失敗任務嘗試中任務嘗試日誌的 `stderr` 檔案中找到該錯誤。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

自訂 JAR 叢集錯誤

以下是自訂 JAR 叢集常見的錯誤。

主題

- 您的 JAR 是否在建立任務時擲回例外狀況？(p. 331)
- 您的 JAR 是否在對應任務中擲回一個錯誤？(p. 331)

您的 JAR 是否在建立任務時擲回例外狀況？

如果您的自訂 JAR 主要程式在建立 Hadoop 任務擲出例外狀況，檢視該狀況的最佳位置為步驟日誌的 `syslog` 檔案。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您的 JAR 是否在對應任務中擲回一個錯誤？

如果您的自訂的 JAR 和映射器在處理輸入資料時擲出了例外狀況，檢視該狀況的最佳位置為任務嘗試日誌的 `syslog` 檔案。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

Hive 叢集錯誤

您通常可在 `syslog` 檔案中找到 Hive 錯誤的原因，您可從 Steps (步驟) 窗格連結至該檔案。如果您無法在該處判斷問題，請查看 Hadoop 任務嘗試錯誤訊息。從 Task Attempts (任務嘗試) 窗格即可連結至該訊息。

以下是 Hive 叢集常見的錯誤。

主題

- 您是否使用最新版的 Hive？(p. 331)
- 您是否在 Hive 指令碼中遇到語法錯誤？(p. 331)
- 任務是否在互動執行時失敗？(p. 332)
- 您在 Amazon S3 與 Hive 之間來回載入資料時是否遇到困難？(p. 332)

您是否使用最新版的 Hive？

最新版的 Hive 包含所有最新的修補程式和錯誤修正，或許可以解決您的問題。

您是否在 Hive 指令碼中遇到語法錯誤？

如果某個步驟失敗，請查看日誌的 `stdout` 檔案中執行 Hive 指令碼的步驟。如果錯誤不是在該處發生，請查看任務嘗試日誌的 `syslog` 檔案中是否有失敗的任務嘗試。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

任務是否在互動執行時失敗？

如果您在主節點上以互動方式執行 Hive，但叢集失敗，請查看任務嘗試日誌中的 `syslog` 項目，了解失敗的任務。如需更多詳細資訊，請參閱 [檢視日誌檔 \(p. 250\)](#)。

您在 Amazon S3 與 Hive 之間來回載入資料時是否遇到困難？

如果您無法存取 Amazon S3 中的資料，請先查看 [您在 Amazon S3 之間來回載入資料時是否遇到困難？\(p. 322\)](#) 中列出的可能原因。如果這些問題都不是原因所在，請考慮下列 Hive 專屬的選項。

- 務必確認您使用的是最新版的 Hive，當中包含所有最新的修補程式和錯誤修正，或許可以解決您的問題。如需詳細資訊，請參閱 [Apache Hive](#)。
- 使用 `INSERT OVERWRITE` 需要列出 Amazon S3 儲存貯體或資料夾的內容。這是一項昂貴的操作。如有可能，請手動刪除路徑而不要使用 Hive 清單，並刪除現有物件。
- 如果您使用早於 5.0 的 Amazon EMR 發行版本，您可以使用 HiveQL 中的下列命令來預先快取叢集上的本機 Amazon S3 清單操作結果：

```
set hive.optimize.s3.query=true;
```

- 盡可能使用靜態分割區。
- 在某些 Hive 和 Amazon EMR 版本中，使用 `ALTER TABLES` 可能會失敗，因為表格存放在與 Hive 所預期不同的位置。解決方法是新增或更新 `/home/hadoop/conf/core-site.xml` 的下列項目：

```
<property>
  <name>fs.s3n.endpoint</name>
  <value>s3.amazonaws.com</value>
</property>
```

VPC 錯誤

以下是 Amazon EMR 中 VPC 組態常見的錯誤。

主題

- [子網路組態無效 \(p. 332\)](#)
- [缺少 DHCP 選項集 \(p. 333\)](#)
- [許可錯誤 \(p. 333\)](#)
- [導致 START_FAILED 的錯誤 \(p. 334\)](#)
- [叢集 Terminated with errors 和 NameNode 啟動失敗 \(p. 334\)](#)

子網路組態無效

在 Cluster Details (叢集詳細資訊) 頁面上的 Status (狀態) 欄位中，您會看到類似下面這樣的錯誤：

The subnet configuration was invalid: Cannot find route to InternetGateway in main RouteTable `rtb-id` for vpc `vpc-id`.

若要解決這個問題，您必須建立網際網路閘道，並將它連接到您的 VPC。如需詳細資訊，請參閱 [將網際網路閘道新增至您的 VPC](#)。

或者，確認您已將 VPC 中的 Enable DNS resolution (啟用 DNS 解析) 和 Enable DNS hostname support (啟用 DNS 主機名稱支援) 設定為啟用狀態。如需詳細資訊，請參閱 [使用 DNS 與您的 VPC 搭配](#)。

缺少 DHCP 選項集

您在叢集系統日誌 (syslog) 中看見發生類似以下錯誤的步驟失敗：

```
ERROR org.apache.hadoop.security.UserGroupInformation (main):  
PrivilegedActionException as:hadoop (auth:SIMPLE) cause:java.io.IOException:  
org.apache.hadoop.yarn.exceptions.ApplicationNotFoundException: Application  
with id 'application_id' doesn't exist in RM.
```

或

```
ERROR org.apache.hadoop.streaming.StreamJob (main): Error Launching job :  
org.apache.hadoop.yarn.exceptions.ApplicationNotFoundException: Application  
with id 'application_id' doesn't exist in RM.
```

若要解決這個問題，您必須設定包含 DHCP 選項集的 VPC，且其參數設定為以下值：

Note

如果您使用 AWS GovCloud (US-West) 區域，請將網域名稱設定為 **us-gov-west-1.compute.internal**，而非下列範例中使用的值。

- domain-name (domain-name) = **ec2.internal**

如果您的區域是 US East (N. Virginia)，請使用 **ec2.internal**。若是其他區域，則使用 **region-name.compute.internal**。以 us-west-2 為例，使用 domain-name (domain-name)=**us-west-2.compute.internal**。

- domain-name-servers (domain-name-servers) = **AmazonProvidedDNS**

如需詳細資訊，請參閱「[DHCP 選項集](#)」。

許可錯誤

在 stderr 日誌中的步驟失敗，表示 Amazon S3 資源沒有適當的許可。這是 403 錯誤，且錯誤會像這樣：

```
Exception in thread "main" com.amazonaws.services.s3.model.AmazonS3Exception: Access Denied  
(Service: Amazon S3; Status Code: 403; Error Code: AccessDenied; Request ID: REQUEST_ID)
```

如果 ActionOnFailure 設為 TERMINATE_JOB_FLOW，那麼這可能會導致叢集終止，且狀態為 SHUTDOWN_COMPLETED_WITH_ERRORS。

解決這個問題的幾種方法包括：

- 如果您在 VPC 中使用的是 Amazon S3 儲存貯體政策，務必藉由建立 VPC 端點，並於建立端點時選取「Policy」(政策) 選項底下的 Allow all (全部允許)，提供所有儲存貯體的存取權限。
- 確認與 S3 資源相關聯的任何政策都包含您啟動叢集所在的 VPC。
- 嘗試從叢集執行下列命令，確認您可以存取儲存貯體

```
hadoop fs -copyToLocal s3://path-to-bucket /tmp/
```

- 您可以在叢集的 log4j.logger.org.apache.http.wire 檔案中將 DEBUG 參數設定為 /home/hadoop/conf/log4j.properties，藉此取得更多特定的偵錯資訊。您嘗試從叢集存取儲存貯體之後，可以查看 stderr 日誌檔。日誌檔將提供更多詳細資訊：

```
Access denied for getting the prefix for bucket - us-west-2.elasticmapreduce with path  
samples/wordcount/input/
```

```
15/03/25 23:46:20 DEBUG http.wire: >> "GET /?prefix=samples%2Fwordcount%2Finput%2F&delimiter=%2F&max-keys=1 HTTP/1.1[\r][\n]"
15/03/25 23:46:20 DEBUG http.wire: >> "Host: us-west-2.elasticmapreduce.s3.amazonaws.com[\r][\n]"
```

導致 START_FAILED 的錯誤

在 AMI 3.7.0 以前，對於已指定主機名稱的 VPC，Amazon EMR 會將子網路的內部主機名稱與自訂網域地址相映射，如下所示：`ip-X.X.X.X.customdomain.com.tld`。例如，如果主機名稱是 `ip-10.0.0.10` 且 VPC 的網域名稱選項設定為 `customdomain.com`，則得到的 Amazon EMR 所映射的主機名稱會是 `ip-10.0.1.0.customdomain.com`。在 `/etc/hosts` 中已新增項目，將主機名稱解析為 `10.0.0.10`。此行為對於 AMI 3.7.0 已改變，Amazon EMR 現在完全允許 VPC 的 DHCP 組態。以往客戶也可以使用引導操作來指定主機名稱映射。

如果您想要保留這種行為，則必須提供自訂網域所需的 DNS 和轉發解析設定。

叢集 Terminated with errors 和 NameNode 啟動失敗

在使用自訂 DNS 網域名稱的 VPC 中啟動 EMR 叢集時，您的叢集可能會失敗，並且在主控台中出現以下錯誤訊息：

```
Terminated with errors  On the master instance(instance-id), bootstrap action 1 returned a non-zero return code
```

失敗是由於 NameNode 無法啟動所導致的結果。這樣將會在 NameNode 日誌中產生下列錯誤訊息，其 Amazon S3 URI 的格式如下：`s3://mybucket/logs/cluster-id/daemons/master instance-id/hadoop-hadoop-namenode-master node hostname.log.gz`：

```
2015-07-23 20:17:06,266 WARN
    org.apache.hadoop.hdfs.server.namenode.FSNamesystem (main): Encountered exception
    loading fsimage  java.io.IOException: NameNode is not formatted.
    at

    org.apache.hadoop.hdfs.server.namenode.FSImage.recoverTransitionRead(FSImage.java:212)
    at

    org.apache.hadoop.hdfs.server.namenode.FSNamesystem.loadFSImage(FSNamesystem.java:1020)
    at

    org.apache.hadoop.hdfs.server.namenode.FSNamesystem.loadFromDisk(FSNamesystem.java:739)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.loadNamesystem(NameNode.java:537)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.initialize(NameNode.java:596)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.<init>(NameNode.java:765)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.<init>(NameNode.java:749)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.createNameNode(NameNode.java:1441)
    at
    org.apache.hadoop.hdfs.server.namenode.NameNode.main(NameNode.java:1507)
```

這是因為有一個潛在問題，那就是在 VPC 中啟動 EMR 叢集時，EC2 執行個體可能有多組完整網域名稱，它會同時使用 AWS 提供的 DNS 伺服器及使用者提供的自訂 DNS 伺服器。如果使用者提供的 DNS 伺服器未對 EMR 叢集中用來指定節點的任何 A 記錄提供任何指標 (PTR) 記錄，那麼叢集以此方式設定時，將會無法啟動。解決方法是針對 EC2 執行個體在 VPC 的任何一個子網路中啟動時所建立的每一個 A 記錄新增 1 個 PTR 記錄。

AWS GovCloud (US-West) 錯誤

AWS GovCloud (US-West) 區域與其他區域不同之處在於其安全性、組態和預設設定。因此，使用下列檢查清單可先對 Amazon EMR 區域特有的 AWS GovCloud (US-West) 錯誤進行故障診斷，再採取較為一般的故障診斷建議。

- 確認您的 IAM 角色設定正確。如需更多詳細資訊，請參閱 [將 Amazon EMR 許可的 IAM 角色設定為 AWS 服務和資源 \(p. 156\)](#)。
- 確認您的 VPC 組態具備正確設定的 DNS 解析/主機名稱支援、網際網路閘道及 DHCP 選項集參數。如需更多詳細資訊，請參閱 [VPC 錯誤 \(p. 332\)](#)。

如果這些步驟無法解決問題，請繼續進行常見 Amazon EMR 錯誤的故障排除步驟。如需更多詳細資訊，請參閱 [Amazon EMR 中的常見錯誤 \(p. 321\)](#)。

其他問題

您是否無法看見您預期在叢集清單頁面或從 ListClusters API 傳回結果中的叢集？

請檢查以下內容：

- 叢集年齡小於兩個月。Amazon EMR 會保留已完成叢集的中繼資料相關資訊兩個月的時間來供您免費參考。主控台不提供從主控台刪除已完成叢集的方式；兩個月後，系統即會自動為您移除。
- 您有檢視叢集的許可。
- 您可以檢視正確的區域。

故障診斷 Lake Formation 叢集 (Beta 版)

本節會逐步解說使用 Amazon EMR 搭配 AWS Lake Formation 時常見問題的故障診斷程序。

工作階段過期

EMR Notebooks 和 Zeppelin 的工作階段過期是由 Lake Formation 的 Maximum CLI/API session duration IAM 角色所控制。此設定的預設值為 1 小時。當工作階段過期發生時，您會在嘗試執行 Spark SQL 命令時，於筆記本項目的輸出中看到下列訊息。

```
Error 401      HTTP ERROR: 401 Problem accessing /sessions/2/statements.  
Reason: JWT token included in request failed validation.  
Powered by Jetty:// 9.3.24.v20180605  
org.springframework.web.client.HttpClientErrorException: 401 JWT token included in request  
failed validation...
```

若要驗證您的工作階段，請重新整理頁面。系統會提示您使用 IdP 重新驗證身分，並重新導向回筆記本。您可以在重新驗證之後繼續執行查詢。

請求的資料表上沒有使用者的許可

嘗試存取您無權存取的資料表時，您會在嘗試執行 Spark SQL 命令時，於筆記本項目的輸出中會看到下例外狀況。

```
org.apache.spark.sql.AnalysisException: org.apache.hadoop.hive.ql.metadata.HiveException:  
  Unable to fetch table table.  
  Resource does not exist or requester is not authorized to access requested permissions.  
(Service: AWSGlue; Status Code: 400; Error Code: AccessDeniedException; Request ID: ...)
```

若要存取資料表，您必須更新 Lake Formation 中與此資料表相關聯的許可，將存取權授予使用者。

插入、建立和更改資料表：Beta 版中不支援

不支援 Lake Formation 政策保護資料庫中插入、建立或更改表格。當執行這些操作時，您會在嘗試執行 Spark SQL 命令時，於筆記本項目的輸出中看到下列例外狀況。

```
java.io.IOException:  
  com.amazon.ws.emr.hadoop.fs.shaded.com.amazonaws.services.s3.model.AmazonS3Exception:  
    Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied;  
    Request ID: ...)
```

如需詳細資訊，請參閱 [整合 AWS Lake Formation 與 Amazon EMR 的限制](#)。

撰寫啟動和管理叢集的應用程式

主題

- [端對端 Amazon EMR Java 原始程式碼範例 \(p. 337\)](#)
- [API 呼叫的常見概念 \(p. 339\)](#)
- [使用軟體開發套件呼叫 Amazon EMR API \(p. 341\)](#)

您可以呼叫其中一項 AWS 開發套件的包裝函式，藉此存取 Amazon EMR API 提供的功能。AWS 軟體開發套件提供特定語言功能，可包裝 Web 服務的 API 並簡化到 Web 服務的連接，為您處理許多連線詳細資訊。如需使用其中一項軟體開發套件呼叫 Amazon EMR 的詳細資訊，請參閱[使用軟體開發套件呼叫 Amazon EMR API \(p. 341\)](#)。

Important

Amazon EMR 的最大請求速率是每 10 秒 1 個請求。

端對端 Amazon EMR Java 原始程式碼範例

開發人員能夠使用自訂 Java 程式碼來呼叫 Amazon EMR API，然後透過 Amazon EMR 主控台或 CLI 執行相同的操作。本節提供的端對端必要步驟會說明如何安裝 AWS Toolkit for Eclipse，並執行功能完整的 Java 來源碼範例；該範例可新增步驟至 Amazon EMR 叢集。

Note

此範例雖著重於 Java，但 Amazon EMR 也推出了一系列的 Amazon EMR 軟體開發套件來支援多種程式語言。如需更多詳細資訊，請參閱[使用軟體開發套件呼叫 Amazon EMR API \(p. 341\)](#)。

此 Java 原始程式碼範例示範如何使用 Amazon EMR API 執行以下任務：

- 擷取 AWS 登入資料，並將其發送給 Amazon EMR 以進行 API 呼叫
- 設定新的自訂步驟與新的預先定義步驟
- 在現有 Amazon EMR 叢集新增步驟
- 從執行中的叢集擷取叢集步驟 ID

Note

此範例將示範如何在現有叢集新增步驟，因此要求您在帳戶中擁有作用中的叢集。

在開始之前，請先安裝符合電腦平台的 Eclipse IDE for Java EE Developers (Eclipse IDE for Java EE Developers) 版本。如需詳細資訊，請前往[Eclipse 下載專區](#)。

接著，安裝適用於 Eclipse 的資料庫開發外掛程式。

安裝資料庫開發 Eclipse 外掛程式

1. 開啟 Eclipse IDE。
2. 選擇 Help (說明)，接著選擇 Install New Software (安裝新軟體)。
3. 在 Work with: (使用以下路徑：) 欄位中，輸入 <http://download.eclipse.org/releases/kepler> 或符合 Eclipse IDE 版本編號的路徑。
4. 在項目清單中，請選擇 Database Development (資料庫開發)，並按一下 Finish (完成)。

5. 在提示時重新啟動 Eclipse。

接著安裝 Toolkit for Eclipse，讓有用且預先設定的原始程式碼專案範本可以使用。

安裝 Toolkit for Eclipse

1. 開啟 Eclipse IDE。
2. 選擇 Help (說明)，接著選擇 Install New Software (安裝新軟體)。
3. 在 Work with: (使用以下路徑 :) 欄位中，輸入 <https://aws.amazon.com/eclipse>。
4. 在項目清單中，請選擇 AWS Toolkit for Eclipse (AWS Toolkit for Eclipse)，並按一下 Finish (完成)。
5. 在提示時重新啟動 Eclipse。

接著，建立新的 AWS Java 專案並執行範例 Java 原始程式碼。

建立新的 AWS Java 專案

1. 開啟 Eclipse IDE。
2. 依序選擇 File (檔案)、New (新增)，接著選擇 Other (其他)。
3. 在 Select a wizard (選取精靈) 對話方塊中，選擇 AWS Java Project (AWS Java 專案)，並按一下 Next (下一步)。
4. 在 New AWS Java Project (新增 AWS Java 專案) 對話方塊的 **Project name:** 欄位中，輸入新專案的名稱，例如 **EMR-sample-code**。
5. 選擇 Configure AWS accounts... (設定 AWS 帳戶...)，並輸入公開和私密存取金鑰，然後選擇 Finish (完成)。如需建立存取金鑰的詳細資訊，請參閱 Amazon Web Services 一般參考中的[如何取得安全登入資料？](#)

Note

請勿直接在程式碼內嵌存取金鑰。Amazon EMR 軟體開發套件可讓您將存取金鑰放入已知位置，如此一來，就不必將其留在程式碼中。

6. 在新的 Java 專案中按一下滑鼠右鍵並選取 src (src) 資料夾，然後選擇 New (新增)，再選擇 Class (類別)。
7. 在 Java Class (Java 類別) 對話方塊的 Name (名稱) 欄位中，輸入新類別的名稱，例如 **main**。
8. 在 Which method stubs would you like to create? (您希望建立哪些 Stub 方法?) 區段中，選擇 public static void main(String[] args) (public static void main(String[] args))，然後按一下 Finish (完成)。
9. 在新的類別中輸入 Java 來源碼，並為範例內的類別和方法新增適當的 import (匯入) 陳述式。為方便起見，完整的原始程式碼列表如下所示。

Note

請將以下範本程式碼中的範例叢集 ID (JobFlowId) (**j-xxxxxxxxxxxxxx**) 替換成帳戶中的有效叢集 ID，您可以在 AWS Management Console 中找到該 ID，亦可使用下列 AWS CLI 命令：

```
aws emr list-clusters --active | grep "Id"
```

除此之外，您還需要將範例 Amazon S3 路徑 (**s3://path/to/my/jarfolder**) 替換成 JAR 的有效路徑。最後，將範例類別名稱 (**com.my.Main1**)，更換為您 JAR 中正確的類別名稱 (如果適用)。

```
import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.AWS Credentials;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.elasticmapreduce.AmazonElasticMapReduce;
```

```
import com.amazonaws.services.elasticmapreduce.AmazonElasticMapReduceClientBuilder;
import com.amazonaws.services.elasticmapreduce.model.*;
import com.amazonaws.services.elasticmapreduce.util.StepFactory;

public class Main {

    public static void main(String[] args) {
        AWSCredentials credentials_profile = null;
        try {
            credentials_profile = new ProfileCredentialsProvider("default").getCredentials();
        } catch (Exception e) {
            throw new AmazonClientException(
                "Cannot load credentials from .aws/credentials file. " +
                "Make sure that the credentials file exists and the profile name is
specified within it.",
                e);
        }

        AmazonElasticMapReduce emr = AmazonElasticMapReduceClientBuilder.standard()
            .withCredentials(new AWSStaticCredentialsProvider(credentials_profile))
            .withRegion(Regions.US_WEST_1)
            .build();

        // Run a bash script using a predefined step in the StepFactory helper class
        StepFactory stepFactory = new StepFactory();
        StepConfig runBashScript = new StepConfig()
            .withName("Run a bash script")
            .withHadoopJarStep(stepFactory.newScriptRunnerStep("s3://jeffgoll/emr-scripts/
create_users.sh"))
            .withActionOnFailure("CONTINUE");

        // Run a custom jar file as a step
        HadoopJarStepConfig hadoopConfig1 = new HadoopJarStepConfig()
            .withJar("s3://path/to/my/jarfolder") // replace with the location of the jar
        to run as a step
            .withMainClass("com.my.Main1") // optional main class, this can be omitted if
        jar above has a manifest
            .withArgs("--verbose"); // optional list of arguments to pass to the jar
        StepConfig myCustomJarStep = new StepConfig("RunHadoopJar", hadoopConfig1);

        AddJobFlowStepsResult result = emr.addJobFlowSteps(new AddJobFlowStepsRequest()
            .withJobFlowId("j-xxxxxxxxxxxxx") // replace with cluster id to run the steps
            .withSteps(runBashScript,myCustomJarStep));

        System.out.println(result.getStepIds());
    }
}
```

10. 選擇 Run (執行)，然後選擇 Run As (依此執行)，最後選取 Java Application (Java 應用程式)。
11. 如果該範例正確執行，一份新步驟的 ID 清單會顯示在 Eclipse IDE 主控台視窗。正確輸出類似如下：

```
[s-39BLQZRJB2E5E, s-1L6A4ZU2SAURC]
```

API 呼叫的常見概念

主題

- [Amazon EMR 的端點 \(p. 340\)](#)
- [在 Amazon EMR 指定叢集參數 \(p. 340\)](#)
- [Amazon EMR 中的可用區域 \(p. 340\)](#)

- 如何在 Amazon EMR 叢集使用其他檔案和程式庫 (p. 340)

當您撰寫呼叫 Amazon EMR API 的應用程式，在呼叫軟體開發套件的一個包裝函式時，有幾個適用的概念。

Amazon EMR 的端點

端點是指 web 服務進入點的 URL。每個 Web 服務請求都必須包含一個端點。該端點指定了建立、描述或終止叢集的 AWS 區域。它的格式為 elasticmapreduce.*regionname*.amazonaws.com。如果您指定一般端點 (elasticmapreduce.amazonaws.com)，Amazon EMR 會將您的請求導向預設區域中的端點。若是 2013 年 3 月 8 日或之後建立的帳戶，預設區域為 us-west-2，若是較舊的帳戶，預設區域則為 us-east-1。

如需 Amazon EMR 端點的詳細資訊，請參閱 Amazon Web Services General Reference 中的 [區域與端點](#)。

在 Amazon EMR 指定叢集參數

該 Instances 參數可讓您設定 EC2 執行個體類型和數量以建立節點來處理資料。Hadoop 將資料處理分散至多個叢集節點。主節點負責持續追蹤核心與任務節點的運作狀態，並輪詢節點的任務結果狀態。核心和任務節點執行實際的資料處理。如果您有一個單一節點的叢集，該節點將同時做為主節點和核心節點。

KeepJobAlive 請求中的 RunJobFlow 參數會在叢集要執行的步驟用完時判斷是否終止叢集。當您得知叢集如預期執行時，設此值為 False。當該叢集暫停，而您正在進行任務流程故障診斷並新增步驟時，請將該值設為 True。這可減少將結果上傳至 Amazon Simple Storage Service (Amazon S3) 所需的時間和費用；您只要重複修改步驟後的程序，即可重新啟動叢集。

如果 KeepJobAlive 為 true，在叢集成功完成其工作後，您必須傳送 TerminateJobFlows 請求，否則該叢集將持續執行並產生 AWS 費用。

如需 RunJobFlow 唯一參數的詳細資訊，請參閱 [RunJobFlow](#)。如需一般請求參數的詳細資訊，請參閱 [常見的請求參數](#)。

Amazon EMR 中的可用區域

Amazon EMR 使用 EC2 執行個體做為節點來處理叢集。這些 EC2 執行個體地點是由可用區域及區域所組成。區域分散在個別的地理區域之中。可用區域為一個區域內的不同位置，可以隔離其他可用區域的故障。每一個可用區域都提供同一區域中其他可用區域的價廉、低延遲網路連線能力。如需 Amazon EMR 區域和端點的清單，請參閱 Amazon Web Services General Reference 中的 [區域與端點](#)。

AvailabilityZone 參數指定了叢集的一般位置。此為選擇性的參數，一般情況下我們並不鼓勵使用它。若未指定 AvailabilityZone，Amazon EMR 會自動挑選該叢集的最佳 AvailabilityZone 值。如果您想要您的執行個體與其他現有執行中的執行個體共存，並且叢集需要從這些執行個體讀取或寫入資料，您可能會發現此參數很有幫助。如需詳細資訊，請參閱 [Amazon EC2 User Guide for Linux Instances](#)。

如何在 Amazon EMR 叢集使用其他檔案和程式庫

有時您可能想在映射器或縮減器應用程式中使用其他檔案或自訂程式庫。例如，您可能想使用將 PDF 檔案轉換為純文字的程式庫。

在使用 Hadoop 串流時快取檔案以供映射器或縮減器使用

- 在 JAR args 欄位，新增下列引數：

```
-cacheFile s3://bucket/path_to_executable#local_path
```

檔案 (local_path) 在映射器的工作目錄中，可以參考該檔案。

使用軟體開發套件呼叫 Amazon EMR API

主題

- [使用適用於 Java 的 AWS 開發套件來建立 Amazon EMR 叢集 \(p. 341\)](#)

AWS 軟體開發套件提供包裝 API 的功能，並協助處理許多連線詳細資訊，例如計算簽章、處理請求重試和錯誤處理。軟體開發套件還包含範本程式碼、教學和其他資源，協助您開始編寫呼叫 AWS 的應用程式。在軟體開發套件中呼叫包裝器函式可以大幅簡化撰寫 AWS 應用程式的過程。

如需如何下載和使用 AWS 開發套件的詳細資訊，請參閱[適用於 Amazon Web Services 的工具](#)下方的軟體開發套件。

使用適用於 Java 的 AWS 開發套件來建立 Amazon EMR 叢集

適用於 Java 的 AWS 開發套件提供搭配 Amazon EMR 功能的三種套件：

- com.amazonaws.services.elasticmapreduce
- com.amazonaws.services.elasticmapreduce.model
- com.amazonaws.services.elasticmapreduce.util

如需這些套件的詳細資訊，請參閱[AWS SDK for Java API Reference](#)。

以下範例說明 SDK 如何利用 Amazon EMR 簡化程式設計。下方程式碼範例使用 StepFactory 物件 (用來建立一般 Amazon EMR 步驟類型的協助程式類別) 來建立已啟用偵錯功能的互動式 Hive 叢集。

```
import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.AWS Credentials;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.elasticmapreduce.AmazonElasticMapReduce;
import com.amazonaws.services.elasticmapreduce.AmazonElasticMapReduceClientBuilder;
import com.amazonaws.services.elasticmapreduce.model.*;
import com.amazonaws.services.elasticmapreduce.util.StepFactory;

public class Main {

    public static void main(String[] args) {
        AWS Credentials credentials_profile = null;
        try {
            credentials_profile = new ProfileCredentialsProvider("default").getCredentials(); // specifies any named profile in .aws/credentials as the credentials provider
        } catch (Exception e) {
            throw new AmazonClientException(
                "Cannot load credentials from .aws/credentials file. " +
                "Make sure that the credentials file exists and that the profile name is defined within it.",
                e);
        }

        // create an EMR client using the credentials and region specified in order to create the cluster
    }
}
```

```
AmazonElasticMapReduce emr = AmazonElasticMapReduceClientBuilder.standard()
    .withCredentials(new AWSStaticCredentialsProvider(credentials_profile))
    .withRegion(Regions.US_WEST_1)
    .build();

    // create a step to enable debugging in the AWS Management Console
StepFactory stepFactory = new StepFactory();
StepConfig enabledebugging = new StepConfig()
    .withName("Enable debugging")
    .withActionOnFailure("TERMINATE_JOB_FLOW")
    .withHadoopJarStep(stepFactory.newEnableDebuggingStep());

    // specify applications to be installed and configured when EMR creates the cluster
Application hive = new Application().withName("Hive");
Application spark = new Application().withName("Spark");
Application ganglia = new Application().withName("Ganglia");
Application zeppelin = new Application().withName("Zeppelin");

// create the cluster
RunJobFlowRequest request = new RunJobFlowRequest()
    .withName("MyClusterCreatedFromJava")
    .withReleaseLabel("emr-5.20.0") // specifies the EMR release version label, we
recommend the latest release
    .withSteps(enabledebugging)
    .withApplications(hive,spark,ganglia,zeppelin)
    .withLogUri("s3://path/to/my/emr/logs") // a URI in S3 for log files is required
when debugging is enabled
    .withServiceRole("EMR_DefaultRole") // replace the default with a custom IAM
service role if one is used
    .withJobFlowRole("EMR_EC2_DefaultRole") // replace the default with a custom EMR
role for the EC2 instance profile if one is used
    .withInstances(new JobFlowInstancesConfig()
        .withEc2SubnetId("subnet-12ab34c56")
        .withEc2KeyName("myEc2Key")
        .withInstanceCount(3)
        .withKeepJobFlowAliveWhenNoSteps(true)
        .withMasterInstanceType("m4.large")
        .withSlaveInstanceType("m4.large"));
}

RunJobFlowResult result = emr.runJobFlow(request);
System.out.println("The cluster ID is " + result.toString());
}
```

至少，您必須通過分別對應至 EMR_DefaultRole 和 EMR_EC2_DefaultRole 的服務角色和 jobflow 角色。您可以透過為相同帳戶叫用此 AWS CLI 命令來執行此動作。首先，檢視該角色是否已存在：

```
aws iam list-roles | grep EMR
```

若執行個體描述檔 (EMR_EC2_DefaultRole) 和服務角色 (EMR_DefaultRole) 皆存在，它們都將顯示於：

```
"RoleName": "EMR_DefaultRole",
"Arn": "arn:aws:iam::AccountID:role/EMR_DefaultRole"
"RoleName": "EMR_EC2_DefaultRole",
"Arn": "arn:aws:iam::AccountID:role/EMR_EC2_DefaultRole"
```

如果預設的角色不存在，您可以使用以下 AWS CLI 命令以建立它們：

```
aws emr create-default-roles
```

AWS Glossary

For the latest AWS terminology, see the [AWS Glossary](#) in the AWS General Reference.