



開發人員指南

AWS HealthLake



AWS HealthLake: 開發人員指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS HealthLake ?	1
的優勢 AWS HealthLake	1
HealthLake 使用案例	2
存取 HealthLake	2
HIPAA 資格和資料安全	3
定價	3
AWS HealthLake 運作方式	4
建立和監控資料存放區	4
FHIR REST API 操作	4
從資源擴充功能自動產生FHIR DocumentReference 資源	5
使用 SQL型查詢進行搜尋	5
使用 FHIRRESTAPI操作搜尋	6
資料匯入的動作	6
資料匯出的動作	6
支援的設定檔驗證	7
驗證資源中指定的FHIR設定檔	8
預先載入的資料類型	10
設定許可	11
註冊 AWS 帳戶	11
建立具有管理存取權的使用者	12
設定IAM使用者或角色以使用 HealthLake (IAM 管理員)	13
在 Lake Formation 中將使用者或角色新增為 Data Lake 管理員 (IAM 管理員)	14
建立資料存放區	17
建立資料存放區 (AWS Management Console)	18
建立資料存放區 (AWS CLI 和 AWS SDKs)	18
匯入檔案	21
設定匯入任務的許可	22
在 中啟動匯入任務 HealthLake	24
使用 API操作匯入檔案	24
啟動匯入任務 (主控台)	24
資訊清單JSON檔案	25
範例：使用 啟動和監控匯入任務 AWS CLI	26
匯出檔案	29
設定匯出任務的許可	30

使用 HealthLake 主控台或 匯出資料 AWS SDKs	32
從資料存放區匯出檔案 (主控台)	33
從資料存放區匯出檔案 (AWS SDKs)	33
使用 FHIRRESTAPI操作匯出資料	34
開始之前	35
授權export請求	35
提出export請求	36
管理您的匯出請求	39
刪除資料存放區	43
刪除資料存放區 (主控台)	43
刪除資料存放區 (AWS SDKs 和 AWS CLI)	43
FHIR REST API 參考	46
支援的資源類型	47
CRUD 操作	49
POST 請求	50
GET 請求	51
PUT 請求	52
DELETE 請求	55
套件請求	55
搜尋資料存放區	63
支援的搜尋參數類型	64
支援的進階搜尋參數 HealthLake	68
支援的搜尋修改器	73
支援的搜尋比較器	73
不支援的搜尋參數 HealthLake	74
使用POST範例搜尋	74
使用GET範例搜尋	84
讀取資源歷史記錄	102
讀取版本特定的FHIR資源歷史記錄	103
病患 \$所有FHIRAPI操作	104
取得與病患相關的所有資源	104
病患 \$所有參數	104
病患 \$所有項目start和 end 屬性	106
匯出FHIRAPI操作	111
使用 查詢 SQL	112
連接您的資料存放區	113

授與 存取權	113
Athena 入門	115
使用 查詢 HealthLake 您的資料存放區 SQL	116
SQL 具有複雜篩選的查詢	122
VPC 端點 (AWS PrivateLink)	129
端點的 HealthLake VPC考量事項	129
為 建立介面VPC端點 HealthLake ;	129
為 建立VPC端點政策 HealthLake	129
在 中標記資源 AWS HealthLake	131
重要通知	132
最佳實務	132
標記需求	132
將標籤新增至資料存放區	133
列出資料存放區的標籤	133
從資料存放區移除標籤	134
監控 HealthLake	135
使用 監控 CloudWatch	135
檢視 HealthLake 指標	137
建立警示	138
FHIR 的 SMART	139
身分驗證要求	140
必要的授權伺服器元素	141
必要的宣告	141
支援的範圍	142
獨立啟動範圍	142
HealthLake 資料存放區FHIR資源特定範圍	142
執行權杖驗證	143
AWS Lambda 函數	144
建立服務角色	149
Lambda 執行角色	152
觸發您的 Lambda 函數	153
為您的 Lambda 函數佈建並行	153
在FHIR啟用的資料存放SMART區上建立	154
建立資料存放區	154
啟用精細授權	155
擷取探索文件	156

FHIR REST 請求範例	157
設定在FHIR合規資料存放SMART區實作 所需的資源	157
用戶端應用程式如何在FHIR啟用資料存放區SMART上啟動和請求 HealthLake 上的資料	159
整合自然語言處理	160
Amazon Comprehend Medical 與 整合 HealthLake	161
與 FHIRRESTAPI操作整合	162
Amazon Comprehend Medical API操作如何整合到 中的範例 HealthLake	162
搜尋參數	178
安全	181
資料保護	181
靜態加密	182
AWS 擁有的KMS金鑰	182
客戶受管KMS金鑰	183
建立客戶受管金鑰	183
使用客戶受管KMS金鑰的必要IAM許可	184
傳輸中加密	191
身分與存取管理	191
目標對象	191
使用身分驗證	192
使用政策管理存取權	194
AWS HealthLake 如何使用 IAM	196
身分型政策範例	202
AWS 受管政策	205
故障診斷	208
使用 AWS CloudTrail記錄 AWS HealthLake API 呼叫	210
AWS HealthLake CloudTrail 中的資訊	210
了解 AWS HealthLake 日誌檔案項目	212
合規驗證	213
恢復能力	214
基礎設施安全	214
安全最佳實務	215
配額	216
服務端點	216
的服務配額 HealthLake	216
故障診斷	222
為什麼我無法建立 HealthLake 資料存放區？	222

超過每個帳戶允許的資料存放區數量	223
如何建立 FHIR RESTful 的授權APIs ?	223
我的資料不是 FHIR R4 格式 - 我是否仍然可以使用 HealthLake ?	224
為什麼在將 FHIR RESTful APIs 用於以客戶受管KMS金鑰加密的資料存放區時，我會收到 AccessDenied 錯誤 ?	224
為什麼匯入失敗 ?	224
如何尋找 DocumentReference無法處理的資源 ?	228
遷移現有資料存放區以使用 Amazon Athena	228
將 Athena 中的搜尋結果連接到其他 AWS 服務	229
Athena 主控台在將資料匯入新資料存放區後無法運作	229
為什麼我會收到 Lake Formation 許可錯誤：lakeformation：新增資料湖管理員 PutDataLakeSettings 時 ?	229
如何開啟 HealthLake整合的自然語言處理功能 ?	229
我的資料存放區狀態不會從建立中變更	230
我的SDK資料存放區建立狀態會傳回例外狀況或未知狀態	230
使用 10MB 文件FHIRPOSTAPI進行操作，HealthLake 以取得 413Request 實體過大錯誤。	230
文件歷史記錄	231
AWS 詞彙表	233
.....	CCXXXiv

什麼是 AWS HealthLake ?

AWS HealthLake 是使用 Healthcare Interoperability FHIR(R4) 規格進行臨床資料擷取、儲存和分析的 HIPAA 合格服務。

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節[如何開啟 HealthLake 整合的自然語言處理功能？](#)中的。

運作狀態資料經常不完整和不一致。它通常非結構化，其中包含臨床備註、實驗室報告、保險索賠、醫療影像、記錄對話和時間序列資料（例如，心臟 ECG 或大腦 EEG 追蹤）中的資訊。

醫療保健供應商可以使用 HealthLake 來存放、轉換、查詢和分析 AWS 雲端中的資料。使用 HealthLake 整合的醫學自然語言處理 (NLP) 功能，您可以從各種來源分析非結構化臨床文字。會使用自然語言處理模型 HealthLake 轉換非結構化資料，並提供強大的查詢和搜尋功能。您可以使用 HealthLake，以安全、合規且可稽核的方式組織、編製索引和建構患者資訊。

HealthLake 也與 Amazon Athena 和 AWS Lake Formation 整合。您可以使用此整合來使用查詢資料存放區 SQL。

的優勢 AWS HealthLake

使用 AWS HealthLake，您可以：

- 快速且輕鬆地擷取運作狀態資料 – 您可以將內部部署 Fast Healthcare 互通性資源 (FHIR) 檔案大量匯入 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括臨床備註、實驗室報告、保險索賠等。然後，您可以在下游應用程式或工作流程中使用資料。
- 使用 FHIR REST API 操作 – HealthLake 支援使用 FHIR REST API 操作在資料存放區上執行 CRUD (Create/Read/Update/Delete) 操作。也支援 FHIR 搜尋。
- 以安全且符合 HIPAA 資格的方式將您的資料存放在 AWS 雲端，您可以稽核 – 您可以將資料儲存為 FHIR 格式，以便輕鬆查詢。HealthLake 會建立每位病患醫療歷史記錄的完整時間檢視，並以 R4 FHIR 標準格式建構。

- **Athena 整合** – 與 Athena HealthLake 的整合意味著您可以建立功能強大的 SQL 型查詢，可用來建立和儲存複雜的篩選條件。然後，您可以在 SageMaker AI 等下游應用程式中使用此資料來訓練機器學習模型或 Amazon QuickSight 來建立儀表板和資料視覺化。
- **使用專業機器學習 (ML) 模型轉換非結構化資料** – 使用 Amazon Comprehend Medical HealthLake 提供整合醫療自然語言處理 (NLP)。原始醫療文字資料會使用專門的 ML 模型進行轉換。這些模型已經過訓練，可了解從非結構化醫療保健資料中擷取有意義的資訊。使用整合式醫療 NLP，您可以自動從醫療文字擷取實體（例如醫療程序和藥物）、實體關係（例如藥物及其用量）和實體特徵（例如陽性或陰性測試結果或程序時間）資料。HealthLake 然後，會根據特徵符號、症狀和條件建立新的資源。這些會新增為新的條件、觀察 MedicationStatement 和資源類型。

HealthLake 使用案例

您可以使用 HealthLake 處理下列醫療保健應用程式：

- **人口運作狀態管理** – HealthLake 協助醫療保健組織分析人口運作狀態趨勢、結果和成本。這有助於組織識別最適合患者人口的介入，並選擇更好的照護管理選項。
- **改善照護品質** – HealthLake 協助醫院、健康保險公司和生命科學組織消除照護差距、改善照護品質，以及透過編譯患者醫療史的完整檢視來降低成本。
- **最佳化醫院效率** – HealthLake 提供醫院金鑰分析和機器學習工具，以提高效率並減少醫院浪費。

存取 HealthLake

您可以透過 AWS Management Console、AWS Command Line Interface (AWS CLI) HealthLake 或存取 AWS SDKs。

1. **AWS Management Console** – 提供可用來存取的 Web 介面 HealthLake。
2. **AWS Command Line Interface (AWS CLI)** – 為廣泛的 AWS 服務提供命令，包括 Windows HealthLake、macOS 和 Linux 支援和。如需安裝的詳細資訊 AWS CLI，請參閱 [AWS Command Line Interface](#)。
3. **AWS SDKs** – AWS 提供 SDKs（軟體開發套件），其中包含適用於各種程式設計語言和平台（Java、Python、Ruby、.NET、iOS、Android 等）的程式庫和範例程式碼。SDKs 提供便捷的方式，以建立 HealthLake 和 的程式設計存取 AWS。如需詳細資訊，請參閱適用於 [AWS Python SDK](#) 的。

HIPAA 資格和資料安全

這是HIPAA符合資格的服務。如需 1996 年美國健康保險可攜性和責任法案 (HIPAA) 的詳細資訊 AWS，以及使用 AWS 服務來處理、存放和傳輸受保護的健康資訊 (PHI)，請參閱[HIPAA概觀](#)。

HealthLake 包含可識別個人身分資訊 (PII) 的連線必須加密。根據預設，所有透過 HTTPS HealthLake 使用的連線TLS都會 HealthLake 儲存加密的客戶內容，並依AWS共同責任原則操作。

定價

如需有關 HealthLake 定價的資訊，請參閱 [AWS HealthLake 定價頁面](#)。為了更好地估計與 相關的潛在成本 HealthLake，您可以使用[HealthLake 定價計算器](#)。

AWS HealthLake 運作方式

AWS HealthLake 會建立資料存放區，以使用 Healthcare Interoperability FHIR(R4) 規格來存放運作狀態記錄。使用 HealthLake，您可以執行下列任務。

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節[如何開啟 HealthLake 整合的自然語言處理功能？](#)中的。

- 建立、監控和刪除資料存放區。
- 使用 `StartFHIRImportJob` 將大量醫療資料從 Amazon Simple Storage Service (Amazon S3) 儲存貯體匯入資料存放區。
- 使用建立、讀取、更新和刪除 (CRUD) 操作來管理存放在資料存放區中的資料。
- 在 Amazon Athena SQL 中使用 `來查詢資料存放區`。
- 在 FHIRRESTAPI 操作中使用 HTTP 用戶端來搜尋資料存放區。
- 啟用 Amazon Comprehend Medical API 操作，使用自然語言處理 () 搜尋資料中的醫療洞見 NLP。

建立和監控資料存放區

透過 HealthLake，您可以建立和監控可存放 Fast Healthcare 互通性資源 (FHIR) 資料的資料存放區。

若要建立新的資料存放區，您可以使用 [CreateFHIRDatastore](#) 或 HealthLake 主控台。若要查看資料存放區的狀態，請使用 [DescribeFHIRDatastore](#)。若要查看多個作用中資料存放區的狀態，請使用 [ListFHIRDatastores](#)。若要刪除資料存放區，請使用 [DeleteFHIRDatastore](#)。

FHIR REST API 操作

您可以使用 FHIRRESTAPI 操作在 HealthLake 資料存放區上執行建立、讀取、更新、刪除 (CRUD) 操作。若要進一步了解如何 HealthLake 支援 FHIRRESTAPI 操作，請參閱 [使用與 HealthLake 資料存放區 FHIRRESTAPI 的互動](#)。

從資源擴充功能自動產生FHIR DocumentReference 資源

Note

當您建立 HealthLake 資料存放區並新增包含的資料時DocumentReference，您的帳戶將會產生費用 AWS。如需詳細資訊，請參閱[AWS HealthLake 定價](#)。

HealthLake NLP 在 DocumentReference 資源類型中找到的文件上提供。若要分析文字，HealthLake 會使用下列 Amazon Comprehend Medical API操作。

- DetectEntitiesV2：檢查臨床文字是否有各種醫療實體，並傳回其特定資訊，例如實體類別、位置和可信度分數。
- InferICD10CM：檢查臨床文字，以將醫療情況偵測為患者記錄中列出的實體，並將這些實體連結至疾病控制中心 ICD-10-CM 知識庫中的標準化概念識別碼。
- InferRxNorm：檢查臨床文字，將藥物偵測為患者記錄中列出的實體，並從國家醫學圖書館連結至 RxNorm 資料庫中的標準化概念識別符。

HealthLake 當資源類型新增至資料存放區時，會自動分析該DocumentReference資源類型中發現的資料。原始DocumentReference資源檔案保持不變。擷取的醫療資訊會自動附加為 FHIR合規的延伸。若要進一步了解 如何在 NLP運作 HealthLake，請參閱 [根據中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。

使用 SQL型查詢進行搜尋

Note

對於 2022 年 11 月 14 日之前建立的資料存放區，您的搜尋僅限於 FHIRRESTAPI操作。若要使用 SQL型查詢來查詢 HealthLake 資料存放區中的資料，請參閱 [在 Amazon Athena SQL中使用查詢 AWS HealthLake 資料存放區](#)。

Amazon Athena 是以無伺服器 SQL為基礎的查詢服務。HealthLake 資料存放區會以 [Apache Iceberg](#) 資料表的形式擷取至 Athena。這些資料表旨在支援大型分析資料集。在 Athena 中，每個FHIR資源類型都以資料表表示。使用 Athena，您只能對資料存放區提出READ請求。若要進一步了解SQL以 為基礎的搜尋，請參閱 [使用查詢 HealthLake 您的資料存放區 SQL](#)。

使用 FHIRRESTAPI 操作搜尋

您可以透過使用支援的搜尋參數指定資源類型，或使用伺服器中找到的資源 ID 來搜尋存放在資料存放區中的運作狀態記錄，而無需指定資源類型。若要進一步了解如何使用 FHIRRESTAPI 操作進行搜尋，請參閱 [使用與 HealthLake 資料存放區 FHIRRESTAPI 的互動](#)。

資料匯入的動作

AWS HealthLake 使用 從 Amazon S3 儲存貯體大量匯入您的檔案。使用主控台或 [StartFHIRImport 任務](#) 來開始匯入任務。匯入檔案之後，您可以使用 [DescribeFHIRImport 任務](#) 來監控任務的狀態。匯入任務完成後，即可將資料新增至 Athena、轉換或分析，並在下游應用程式中使用。

資料匯出的動作

使用 HealthLake 將大量檔案匯出至 Amazon S3 儲存貯體。使用 主控台或 [StartFHIRExport 任務](#) 來開始匯出任務。匯出檔案之後，您可以使用 [DescribeFHIRExport 任務](#) 來監控任務的狀態，並檢視其屬性。匯出任務完成後，您可以使用 Amazon 視覺化資料，QuickSight 或使用其他服務存取資料 AWS。

AWS HealthLake 支援的FHIR設定檔驗證

HealthLake 支援基本 [FHIR R4 規格](#)。R4 規格中包含的是FHIR設定檔。設定檔用於FHIR資源類型，以使用基本資源類型的限制條件和/或延伸來定義更具體的資源類型定義。例如，FHIR設定檔可以識別必要欄位，例如延伸模組和值集。資源可以支援多個設定檔。HealthLake 所有資料存放區都支援使用FHIR設定檔。

將資料新增至 HealthLake 資料存放區時，不需要新增FHIR設定檔。如果在新增或更新資源時未指定FHIR設定檔，則資源只會根據基本 FHIR R4 結構描述進行驗證。

FHIR 資源符合的設定檔會包含在資源中，再擷取至其中 HealthLake。當將指定的FHIR設定檔新增至 HealthLake 您的資料存放區時，會 HealthLake 驗證該設定檔。

FHIR 設定檔在實作指南中指定。會 HealthLake 驗證下列實作指南中定義的FHIR設定檔。

支援的FHIR設定檔 HealthLake

名稱	版本	實作指南	功能
美國核心	3.1.1	http://hl7.org/fhir/us/core/STU3.1.1/	預設
美國核心	4.0.0	https://hl7.org/fhir/us/core/STU4/index.html	支援
CARIN 藍色按鈕	1.1.0	http://hl7.org/fhir/us/car-in-bb/STU1.1/	預設
CARIN 藍色按鈕	1.0.0	https://hl7.org/fhir/us/car-in-bb/STU1/	支援
Da Vinci Payer 資料交換	1.0.0	https://hl7.org/fhir/us/davinci-pdex/	預設
Da Vinci 運作狀態記錄交換 (HREx)	0.2.0	https://hl7.org/fhir/us/davinci-hrex/2020Sep/	預設
Da Vinci PDEX 計畫淨額	1.1.0	https://hl7.org/fhir/us/davinci-pdex-plan-net/STU1.1/	預設

名稱	版本	實作指南	功能
DaVinci PDEX 計畫淨額	1.0.0	https://hl7.org/fhir/us/davinci-pdex-plan-net/STU1/	支援
DaVinci Payer Data Exchange (PDex) 美國藥物配方	1.1.0	https://hl7.org/fhir/us/davinci-drug-formulary/STU1.1/	預設
DaVinci Payer Data Exchange (PDex) 美國藥物配方	1.0.1	https://hl7.org/fhir/us/davinci-drug-formulary/STU1.0.1/	支援
國家衛生局的 Ayushman Bharat 數位任務 (ABDM)	2.0	https://www.nrce.in/ndhm/fhir/r4/index.html	預設

驗證資源中指定的FHIR設定檔

若要驗證FHIR設定檔，請使用實作指南中URL指定的設定檔，將其新增至個別資源的 `profile` 元素。

FHIR 當您將新資源新增至資料存放區時，設定檔會經過驗證。若要新增資源，您可以使用 `StartFHIRImport` 任務API操作、提出新增資源的POST請求，或進行 `PUT` 更新現有資源。

Example – 查看在資源中參考的FHIR描述檔

設定檔URL會新增至 `"meta" : "profile"` 索引鍵/值對中的 `profile` 元素。為了清楚起見，已截斷此資源。

```
{
  "resourceType": "Patient",
  "id": "abcd1234efgh5678hijk9012",
  "meta": {
    "lastUpdated": "2023-05-30T00:48:07.8443764-07:00",
    "profile": [
      "http://hl7.org/fhir/us/core/StructureDefinition/us-core-patient"
    ]
  }
}
```

```
}
```

Example – 如何參考非預設支援的FHIR設定檔

驗證受支援的非預設設定檔（例如 CarinBB 1.0.0）– 在 `meta.profile` 元素URL中新增版本 URL（以 '|' 分隔）和基本設定檔的設定檔。為了清楚起見，已截斷此範例資源。

```
{
  "resourceType": "ExplanationOfBenefit",
  "id": "sample-EOB",
  "meta": {
    "lastUpdated": "2024-02-02T05:56:09.4+00:00",
    "profile": [
      "http://hl7.org/fhir/us/carin-bb/StructureDefinition/C4BB-ExplanationOfBenefit-Pharmacy|1.0.0",
      "http://hl7.org/fhir/us/carin-bb/StructureDefinition/C4BB-ExplanationOfBenefit-Pharmacy"
    ]
  }
}
```

預先載入的資料類型

HealthLake 僅支援SYNTHEA預先載入的資料類型。[Synthea](#) 是一種合成病患產生器，可建立模型產生病患的醫療史模型。它是一種開放原始碼 Git 儲存庫，允許 HealthLake 產生 FHIR R4-compliant資源套件，讓使用者可以在不使用實際病患資料的情況下測試模型。

下列資源類型可在預先載入的資料存放區中使用。

支援的 Synthea 資源類型

AllergyIntolerance	位置
CarePlan	MedicationAdministration
CareTeam	MedicationRequest
取得	觀察
條件	組織
裝置	病患
DiagnosticReport	從業人員
遇到	PractitionerRole
ExplanationofBenefit	程序
ImagingStudy	證明
預防接種	

設定開始使用 的許可 AWS HealthLake

在本章中，您可以使用 AWS Management Console 來設定開始使用 AWS HealthLake 和建立資料存放區所需的許可。若要設定建立資料存放區的許可，您可以建立使用者IAM或角色，其為資料湖管理員。HealthLake 您可以在 AWS Lake Formation 中將此使用者設定為資料湖管理員。資料湖管理員授予 Lake Formation 使用 Amazon Athena 查詢資料存放區所需的資源存取權。

在 中建立資料存放區後 HealthLake，您可以設定將檔案匯入資料存放區或匯出檔案的許可。如需設定匯入檔案許可的詳細資訊，請參閱 [設定匯入任務的許可](#)。如需設定匯出檔案許可的詳細資訊，請參閱 [設定匯出任務的許可](#)。

主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)
- [設定IAM使用者或角色以使用 HealthLake \(IAM 管理員 \)](#)
- [在 Lake Formation 中將使用者或角色新增為 Data Lake 管理員 \(IAM 管理員 \)](#)

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟以建立。

註冊 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時前往 <https://aws.amazon.com/> 並選擇我的帳戶，檢視目前的帳戶活動並管理您的帳戶。

建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者 [AWS Management Console](#) 身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的 [以根使用者身分登入](#)。

2. 為您的根使用者開啟多重驗證 (MFA)。

如需說明，請參閱 IAM 《使用者指南》中的 [為您的 AWS 帳戶 根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM 身分中心。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的 [啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的 [使用預設值設定使用者存取權 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用 IAM Identity Center 使用者登入，請使用您建立 IAM Identity Center 使用者時 URL 傳送到您電子郵件地址的登入。

如需使用 IAM Identity Center 使用者登入的說明，請參閱 AWS 登入 《使用者指南》中的 [登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限許可最佳實務的許可集。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [建立許可集](#)。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

設定IAM使用者或角色以使用 HealthLake (IAM 管理員)

角色：IAM管理員

可建立IAM使用者和角色，並可新增資料湖管理員的使用者。

本主題中的這些步驟必須由IAM管理員執行。

若要將 HealthLake 資料存放區連線至 Athena，您需要建立使用者IAM或角色，其為資料湖管理員和 HealthLake 管理員。此新使用者或角色會透過 AWS Lake Formation 授予資料存放區中資源的存取權，並已將AmazonHealthLakeFullAccess AWS 受管政策新增至其使用者或角色。

Important

做為資料湖管理員IAM的使用者或角色無法建立新的資料湖管理員。若要新增其他資料湖管理員，您必須使用已授予AdministratorAccess存取權IAM的使用者或角色。

建立管理員

1. 將 **AmazonHealthlakeFullAccess** IAM AWS 受管政策新增至組織中的使用者或角色。

如果您不熟悉建立IAM使用者，請參閱IAM《使用者指南》中的[建立IAM使用者](#)和[政策概觀 AWS IAM](#)。

2. 授予IAM使用者或角色對 AWS Lake Formation 的存取權。
 - 將下列IAM AWS 受管政策新增至組織中的使用者或角色：**AWSLakeFormationDataAdmin**

Note

AWSLakeFormationDataAdmin 政策會授予所有 AWS Lake Formation 資源的存取權。建議您一律使用完成任務所需的最低許可。如需詳細資訊，請參閱 IAM 使用者指南中的[IAM最佳實務](#)。

3. 將下列內嵌政策新增至使用者或角色。如需詳細資訊，請參閱IAM《使用者指南》中的[內嵌政策](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-logging-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShareInvitations",
        "ram:AcceptResourceShareInvitation",
        "glue:CreateDatabase",
        "glue>DeleteDatabase"
      ],
      "Resource": "*"
    }
  ]
}
```

如需AWSLakeFormationDataAdmin政策的詳細資訊，請參閱 [Lake Formation 開發人員指南中的 Lake Formation 角色和IAM許可參考](#)。AWS

在 Lake Formation 中將使用者或角色新增為 Data Lake 管理員 (IAM 管理員)

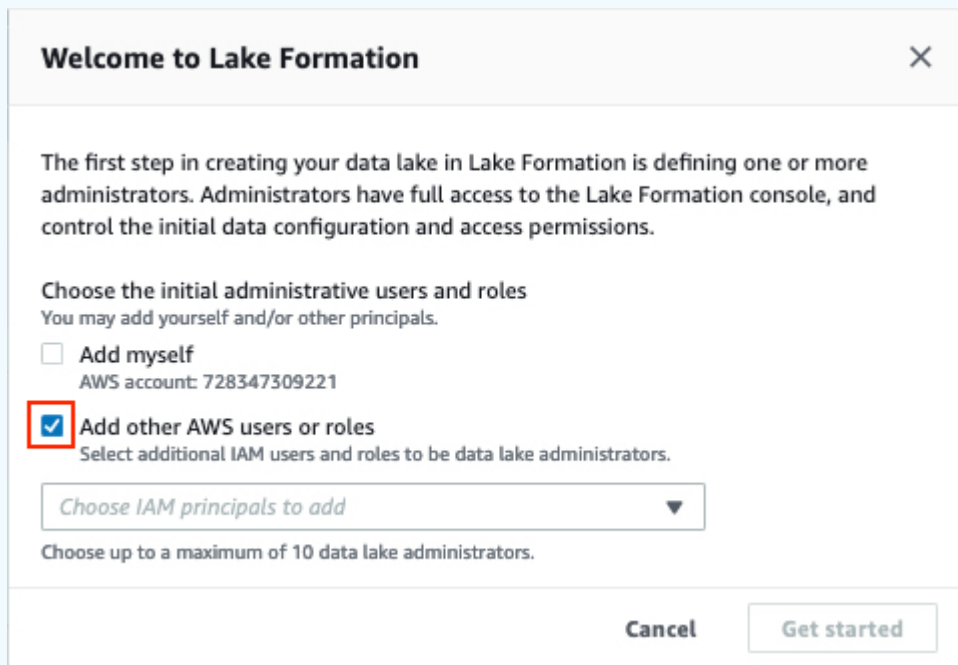
接著，IAM管理員需要新增步驟 1 中建立的使用者或角色，做為 Lake Formation 中的資料湖管理員。

將IAM使用者或角色新增為資料湖管理員

1. 開啟 AWS Lake Formation 主控台：<https://console.aws.amazon.com/lakeformation/>

Note

如果這是您第一次造訪 Lake Formation，會出現歡迎使用 Lake Formation 對話方塊，要求您定義 Lake Formation 管理員。



Welcome to Lake Formation

The first step in creating your data lake in Lake Formation is defining one or more administrators. Administrators have full access to the Lake Formation console, and control the initial data configuration and access permissions.

Choose the initial administrative users and roles
You may add yourself and/or other principals.

☐ Add myself
AWS account: 728347309221

☒ Add other AWS users or roles
Select additional IAM users and roles to be data lake administrators.

Choose IAM principals to add ▼

Choose up to a maximum of 10 data lake administrators.

Cancel Get started

2. 將新使用者或角色指派為 AWS Lake Formation 資料湖管理員。

- 選項 1：如果您收到歡迎使用 Lake Formation 對話方塊。
 1. 選擇新增其他 AWS 使用者或角色。
 2. 選擇向下箭頭 (▼)。
 3. 選擇您希望同時成為 Lake Formation HealthLake 管理員的管理員。
 4. 選擇開始使用。
- 選項 2：使用導覽窗格 (≡)。
 1. 選擇導覽窗格 (≡)。
 2. 在許可下，選擇管理角色和任務。
 3. 在資料湖管理員區段中，選取選擇管理員。
 4. 在管理資料湖管理員對話方塊中，選擇向下箭頭 (▼)。

5. 接下來，選取或搜尋您也想要成為 Lake Formation 管理員的 HealthLake 管理員使用者或角色。
 6. 選擇 Save (儲存)。
3. 變更要由 Lake Formation 管理的預設安全設定。HealthLake 資料存放區資源需要由 Lake Formation 管理，而非 IAM。若要更新，請參閱 AWS Lake Formation 開發人員指南中的[變更預設許可模型](#)。

在 中建立資料存放區 AWS HealthLake

完成後[設定開始使用的許可 AWS HealthLake](#)，您就可以建立資料存放區。在 中 AWS HealthLake，您使用資料存放區將資料存放為 HL7FHIR(R4) 格式。本章中的主題說明如何建立資料存放區。

若要同時建立已啟用分析的資料存放區，並在 Athena 中授予存取權，請將 AWSLakeFormationDataAdmin 受管政策新增至您的IAM使用者、群組或角色。此AWSLakeFormationDataAdmin政策可讓您建立資料湖管理員，並授予 Athena 中資料存放區的存取權。如需設定許可的資訊，請參閱 [設定開始使用的許可 AWS HealthLake](#)。

HealthLake 也與 整合 AWS CloudTrail。您可以使用 CloudTrail 來提供使用者、角色或服務 AWS in. CloudTrail captures 所採取動作的記錄 HealthLake，並將 的所有API呼叫和主控台動作 HealthLake 擷取為事件。如需進一步了解，請參閱 [使用 AWS CloudTrail記錄 AWS HealthLake API 呼叫](#)。

若要進一步了解 支援的 Fast Healthcare 互通性資源 (FHIR) 資源類型 HealthLake，請參閱 [中支援 FHIR的資源類型 AWS HealthLake](#)。

Amazon Athena 相容性

HealthLake 2022 年 11 月 14 日之前建立的日期存放區無法使用 Athena 執行SQL查詢。若要在預先存在的資料存放區上使用 Athena 搜尋功能，請先將資料遷移至新的資料存放區。若要進一步了解遷移預先存在的資料存放區，請參閱 [遷移現有資料存放區以使用 Amazon Athena](#)。

建立資料存放區之後，您可以使用 [API_DescribeFHIRDatastore](#)或 [API_ListFHIRDatastores.html](#) API 操作來取得其屬性，包括其狀態。或者，您可以在 HealthLake 主控台的資料存放區頁面上找到資料存放區狀態和其他詳細資訊。

HealthLake 資料存放區可以有列狀態：

- 建立 – 正在建立您的資料存放區。
- 作用中 – 您的資料存放區處於作用中狀態。您可以從中匯入和匯出資料。您也可以管理和搜尋存放在資料存放區中的FHIR資源。
- 刪除 – 正在刪除您的資料存放區。
- 已刪除 – 您的資料存放區已刪除。

主題

- [建立資料存放區 \(AWS Management Console\)](#)
- [建立資料存放區 \(AWS CLI 和 AWS SDKs\)](#)

建立資料存放區 (AWS Management Console)

HealthLake 主控台差異

HealthLake 主控台不支援在 FHIR 啟用的資料存放區 SMART 上建立。若要在 FHIR 啟用的資料存放區 SMART 上建立，您必須使用 AWS CLI 或其中一個 AWS 支援的 SDKs。如需進一步了解，請參閱 [SMART 將 FHIR 與整合 AWS HealthLake](#)。此外，當您檢視個別資料存放區的詳細資訊頁面 HealthLake 時，主控台不會區分支援的兩種類型的資料存放區。

建立 HealthLake 資料存放區

1. <https://console.aws.amazon.com//healthlake/> 在家中開啟 HealthLake 主控台。
2. 開啟導覽窗格 (≡)。
3. 然後選擇資料存放區。
4. 接著，選擇建立資料存放區。
5. 在資料存放區設定區段中，針對資料存放區名稱指定名稱。
6. (選用) 在資料存放區設定區段中，針對預先載入範例資料，選取核取方塊以預先載入 Synthea 資料。
 - Synthea 資料是預先載入的範例資料集。如需詳細資訊，請參閱 [預先載入的資料類型](#)。
7. 在資料存放區加密區段中，選擇使用 AWS 擁有的金鑰 (預設) 或選擇不同的 AWS KMS 金鑰 (進階)。
8. 在標籤 - 選用區段中，您可以將標籤新增至資料存放區。
 - 若要進一步了解如何標記資料存放區，請參閱 [將標籤新增至資料存放區](#)。
9. 接著，選擇建立資料存放區。資料存放區的狀態可在資料存放區頁面上取得。

建立資料存放區 (AWS CLI 和 AWS SDKs)

您可以使用下列程式碼範例來建立 HealthLake 資料存放區。

AWS CLI

下列範例示範搭配使用 `CreateFHIRDatastore` 操作 AWS CLI。若要執行範例，您必須安裝 AWS CLI。建立資料存放區時，靜態加密預設為 AWS 擁有的 KMS 金鑰，除非另有指定。若要進一步了解加密，HealthLake 請參閱 REST。 [在 REST 的 加密 AWS HealthLake](#)

此範例格式適用於 Unix、Linux 和 macOS。對於 Windows，將每一行結尾的反斜線 (\) Unix 接續字元替換為斜線 (^)。

```
aws healthlake create-fhir-datastore \  
  --datastore-type-version R4 \  
  --preload-data-config PreloadDataType="SYNTHETA" \  
  --datastore-name "your-data-store-name"
```

成功時，您會得到下列 JSON 回應。當您的資料存放區準備好擷取資料時，狀態會變更為 ACTIVE。若要進一步了解如何將資料匯入 HealthLake 資料存放區，請參閱[將檔案匯入 HealthLake 資料存放區](#)。

```
{  
  "DatastoreId": "eeb8005725ae22b35b4edbd68cf2dfd",  
  "DatastoreArn": "arn:aws:healthlake:us-west-2:111122223333:datastore/fhir/  
eeb8005725ae22b35b4edbd68cf2dfd",  
  "DatastoreStatus": "CREATING",  
  "DatastoreEndpoint": "https://healthlake.us-west-2.amazonaws.com/datastore/  
eeb8005725ae22b35b4edbd68cf2dfd/r4/"  
}
```

若要檢視所有資料存放區資料存放區的清單，您可以使用 [ListFHIRDataStore](#) 操作。您也可以可以在 HealthLake 主控台中查看作用中資料存放區的清單。

Python (boto3)

下列範例示範如何使用 `create_fhir_datastore` 操作建立 HealthLake 資料存放區。建立靜態資料存放區加密時，除非另有指定，否則預設為擁有 AWS 的 AWS KMS 金鑰。若要進一步了解加密，HealthLake 請參閱 REST [在 REST 的 加密 AWS HealthLake](#)。

```
import boto3  
import logging #built in logging library  
from botocore.exceptions import ClientError, ValidationError #specific exception  
ClientError from the boto3 library
```

```
def create_healthlake_datastore(DatastoreName=None):
    '''
    :param DatastoreName: the name of the data store, string
    :param:
    :return: True if the data store is created, else False
    '''

    # Create an Amazon Healthlake data store
    # Should we say something about region setting?
    # Should this example have some handling KMS keys

    try:
        if DatastoreName is None:
            healthlake_client = boto3.client('healthlake')
            healthlake_client.create_fhir_datastore(DatastoreTypeVersion='R4')

        else:
            healthlake_client = boto3.client('healthlake')
            healthlake_client.create_fhir_datastore(DatastoreTypeVersion='R4',
                                                    DatastoreName=DatastoreName)

    except (ClientError, ValidationError) as e:
        logging.error(e)
        return False

    return True

# Run the function above
create_healthlake_datastore(DatastoreName='test-datastore-delete-me-2')
```

資料存放區可以有四種狀態之一。`list_fhir_datastores` 使用檢視 HealthLake 資料存放區的清單，無論狀態為何。此範例示範如何根據資料存放區的狀態進行篩選。

```
import boto3

healthlake_client = boto3.client('healthlake')
data_store_list = healthlake_client.list_fhir_datastores(Filter={'DatastoreStatus':
    'ACTIVE'})
print(data_store_list)
```

若要進一步了解，請參閱 Boto3 文件[list_fhir_datastore](#)中的。

將檔案匯入 HealthLake 資料存放區

完成後在 [中建立資料存放區 AWS HealthLake](#)，您可以從 Amazon Simple Storage Service (Amazon S3) 儲存貯體將檔案匯入資料存放區。若要匯入檔案，您可以使用 HealthLake 主控台或 StartFHIRImportJobAPI 操作啟動匯入任務。

當您建立匯入任務時，您可以在 Amazon S3 中指定輸入資料的位置、輸出日誌檔的 Amazon S3 儲存貯體位置、授予儲存貯體 HealthLake 存取權IAM的角色，以及客戶擁有或 AWS 擁有的 AWS Key Management Service 金鑰。HealthLake 使用此金鑰來加密來源位置中的資料，並用來解密資料，HealthLake 以允許匯入。如需設定匯入任務許可的詳細資訊，請參閱 [設定匯入任務的許可](#)。若要進一步了解建立和使用 AWS KMS 金鑰，請參閱 [金鑰管理服務開發人員指南中的建立AWS金鑰](#)。

HealthLake 接受以新行分隔的 JSON(.ndjson) 格式的輸入檔案，其中每一行都包含有效的FHIR資源。您可以使用 API 操作 DescribeFHIRImportJob 和 ListFHIRImportJobs 來描述和列出正在進行的匯入任務。

對於每個匯入任務，HealthLake 會產生manifest.json檔案。此日誌說明匯入任務的成功和失敗。將檔案 HealthLake 輸出到您在建立匯入任務時指定的 Amazon S3 儲存貯體。如需詳細資訊，請參閱 [資訊清單JSON檔案](#)。

您可以對匯入或匯出任務進行佇列。這些非同步匯入或匯出任務會以 FIFO (先進先出) 方式處理。您可以在匯入或匯出任務進行時建立、讀取、更新或刪除FHIR資源。

使用預先載入的資料或匯入資料填入資料存放區之後，您就可以開始在 Amazon Athena SQL 中使用查詢資料存放區。如需詳細資訊，請參閱在 [Amazon Athena SQL中使用查詢 AWS HealthLake 資料存放區](#)。

主題

- [設定匯入任務的許可](#)
- [在中啟動匯入任務 HealthLake](#)
- [資訊清單JSON檔案](#)
- [範例：使用啟動和監控匯入任務 AWS CLI](#)

設定匯入任務的許可

將檔案匯入資料存放區之前，您必須授予 HealthLake 許可，才能存取 Amazon S3 中的輸入和輸出儲存貯體。若要授予 HealthLake 存取權，您可以為 建立IAM服務角色 HealthLake、將信任政策新增至角色以授予 HealthLake 擔任角色許可，並將許可政策連接至授予其存取 Amazon S3 儲存貯體的角色。

當您建立匯入任務時，您可以指定此角色的 Amazon Resource Name (ARN) `DataAccessRoleArn`。如需IAM角色和信任政策的詳細資訊，請參閱[IAM角色](#)。

設定許可之後，您就可以使用匯入任務將檔案匯入資料存放區。如需詳細資訊，請參閱[在中啟動匯入任務 HealthLake](#)。

設定匯入許可

1. 如果尚未建立輸出日誌檔案的目的地 Amazon S3 儲存貯體。Amazon S3 儲存貯體必須與 服務位於相同的 AWS 區域，且所有選項都必須開啟封鎖公開存取。若要進一步了解，請參閱[使用 Amazon S3 封鎖公有存取](#)。Amazon 擁有或客戶擁有的KMS金鑰也必須用於加密。若要進一步了解如何使用KMS金鑰，請參閱 [Amazon Key Management Service](#)。
2. 為 建立資料存取服務角色，HealthLake 並授予 HealthLake 服務許可，以使用下列信任政策來擔任該角色。HealthLake 會使用此角色來寫入輸出 Amazon S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": ["healthlake.amazonaws.com"]
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "your-account-id"
      },
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:healthlake:us-west-2:account:datastore/
fhir/data store ID"
      }
    }
  }]
}
```

3. 將許可政策新增至允許其存取 Amazon S3 儲存貯體的資料存取角色。amzn-s3-demo-bucket 以儲存貯體的名稱取代。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetEncryptionConfiguration"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-logging-bucket/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey*"
    ],
    "Resource": [
      "arn:aws:kms:us-east-1:012345678910:key/d330e7fc-b56c-4216-a250-f4c43ef46e83"
    ],
    "Effect": "Allow"
  }
]
```

在 中啟動匯入任務 HealthLake

建立資料存放區並設定匯入任務 ([設定匯入任務的許可](#)) 的許可後，您可以開始使用匯入任務來匯入檔案。您可以使用 AWS HealthLake 主控台或匯入 API、[start-fhir-import-job API](#)來啟動 AWS HealthLake 匯入任務。

主題

- [使用 API操作匯入檔案](#)
- [啟動匯入任務（主控台）](#)

使用 API操作匯入檔案

先決條件

使用 AWS HealthLake API操作時，您必須先建立 AWS Identity and Access Management (IAM) 政策，並將其連接至 IAM角色。若要進一步了解IAM角色和信任政策，請參閱[IAM政策和許可](#)。客戶也必須使用KMS金鑰進行加密。若要進一步了解如何使用KMS金鑰，請參閱 [Amazon Key Management Service](#)。

若要匯入檔案 (API)，請使用下列步驟。

1. 將資料上傳至 Amazon S3 儲存貯體。
2. 使用 [start-fhir-import-job API](#)API操作。當您啟動任務時，請指定包含輸入檔案的 Amazon S3 儲存貯體名稱、您要用於加密的KMS金鑰，以及輸出資料組態。
3. 若要進一步了解FHIR匯入任務，請使用 [describe-fhir-import-job](#)操作來取得任務的 ID、ARN、名稱、開始時間、結束時間和目前狀態。使用 [list-fhir-import-job](#)顯示所有匯入任務及其狀態。

啟動匯入任務（主控台）

若要使用 主控台匯入檔案，您可以將資料上傳至 Amazon S3 儲存貯體，

若要匯入檔案，請使用下列步驟。

1. 將資料上傳至 Amazon S3 儲存貯體。
2. <https://console.aws.amazon.com/healthlake/>在家中開啟 HealthLake 主控台。
3. 前往資料存放區的資料存放區詳細資訊頁面，然後選擇匯入。
4. 指定您的 Amazon S3 儲存貯體，並建立或識別您要使用IAM的角色和KMS金鑰。

5. 選擇匯入資料。

資訊清單JSON檔案

對於每個匯入任務，HealthLake 會產生 `manifest.json` file. HealthLake output 將檔案輸出到您在建立匯入任務時指定的 Amazon S3 儲存貯體。

`manifest.json` 檔案說明匯入任務的成功和失敗。日誌檔案會組織成兩個資料夾，名為 SUCCESS 和 FAILURE。輸出檔案可能包含敏感資訊，因此當您建立匯入任務時，您必須同時提供輸出 Amazon S3 儲存貯體和 AWS KMS 金鑰以進行加密。

以下是輸出 `manifest.json` 檔案的範例。我們建議您使用此檔案作為故障診斷失敗匯入任務的第一步。它提供每個檔案的詳細資訊，以及導致匯入任務失敗的原因。

```
{
  "inputDataConfig": {
    "s3Uri": "s3://amzn-s3-demo-source-bucket/healthlake-input/invalidInput/"
  },
  "outputDataConfig": {
    "s3Uri": "s3://amzn-s3-demo-logging-bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/",
    "encryptionKeyID": "arn:aws:kms:us-west-2:123456789012:key/fbbbfee3-20b3-42a5-a99d-c48c655ed545"
  },
  "successOutput": {
    "successOutputS3Uri": "s3://amzn-s3-demo-logging-bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/SUCCESS/"
  },
  "failureOutput": {
    "failureOutputS3Uri": "s3://amzn-s3-demo-logging-bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/FAILURE/"
  },
  "numberOfScannedFiles": 1,
  "numberOfFilesImported": 1,
  "sizeOfScannedFilesInMB": 0.023627,
  "sizeOfDataImportedSuccessfullyInMB": 0.011232,
  "numberOfResourcesScanned": 9,
  "numberOfResourcesImportedSuccessfully": 4,
  "numberOfResourcesWithCustomerError": 5,
```

```
"numberOfResourcesWithServerError": 0
}
```

範例：使用 啟動和監控匯入任務 AWS CLI

下列範例示範如何使用 AWS Command Line Interface 啟動和監控匯入任務。您也可以使用 [start-fhir-import-job API](#)。

```
aws healthlake start-fhir-import-job \
--input-data-config S3Uri=s3://amzn-s3-demo-source-bucket/inputFolder/ \
--datastore-id (Datastore ID) \
--data-access-role-arn "arn:aws:iam::012345678910:role/DataAccessRole" \
--job-output-data-config '{"S3Configuration": {"S3Uri":"s3://amzn-s3-demo-logging-bucket/healthlake-output", "KmsKeyId":"arn:aws:kms:us-east-1:012345678910:key/d330e7fc-b56c-4216-a250-f4c43ef46e83"}}' \
--region us-east-1
```

當匯入任務開始時，您將收到以下確認。

```
{
  "JobId": "8a4077553e9a485ad889c1a89c7541f0",
  "JobStatus": "SUBMITTED",
  "DatastoreId": "32839038a2f47f17c2fe0f53f0c3a0ba"
}
```

若要監控匯入任務的狀態，或了解其組態屬性，請使用 [describe-fhir-import-job](#) API 或 AWS CLI 命令，如下列範例所示。

```
aws healthlake describe-fhir-import-job \
--datastore-id (Datastore ID) \
--job-id c145fbb27b192af392f8ce6e7838e34f \
--region us-east-1
```

您會收到以下資訊以回應。

```
{
  "ImportJobProperties": {
    "InputDataConfig": {
      "S3Uri": "s3://amzn-s3-demo-source-bucket/(Prefix Name)/"
    },
    "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role Name)",
    "JobStatus": "COMPLETED",
    "JobId": "c145fbb27b192af392f8ce6e7838e34f",
    "SubmitTime": 1606272542.161,
    "EndTime": 1606272609.497,
    "DatastoreId": "(Datastore ID)"
  }
}
```

若要查看所有匯入任務的清單，請使用 [list-fhir-import-jobs](#) API 或 AWS CLI 命令，如下列範例所示。您可以新增一或多個篩選條件來限制結果。

```
aws healthlake list-fhir-import-jobs \
--datastore-id (Datastore ID) \
--submitted-before (DATE like 2024-10-13T19:00:00Z) \
--submitted-after (DATE like 2020-10-13T19:00:00Z ) \
--job-name "FHIR-IMPORT" \
--job-status SUBMITTED \
--max-results (Integer between 1 and 500)
```

您會收到以下資訊以回應。

```
{
  "ImportJobProperties": {
    "OutputDataConfig": {
      "S3Uri": "s3://(Bucket Name)/(Prefix Name)/",
      "S3Configuration": {
        "S3Uri": "s3://(Bucket Name)/(Prefix Name)/",
        "KmsKeyId" : "(KmsKey Id)"
      },
    },
    "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role Name)",
    "JobStatus": "COMPLETED",
    "JobId": "c145fbb27b192af392f8ce6e7838e34f",
    "JobName" "FHIR-IMPORT",
```

```
    "SubmitTime": 1606272542.161,  
    "EndTime": 1606272609.497,  
    "DatastoreId": "(Datastore ID)"  
  }  
}  
"NextToken": String
```

從 HealthLake 資料存放區匯出檔案

建立資料存放區並匯入資料（或者如果您使用預先載入的範例資料）之後，您可以將資料匯出至 Amazon S3 儲存貯體。若要從資料存放區匯出 HealthLake 資料，請使用下列操作。

- 使用 `StartFHIRExportJob` API 操作 AWS SDKs 提出匯出請求 HealthLake。
 - 此操作僅支援提出全系統的匯出請求。
- 使用 `export` 語法 HealthLake FHIR 提出匯出請求 REST API。
 - 此操作支援提出全系統、病患和群組匯出請求。您也可以套用參數，進一步篩選匯出請求中的資料。

Important

HealthLake SDK 使用 `StartFHIRExportJob` API 操作匯出請求，以及使用 `StartFHIRExportJobWithPost` API 操作 FHIR REST API 匯出請求會有不同的 IAM 動作。使用 SDK 匯出 `StartFHIRExportJob` 和使用 FHIR REST API 匯出的每個 IAM 動作 `StartFHIRExportJobWithPost`，都可以分別處理允許/拒絕許可。如果您想要同時限制 SDK 和 FHIR REST API 匯出，請務必拒絕每個 IAM 動作的許可。

這兩種操作都僅支援將檔案匯出至 Amazon S3 (S3) 儲存貯體。資料 HealthLake 存放區中的所有檔案都會匯出為以新行分隔的 JSON(.ndjson) 檔案，其中每一行都包含有效的 FHIR 資源。

這兩種操作都需要服務角色。其中，HealthLake 必須定義為服務主體，而且您必須定義您要匯出檔案的 Amazon Simple Storage Service (S3) 儲存貯體。如需進一步了解，請參閱 [設定匯出任務的許可](#)。

您可以對匯入或匯出任務進行佇列。這些非同步匯入或匯出任務會以 FIFO（先進先出）方式處理。您可以在匯入或匯出任務進行時建立、讀取、更新或刪除 FHIR 資源。

若要從 HealthLake 資料存放區匯出檔案，請參閱下列各節。

- [設定匯出任務的許可](#)
- [使用 HealthLake 主控台或從資料存放區匯出檔案 AWS SDKs](#)
- [使用 FHIR REST API 操作從 HealthLake 資料存放區匯出資料](#)

設定匯出任務的許可

從資料存放區匯出檔案之前，您必須授予 HealthLake 許可，才能存取 Amazon S3 中的輸出儲存貯體。若要授予 HealthLake 存取權，您可以為 建立IAM服務角色 HealthLake、將信任政策新增至角色以授予 HealthLake 擔任角色許可，以及將許可政策連接至授予其存取 Amazon S3 儲存貯體的角色。

如果您已在 HealthLake 中為 建立角色[設定匯入任務的許可](#)，則可以重複使用該角色，並授予此主題中列出的匯出 Amazon S3 儲存貯體額外許可。若要進一步了解IAM角色和信任政策，請參閱[IAM政策和許可](#)。

Important

HealthLake SDK 使用 StartFHIRExportJob API 操作匯出請求，以及使用 StartFHIRExportJobWithPostAPI操作FHIRRESTAPI匯出請求有不同的IAM動作。使用 SDK 匯出StartFHIRExportJob和使用 FHIR REST API 匯出的每個IAM動作StartFHIRExportJobWithPost，都可以分別處理允許/拒絕許可。如果您想要同時限制 SDK和 FHIR REST API 匯出，請務必拒絕每個IAM動作的許可。如果您提供使用者完整存取權 HealthLake，則不需要變更IAM使用者許可。

設定許可的使用者或角色必須具有許可，才能建立角色、建立政策，以及將政策連接至角色。下列IAM政策會授予這些許可。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": ["iam:CreateRole", "iam:CreatePolicy", "iam:AttachRolePolicy"],
    "Effect": "Allow",
    "Resource": "*"
  }, {
    "Action": "iam:PassRole"
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "healthlake.amazonaws.com"
      }
    }
  }
]}
```

設定匯出許可

1. 如果尚未，請為您要從資料存放區匯出的資料建立目的地 Amazon S3 儲存貯體。Amazon S3 儲存貯體必須與服務位於相同的AWS區域，且所有選項都必須開啟封鎖公開存取。若要進一步了解，請參閱[使用 Amazon S3 封鎖公有存取](#)。Amazon 擁有或客戶擁有的KMS金鑰也必須用於加密。若要進一步了解如何使用KMS金鑰，請參閱 [Amazon Key Management Service](#)。
2. 如果您尚未建立資料存取服務角色，請為 建立資料存取服務角色，HealthLake 並授予 HealthLake 服務許可，以使用下列信任政策來擔任該角色。HealthLake 會使用此角色來寫入輸出 Amazon S3 儲存貯體。如果您已在 中建立一個 [設定匯入任務的許可](#)，您可以在下一個步驟中重複使用它，並授予 Amazon S3 儲存貯體的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": ["healthlake.amazonaws.com"]
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "your-account-id"
      },
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:healthlake:us-west-2:account:datastore/
fhir/data store ID"
      }
    }
  }]
}
```

3. 將許可政策新增至資料存取角色，以允許其存取您的輸出 Amazon S3 儲存貯體。amzn-s3-demo-bucket 以儲存貯體的名稱取代。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetEncryptionConfiguration"
    ]
  }]
}
```

```

    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-logging-bucket/*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey*"
    ],
    "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/d330e7fc-b56c-4216-a250-f4c43ef46e83"
    ],
    "Effect": "Allow"
}]
}

```

使用 HealthLake 主控台或 從資料存放區匯出檔案 AWS SDKs

完成後[設定匯出任務的許可](#)，您可以將檔案從資料存放區匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。若要從資料存放區匯出檔案，請在其中啟動匯出任務 HealthLake。匯出任務會以新行分隔 JSON(.ndjson) 格式從您的資料存放區匯出檔案，其中每一行都包含有效的 FHIR 資源。啟動匯出任務時，您必須指定加密的 AWS KMS 金鑰。若要進一步了解如何建立 KMS 金鑰，請參閱 AWS Key Management Service 開發人員指南中的[建立金鑰](#)。

下列主題說明如何使用 AWS HealthLake 主控台啟動匯出任務，以及使用 [start-fhir-export-job API](#) 操作啟動 AWS SDKs。

主題

- [從資料存放區匯出檔案（主控台）](#)

- [從資料存放區匯出檔案 \(AWS SDKs\)](#)

從資料存放區匯出檔案（主控台）

若要匯出檔案（主控台），請使用下列步驟。

1. 在與 相同的區域中建立輸出 S3 儲存貯體 HealthLake。
2. 若要啟動新的匯出任務，請識別輸出 Amazon S3 儲存貯體，並建立或識別您要使用IAM的角色。若要進一步了解IAM角色和信任政策，請參閱[IAM角色](#)。也請使用KMS金鑰加密。若要進一步了解如何使用KMS金鑰，請參閱 [Amazon Key Management Service](#)。
3. 若要查看匯出任務的狀態，請使用 [ListFHIRExportJobs](#)API操作。

從資料存放區匯出檔案 (AWS SDKs)

若要使用 從資料存放區匯出檔案 AWS SDKs，請使用 [start-fhir-export-job](#)操作。下列程式碼說明如何使用SDK適用於 Python 的 (Boto3) 啟動匯出任務。

```
import boto3

client = boto3.client('healthlake')

response = client.start_fhir_export_job(
    JobName='job name',
    OutputDataConfig={
        'S3Configuration': {
            'S3Uri': 's3://amzn-s3-demo-bucket/output-folder',
            'KmsKeyId': 'arn:aws:kms:us-west-2:account-number:key/AWS KMS key ID'
        }
    },
    DatastoreId='data store ID',
    DataAccessRoleArn='role ARN',
)
print(response['JobStatus'])
```

若要取得FHIR匯出任務的 ID、ARN、名稱、開始時間、結束時間和目前狀態，請使用 [describe-fhir-export-job](#)。使用 [list-fhir-export-jobs](#) 列出所有匯出任務及其狀態。

下列程式碼說明如何使用 SDK for Python (Boto3) 取得特定匯出任務的屬性。

```
import boto3

client = boto3.client('healthlake')

describe_response = client.describe_fhir_export_job(
    DatastoreId=datastoreId,
    JobId=jobId
)
print(describe_response['ExportJobProperties'])
```

使用 FHIRRESTAPI 操作從 HealthLake 資料存放區匯出資料

完成 [後設定匯出任務的許可](#)，您可以使用 FHIRRESTAPI 操作從 HealthLake 資料存放區匯出資料。若要使用 FHIR REST 提出匯出請求 API，您必須擁有具有必要許可 IAM 的使用者、群組或角色、指定 \$export 做為 POST 請求的一部分，並在請求內文中包含請求參數。根據 FHIR 規格，FHIR 伺服器必須支援 GET 請求，且可以支援 POST 請求。為了支援其他參數，需要內文才能啟動匯出，因此 HealthLake 支援 POST 請求。

Important

HealthLake 在 2023 年 6 月 1 日之前建立的資料存放區僅支援全系統匯出的 FHIRRESTAPI 以基礎的匯出任務請求。

HealthLake 在 2023 年 6 月 1 日之前建立的資料存放區不支援使用資料存放區端點上的 GET 請求來取得匯出狀態。

您使用提出的所有匯出請求 FHIRRESTAPI 都會以 ndjson 格式傳回，並匯出至 Amazon S3 儲存貯體。每個 S3 物件只會包含單一 FHIR 資源類型。

您可以根據 AWS 帳戶配額將匯出請求排入佇列。若要進一步了解與相關聯的 Service Quotas HealthLake，請參閱 [AWS HealthLake 端點和配額](#)。

HealthLake 支援下列三種類型的匯出端點請求。

Type	描述	語法
系統匯出	從 HealthLake FHIR 伺服器匯出所有資料。	POST https://healthlake. your-region .amazonaws.com/datastore/ your-datastore-id /r4/\$export

Type	描述	語法
所有病患	匯出所有與病患相關的所有資料，包括與病患資源類型相關聯的資源類型。	POST https://healthlake. your-region .amazonaws.com/datastore/ your-datastore-id /r4/Patient/\$export
病患群組	匯出與群組 ID 所指定之病患群組相關的所有資料。	POST https://healthlake. your-region .amazonaws.com/datastore/ your-datastore-id /r4/Group/ ID /\$export

開始之前

符合下列需求，以使用 FHIR REST API 的 提出匯出請求 HealthLake。

- 您必須已設定具有進行匯出請求必要許可的使用者、群組或角色。如需進一步了解，請參閱 [授權export請求](#)。
- 您必須已建立服務角色，將 HealthLake 存取權授予要匯出資料的 Amazon S3 儲存貯體。服務角色也必須指定 HealthLake 為服務主體。如需設定許可的詳細資訊，請參閱[設定匯出任務的許可](#)。

授權export請求

若要使用 FHIR REST 成功匯出請求API，請使用 或 OAuth2.0 授權您的使用者、群組IAM或角色。您也必須具有服務角色。

使用 授權請求 IAM

當您提出\$export請求時，使用者、群組或角色必須具有 StartFHIRExportJobWithPost、DescribeFHIRExportJobWithGet和 CancelFHIRExportJobWithDeleteIAM動作包含在政策中。

Important

HealthLake SDK 使用 StartFHIRExportJob API 操作匯出請求，以及使用 StartFHIRExportJobWithPostAPI操作FHIRRESTAPI匯出請求有不同的IAM動作。使用 SDK 匯出StartFHIRExportJob和使用 FHIR REST API 匯出的每個IAM動作StartFHIRExportJobWithPost，都可以分別處理允許/拒絕許可。如果您想要同時限制 SDK和 FHIR REST API 匯出，請務必拒絕每個IAM動作的許可。

在 FHIR(OAuth 2.0) SMART上使用 授權請求

當您在FHIR已啟用 HealthLake 的資料存放SMART區上提出\$export請求時，您需要指派適當的範圍。若要進一步了解支援的 範圍，請參閱 [HealthLake 資料存放區FHIR資源特定範圍](#)。

提出export請求

本節說明使用 FHIR REST 提出匯出請求時必須採取的必要步驟API。

為了避免 AWS 您的帳戶意外產生費用，我們建議您在未提供export語法的情況下提出請求來測試您的POST請求。

若要提出請求，您必須執行下列動作：

1. 在支援端點URL的POST請求export中指定。
2. 指定所需的標頭參數。
3. 指定定義必要參數的請求內文。

步驟 1：在支援端點URL的POST請求export中指定

HealthLake 支援三種類型的大量匯出端點請求。若要提出大量匯出請求，您必須在三個支援的端點之一上提出POST以 為基礎的請求。下列範例示範如何在請求 export中指定 URL。

- POST `https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/$export`
- POST `https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Patient/$export`
- POST `https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Group/ID/$export`

在該POST請求字串中，您可以使用下列支援的搜尋參數。

支援的搜尋參數

HealthLake 在大量匯出請求中支援下列搜尋修飾詞。

這些範例包含特殊字元，在提交請求之前必須先編碼。

名稱	是否為必要？	描述	範例
_outputFormat	否	要產生之請求的大量資料檔案的格式。接受的值為 application/fhir+ndjson、application/ndjson、ndjson。	
_type	否	您想要包含在匯出任務中的逗號分隔 FHIR 資源類型的字串。我們建議包含，_type 因為匯出所有資源時，這可能會有成本影響。	&_type=MedicationStatement, Observation
_since	否	在日期時間戳記當天或之後修改的資源類型。如果資源類型沒有上次更新的時間，它們將包含在回應中。	&_since=2024-05-09T00%3A00%3A00Z

步驟 2：指定必要的標頭參數

若要使用 FHIR REST 提出匯出請求 API，您必須指定下列兩個標頭參數。

- Content-Type：application/fhir+json
- 偏好：respond-async

接著，您必須在請求內文中指定必要的元素。

步驟 3：指定請求內文，會定義所需的參數。

匯出請求也需要 JSON 格式的內文。內文可以包含下列參數。

金鑰	是否為必要？	描述	Value
DataAccessRoleArn	是	HealthLake 服務角色ARN的。使用的服務角色必須指定 HealthLake 為服務主體。	arn:aws:iam:: 444455556666 :role/ your-healthlake-service-role
JobName	否	匯出請求的名稱。	your-export-job-name
S3Uri	是	OutputDataConfig 金鑰的一部分。將下載匯出資料的URI目的地儲存貯體 S3。	s3://DOC-EXAMPLE-DESTINATION-BUCKET/ EXPORT-JOB /
KmsKeyId	是	OutputDataConfig 金鑰的一部分。用於保護 Amazon S3 儲存貯體ARN的 AWS KMS 金鑰。	arn:aws:kms: region-of-bucket:123456789012 :key/ 1234abcd-12ab-34cd-56ef-1234567890ab

Example – 使用 提出的匯出請求內文 FHIR REST API

若要使用 FHIR REST 提出匯出請求API，您必須指定內文，如下所示。

```
{
  "DataAccessRoleArn": "arn:aws:iam::444455556666:role/your-healthlake-service-role",
  "JobName": "your-export-job",
  "OutputDataConfig": {
    "S3Configuration": {
      "S3Uri": "s3://DOC-EXAMPLE-DESTINATION-BUCKET/EXPORT-JOB",
      "KmsKeyId": "arn:aws:kms:region-of-bucket:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  }
}
```

```
}  
}
```

當您的請求成功時，您將會收到下列回應。

回應標頭

```
content-location: https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/export/your-export-request-job-id
```

回應內文

```
{  
  "datastoreId": "your-data-store-id",  
  "jobStatus": "SUBMITTED",  
  "jobId": "your-export-request-job-id"  
}
```

管理您的匯出請求

成功提出匯出請求後，您可以使用 `export` 來描述目前匯出請求的狀態，以及取消目前的匯出請求 `export`，藉此管理該請求。

當您使用 REST 取消匯出請求時API，將僅向您收取截至您提交取消請求之前匯出的資料部分費用。

下列主題說明如何取得或取消目前匯出請求的狀態。

取消匯出請求

若要取消匯出請求，請提出DELETE請求，並在請求 中提供任務 IDURL。

```
DELETE https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
export/your-export-request-job-id
```

當您的請求成功時，您會收到以下內容。

```
{  
  "exportJobProperties": {  
    "jobId": "your-original-export-request-job-id",  
    "jobStatus": "CANCEL_SUBMITTED",
```

```

    "datastoreId": "your-data-store-id"
  }
}

```

當您的請求不成功時，您會收到以下內容。

```

{
  "resourceType": "OperationOutcome",
  "issue": [
    {
      "severity": "error",
      "code": "not-supported",
      "diagnostics": "Interaction not supported."
    }
  ]
}

```

描述匯出請求

若要取得匯出請求的狀態，請使用 `export` 和 提出GET請求 **`export-request-job-id`**。

```

GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
export/your-export-request-id

```

JSON 回應將包含 `ExportJobProperties` 物件。它可能包含下列索引鍵：值對。

名稱	是否為必要？	描述	Value
<code>DataAccessRoleArn</code>	否	HealthLake 服務角色ARN的。使用的服務角色必須指定 HealthLake 為服務主體。	<code>arn:aws:iam:: 444455556666 :role/your-healthlake-service-role</code>
<code>SubmitTime</code>	否	匯出任務提交的日期。	<code>Apr 21, 2023 5:58:02</code>
<code>EndTime</code>	否	匯出任務完成的時間。	<code>Apr 21, 2023 6:00:08 PM</code>

名稱	是否為必要？	描述	Value
JobName	否	匯出請求的名稱。	your-export-job-name
JobStatus	否		有效的 值如下： SUBMITTED IN_PROGRESS COMPLETED _WITH_ERRORS COMPLETED FAILED
S3Uri	是	OutputDataConfig 物件的一部分。要下載匯出資料的目的地儲存貯體 URI Amazon S3。	s3://DOC-EXAMPLE-DESTINATION-BUCKET/ EXPORT-JOB /
KmsKeyId	是	OutputDataConfig 物件的一部分。用於保護 Amazon S3 儲存貯體ARN的 AWS KMS 金鑰。	arn:aws:kms: region-of-bucket:123456789012 :key/1234abcd-12ab-34cd-56ef-1234567890ab

Example：描述使用 提出之匯出請求的內文 FHIR REST API

成功時，您會收到下列JSON回應。

```
{
  "exportJobProperties": {
    "jobId": "your-export-request-id",
    "jobName": "your-export-job",
    "jobStatus": "SUBMITTED",
    "submitTime": "Apr 21, 2023 5:58:02 PM",
    "endTime": "Apr 21, 2023 6:00:08 PM",
```

```
"datastoreId": "your-data-store-id",
"outputDataConfig": {
  "s3Configuration": {
    "S3Uri": "s3://DOC-EXAMPLE-DESTINATION-BUCKET/EXPORT-JOB",
    "KmsKeyId": "arn:aws:kms:region-of-
bucket:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
},
"DataAccessRoleArn": "arn:aws:iam::444455556666:role/your-healthlake-service-role",
}
```

在 中刪除資料存放區 HealthLake

刪除資料存放區是非同步操作。啟動後，狀態會變更為刪除。資料存放區會維持刪除狀態，直到日期存放區中的所有FHIR資料也移除所需的基礎基礎設施為止。

移除資料和基礎設施後，HealthLake 您的資料存放區狀態會變更為已刪除。刪除後，您的資料存放區的詳細資訊只能使用 `DescribeFHIRDataStore` 和 `ListFHIRDataStores` 操作七天。七天後，刪除的資料存放區將不會出現在結果中。

若要成功刪除資料存放區，提出請求的使用者、群組或角色必須將 IAM 動作 `glue:DeleteDatabase` 新增至其 IAM 政策。此 IAM 動作不包含在 受管政策 中 `AWS AmazonHealthLakeFullAccess`。

您可以使用 AWS Management Console AWS SDKs 或 刪除資料存放區 AWS CLI。

主題

- [刪除資料存放區（主控台）](#)
- [刪除資料存放區 \(AWS SDKs 和 AWS CLI\)](#)

刪除資料存放區（主控台）

若要使用 主控台刪除資料存放區，請在資料存放區頁面上選擇您的資料存放區，然後選擇刪除。

刪除 HealthLake 資料存放區

1. <https://console.aws.amazon.com//healthlake/> 開啟 HealthLake 主控台。
2. 開啟導覽窗格 (≡)。
3. 然後，選擇資料存放區。
4. 在資料存放區頁面上，選擇您要刪除的資料存放區旁的選項。
5. 然後，選擇刪除
6. 在對話方塊中類型中，**delete** 確認您想要刪除選取的資料存放區。
7. 再選擇 Delete (刪除)。然後，資料存放區的狀態將從作用中變更為刪除。

刪除資料存放區 (AWS SDKs 和 AWS CLI)

您可以使用以下程式碼範例來刪除 HealthLake 資料存放區。

AWS CLI

下列範例示範搭配使用 DeleteFHIRDatastore操作 AWS CLI。若要執行範例，您必須安裝 AWS CLI。

```
aws healthlake delete-fhir-datastore --datastore-id
'eeb8005725ae22b35b4edbd6c68cf2dfd'
```

成功時，您會得到下列JSON回應。

```
{
  "DatastoreProperties": {
    "DatastoreId": "eeb8005725ae22b35b4edbd6c68cf2dfd",
    "DatastoreArn": "arn:aws:healthlake:us-west-2:728347309221:datastore/fhir/",
    "DatastoreName": "delete-me",
    "DatastoreStatus": "ACTIVE",
    "CreatedAt": "2022-10-03T10:53:45.020000-07:00",
    "DatastoreTypeVersion": "R4",
    "DatastoreEndpoint": "https://healthlake.us-west-2.amazonaws.com/
datastore/5b6e4cd798289a4ab8dad6c1002dd731/r4/",
    "SseConfiguration": {
      "KmsEncryptionConfig": {
        "CmkType": "AWS_OWNED_KMS_KEY"
      }
    },
    "PreloadDataConfig": {
      "PreloadDataType": "SYNTHESIS"
    }
  }
}
```

Python (boto3)

for Python AWS SDK支援採用單一參數的 describe_fhir_datastore方法DatastoreId。

```
import boto3

#Create a Healthlake client
healthlake_client = boto3.client('healthlake')

#Call the describe_fhir_datastore method
data_store_details =
    healthlake_client.describe_fhir_datastore(DatastoreId='cdf8f1557e57c543bdc627fb8f12b7fd')
```

```
print(data_store_details)
```

成功時，它會傳回 python 字典。

```
{'DatastoreProperties': {'DatastoreId': 'cdf8f1557e57c543bdc627fb8f12b7fd',
  'DatastoreArn': 'arn:aws:healthlake:us-west-2:728347309221:datastore/fhir/
cdf8f1557e57c543bdc627fb8f12b7fd', 'DatastoreName': '08-24-2022-test-data-
store', 'DatastoreStatus': 'ACTIVE', 'CreatedAt': datetime.datetime(2022,
  8, 23, 22, 12, 14, 359000, tzinfo=tzlocal()), 'DatastoreTypeVersion': 'R4',
  'DatastoreEndpoint': 'https://healthlake.us-west-2.amazonaws.com/datastore/
cdf8f1557e57c543bdc627fb8f12b7fd/r4/', 'SseConfiguration': {'KmsEncryptionConfig':
  {'CmkType': 'AWS_OWNED_KMS_KEY'}}, 'PreloadDataConfig': {'PreloadDataType':
  'SYNTHEA'}}, 'ResponseMetadata': {'RequestId': 'aef4b268-ad4b-4b57-
bc97-2da956356835', 'HTTPStatusCode': 200, 'HTTPHeaders': {'date': 'Wed, 05 Oct
  2022 01:21:44 GMT', 'content-type': 'application/x-amz-json-1.0', 'content-
length': '547', 'connection': 'keep-alive', 'x-amzn-requestid': 'aef4b268-ad4b-4b57-
bc97-2da956356835'}, 'RetryAttempts': 0}}
```

若要一次傳回多個資料存放區的詳細資訊，請使用 `ListFHIRDatastore`

使用 `DeleteFHIRDataStore` 命令，AWS CLI 如下列範例所示。您也可以使用 [delete-fhir-datastore API](#) 或主控台刪除資料存放區。刪除資料存放區會移除資料存放區和基礎基礎設施中包含的所有 FHIR 資源版本。與已刪除資料存放區相關的日誌會依照 HIPAA 指導方針保留在服務帳戶內。

```
aws healthlake delete-fhir-datastore
  --datastore-id (Data Store ID)
```

如下列範例 JSON 回應所示，狀態會變更為「DELETING」，以確認資料存放區及其內容正在刪除中。

```
{
  "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/
datastore/eeb8005725ae22b35b4edbd68cf2dfd/r4/",
  "DatastoreArn": "arn:aws:healthlake:us-east-1:(AWS Account ID):datastore/(Datastore
ID)",
  "DatastoreStatus": "DELETING",
  "DatastoreId": "(Datastore ID)"
}
```

使用與 HealthLake 資料存放區 FHIR REST API 的互動

在 AWS HealthLake 中，您使用 Fast Healthcare Interoperability Resources (FHIR) REST API 互動來管理和搜尋資料存放區中的 FHIR 資源。FHIR REST API 互動用於對資料存放區中的資源執行建立、讀取、更新和刪除 (CRUD) 互動。您也可以使用 GET 或 POST HTTP 請求來形成複雜的搜尋字串，因為 HealthLake FHIR 支援支援的搜尋操作子集。

基於一致性目的，FHIR 資源類型會根據 HL7 FHIR R4 [StructureDefinition](#) 資源進行驗證。若要尋找作用中 HealthLake 資料存放區的 FHIR 相關功能，請提出中 metadata 指定的 GET 請求 URL，如下所示。

```
GET https://healthlake.region.amazonaws.com/datastore/datastore-id/r4/metadata
```

成功後，您將收到 200 HTTP 回應代碼和 HealthLake 資料存放區的功能陳述式。如需詳細資訊，請參閱 HL7 FHIR R4 文件 [CapabilityStatement](#) 中的。

下表列出支援 FHIR 的互動 AWS HealthLake。

FHIR 支援的互動 AWS HealthLake

FHIR 互動	描述
整個系統互動	
capabilities	取得系統的功能陳述式
batch/transaction	在單一互動中更新、建立或刪除一組資源
類型層級互動	
create	使用伺服器指派的 ID 建立新的資源
search	根據某些篩選條件搜尋資源類型
history	擷取特定資源類型的變更歷史記錄
執行個體層級互動	
read	讀取資源的目前狀態

FHIR 互動	描述
history	讀取特定資源的變更歷史記錄
vread	讀取特定版本資源的狀態
update	依資源的 ID 更新資源（或如果是新資源，請建立）
delete	刪除資源

主題

- [中支援FHIR的資源類型 AWS HealthLake](#)
- [在 HealthLake 資料存放區上執行建立、讀取、更新和刪除 \(CRUD\) 操作](#)
- [使用 FHIRRESTAPI操作搜尋 HealthLake 資料存放區](#)
- [讀取FHIR資源歷史記錄](#)
- [使用病患 \\$所有FHIRRESTAPI操作取得病患資料](#)
- [使用 \\$export 從 HealthLake 資料存放區匯出資料](#)

中支援FHIR的資源類型 AWS HealthLake

下表列出 支援的 FHIR R4 資源類型 AWS HealthLake。如需詳細資訊，請參閱 HL7 FHIR R4 文件中的[資源索引](#)。

FHIR 支援的 R4 資源類型 HealthLake

帳戶	DetectedIssue	發票	從業者
ActivityDefinition	裝置	程式庫	PractitionerRole
AdverseEvent	DeviceDefinition	連結	程序
AllergyIntolerance	DeviceMetric	清單	證明
預約	DeviceUseStatement	位置	問卷
AppointmentResponse	DeviceRequest	量值	QuestionnaireResponse

AuditEvent-請參閱備註	DiagnosticReport	MeasureReport	RelatedPerson
二進位	DocumentManifest	媒體	RequestGroup
BodyStructure	DocumentReference	藥物	ResearchStudy
套件 - 請參閱備註	EffectEvidenceSynthesis	MedicationAdministration	ResearchSubject
CapabilityStatement	遇到	MedicationDispense	RiskAssessment
CarePlan	端點	MedicationKnowledge	RiskEvidenceSynthesis
CareTeam	EpisodeOfCare	MedicationRequest	排程
ChargeItem	EnrollmentRequest	MedicationStatement	ServiceRequest
ChargeItemDefinition	EnrollmentResponse	MessageHeader	Slot
取得	ExplanationOfBenefit	MolecularSequence	樣本
ClaimResponse	FamilyMemberHistory	NutritionOrder	StructureDefinition
Communication	旗標	觀察	StructureMap
CommunicationRequest	目標	OperationOutcome	物質
合成	群組	組織	SupplyDelivery
ConceptMap	GuidanceResponse	OrganizationAffiliation	SupplyRequest
條件	HealthcareService	參數	任務
同意	ImagingStudy	病患	ValueSet
合約	預防接種	PaymentNotice	VisionPrescription

涵蓋範圍	ImmunizationEvaluation	PaymentReconciliation	VerificationResult
CoverageEligibilityRequest	ImmunizationRecommendation	個人	
CoverageEligibilityResponse	InsurancePlan	PlanDefinition	

⚠ FHIR 規格和 HealthLake

- 您不能使用下列資源類型提出 GET 或 POST 請求：二進位 OperationOutcome、套件和參數。
- AuditEvent — 您可以建立或讀取 AuditEvent 資源，但無法更新或刪除。
- 套件 — HealthLake 管理套件請求的方式有多種。如需詳細資訊，請參閱[使用 Bundle 管理多個FHIR資源](#)。
- VerificationResult — 此資源類型僅支援 2023 年 12 月 9 日之後建立的資料存放區。

在 HealthLake 資料存放區上執行建立、讀取、更新和刪除 (CRUD) 操作

雖然您在管理資料存放區、匯入資料和匯出資料時使用原生 AWS 動作，但您可以使用四個主要 FHIRHTTP 操作在 HealthLake 資料存放區中建立 (POST)、讀取 (GET)、更新 (PUT) 和刪除 (DELETE) FHIR 資源。下列主題說明如何使用 FHIRRESTAPI 服務在 HealthLake 資料存放區上執行建立、讀取、更新和刪除 (CRUD) 操作。您必須使用 Signature 第 4 版簽署程序來驗證 HealthLake API 透過 HTTP 用戶端傳送的請求。若要進一步了解，請參閱中的[簽章第 4 版簽署程序](#) AWS 一般參考。

主題

- [使用 建立資源 POST](#)
- [使用 讀取資源 GET](#)
- [使用 更新資源 PUT](#)
- [使用 刪除資源 DELETE](#)
- [使用 Bundle 管理多個FHIR資源](#)

使用 建立資源 POST

您可以使用 POST 請求在 HealthLake 資料存放區中建立新的資源。POST 請求不需要您提供 id 元素。成功建立資源時，HealthLake 伺服器會傳回 201 已建立 HTTP 狀態碼。

Note

當您對 DocumentReference 資源類型提出 POST 請求時，不會修改現有的延伸模組。反之，AWS HealthLake 會將具有現有擴充功能的新擴充功能新增至您的資料存放區。如需如何在 DocumentReference 資源類型上使用 HealthLake 自然語言處理 (NLP) 來擷取重要醫療資料的詳細資訊，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生 FHIR DocumentReference 資源 AWS HealthLake](#)。

Example 使用 **POST** 請求建立 **Patient** 資源。

若要建立 HealthLake 資料存放區 POST 請求，請使用資料存放區的端點，並提供 JSON 請求內文。若要尋找資料存放區的端點，請在 HealthLake 主控台中查看資料存放區下的，或使用 AWS HealthLake API 參考中的 [DescribeFHIRDatastore](#) 操作。

POST Request

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient
```

JSON Request Body

```
{  
  "resourceType": "Patient",  
  "identifier": [ { "system": "urn:oid:1.2.36.146.595.217.0.1", "value":  
"12345" } ],  
  "name": [ {  
    "family": "Silva",  
    "given": ["Ana", "Carolina"]  
  } ],  
  "gender": "female",  
  "birthDate": "1992-02-10"  
}
```

JSON 回應

若要確認建立病患資源，您將收到201已建立HTTP的狀態碼和下列JSON回應。

```
{
  "resourceType": "Patient",
  "identifier": [
    {
      "system": "urn:oid:1.2.36.146.595.217.0.1",
      "value": "12345"
    }
  ],
  "name": [
    {
      "family": "Silva",
      "given": [
        "Ana",
        "Carolina"
      ]
    }
  ],
  "gender": "female",
  "birthDate": "1992-02-10",
  "id": "274b408a-1201-4e9f-a621-1df937f1a26d",
  "meta": {
    "lastUpdated": "2022-06-13T23:31:24.427Z"
  }
}
```

使用 讀取資源 GET

此範例說明如何使用 GET 請求讀取病患FHIR資源。

Example 使用 **GET**請求讀取特定**Patient**資源。

若要建立 HealthLake 資料存放區GET請求，請使用資料存放區的端點。若要尋找資料存放區的端點，請查看 HealthLake 主控台內的資料存放區，或使用 AWS HealthLake API 參考中的 [DescribeFHIRDatastore](#) 操作。

您也必須包含資源類型**Patient**和有效的識別符 **2de04858-ba65-44c1-8af1-f2fe69a977d9**。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
Patient/2de04858-ba65-44c1-8af1-f2fe69a977d9
```

JSON 回應

成功後，您將收到一個200HTTP狀態碼和以下JSON回應。

```
{
  "resourceType": "Patient",
  "active": true,
  "name": [
    {
      "use": "official",
      "family": "Doe",
      "given": [
        "Jane"
      ]
    },
    {
      "use": "usual",
      "given": [
        "Jane"
      ]
    }
  ],
  "gender": "female",
  "birthDate": "1966-09-01",
  "meta": {
    "lastUpdated": "2020-11-23T06:24:13.202Z"
  },
  "id": "2de04858-ba65-44c1-8af1-f2fe69a977d9"
}
```

使用 更新資源 PUT

下列範例示範如何使用 PUT更新病患FHIR資源類型中病患的詳細資訊。此外，當您對尚未建立的資源提出PUT請求時，它會建立初始版本。

如果資源已更新，您的請求將傳回200HTTP狀態碼，或者如果建立新資源，則將傳回201HTTP狀態碼。

Note

當您對DocumentReference資源類型提出PUT請求時，不會修改現有的延伸模組。反之，AWS HealthLake 會將具有現有擴充功能的新擴充功能新增至您的資料存放區。如需如何

在DocumentReference資源類型上使用 HealthLake 自然語言處理 (NLP) 來擷取重要醫療資料的詳細資訊，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。

Example 使用 **PUT**請求更新**Patient**資源類型

當您提出PUT請求時，您將需要資料存放區的端點、要更新的資源類型名稱、識別符和JSON請求內文。

如果您使用 PUT建立新的資源，則會使用提供的識別符來建立新的資源。

PUT Request

有效PUT請求的範例結構：

```
PUT https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/2de04858-ba65-44c1-8af1-f2fe69a977d9
```

JSON Request Body

用來更新指定病患資源的範例JSON內文。

```
{  
  "id": "2de04858-ba65-44c1-8af1-f2fe69a977d9",  
  "resourceType": "Patient",  
  "active": true,  
  "name": [  
    {  
      "use": "official",  
      "family": "Doe",  
      "given": [  
        "Jane"  
      ]  
    },  
    {  
      "use": "usual",  
      "given": [  
        "Jane"  
      ]  
    }  
  ],  
}
```

```
"gender": "female",
"birthDate": "1985-12-31"
}
```

JSON 回應

您將收到下列項目 JSON，以確認變更：

```
{
  "id": "2de04858-ba65-44c1-8af1-f2fe69a977d9",
  "resourceType": "Patient",
  "active": true,
  "name": [{
    "use": "official",
    "family": "Doe",
    "given": [
      "Jane"
    ]
  }],
  {
    "use": "usual",
    "given": [
      "Jane"
    ]
  }
],
  "gender": "female",
  "birthDate": "1985-12-31",
  "meta": {
    "lastUpdated": "2020-11-23T06:43:45.133Z"
  }
}
```

條件式更新

條件式更新允許根據某些識別搜尋條件更新現有資源，而不是根據邏輯 ID。當伺服器處理此更新時，它會針對資源類型使用其標準搜尋功能執行搜尋，目標是解決此請求的單一邏輯 ID。

其採取的動作取決於找到多少相符項目：

- 沒有相符項目，請求內文中沒有提供 ID：伺服器會建立資源。
- 沒有相符項目、提供的 ID 和資源，並不存在 ID：伺服器會將互動視為更新為建立互動。

- 沒有相符項目、提供的 ID 和已存在：伺服器拒絕更新並發生錯誤409 Conflict。
- One Match，未提供資源 ID OR（提供的資源 ID 且符合找到的資源）：伺服器會針對上述相符資源執行更新，如果資源已更新，伺服器會SHALL傳回 200 OK；
- 一個相符，提供資源 ID，但與找到的資源不相符：伺服器傳回409 Conflict錯誤，指出用戶端 ID 規格是 的問題 OperationOutcome
- 多個相符項目：伺服器傳回412 Precondition Failed錯誤，指出用戶端的條件不夠選擇性，最好使用 OperationOutcome

Example – 更新名稱為 Peter 的患者資源，出生日期為 2000 年 1 月 1 日，電話號碼為 1234567890：

```
PUT https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?name=peter&birthdate=2000-01-01&phone=1234567890
```

使用 刪除資源 DELETE

若要刪除 HealthLake 資料存放區中的資源，您必須提出DELETEHTTP請求。

Example 使用 **DELETE**請求刪除特定**Patient**資源類型。

若要建立DELETE請求，請使用資料存放區的端點。若要尋找資料存放區的端點，請在 HealthLake 主控台中查看資料存放區下的，或使用 AWS HealthLake API 參考中找到的 [DescribeFHIRDatastore](#) 操作。

您還必須包含資源類型和有效的識別符。

```
DELETE https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/2de04858-ba65-44c1-8af1-f2fe69a977d9
```

HTTP 回應

成功後，您將收到一個204HTTP狀態碼，確認資源已不在資料存放區中。當刪除請求失敗時，您將收到一個 400 系列HTTP狀態碼，指出DELETE請求失敗的原因。

使用 Bundle 管理多個FHIR資源

在 HL7 FHIR R4 規格中，套件只是 資源的集合。HealthLake 支援在FHIRRESTAPI請求中建立套件資源類型，並使用套件交易在單一FHIRRESTAPI請求中執行多個CRUD操作。在套件交易中，您必須指定 套件類型，如 FHIRRESTAPI請求batch中所示。

所有套件請求都會由 記錄 AWS CloudTrail。若要進一步了解 CloudTrail 如何搭配 使用 HealthLake，請參閱 [使用 AWS CloudTrail 記錄 AWS HealthLake API 呼叫](#)。

HL7 FHIR R4 資源（外部）

- 若要閱讀完整規格，請參閱FHIR文件索引中的[資源類型：套件](#)。
- 若要閱讀有關使用 FHIR REST 的批次互動API，請參閱 FHIR 文件索引[FHIRREST中的使用 的批次互動API](#)。

以下各節說明如何建構FHIRRESTAPI請求，以建立新的套件資源或使用套件交易個別處理資源。

 HealthLake 主控台、AWS CLI和 之間的差異 AWS SDKs
HealthLake 主控台僅支援在FHIRRESTAPI請求 中指定套件資源類型的套件類型操作URL。

使用FHIR套件執行多個CRUD操作

當您的請求 中未指定資源類型時URL，FHIRRESTAPI請求會剖析為個別資料存放區交易。JSON 本文提供的每個CRUD操作都會進行評估，並傳回特定HTTP狀態碼。HealthLake 支援套件類型 batch。

若要在單一FHIRRESTAPI請求中執行多個CRUD操作，請執行下列動作：

下列清單顯示套件請求中使用的FHIRRESTAPI請求內文截斷部分。如需完整的請求內文，請參閱[建立涉及多個CRUD操作的套件請求](#)。

1. 請勿在您的POST請求中指定資源類型：

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
```

2. 在請求內文中，將套件類型指定為 "type": "batch"
3. 在請求內文中，為以 resource金鑰開始的每個CRUD互動指定資源特定的資料。
4. 每個CRUD操作在請求內文request中指定為，如下所示：

```
{ ...  
  "request" : {  
    "method" : "HTTP-VERB",  
    "url" : "FHIR-RESOURCE-TYPE-URL"  
  }  
}
```

$$\left. \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \right\}$$

在JSON回應中，您會取得請求中指定之每個CRUD操作HTTP的狀態碼。

HealthLake 限制套件交易

- 若要進一步了解 套件 HealthLake 的限制，請參閱 [AWS HealthLake 端點和配額](#)。

以下是包含多個操作的 Bundle CRUD 操作範例。

Example – 建立涉及多個CRUD操作的套件請求。

若要提出執行多個CRUD操作的FHIRRESTAPI請求，您必須使用資料存放區端點提出POST請求，並提供JSON請求內文。

您可以在 HealthLake 主控台的資料存放區下找到資料存放區的端點，或使用 AWS HealthLake API 參考中的 [DescribeFHIRDatastore](#) 操作。

POST Request

使用資料存放區的端點提出POST請求。使用下一個索引標籤JSON，請求內文來查看請求內文的必要元素。

POST <https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/>

JSON Request Body

在請求內文中，您必須提供下列金鑰：值對，以及有關個別CRUD請求的任何其他FHIR資源特定資料。第一個範例顯示一個截斷的JSON請求內文，強調所需的元素。第二個範例顯示完整的JSON請求內文。

```
{
  "resourceType": "Bundle",
  "id": "bundle-batch-operation",
  "meta": {
    "lastUpdated": "2014-08-18T01:43:30Z"
  },
  "type": "batch", ## Required
  "entry": [
```

```

{
  ## CRUD Transaction - 1
  "resource": {
    "resourceType": "Patient",
    ...
  },
  "request": { ## Required
    "method": "POST",
    "url": "Patient"
  }
},
{
  ## CRUD Transaction - 2
  "resource": {
    "resourceType": "Medication",
    ...
  },
  "request": { ## Required
    "method": "POST",
    "url": "Medication"
  }
}
]
}

```

以下是顯示建立新的 Patient Medication 資源類型的完整範例。

```

{
  "resourceType": "Bundle",
  "id": "bundle-transaction",
  "meta": {
    "lastUpdated": "2014-08-18T01:43:30Z"
  },
  "type": "batch",
  "entry": [
    {
      "resource": {
        "resourceType": "Patient",
        "meta": {
          "lastUpdated": "2022-06-03T17:53:36.724Z"
        },
        "text": {
          "status": "generated",

```

```
    "div": "Some narrative"
  },
  "active": true,
  "name": [
    {
      "use": "official",
      "family": "Jackson",
      "given": [
        "Mateo",
        "James"
      ]
    }
  ],
  "gender": "male",
  "birthDate": "1974-12-25"
},
"request": {
  "method": "POST",
  "url": "Patient"
}
},
{
  "resource": {
    "resourceType": "Medication",
    "id": "med0310",
    "contained": [
      {
        "resourceType": "Substance",
        "id": "sub03",
        "code": {
          "coding": [
            {
              "system": "http://snomed.info/sct",
              "code": "55452001",
              "display": "Oxycodone (substance)"
            }
          ]
        }
      }
    ]
  }
},
"code": {
  "coding": [
    {
      "system": "http://snomed.info/sct",
```

```

        "code": "430127000",
        "display": "Oral Form Oxycodone (product)"
      }
    ]
  },
  "form": {
    "coding": [
      {
        "system": "http://snomed.info/sct",
        "code": "385055001",
        "display": "Tablet dose form (qualifier value)"
      }
    ]
  },
  "ingredient": [
    {
      "itemReference": {
        "reference": "#sub03"
      },
      "strength": {
        "numerator": {
          "value": 5,
          "system": "http://unitsofmeasure.org",
          "code": "mg"
        },
        "denominator": {
          "value": 1,
          "system": "http://terminology.hl7.org/CodeSystem/v3-orderableDrugForm",
          "code": "TAB"
        }
      }
    }
  ]
},
"request": {
  "method": "POST",
  "url": "Medication"
}
}

```

JSON 回應

若要確認建立範例套件交易中指定的資源，您會取得每個包含CRUD操作的201已建立HTTP狀態碼。當CRUD操作失敗時，您會取得 400 系列HTTP狀態，指出個別請求失敗的原因。

```
{
  "resourceType": "Bundle",
  "type": "batch-response",
  "timestamp": "2022-06-15T01:31:34.300+00:00",
  "entry": [
    {
      "response": {
        "status": "201",
        "location": "Patient/fd68ce38-ba30-4459-9eeb-476ad9f4f4ca",
        "lastModified": "2022-06-15T01:31:34.180+00:00"
      }
    },
    {
      "response": {
        "status": "201",
        "location": "Medication/5bf3b8cc-4076-4219-aba1-e2c53d7916f4",
        "lastModified": "2022-06-15T01:31:34.180+00:00"
      }
    }
  ]
}
```

將資源分組為套件資源類型

若要建立新的套件資源類型，您必須在 FHIR REST API 請求Bundle中指定，並提供有效的JSON內文，其中包含您想要分組在一起的資源。

在請求 中指定套件時URL，JSON請求內文的內容會依原樣儲存在 HealthLake 您的資料存放區中。因此，無法對個別資源類型執行任何CRUD操作。此類型的套件會獲指派一個新的資源 ID。因為資源是依原狀儲存，所以您無法對儲存在套件資源類型中的個別資源提出GET或POST請求。

Note

HL7 FHIR R4 規格也支援使用[群組](#)、[合成](#)和[清單](#)來分組資源。當您建立這些資源類型時，不會直接包含個別資源。反之，他們會使用 Reference元素來指向個別資源。因此，使用這些資源類型可讓您修改其中包含的個別資源。

若要建立Bundle資源類型，您必須在POST請求中指定它，並提供JSON列舉您想要包含的資源。

Example – 使用 **POST** 請求建立套件資源

若要建立bundle資源，請執行下列動作

1. 格式化FHIRRESTAPI請求，如下所示：

POST **https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Bundle**

2. 提供內JSON文，指定您要分組在一起的資源。此範例將兩個病患資源分組。

```
{
  "resourceType": "Bundle",
  "id": "bundle-transaction",
  "meta": {
    "lastUpdated": "2018-03-11T11:22:16Z"
  },
  "type": "document",
  "entry": [
    {
      "resource": {
        "resourceType": "Patient",
        "name": [
          {
            "family": "Smith",
            "given": [
              "Jane"
            ]
          }
        ],
        "gender": "female",
        "address": [
          {
            "line": [
              "123 Main St."
            ],
            "city": "Anycity",
            "state": "Any State",
            "postalCode": "12345"
          }
        ]
      }
    ]
  ]
}
```

```
    },
    {
      "resource": {
        "resourceType": "Patient",
        "name": [
          {
            "family": "Jackson",
            "given": [
              "Mateo"
            ]
          }
        ],
        "gender": "male",
        "address": [
          {
            "line": [
              "1234 Main St."
            ],
            "city": "Anycity",
            "state": "Any State",
            "postalCode": "12345"
          }
        ]
      }
    }
  ]
}
```

使用 FHIRRESTAPI操作搜尋 HealthLake 資料存放區

HealthLake 支援使用標準中提供的RESTAPI操作來搜尋資料存放區FHIR。在本節中，您會找到如何在多種不同資源類型上提出 GET和 POST請求的範例。

Note

對於涉及個人身分識別資訊 (PII) 或受保護健康資訊 (PHI) 的查詢，建議使用POST請求。在POST請求中， PII或 PHI 會新增為請求內文的一部分，並在傳輸中加密。

FHIR 規格支援多個搜尋參數類型，但僅 HealthLake 支援子集。如需詳細資訊，請參閱 [支援的搜尋參數類型](#) 和 [支援的進階搜尋參數 HealthLake](#)。

使用 FHIRRESTAPI 操作搜尋資料存放區。

- [支援的搜尋參數類型](#)
- [支援的進階搜尋參數 HealthLake](#)
 - [_include](#)
 - [_revinclude](#)
 - [_summary](#)
 - [_elements](#)
 - [_total](#)
 - [_sort](#)
 - [_count](#)
 - [Chaining and Reverse Chaining\(_has\)](#)
- [支援的搜尋修改器](#)
- [支援的搜尋比較器](#)
- [不支援的搜尋參數 HealthLake](#)
- [使用POST範例搜尋](#)
- [使用GET範例搜尋](#)

支援的搜尋參數類型

下表顯示 中支援的搜尋參數類型 HealthLake。

支援的搜尋參數類型

搜尋參數	描述
_id	資源 ID (非完整 URL)
_lastUpdated	上次更新日期。伺服器可自行決定邊界精確度。
_tag	依資源標籤搜尋。
_profile	搜尋所有以設定檔標記的資源。
_安全性	搜尋套用至此資源的安全標籤。
_source	搜尋資源來源。

搜尋參數	描述
_text	搜尋資源的敘述。
createdAt	搜尋自訂延伸模組 - createdAt。

 Note

下列搜尋參數僅支援 2023 年 12 月 9 日之後建立的資料存放區：
_security、_source、_text、createdAt。

下表顯示如何根據指定資源類型的指定資料類型修改查詢字串的範例。為了清楚起見，範例欄中的特殊字元尚未編碼。若要讓查詢成功，請確定查詢字串已正確編碼。

搜尋參數類型	詳細資訊	範例
Number	搜尋指定資源中的數值。觀察到重要的數字。 依搜尋參數值，有效位數在 中是特定的，前導零除外。 允許比較字首。	[parameter]=100 [parameter]=1e2 [parameter]=1t100
日期/DateTime	搜尋特定日期或時間。預期的格式是 yyyy-mm-ddThh:mm:ss[Z (+ -)hh:mm]，但可能會有所不同。 接受下列資料類型：date、dateTime、Period、instant 和 Timing。如需在搜尋中使用這些資料類型的詳細資訊，請參閱 FHIR 文件索引中的 日期。	[parameter]=eq2013-01-14 [parameter]=gt2013-01-14T10:00 [parameter]=ne2013-01-14

搜尋參數類型	詳細資訊	範例
	允許比較字首。	
字串	以區分大小寫的方式搜尋一系列字元。 支援 <code>HumanName</code> 和 <code>Address</code> 類型。如需詳細資訊，請參閱 FHIR 文件索引中的 HumanName 資料類型 項目和 Address 資料類型 項目。 使用 <code>:text</code> 修改器支援進階搜尋。	<code>[base]/Patient?given=eve</code> <code>[base]/Patient?given:contains=eve</code>
權杖	搜尋與字元字串相符的項目 <code>close-to-exact</code>，通常與一對醫療程式碼值相比。 區分大小寫會連結到建立查詢時使用的程式碼系統。以訂閱為基礎的查詢有助於減少與區分大小寫相關的問題。為了清楚起見，<code> </code> 尚未編碼。	<code>[parameter]=[system] [code]</code>：這裡 <code>[system]</code> 參考編碼系統，並 <code>[code]</code> 參考該特定系統中找到的程式碼值。 <code>[parameter]=[code]</code>：在這裡，您的輸入將符合程式碼或系統。 <code>[parameter]= [code]</code>：在此，您的輸入將符合程式碼，且系統屬性沒有識別符。

搜尋參數類型	詳細資訊	範例
複合	使用修改器\$和,操作,在單一資源類型中搜尋多個參數。 允許比較字首。	/Patient?language=FR,NL&language=EN Observation?component-code-value-quantity=http://loinc.org 8480-6\$lt60 [base]/Group?characteristic-value=gender\$mixed
數量	搜尋數字、系統和程式碼做為值。號碼是必要項目,但系統和程式碼是選用項目。根據數量資料類型。如需詳細資訊,請參閱 FHIR 文件索引中的數量。 使用下列假設語法 [parameter]=[prefix][number][system][code]	[base]/Observation?value-quantity=5.4 http://unitsofmeasure.org mg [base]/Observation?value-quantity=5.4 http://unitsofmeasure.org mg [base]/Observation?value-quantity=5.4 http://unitsofmeasure.org mg [base]/Observation?value-quantity=le5.4 http://unitsofmeasure.org mg
參考資料	搜尋其他資源的參考。	[base]/Observation?subject=Patient/23 test

搜尋參數類型	詳細資訊	範例
URI	搜尋明確識別特定資源的字元字串。	[base]/ValueSet?url=http://acme.org/fhir/ValueSet/123
特別	根據整合的醫療NLP延伸進行搜尋。	

支援的進階搜尋參數 HealthLake

HealthLake 支援下列進階搜尋參數。

名稱	描述	範例	功能
<code>_include</code>	用來請求在搜尋請求中傳回其他資源。它會傳回由目標資源執行個體參考的資源。	Encounter? _include=Encounter:subject	
<code>_revinclude</code>	用來請求在搜尋請求中傳回其他資源。它會傳回參考主要資源執行個體的資源。	Patient? _id= patient-identifier &_revinclude=Encounter:patient	
<code>_summary</code>	摘要可用來請求資源的子集。	Patient? summary=text	支援下列摘要參數： _summary=true 、 _summary=false 、 _summary=text 、 _summary=data 。
<code>_element</code>	請求傳回一組特定的元素，做為搜尋結果中資源的一部分。	Patient? elements=identifie	

名稱	描述	範例	功能
		<code>r,active,link</code>	
<code>_total</code>	傳回符合搜尋參數的資源數目。	<code>Patient?_total=accurate</code>	支援 <code>_total=accurate</code> 、 <code>_total=none</code> 。
<code>_sort</code>	使用逗號分隔清單，指出傳回搜尋結果的排序順序。 - 字首可用於逗號分隔清單中的任何排序規則，以表示遞減順序。	<code>Observation?_sort=status,-date</code>	支援依類型 的欄位排序 <code>Number</code> 、 <code>String</code> 、 <code>Quantity</code> 、 <code>Token</code> 、 <code>URI</code> 、 <code>Reference</code> 。只有 2023 年 12 月 9 日之後建立的資料存放區 <code>Date</code> 才支援依 排序。最多支援 5 個排序規則。
<code>_count</code>	控制每個搜尋套件頁面要傳回多少資源。	<code>Patient?_count=100</code>	頁面大小上限為 100。
<code>chainin</code>	搜尋參考資源的元素。會將鏈結搜尋，導向至參考資源內的元素。	<code>DiagnosticReport?subject:Patient.name=peter</code>	
<code>reverse chainin (_has)</code>	根據參考資源的元素來搜尋資源。	<code>Patient?_has:Observation:patient:code=1234-5</code>	

`_include`

在搜尋查詢 `_include` 中使用 也允許傳回其他指定的 FHIR 資源。使用 `_include` 來包含向前連結的資源。

Example – 用來 **_include** 尋找患者或診斷為咳嗽的患者群組

您會搜尋指定咳嗽診斷碼Condition的資源類型，然後使用 **_include** 指定您希望該診斷subject的也傳回。在Condition資源類型中，**subject** 是指病患資源類型或群組資源類型。

為了清楚起見，範例中的特殊字元尚未編碼。若要讓查詢成功，請確定查詢字串已正確編碼。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Condition?code=49727002&_include=Condition:subject
```

_revinclude

在搜尋查詢**_revinclude**中使用 也允許傳回其他指定的FHIR資源。使用 **_revinclude** 來包含向後連結的資源。

Example – 使用 **_revinclude** 來包含連結至特定病患的相關事件和觀察資源類型

若要進行此搜尋，您必須先在**_id**搜尋參數中指定其識別符Patient來定義個人。然後，您可以使用結構**Encounter:patient**和 指定其他FHIR資源**Observation:patient**。

為了清楚起見，範例中的特殊字元尚未編碼。若要讓查詢成功，請確定查詢字串已正確編碼。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_id=patient-  
identifier&_revinclude=Encounter:patient&_revinclude=Observation:patient
```

_summary

在搜尋查詢**_summary**中使用 可讓使用者請求FHIR資源的子集。它可以包含下列其中一個值：**true**，**text**，**data**，**false**。任何其他值都會被視為無效。傳回的資源會在 **meta.tag 'SUBSETTED'** 中標示為 **，** 表示資源不完整。

- **true**：傳回資源基本定義中標記為「摘要」的所有支援元素。
- **text**：僅傳回「文字」、「id」、「中繼」元素，以及僅傳回頂層強制性元素。
- **data**：傳回除「文字」元素以外的所有部分。
- **false**：傳回資源的所有部分（多個）

在單一搜尋請求中，**_summary=text**無法與 **_include**或 **_revinclude** 搜尋參數結合。

Example – 取得資料存放區中病患資源的「文字」元素。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_summary=text
```

_elements

在搜尋查詢 **_elements** 中使用 允許請求特定 FHIR 資源元素。傳回的資源會在 `meta.tag` 'SUBSETTED' 中標示為 ，表示資源不完整。

_elements 參數包含以逗號分隔的基本元素名稱清單，例如在資源根層級定義的元素。只有列出的元素才會傳回。如果 **_elements** 參數值包含無效的元素，伺服器會忽略它們並傳回必要元素和有效元素。

_elements 不適用於包含的資源（傳回的搜尋模式為 的資源 `include`）。

在單一搜尋請求中，**_elements** 無法與 **_summary** 搜尋參數結合。

Example – 取得 HealthLake 資料存放區中病患資源的「識別符」、「作用中」、「連結」元素。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_elements=identifier,active,link
```

_total

在搜尋查詢 **_total** 中使用 會傳回符合所請求搜尋參數的資源數量。HealthLake 會在搜尋回應的 中傳回相符資源（傳回的搜尋模式為 的資源 `match`）`Bundle.total` 的總數。

_total 支援 `accurate`、`none` 參數值。**_total=estimate** 不支援。任何其他值都會被視為無效。**_total** 不適用於包含的資源（傳回的搜尋模式為 的資源 `include`）。

Example – 取得資料存放區中病患資源的總數：

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_total=accurate
```

_sort

在搜尋查詢 **_sort** 中使用 會依特定順序排列結果。結果會根據逗號分隔的排序規則清單，依優先順序排序。排序規則應該是有效的搜尋參數。任何其他值都會被視為無效。

在單一搜尋請求中，您最多可以使用 5 個排序搜尋參數。您可以選擇使用 - 字首來表示遞減順序。伺服器預設會依遞增順序排序。

支援的排序搜尋參數類型為：Number, String, Date, Quantity, Token, URI, Reference。如果搜尋參數是指巢狀的元素，則不支援此搜尋參數進行排序。例如，在資源類型的「名稱」上搜尋病患參考具有 HumanName 資料類型的 Patient.name 元素會被視為巢狀。因此，不支援依「名稱」排序病患資源。

Example – 在資料存放區中取得病患資源，並依出生日期以遞增順序排序：

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_sort=birthdate
```

_count

參數 _count 定義為對伺服器的指示，說明在單一頁面中應傳回多少資源。

頁面大小上限為 100。大於 100 的任何值都是無效的。_count=0 不支援。

Example – 搜尋病患資源，並將搜尋頁面大小設定為 25：

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_count=25
```

Chaining and Reverse Chaining(_has)

中的鏈結和反向鏈結 FHIR 提供更有效率且更精簡的方式，以取得互連的資料、減少對多個個別查詢的需求，並讓開發人員和使用者更方便地擷取資料。

如果任何層級的遞迴傳回超過 100 個結果，HealthLake 將傳回 4xx，以保護資料存放區免於超載並導致多個分頁。

Example – 鏈結 - 取得所有指向病患 DiagnosticReport，其中病患名稱為 Peter。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
DiagnosticReport?subject:Patient.name=peter
```

Example – 反向鏈結 - 取得病患資源，其中病患資源由至少一個觀察參考，其中觀察的程式碼為 1234，而觀察是指病患搜尋參數中的病患資源。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient?_has:Observation:patient:code=1234
```

支援的搜尋修改器

搜尋修飾詞會與字串型欄位搭配使用。中的所有搜尋修改器都 HealthLake 使用布林式邏輯。例如，您可以 `:contains` 指定指定較大的字串欄位應包含一個小字串，以便將其包含在搜尋結果中。

支援的搜尋修改器

搜尋修改器	Type
<code>: 遺漏</code>	除了 之外的所有參數 Composite
<code>: exact</code>	字串
<code>: 包含</code>	字串
<code>: not</code>	權杖
<code>: text</code>	權杖
<code>: 識別符</code>	參考資料

支援的搜尋比較器

您可以使用搜尋比較器來控制搜尋中相符項目的性質。您可以在搜尋數字、日期和數量欄位時使用比較器。下表列出 支援的搜尋比較器及其定義 HealthLake。

支援的搜尋比較器

搜尋比較器	描述
<code>eq</code>	資源中 參數的值等於提供的值。
<code>ne</code>	資源中 參數的值不等於提供的值。
<code>gt</code>	資源中 參數的值大於提供的值。
<code>lt</code>	資源中 參數的值小於提供的值。

搜尋比較器	描述
ge	資源中 參數的值大於或等於提供的值。
le	資源中 參數的值小於或等於提供的值。
sa	資源中 參數的值會在提供的值後開始。
eb	資源中 參數的值在提供的值之前結束。

不支援的搜尋參數 HealthLake

如需支援搜尋參數的完整清單，請參閱[FHIR搜尋參數登錄檔](#)。HealthLake 支援所有搜尋參數，資料表中列出的參數除外。

不支援的搜尋參數

套件組成	Location-near
套件識別符	Consent-source-reference
套件訊息	合約病患
套件類型	資源內容
套件時間戳記	資源查詢

使用POST範例搜尋

您可以透過提出POST請求來搜尋 HealthLake 資料存放區。您可以在 URI或 請求內文中提供查詢參數，但無法在單一請求中使用兩者。

本主題中的範例遵循該最佳實務。

Note

對於涉及個人身分識別資訊 (PII) 或受保護健康資訊 (PHI) 的查詢，建議使用POST請求。在POST請求中，PII或 PHI 會新增為請求內文的一部分，並在傳輸中加密。

在POST請求內文中使用 參數提出請求時，請使用 Content-Type: application/x-www-form-urlencoded 做為 標頭的一部分。

本主題提供如何使用下列資源類型POST來搜尋 的範例。

- 年齡：年齡不是 中定義的資源類型FHIR。相反地，年齡會擷取為病患資源類型的一部分。若要根據特定年齡或年齡範圍搜尋一組患者，請使用 [the section called “支援的搜尋比較器”](#)。如需詳細資訊，請參閱 FHIR 文件索引中的[資源類型：病患](#)。
- 條件：此資源類型會儲存與臨床概念相關的詳細資訊，例如診斷、情況、臨床條件和問題已上升到關注程度。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：條件](#)。會根據 中找到的文件 HealthLake 建立新的條件 DocumentReference。在提出POST請求時，預設會排除這些新增項目。若要包含它們，您必須在搜尋中為條件資源指定有效的識別符。
- DocumentReference：支援此資源類型 HealthLake。此資源類型支援參考任何類型的文件。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：DocumentReference](#) HealthLake 也提供 中文文件的整合自然語言處理 (NLP) DocumentReference。如需進一步了解，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。
- 位置：此資源類型包括偶發位置（用於醫療保健的地方，無需事先指定或授權）和專用、正式指定的位置。如需詳細資訊，請參閱 FHIR 文件索引中的[資源類型：位置](#)。
- 觀察：對病患、裝置或其他主體所做的測量和簡單聲明。會根據資源中找到的文件 HealthLake 建立新的觀察 DocumentReference 資源。若要進一步了解如何 HealthLake 建立新資源，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。在提出POST請求時，預設會排除這些新增項目。若要包含它們，您必須在搜尋中為觀察資源指定有效的識別符。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：觀察](#)。

每個索引標籤顯示如何搜尋指定資源類型的範例。它包含如何在請求內文中指定請求的範例。

Age

使用下列項目，對Patient資源類型提出 POST型搜尋請求。此搜尋使用eq搜尋比較器來搜尋 1997 年出生的個人。

您必須指定請求URL和請求內文。以下是請求 的範例URL。

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/_search
```

若要在搜尋中指定年份 1997，您可以將下列元素新增至請求內文。

```
birthdate=eq1997
```

JSON 回應

成功時，您會取得200HTTP回應代碼和類似的JSON回應。

Condition

使用下列項目對Condition資源類型提出POST請求。此搜尋會尋找 HealthLake 資料存放區中包含醫療碼 的位置72892002。

您必須指定請求URL和請求內文。以下是請求 的範例URL。

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Condition/_search
```

若要指定您要搜尋的醫療碼，請將此JSON元素新增至請求內文。

```
code=72892002
```

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，下列JSON回應已截斷。

```
{  
  "resourceType": "Bundle",  
  "type": "searchset",  
  "entry": [{  
    "resource": {  
      "resourceType": "Condition",  
      "id": "0063326c-6b42-4d13-af2f-1efe0a65f016",  
      "meta": {  
        "lastUpdated": "2022-08-23T00:22:49.681Z"  
      },  
      "clinicalStatus": {  
        "coding": [{  
          "system": "http://terminology.hl7.org/CodeSystem/condition-clinical",  
          "code": "resolved"  
        }]  
      },  
      "verificationStatus": {  
        "coding": [{  
          "system": "http://terminology.hl7.org/CodeSystem/condition-ver-status",
```

```
    "code": "confirmed"
  ]
},
"code": {
  "coding": [{
    "system": "http://snomed.info/sct",
    "code": "72892002",
    "display": "Normal pregnancy"
  }],
  "text": "Normal pregnancy"
},
"subject": {
  "reference": "Patient/5fc0070a-696a-4855-94a9-175f1c641a33"
},
"encounter": {
  "reference": "Encounter/44078ab9-7ac7-4731-9ac8-4b3ff21a7bdb"
},
"onsetDateTime": "2019-08-15T01:19:17-07:00",
"abatementDateTime": "2020-03-26T01:19:17-07:00",
"recordedDate": "2019-08-15T01:19:17-07:00"
},
"search": {
  "mode": "match"
}
},
{
  "resource": {
    "resourceType": "Condition",
    "id": "d00afdb2-1d2c-44fe-9f3b-033c0fe751a3",
    "meta": {
      "lastUpdated": "2022-08-23T00:20:47.100Z"
    },
    "clinicalStatus": {
      "coding": [{
        "system": "http://terminology.hl7.org/CodeSystem/condition-clinical",
        "code": "resolved"
      }]
    },
    "verificationStatus": {
      "coding": [{
        "system": "http://terminology.hl7.org/CodeSystem/condition-ver-status",
        "code": "confirmed"
      }]
    }
  },

```

```
{
  "code": {
    "coding": [{
      "system": "http://snomed.info/sct",
      "code": "72892002",
      "display": "Normal pregnancy"
    }],
    "text": "Normal pregnancy"
  },
  "subject": {
    "reference": "Patient/d0a5cd1e-8da7-41bd-9b2f-41eef45246e5"
  },
  "encounter": {
    "reference": "Encounter/73758e67-4aaf-4e80-982b-8821f0b6fdfb"
  },
  "onsetDateTime": "2019-06-13T20:37:40-07:00",
  "abatementDateTime": "2020-01-23T19:37:40-08:00",
  "recordedDate": "2019-06-13T20:37:40-07:00"
},
"search": {
  "mode": "match"
}
}
```

DocumentReference

若要查看在DocumentReference資源類型上提出POST請求時 HealthLake，整合自然語言處理 (NLP) 的結果，請格式化請求，如下所示。

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
DocumentReference/_search
```

若要指定您要參考的 DocumentReference 元素，請參閱 [搜尋參數](#)。您將在請求內文中將那些指定為 JSON。

```
_lastUpdated=1e2021-12-19&infer-icd10cm-entity-text-concept-score;=streptococcal|
0.6&infer-rxnorm-entity-text-concept-score=Amoxicillin|0.8
```

此查詢字串使用多個搜尋參數來搜尋用於產生整合醫療NLP結果的 Amazon Comprehend Medical API操作。

Location

使用下列項目對Location資源類型提出POST請求。此搜尋會尋找 HealthLake 資料存放區中包含城市名稱波士頓做為地址一部分的位置。

您必須指定請求URL和請求內文。以下是請求 的範例URL。

```
POST https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Location/_search
```

若要在搜尋中指定波士頓，請將下列元素新增至請求內文：

```
address=Boston
```

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，已截斷JSON回應。

```
{
  "resourceType": "Bundle",
  "type": "searchset",
  "entry": [{
    "resource": {
      "resourceType": "Location",
      "id": "0a6903c7-25c5-4ae4-8354-be88f9c5f2ee",
      "meta": {
        "lastUpdated": "2022-08-23T00:24:24.570Z"
      },
      "status": "active",
      "name": "BRIGHAM AND WOMEN'S HOSPITAL",
      "telecom": [{
        "system": "phone",
        "value": "6177325500"
      }],
      "address": {
        "line": [
          "75 FRANCIS STREET"
        ],
        "city": "BOSTON",
        "state": "MA",
        "postalCode": "02115",
        "country": "US"
      }
    },
  ]
}
```

```
"position": {
  "longitude": -71.020173,
  "latitude": 42.33196
},
"managingOrganization": {
  "reference": "Organization/27379046-608b-32f0-9df7-8c833cf5d11d",
  "display": "BRIGHAM AND WOMEN'S HOSPITAL"
}
},
"search": {
  "mode": "match"
}
},
{
  "resource": {
    "resourceType": "Location",
    "id": "ca5e7f65-4eb5-4bff-9a6f-07bc80acf8d0",
    "meta": {
      "lastUpdated": "2022-08-23T00:20:47.100Z"
    },
    "status": "active",
    "name": "BETH ISRAEL DEACONESS MEDICAL CENTER",
    "telecom": [{
      "system": "phone",
      "value": "6176677000"
    }],
    "address": {
      "line": [
        "330 BROOKLINE AVENUE"
      ],
      "city": "BOSTON",
      "state": "MA",
      "postalCode": "02215",
      "country": "US"
    },
    "position": {
      "longitude": -71.020173,
      "latitude": 42.33196
    },
    "managingOrganization": {
      "reference": "Organization/cb6a50e0-af76-3758-99ad-3200ede03fff",
      "display": "BETH ISRAEL DEACONESS MEDICAL CENTER"
    }
  }
}
```

```
},
"search": {
  "mode": "match"
}
]
}
```

Observation

使用下列項目對Observation資源類型提出 POST型搜尋請求。此搜尋使用value-concept搜尋參數來尋找醫療碼 266919005。此狀態表示 Never smoker。

您必須指定請求URL和請求內文。以下是請求 的範例URL。

POST [https://healthlake.**your-region**.amazonaws.com/datastore/**your-datastore-id**/r4/Observation/_search](https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Observation/_search)

若要指定狀態，請在 Never smoker 內文value-concept=266919005中設定 JSON。

value-concept=266919005

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，下列JSON回應已截斷。

```
{
  "resourceType": "Bundle",
  "type": "searchset",
  "link": [{
    "relation": "next",
    "url": "https://healthlake.us-west-2.amazonaws.com/
datastore/3651c6d3c1e81e785adba06b710b52a9/r4/0bservation?value-
concept=266919005&=AAMA-
EFRSURBSG1pcGIyN250ZG9WRXVnTTF0dmtxQk9Bb3Y0YjhhVcVdUMGV0eVozNmdjQU9nRjRNUUtscjhCZ1NMUG84VGNgN
}],
  "entry": [{
    "resource": {
      "resourceType": "Observation",
      "id": "000038e0-71c6-4cc0-9c6c-50c8b1c53309",
      "meta": {
        "lastUpdated": "2022-11-03T01:02:38.981Z"
      }
    }
  ]
}
```

```
"status": "final",
"category": [{
  "coding": [{
    "system": "http://terminology.hl7.org/CodeSystem/observation-category",
    "code": "survey",
    "display": "survey"
  }]
}],
"code": {
  "coding": [{
    "system": "http://loinc.org",
    "code": "72166-2",
    "display": "Tobacco smoking status NHIS"
  }],
  "text": "Tobacco smoking status NHIS"
},
"subject": {
  "reference": "Patient/598c9d7a-0494-448e-a81e-d50e3606e8db"
},
"encounter": {
  "reference": "Encounter/86bdee4a-2aa9-474a-b43f-6237cd68e512"
},
"effectiveDateTime": "2019-12-11T19:44:57-08:00",
"issued": "2019-12-11T19:44:57.438-08:00",
"valueCodeableConcept": {
  "coding": [{
    "system": "http://snomed.info/sct",
    "code": "266919005",
    "display": "Never smoker"
  }],
  "text": "Never smoker"
}
},
"search": {
  "mode": "match"
}
},
{
  "resource": {
    "resourceType": "Observation",
    "id": "0c2f6260-e671-4cfd-ac3d-e75f073fa3cd",
    "meta": {
      "lastUpdated": "2022-11-03T01:05:21.488Z"
```

```
    },
    "status": "final",
    "category": [{
      "coding": [{
        "system": "http://terminology.hl7.org/CodeSystem/observation-category",
        "code": "survey",
        "display": "survey"
      }]
    }],
    "code": {
      "coding": [{
        "system": "http://loinc.org",
        "code": "72166-2",
        "display": "Tobacco smoking status NHIS"
      }],
      "text": "Tobacco smoking status NHIS"
    },
    "subject": {
      "reference": "Patient/89d9a9b7-9720-4881-a2ab-d7907544b26f"
    },
    "encounter": {
      "reference": "Encounter/8ebba7b0-fdfc-4ec1-a9aa-907cccf60925"
    },
    "effectiveDateTime": "2018-11-17T03:59:36-08:00",
    "issued": "2018-11-17T03:59:36.550-08:00",
    "valueCodeableConcept": {
      "coding": [{
        "system": "http://snomed.info/sct",
        "code": "266919005",
        "display": "Never smoker"
      }],
      "text": "Never smoker"
    }
  },
  "search": {
    "mode": "match"
  }
}
```

使用GET範例搜尋

您可以透過提出GET請求來搜尋 HealthLake 資料存放區。HealthLake 僅支援提供查詢參數作為 的一部分URI，而非請求內文的一部分。

Note

對於涉及個人身分識別資訊 (PII) 或受保護健康資訊 (PHI) 的查詢，建議使用POST請求。在POST請求中，PII或PHI會新增為請求內文的一部分，並在傳輸中加密。

主題提供如何使用 GET中支援的資源類型進行搜尋的範例 HealthLake。

- 年齡：年齡不是 中定義的資源類型FHIR。相反地，年齡會擷取為病患資源類型的一部分。若要根據特定年齡或年齡範圍搜尋一組患者，您需要使用 [the section called “支援的搜尋比較器”](#)。如需詳細資訊，請參閱 FHIR 文件索引中的[資源類型：病患](#)。
- 條件：此資源類型會儲存與臨床概念相關的詳細資訊，例如診斷、情況、臨床條件和問題已上升到關注程度。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：條件](#)。會根據 中的文件 HealthLake 建立新的條件 DocumentReference。在提出POST請求時，預設會排除這些新增項目。若要包含它們，您必須在搜尋中為條件資源指定有效的識別符。
- DocumentReference：支援此資源類型 HealthLake。此資源類型支援參考任何類型的文件。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：DocumentReference](#)。HealthLake 也提供 中文文件的整合自然語言處理 (NLP) DocumentReference。如需進一步了解，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。
- 位置：此資源類型包括偶發位置（用於醫療保健的地方，無需事先指定或授權）和專用、正式指定的位置。如需詳細資訊，請參閱 FHIR 文件索引中的[資源類型：位置](#)。
- 觀察：對病患、裝置或其他主體所做的測量和簡單聲明。會根據資源中找到的文件 HealthLake 建立新的觀察 DocumentReference 資源。若要進一步了解如何 HealthLake 建立新資源，請參閱 [根據 中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。在提出POST請求時，預設會排除這些新增項目。若要包含它們，您必須在搜尋中為觀察資源指定有效的識別符。若要進一步了解，請參閱 FHIR 文件索引中的[資源類型：觀察](#)。

每個索引標籤都會顯示如何搜尋指定資源類型的範例。其中包含如何在 中指定請求的範例URI，以及相關的JSON回應。

Age

使用下列項目，對Patient資源類型提出GET以 為基礎的搜尋請求。此搜尋使用eq搜尋比較器來搜尋 1997 年出生的個人。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4//
Patient?birthdate=eq1997
```

JSON 回應

成功時，您會收到200HTTP回應代碼。

Condition

使用下列項目對Condition資源類型提出GET請求。此搜尋會尋找 HealthLake 資料存放區中包含醫療碼 的位置72892002。

您必須指定請求URL和請求內文。以下是請求 的範例URL。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
Condition?code=72892002
```

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，下列JSON回應已截斷。

```
{
  "resourceType": "Bundle",
  "type": "searchset",
  "entry": [{
    "resource": {
      "resourceType": "Condition",
      "id": "0063326c-6b42-4d13-af2f-1efe0a65f016",
      "meta": {
        "lastUpdated": "2022-08-23T00:22:49.681Z"
      },
      "clinicalStatus": {
        "coding": [{
          "system": "http://terminology.hl7.org/CodeSystem/condition-clinical",
          "code": "resolved"
        }]
      },
      "verificationStatus": {
        "coding": [{
```

```
    "system": "http://terminology.hl7.org/CodeSystem/condition-ver-status",
    "code": "confirmed"
  ]],
},
"code": {
  "coding": [{
    "system": "http://snomed.info/sct",
    "code": "72892002",
    "display": "Normal pregnancy"
  }],
  "text": "Normal pregnancy"
},
"subject": {
  "reference": "Patient/5fc0070a-696a-4855-94a9-175f1c641a33"
},
"encounter": {
  "reference": "Encounter/44078ab9-7ac7-4731-9ac8-4b3ff21a7bdb"
},
"onsetDateTime": "2019-08-15T01:19:17-07:00",
"abatementDateTime": "2020-03-26T01:19:17-07:00",
"recordedDate": "2019-08-15T01:19:17-07:00"
},
"search": {
  "mode": "match"
}
},
{
  "resource": {
    "resourceType": "Condition",
    "id": "d00afdb2-1d2c-44fe-9f3b-033c0fe751a3",
    "meta": {
      "lastUpdated": "2022-08-23T00:20:47.100Z"
    },
    "clinicalStatus": {
      "coding": [{
        "system": "http://terminology.hl7.org/CodeSystem/condition-clinical",
        "code": "resolved"
      }]
    },
    "verificationStatus": {
      "coding": [{
        "system": "http://terminology.hl7.org/CodeSystem/condition-ver-status",
        "code": "confirmed"
      }]
    }
  }
}
```

```

    },
    "code": {
      "coding": [{
        "system": "http://snomed.info/sct",
        "code": "72892002",
        "display": "Normal pregnancy"
      }],
      "text": "Normal pregnancy"
    },
    "subject": {
      "reference": "Patient/d0a5cd1e-8da7-41bd-9b2f-41eef45246e5"
    },
    "encounter": {
      "reference": "Encounter/73758e67-4aaf-4e80-982b-8821f0b6fdfb"
    },
    "onsetDateTime": "2019-06-13T20:37:40-07:00",
    "abatementDateTime": "2020-01-23T19:37:40-08:00",
    "recordedDate": "2019-06-13T20:37:40-07:00"
  },
  "search": {
    "mode": "match"
  }
}
]
}

```

DocumentationReference

此範例示範如何為診斷為鏈球菌且也獲開立 amoxicillin 的患者，在DocumentReference資源類型上建立搜尋請求。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/DocumentReference?_lastUpdated=1e2021-12-19&infer-icd10cm-entity-text-concept-score;=streptococcal|0.6&infer-rxnorm-entity-text-concept-score=Amoxicillin|0.8
```

成功後，您會收到下列JSON回應。

```

{
  "resourceType": "Bundle",
  "type": "searchset",
  "entry": [
    {
      "resource": {

```

```

    "resourceType": "DocumentReference",
    "id": "985c3e94-4219-4c79-97a1-c94694525e24",
    "meta": {
      "lastUpdated": "2020-11-23T06:09:10.719Z"
    },
    "extension": [
      {
        "url": "http://healthlake.amazonaws.com/aws-cm/",
        "extension": [
          {
            "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/",
            "extension": [
              {
                "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/raw-
response",
                "valueString": "{Entities: [{Id: 0,Text: otitis media,Category:
MEDICAL_CONDITION,Type: DX_NAME,Score: 0.9815994,BeginOffset: 151,EndOffset:
163,Attributes: [],Traits: [{Name: DIAGNOSIS,Score: 0.95042425}],ICD10CMConcepts:
[{Description: Otitis media, unspecified, unspecified ear,Code: H66.90,Score:
0.7176407}, {Description: Otitis media, unspecified,Code: H66.9,Score:
0.6930445}, {Description: Otitis media, unspecified, left ear,Code: H66.92,Score:
0.688161}, {Description: Otitis media, unspecified, bilateral,Code: H66.93,Score:
0.6748094}, {Description: Otitis media, unspecified, right ear,Code:
H66.91,Score: 0.6645618}]], {Id: 1,Text: streptococcal sore throat,Category:
MEDICAL_CONDITION,Type: DX_NAME,Score: 0.92208487,BeginOffset: 461,EndOffset:
486,Attributes: [],Traits: [],ICD10CMConcepts: [{Description: Streptococcal
pharyngitis,Code: J02.0,Score: 0.55638546}, {Description: Acute streptococcal
tonsillitis, unspecified,Code: J03.00,Score: 0.53159785}, {Description:
Streptococcal sepsis, unspecified,Code: A40.9,Score: 0.51865804}, {Description:
Acute pharyngitis, unspecified,Code: J02.9,Score: 0.45085955}, {Description:
Streptococcal infection, unspecified site,Code: A49.1,Score: 0.41550553}]],
{Id: 3,Text: disorder,Category: MEDICAL_CONDITION,Type: DX_NAME,Score:
0.9191257,BeginOffset: 488,EndOffset: 496,Attributes: [],Traits: [{Name:
DIAGNOSIS,Score: 0.93372077}],ICD10CMConcepts: [{Description: Parkinson's
disease,Code: G20,Score: 0.6959145}, {Description: Illness, unspecified,Code:
R69,Score: 0.68428487}, {Description: Disorder of bone, unspecified,Code:
M89.9,Score: 0.6542605}, {Description: Unspecified mental disorder due to known
physiological condition,Code: F09,Score: 0.6240179}, {Description: Mental disorder,
not otherwise specified,Code: F99,Score: 0.61046}]]],ModelVersion: 0.1.0}"
              },
            {
              "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
model-version",
              "valueString": "0.1.0"
            }
          ]
        }
      ]
    ]
  }
}

```

```

    },
    {
      "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-
cm-icd10-entity",
      "extension": [
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-id",
          "valueInteger": 0
        },
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-text",
          "valueString": "otitis media"
        },
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-begin-offset",
          "valueInteger": 151
        },
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-end-offset",
          "valueInteger": 163
        },
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-score",
          "valueDecimal": 0.9815994
        },
        {
          "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/
aws-cm-icd10-entity-ConceptList",
          "extension": [
            {
              "url": "http://healthlake.amazonaws.com/aws-cm/infer-
icd10/aws-cm-icd10-entity-Concept",
              "extension": [
                {
                  "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Code",
                  "valueString": "H66.90"
                },
                {

```

```

        "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Description",
        "valueString": "Otitis media, unspecified,
unspecified ear"
    },
    {
        "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Score",
        "valueDecimal": 0.7176407
    }
]
},
{
    "url": "http://healthlake.amazonaws.com/aws-cm/infer-
icd10/aws-cm-icd10-entity-Concept",
    "extension": [
        {
            "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Code",
            "valueString": "H66.9"
        },
        {
            "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Description",
            "valueString": "Otitis media, unspecified"
        },
        {
            "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Score",
            "valueDecimal": 0.6930445
        }
    ]
},
{
    "url": "http://healthlake.amazonaws.com/aws-cm/infer-
icd10/aws-cm-icd10-entity-Concept",
    "extension": [
        {
            "url": "http://healthlake.amazonaws.com/aws-cm/
infer-icd10/aws-cm-icd10-entity-Concept-Code",
            "valueString": "H66.92"
        }
    ]
}
}

```

Location

使用下列項目對Location資源類型提出GET請求。此搜尋會尋找 HealthLake 資料存放區中包含城市名稱波士頓做為地址一部分的位置。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4//  
Location?address=boston
```

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，已截斷JSON回應。

```
{  
  "resourceType": "Bundle",  
  "type": "searchset",  
  "entry": [  
    {  
      "resource": {  
        "resourceType": "Location",  
        "id": "0a6903c7-25c5-4ae4-8354-be88f9c5f2ee",  
        "meta": {  
          "lastUpdated": "2022-08-23T00:24:24.570Z"  
        },  
        "status": "active",  
        "name": "BRIGHAM AND WOMEN'S HOSPITAL",  
        "telecom": [  
          {  
            "system": "phone",  
            "value": "6177325500"  
          }  
        ],  
        "address": {  
          "line": [  
            "75 FRANCIS STREET"  
          ],  
          "city": "BOSTON",  
          "state": "MA",  
          "postalCode": "02115",  
          "country": "US"  
        },  
        "position": {
```

```

        "longitude": -71.020173,
        "latitude": 42.33196
    },
    "managingOrganization": {
        "reference":
"Organization/27379046-608b-32f0-9df7-8c833cf5d11d",
        "display": "BRIGHAM AND WOMEN'S HOSPITAL"
    }
},
"search": {
    "mode": "match"
}
},
{
    "resource": {
        "resourceType": "Location",
        "id": "3cc3ad99-e0ff-48b4-b277-052abfc41058",
        "meta": {
            "lastUpdated": "2022-08-23T00:19:37.029Z"
        },
        "status": "active",
        "name": "NEW ENGLAND BAPTIST HOSPITAL",
        "telecom": [
            {
                "system": "phone",
                "value": "6177545800"
            }
        ],
        "address": {
            "line": [
                "125 PARKER HILL AVENUE"
            ],
            "city": "BOSTON",
            "state": "MA",
            "postalCode": "02120",
            "country": "US"
        },
        "position": {
            "longitude": -71.020173,
            "latitude": 42.33196
        },
        "managingOrganization": {
            "reference": "Organization/9a7149fa-49fc-3c87-b935-
d29c55808717",

```

```

        "display": "NEW ENGLAND BAPTIST HOSPITAL"
      }
    },
    "search": {
      "mode": "match"
    }
  },
  {
    "resource": {
      "resourceType": "Location",
      "id": "3f956715-3890-4235-85be-3fba5e3488ee",
      "meta": {
        "lastUpdated": "2022-08-23T00:23:38.981Z"
      },
      "status": "active",
      "name": "MASSACHUSETTS GENERAL HOSPITAL",
      "telecom": [
        {
          "system": "phone",
          "value": "6177262000"
        }
      ],
      "address": {
        "line": [
          "55 FRUIT STREET"
        ],
        "city": "BOSTON",
        "state": "MA",
        "postalCode": "02114",
        "country": "US"
      },
      "position": {
        "longitude": -71.020173,
        "latitude": 42.33196
      },
      "managingOrganization": {
        "reference": "Organization/d78e84ec-30aa-3bba-a33a-f29a3a454662",
        "display": "MASSACHUSETTS GENERAL HOSPITAL"
      }
    },
    "search": {
      "mode": "match"
    }
  }
}

```

```
    },
    {
      "resource": {
        "resourceType": "Location",
        "id": "6cc07b51-7287-443c-b772-c864f7831e13",
        "meta": {
          "lastUpdated": "2022-08-23T00:21:11.045Z"
        },
        "status": "active",
        "name": "TUFTS MEDICAL CENTER",
        "telecom": [
          {
            "system": "phone",
            "value": "6176365000"
          }
        ],
        "address": {
          "line": [
            "800 WASHINGTON STREET"
          ],
          "city": "BOSTON",
          "state": "MA",
          "postalCode": "02111",
          "country": "US"
        },
        "position": {
          "longitude": -71.020173,
          "latitude": 42.33196
        },
        "managingOrganization": {
          "reference": "Organization/b7175ab4-bde5-3848-891b-579bccb77c7c",
          "display": "TUFTS MEDICAL CENTER"
        }
      },
      "search": {
        "mode": "match"
      }
    },
    {
      "resource": {
        "resourceType": "Location",
        "id": "8101300f-f685-49e7-b428-43b7855c39ee",
        "meta": {
```

```

        "lastUpdated": "2022-08-23T00:22:06.474Z"
      },
      "status": "active",
      "name": "BOSTON CHILDREN'S HOSPITAL",
      "telecom": [
        {
          "system": "phone",
          "value": "6177356000"
        }
      ],
      "address": {
        "line": [
          "300 LONGWOOD AVENUE"
        ],
        "city": "BOSTON",
        "state": "MA",
        "postalCode": "02115",
        "country": "US"
      },
      "position": {
        "longitude": -71.020173,
        "latitude": 42.33196
      },
      "managingOrganization": {
        "reference": "Organization/d7b11827-25f2-350b-bcd8-939fc59851b0",
        "display": "BOSTON CHILDREN'S HOSPITAL"
      }
    },
    "search": {
      "mode": "match"
    }
  },
  {
    "resource": {
      "resourceType": "Location",
      "id": "8b7641d3-6997-48bb-bd60-23e35dfaae9d",
      "meta": {
        "lastUpdated": "2022-08-23T00:20:47.099Z"
      },
      "status": "active",
      "name": "BRIGHAM AND WOMEN'S FAULKNER HOSPITAL",
      "telecom": [
        {

```

```

        "system": "phone",
        "value": "6179837000"
    }
],
"address": {
    "line": [
        "1153 CENTRE STREET"
    ],
    "city": "BOSTON",
    "state": "MA",
    "postalCode": "02130",
    "country": "US"
},
"position": {
    "longitude": -71.020173,
    "latitude": 42.33196
},
"managingOrganization": {
    "reference": "Organization/d733d4a9-080d-3593-
b910-2366e652b7ea",
    "display": "BRIGHAM AND WOMEN'S FAULKNER HOSPITAL"
}
},
"search": {
    "mode": "match"
}
},
{
    "resource": {
        "resourceType": "Location",
        "id": "998ef80b-7b58-4dc3-99ac-c440ec9e282d",
        "meta": {
            "lastUpdated": "2022-08-23T00:21:11.046Z"
        },
        "status": "active",
        "name": "BRIGHAM AND WOMEN'S FAULKNER HOSPITAL",
        "telecom": [
            {
                "system": "phone",
                "value": "6179837000"
            }
        ],
        "address": {
            "line": [

```

```
        "1153 CENTRE STREET"
      ],
      "city": "BOSTON",
      "state": "MA",
      "postalCode": "02130",
      "country": "US"
    },
    "position": {
      "longitude": -71.020173,
      "latitude": 42.33196
    },
    "managingOrganization": {
      "reference": "Organization/d733d4a9-080d-3593-
b910-2366e652b7ea",
      "display": "BRIGHAM AND WOMEN'S FAULKNER HOSPITAL"
    }
  },
  "search": {
    "mode": "match"
  }
},
{
  "resource": {
    "resourceType": "Location",
    "id": "c454bed3-7013-4376-81cf-4f49342f1402",
    "meta": {
      "lastUpdated": "2022-08-23T00:24:24.573Z"
    },
    "status": "active",
    "name": "MASSACHUSETTS GENERAL HOSPITAL",
    "telecom": [
      {
        "system": "phone",
        "value": "6177262000"
      }
    ],
    "address": {
      "line": [
        "55 FRUIT STREET"
      ],
      "city": "BOSTON",
      "state": "MA",
      "postalCode": "02114",
      "country": "US"
    }
  }
}
```

```

    },
    "position": {
      "longitude": -71.020173,
      "latitude": 42.33196
    },
    "managingOrganization": {
      "reference": "Organization/d78e84ec-30aa-3bba-a33a-f29a3a454662",
      "display": "MASSACHUSETTS GENERAL HOSPITAL"
    }
  },
  "search": {
    "mode": "match"
  }
},
{
  "resource": {
    "resourceType": "Location",
    "id": "ca5e7f65-4eb5-4bff-9a6f-07bc80acf8d0",
    "meta": {
      "lastUpdated": "2022-08-23T00:20:47.100Z"
    },
    "status": "active",
    "name": "BETH ISRAEL DEACONESS MEDICAL CENTER",
    "telecom": [
      {
        "system": "phone",
        "value": "6176677000"
      }
    ],
    "address": {
      "line": [
        "330 BROOKLINE AVENUE"
      ],
      "city": "BOSTON",
      "state": "MA",
      "postalCode": "02215",
      "country": "US"
    },
    "position": {
      "longitude": -71.020173,
      "latitude": 42.33196
    },
    "managingOrganization": {

```

```

    "reference": "0rganization/cb6a50e0-
af76-3758-99ad-3200ede03fff",
    "display": "BETH ISRAEL DEACONESS MEDICAL CENTER"
  }
},
"search": {
  "mode": "match"
}
}
]
}

```

Observation

使用下列項目，對Observation資源類型提出GET以 為基礎的搜尋請求。此搜尋使用value-concept搜尋參數來尋找醫療碼 266919005。此狀態表示 Never smoker。

您必須指定請求URL和查詢字串。以下是請求的範例URL。

POST <https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/Observation?value-concept=266919005>

若要指定狀態，Never smoker請將 value-concept=266919005設定為查詢字串。

JSON 回應

成功時，您會收到200HTTP回應代碼。為了清楚起見，下列JSON回應已截斷。

```
{
  "resourceType": "Bundle",
  "type": "searchset",
  "link": [{
    "relation": "next",
    "url": "https://healthlake.us-west-2.amazonaws.com/
datastore/3651c6d3c1e81e785adba06b710b52a9/r4/0bservation?value-
concept=266919005&=AAMA-
EFRSURBSGLpcGIyN250ZG9WRXVnTTF0dmtxQk9Bb3Y0YjhVcVdUMGV0eVozNmdjQU9nRjRNUUtscljCZ1NMUG84VGNqM
  }],
  "entry": [{
    "resource": {
      "resourceType": "Observation",
      "id": "000038e0-71c6-4cc0-9c6c-50c8b1c53309",
      "meta": {
```

```
    "lastUpdated": "2022-11-03T01:02:38.981Z"
  },
  "status": "final",
  "category": [{
    "coding": [{
      "system": "http://terminology.hl7.org/CodeSystem/observation-category",
      "code": "survey",
      "display": "survey"
    }]
  }],
  "code": {
    "coding": [{
      "system": "http://loinc.org",
      "code": "72166-2",
      "display": "Tobacco smoking status NHIS"
    }],
    "text": "Tobacco smoking status NHIS"
  },
  "subject": {
    "reference": "Patient/598c9d7a-0494-448e-a81e-d50e3606e8db"
  },
  "encounter": {
    "reference": "Encounter/86bdee4a-2aa9-474a-b43f-6237cd68e512"
  },
  "effectiveDateTime": "2019-12-11T19:44:57-08:00",
  "issued": "2019-12-11T19:44:57.438-08:00",
  "valueCodeableConcept": {
    "coding": [{
      "system": "http://snomed.info/sct",
      "code": "266919005",
      "display": "Never smoker"
    }],
    "text": "Never smoker"
  }
},
"search": {
  "mode": "match"
}
},
{
  "resource": {
    "resourceType": "Observation",
    "id": "0c2f6260-e671-4cfd-ac3d-e75f073fa3cd",
```

```
{
  "meta": {
    "lastUpdated": "2022-11-03T01:05:21.488Z"
  },
  "status": "final",
  "category": [{
    "coding": [{
      "system": "http://terminology.hl7.org/CodeSystem/observation-category",
      "code": "survey",
      "display": "survey"
    }]
  }],
  "code": {
    "coding": [{
      "system": "http://loinc.org",
      "code": "72166-2",
      "display": "Tobacco smoking status NHIS"
    }],
    "text": "Tobacco smoking status NHIS"
  },
  "subject": {
    "reference": "Patient/89d9a9b7-9720-4881-a2ab-d7907544b26f"
  },
  "encounter": {
    "reference": "Encounter/8ebba7b0-fdfc-4ec1-a9aa-907cccf60925"
  },
  "effectiveDateTime": "2018-11-17T03:59:36-08:00",
  "issued": "2018-11-17T03:59:36.550-08:00",
  "valueCodeableConcept": {
    "coding": [{
      "system": "http://snomed.info/sct",
      "code": "266919005",
      "display": "Never smoker"
    }],
    "text": "Never smoker"
  }
},
"search": {
  "mode": "match"
}
}
```

讀取FHIR資源歷史記錄

FHIR history 互動會擷取 HealthLake 資料存放區中特定FHIR資源的歷史記錄。使用此互動，您可以判斷FHIR資源的內容如何隨著時間而變更。在與稽核日誌協調時，查看修改前後的資源狀態也很有用。

Note

FHIR 根據預設，資源history會在 10/25/2024 之後建立的所有 HealthLake 資料存放區中啟用。如果您的資料存放區在此日期之前建立，您可以提交支援票證以啟用FHIRhistory互動。使用 建立案例[AWS Support Center Console](#)。若要建立案例，請登入您的 AWS 帳戶，然後選擇建立案例。

使用 HTTP GET命令執行history互動。FHIR 互動 create、update和 delete會產生要儲存之資源的歷史版本。HealthLake 支援FHIRhistory互動的下列搜尋參數。

HealthLake 支援FHIR**history**的互動搜尋參數

搜尋參數	描述
<code>_count : integer</code>	頁面上搜尋結果的數量上限。伺服器將傳回請求的數目，或資料存放區預設允許的搜尋結果數量上限，以較低者為準。
<code>_since : instant</code>	僅包含指定即時時或之後建立的資源版本。
<code>_at : date(Time)</code>	僅包含日期時間值中指定期間內某個時間點的目前資源版本。如需詳細資訊，請參閱 HL7 FHIR RESTful API 文件 date 中的。

下列範例會傳回 中FHIRPatient資源每頁 100 個歷史搜尋結果 HealthLake。若要檢視整個URL路徑，請捲動至複製按鈕。的格式URL為：

```
GET https://healthlake.region.amazonaws.com/datastore/datastore-id/r4/Patient/id/  
_history?_count=100
```

歷史記錄互動的傳回內容包含在FHIR資源 中[Bundle](#)，類型設定為 `history`。它包含指定的版本歷史記錄，最後以最舊版本排序，並包含已刪除的資源。如需`history`互動的其他資訊，請參閱 HL7 FHIR RESTful API 文件[history](#)中的。

Note

您可以選擇退出`history`特定FHIR資源類型。若要選擇退出，請使用 建立案例[AWS Support Center Console](#)。若要建立案例，請登入您的 AWS 帳戶，然後選擇建立案例。

讀取版本特定的FHIR資源歷史記錄

FHIR `vread` 互動會針對 HealthLake 資料存放區中的資源執行版本特定的讀取。使用此互動，您可以檢視FHIR資源的內容，如同過去的特定時間一樣。

HealthLake 宣告它支援每個支援資源[CapabilityStatement.rest.resource.versioning](#)的版本控制。HealthLake 所有資料存放區在所有資源上都包含 `Resource.meta.versionId(vid)`。

啟用FHIR`history`互動時（預設為在 10/25/2024 之後建立的資料存放區，或應請求為較舊的資料存放區），`Bundle`回應會包含 `vid`做為 的一部分[location](#)。在下列範例中，`vid`會顯示為數字 1。若要檢視完整範例，請參閱範例 [Bundle/bundle-response \(JSON\)](#)。

```
"response" : {
  "status" : "201 Created",
  "location" : "Patient/12423/_history/1",
  ...}
```

使用 HTTP `GET`命令執行`vread`互動。下列`vread`互動會傳回單一執行個體，其中包含為 所指定版本 FHIR `Patient`之資源中繼資料所指定的內容`vid`。若要在下列範例中檢視整個URL路徑，請捲動至複製按鈕。的格式URL為：

```
GET https://healthlake.region.amazonaws.com/datastore/datastore-id/r4/Patient/id/_history/vid
```

Note

如果您在讀取FHIR資源`vread`時不使用 `history`互動，HealthLake 一律會傳回資源中繼資料的最新版本。

如需 `vread` 互動的其他資訊，請參閱 HL7 FHIR 靜態 API 文件中 [vread](#) 的。

使用病患 \$ 所有 FHIR REST API 操作取得病患資料

病患 \$ 每項操作都會用來查詢 FHIR 病患資源，以及與該病患相關的任何其他資源。此操作可用來提供病患存取其整個記錄的權限，或讓提供者執行與病患相關的大量資料下載。HealthLake 支援特定病患 ID 的 \$ 所有項目。

Note

2024 年 2 月 27 日之後建立的資料存放區目前支援病患 \$ 所有操作。

取得與病患相關的所有資源

病患 \$ 每項操作是可叫用 REST API 的操作，如以下範例所示。

GET Request

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/patient-id/$everything
```

Note

回應中的資源會依資源類型和資源 ID 排序。
回應一律會填入 `Bundle.total`。

病患 \$ 所有參數

HealthLake 支援下列查詢參數

參數	詳細資訊
入門	取得指定開始日期之後的所有病患資料。
end	在指定的結束日期之前取得所有病患資料。

參數	詳細資訊
since	取得指定日期後更新的所有病患資料。
_type	取得特定資源類型的患者資料。
_count	取得病患資料並指定頁面大小。

Example - 取得指定開始日期之後的所有病患資料

病患 \$所有項目都可以使用start篩選條件，只查詢特定日期之後的資料。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/patient-id/$everything?start=2024-03-15T00:00:00.000Z
```

Example - 在指定的結束日期之前取得所有病患資料

病患 \$所有項目都可以使用end篩選條件，只查詢特定日期之前的資料。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/patient-id/$everything?end=2024-03-15T00:00:00.000Z
```

Example - 在指定日期後更新所有病患資料

病患 \$所有項目都可以使用since篩選條件，只查詢特定日期之後更新的資料。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/patient-id/$everything?since=2024-03-15T00:00:00.000Z
```

Example - 取得特定資源類型的患者資料

病患 \$所有項目都可以使用_type篩選條件來指定要包含在回應中的特定資源類型。您可以在逗號分隔清單中指定多種資源類型。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/patient-id/$everything?_type=Observation,Condition
```

Example - 取得病患資料並指定頁面大小

病患 \$所有項目都可以使用 `_count` 來設定頁面大小。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/
Patient/patient-id/$everything?_count=15
```

病患 \$所有項目 **start** 和 **end** 屬性

HealthLake 支援啟動和結束查詢參數的下列資源屬性。

資源	資源元素
帳戶	Account.servicePeriod.start
AdverseEvent	AdverseEvent.date
AllergyIntolerance	AllergyIntolerance.recordedDate
預約	Appointment.start
AppointmentResponse	AppointmentResponse.start
AuditEvent	AuditEvent.period.start
基本	Basic.created
BodyStructure	NO_DATE
CarePlan	CarePlan.period.start
CareTeam	CareTeam.period.start
ChargeItem	ChargeItem.occurrenceDateTime , ChargeItem.occurrencePeriod.start , ChargeItem.occurrenceTiming.event

資源	資源元素
取得	Claim.billablePeriod.start
ClaimResponse	ClaimResponse.created
ClinicalImpression	ClinicalImpression.date
Communication	Communication.sent
CommunicationRequest	CommunicationRequest.occurrenceDateTime , CommunicationRequest.occurrencePeriod.start
合成	Composition.date
條件	條件。recordedDate
同意	同意。dateTime
涵蓋範圍	Coverage.period.start
CoverageEligibilityRequest	CoverageEligibilityRequest.created
CoverageEligibilityResponse	CoverageEligibilityResponse.created
DetectedIssue	DetectedIssue.已識別
DeviceRequest	DeviceRequest.authoredOn

資源	資源元素
DeviceUse Statement	DeviceUseStatement.recordedOn
DiagnosticReport	DiagnosticReport.effective
DocumentManifest	DocumentManifest.created
DocumentReference	DocumentReference.context.period.start
遇到	Encounter.period.start
EnrollmentRequest	EnrollmentRequest.created
EpisodeOf Care	EpisodeOfCare.period.start
ExplanationOfBenefit	ExplanationOfBenefit.billablePeriod.start
FamilyMemberHistory	NO_DATE
旗標	Flag.period.start
目標	目標。statusDate
群組	NO_DATE
ImagingStudy	ImagingStudy.started
預防接種	Immunization.recorded

資源	資源元素
ImmunizationEvaluation	ImmunizationEvaluation.date
ImmunizationRecommendation	ImmunizationRecommendation.date
發票	Invoice.date
清單	List.date
MeasureReport	MeasureReport.period.start
媒體	媒體。發行
MedicationAdministration	MedicationAdministration.effective
MedicationDispense	MedicationDispense.whenPrepared
MedicationRequest	MedicationRequest.authoredOn
MedicationStatement	MedicationStatement.dateAsserted
MolecularSequence	NO_DATE
NutritionOrder	NutritionOrder.dateTime
觀察	Observation.effective

資源	資源元素
病患	NO_DATE
個人	NO_DATE
程序	Procedure.performed
證明	Provenance.occurredPeriod.start、Provenance。occurredDateTime
QuestionnaireResponse	QuestionnaireResponse.authored
RelatedPerson	NO_DATE
RequestGroup	RequestGroup.authoredOn
ResearchSubject	ResearchSubject.period
RiskAssessment	RiskAssessment.occurrenceDateTime , RiskAssessment.occurrencePeriod.start
排程	排程。planningHorizon
ServiceRequest	ServiceRequest.authoredOn
樣本	樣本。receivedTime
SupplyDelivery	SupplyDelivery.occurrenceDateTime , SupplyDelivery.occurrencePeriod.start , SupplyDelivery.occurrenceTiming.event
SupplyRequest	SupplyRequest.authoredOn

資源	資源元素
VisionPrescription	VisionPrescription.dateWritten

使用 \$export 從 HealthLake 資料存放區匯出資料

使用 FHIR REST API 指定 \$export 做為請求的一部分來提出匯出 POST 請求，並在請求的內文中包含請求參數。根據 FHIR 規格，FHIR 伺服器必須支援 GET 請求，並且可以支援 POST 請求。為了支援其他參數，需要內文才能啟動匯出，因此 HealthLake 支援 POST 請求。

Important

HealthLake 在 2023 年 6 月 1 日之前建立的資料存放區僅支援全系統匯出的 FHIR REST API 以基礎的匯出任務請求。

HealthLake 在 2023 年 6 月 1 日之前建立的資料存放區不支援使用資料存放區端點上的 GET 請求來取得匯出狀態。

您使用提出的所有匯出請求 FHIR REST API 都會以 ndjson 格式傳回，並匯出至 Amazon S3 儲存貯體。每個 S3 物件只會包含單一 FHIR 資源類型。

您可以一次為每個 AWS 帳戶提出單一匯出請求。若要進一步了解與相關聯的 Service Quotas HealthLake，請參閱 [AWS HealthLake 端點和配額](#)。

若要進一步了解如何使用匯出請求 FHIR REST API，請參閱 [使用 FHIR REST API 操作從 HealthLake 資料存放區匯出資料](#)。

在 Amazon Athena SQL 中使用 查詢 AWS HealthLake 資料存放區

當您建立 HealthLake 資料存放區時，高度巢狀 FHIR 的資料結構會擷取至 Amazon Athena，並自動轉換為 Iceberg 資料表，可透過 查詢 SQL。授予對此新資源的存取權是使用 AWS Lake Formation 進行管理。每個 FHIR 資源類型都以 Athena 中的個別資料表表示。

Important

對於 2022 年 11 月 14 日之前建立的資料存放區，您必須將現有的資料存放區遷移至新的資料存放區，才能使用 來查詢 SQL。如需協助，請參閱 [遷移現有資料存放區以使用 Amazon Athena](#)。

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節 [如何開啟 HealthLake 整合的自然語言處理功能？](#) 中的。

若要建立 HealthLake 資料存放區，您必須將其他 IAM 政策和服務角色新增至身為 HealthLake 管理員 IAM 的使用者或角色。如需設定許可的詳細資訊，請參閱 [設定開始使用的許可 AWS HealthLake](#)。

HealthLake 資料存放區會以 Iceberg 資料表的形式擷取至 Athena。若要進一步了解 Iceberg 資料表如何在 Athena 中運作，請參閱 Athena 使用者指南中的 [使用 Iceberg 資料表](#)。

HealthLake 支援 Athena 中 HealthLake 資料存放區的資料 READ 操作。若要進一步了解使用 操作 建立、讀取、更新和刪除 (CRUD) FHIR REST API 操作，請參閱 [使用與 HealthLake 資料存放區 FHIR REST API 的互動](#) 進一步了解 CRUD 操作如何影響 Athena 中的資料。

本章中的主題說明如何將 HealthLake 資料存放區連線至 Athena、如何使用 查詢 SQL，以及如何將結果與其他 AWS 服務連線以進行進一步分析。

內容

- [將資料存放區連線至 Amazon Athena](#)
 - [授予使用者、群組或角色存取 HealthLake 資料存放區的權限 \(AWS Lake Formation 主控台\)](#)

- [Athena 入門](#)
- [使用 查詢 HealthLake 您的資料存放區 SQL](#)
- [具有複雜篩選的範例SQL查詢](#)

將資料存放區連線至 Amazon Athena

Important

2022 年 11 月 14 日之後，存取IAM需求 HealthLake 已變更。若要在 Athena 中建立資料存放區並授予存取權，您必須將 AWSLakeFormationDataAdmin 受管政策新增至您的IAM使用者、群組或角色。您可以使用 AWSLakeFormationDataAdmin政策來建立資料湖管理員，並授予 Athena 中資料存放區的存取權。

本主題概述建立 Athena 使用者、群組或角色的必要步驟，並授予他們存取 HealthLake 資料存放區中找到FHIR的資源。

- [授予使用者、群組或角色對 HealthLake 資料存放區的存取權 \(AWS Lake Formation 主控台\)](#)
- [設定 Athena 帳戶](#)

授予使用者、群組或角色存取 HealthLake 資料存放區的權限 (AWS Lake Formation 主控台)

角色：HealthLake 管理員

HealthLake 管理員角色是 AWS Lake Formation 中的資料湖管理員。他們授予 Lake Formation 中 HealthLake 資料存放區的存取權。

對於每個建立的資料存放區，AWS Lake Formation 主控台中會顯示兩個項目。一個項目是資源連結。資源連結名稱一律以斜體顯示。每個資源連結都會顯示其連結共用資源的名稱和擁有者。對於 HealthLake 所有資料存放區，共用資源擁有者是 HealthLake 服務帳戶。另一個項目是 HealthLake 服務帳戶中 HealthLake 的資料存放區。此程序中的步驟會使用資源連結的資料存放區。

若要進一步了解資源連結，請參閱 Lake [Formation 開發人員指南中的資源連結如何在 Lake Formation 中運作](#)。AWS

若要讓使用者、群組或角色能夠在 Athena 中查詢資料，您必須授予資源資料庫的描述許可。然後，您必須在資料表上授予選取和描述。

STEP 1：授予 HealthLake 資料存放區資源連結資料庫的 DESCRIBE 許可

1. 開啟 AWS Lake Formation 主控台：<https://console.aws.amazon.com/lakeformation/>
2. 在主要導覽列中，選擇資料庫。
3. 在資料庫頁面上，選擇斜體資料存放區名稱旁的選項按鈕。
4. 選擇動作 (▼)。
5. 選擇 Grant (授予)。
6. 在授予資料許可頁面的主體下，選擇 IAM 使用者或角色。
7. 在 IAM 使用者或角色下，使用向下箭頭 (▼)，或搜尋您想要在 Athena 中查詢 IAM 的使用者、角色或群組。
8. 在 LF 標籤或目錄資源卡下，選擇具名資料目錄資源選項。
9. 在資料庫下，使用向下箭頭 (▼) 選擇您要共用存取權 HealthLake 的資料存放區資料庫。
10. 在資源連結許可卡中，在資源連結許可下，選擇描述。

當授予成功時，會出現授予許可成功橫幅。若要檢視您剛授予的許可，請選擇 Data lake 許可。在資料表中尋找使用者、群組和角色。在許可欄下，您會看到描述已列出。

現在您必須使用目標上的授予，在資料庫中的所有資料表上授予選取和描述。

STEP 2：授予資料 HealthLake 存放區資源連結中所有資料表的存取權

1. 開啟 AWS Lake Formation 主控台：<https://console.aws.amazon.com/lakeformation/>
2. 在主要導覽列中，選擇資料庫。
3. 在資料庫頁面上，選擇斜體資料存放區名稱旁的選項按鈕。
4. 選擇動作 (▼)。
5. 選擇對目標授予。
6. 在授予資料許可頁面的主體下，選擇 IAM 使用者或角色。
7. 在 IAM 使用者或角色下，使用向下箭頭 (▼) 或搜尋您想要在 Athena 中查詢 IAM 的使用者、群組或角色。
8. 在 LF 標籤或目錄資源卡下，選擇具名資料目錄資源選項。
9. 在資料庫下，使用向下箭頭 (▼) 選擇您要授予存取權 HealthLake 的資料存放區資料庫。

10. 在資料表下，選擇所有資料表以與 HealthLake 使用者共用所有資料表。
11. 在資料表許可卡的資料表許可下，選擇描述和選取。
12. 選擇 Grant (授予)。

選擇授予後，會出現授予許可成功橫幅。指定的使用者可以在 Athena 中的 HealthLake 資料存放區上進行查詢。

Athena 入門

HealthLake 使用者

HealthLake 使用者將使用 Athena 主控台 AWS CLI，或 AWS SDKs 查詢 HealthLake 管理員與其共用 HealthLake 的資料存放區。

若要使用 Athena 查詢資料存放區，您必須執行下列三件事。

- 透過 Lake Formation 授予 IAM 使用者或角色對 HealthLake 資料存放區的存取權。如需進一步了解，請參閱 [授予使用者、群組或角色存取 HealthLake 資料存放區的權限 \(AWS Lake Formation 主控台\)](#)。
- 為您的 HealthLake 資料存放區建立工作群組。
- 指定 Amazon S3 儲存貯體來存放查詢結果。

若要開始使用 Athena，請將 AmazonAthenaFullAccess 和 AmazonS3FullAccess AWS 受管政策新增至您的使用者、群組或角色。使用 AWS 受管政策是開始使用新服務的好方法。請記住，AWS 受管政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。當您使用 IAM 政策設定許可時，只會授予執行任務所需的許可。若要進一步了解 IAM 並套用最低權限，請參閱 IAM 《使用者指南》中的 [套用最低權限許可](#)。

Important

若要查詢 Athena 中的 HealthLake 資料存放區，您必須使用 Athena 引擎第 3 版。

工作群組是資源，因此您可以使用 IAM 型政策來控制對特定工作群組的存取。若要進一步了解，請參閱《Athena 使用者指南》中的 [使用工作群組來控制查詢存取和成本](#)。

若要進一步了解設定工作群組，請參閱 Athena 使用者指南<https://docs.aws.amazon.com/athena/latest/ug/workgroups-procedure.html>中的。

Note

Amazon S3 儲存貯體所在的區域，Athena 主控台必須相符。

您必須指定 Amazon S3 中的查詢結果儲存貯體位置，然後才能執行查詢，否則您必須使用已指定儲存貯體，且其組態可覆寫用戶端設定的工作群組。每個執行的查詢都會自動儲存輸出檔案。

如需在 Athena 主控台中指定查詢結果位置的詳細資訊，請參閱《Amazon Athena 使用者指南》中的[使用 Athena 主控台指定查詢結果位置](#)。

若要查看如何在 Athena 中查詢 HealthLake 資料存放區的範例，請參閱[使用 查詢 HealthLake 您的資料存放區 SQL](#)。

使用 查詢 HealthLake 您的資料存放區 SQL

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節[如何開啟 HealthLake 整合的自然語言處理功能？](#)中的。

本主題中的所有範例都使用 Synthea 建立的虛構資料。若要進一步了解如何建立預先載入 Synthea 資料的資料存放區，請參閱[在中建立資料存放區 AWS HealthLake](#)。

當您將 HealthLake 資料存放區匯入 Athena 時，HealthLake 資料存放區中的每個資源類型都會轉換為資料表。這些資料表可以個別查詢，也可以使用 SQL 型查詢做為群組。由於資料存放區的結構，您的資料會以多種不同的資料類型匯入 Athena。若要進一步了解如何建立可存取這些資料類型的 SQL 查詢，請參閱《Amazon Athena 使用者指南》中的[查詢具有複雜類型和巢狀結構的陣列](#)。

對於資源類型中的每個元素，FHIR 規格會定義基數。元素的基數定義了此元素可以出現的次數的下限和上限。建構 SQL 查詢時，您必須將此納入考量。例如，我們來看看[資源類型中的一些元素：病患](#)。

- 元素：名稱 FHIR 規格會將基數設定為 0..*。

元素會擷取為陣列。

```
[{
  id = null,
  extension = null,
  use = official,
  _use = null,
  text = null,
  _text = null,
  family = Wolf938,
  _family = null,
  given = [Noel608],
  _given = null,
  prefix = null,
  _prefix = null,
  suffix = null,
  _suffix = null,
  period = null
}]
```

在 Athena 中，若要查看如何擷取資源類型，請在資料表和檢視下搜尋它。若要存取此陣列中的元素，您可以使用點表示法。以下是存取 `given` 和 `family` 值的簡單範例。

```
SELECT
  name[1].given as FirstName,
  name[1].family as LastName
FROM Patient
```

- 元素：MaritalStatusFHIR規格會將基數設定為 0..1。

此元素擷取為 JSON。

```
{
  id = null,
  extension = null,
  coding = [
    {
      id = null,
      extension = null,
      system = http://terminology.hl7.org/CodeSystem/v3-MaritalStatus,
      _system = null,
      version = null,
      _version = null,
    }
  ]
}
```

```
code = S,  
_code = null,  
display = Never Married,  
_display = null,  
userSelected = null,  
_userSelected = null  
}  
  
],  
text = Never Married,  
_text = null  
}
```

在 Athena 中，若要查看如何擷取資源類型，請在資料表和檢視下搜尋它。若要存取 中的鍵/值對JSON，您可以使用點符號。由於這不是陣列，因此不需要陣列索引。以下是存取 值的簡單範例text。

```
SELECT  
    maritalstatus.text as MaritalStatus  
FROM Patient
```

若要進一步了解如何存取和搜尋 JSON，請參閱 Athena 使用者指南中的[查詢JSON](#)。

Athena Data Manipulation Language (DML) 查詢陳述式是以 Trino 為基礎。Athena 不支援 Trino 的所有功能，並且存在重大差異。若要進一步了解，請參閱《Amazon Athena 使用者指南》中的[DML查詢、函數和運算子](#)。

此外，Athena 支援您在建立資料 HealthLake 存放區查詢時可能遇到的多種資料類型。若要進一步了解 Athena 中的資料類型，請參閱《[Amazon Athena 使用者指南](#)》中的 [Amazon Athena 中的資料類型](#)。Amazon Athena

若要進一步了解SQL查詢如何在 Athena 中運作，請參閱《[SQLAmazon Athena 使用者指南](#)》中的 Amazon Athena 參考。

每個索引標籤顯示如何使用 Athena 搜尋指定資源類型和相關元素的範例。

Element: Extension

元素extension用於在資料存放區中建立自訂欄位。

此範例說明如何存取 Patient 資源類型中找到的 extension元素功能。

當您 HealthLake 的資料存放區匯入 Athena 時，資源類型的元素剖析方式會有所不同。由於的結構element是變數，因此無法在結構描述中完整指定。為了處理該變異性，陣列內的元素會以字串形式傳遞。

在的資料表描述中Patient，您可以看到extension描述為的元素array<string>，這表示您可以使用索引值來存取陣列的元素。不過，若要存取字串的元素，您必須使用 json_extract。

以下是在患者資料表中找到的 extension元素的單一項目。

```
[{
  "valueString": "Kerry175 Cummerata161",
  "url": "http://hl7.org/fhir/StructureDefinition/patient-mothersMaidenName"
},
{
  "valueAddress": {
    "country": "DE",
    "city": "Hamburg",
    "state": "Hamburg"
  },
  "url": "http://hl7.org/fhir/StructureDefinition/patient-birthPlace"
},
{
  "valueDecimal": 0.0,
  "url": "http://synthetichealth.github.io/synthea/disability-adjusted-life-years"
},
{
  "valueDecimal": 5.0,
  "url": "http://synthetichealth.github.io/synthea/quality-adjusted-life-years"
}
]
```

即使這是有效的 JSON，Athena 仍會將其視為字串。

此SQL查詢範例示範如何建立包含 patient-mothersMaidenName和 patient-birthPlace元素的資料表。若要存取這些元素，您需要使用不同的陣列索引和 json_extract。

```
SELECT
  extension[1],
  json_extract(extension[1], '$.valueString') AS MothersMaidenName,
  extension[2],
  json_extract(extension[2], '$.valueAddress.city') AS birthPlace
FROM patient
```

若要進一步了解涉及的查詢JSON，請參閱《Amazon Athena 使用者指南》中的[從 擷取資料 JSON](#)。

Element: birthDate (Age)

年齡不是 中病患資源類型的元素FHIR。以下是根據年齡篩選的搜尋的兩個範例。

由於年齡不是 元素，我們使用 birthDate進行SQL查詢。若要查看 元素如何擷取至 FHIR，請在資料表和檢視下搜尋資料表名稱。您可以看到它是類型字串。

範例 1：計算年齡的值

在此範例SQL查詢中，我們使用內建SQL工具 current_date和 year 來擷取這些元件。然後，我們將它們減去，以傳回病患的實際年齡作為稱為 的資料欄age。

```
SELECT
  (year(current_date) - year(date(birthdate))) as age
FROM patient
```

範例 2：針對在 2019-01-01和 之前出生的患者進行篩選male。

SQL 查詢會示範如何使用 CAST函數將birthDate元素轉換為類型 DATE，以及如何根據 WHERE子句中的兩個條件進行篩選。由於元素預設會擷取為類型字串，因此我們必須CAST將其擷取為類型 DATE。然後，您可以使用<運算子將其與不同的日期 進行比較2019-01-01。使用 AND，您可以將第二個條件新增至 WHERE子句。

```
SELECT birthdate
FROM patient
-- we convert birthdate (varchar) to date > cast that as date too
WHERE CAST(birthdate AS DATE) < CAST('2019-01-01' AS DATE) AND gender = 'male'
```

Resource type: Location

此範例顯示搜尋城市名稱為 Attleboro 的位置資源類型內的位置。

```
SELECT *
FROM Location
WHERE address.city='ATTLEBORO'
LIMIT 10;
```

Element: Age

```
SELECT birthdate
```

```
FROM patient
-- we convert birthdate (varchar) to date > cast that as date too
WHERE CAST(birthdate AS DATE) < CAST('2019-01-01' AS DATE) AND gender = 'male'
```

Resource type: Condition

資源類型條件會存放與已上升到關注層級的問題相關的診斷資料。HealthLake的整合醫療自然語言處理 (NLP) 會根據Condition資源類型中發現的詳細資訊產生新的 DocumentReference 資源。產生新資源時，會將標籤 HealthLake 附加SYSTEM_GENERATED至 meta元素。此範例SQL查詢示範如何搜尋條件資料表並傳回結果，其中SYSTEM_GENERATED的結果已被移除。

若要進一步了解整合的自然語言處理 (NLP) HealthLake，請參閱 [根據中資源類型的自然語言處理 \(NLP\)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake](#)。

```
SELECT *
FROM condition
WHERE meta.tag[1] is NULL
```

您也可以指定的字串元素內搜尋，進一步篩選查詢。modifierextension 元素包含有關使用哪個DocumentReference資源來產生一組條件的詳細資訊。同樣地，您必須使用 json_extract來存取以字串的形式帶入 Athena 的巢狀JSON元素。

此範例SQL查詢示範如何搜尋根據特定 Condition產生的所有 DocumentReference。使用將JSON元素CAST設定為字串，以便您可以使用 LIKE 進行比較。

```
SELECT
    meta.tag[1].display as SystemGenerated,
    json_extract(modifierextension[4], '$.valueReference.reference') as
    DocumentReference
FROM condition
WHERE meta.tag[1].display = 'SYSTEM_GENERATED'

AND CAST(json_extract(modifierextension[4], '$.valueReference.reference') as
    VARCHAR) LIKE '%DocumentReference/67aa0278-8111-40d0-8adc-43055eb9d18d%'
```

Resource type: Observation

資源類型觀察會儲存對病患、裝置或其他主體所做的測量和簡單聲明。HealthLake的整合自然語言處理 (NLP) 會根據Observation資源中發現的詳細資訊產生新的DocumentReference資源。此範例SQL查詢包含WHERE meta.tag[1] is NULL註解，這表示SYSTEM_GENERATED結果會包含在內。

```
SELECT valueCodeableConcept.coding[1].code
FROM Observation
WHERE valueCodeableConcept.coding[1].code = '266919005'
-- WHERE meta.tag[1] is NULL
```

此欄已匯入為 [struct](#)。因此，您可以使用點符號存取其中的元素。

Resource type: MedicationStatement

MedicationStatement 是一種 FHIR 資源類型，可用來存放有關患者已使用、正在使用或未來將使用之藥物的詳細資訊。HealthLake 的整合醫療自然語言處理 (NLP) 會根據 MedicationStatement 資源類型中找到的文件產生新 DocumentReference 資源。產生新資源時，會將標籤 HealthLake 附加 SYSTEM_GENERATED 至 meta 元素。此範例 SQL 查詢示範如何建立查詢，使用單一患者的識別符根據該查詢進行篩選，並尋找由整合 HealthLake 的所新增的資源 NLP。

```
SELECT *
FROM medicationstatement
WHERE meta.tag[1].display = 'SYSTEM_GENERATED' AND subject.reference =
  'Patient/0679b7b7-937d-488a-b48d-6315b8e7003b';
```

若要進一步了解 HealthLake 整合的醫療 NLP，請參閱 [根據中資源類型的自然語言處理 \(NLP\)，使用自動產生 FHIR DocumentReference 資源 AWS HealthLake](#)。

具有複雜篩選的範例 SQL 查詢

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節 [如何開啟 HealthLake 整合的自然語言處理功能？](#) 中的。

本主題中的範例包括 HealthLake 與使用複雜篩選的 Athena 整合的 SQL 查詢。

Example 根據人口統計資料建立篩選條件

建立病患群組時，識別正確的病患人口統計資料非常重要。此範例查詢示範如何使用 Trino 點表示法，以及 json_extract 篩選 HealthLake 資料存放區中的資料。

```
SELECT
```

```

    id
  , CONCAT(name[1].family, ' ', name[1].given[1]) as name
  , (year(current_date) - year(date(birthdate))) as age
  , gender as gender
  , json_extract(extension[1], '$.valueString') as MothersMaidenName
  , json_extract(extension[2], '$.valueAddress.city') as birthPlace
  , maritalstatus.coding[1].display as maritalstatus
  , address[1].line[1] as addressline
  , address[1].city as city
  , address[1].district as district
  , address[1].state as state
  , address[1].postalcode as postalcode
  , address[1].country as country
  , json_extract(address[1].extension[1], '$.extension[0].valueDecimal') as latitude
  , json_extract(address[1].extension[1], '$.extension[1].valueDecimal') as longitude
  , telecom[1].value as telNumber
  , deceasedboolean as deceasedIndicator
  , deceaseddatetime
FROM database.patient;

```

使用 Athena 主控台，您可以進一步排序和下載結果。

Example 為病患及其相關條件建立篩選條件

此範例查詢示範如何尋找和排序 HealthLake 資料存放區中找到之病患的所有相關條件。

```

SELECT
  patient.id as patientId
  , condition.id as conditionId
  , CONCAT(name[1].family, ' ', name[1].given[1]) as name
  , condition.meta.tag[1].display
  , json_extract(condition.modifierextension[1], '$.valueDecimal') AS confidenceScore
  , category[1].coding[1].code as categoryCode
  , category[1].coding[1].display as categoryDescription
  , code.coding[1].code as diagnosisCode
  , code.coding[1].display as diagnosisDescription
  , onsetdatetime
  , severity.coding[1].code as severityCode
  , severity.coding[1].display as severityDescription
  , verificationstatus.coding[1].display as verificationStatus
  , clinicalstatus.coding[1].display as clinicalStatus
  , encounter.reference as encounterId
  , encounter.type as encountertype
FROM database.patient, condition

```

```
WHERE CONCAT('Patient/', patient.id) = condition.subject.reference
ORDER BY name;
```

您可以使用 Athena 主控台進一步排序這些結果，或下載這些結果以進行進一步分析。

Example 為病患及其相關觀察建立篩選條件

此範例查詢示範如何尋找和排序 HealthLake 資料存放區中找到之病患的所有相關觀察。

```
SELECT
  patient.id as patientId
  , observation.id as observationId
  , CONCAT(name[1].family, ' ', name[1].given[1]) as name
  , meta.tag[1].display
  , json_extract(modifierextension[1], '$.valueDecimal') AS confidenceScore
  , status
  , category[1].coding[1].code as categoryCode
  , category[1].coding[1].display as categoryDescription
  , code.coding[1].code as observationCode
  , code.coding[1].display as observationDescription
  , effectivedatetime
  , CASE
    WHEN valuequantity.value IS NOT NULL THEN CONCAT(CAST(valuequantity.value AS
  VARCHAR),' ',valuequantity.unit)
      WHEN valueCodeableConcept.coding [ 1 ].code IS NOT NULL THEN
  CAST(valueCodeableConcept.coding [ 1 ].code AS VARCHAR)
      WHEN valuestring IS NOT NULL THEN CAST(valuestring AS VARCHAR)
      WHEN valueboolean IS NOT NULL THEN CAST(valueboolean AS VARCHAR)
      WHEN valueinteger IS NOT NULL THEN CAST(valueinteger AS VARCHAR)
      WHEN valueratio IS NOT NULL THEN CONCAT(CAST(valueratio.numerator.value AS
  VARCHAR),'/',CAST(valueratio.denominator.value AS VARCHAR))
      WHEN valuerange IS NOT NULL THEN CONCAT(CAST(valuerange.low.value AS
  VARCHAR),'-',CAST(valuerange.high.value AS VARCHAR))
      WHEN valueSampledData IS NOT NULL THEN CAST(valueSampledData.data AS VARCHAR)
      WHEN valueTime IS NOT NULL THEN CAST(valueTime AS VARCHAR)
      WHEN valueDateTime IS NOT NULL THEN CAST(valueDateTime AS VARCHAR)
      WHEN valuePeriod IS NOT NULL THEN valuePeriod.start
      WHEN component[1] IS NOT NULL THEN CONCAT(CAST(component[2].valuequantity.value
  AS VARCHAR),' ',CAST(component[2].valuequantity.unit AS VARCHAR),
  '/', CAST(component[1].valuequantity.value AS VARCHAR),'
  ',CAST(component[1].valuequantity.unit AS VARCHAR))
      END AS observationvalue
  , encounter.reference as encounterId
  , encounter.type as encountertype
```

```
FROM database.patient, observation
WHERE CONCAT('Patient/', patient.id) = observation.subject.reference
ORDER BY name;
```

Example 為病患及其相關程序建立篩選條件

將程序連接到病患是醫療保健的重要層面。此SQL查詢示範如何使用病患和程序資源類型在 Athena 中執行此操作。此SQL查詢會傳回 HealthLake 資料存放區中找到的所有病患及其相關程序。

```
SELECT
  patient.id as patientId
  , PROCEDURE.id as procedureId
  , CONCAT(name[1].family, ' ', name[1].given[1]) as name
  , status
  , category.coding[1].code as categoryCode
  , category.coding[1].display as categoryDescription
  , code.coding[1].code as procedureCode
  , code.coding[1].display as procedureDescription
  , performeddatetime
  , performer[1]
  , encounter.reference as encounterId
  , encounter.type as encountertype
FROM database.patient, procedure
WHERE CONCAT('Patient/', patient.id) = procedure.subject.reference
ORDER BY name;
```

現在，您可以使用 Athena 主控台下載結果以進行進一步分析，或對其進行排序，以進一步了解結果。

Example 為病患及其相關處方建立篩選條件

查看病患目前正在使用之藥物的目前清單非常重要。使用 Athena，您可以撰寫查詢，該SQL查詢同時使用 HealthLake 資料存放區中發現的病患 MedicationRequest 和資源類型。

此SQL查詢會聯結匯入 Athena 的患者和 MedicationRequest 資料表。它也會使用點表示法，將處方組織到個別項目中。

```
SELECT
  patient.id as patientId
  , medicationrequest.id as medicationrequestid
  , CONCAT(name[1].family, ' ', name[1].given[1]) as name
  , status
  , statusreason.coding[1].code as categoryCode
  , statusreason.coding[1].display as categoryDescription
```

```

, category[1].coding[1].code as categoryCode
, category[1].coding[1].display as categoryDescription
, priority
, donotperform
, encounter.reference as encounterId
, encounter.type as encountertype
, medicationcodeableconcept.coding[1].code as medicationCode
, medicationcodeableconcept.coding[1].display as medicationDescription
, dosageinstruction[1].text as dosage
FROM database.patient, medicationrequest
WHERE CONCAT('Patient/', patient.id ) = medicationrequest.subject.reference
ORDER BY name

```

您可以使用 Athena 主控台來排序結果，或下載結果以進行進一步分析。

Example 查看 MedicationStatement 資源類型中找到的藥品

範例查詢說明如何使用 組織JSON匯入 Athena 的巢狀 SQL。查詢使用 meta 元素來指出 HealthLake 整合的自然語言處理 () 新增藥品的時間 NLP。若要進一步了解 HealthLake 與 Amazon Comprehend Medical 的整合，請參閱 [根據中資源類型的自然語言處理 \(NLP\)，使用自動產生 FHIR DocumentReference 資源 AWS HealthLake](#)。它也使用 json_extract 來搜尋 JSON 字串陣列內的資料。

```

SELECT
  medicationcodeableconcept.coding[1].code as medicationCode
  , medicationcodeableconcept.coding[1].display as medicationDescription
  , meta.tag[1].display
  , json_extract(modifierextension[1], '$.valueDecimal') AS confidenceScore
FROM medicationstatement;

```

您可以使用 Athena 主控台來下載或排序這些結果。

Example 針對特定疾病類型篩選

此範例示範如何找到一組 18 到 75 歲且已被診斷為糖尿病的患者。

```

SELECT patient.id as patientId,
  condition.id as conditionId,
  CONCAT(name [ 1 ].family, ' ', name [ 1 ].given [ 1 ]) as name,
  (year(current_date) - year(date(birthdate))) AS age,
CASE
  WHEN condition.encounter.reference IS NOT NULL THEN condition.encounter.reference
  WHEN observation.encounter.reference IS NOT NULL THEN observation.encounter.reference

```

```

END as encounterId,
CASE
  WHEN condition.encounter.type IS NOT NULL THEN observation.encounter.type
  WHEN observation.encounter.type IS NOT NULL THEN observation.encounter.type
END AS encountertype,
condition.code.coding [ 1 ].code as diagnosisCode,
condition.code.coding [ 1 ].display as diagnosisDescription,
observation.category [ 1 ].coding [ 1 ].code as categoryCode,
observation.category [ 1 ].coding [ 1 ].display as categoryDescription,
observation.code.coding [ 1 ].code as observationCode,
observation.code.coding [ 1 ].display as observationDescription,
effectivedatetime AS observationDateTime,
CASE
  WHEN valuequantity.value IS NOT NULL THEN CONCAT(CAST(valuequantity.value AS
VARCHAR),' ',valuequantity.unit)
  WHEN valueCodeableConcept.coding [ 1 ].code IS NOT NULL THEN
CAST(valueCodeableConcept.coding [ 1 ].code AS VARCHAR)
  WHEN valuestring IS NOT NULL THEN CAST(valuestring AS VARCHAR)
  WHEN valueboolean IS NOT NULL THEN CAST(valueboolean AS VARCHAR)
  WHEN valueinteger IS NOT NULL THEN CAST(valueinteger AS VARCHAR)
  WHEN valueratio IS NOT NULL THEN CONCAT(CAST(valueratio.numerator.value AS
VARCHAR),'/',CAST(valueratio.denominator.value AS VARCHAR))
  WHEN valuerange IS NOT NULL THEN CONCAT(CAST(valuerange.low.value AS
VARCHAR),'-',CAST(valuerange.high.value AS VARCHAR))
  WHEN valueSampledData IS NOT NULL THEN CAST(valueSampledData.data AS VARCHAR)
  WHEN valueTime IS NOT NULL THEN CAST(valueTime AS VARCHAR)
  WHEN valueDateTime IS NOT NULL THEN CAST(valueDateTime AS VARCHAR)
  WHEN valuePeriod IS NOT NULL THEN valuePeriod.start
  WHEN component[1] IS NOT NULL THEN CONCAT(CAST(component[2].valuequantity.value
AS VARCHAR),' ',CAST(component[2].valuequantity.unit AS VARCHAR),
'/', CAST(component[1].valuequantity.value AS VARCHAR),'
',CAST(component[1].valuequantity.unit AS VARCHAR))
  END AS observationvalue,
CASE
  WHEN condition.meta.tag [ 1 ].display = 'SYSTEM GENERATED' THEN 'YES'
  WHEN condition.meta.tag [ 1 ].display IS NULL THEN 'NO'
  WHEN observation.meta.tag [ 1 ].display = 'SYSTEM GENERATED' THEN 'YES'
  WHEN observation.meta.tag [ 1 ].display IS NULL THEN 'NO'
  END AS IsSystemGenerated,
CAST(
  json_extract(
    condition.modifierextension [ 1 ],
    '$.valueDecimal'
  ) AS int

```

```
    ) AS confidenceScore
FROM database.patient,
     database.condition,
     database.observation
WHERE CONCAT('Patient/', patient.id) = condition.subject.reference
      AND CONCAT('Patient/', patient.id) = observation.subject.reference
      AND (year(current_date) - year(date(birthdate))) >= 18
      AND (year(current_date) - year(date(birthdate))) <= 75
      AND condition.code.coding [ 1 ].display like ('%diabetes%');
```

現在您可以使用 Athena 主控台來排序結果，或下載結果以進行進一步分析。

AWS HealthLake 和介面VPC端點 (AWS PrivateLink)

您可以建立介面VPC端點，AWS HealthLake 在 VPC和 之間建立私有連線。介面VPC端點採用 [AWS PrivateLink](#)這是一種可用來私下存取的技術 HealthLake，APIs無需網際網路閘道、NAT裝置、VPN連線或 AWS Direct Connect 連線。您 中的執行個體VPC不需要公有 IP 地址即可與 通訊 HealthLake；APIs。您的 VPC與 之間的流量 HealthLake； 不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[介面VPC端點 \(AWS PrivateLink\)](#)。

端點的 HealthLake VPC考量事項

在您設定 的介面VPC端點之前 HealthLake，請務必檢閱 Amazon VPC使用者指南中的[介面端點屬性和限制](#)。

HealthLake 支援從您的 呼叫其所有API動作VPC。

為 建立介面VPC端點 HealthLake；

您可以使用 Amazon VPC主控台或 AWS Command Line Interface () 為 HealthLake建立VPC端點；服務AWS CLI。如需詳細資訊，請參閱《Amazon VPC使用者指南》中的[建立介面端點](#)。

HealthLake使用下列服務名稱建立 的VPC端點：

- com.amazonaws*region*..healthlake

如果您DNS為端點開啟私有，則可以使用區域的預設DNS名稱向 HealthLake 提出API請求。例如：*healthlake.us-east-1.amazonaws.com*。

如需詳細資訊，請參閱《Amazon VPC使用者指南》中的[透過介面端點存取服務](#)。

為 建立VPC端點政策 HealthLake

您可以將端點政策連接至控制 存取的VPC端點 HealthLake。此政策會指定下列資訊：

- 可執行動作的主體。

- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon VPC使用者指南》中的[使用VPC端點控制對服務的存取](#)。

範例：HealthLake 動作的VPC端點政策

以下是的端點政策範例 HealthLake。連接至端點時，此政策會授予所有資源上所有主體的CreateFHIRDatastore動作存取權 HealthLake。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "healthlake:create-fhir-datastore"
      ],
      "Resource": "*"
    }
  ]
}
```

在 中標記資源 AWS HealthLake

您可以用標籤的形式將中繼資料指派給 AWS 資源。每個標籤都是由使用者定義的金鑰和值組成的標籤。標籤可協助您管理、識別、組織、搜尋及篩選資源。

本主題描述常用的標記類別和策略，協助您實作一致且有效的標記策略。以下各節假設對AWS資源、標記、詳細帳單和 AWS Identity and Access Management (IAM) 的基本了解IAM。

每個標籤有兩個部分：

- 標籤金鑰（例如 CostCenter，環境或專案）。標籤鍵會區分大小寫。
- 標籤值（例如 111122223333 或 Production）。與標籤鍵相同，標籤值會區分大小寫。

您可使用標籤來依照用途、擁有者、環境或其他條件分類資源。如需詳細資訊，請參閱 [AWS 標記策略](#)。

您可以從每個資源的服務主控台、服務或一次新增、變更API或移除一個資源的標籤AWSCLI。

若要啟用標記，請確定 TagResources 已獲得授權。您可以連接 IAM政策 TagResources 進行授權，如下列範例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "healthlake:CreateFHIRDatastore",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "healthlake:TagResource",
      "Resource": "*"
    }
  ]
}
```

重要通知

AWS HealthLake 根據AWS共同責任模型政策保護客戶資料。這表示所有客戶資料都會在轉換和靜態時加密。不過，並非所有資料存放區或任務型操作的客戶輸入名稱都會被編排。它們不應包含個人身分識別資訊或受保護的健康資訊。如需詳細資訊，請參閱 AWS HealthLake 安全章節。

最佳實務

當您建立 AWS 資源的標記策略時，請遵循最佳實務：

- 請勿將個人身分識別資訊 (PII)、個人健康資訊 (PHI) 或其他敏感資訊存放在標籤中。
- 使用標準化、區分大小寫的標籤格式，並統一套用在所有資源類型上。
- 考慮支援多種用途的標籤準則，例如資源存取控制管理、成本追蹤、自動化和組織。
- 使用自動化工具來協助管理資源標籤。[AWS資源群組](#)和[資源群組標記API](#)可對標籤進行程式設計控制，使其能夠自動管理、搜尋和篩選標籤和資源。
- 當您使用更多標籤時，標記會更有效率。
- 標籤可以隨著使用者的需求變更而編輯或修改，但若要更新存取控制標籤，您還必須更新參考這些標籤的政策，以控制對資源的存取。

標記需求

標籤均擁有以下要求：

- 金鑰不能以 `aws:` 為字首。
- 索引鍵在標籤集內必須是唯一的。
- 索引鍵必須介於 1 到 128 個允許的字元之間。
- 值必須介於 0 到 256 個允許的字元之間。
- 值在每個標籤集中不需要是唯一的。
- 索引鍵和值的允許字元為 Unicode 字母、數字、空格和下列任何符號：`_ . : / = + - @`。
- 金鑰和值會區分大小寫。

將標籤新增至資料存放區

將標籤新增至資料存放區可協助您識別和組織資源，並管理對這些AWS資源的存取。首先，您將一或多個標籤（鍵/值對）新增至資料存放區。每個使用者最多可使用 50 個標籤。對於您可以在索引鍵和值欄位中使用的字元也有限制。

擁有標籤後，您可以建立IAM政策，根據這些標籤管理對資料存放區的存取。您可以使用 HealthLake 主控台或 AWS CLI 將標籤新增至資料存放區。新增標籤到儲存庫可能會影響存取該儲存庫。將標籤新增至資料存放區之前，請務必檢閱任何可能使用標籤來控制存取資料存放區等資源IAM的政策。

請依照下列步驟，使用 AWS CLI 將標籤新增至 HealthLake 資料存放區。若要在建立標籤時將標籤新增至資料存放區，請參閱 [在中建立資料存放區 AWS HealthLake](#)。

在終端機或命令列，執行 tag-resource 命令，指定您要新增標籤的資料存放區的 Amazon Resource Name (ARN)，以及您要新增的標籤的索引鍵和值。您可以將多個標籤新增至資料存放區。金鑰和值欄位中可以使用的字元也有限制，例如[標記需求](#)，若要在建立資料存放區時將標籤新增至資料存放區，請在 中使用下列命令 AWS CLI。資料存放區的名稱為 Test_Data_Store，兩個新增的標籤與索引鍵分別為 key1 和 key2，值為 value1 和 value2

```
aws healthlake create-fhir-datastore --datastore-type-version R4 --preload-data-config
PreloadDataType="SYNTHEA" --datastore-name "Test_Data_Store" --tags '[{"Key": "key1",
"Value": "value1"}, {"Key": "key2", "Value": "value2"}]' --region us-east-1
```

若要將標籤新增至現有的資料存放區，請執行下列範例命令：

```
aws healthlake tag-resource --resource-arn "arn:aws:healthlake:us-
east-1:691207106566:datastore/fhir/0725c83f4307f263e16fd56b6d8ebdbe" --tags '[{"Key":
"key1", "Value": "value1"}]' --region us-east-1
```

如果成功，此命令不會傳回任何回應。

列出資料存放區的標籤

請依照下列步驟使用 AWS CLI 來檢視 HealthLake 資料存放區的AWS標籤清單。若未新增標籤，傳回的清單空白。

在終端機或命令列，`list-tags-for-resource`執行 命令，如下列範例所示。

```
aws healthlake-test list-tags-for-resource --resource-arn "arn:aws:healthlake:us-east-1:674914422125:datastore/fhir/0725c83f4307f263e16fd56b6d8ebdbe" --region us-east-1
```

```
{
  "tags": {
    "key": "value",
    "key1": "value1"
  }
}
```

從資料存放區移除標籤

您可以移除與資料存放區相關聯的一或多個標籤。移除標籤不會從其他 AWS 資源刪除與該標籤相關聯的標籤。

在終端機或命令列，執行 `untag-resource` 命令，指定您要移除標籤的資料存放區的 Amazon Resource Name (ARN)，以及您要移除標籤的標籤索引鍵。

```
aws healthlake untag-resource --resource-arn "arn:aws:healthlake:us-east-1:674914422125:datastore/fhir/b91723d65c6fdeb1d26543a49d2ed1fa" --tag-keys '["key1"]' --region us-east-1
```

如果成功，此命令不會傳回回應。若要驗證與資料存放區相關聯的標籤，請執行 `list-tags-for-resource` 命令。

監控 HealthLake

監控是維護 HealthLake 和其他 AWS 解決方案可靠性、可用性和效能的重要部分。AWS 提供下列監控工具，讓您監看 HealthLake、報告錯誤，並適時採取自動動作：

- Amazon CloudWatch 會 AWS 即時監控您的 AWS 資源和，以及您在 上執行的應用程式。您可以收集 and 追蹤指標、建立自訂儀表板，以及設定警示，在指定的指標達到特定閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 用量或其他指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。
- AWS CloudTrail 會擷取由您的帳戶或代表您的帳戶 AWS 發出的 API 呼叫和相關事件。其接著會將日誌檔案交付到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、這些呼叫的來源 IP 地址，以及它們的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/>。

主題

- [HealthLake 使用 Amazon 監控 CloudWatch](#)

HealthLake 使用 Amazon 監控 CloudWatch

您可以使用 監控 HealthLake CloudWatch，這會收集原始資料並將其處理為可讀取、近乎即時的指標。這些統計資料會保留 15 個月，因此您可以使用該歷史資訊，並更深入了解 Web 應用程式或服務的效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

系統會報告所有 的指標 HealthLake APIs，包括下列項目。

- 資料存放區管理 APIs — CreateFHIRDatastore、DeleteFHIRDatastore、DescribeFHIRDatastore、ListFHIRDatastores
- 匯入和匯出 APIs — StartFHIRImport 任務、ListFHIRImport 任務、DescribeFHIRImport 任務、StartFHIRExport 任務、ListFHIRExport 任務、DescribeFHIRExport 任務
- HTTP REST 用戶端和資源管理 APIs — CreateResource、DeleteResource GetCapabilities、ReadResource SearchAll、SearchWithGet、SearchWithPost、UpdateResource。
- 標記 APIs — ListTagsForResource、TagResource、UntagResource

下表列出 HealthLake 的指標和維度。

系統會報告下列指標。每個都會以使用者指定資料範圍的頻率計數顯示。

指標

指標	描述
呼叫計數	對的呼叫數APIs。您可以針對帳戶或指定的資料存放區報告此問題。 單位：計數 有效統計資料：總和、計數 維度：操作、資料存放區 ID、資料存放區類型
成功的請求	成功API請求的數量。 單位：計數 有效的統計資訊：總和、平均 維度：操作、資料存放區、資料存放區類型
使用者錯誤	由於使用者錯誤而失敗的請求數量。 單位：計數 有效的統計資訊：總和、平均 維度：操作、資料存放區 ID、資料存放區類型
伺服器錯誤	由於伺服器錯誤而失敗的請求數量。 單位：計數 有效的統計資訊：總和、平均 維度：操作、資料存放區 ID、資料存放區類型
調節的請求	已調節的請求數量。此指標不包含在使用者或伺服器錯誤計數中。 單位：計數

指標	描述
	有效的統計資訊：總和、平均
	維度：操作、資料存放區 ID、資料存放區類型
Latency (延遲)	處理使用者請求所需的時間，以毫秒為單位。
	單位：毫秒
	有效統計資訊：下限、上限、平均數
	維度：操作、資料存放區 ID、資料存放區類型

會報告下列維度。

維度

維度	描述
作業	使用的 API 操作
DataStoreID	API 請求中包含的資料存放區
DataStoreType	資料存放區的類型（目前僅支援 FHIR R4）

您可以使用 HealthLake AWS 管理主控台、AWS CLI 或取得的指標 CloudWatch API。您可以透過其中一個 Amazon AWS 軟體開發套件 CloudWatch API (SDKs) 或 CloudWatch API 工具使用。HealthLake 主控台會根據來自的原始資料顯示圖形 CloudWatch API。

您必須擁有適當的 CloudWatch 許可，才能使用進行監控 HealthLake CloudWatch。如需詳細資訊，請參閱《[Amazon 使用者指南](#)》中的 [Amazon 的身分驗證和存取控制 CloudWatch](#)。CloudWatch

檢視 HealthLake 指標

檢視指標 CloudWatch（主控台）

1. 登入 AWS 管理主控台，並開啟 [CloudWatch 主控台](#)。
2. 選擇指標，選擇所有指標，然後選擇 AWS/HealthLake。
3. 選擇維度、選擇指標名稱，再選擇 Add to graph (新增至圖形)。

4. 選擇日期範圍的值。所選日期範圍的指標計數會顯示在圖形中。

使用 建立警示 CloudWatch

CloudWatch 警示會在指定的期間內監看單一指標，並執行一或多個動作：傳送通知至 Amazon Simple Notification Service (AmazonSNS) 主題或 Auto Scaling 政策。動作是以您指定的數個期間內相對於指定閾值的指標值為基礎。警示變更狀態時，CloudWatch 也可以傳送 Amazon SNS 訊息給您。

CloudWatch 只有在狀態變更且在您指定的期間持續存在時，警示才會叫用動作。

檢視指標 CloudWatch (主控台)

1. 登入 AWS 管理主控台，並開啟 [CloudWatch 主控台](#)。
2. 選擇 Alarms (警示)，然後選擇 Create Alarm (建立警示)。
3. 選擇 AWS/HealthLake，然後選擇指標。
4. 對於 Time Range (時間範圍)，選擇要監控的時間範圍，然後選擇 Next (下一步)。
5. 輸入 Name (名稱) 和 Description (描述)。
6. 針對常式，選擇 $\geq$ ，然後輸入最大值。
7. 如果您想要在達到警示狀態時 CloudWatch 傳送電子郵件，請在動作區段中，針對每當此警示，選擇狀態為 ALARM。對於傳送通知至，請選擇郵寄清單，或選擇新增清單並建立新的郵寄清單。
8. 在 Alarm Preview (警示預覽) 區段中預覽警示。如果警示符合您的要求，選擇 Create Alarm (建立警示)。

SMART 將 FHIR與 整合 AWS HealthLake

FHIR 啟用 HealthLake 資料存放區的可替代醫療應用程式和可重複使用技術 (SMART) 允許 SMARTFHIR合規應用程式存取儲存在 HealthLake 資料存放區中的資料。透過使用第三方授權伺服器驗證和授權請求，以及在其中設定其他資源，即可存取 HealthLake 資料 AWS。

若要在 SMART 上使用 FHIR搭配 HealthLake 資料存放區，您必須在 [CreateFHIRDatastore](#) API請求中提供下列項目。

- 將設定為[AuthorizationStrategy](#)等於 SMART_ON_FHIR_V1。
- 將設定為[IdpLambdaArn](#)等於 AWS Lambda 您建立ARN的，以使用授權伺服器管理權杖解碼。
- 定義授權伺服器中指定的[中繼資料](#)元素。這些中繼資料元素會在 Discovery Document 中傳回。如需進一步了解，請參閱 [在FHIR已啟用 HealthLake 資料存放區的探索文件SMART上擷取](#)。
- 選用：[FineGrainedAuthorizationEnabled](#)如果您已在授權伺服器上設定精細授權，請啟用。

您可以使用 AWS Command Line Interface (AWS CLI) 或透過其中一個 AWS 支援的，在FHIR啟用的資料存放SMART區上建立 SDKs。使用 HealthLake 主控台不支援在FHIR啟用 HealthLake 的資料存放SMART區上建立。如需進一步了解，請參閱 [在FHIR啟用的資料存放SMART區上建立](#)。

若要在請求中指定這些參數，您需要在其他 AWS 服務 (AWS Secrets Manager 和 AWS Lambda) 中設定資源、建立新的IAM服務角色，以及在SMARTFHIR合規的授權伺服器上設定。使用區段 [設定必要資源，以在FHIR合規的資料存放SMART區實作](#)，以進一步了解設定必要資源，並查看FHIR應用程式 SMART上 如何與 互動的高階概觀 HealthLake。

這表示 AWS Identity and Access Management 您不會透過 管理使用者登入資料，而是在SMARTFHIR合規的授權伺服器上使用。

HealthLake 支援 FHIR 1.0 SMART版。若要進一步了解此架構，請參閱[SMART應用程式啟動架構實作指南 1.0 版](#)。

若要在 SMART上使用 授權和驗證資料存放區的請求FHIR，HealthLake 支援使用：

- OpenID (AuthN) 整合：用於驗證該人員或用戶端應用程式是他們聲稱是誰（或什麼）。
- OAuth 2.0 (AuthZ) 整合：用於授權 HealthLake 資料存放區中的哪些FHIR資源，驗證的請求也可以讀取或寫入資料。這是由授權伺服器中設定的範圍所定義

內容

- [SMART 上的 的身分驗證需求 FHIR](#)
 - [在FHIR啟用 HealthLake 的資料存放SMART區上建立 所需的授權伺服器元素](#)
 - [在FHIR已啟用 HealthLake 的資料存放區SMART上完成FHIRRESTAPI請求所需的宣告](#)
- [支援SMARTFHIROAuth的範圍 HealthLake](#)
 - [獨立啟動範圍](#)
 - [HealthLake 資料存放區FHIR資源特定範圍](#)
- [使用 AWS Lambda 搭配FHIR啟用 SMART HealthLake 的資料存放區進行字符驗證](#)
 - [建立 AWS Lambda 函數](#)
 - [修改 Lambda 函數的執行角色](#)
 - [建立 HealthLake 服務角色，以用於解碼 的 AWS Lambda 函數 JWT](#)
 - [建立新的IAM政策](#)
 - [為 HealthLake \(IAM 主控台 \) 建立服務角色](#)
 - [Lambda 執行角色](#)
 - [允許 HealthLake 觸發您的 Lambda 函數](#)
 - [為您的 Lambda 函數佈建並行](#)
- [在FHIR已啟用 HealthLake 的資料存放區SMART上建立](#)
 - [使用 在FHIR啟用 HealthLake 的資料存放SMART區上 AWS CLI 建立](#)
- [在FHIR已啟用 HealthLake 的資料存放SMART區上使用精細授權](#)
- [在FHIR已啟用 HealthLake 資料存放區的探索文件SMART上擷取](#)
- [在SMART已啟用 HealthLake 的資料存放區提出FHIRRESTAPI請求](#)
- [設定在FHIR合規資料存放SMART區實作 所需的資源](#)
 - [用戶端應用程式如何在FHIR啟用資料存放區SMART上啟動和請求 HealthLake 上的資料](#)

SMART 上的 的身分驗證需求 FHIR

若要存取FHIR HealthLake 資料存放區SMART上的 中的FHIR資源，用戶端應用程式必須由 OAuth 2.0 合規的授權伺服器授權，並在FHIRRESTAPI請求中呈現 OAuth Bearer 權杖。若要尋找授權伺服器的端點，請透過 Well-Known Uniform Resource Identifier 使用 HealthLake SMARTFHIR探索文件上的 。若要進一步了解此程序，請參閱[在FHIR已啟用 HealthLake 資料存放區的探索文件SMART上擷取](#)。

當您SMART在FHIR HealthLake 資料存放區上建立時，您必須在 `CreateFHIRDatastore` 請求的 `metadata` 元素中定義授權伺服器的端點和字符端點。若要進一步了解定義 `metadata` 元素，請參閱 [在FHIR已啟用 HealthLake 的資料存放區SMART上建立](#)。

使用授權伺服器端點，用戶端應用程式將使用授權服務驗證使用者。一旦授權和驗證，授權服務會產生 JSON Web 權杖 (JWT)，並傳遞給用戶端應用程式。此權杖包含允許用戶端應用程式使用FHIR的資源範圍，進而限制使用者可存取的資料。或者，如果提供了啟動範圍，則回應將包含這些詳細資訊。若要進一步了解所支援FHIR範圍SMART的 HealthLake，請參閱 [支援SMARTFHIROAuth的範圍 HealthLake](#)。

使用授權伺服器JWT授予的，用戶端應用程式會在FHIR啟用 HealthLake 的資料存放SMART區上FHIRRESTAPI呼叫。若要驗證和解碼 JWT，您需要建立 Lambda 函數。收到FHIRRESTAPI請求時，會代表您 HealthLake 叫用此 Lambda 函數。若要查看入門 Lambda 函數範例，請參閱 [使用 AWS Lambda 搭配FHIR啟用 SMART HealthLake 的資料存放區進行字符驗證](#)。

在FHIR啟用 HealthLake 的資料存放SMART區上建立所需的授權伺服器元素

在 `CreateFHIRDatastore` 請求中，您需要提供授權端點和字符端點，做為 `IdentityProviderConfiguration` 物件中 `metadata` 元素的一部分。授權端點和權杖端點都是必要的。若要查看 `CreateFHIRDatastore` 請求中如何指定的範例，請參閱 [在FHIR已啟用 HealthLake 的資料存放區SMART上建立](#)。

在FHIR已啟用 HealthLake 的資料存放區SMART上完成FHIRRESTAPI請求所需的宣告

您的 AWS Lambda 函數必須包含下列宣告，才能在FHIR啟用 SMART HealthLake 的資料存放區上將其視為有效的FHIRRESTAPI請求。

- `nbf` : [\(非之前 \) 宣告](#) — "nbf" (非之前) 宣告會識別JWTMUSTNOT接受處理之前的時間。處理 "nbf" 宣告需要目前date/time MUST be after or equal to the not-before date/time列於 "nbf" 宣告中的。我們提供的 Lambda 函數範例iat會從伺服器回應轉換為 nbf。
- `exp` : [\(過期時間 \) 宣告](#) — 「過期」 (過期時間) 宣告會識別 當天或之後JWT的過期時間，而不得接受處理。
- `isAuthorized` : 布林值設定為 True。表示請求已在授權伺服器上獲得授權。
- `aud` : [\(對象 \) 宣告](#) — 「音訊」 (對象) 宣告會識別 JWT 要用於的收件人。這必須是FHIR啟用 HealthLake 資料存放區端點SMART的。
- `scope` : 這必須至少是一個FHIR資源相關範圍。此範圍在您的授權伺服器上定義。若要進一步了解接受FHIR的資源相關範圍 HealthLake，請參閱 [HealthLake 資料存放區FHIR資源特定範圍](#)。

支援SMARTFHIROAuth的範圍 HealthLake

HealthLake 使用 OAuth 2.0 做為授權通訊協定。在授權伺服器上使用此通訊協定，可讓您定義用戶端應用程式在 HealthLake 資料存放區中可以具有讀取和/或寫入存取權FHIR的資源。

FHIR 架構SMART上的 定義一組可以從授權伺服器請求的範圍。若要檢視FHIR架構SMART上 中的範圍定義，請參閱 HL7 FHIR 資源指南中的 [SMART FHIR 範圍](#)。

例如，僅設計為允許患者檢視其實驗室結果或檢視其聯絡詳細資訊的用戶端應用程式，應僅獲授權請求（透過FHIRREST請求）read範圍。若要將這些定義為範圍，您會提供類似下列的字串patient/Observation.read。這可讓用戶端應用程式以唯讀方式請求存取Observation資源類型Patient。

獨立啟動範圍

HealthLake 支援獨立啟動模式範圍 launch/patient。

在獨立啟動模式中，用戶端應用程式會請求存取病患的臨床資料，因為用戶端應用程式不知道使用者和病患。因此，用戶端應用程式的授權請求會明確請求傳回病患範圍。身分驗證成功後，授權伺服器會發出存取字符，其中包含請求的啟動病患範圍。所需的病患內容會與 授權伺服器回應中的存取權杖一起提供。

支援的啟動模式範圍

範圍	描述
launch/patient	2.0 OAuth 授權請求中的參數，要求在授權回應中傳回該病患資料。

HealthLake 資料存放區FHIR資源特定範圍

HealthLake 定義三個層級的範圍。

- 病患特定範圍會授予單一病患特定資料的存取權。在啟動內容中指定了哪些病患。
- 使用者層級範圍會授予使用者可存取的特定資料的存取權。
- 系統層級範圍會授予 HealthLake 資料存放區中所有FHIR資源的讀取/寫入存取權。

下表顯示建構 支援之FHIR資源相關範圍的語法 HealthLake。一般格式如下：

```
( 'patient' | 'user' | 'system' ) '/' ( fhir-resource | '*' ) '.' ( 'read' | 'write' | '*' )
```

HealthLake 資料存放區上支援的授權範圍

範圍語法	範例範圍	結果
patient/(fhir-resource '*').('read' 'write' '*')	patient/AllergyIntolerance.*	用戶端應用程式可以讀取/寫入對過敏的存取權。
user/(fhir-resource '*').('read' 'write' '*')	user/Observation.read	用戶端應用程式將具有所有記錄觀察的讀取存取權。
system/('read' 'write' '*')	system/*.*	用戶端應用程式可以讀取/寫入所有資料。

使用 AWS Lambda 搭配 FHIR 啟用 SMART HealthLake 的資料存放區進行字符驗證

當您在 FHIR 啟用 HealthLake 的資料存放 SMART 區上建立時，您需要在 `CreateFHIRDatastore` 請求中提供 AWS Lambda 函數 ARN。Lambda 函數的 ARN 是使用 `IdpLambdaArn` 參數在 `IdentityProviderConfiguration` 物件中指定。

您必須先建立 Lambda 函數，才能在 FHIR 啟用 HealthLake 的資料存放 SMART 區上建立。建立資料存放區後，就 ARN 無法變更 Lambda。若要查看 ARN 您在建立資料存放區時指定的 Lambda，請使用 `DescribeFHIRDatastoreAPI` 操作。

若要在 FHIR 啟用 SMART HealthLake 的資料存放區上成功 FHIR REST 請求，您的 Lambda 函數需要執行下列動作：

- Lambda 函數必須在 1 秒內將回應傳回至 HealthLake 資料存放區端點。
- 解碼用戶端應用程式所傳送 REST API 請求的授權標頭中提供的存取字符。
- 指派具有足夠許可可執行 FHIR REST API 請求 IAM 的服務角色。
- 需要下列宣告才能完成 FHIR REST API 請求。如需進一步了解，請參閱 [必要的宣告](#)。

- nbf
- exp
- isAuthorized
- aud
- scope

使用 Lambda 時，除了 Lambda 函數之外，還需要建立執行角色和資源型政策。Lambda 函數的執行角色是授予函數存取執行時間所需AWS服務和資源的許可IAM。您提供的資源型政策必須允許 代表您 HealthLake 叫用您的 函數。

本主題中的各節說明來自用戶端應用程式和解碼回應的範例請求、建立 AWS Lambda 函數所需的步驟，以及如何建立 HealthLake 可擔任的資源型政策。

- [第 1 部分：建立 Lambda 函數](#)
- [第 2 部分：建立 AWS Lambda 函數使用 HealthLake 的服務角色](#)
- [第 3 部分：更新 Lambda 函數的執行角色](#)
- [第 4 部分：將資源政策新增至 Lambda 函數](#)
- [第 5 部分：為您的 Lambda 函數佈建並行](#)

建立 AWS Lambda 函數

HealthLake 收到FHIR啟用 SMART HealthLake 資料存放區的請求時，會觸發在此主題中建立的 Lambda 函數。來自用戶端應用程式的請求包含RESTAPI呼叫，以及包含存取權杖的授權標頭。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Authorization: Bearer i8hweunweunweofiwweoijewiwe
```

本主題中的範例 Lambda AWS Secrets Manager 函數用於隱藏與授權伺服器相關的登入資料。我們強烈建議不要直接在 Lambda 函數中提供授權伺服器登入詳細資訊。

Example 驗證包含授權持有者權杖的FHIRREST請求

Lambda 函數範例示範如何在FHIR啟用 HealthLake 資料存放SMART區上驗證傳送至 的FHIRREST請求。若要查看 step-by-steps如何實作此 Lambda 函數的指示，請參閱 [使用 建立 Lambda 函數 AWS Management Console](#)。

如果FHIRRESTAPI請求不包含有效的資料存放區端點、存取權杖和REST操作，Lambda 函數將會失敗。若要進一步了解必要的授權伺服器元素，請參閱 [必要的宣告](#)。

```
import base64
import boto3
import logging
import json
import os
from urllib import request, parse

logger = logging.getLogger()
logger.setLevel(logging.INFO)

## Uses Secrets manager to gain access to the access key ID and secret access key for
the authorization server
client = boto3.client('secretsmanager', region_name="region-of-datastore")
response = client.get_secret_value(SecretId='name-specified-by-customer-in-
secretsmanager')
secret = json.loads(response['SecretString'])
client_id = secret['client_id']
client_secret = secret['client_secret']

unencoded_auth = f'{client_id}:{client_secret}'
headers = {
    'Authorization': f'Basic {base64.b64encode(unencoded_auth.encode()).decode()}',
    'Content-Type': 'application/x-www-form-urlencoded'
}

auth_endpoint = os.environ['auth-server-base-url'] # Base URL of the Authorization
server
user_role_arn = os.environ['iam-role-arn'] # The IAM role client application will use
to complete the HTTP request on the datastore

def lambda_handler(event, context):
    if 'datastoreEndpoint' not in event or 'operationName' not in event or
'bearerToken' not in event:
        return {}

    datastore_endpoint = event['datastoreEndpoint']
    operation_name = event['operationName']
    bearer_token = event['bearerToken']
```

```

    logger.info('Datastore Endpoint [{}], Operation Name:
    [{}]'.format(datastore_endpoint, operation_name))

    ## To validate the token
    auth_response = auth_with_provider(bearer_token)
    logger.info('Auth response: [{}]'.format(auth_response))
    auth_payload = json.loads(auth_response)
    ## Required parameters needed to be sent to the datastore endpoint for the HTTP
    request to go through
    auth_payload["isAuthorized"] = bool(auth_payload["active"])
    auth_payload["nbf"] = auth_payload["iat"]
    return {"authPayload": auth_payload, "iamRoleARN": user_role_arn}

## access the server
def auth_with_provider(token):
    data = {'token': token, 'token_type_hint': 'access_token'}
    req = request.Request(url=auth_endpoint + '/v1/introspect',
    data=parse.urlencode(data).encode(), headers=headers)
    with request.urlopen(req) as resp:
        return resp.read().decode()

```

使用 建立 Lambda 函數 AWS Management Console

此程序假設您已在SMARTFHIR已啟用 HealthLake 的資料存放區上處理FHIRRESTAPI請求時，建立 HealthLake 您要擔任的服務角色。如果您尚未建立服務角色，您仍然可以建立 Lambda 函數。您需要先新增服務角色ARN的，Lambda 函數才能運作。若要進一步了解如何建立服務角色並在 Lambda 函數中指定該角色，請參閱：[建立 HealthLake 服務角色，以用於解碼的 AWS Lambda 函數 JWT](#)

建立 Lambda 函數 (AWS Management Console)

1. 開啟 Lambda 主控台中的 [函數頁面](#)。
2. 選擇 建立函數。
3. 選取從頭開始撰寫。
4. 在基本資訊下，輸入函數名稱。在執行時間下選擇以 python 為基礎的執行時間。
5. 執行角色 請選擇 建立具備基本 Lambda 許可的新角色。

Lambda 會建立[執行角色](#)，授予函數將日誌上傳至 Amazon 的許可 CloudWatch。Lambda 函數會在您叫用函數時擔任執行角色，並使用執行角色來建立的登入資料 AWS SDK。

6. 選擇程式碼索引標籤，然後新增範例 Lambda 函數。

如果您尚未為 Lambda 函數建立要使用的服務角色，則需要先建立該角色，範例 Lambda 函數才能運作。若要進一步了解如何為 Lambda 函數建立服務角色，請參閱 [建立 HealthLake 服務角色，以用於解碼的 AWS Lambda 函數 JWT](#)。

```
import base64
import boto3
import logging
import json
import os
from urllib import request, parse

logger = logging.getLogger()
logger.setLevel(logging.INFO)

## Uses Secrets manager to gain access to the access key ID and secret access key
for the authorization server
client = boto3.client('secretsmanager', region_name="region-of-datastore")
response = client.get_secret_value(SecretId='name-specified-by-customer-in-secretsmanager')
secret = json.loads(response['SecretString'])
client_id = secret['client_id']
client_secret = secret['client_secret']

unencoded_auth = f'{client_id}:{client_secret}'
headers = {
    'Authorization': f'Basic {base64.b64encode(unencoded_auth.encode()).decode()}',
    'Content-Type': 'application/x-www-form-urlencoded'
}

auth_endpoint = os.environ['auth-server-base-url'] # Base URL of the Authorization
server
user_role_arn = os.environ['iam-role-arn'] # The IAM role client application will
use to complete the HTTP request on the datastore

def lambda_handler(event, context):
    if 'datastoreEndpoint' not in event or 'operationName' not in event or
    'bearerToken' not in event:
        return {}

    datastore_endpoint = event['datastoreEndpoint']
    operation_name = event['operationName']
```

```

bearer_token = event['bearerToken']
logger.info('Datastore Endpoint [{}], Operation Name:
[{}]' .format(datastore_endpoint, operation_name))

## To validate the token
auth_response = auth_with_provider(bearer_token)
logger.info('Auth response: [{}]' .format(auth_response))
auth_payload = json.loads(auth_response)
## Required parameters needed to be sent to the datastore endpoint for the HTTP
request to go through
auth_payload["isAuthorized"] = bool(auth_payload["active"])
auth_payload["nbf"] = auth_payload["iat"]
return {"authPayload": auth_payload, "iamRoleARN": user_role_arn}

## Access the server
def auth_with_provider(token):
    data = {'token': token, 'token_type_hint': 'access_token'}
    req = request.Request(url=auth_endpoint + '/v1/introspect',
data=parse.urlencode(data).encode(), headers=headers)
    with request.urlopen(req) as resp:
        return resp.read().decode()

```

修改 Lambda 函數的執行角色

建立 Lambda 函數後，您需要更新執行角色，以包含呼叫 Secrets Manager 的必要許可。在 Secrets Manager 中，您建立的每個秘密都有 ARN。若要套用最低權限，執行角色應只能存取 Lambda 函數執行所需的資源。

您可以在 IAM 主控台中搜尋 Lambda 函數，或在 Lambda 主控台中選擇組態，以修改 Lambda 函數的執行角色。若要進一步了解如何管理 Lambda 函數執行角色，請參閱 [Lambda 執行角色](#)。

Example 授予 存取權的 Lambda 函數執行角色 **GetSecretValue**

將 IAM 動作新增至 GetSecretValue 執行角色，會授予範例 Lambda 函數運作所需的許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",

```

```
"Resource": "arn:aws:secretsmanager:your-region:your-aws-account-  
id:secret:secret-name-DKodTA"  
  }  
]  
}
```

此時，您已建立 Lambda 函數，可用於驗證在 FHIR 啟用 HealthLake 資料存放 SMART 區時傳送至您之 FHIR REST 請求中提供的存取字符。

建立 HealthLake 服務角色，以用於解碼的 AWS Lambda 函數 JWT

角色：IAM 管理員

可新增或移除 IAM 政策，並建立新 IAM 身分的使用者。

服務角色

服務角色是 [IAM](#) 服務擔任的角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 《使用者指南》中的 [建立角色以將許可委派給 AWS 服務](#)。

JSON 在 Web 權杖 (JWT) 解碼後，Lambda 也需要傳回 IAM 角色的授權 ARN。此角色必須具有執行 REST API 請求的必要許可，否則會因為許可不足而失敗。

使用 設定自訂政策時 IAM，最好授予所需的最低許可。若要進一步了解，請參閱 IAM 《使用者指南》中的 [套用最低權限許可](#)。

建立要在授權 Lambda 函數中指定的 HealthLake 服務角色需要兩個步驟。

- 首先，您需要建立 IAM 政策。政策必須指定您在授權伺服器中為 提供範圍 FHIR 的資源存取權。
- 其次，您需要建立服務角色。當您建立角色時，您可以指定信任關係，並連接您在步驟 1 中建立的政策。信任關係會指定 HealthLake 為服務主體。在此步驟中，您需要指定 HealthLake 資料存放區 ARN 和 AWS 帳戶 ID。

建立新的 IAM 政策

您在授權伺服器中定義的範圍會決定已驗證的使用者在 HealthLake 資料存放區中可存取哪些 FHIR 資源。

您建立IAM的政策可以根據您定義的範圍量身打造。

您可以在IAM政策陳述式的 Action元素中定義下列動作。您可以針對Action表格中的每個 定義 Resource types。在 HealthLake 資料存放區中，是唯一可在IAM許可政策陳述式的 Resource元素中定義的支援資源類型。

個別FHIR資源不是您可以定義為IAM許可政策中 元素的資源。

由 定義的動作 HealthLake

動作	描述	存取層級	資源類型 (必要)
CreateResource	准許建立資源	寫入	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>
DeleteResource	准許刪除資源	寫入	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>
ReadResource	准許讀取資源	讀取	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>
SearchWithGet	准許使用 GET方法搜尋資源	讀取	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>
SearchWithPost	准許使用 POST方法搜尋資源	讀取	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>
StartFHIRExportJobWithPost	准許使用 開始FHIR匯出任務 GET	寫入	資料存放區ARN : <code>arn : aws : healthlakeyour-region : 111122223333 : datastore/fhir/your-datastore-id</code>

動作	描述	存取層級	資源類型 (必要)
UpdateResource	准許更新資源	寫入	資料存放區ARN : <code>arn : aws : healthlake:your-region : 111122223333 : datastore/fhir/your-datastore-id</code>

若要開始使用，您可以使用 `AmazonHealthLakeFullAccess`。此政策會授予資料存放區中所有FHIR資源的讀取、寫入、搜尋和匯出。若要授予資料存放區的唯讀許可，請使用 `AmazonHealthLakeReadOnlyAccess`。

若要進一步了解如何使用 AWS Management Console AWS CLI或 IAM 建立自訂政策SDKs，請參閱IAM 《使用者指南》中的[建立IAM](#)政策。

為 HealthLake (IAM 主控台) 建立服務角色

使用此程序來建立服務角色。建立服務時，您也需要指定 IAM政策。

建立 HealthLake (IAM 主控台) 的服務角色

1. 登入 AWS Management Console 並在 開啟IAM主控台<https://console.aws.amazon.com/iam/>。
2. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)。
3. 然後，選擇 Create role (建立角色)。
4. 在選取信任實體頁面上，選擇自訂信任政策。
5. 接著，在自訂信任政策下，更新範例政策，如下所示。**your-account-id** 將取代為您的帳戶號碼，並新增您要用於匯入或匯出任務的資料存放ARN區的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "Service": "healthlake.amazonaws.com"
      },
    },
  ],
}
```

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "your-account-id"
  },
  "ArnEquals": {
    "aws:SourceArn": "arn:aws:healthlake:your-region:your-account-id:datastore/fhir/your-datastore-id"
  }
}
]
```

6. 然後選擇下一步。
7. 在新增許可頁面上，選擇您希望 HealthLake 服務擔任的政策。若要尋找您的政策，請在許可政策下搜尋。
8. 然後，選擇連接政策。
9. 然後在 名稱 中，檢閱角色名稱 下的建立頁面，然後輸入名稱。
10. (選用) 接著在描述下，為您的角色新增簡短描述。
11. 如果可能，請輸入角色名稱或角色名稱字尾，以協助您識別此角色的用途。角色名稱在您的 中必須是唯一的 AWS 帳戶。它們無法透過大小寫進行區分。例如，您無法建立名為 **PRODRole** 和 **prodrrole** 的角色。因為有各種實體可能會參照角色，所以您無法在建立角色之後編輯角色名稱。
12. 檢閱角色詳細資訊，然後選擇建立角色。

若要了解如何在範例 Lambda 函數ARN中指定角色，請參閱 [建立 AWS Lambda 函數](#)。

Lambda 執行角色

Lambda 函數的執行角色是授予函數存取 AWS 服務和資源的許可IAM。本頁提供有關如何建立、檢視和管理 Lambda 函數執行角色的資訊。

根據預設，當您使用 建立新的 Lambda 函數時，Lambda 會建立具有最少許可的執行角色 AWS Management Console。若要管理執行角色中授予的許可，請參閱 Lambda 開發人員指南中的[在 IAM 主控台中建立執行角色](#)。

本主題中提供的 Lambda 函數範例使用 Secrets Manager 來隱藏授權伺服器的憑證。

如同您建立的任何IAM角色，遵循最低權限最佳實務非常重要。在開發片語期間，有時您可能會授予超出必要範圍的許可。在生產環境中發佈您的函數之前，最佳實務是調整政策以僅包含必要的許可。如需詳細資訊，請參閱IAM《使用者指南》中的[套用最低權限](#)。

允許 HealthLake 觸發您的 Lambda 函數

因此，HealthLake 可以代表您叫用 Lambda 函數，您必須執行下列動作：

- 您需要將設定為IdpLambdaArn等於 HealthLake 要在CreateFHIRDatastore請求中呼叫ARN的 Lambda 函數的。
- 您需要以資源為基礎的政策 HealthLake，允許代表您叫用 Lambda 函數。

當 SMART 在FHIR已啟用 HealthLake 的資料存放區上 HealthLake 收到FHIRRESTAPI請求時，它需要許可，才能代表您叫用資料存放區建立時指定的 Lambda 函數。若要授予 HealthLake 存取權，您將使用以資源為基礎的政策。若要進一步了解如何為 Lambda 函數建立以資源為基礎的政策，請參閱《AWS Lambda 開發人員指南》中的[允許 AWS 服務呼叫 Lambda 函數](#)。

為您的 Lambda 函數佈建並行

Important

HealthLake 需要 Lambda 函數的最大執行時間少於一秒 (1000 毫秒)。
如果您 Lambda 函數超過執行時間限制，您會收到TimeOut例外狀況。

為了避免發生此例外狀況，建議您設定佈建並行。您可以在增加呼叫前配置佈建並行，來確保所有請求均由具有低延遲的初始化執行個體所提供。若要進一步了解如何設定佈建並行，請參閱 Lambda 開發人員指南中的[設定佈建並行](#)

若要查看 Lambda 函數的平均執行時間，目前請使用 Lambda 主控台上 Lambda 函數的監控頁面。根據預設，Lambda 主控台會提供持續時間圖表，顯示函數程式碼處理事件的平均、最短和最長時間。若要進一步了解監控 Lambda 函數，請參閱 [Lambda 開發人員指南中的 Lambda 主控台中的監控函數](#)。

如果您已為 Lambda 函數佈建並行，並想要監控它，請參閱 Lambda 開發人員指南中的[監控並行](#)。

在FHIR已啟用 HealthLake 的資料存放區SMART上建立

若要搭配 使用FHIR架構SMART上的 HealthLake，請使用 `CreateFHIRDatastore` 請求中指定的 `IdentityProviderConfiguration` 參數建立 HealthLake 資料存放區。在 `IdentityProviderConfiguration` 參數中，您指定下列資訊：

- 將 設定為 [AuthorizationStrategy](#) 等於 `SMART_ON_FHIR_V1`。
- 將 設定為 [IdpLambdaArn](#) 等於 AWS Lambda 您建立ARN的，以使用授權伺服器管理權杖解碼。
- 將授權伺服器中指定的 [中繼資料](#) 元素定義為JSON區塊。這些中繼資料元素會在 Discovery Document 中傳回。
- 選用：啟用 [FineGrainedAuthorizationEnabled](#)。指定 `True` 使用 提供的精細授權 HealthLake

您可以使用 AWS Command Line Interface (AWS CLI) 或透過其中一個 AWS 支援的，在FHIR啟用的資料存放SMART區上建立 SDKs。使用 HealthLake 主控台不支援SMART在FHIR啟用 HealthLake 的資料存放區上建立。

使用 在FHIR啟用 HealthLake 的資料存放SMART區上 AWS CLI 建立

您可以使用下列程式碼範例，使用 在FHIR已啟用 HealthLake 的資料存放區SMART上建立 AWS CLI。在FHIR啟用 HealthLake 的資料存放SMART區上建立 時，您必須指定 [identity-provider-configuration](#) 參數。

在 `identity-provider-configuration` 參數中，您可以選擇性地啟用精細授權，方法是將 設定為 `FineGrainedAuthorizationEnabled` 等於 `True`。若要進一步了解精細授權，請參閱 [在FHIR已啟用 HealthLake 的資料存放SMART區上使用精細授權](#)。以下範例包含一個特殊字元 `\`，以指示換行或做為逸出字元。這是為了清楚起見。

```
aws healthlake create-fhir-datastore \
  --region us-east-1 \
  --datastore-name "your-data-store-name" \
  --datastore-type-version R4 \
  --preload-data-config PreloadDataType="SYNTHEA" \
  --sse-configuration '{ "KmsEncryptionConfig": { \
    "CmkType": "customer-managed-kms-key1", \
    "KmsKeyId": "arn:aws:kms:us-east-1:your-account-id:key/your-key-id" } }' \
  --identity-provider-configuration \
    '{"AuthorizationStrategy": "SMART_ON_FHIR_V1", \
    "FineGrainedAuthorizationEnabled": boolean-false-by-default, \
```

```

    "IdpLambdaArn": "arn:aws:lambda:your-region:your-account-id:function:your-lambda-name" \
    "Metadata": "{\"issuer\": \"https://ehr.example.com\", \"jwks_uri\": \"https://ehr.example.com/.well-known/jwks.json\", \"authorization_endpoint\": \"https://ehr.example.com/auth/authorize\", \"token_endpoint\": \"https://ehr.token.com/auth/token\", \"token_endpoint_auth_methods_supported\": [\"client_secret_basic\", \"foo\"], \"grant_types_supported\": [\"client_credential\", \"foo\"], \"registration_endpoint\": \"https://ehr.example.com/auth/register\", \"scopes_supported\": [\"openid\", \"profile\", \"launch\"], \"response_types_supported\": [\"code\"], \"management_endpoint\": \"https://ehr.example.com/user/manage\", \"introspection_endpoint\": \"https://ehr.example.com/user/introspect\", \"revocation_endpoint\": \"https://ehr.example.com/user/revoke\", \"code_challenge_methods_supported\": [\"S256\"], \"capabilities\": [\"launch-ehr\", \"sso-openid-connect\", \"client-public\"]}"'

```

成功時，您會收到下列JSON回應：

```

{
  "DatastoreArn": "arn:aws:healthlake:your-region:111122223333:datastore/fhir/your-datastore-id",
  "DatastoreEndpoint": "https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/",
  "DatastoreId": "your-data-store-id",
  "DatastoreStatus": "data-store-creation-status"
}

```

在FHIR已啟用 HealthLake 的資料存放SMART區上使用精細授權

僅 [Scopes](#) 就請求者有權在資料存放區中存取的資料而言，並不會為您提供必要的具體性。使用精細授權可在FHIR啟用 HealthLake 的資料存放SMART區授予存取權時，實現更高層級的特異性。若要使用精細授權，請在 `CreateFHIRDatastore` 請求的 `IdentityProviderConfiguration` 參數 `True` 中將設定為 `FineGrainedAuthorizationEnabled` 等於。

如果您啟用精細授權，您的授權伺服器會傳回 `fhirUser` 範圍 `id_token` 以及存取權杖。這允許用戶端應用程式擷取有關使用者的資訊。用戶端應用程式應將 `fhirUser` 宣告視為代表目前使用者FHIR的資源URI的。此值可以為 `Patient`、`Practitioner` 或 `RelatedPerson`。授權伺服器的回應也包含定義使用者可存取哪些資料 `user/` 的範圍。這會使用針對與FHIR資源特定範圍相關的範圍定義的語法：

```
user/(fhir-resource | '*').('read' | 'write' | '*')
```

以下是如何使用精細授權進一步指定資料存取相關FHIR資源類型的範例。

- 當 `fhirUser` 是 `Practitioner`，精細授權會決定使用者可存取的患者集合。`fhirUser` 僅允許病患參考 `fhirUser` 作為一般從業人員的那些病患存取。

```
Patient.generalPractitioner : [{Reference(Practitioner)}]
```

- 當 `fhirUser` 是 `Patient` 或 `RelatedPerson` 且請求中參考的患者與不同時 `fhirUser`，精細授權會決定請求患者對 `fhirUser` 的存取。在請求 `Patient` 的資源中指定關係時，允許存取。

```
Patient.link.other : {Reference(Patient|RelatedPerson)}
```

在FHIR已啟用 HealthLake 資料存放區的探索文件SMART上擷取

若要讓用戶端應用程式提出成功的FHIRREST請求，它需要收集 HealthLake 資料存放區中定義的授權要求。此請求不需要授權（熊字符）即可成功。

若要這樣做，請提出GET請求並附加 `/.well-known/smart-configuration` 到資料存放區的端點

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/.well-known/smart-configuration
```

這會將 HealthLake 資料存放區的探索文件傳回為 JSON Blob。您可以在其中找到 `authorization_endpoint` 和 `token_endpoint` 以及 HealthLake 資料存放區中定義的規格和功能。

```
{
  "authorization_endpoint": "https://oidc.example.com/authorize",
  "token_endpoint": "https://oidc.example.com/oauth/token",
  "capabilities": [
    "launch-ehr",
    "client-public"
  ]
}
```

URLs 成功啟動用戶端應用程式時需要

- 授權端點：授權用戶端應用程式或使用者URL所需的。
- 權杖端點：用戶端應用程式用來與其通訊的授權伺服器的端點。

在SMART已啟用 HealthLake 的資料存放區提出FHIRRESTAPI請求

您可以在FHIR啟用 SMART HealthLake 的資料存放區上提出FHIRRESTAPI請求。下列範例顯示來自用戶端應用程式的請求，其中包含授權標頭JWT中的，以及 Lambda 應如何解碼回應。用戶端應用程式請求經過授權和驗證後，必須從授權伺服器收到承載符記。在FHIR啟用 SMART HealthLake 的資料存放區傳送FHIRRESTAPI請求時，請使用授權標頭中的承載符記。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/  
Patient/[ID]  
Authorization: Bearer auth-server-provided-bearer-token
```

因為在授權標頭中找到承載符記，而且沒有 AWS IAM偵測到任何身分，因此在建立FHIR啟用 SMART HealthLake 的資料存放區時，會 HealthLake 叫用指定的 Lambda 函數。當您的 Lambda 函數成功解碼字符時，此處是傳送至 的範例回應 HealthLake。

```
{  
  "authPayload": {  
    "iss": "https://authorization-server-endpoint/oauth2/token", # The issuer  
    identifier of the authorization server  
    "aud": "https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/  
r4/", # Required, data store endpoint  
    "iat": 1677115637, # Identifies the time at which the token was issued  
    "nbf": 1677115637, # Required, the earliest time the JWT would be valid  
    "exp": 1997877061, # Required, the time at which the JWT is no longer valid  
    "isAuthorized": "true", # Required, boolean indicating the request has been  
    authorized  
    "uid": "100101", # Unique identifier returned by the auth server  
    "scope": "system/*.*" # Required, the scope of the request  
  },  
  "iamRoleARN": "iam-role-arn" #Required, IAM role to complete the request  
}
```

設定在FHIR合規資料存放SMART區實作 所需的資源

本主題說明您在外部 AWS 帳戶中佈建 所需的資源 HealthLake、在FHIR啟用 HealthLake 的資料存放區SMART上建立，以及在FHIR用戶端應用程式SMART上 如何與授權伺服器和 HealthLake 資料存放區互動。

此工作流程中的步驟會定義處理SMARTFHIR請求的基本步驟，以及成功所需的資源。

在 SMART FHIR請求程序中，三個應用程式可一起運作：

- 最終使用者：通常，使用FHIR應用程式SMART上的第三方來存取資料存放區中的 HealthLake 資料的患者或臨床醫生。
- SMART FHIR 應用程式上的（稱為用戶端應用程式）：想要存取 HealthLake 資料存放區中資料的應用程式。
- 授權伺服器：符合 OpenID Connect 標準的伺服器，能夠驗證使用者並發出存取字符。
- HealthLake 資料存放區：在FHIR啟用 HealthLake 的資料存放區SMART上，使用 Lambda 函數來回應提供承載符記的FHIRREST請求。

若要讓這些應用程式一起運作，您需要建立下列資源。

我們建議您SMART在設定授權伺服器、定義必要的範圍，並建立 AWS Lambda 函數來處理字符檢查之後，在FHIR已啟用 HealthLake 的資料存放區上建立。

1. 設定授權伺服器端點 — 授權伺服器

若要在FHIR架構SMART上使用，您需要設定第三方授權伺服器，以驗證在資料存放區上提出的 FHIRREST請求。若要進一步了解設定將使用的授權伺服器端點 HealthLake，請參閱 [SMART 上的 身分驗證需求 FHIR](#)。

2. 定義範圍以控制誰可以存取授權伺服器上 HealthLake 資料存放區中的哪些資料：授權伺服器

FHIR 架構SMART上的 使用OAuth範圍來判斷已驗證請求可存取FHIR的資源，以及存取的程度。定義範圍是為最低權限設計的一種方式。若要進一步了解FHIR架構SMART上 和 所支援之 定義的範圍，HealthLake 請參閱 [支援SMARTFHIROAuth的範圍 HealthLake](#)。

3. 設定能夠執行權杖檢查的 AWS Lambda 函數 - AWS 您的帳戶

用戶端應用程式在FHIR已啟用 SMART 的資料存放區上傳送的FHIRREST請求將包含 JSON Web 權杖 (JWT)。若要進一步了解如何設定能夠解碼和驗證 Lambda 函數，請參閱[解碼 JWT](#)。

4. 在FHIR啟用 HealthLake 的資料存放SMART區上建立 - AWS 您的帳戶

若要在FHIR HealthLake 資料存放區SMART上建立，您需要提供 IdentityProviderConfiguration。若要進一步了解 CreateFHIRDatastore 請求中所需的IdentityProviderConfiguration參數，請參閱[在FHIR啟用 HealthLake 的資料存放區SMART上建立](#)。

用戶端應用程式如何在FHIR啟用資料存放區SMART上啟動和請求 HealthLake 上的資料

本節說明用戶端應用程式如何在 SMART FHIR 內容中使用 啟動，並能夠在 HealthLake 資料存放區上提出成功的FHIRREST請求。

1. 用戶端應用程式向 Well-Known Uniform Resource Identifier 提出GET請求

SMART 已啟用的用戶端應用程式需要提出GET請求，才能尋找 HealthLake 資料存放區的授權端點。這是透過 Well-Known Uniform Resource Identifier (URI) 請求來完成的。若要進一步了解，請參閱在[FHIR已啟用 HealthLake 資料存放區的探索文件SMART上擷取](#)。

2. 請求存取和範圍

用戶端應用程式使用授權伺服器的授權端點，讓使用者可以登入。此程序會驗證使用者。範圍用於定義用戶端應用程式可以存取 HealthLake 的資料存放區中的哪些FHIR資源。若要進一步了解定義範圍，請參閱 [支援SMARTFHIROAuth的範圍 HealthLake](#)。

3. 存取權杖

現在使用者已通過身分驗證，用戶端應用程式會從授權伺服器接收JWT存取權杖。當用戶端應用程式傳送FHIRREST請求至 時，會提供此字符 HealthLake。若要進一步了解如何使用 Lambda 函數解碼 JWT，請參閱 [執行權杖驗證](#)。

4. 在FHIR已啟用 HealthLake 的資料存放SMART區上提出FHIRREST請求

現在，用戶端應用程式可以使用授權伺服器提供的存取權杖，將FHIRREST請求傳送至 HealthLake 資料存放區端點。若要查看範例FHIRREST請求，請參閱 [在SMART已啟用 HealthLake 的資料存放區提出FHIRRESTAPI請求](#)。

5. 驗證JWT存取權杖

若要驗證FHIRREST請求中傳送的存取權杖，請使用 Lambda 函數。若要了解如何建立可執行權杖簡介的 Lambda 函數，請參閱 [建立 AWS Lambda 函數](#)。

根據 中資源類型的自然語言處理 (NLP)，使用自動產生FHIR DocumentReference 資源 AWS HealthLake

Note

在 2023 年 2 月 20 日之後，HealthLake 資料存放區預設不會使用整合的自然語言處理 (NLP)。如果您有興趣在資料存放區上開啟此功能，請參閱疑難排解章節[如何開啟 HealthLake 整合的自然語言處理功能？](#)中的。

如果您已開啟 Amazon Comprehend Medical 的整合 NLP，則當您建立或更新 DocumentReference 資源時，會在 AWS 您的帳戶中產生費用。如需詳細資訊，請參閱[AWS HealthLake 定價](#)。

Amazon Comprehend Medical 不適用於亞太區域（孟買）。在亞太區域（孟買）區域建立 HealthLake 的資料存放區不支援整合的自然語言處理 (NLP)。

HealthLake 會自動為您提供整合的自然語言處理 (NLP)，使用 Amazon Comprehend Medical 處理 DocumentReference 資源類型中所存放資料的非結構化資料處理。若要這樣做，請 HealthLake 呼叫 Amazon Comprehend Medical DetectEntities-V2、InferICD10-CM 和 InferRxNorm API 操作。結果會自動附加到 DocumentReference 資源做為延伸。當 Amazon Comprehend Medical API 操作偵測到 SIGN、SYMPTOM 和的特徵 DIAGNOSIS 時，會自動產生 Linkage 資源類型。新條件和觀察資源是從以 SIGN、SYMPTOM 或 特徵識別的實體建立 DIAGNOSIS，它們會連結到具有此連結資源的來源文件。

對於整合所產生的資源 NLP，您可以提出 GET 請求，但不支援搜尋這些新資源。

若要進一步了解如何使用 與 Athena HealthLake 的整合來搜尋這些延伸模組，請參閱 [使用 查詢 HealthLake 您的資料存放區 SQL](#)。

內容

- [Amazon Comprehend Medical 如何與 整合 HealthLake](#)
 - [與 FHIR REST API 操作整合](#)
 - [Amazon Comprehend Medical API 操作如何整合到 中的範例 HealthLake](#)
- [搜尋參數](#)

Amazon Comprehend Medical 如何與 整合 HealthLake

HealthLake 使用 Amazon Comprehend Medical 推斷 DocumentReference 資源類型中找到的資料。Amazon Comprehend Medical API 操作 DetectEntities-V2、InferICD10-CM 和 InferRxNorm 會將醫療情況 InferRxNorm 偵測為特徵。每個操作都提供不同的洞見。

語言支援

Amazon Comprehend Medical API 操作只會偵測英文文字的醫療實體。

- DetectEntities-V2：檢查各種醫療實體的臨床文字，並傳回其特定資訊，例如實體類別、位置和可信度分數。
- InferICD10-CM：將病患記錄中的醫療情況偵測為實體，並將這些實體連結至 ICD-10-CM 知識庫中的標準化概念識別符，該知識庫來自 CDC 經世界衛生組織 (WHO) 授權的國家健康統計中心。
- InferRxNorm：將藥物偵測為患者記錄中列出的實體，並將其連結至 RxNorm 國家醫學圖書館資料庫中的標準化概念識別符。

每個 API 操作支援的特徵為 SIGN、SYMPTOM 和 DIAGNOSIS。如果偵測到特徵，則會將其新增為 HealthLake 資料存放區中不同位置的 FHIR 合規延伸。

新增擴充功能的位置。

- DocumentReference：Amazon Comprehend Medical API 操作的結果會新增為 DocumentReference 資源類型中找到 extension 的每個文件的。延伸模組中的結果分為兩個群組。您可以根據其，在結果中找到它們 URL。
 - <http://healthlake.amazonaws.com/system-generated-resources/>
 - 這些是 建立或新增至 的資源類型 HealthLake。
 - <http://healthlake.amazonaws.com/aws-cm/>
 - 將 Amazon Comprehend Medical API 操作的原始輸出新增至 HealthLake 您的資料存放區的位置。
- Linkage：此資源類型會因為整合的而新增或建立 NLP。特定上的 GET 請求會 Linkage 傳回連結資源清單。若要識別 Linkage 是否已新增 HealthLake，請尋找新增的 "tag": [{"display": "SYSTEM_GENERATED"}] 鍵/值對。若要進一步了解 Linkage 的 FHIR 規格，請參閱 FHIR 文件索引中的 [資源類型：Linkage](#)。
- FHIR Amazon Comprehend Medical API 操作所產生的資源類型。

- **Observation**：具有特徵為 SIGN 或 時，Amazon Comprehend Medical API operations DetectEntities-V2 和 InferICD10-CM 新增至其中的結果 SYMPTOM。
- **Condition**：在特徵為 時，會將 Amazon Comprehend Medical API operations DetectEntities-V2 和 InferICD10-CM 的結果新增至其中 DIAGNOSIS。
- **MedicationStatement**：將 Amazon Comprehend Medical API 操作的結果 InferRxNorm 新增至其中。

與 FHIR REST API 操作整合

根據預設，Amazon Comprehend Medical API 操作在發出 GET 請求時不會傳回偵測到的特徵。

若要查看這些資源類型的整合 NLP 操作結果，您必須指定已知的 ID。

- Linkage
- Observation
- Condition
- MedicationStatement

在 DocumentReference 資源類型外的整合 NLP 操作結果，只能使用指定 ID 已知包含 Amazon Comprehend Medical API 操作結果的 GET 請求取得。

Amazon Comprehend Medical API 操作如何整合到 中的範例 HealthLake

範例 1：擷取至 HealthLake 資料存放區的患者記錄

以下是根據病患與醫療專業人員的相遇而建立的範例臨床備註。

合成資料

此範例中的文字是合成內容，不包含個人健康資訊 (PHI)。

1991-08-31

Chief Complaint
- Headache

- Sinus Pain
- Nasal Congestion
- Sore Throat
- Pain with Bright Lights
- Nasal Discharge
- Cough

History of Present Illness

Jerónimo599

is a 4 month-old non-hispanic white male.

Social History

Patient has never smoked.

Patient comes from a middle socioeconomic background.

Patient currently has Aetna.

Allergies

No Known Allergies.

Medications

No Active Medications.

Assessment and Plan

Patient is presenting with bee venom (substance), mold (organism), house dust mite (organism), animal dander (substance), grass pollen (substance), tree pollen (substance), lisinopril, sulfamethoxazole / trimethoprim, fish (substance).

Plan

The patient was prescribed the following medications:

- astemizole 10 mg oral tablet
- nda020800 0.3 ml epinephrine 1 mg/ml auto-injector

The patient was placed on a careplan:

- self-care interventions (procedure)

提醒您，此資訊在 DocumentReference 資源中以 base64 格式編碼。當本文件擷取至 HealthLake 並完成 Amazon Comprehend Medical API 操作時，若要查看結果，您可以從 DocumentReference 資源類型的 GET 請求開始。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/DocumentReference
```

當 Amazon Comprehend Medical API 操作成功時，請在 extension 連結到下列項目的 中尋找這些鍵/值對 "url": "http://healthlake.amazonaws.com/aws-cm/"

```
{
  "url": "http://healthlake.amazonaws.com/aws-cm/status/",
  "valueString": "SUCCESS"
},
{
  "url": "http://healthlake.amazonaws.com/aws-cm/message/",
  "valueString": "The Amazon HealthLake integrated medical NLP operation was successful."
}
```

下列標籤顯示如何根據資源類型，在您的 HealthLake 資料存放區中報告擷取的醫療記錄。

DocumentReference

若要查看單一 DocumentReference 資源類型的結果，請提出 GET 請求，其中提供特定資源 id 的。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed
```

成功時，您會取得 200 HTTP 回應代碼和下列 JSON 回應（為了清楚起見而截斷）。

以下是 `http://healthlake.amazonaws.com/system-generated-resources/` 部分。您可以看到 Linkage/`e366d29f-2c22-4c19-866e-09603937935a` 已新增新的。您也可以查看 HealthLake 已將推論型問題清單新增至特定 ObservationCondition 和資源類型的位置。

若要查看這些資源類型的修訂方式，請選擇相關的標籤。

```
{
  "extension": [
    {
      "url": "http://healthlake.amazonaws.com/linkage",
      "valueReference": {
        "reference": "Linkage/e366d29f-2c22-4c19-866e-09603937935a"
      }
    }
  ]
}
```

```

    }
  },
  {
    "url": "http://healthlake.amazonaws.com/nlp-entity",
    "valueReference": {
      "reference": "Observation/c6e0a3ff-7a17-4d8b-bfd0-d02d7da090c5"
    }
  },
  {
    "url": "http://healthlake.amazonaws.com/nlp-entity",
    "valueReference": {
      "reference": "Condition/0854e1f3-894d-448e-a8d9-3af5b9902baf"
    }
  }
],
"url": "http://healthlake.amazonaws.com/system-generated-resources/"
}

```

Linkage

若要查看單一Linkage資源類型的結果，請提出 GET 請求，其中提供特定資源ID的。

```

GET https://healthlake.your-region.amazonaws.com/
datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd6c68cf2dfd/r4/
Linkage/e366d29f-2c22-4c19-866e-09603937935a

```

成功時，您會收到200HTTP回應代碼，以及下列截斷的JSON回應。

回應包含 `item` 元素。其中，索引鍵值對 `"type": "source"` 會指出用來修改 `Condition` 和 `Observations` 列於索引 `"type": "alternate"` 鍵值對下的特定 `DocumentReference` 項目。

您也會看到 `meta` 元素和對應的鍵/值對 `"tag": [{"display": "SYSTEM_GENERATED"}]`，指出這些資源是由 建立 HealthLake。

```

{
  "resourceType": "Linkage",
  "id": "e366d29f-2c22-4c19-866e-09603937935a",
  "active": true,
  "item": [
    {
      "type": "alternate",

```

```

    "resource": {
      "reference": "Observation/c6e0a3ff-7a17-4d8b-bfd0-d02d7da090c5",
      "type": "Observation"
    },
    {
      "type": "alternate",
      "resource": {
        "reference": "Condition/9d5c1ef6-f822-4faf-b55f-7c70f2a4aa8d",
        "type": "Condition"
      }
    },
    {
      "type": "source",
      "resource": {
        "reference": "DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed",
        "type": "DocumentReference"
      }
    }
  ],
  "meta": {
    "lastUpdated": "2022-10-21T19:38:31.327Z",
    "tag": [{
      "display": "SYSTEM_GENERATED"
    }]
  }
}

```

Resource type: Observation

若要查看單一Observation資源類型的結果，請提出 GET 請求，其中提供特定資源ID的。

```

GET https://healthlake.your-region.amazonaws.com/
datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/
Observation/e366d29f-2c22-4c19-866e-09603937935a

```

Amazon Comprehend Medical API操作的結果會修訂為下列元素：code、meta和modifierExtension。

code

類型的元素CodeableConcept。若要進一步了解，請參閱 FHIR 文件索引[CodeableConcept](#)中的。

HealthLake 會附加下列三個鍵/值對。

- "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/" : URL是指特定的 Amazon Comprehend Medical API操作。在此情況下，InferICD10CM。
- "code": "A52.06" : 其中 A52.06是 ICD-10-CM 程式碼，用於識別在 疾病控制中心知識庫中找到的概念。
- "display": "Other syphilitic heart involvement" : 其中 "Other syphilitic heart involvement"是 內科中的 ICD-10-CM 程式碼的長描述。

下列截斷JSON的回應僅包含 code元素。

```
"code": {
  "coding":
  [
    {
      "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/",
      "code": "A52.06",
      "display": "Other syphilitic heart involvement"
    }
  ],
  "text": "Other syphilitic heart involvement"
}
```

若要了解模型對指派的 ICD-10-CM 程式碼正確之可信度，請使用 modifierExtension元素。

meta

meta 元素包含中繼資料，指出code元素是否包含 Amazon Comprehend Medical API操作新增的詳細資訊。

下列截斷JSON的回應僅包含 meta元素。

```
"meta": {
  "lastUpdated": "2022-10-21T19:38:30.879Z",
  "tag": [{
    "display": "SYSTEM_GENERATED"
  }]
}
```

modifierExtension

`modifierExtension` 元素包含有關 `code` 元素中指定程式碼之可信度層級的更多詳細資訊。它還具有鍵值對，提供用於 `DocumentReference` 產生結果和相關 `Linkage` 資源類型的原始檔的連結。

對於每個新增的 `coding` 元素，您會看到 `entity-score` 和 `entity-Concept-Score` 新增至 `modifierExtension`。對於鍵/值對中的每個值，您會看到分數。對於 `entity-score`，此分數是 Amazon Comprehend Medical 對偵測準確性的可信度。對於 `entity-Concept-Score`，此分數是 Amazon Comprehend Medical 認為實體準確連結到 ICD-10-CM 概念的可信度。

下列截斷JSON的回應僅包含 `modifierExtension` 元素。

```
"modifierExtension": [{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-score",
  "valueDecimal": 0.45005733
},
{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-Concept-Score",
  "valueDecimal": 0.1111792
},
{
  "url": "http://healthlake.amazonaws.com/system-generated-linkage",
  "valueReference": {
    "reference": "Linkage/e366d29f-2c22-4c19-866e-09603937935a"
  }
},
{
  "url": "http://healthlake.amazonaws.com/source-document-reference",
  "valueReference": {
    "reference": "DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed"
  }
}
]
```

完整JSON回應

```
{
  "subject": {
    "reference": "Patient/0679b7b7-937d-488a-b48d-6315b8e7003b"
  },
  "resourceType": "Observation",
  "status": "unknown",
```

```

"code": {
  "coding": [{
    "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/",
    "code": "A52.06",
    "display": "Other syphilitic heart involvement"
  }],
  "text": "Other syphilitic heart involvement"
},
"meta": {
  "lastUpdated": "2022-10-21T19:38:30.879Z",
  "tag": [{
    "display": "SYSTEM_GENERATED"
  }]
},
"modifierExtension": [{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-score",
  "valueDecimal": 0.45005733
},
{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-Concept-Score",
  "valueDecimal": 0.1111792
},
{
  "url": "http://healthlake.amazonaws.com/system-generated-linkage",
  "valueReference": {
    "reference": "Linkage/e366d29f-2c22-4c19-866e-09603937935a"
  }
},
{
  "url": "http://healthlake.amazonaws.com/source-document-reference",
  "valueReference": {
    "reference": "DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed"
  }
}
],
"id": "7e88c7c5-21a5-4dd7-8fc2-a02474fba583"
}

```

Condition

若要查看單一Condition資源類型的結果，請提出 GET 請求，其中提供特定資源ID的。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/Condition/b06d343d-ddb8-4f36-82cb-853fcd434dfd
```

Amazon Comprehend Medical API操作的結果會修訂為下列元素：code、meta和modifierExtension。

code

類型的元素CodeableConcept。若要進一步了解，請參閱 FHIR 文件索引[CodeableConcept](#)中的。

HealthLake 會附加下列三個鍵/值對。

- "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/"：URL是指特定的 Amazon Comprehend Medical API操作。在此情況下，InferICD10CM。
- "code": "I70.0"：其中 A52.06是 ICD-10-CM 程式碼，用於識別在疾病控制中心知識庫中找到的概念。
- "display": "Atherosclerosis of aorta"：其中 "Other syphilitic heart involvement"是 內科中的 ICD-10-CM 程式碼的長描述。

下列截斷JSON的回應僅包含 code元素。

```
{
  "code": {
    "coding": [
      {
        "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/",
        "code": "I70.0",
        "display": "Atherosclerosis of aorta"
      }
    ],
    "text": "Atherosclerosis of aorta"
  }
}
```

若要了解模型對指派的 ICD-10-CM 程式碼正確之可信度，請使用 modifierExtension元素。

meta

meta 元素包含中繼資料，指出code元素是否包含 Amazon Comprehend Medical API操作新增的詳細資訊。

下列截斷JSON的回應僅包含 meta元素。

```
"meta": {
  "lastUpdated": "2022-10-21T19:38:30.877Z",
  "tag": [{
    "display": "SYSTEM_GENERATED"
  }]
}
```

modifierExtension

modifierExtension 元素包含有關 code 元素中指定程式碼之可信度層級的更多詳細資訊。它還具有鍵值對，提供用於 DocumentReference 產生結果和相關 Linkage 資源類型的原始檔的連結。

對於每個新增的coding元素，您會看到 entity-score和 entity-Concept-Score 新增至 modifierExtension。對於鍵/值對中的每個值，您會看到分數。對於 entity-score，此分數是 Amazon Comprehend Medical 對偵測準確性的可信度。對於 entity-Concept-Score，此分數是 Amazon Comprehend Medical 認為實體準確連結到 ICD-10-CM 概念的可信度。

下列截斷JSON的回應僅包含 modifierExtension元素。

```
"modifierExtension": [{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-score",
  "valueDecimal": 0.94417894
},
{
  "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-Concept-Score",
  "valueDecimal": 0.8458298
},
{
  "url": "http://healthlake.amazonaws.com/system-generated-linkage",
  "valueReference": {
    "reference": "Linkage/e366d29f-2c22-4c19-866e-09603937935a"
  }
},
{
  "url": "http://healthlake.amazonaws.com/source-document-reference",
```

```

    "valueReference": {
      "reference": "DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed"
    }
  }
]

```

完整JSON回應

```

{
  "subject": {
    "reference": "Patient/0679b7b7-937d-488a-b48d-6315b8e7003b"
  },
  "resourceType": "Condition",
  "code": {
    "coding": [{
      "system": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/",
      "code": "I70.0",
      "display": "Atherosclerosis of aorta"
    }],
    "text": "Atherosclerosis of aorta"
  },
  "meta": {
    "lastUpdated": "2022-10-21T19:38:30.877Z",
    "tag": [{
      "display": "SYSTEM_GENERATED"
    }]
  },
  "modifierExtension": [{
    "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-score",
    "valueDecimal": 0.94417894
  },
  {
    "url": "http://healthlake.amazonaws.com/aws-cm/infer-icd10/aws-cm-icd10-entity-Concept-Score",
    "valueDecimal": 0.8458298
  },
  {
    "url": "http://healthlake.amazonaws.com/system-generated-linkage",
    "valueReference": {
      "reference": "Linkage/e366d29f-2c22-4c19-866e-09603937935a"
    }
  },

```

```
{
  "url": "http://healthlake.amazonaws.com/source-document-reference",
  "valueReference": {
    "reference": "DocumentReference/0e938f03-da7f-4178-acd8-eea9586c46ed"
  }
},
"id": "b06d343d-ddb8-4f36-82cb-853fcd434dfd"
}
```

範例 2：DocumentReference 包含 MedicationStatement 資源類型的

以下是根據病患與醫療專業人員的接觸而建立的臨床備註範例。

合成資料

此範例中的文字是合成內容，不包含個人健康資訊 (PHI)。

Tom is not prescribed Advil

下列標籤顯示如何根據資源類型，在您的 HealthLake 資料存放區中報告擷取的醫療記錄。

DocumentReference

若要查看單一 DocumentReference 資源類型的結果，請提出 GET 請求，其中提供特定資源 ID 的。

```
GET https://healthlake.your-region.amazonaws.com/datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/DocumentReference/c549125d-a218-421f-b8bf-23614c5e796c
```

成功時，您會收到 200 HTTP 回應代碼和下列截斷的 JSON 回應。

鍵/值對 "url": "http://healthlake.amazonaws.com/system-generated-resources/" 表示 Amazon Comprehend Medical API 操作 extension 已新增其中的資源類型。您可以看到新的 Linkage 資源類型和多個 MedicationStatement 資源。

```
"extension": [{
```

```

"extension": [{
  "url": "http://healthlake.amazonaws.com/linkage",
  "valueReference": {
    "reference": "Linkage/394bb244-177b-4409-8657-26b20ed56dd7"
  }
},
{
  "url": "http://healthlake.amazonaws.com/nlp-entity",
  "valueReference": {
    "reference": "MedicationStatement/cbf6af10-b0b9-451c-bdde-99611e3498a8"
  }
},
{
  "url": "http://healthlake.amazonaws.com/nlp-entity",
  "valueReference": {
    "reference": "MedicationStatement/9a89b0d3-6681-45ca-9926-27951edce5c7"
  }
},
{
  "url": "http://healthlake.amazonaws.com/nlp-entity",
  "valueReference": {
    "reference": "MedicationStatement/4a01f6c8-5f3a-4122-80ab-405312f96aa2"
  }
},
{
  "url": "http://healthlake.amazonaws.com/nlp-entity",
  "valueReference": {
    "reference": "MedicationStatement/fbfb77d8-70cf-4579-b4c0-d6fe3c01656b"
  }
},
{
  "url": "http://healthlake.amazonaws.com/nlp-entity",
  "valueReference": {
    "reference": "MedicationStatement/1340c9ce-9c48-4bf9-9b2f-d0ab027f5e0b"
  }
}
],
"url": "http://healthlake.amazonaws.com/system-generated-resources/"
}

```

Linkage

若要查看單一Linkage資源類型的結果，請提出 GET 請求，其中提供特定資源ID的。

```
GET https://https://healthlake.your-region.amazonaws.com/  
datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/  
Linkage/394bb244-177b-4409-8657-26b20ed56dd7
```

成功時，您會收到200HTTP回應代碼和下列JSON回應。

回應包含 item元素。其中，索引鍵/值對"type": "source"會指出用來修改MedicationStatement資源類型的特定DocumentReference項目。

您也可以看到 meta元素和對應的鍵值對 "tag": [{"display": "SYSTEM_GENERATED"}]，指出這些資源是由 建立 HealthLake。

```
{  
  "resourceType": "Linkage",  
  "id": "394bb244-177b-4409-8657-26b20ed56dd7",  
  "active": true,  
  "item": [{  
    "type": "alternate",  
    "resource": {  
      "reference": "MedicationStatement/cbf6af10-b0b9-451c-bdde-99611e3498a8",  
      "type": "MedicationStatement"  
    }  
  },  
  {  
    "type": "alternate",  
    "resource": {  
      "reference": "MedicationStatement/9a89b0d3-6681-45ca-9926-27951edce5c7",  
      "type": "MedicationStatement"  
    }  
  },  
  {  
    "type": "alternate",  
    "resource": {  
      "reference": "MedicationStatement/4a01f6c8-5f3a-4122-80ab-405312f96aa2",  
      "type": "MedicationStatement"  
    }  
  },  
  {  
    "type": "alternate",  
    "resource": {  
      "reference": "MedicationStatement/fbfb77d8-70cf-4579-b4c0-d6fe3c01656b",  
      "type": "MedicationStatement"  
    }  
  }  
}
```

```

    },
    {
      "type": "alternate",
      "resource": {
        "reference": "MedicationStatement/1340c9ce-9c48-4bf9-9b2f-d0ab027f5e0b",
        "type": "MedicationStatement"
      }
    },
    {
      "type": "source",
      "resource": {
        "reference": "DocumentReference/c549125d-a218-421f-b8bf-23614c5e796c",
        "type": "DocumentReference"
      }
    }
  ],
  "meta": {
    "lastUpdated": "2022-10-24T20:05:03.501Z",
    "tag": [{
      "display": "SYSTEM_GENERATED"
    }]
  }
}

```

MedicationStatement

若要查看單一MedicationStatement資源類型的結果，請提出 GET 請求，其中提供特定資源ID的。

```

GET https://healthlake.your-region.amazonaws.com/
datastore/your-datastore-id/r4/eeb8005725ae22b35b4edbd68cf2dfd/r4/
MedicationStatement/9a89b0d3-6681-45ca-9926-27951edce5c7

```

MedicationStatement 資源類型是找到 Amazon Comprehend Medical InferRxNorm API 操作結果的位置。結果會修訂為下列元素：medicationCodeableConcept、meta和modifierExtension。

medicationCodeableConcept

類型的元素CodeableConcept。若要進一步了解，請參閱 FHIR 文件索引[CodeableConcept](#)中的。

HealthLake 會附加下列三個鍵/值對。

- "system": "http://healthlake.amazonaws.com/aws-cm/infer-rxnorm/": URL 是指特定的 Amazon Comprehend Medical API操作。在這種情況下，InferRxNorm。
- "code": "731533": 其中 731533 是 RxNorm 概念 ID，也稱為 RxCUI。
- "display": "ibuprofen 200 MG Oral Capsule [Advil]": 其中 ibuprofen 200 MG Oral Capsule [Advil]是 RxNorm 概念的描述。

下列截斷JSON的回應僅包含 MedicationStatement元素。

```
"medicationCodeableConcept": {
  "coding": [
    {
      "system": "http://healthlake.amazonaws.com/aws-cm/infer-rxnorm/",
      "code": "731533",
      "display": "ibuprofen 200 MG Oral Capsule [Advil]"
    }
  ]
}
```

meta

meta 元素包含中繼資料，指出code元素是否包含 Amazon Comprehend Medical API操作新增的詳細資訊。

下列截斷JSON的回應僅包含 meta元素。

```
"meta": {
  "lastUpdated": "2022-10-24T20:05:02.800Z",
  "tag": [
    {
      "display": "SYSTEM_GENERATED"
    }
  ]
}
```

modifierExtension

modifierExtension 元素包含鍵值對，提供用來 DocumentReference 產生結果的原始連結和相關 Linkage 資源類型。

```
"modifierExtension": [
```

```

{
  "url": "http://healthlake.amazonaws.com/system-generated-linkage",
  "valueReference": {
    "reference": "Linkage/394bb244-177b-4409-8657-26b20ed56dd7"
  }
},
{
  "url": "http://healthlake.amazonaws.com/source-document-reference",
  "valueReference": {
    "reference": "DocumentReference/c549125d-a218-421f-b8bf-23614c5e796c"
  }
}
]

```

搜尋參數

下表列出整合式醫療的可搜尋屬性NLP。

搜尋參數

搜尋參數	尋找的相符項目
detectEntities-entity-category	CM AWS 延伸模組中 DetectEntities 子延伸中的實體類別
detectEntities-entity-text	CM AWS 延伸模組中 DetectEntities 子延伸中的實體文字
detectEntities-實體-類型	CM AWS 延伸模組中 DetectEntities 子延伸中的實體類型
detectEntities-實體分數	AWS CM 延伸模組中 DetectEntities 子延伸中的實體分數
infer-icd10cm-entity-text	CM 延伸模組內 InferICD10CM AWS 子延伸中的實體文字
infer-icd10cm-entity-score	CM 延伸模組內 InferICD10CM AWS 子延伸中的實體分數

搜尋參數	尋找 的相符項目
infer-icd10cm-entity-concept-code	CM 延伸模組內 InferICD10CM AWS 子延伸中的實體概念碼
infer-icd10cm-entity-concept-description	AWS CM 延伸模組 InferICD10CM 子延伸中的實體概念描述
infer-icd10cm-entity-concept-score	CM 延伸模組內 InferICD10CM AWS 子延伸中的實體概念分數
infer-rxnorm-entity-score	CM AWS 延伸模組中 InferRxNorm 子延伸中的實體分數
infer-rxnorm-entity-text	CM AWS 延伸模組中 InferRxNorm 子延伸中的實體文字
infer-rxnorm-entity-concept- 程式碼	AWS CM 延伸模組中 InferRxNorm 子延伸中的實體概念碼
infer-rxnorm-entity-concept- 描述	AWS CM 延伸模組中 InferRxNorm 子延伸中的實體概念描述
infer-rxnorm-entity-concept- 分數	AWS CM 延伸模組中 InferRxNorm 子延伸中的實體概念分數

為了符合 `EntityText` 和 `EntityCategory` 屬於相同實體的條件，HealthLake 提供特殊搜尋。下表說明 中支援的特殊搜尋參數 HealthLake。

搜尋參數

搜尋參數	傳回相符項目
detectEntities-entity-text-category	如果 <code>DetectEntities</code> 子延伸中至少有一個實體同時符合 <code>entityText</code> 和 <code>entityCategory</code> 。
detectEntities-entity-type-score	如果 <code>DetectEntities</code> 子延伸中至少有一個實體同時符合 <code>entityType</code> 和 <code>entityScore</code> 。

搜尋參數	傳回相符項目
detectEntities-entity-text-score	如果 DetectEntities 子延伸中至少有一個實體同時符合 entityText 和 entityScore。
detectEntities-entity-text-type	如果 DetectEntities 子延伸中至少有一個實體同時符合 entityText 和 entityType。
detectEntities-entity-category-score	如果至少有一個實體同時符合 entityCategory 和 entityScore。
infer-icd10cm-entity-text-concept-code	如果 InferICD10CM 子延伸中至少有一個符合的實體，entityText 且 conceptCode 該實體至少有一個符合程式碼的實體。
infer-icd10 cm-entity-text-concept分數	如果 InferICD10CM 子延伸中至少有一個符合的實體，entityText 且 conceptScore 該實體至少有一個符合分數的實體。
infer-icd10cm-entity-concept-description-concept-score	如果 InferICD10CM 子延伸中的實體中至少有一個符合概念描述和的概念conceptScore。
infer-rxnorm-entity-text-concept-code	如果 InferRxNorm 子延伸中至少有一個符合的實體，entityText 且 conceptCode 該實體至少有一個符合程式碼的實體。
infer-rxnorm-entity-text-concept-score	如果 InferRxNorm 子延伸中至少有一個符合的實體，entityText 且 conceptScore 該實體至少有一個符合分數的實體。
infer-rxnorm-entity-concept-description-concept-score	如果 InferRxNorm 子延伸中的實體中至少有一個符合概念描述和的概念conceptScore。

中的安全性 AWS HealthLake

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

安全是 AWS 和 之間的共同責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

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

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

主題

- [中的資料保護 AWS HealthLake](#)
- [在 REST 的 加密 AWS HealthLake](#)
- [的傳輸中加密 AWS HealthLake](#)
- [的身分和存取管理 AWS HealthLake](#)
- [使用 AWS CloudTrail記錄 AWS HealthLake API 呼叫](#)
- [的合規驗證 AWS HealthLake](#)
- [中的彈性 AWS HealthLake](#)
- [AWS HealthLake 中的基礎設施安全](#)
- [AWS HealthLake 中的安全最佳實務](#)

中的資料保護 AWS HealthLake

AWS [共同責任模型](#)適用於 中的資料保護 AWS HealthLake。如此模型所述，AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權](#)。[FAQ](#)如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格上的[AWS 共同責任模型和GDPR](#)部落格文章。

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

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

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 HealthLake 或其他 AWS 服務 使用 主控台API AWS CLI、或 時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您將 URL提供給外部伺服器，強烈建議您在 中不要包含登入資料資訊URL，以驗證您對該伺服器的請求。

在 REST 的 加密 AWS HealthLake

HealthLake 根據預設提供加密，使用服務擁有的 AWS Key Management Service (AWS KMS) 金鑰來保護靜態敏感客戶資料。也支援客戶管理的KMS金鑰，而且從資料存放區匯入和匯出檔案時都需要此金鑰。若要進一步了解客戶受管KMS金鑰，請參閱 [Amazon Key Management Service](#)。建立資料存放區時，客戶可以選擇AWS擁有KMS的金鑰或客戶管理的KMS金鑰。建立資料存放區後，就無法變更加密組態。如果資料存放區使用AWS擁有的KMS金鑰，則其將表示為 `AWS_OWNED_KMS_KEY`，而且您不會看到用於靜態加密的特定金鑰。

AWS 擁有的KMS金鑰

HealthLake 根據預設，會使用這些金鑰自動加密潛在的敏感資訊，例如個人識別或靜態私有健康資訊 (PHI) 資料。AWS擁有的KMS金鑰不會儲存在您的帳戶中。它們是AWS擁有和管理的KMS金鑰集合的一部分，可用於多個AWS帳戶。AWS服務可以使用AWS擁有的KMS金鑰來保護您的資料。您無法檢視、管理、使用AWS擁有的KMS金鑰或稽核其使用方式。不過，您不需要進行任何工作或變更任何程式，即可保護加密資料的金鑰。

如果您使用AWS擁有的KMS金鑰，則不會向您收取月費或使用費，而且這些金鑰不會計入您帳戶的AWSKMS配額。如需詳細資訊，請參閱[AWS擁有的金鑰](#)。

客戶受管KMS金鑰

HealthLake 支援使用您建立、擁有和管理的對稱客戶受管KMS金鑰，以透過現有AWS擁有的加密新增第二層加密。您可以完全控制此層加密，因此能執行以下任務：

- 建立和維護金鑰政策、IAM政策和授與
- 輪換金鑰密碼編譯資料
- 啟用和停用金鑰政策
- 新增標籤
- 建立金鑰別名
- 安排金鑰供刪除

您也可以使用 CloudTrail 來追蹤 AWS KMS 代表您 HealthLake 傳送至 的請求。AWS KMS 需支付額外費用。如需詳細資訊，請參閱[客戶擁有的金鑰](#)。

建立客戶受管金鑰

您可以使用 AWS管理主控台或 建立對稱客戶受管金鑰 AWS KMS APIs。

請遵循 AWS Key Management Service 開發人員指南中的[建立對稱客戶受管金鑰](#)的步驟。

金鑰政策會控制客戶受管金鑰的存取權限。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶自管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱 AWS 金鑰管理服務開發人員指南中的[管理對客戶受管金鑰的存取](#)。

若要將客戶受管金鑰與 HealthLake 資源搭配使用，[km : CreateGrant](#) 必須在金鑰政策中允許操作。這會將授予新增至客戶受管金鑰，以控制對指定KMS金鑰的存取，讓使用者存取 [kms : grant 操作](#) HealthLake 所需的許可。如需詳細資訊，請參閱[使用授予](#)。

若要將客戶受管KMS金鑰與 HealthLake 資源搭配使用，金鑰政策中必須允許下列API操作：

- kms : CreateGrant 新增授予至特定客戶受管KMS金鑰，允許存取授予操作。
- kms : DescribeKey 提供驗證金鑰所需的客戶受管金鑰詳細資訊。這是所有操作的必要項目。
- kms : GenerateDataKey 提供存取權，以加密所有寫入操作的靜態資源。
- kms : Decrypt 可讓您存取加密資源的讀取或搜尋操作。

以下是政策陳述式範例，可讓使用者建立資料存放區並與 AWS HealthLake 其中使用該金鑰加密的資料存放區互動：

```
"Statement": [
  {
    "Sid": "Allow access to create data stores and do CRUD/search in AWS
HealthLake",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:HealthLakeFullAccessRole"
    },
    "Action": [
      "kms:DescribeKey",
      "kms:CreateGrant",
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "healthlake.amazonaws.com",
        "kms:CallerAccount": "111122223333"
      }
    }
  }
]
```

使用客戶受管KMS金鑰的必要IAM許可

使用客戶受管KMS金鑰建立啟用 AWS KMS 加密的資料存放區時，建立 HealthLake 資料存放區的使用者或角色需要金鑰政策和IAM政策的許可。

您可以使用 [kms : ViaService condition 金鑰](#)，將KMS金鑰的使用限制為僅來自的請求 HealthLake。

如需金鑰政策的詳細資訊，請參閱 AWS 金鑰管理服務開發人員指南中的[啟用IAM政策](#)。

建立儲存庫IAM的使用者、IAM角色或AWS帳戶必須具有 kms:CreateGrant、kms : GenerateDataKey 和 kms:DescribeKey 許可，以及必要的 HealthLake許可。

如何在 中使用 HealthLake 授予 AWS KMS

HealthLake 需要[授予](#)才能使用您的客戶受管KMS金鑰。當您建立使用客戶受管KMS金鑰加密的資料存放區時，會透過傳送[CreateGrant](#)請求至 AWS 來代表您 HealthLake 建立授予KMS。中的授予 AWSKMS用於授予 HealthLake 存取客戶帳戶中的KMS金鑰的權限。

不應撤銷或淘汰代表您 HealthLake 建立的授予。如果您撤銷或淘汰授予您帳戶中AWSKMS金鑰使用 HealthLake 許可的授予，HealthLake 無法存取此資料、加密推送到資料存放區的新FHIR資源，或在提取時解密這些資源。當您撤銷或淘汰的授予時 HealthLake，變更會立即發生。若要撤銷存取權，您應該刪除資料存放區，而不是撤銷授予。刪除資料存放區時，會代表您 HealthLake 淘汰授予。

監控 的加密金鑰 HealthLake

您可以使用 CloudTrail 來追蹤在使用客戶受管KMS金鑰時代表您 HealthLake 傳送到 AWS KMS 的請求。日誌中的 CloudTrail 日誌項目會在 userAgent 欄位中顯示 healthlake.amazonaws.com，以清楚區分提出的請求 HealthLake。

下列範例是 CreateGrant GenerateDataKey、和 CloudTrail 的事件，DescribeKey 用於監控呼叫 AWS KMS 的操作 HealthLake，以存取客戶受管金鑰加密的資料。

以下說明如何使用 CreateGrant 來允許 HealthLake 存取客戶提供的KMS金鑰，HealthLake 並可使用該KMS金鑰來加密所有靜態客戶資料。

使用者不需要建立自己的授予。會透過傳送 CreateGrant 請求至 AWS 來代表您 HealthLake 建立授予 KMS。中的授予 AWS KMS 用於授予 HealthLake 存取客戶帳戶中的 AWS KMS 金鑰的權限。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEROLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLEKEYID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEROLE",
        "arn": "arn:aws:iam::111122223333:role/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Sampleuser01"
      }
    }
  }
}
```

```

    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2021-06-30T19:33:37Z",
        "mfaAuthenticated": "false"
    }
},
"invokedBy": "healthlake.amazonaws.com"
},
"eventTime": "2021-06-30T20:31:15Z",
"eventSource": "kms.amazonaws.com",
"eventName": "CreateGrant",
"awsRegion": "us-east-1",
"sourceIPAddress": "healthlake.amazonaws.com",
"userAgent": "healthlake.amazonaws.com",
"requestParameters": {
    "operations": [
        "CreateGrant",
        "Decrypt",
        "DescribeKey",
        "Encrypt",
        "GenerateDataKey",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant"
    ],
    "granteePrincipal": "healthlake.us-east-1.amazonaws.com",
    "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN",
    "retiringPrincipal": "healthlake.us-east-1.amazonaws.com"
},
"responseElements": {
    "grantId": "EXAMPLE_ID_01"
},
"requestID": "EXAMPLE_ID_02",
"eventID": "EXAMPLE_ID_03",
"readOnly": false,
"resources": [
    {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
    }
],

```

```

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

```

下列範例示範如何使用 `GenerateDataKey` 來確保使用者在儲存資料之前，擁有加密資料的必要許可。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEUSER",
    "arn": "arn:aws:sts::111122223333:assumed-role/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLEKEYID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEROLE",
        "arn": "arn:aws:iam::111122223333:role/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Sampleuser01"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2021-06-30T21:17:06Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "invokedBy": "healthlake.amazonaws.com",
  "eventTime": "2021-06-30T21:17:37Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "healthlake.amazonaws.com",
  "userAgent": "healthlake.amazonaws.com",
  "requestParameters": {
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
  }
}

```

```

},
"responseElements": null,
"requestID": "EXAMPLE_ID_01",
"eventID": "EXAMPLE_ID_02",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

下列範例顯示 如何 HealthLake 呼叫 Decrypt 操作，以使用儲存的加密資料金鑰來存取加密的資料。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEUSER",
    "arn": "arn:aws:sts::111122223333:assumed-role/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLEKEYID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEROLE",
        "arn": "arn:aws:iam::111122223333:role/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Sampleuser01"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2021-06-30T21:17:06Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}

```

```

    },
    "invokedBy": "healthlake.amazonaws.com"
  },
  "eventTime": "2021-06-30T21:21:59Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "healthlake.amazonaws.com",
  "userAgent": "healthlake.amazonaws.com",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
  },
  "responseElements": null,
  "requestID": "EXAMPLE_ID_01",
  "eventID": "EXAMPLE_ID_02",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

下列範例顯示 HealthLake 如何使用 DescribeKey 操作來驗證 AWS KMS 客戶擁有的 AWS KMS 金鑰是否處於可用狀態，並在使用者無法運作時協助進行故障診斷。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEUSER",
    "arn": "arn:aws:sts::111122223333:assumed-role/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLEKEYID",

```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEROLE",
        "arn": "arn:aws:iam::111122223333:role/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Sampleuser01"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2021-07-01T18:36:14Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "healthlake.amazonaws.com"
  },
  "eventTime": "2021-07-01T18:36:36Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DescribeKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "healthlake.amazonaws.com",
  "userAgent": "healthlake.amazonaws.com",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
  },
  "responseElements": null,
  "requestID": "EXAMPLE_ID_01",
  "eventID": "EXAMPLE_ID_02",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE_KEY_ARN"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

進一步了解

下列資源提供靜態資料加密的詳細資訊。

如需 [AWS Key Management Service 基本概念](#) 的詳細資訊，請參閱 AWS KMS 文件。

如需 AWS KMS 文件中 [安全最佳實務](#) 的詳細資訊。

的傳輸中加密 AWS HealthLake

AWS HealthLake 使用 TLS 1.2 透過公有端點和後端服務加密傳輸中的資料。

的身分和存取管理 AWS HealthLake

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可以經過身分驗證（登入）和授權（具有許可）來使用 HealthLake 資源。IAM 是您可以免費使用 AWS 服務的，無需額外費用。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS HealthLake 如何使用 IAM](#)
- [的身分型政策範例 AWS HealthLake](#)
- [AWS 的 受管政策 AWS HealthLake](#)
- [對 AWS HealthLake 身分和存取進行故障診斷](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在其中執行的工作 HealthLake。

服務使用者 – 如果您使用 HealthLake 服務來執行您的任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 HealthLake 功能來執行工作時，您可能需要額外的許可。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 HealthLake 中的某項功能，請參閱 [對 AWS HealthLake 身分和存取進行故障診斷](#)。

服務管理員 – 如果您負責公司 HealthLake 的資源，您可能擁有 的完整存取權 HealthLake。您的任務是判斷您的服務使用者應存取哪些 HealthLake 功能和資源。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，瞭解 IAM 的基本概念。若要進一步了解貴公司如何IAM搭配 使用 HealthLake，請參閱 [AWS HealthLake 如何使用 IAM](#)。

IAM 管理員：如果您是IAM管理員，您可能想要了解如何撰寫政策以管理存取權的詳細資訊 HealthLake。若要檢視您可以在 中使用的以 HealthLake 身為基礎的政策範例IAM，請參閱 [的身分型政策範例 AWS HealthLake](#)。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任 IAM角色來驗證（登入 AWS）。

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

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《使用者指南》中的[如何登入您的 AWS 帳戶](#)。

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽章第 [AWS 4 版以取得API請求](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。若要進一步了解，請參閱AWS IAM Identity Center 《使用者指南》中的[多重要素驗證](#)，以及《IAM 使用者指南》[AWS 中的多重要素驗證IAM](#)。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱IAM 《使用者指南》中的[需要根使用者憑證](#)的任務。

聯合身分

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

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

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱AWS IAM Identity Center 《使用者指南》中的[什麼是 IAM Identity Center？](#)。

IAM 使用者和群組

[IAM 使用者](#)是 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。如果可能，我們建議您依賴臨時登入資料，而不是建立具有密碼和存取金鑰等長期登入資料IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者長期登入資料，建議您輪換存取金鑰。如需詳細資訊，請參閱IAM 《使用者指南》中的[針對需要長期憑證的使用案例定期輪換存取金鑰](#)。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。若要進一步了解，請參閱IAM 《使用者指南》中的[IAM使用者使用案例](#)。

IAM 角色

[IAM 角色](#)是 中具有特定許可 AWS 帳戶 的身分。它與 IAM 使用者相似，但是不會與特定人員建立關聯。若要暫時在 中擔任IAM角色 AWS Management Console，您可以從[使用者切換至IAM角色（主控台）](#)。您可以透過呼叫 或 AWS API AWS CLI 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱IAM 《使用者指南》中的[擔任角色的方法](#)。

使用臨時登入資料的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，

請參閱IAM《使用者指南》中的[為第三方身分提供者（聯合）建立角色](#)。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在驗證後可存取哪些內容，IAM Identity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。

- 臨時IAM使用者許可 – IAM使用者或角色可以擔任 IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (受信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱IAM《使用者指南》[中的跨帳戶資源存取IAM](#)。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中呼叫 時，該服務通常會在 Amazon 中執行應用程式，EC2或在 Amazon S3 中存放物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉送存取工作階段 (FAS) – 當您使用IAM使用者或角色在 中執行動作時 AWS，您被視為委託人。當您使用某些服務時，您可以執行 動作，然後在不同的服務中啟動另一個動作。FAS會使用呼叫的委託人許可 AWS 服務，結合 對下游服務 AWS 服務 提出請求的請求。FAS只有在服務收到請求時，才會提出請求，要求 與其他 AWS 服務 或 資源的互動完成。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求時的政策詳細資訊，請參閱[轉送存取工作階段](#)。
- 服務角色 – 服務角色是[IAM](#)服務擔任的角色，以代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱IAM《使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理EC2執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時登入資料。如需詳細資訊，請參閱IAM《使用者指南》中的[使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到 AWS 身分或資源 AWS 來控制 中的存取。政策是 中的物件，當與身分或資源建立關聯時，AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以JSON文

件 AWS 形式存放在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱IAM《使用者指南》中的[JSON政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

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

身分型政策

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。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型政策，請參閱IAM《使用者指南》中的[使用客戶受管政策定義自訂IAM許可](#)。

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

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主體（帳戶成員、使用者或角色）具有存取資源的許可。ACLs 類似於以資源為基礎的政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，請參閱《Amazon Simple Storage Service 開發人員指南》中的[存取控制清單 \(ACL\) 概觀](#)。

其他政策類型

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

- **許可界限** – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱IAM《使用者指南》中的[IAM實體的許可界限](#)。
- **服務控制政策 (SCPs)** – SCPs 是為組織或組織單位 (OU) in. 指定最大許可JSON的政策 AWS Organizations，AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個服務。如果您啟用組織中的所有功能，則可以將服務控制政策 (SCPs) 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊 SCPs，請參閱AWS Organizations《使用者指南》中的[服務控制政策](#)。
- **資源控制政策 (RCPs)** – RCPs 是可用來設定帳戶中資源可用許可上限JSON的政策，而無需更新連接到您擁有之每個資源IAM的政策。RCP 限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 的詳細資訊 RCPs，包括 AWS 服務 支援 的清單RCPs，請參閱 AWS Organizations 使用者指南中的[資源控制政策 \(RCPs\)](#)。
- **工作階段政策** – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南中的[政策評估邏輯](#)。

AWS HealthLake 如何使用 IAM

在您使用 IAM 管理 的存取權之前 HealthLake，請先了解哪些IAM功能可與 搭配使用 HealthLake。

IAM 您可以搭配 使用的功能 AWS HealthLake

IAM 功能	HealthLake 支援
身分型政策	是

IAM 功能	HealthLake 支援
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACLs	否
ABAC (政策中的標籤)	是
暫時性憑證	是
主體許可	是
服務角色	是
服務連結角色	否

若要深入了解 HealthLake 和其他 AWS 服務如何搭配大多數 IAM 功能使用，請參閱 IAM 使用者指南中的 [AWS 服務 IAM](#)。

的身分型政策 AWS HealthLake

支援身分型政策：是

身分型政策是您可以連接到身分的 JSON 許可政策文件，例如 IAM 使用者、使用者群組或角色。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型政策，請參閱 IAM 使用者指南中的 [使用客戶受管政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您可以在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素參考](#)。

的身分型政策範例 AWS HealthLake

若要檢視 HealthLake 身分型政策的範例，請參閱 [的身分型政策範例 AWS HealthLake](#)。

中的資源型政策 AWS HealthLake

支援資源型政策：否

資源型政策是您連接到資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為以資源為基礎政策的委託人。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的IAM管理員也必須授予委託人實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱IAM《使用者指南》[中的跨帳戶資源存取IAM](#)。

的政策動作 AWS HealthLake

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符API操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 HealthLake 動作清單，請參閱服務授權參考中的 [定義的動作 AWS HealthLake](#)。

中的政策動作在動作之前 HealthLake 使用下列字首：

```
healthlake
```

若要在單一陳述式中指定多個動作，請以逗號分隔每個動作。

```
"Action": [
```

```
"healthlake:action1",  
"healthlake:action2"  
]
```

若要檢視 HealthLake 身分型政策的範例，請參閱 [的身分型政策範例 AWS HealthLake](#)。

的政策資源 AWS HealthLake

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素會指定 動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\) 指定資源](#)。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 HealthLake 資源類型及其的清單 ARNs，請參閱服務授權參考中的 [定義的資源 AWS HealthLake](#)。若要了解您可以使用哪些動作來指定每個資源 ARN 的，請參閱 [定義的動作 AWS HealthLake](#)。

若要檢視 HealthLake 身分型政策的範例，請參閱 [的身分型政策範例 AWS HealthLake](#)。

的政策條件索引鍵 AWS HealthLake

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

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

您也可以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](#)。

AWS 支援全域條件金鑰和服務特定的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南中的[AWS 全域條件內容索引鍵](#)。

若要查看 HealthLake 條件金鑰清單，請參閱服務授權參考中的 [的條件金鑰 AWS HealthLake](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [定義的動作 AWS HealthLake](#)。

若要檢視 HealthLake 身分型政策的範例，請參閱 [的身分型政策範例 AWS HealthLake](#)。

中的存取控制清單 (ACLs) AWS HealthLake

支援 ACLs：否

存取控制清單 (ACLs) 控制哪些主體（帳戶成員、使用者或角色）具有存取資源的許可。ACLs 類似於以資源為基礎的政策，雖然它們不使用JSON政策文件格式。

屬性型存取控制 (ABAC) 搭配 AWS HealthLake

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種根據屬性定義許可的授權策略。在 AWS 中，這些屬性稱為標籤。您可以將標籤連接至IAM實體（使用者或角色）和許多 AWS 資源。標記實體和資源是 ABAC 的第一步。然後，您可以設計ABAC政策，在主體的標籤符合他們嘗試存取之資源上的標籤時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的[條件元素](#)中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需詳細資訊ABAC，請參閱IAM《使用者指南》中的[使用ABAC授權定義許可](#)。若要檢視教學課程，其中包含設定 ABAC 的步驟，請參閱IAM《使用者指南》中的[使用屬性型存取控制 \(ABAC\)](#)。

搭配 使用暫時登入資料 AWS HealthLake

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱IAM《使用者指南》中的[AWS 服務 使用 IAM](#)。

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

您可以使用 AWS CLI 或 手動建立臨時登入資料 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [中的臨時安全登入IAM](#)資料。

的跨服務主體許可 AWS HealthLake

支援轉送存取工作階段 (FAS)：是

當您使用 IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。當您使用某些服務時，您可以執行 動作，然後啟動不同服務中的另一個動作。FAS會使用呼叫 的委託人許可 AWS 服務，並結合對下游服務 AWS 服務 提出請求的請求。請求FAS只有在服務收到請求時才會提出，需要與其他 AWS 服務 或 資源互動才能完成。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求時的政策詳細資訊，請參閱[轉送存取工作階段](#)。

AWS HealthLake 的服務角色

支援服務角色：是

服務角色是IAM服務擔任的角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱IAM《使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。

如需服務角色和完整存取 所需的內嵌政策的相關資訊 AWS HealthLake，請參閱 [設定開始使用 的許可 AWS HealthLake](#)。

Warning

變更服務角色的許可可能會中斷 HealthLake 功能。只有在 HealthLake 提供指引時，才能編輯服務角色。

的服務連結角色 AWS HealthLake

支援服務連結角色：否

服務連結角色是連結至的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱[AWS 使用的服務IAM](#)。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 AWS HealthLake

根據預設，使用者和角色不具備建立或修改 HealthLake 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立以 IAM 身分為基礎的 JSON 政策，請參閱 IAM 使用者指南中的[建立 IAM 政策（主控台）](#)。

如需定義的動作和資源類型的詳細資訊 HealthLake，包括 ARNs 每個資源類型的格式，請參閱服務授權參考中的[的動作、資源和條件索引鍵 AWS HealthLake](#)。

主題

- [政策最佳實務](#)
- [使用 AWS HealthLake 主控台](#)
- [在 中存取 AWS HealthLake 資料存放區 Amazon Athena](#)
- [允許使用者檢視自己的許可](#)

政策最佳實務

以身分為基礎的政策會判斷是否有人可以建立、存取或刪除您帳戶中 HealthLake 的資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義

特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱IAM《使用者指南》中的 [AWS 受管政策](#) 或 [AWS 任務函數的受管政策](#)。

- 套用最低權限許可 – 當您使用 IAM 政策設定許可時，只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱IAM《使用者指南》[中的政策和許可IAM](#)。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱IAM《使用者指南》中的[IAMJSON政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，使政策符合IAM政策語言 (JSON) 和IAM最佳實務。IAMAccess Analyzer 提供超過 100 個政策檢查和可行的建議，以協助您撰寫安全且實用的政策。如需詳細資訊，請參閱IAM《使用者指南》中的[使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 中的IAM使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求，請將MFA條件新增至您的政策。如需詳細資訊，請參閱IAM《使用者指南》中的[使用 安全API存取MFA](#)。

如需 中最佳實務的詳細資訊IAM，請參閱IAM《使用者指南》[中的安全最佳實務IAM](#)。

使用 AWS HealthLake 主控台

若要存取 AWS HealthLake 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 HealthLake 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，只允許存取與其嘗試執行API的操作相符的動作。

若要完整存取 HealthLake，請將下列政策連接至IAM使用者或角色：

AmazonHealthLakeFullAccess和 AWSLakeFormationDataAdmin。您也需要連接內嵌 HealthLake 政策，即服務角色。服務角色是[IAM](#)服務擔任的角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱IAM《使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。如需建立所需服務角色的內嵌政策的相關資訊，請參閱 [設定開始使用的許可 AWS HealthLake](#)。您還必須使用 AWS Lake Formation 主控台或 CLI，將 HealthLake 管理員指派為 AWS Lake Formation Data Lake 管理員。如需詳細資訊，請參閱[設定開始使用的許可 AWS HealthLake](#)。

在 中存取 AWS HealthLake 資料存放區 Amazon Athena

如果您想要為使用者和角色提供 中 HealthLake 資料存放區的存取權 Amazon Athena，請將下列IAM 政策連接至角色或使用者：AmazonAthenaFullAccess 和 AmazonS3FullAccess。Select和 Describe 也需要由 AWS Lake Formation. AWS Lake Formation table 管理的資料表上的許可，由 AWS Lake Formation 主控台 中的 AWS Lake Formation 管理員或透過 授予許可CLI。如需詳細資訊，請參閱 [設定開始使用 的許可 AWS HealthLake](#)

允許使用者檢視自己的許可

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完成此動作的許可，或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

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

AWS 的 受管政策 AWS HealthLake

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。AWS 服務當新的啟動或新的API操作可用於現有服務時，AWS 很有可能更新受管政策。

如需詳細資訊，請參閱IAM 使用者指南中的[AWS 受管政策](#)。

AWS 受管政策：AmazonHealthLakeFullAccess

此AmazonHealthLakeFullAccess政策提供的完整存取權 HealthLake。將此政策連接至其使用者或角色後，使用者可以使用 HealthLake 來存取、查詢、匯入和匯出資料 HealthLake。若要在中執行許多常見動作 HealthLake，您必須將其他政策新增至使用者或角色。如需詳細資訊，請參閱[設定開始使用的許可 AWS HealthLake](#) 和 [HealthLake 操作和許可](#)。

您可將 AmazonHealthLakeFullAccess 政策連接到 IAM 身分。

此政策授予 *administrative and contributor* 許可，允許使用者和角色使用查詢、搜尋、匯入和匯出 HealthLake，也可讓代表具有這些許可的使用者和角色 HealthLake 執行動作。

許可詳細資訊

此政策包含下列陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS 受管政策：AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess 政策會授予其他服務中 HealthLake 和 相關資源的唯讀存取和許可 AWS。將此政策套用到您想要授予查詢和檢視 HealthLake 資料存放區功能的使用者，但不能建立或變更他們的能力。

您可將 AmazonHealthLakeReadOnlyAccess 政策連接到 IAM 身分。

此政策會授予 *read-only* 許可，以允許使用者和角色查詢 HealthLake。

許可詳細資訊

此政策包含下列陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "healthlake:SearchEverything"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

HealthLake 操作和許可

下表列出 中的典型操作， HealthLake 以及執行這些操作所需的許可。

HealthLake 操作	所需的許可
在 中建立資料存放區 HealthLake	AmazonHealthLakeFu llAccess AmazonLakeFormatio nDataAdmin 、內嵌 政策和 AWS Lake Formation 管理員許可由 管理 AWS Lake Formation
在 中刪除資料存放區 HealthLake	AmazonHealthLakeFu llAccess 、 AmazonLakeFormatio nDataAdmin 內嵌政策和 AWS Lake Formation 管理員許可由 管理 AWS Lake Formation

HealthLake 操作	所需的許可
在 中列出、搜尋或查詢資料存放區 HealthLake	AmazonHealthLakeReadOnlyAccess
使用 查詢資料存放區 Amazon Athena	AmazonAthenaFullAccess 受管理之資料表的 AmazonS3FullAccess 、AWS Lake Formation Select 和 Describe 許可 AWS Lake Formation
從 匯入資料 HealthLake	請參閱 設定匯入任務的許可 。
從 匯出資料 HealthLake	請參閱 從資料存放區匯出檔案 (AWS SDKs) 。

HealthLake 受 AWS 管政策的更新

檢視 HealthLake 自此服務開始追蹤這些變更以來，AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 HealthLake 文件歷史記錄頁面上的RSS摘要。

變更	描述	日期
AmazonHealthLakeFullAccess	AmazonHealthLakeFullAccess 允許完整存取所需的政策 HealthLake。	2022 年 11 月 14 日
AmazonHealthLakeReadOnlyAccess	AmazonHealthLakeReadOnlyAccess 唯讀存取所需的政策 HealthLake。	2022 年 11 月 14 日
HealthLake 已開始追蹤變更	HealthLake 已開始追蹤其 AWS 受管政策的變更。	2022 年 11 月 14 日

對 AWS HealthLake 身分和存取進行故障診斷

使用下列資訊來協助您診斷和修正使用 HealthLake 和 時可能遇到的常見問題IAM。

主題

- [我無權在 中執行動作 AWS HealthLake](#)

- [我無權執行 iam : PassRole](#)
- [我想要允許 AWS 帳戶外的人員存取我的 AWS HealthLake 資源](#)

我無權在 中執行動作 AWS HealthLake

如果 AWS Management Console 告訴您未獲授權執行 動作，則您必須聯絡管理員尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

當mateojacksonIAM使用者嘗試使用 主控台檢視虛構`my-example-widget`資源的詳細資訊，但沒有虛構healthlake:`GetWidget`許可時，會發生下列範例錯誤。

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `my-example-widget` 動作存取 healthlake:`GetWidget` 資源。

我無權執行 iam : PassRole

如果您收到錯誤，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 HealthLake。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

以下範例錯誤會在名為 marymajor 的 IAM 使用者嘗試使用主控台在 HealthLake 中執行動作時發生。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 AWS HealthLake 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援資源型政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策來授予人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 HealthLake 支援這些功能，請參閱 [AWS HealthLake 如何使用 IAM](#)。
- 若要了解如何在您 AWS 帳戶擁有的資源間提供存取權，請參閱 IAM 使用者指南中的[AWS 帳戶 在您擁有的另一個資源中為IAM使用者提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱IAM《使用者指南》中的[提供存取權給第三方 AWS 帳戶 擁有](#)。
- 若要了解如何透過聯合身分提供存取權，請參閱IAM《使用者指南》中的[提供存取權給外部驗證的使用者（聯合身分）](#)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱IAM《使用者指南》[中的跨帳戶資源存取IAM](#)。

使用 AWS CloudTrail記錄 AWS HealthLake API 呼叫

AWS HealthLake 已與 整合 AWS CloudTrail，此服務提供使用者、角色或服務 AWS in HealthLake. CloudTrail captures 的所有 API呼叫 HealthLake 作為事件所採取動作的記錄。擷取的呼叫包括從 HealthLake 主控台的呼叫，以及對 HealthLake API操作的程式碼呼叫。如果您建立追蹤，則可以啟用事件持續交付 CloudTrail至 Amazon S3 儲存貯體，包括 的事件 HealthLake。如果您未設定追蹤，仍然可以在 CloudTrail 主控台中檢視事件歷史記錄中的最新事件。使用 收集的資訊 CloudTrail，您可以判斷對 提出的請求 HealthLake、提出請求的 IP 地址、提出請求的人員、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 使用者指南](#)。

AWS HealthLake CloudTrail 中的資訊

CloudTrail 當您建立 AWS 帳戶時，會在您的帳戶上啟用。當活動在 中發生時 HealthLake，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。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[使用事件歷史記錄檢視 CloudTrail 事件](#)。

若要求持續記錄您 AWS 帳戶中的事件，包括 的事件 HealthLake，請建立追蹤。線索可讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。追蹤會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。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 的 Amazon SNS Notifications CloudTrail](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)以及[從多個帳戶接收 CloudTrail日誌檔案](#)

所有 HealthLake 動作都會由 記錄，CloudTrail 並記載於 [HealthLake API 參考](#)和本開發人員指南中，以了解使用 FHIR REST 執行的動作API。例如，對下列動作的呼叫會在 CloudTrail 日誌檔案中產生項目：

- DescribeFHIRImportJob
- DescribeFHIRExportJob
- StartFHIRImportJob
- ListFHIRImportJobs
- StartFHIRExportJob
- ListFHIRExportJobs
- CreateFHIRDatastore
- ListFHIRDatastores
- DeleteFHIRDatastore
- DescribeFHIRDatastore
- UpdateResource
- CreateResource
- DeleteResource
- ReadResource
- GetCapabilities
- SearchWithGet
- SearchWithPost

每一筆事件或日誌專案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：

- 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憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

了解 AWS HealthLake 日誌檔案項目

線索是一種組態，可讓您將事件做為日誌檔案交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。事件代表來自任何來源的單一請求，並包含所請求動作、動作的日期和時間、請求參數等資訊。CloudTrail log 檔案不是公開API呼叫的排序堆疊追蹤，因此不會以任何特定順序顯示。

下列範例顯示示範 CreateFHIRDatastore動作的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO0A2B3ZH0ADD20J4AHJX:git
full_access_iam_role580074395690222150",
    "arn": "arn:aws:sts::691207106566:assumed-role/
colossusfrontend_full_access_iam_role/_iam_role580074395690222150",
    "accountId": "AccountID",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO0A2B3ZH0ADD20J4AHJX",
        "arn": "arn:aws:iam::691207106566:role/full_access_iam_role",
        "accountId": "AccountID",
        "userName": "full_access_iam_role"
      },
      "webIdFederationData": {

    },
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2020-11-20T00:08:15Z"
    }
  },
  "eventTime": "2020-11-20T00:08:16Z",
  "eventSource": "healthlake.amazonaws.com",
  "eventName": "CreateFHIRDatastore",
  "awsRegion": "us-east-1",
```

```

    "sourceIPAddress": "3.213.247.1",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "datastoreName":
"testCreateFHIRDatastore_GBYAZFCLLBLSUTOYYFQZRLBLQJNFOYQVRPZBOJAIIUAHICAEAGIWLNVQEYAMSXVWMBLXC
        "datastoreTypeVersion": "R4",
        "clientToken": "d737ffe0-14dd-44cc-9f0a-fdf59b26c66b"
    },
    "responseElements": {
        "datastoreId": "datastoreId",
        "datastoreArn": "arn:aws:healthlake:us-
east-1:691207106566:datastore/55576c487ff4975262b10d1d65eb4509",
        "datastoreStatus": "CREATING",
        "datastoreEndpoint": "datastore_endpoint/"
    },
    "requestID": "68e62bdd-d2d4-44c1-af69-e6f055a69f99",
    "eventID": "7ef483dc-5dca-469e-823a-7d9e3a7fe924",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "691207106566"
}

```

的合規驗證 AWS HealthLake

第三方稽核人員 AWS HealthLake 會在多個合規計畫中評估 的安全性和 AWS 合規性。對於 HealthLake 這包含 HIPAA。

若要了解 是否 AWS 服務 在特定合規計畫的範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計畫。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[在 中下載報告 AWS Artifact](#)。

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

- [安全合規與治理](#) - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- [Amazon Web Services HIPAA上安全與合規架構](#) - 此白皮書說明公司如何使用 AWS 來建立HIPAA 符合 資格的應用程式。

 Note

並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱[HIPAA合格服務參考](#)。

- [AWS 合規資源](#) – 此工作手冊和指南的集合可能適用於您的產業和位置。
- [AWS 客戶合規指南](#) – 透過合規的角度了解共同的責任模型。本指南摘要說明保護 AWS 服務 指南並映射到跨多個架構之安全控制的最佳實務（包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)）。
- AWS Config 開發人員指南中的[使用 規則評估資源](#) – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。
- [Amazon GuardDuty](#) – 透過監控您的環境是否有可疑和惡意活動，這可 AWS 服務 偵測對您的 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可以協助您滿足特定合規架構強制要求的入侵偵測需求DSS，以解決各種合規要求，例如 PCI。
- [AWS Audit Manager](#) – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

中的彈性 AWS HealthLake

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎。AWS 區域提供多個實體分隔和隔離的可用區域，這些區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱[AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施之外，HealthLake 還提供數種功能，以協助支援您的資料彈性和備份需求。

AWS HealthLake 中的基礎設施安全

作為受管服務，AWS HealthLake 受到 [Amazon Web Services：安全程序概觀](#) 白皮書中所述 AWS 的全球網路安全程序的保護。

您可以使用 AWS 已發佈的 API 呼叫，HealthLake 透過網路存取。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。我們建議使用 TLS 1.2 或更新版本。用戶端還必須支援具有完美前向秘密 (PFS) 的密碼套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral 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。

AWS HealthLake 中的安全最佳實務

AWS HealthLake 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

- 實作最低權限存取。
- 盡可能使用 Customer-Managed-Keys (CMKs) 來加密您的資料。若要進一步了解 CMKs，請參閱 [Amazon Key Management Service](#)。
- 在資料存放 PII 區中查詢 PHI 或 GET 時，使用搜尋搭配 POST，而非使用 搜尋。
- 限制對敏感和重要稽核函數的存取。
- 透過更新或大量匯入 建立資源時 APIs，請勿使用 PHI 或 PII，包括任何可見欄位或邏輯 FHIR ID () 中的資料存放區和任務名稱 LID。
- 傳送建立、讀取、更新、刪除或搜尋請求時，請勿 PHI 在 HTTP 標頭中使用。
- 啟用 AWS CloudTrail 以稽核 AWS HealthLake 使用，並確保沒有非預期的活動。
- 檢閱安全使用 Amazon S3 儲存貯體的最佳實務。若要進一步了解，請參閱《Amazon S3 使用者指南》中的 [安全最佳實務](#)。

AWS HealthLake 端點和配額

下列各節包含 AWS HealthLake 配額和端點的相關資訊。對於可調整配額，您可以使用 [Service Quotas 主控台](#) 請求增加配額。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的 [請求提高配額](#)。

服務端點

資料表顯示指定區域中可用的 HealthLake 服務端點。

區域名稱	區域	端點	通訊協定	
美國東部 (俄亥俄)	us-east-2	healthlake.us-east-2.amazonaws.com	HTTPS	
		healthlake-fips.us-east-2.amazonaws.com	HTTPS	
美國東部 (維吉尼亞北部)	us-east-1	healthlake.us-east-1.amazonaws.com	HTTPS	
		healthlake-fips.us-east-1.amazonaws.com	HTTPS	
美國西部 (奧勒岡)	us-west-2	healthlake.us-west-2.amazonaws.com	HTTPS	
		healthlake-fips.us-west-2.amazonaws.com	HTTPS	
亞太區域 (孟買)	ap-south-1	healthlake.ap-south-1.amazonaws.com	HTTPS	
亞太區域 (悉尼)	ap-southeast-2	healthlake.ap-southeast-2.amazonaws.com	HTTPS	
歐洲 (倫敦)	eu-west-2	healthlake.eu-west-2.amazonaws.com	HTTPS	

的服務配額 HealthLake

以下是 的預設配額 HealthLake。

名稱	預設	可調整	描述
醫療備註中的字元數	每個受支援的區域：10,000	否	資源 DocumentReference 類型 (POST/PUT 請求) 中個別醫療備註中的字元數上限。
並行 StartFHIRImport任務數量	每個受支援的區域：1	否	並行 StartFHIRImport任務的最大數量。
concurrentStartFHIRExportJob 任務數量	每個受支援的區域：1	否	並行 StartFHIRExport任務的最大數量。
每個帳戶的資料存放區數量	每個受支援的區域：10	是	每個帳戶的預設作用中資料存放區數量上限。
StartFHIRImport任務中的檔案數量	每個受支援的區域：10,000	否	StartFHIRImport任務中的檔案數量上限。
每個套件的資源數量	每個支援的區域：160	否	套件請求中允許的資源數量上限。
每個帳戶的套件請求率	每個受支援的區域：20	是	您可以為每個帳戶每秒提出的POST套件請求數量上限。
每個資料存放區的套件請求速率	每個受支援的區域：10	是	您可以為每個資料存放區每秒提出的POST套件請求數量上限。在 8/21/2023 之前建立的資料存放區每秒將限制為 1 個請求。
DELETE 每個帳戶使用的 CancelFHIRExport任務請求率	每個受支援的區域：1	否	您可以使用 為每個帳戶每分鐘DELETE提出的 C

名稱	預設	可調整	描述
			ancelFHIRExport任務請求數目上限。
每個帳戶的 CreateFHIRDatastore 請求率	每個受支援的區域：1	否	每個帳戶每分鐘可以提出的 CreateFHIRDatastore 請求數目上限。
每個帳戶的DELETE請求率	每個受支援的區域：2,000	<u>是</u>	每個帳戶每秒可提出的DELETE請求數上限。
每個資料存放區的DELETE請求率	每個受支援的區域：1,000	<u>是</u>	每個資料存放區每秒可以提出的DELETE請求數量上限。在 8/21/2023 之前建立的資料存放區每秒限制為 100 個請求。
每個帳戶的 DeleteFHIRDatastore 請求率	每個受支援的區域：1	否	每個帳戶每分鐘可以提出的 DeleteFHIRDatastore 請求數目上限。
每個帳戶的 DescribeFHIRDatastore 請求率	每個受支援的區域：10	否	每個帳戶每秒可以提出的 DescribeFHIRDatastore 請求數目上限。
每個帳戶的 DescribeFHIRExport任務請求率	每個受支援的區域：10	否	每個帳戶每秒可以提出的 DescribeFHIRExport任務請求數目上限。
GET 每個帳戶使用的 DescribeFHIRExport任務請求率	每個受支援的區域：10	否	您可以使用 為每個帳戶每秒GET提出的 DescribeFHIRExport任務請求數量上限。

名稱	預設	可調整	描述
每個帳戶的 DescribeFHIRImport 任務請求率	每個受支援的區域：10	否	每個帳戶每秒可以提出的 DescribeFHIRImport 任務請求數目上限。
每個帳戶的探索請求率	每個受支援的區域：10	否	每個帳戶每分鐘可以提出的探索請求數量上限。
每個帳戶的 GET 請求率	每個支援的區域：6,000	是	每個帳戶每秒可以提出的 GET 請求數量上限。
每個資料存放區的 GET 請求率	每個受支援的區域：3,000	是	每個資料存放區每秒可以提出的 GET 請求數量上限。在 8/21/2023 之前建立的資料存放區每秒限制為 100 個請求。
每個帳戶的 GetCapabilities 請求率	每個受支援的區域：10	否	每個帳戶每秒可以提出的 GetCapabilities 請求數量上限。
每個帳戶的 ListFHIRDatastores 請求率	每個受支援的區域：10	否	您可以為每個帳戶每秒提出的 ListFHIRDatastores 請求數目上限。
每個帳戶的 ListFHIRExport 任務請求率	每個受支援的區域：10	否	您可以為每個帳戶每秒提出的 ListFHIRExport 任務請求數量上限。
每個帳戶的 ListFHIRImport 任務請求率	每個受支援的區域：10	否	您可以為每個帳戶每秒提出的 ListFHIRImport 任務請求數量上限。
每個帳戶的 ListTagsForResource 請求率	每個受支援的區域：10	否	每個帳戶每秒可提出的 ListTagsForResource 請求數上限。

名稱	預設	可調整	描述
每個帳戶的POST請求率	每個受支援的區域：2,000	是	每個帳戶每秒可提出的POST請求數上限。
每個資料存放區的POST請求率	每個受支援的區域：1,000	是	每個資料存放區每秒可以提出的POST請求數量上限。在 8/21/2023 之前建立的資料存放區每秒限制為 100 個請求。
每個帳戶的PUT請求率	每個受支援的區域：2,000	是	每個帳戶每秒可以提出的PUT請求數量上限。
每個資料存放區的PUT請求率	每個受支援的區域：1,000	是	每個資料存放區每秒可以提出的PUT請求數量上限。在 8/21/2023 之前建立的資料存放區每秒限制為 100 個請求。
每個帳戶的 S tartFHIRExport任務請求率	每個受支援的區域：1	否	您可以為每個帳戶每分鐘提出的 S tartFHIRExport任務請求數目上限。
POST 每個帳戶使用的 S tartFHIRExport任務請求率	每個受支援的區域：1	否	您可以使用為每個帳戶每分鐘POST提出的 S tartFHIRExport任務請求數目上限。
每個帳戶的 S tartFHIRImport任務請求率	每個受支援的區域：1	否	您可以為每個帳戶每分鐘提出的 S tartFHIRImport任務請求數目上限。
每個帳戶的 TagResource 請求率	每個受支援的區域：10	否	您可以每秒提出的最大 TagResource 請求數。

名稱	預設	可調整	描述
每個帳戶的 UntagResource 請求率	每個受支援的區域：10	否	每個帳戶每秒可提出的 UntagResource 請求數上限。
GET 每個帳戶使用 的搜尋請求率	每個受支援的區域：200	是	您可以使用 為每個帳戶每秒GET提出的搜尋請求數量上限。
GET 每個資料存放區使用 的搜尋請求率	每個受支援的區域：100	是	您可以使用 為每個資料存放區每秒GET提出的搜尋請求數量上限。
POST 每個帳戶使用 的搜尋請求率	每個受支援的區域：200	是	您可以使用 每秒POST提出的搜尋請求數目上限。
POST 每個資料存放區使用 的搜尋請求率	每個受支援的區域：100	是	您可以使用 為每個資料存放區每秒POST提出的搜尋請求數量上限。
個別匯入檔案的大小	所有受支援的區域：5 GB	否	StartFHIRImport任務中包含之個別檔案的大小上限（以 GB 為單位）。
匯入任務大小總計	每個支援的區域：500 GB	否	匯入任務中包含之所有檔案的大小上限（以 GB 為單位）。

故障診斷

下列文件可協助您疑難排解使用 時可能遇到的問題 AWS HealthLake。

主題

- [為什麼我無法建立 HealthLake 資料存放區？](#)
- [超過每個帳戶允許的資料存放區數量](#)
- [如何建立 FHIR RESTful 的授權APIs？](#)
- [我的資料不是 FHIR R4 格式 - 我是否仍然可以使用 HealthLake？](#)
- [為什麼在將 FHIR RESTful APIs 用於以客戶受管KMS金鑰加密的資料存放區時，我會收到 AccessDenied 錯誤？](#)
- [為什麼匯入失敗？](#)
- [如何尋找 DocumentReference無法處理的資源？](#)
- [遷移現有資料存放區以使用 Amazon Athena](#)
- [將 Athena 中的搜尋結果連接到其他 AWS 服務](#)
- [Athena 主控台在將資料匯入新資料存放區後無法運作](#)
- [為什麼我會收到 Lake Formation 許可錯誤：lakeformation：新增資料湖管理員PutDataLakeSettings 時？](#)
- [如何開啟 HealthLake整合的自然語言處理功能？](#)
- [我的資料存放區狀態不會從建立中變更](#)
- [我的SDK資料存放區建立狀態會傳回例外狀況或未知狀態](#)
- [使用 10MB 文件FHIRPOSTAPI進行操作，HealthLake 以取得 413Request 實體過大錯誤。](#)

為什麼我無法建立 HealthLake 資料存放區？

在 2022 年 11 月 14 日 HealthLake 更新建立新資料存放區所需的必要IAM許可。如果您尚未更新連接到存取 的使用者或角色的政策，HealthLake 您會收到下列錯誤。

```
AccessDeniedException: Insufficient Lake Formation permission(s): Required Database on Catalog
```

若要檢視建立資料存放區的更新IAM政策需求，請參閱 AWS 受管政策：

AmazonHealthLakeFullAccess。如需 step-by-step如何將這些政策新增至IAM使用者或角色的指示，請參閱 [設定開始使用的許可 AWS HealthLake](#)。

若要建立資料存放區，您也需要使用對稱的客戶擁有或 Amazon 擁有的KMS金鑰。請確定您在IAM政策中擁有正確的許可。若要進一步了解 AWS KMS，請參閱《AWS Key Management Service 開發人員指南[AWS Key Management Service](#)》中的。

超過每個帳戶允許的資料存放區數量

HealthLake 每個帳戶的配額為 10 個資料存放區。若要了解如何請求提高配額，請造訪 [AWS Support Center](#)。

如何建立 FHIR RESTful 的授權APIs？

使用者應使用 Signature 第 4 版簽署程序，將身分驗證 HealthLake API新增至透過HTTP用戶端傳送的請求。若要進一步了解，請參閱[簽章第 4 版簽署程序](#)。

若要使用AWSSDK適用於 Python 的 建立 sigv4 授權，請建立類似下列範例的指令碼。

```
import boto3
import requests
import json
from requests_auth_aws_sigv4 import AWSSigV4

# Set the input arguments
data_store_endpoint = 'https://healthlake.us-east-1.amazonaws.com/datastore/<datastore id>/r4/'
resource_path = "Patient"
requestBody = {"resourceType": "Patient", "active": True, "name": [{"use": "official", "family": "Dow", "given": ["Jen"]}, {"use": "usual", "given": ["Jen"]}], "gender": "female", "birthDate": "1966-09-01"}
region = 'us-east-1'

#Frame the resource endpoint
resource_endpoint = data_store_endpoint+resource_path
session = boto3.session.Session(region_name=region)
client = session.client("healthlake")
```

```
# Frame authorization
auth = AWSSigV4("healthlake", session=session)

# Calling data store FHIR endpoint using SigV4 auth

r = requests.post(resource_endpoint, json=requestBody, auth=auth, )
print(r.json())
```

如需使用適用於 Python AWSSDK 的 sigv4 授權的詳細資訊，請參閱 [Boto3 登入資料主題](#)。

我的資料不是 FHIR R4 格式 - 我是否仍然可以使用 HealthLake ？

只能將 FHIR R4 格式的資料匯入 HealthLake 資料存放區。如需提供產品以協助使用者轉換資料的合作夥伴清單，請參閱 [AWS HealthLake 合作夥伴](#)。

為什麼在將 FHIR RESTful APIs 用於以客戶受管KMS金鑰加密的資料存放區時，我會收到 AccessDenied 錯誤？

使用者或角色需要客戶受管金鑰和IAM政策的許可，才能存取資料存放區。使用者必須具有使用客戶受管金鑰的必要IAM許可。如果使用者已撤銷或淘汰授予 HealthLake使用客戶受管KMS金鑰許可的授予，HealthLake 將傳回 AccessDenied錯誤。

HealthLake 必須具備存取客戶資料的許可、加密匯入資料存放區的新FHIR資源，以及在請求資源時解密FHIR資源。

若要進一步了解，請參閱[對金鑰存取進行故障診斷](#)。

為什麼匯入失敗？

成功的匯入任務將產生具有 output inputFileName.ndjson 檔案的資料夾，但個別記錄可能無法匯入。發生這種情況時，會產生第二個FAILURE資料夾，其中包含無法匯入的記錄清單。存取資訊清單檔案的任務輸出位置為 JobPropertiesJobOutputDataConfig。S3Configuration.S3Uri。

此資訊清單檔案包含任務輸出的詳細資訊，例如所有成功回應的位置 (successOutput.successOutputS3Uri)、所有失敗回應的位置 (failureOutput.failureOutputS3Uri) 和其他任務指標。資訊清單檔案的內容可透過程式設計方式剖析。下列範例資訊清單檔案會列出 Amazon S3 儲存貯體的輸入和輸出，以及掃描的資源數量和成功匯入的資源數量等資訊。

```

{
  "inputDataConfig": {
    "s3Uri": "s3://amzn-s3-demo-source-bucket/healthlake-input/invalidInput/"
  },
  "outputDataConfig": {
    "s3Uri": "s3://amzn-s3-demo-logging-  

bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/",
    "encryptionKeyID": "arn:aws:kms:us-west-2:123456789012:key/  

fbbbfee3-20b3-42a5-a99d-c48c655ed545"
  },
  "successOutput": {
    "successOutputS3Uri": "s3://amzn-s3-demo-logging-  

bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/  

SUCCESS/"
  },
  "failureOutput": {
    "failureOutputS3Uri": "s3://amzn-s3-demo-logging-  

bucket/32839038a2f47f17c2fe0f53f0c3a0ba-FHIR_IMPORT-19dd7bb7bcc8ee12a09bf6d322744a3d/  

FAILURE/"
  },
  "numberOfScannedFiles": 1,
  "numberOfFilesImported": 1,
  "sizeOfScannedFilesInMB": 0.023627,
  "sizeOfDataImportedSuccessfullyInMB": 0.011232,
  "numberOfResourcesScanned": 9,
  "numberOfResourcesImportedSuccessfully": 4,
  "numberOfResourcesWithCustomerError": 5,
  "numberOfResourcesWithServerError": 0
}

```

若要分析匯入任務失敗的原因，請使用 `DescribeFHIRImport` 任務 API 來分析 `JobProperties`。建議採用以下方法：

- 如果狀態為 `FAILED` 且訊息存在，則失敗與任務參數相關，例如輸入資料大小或輸入檔案超出 HealthLake 配額的數量。
- 如果匯入任務狀態為 `COMPLETED_WITH_ERRORS`，請檢查資訊清單檔案 `Manifest.json`，以取得檔案未成功匯入的資訊。
- 如果匯入任務狀態為 `FAILED` 且訊息不存在，請前往任務輸出位置以存取資訊清單檔案 `Manifest.json`。

對於每個輸入檔案，都有失敗的輸出檔案，其中包含任何無法匯入之資源的輸入檔案名稱。回應包含對應於輸入資料位置的行號 (lineId)、FHIR回應物件 (UpdateResourceResponse) 和回應的狀態碼 (statusCode)。

範例輸出檔案看起來如下所示：

```
{
  "lineId": 3,
  "UpdateResourceResponse": {
    "jsonBlob": {
      "resourceType": "OperationOutcome",
      "issue": [
        {
          "severity": "error",
          "code": "processing",
          "diagnostics": "1 validation error detected: Value 'Patient123' at 'resourceType' failed to satisfy constraint: Member must satisfy regular expression pattern: [A-Za-z]{1,256}",
          "statusCode": 400
        }
      ]
    }
  }
},
{
  "lineId": 5,
  "UpdateResourceResponse": {
    "jsonBlob": {
      "resourceType": "OperationOutcome",
      "issue": [
        {
          "severity": "error",
          "code": "processing",
          "diagnostics": "This property must be a simple value, not a com.google.gson.JsonArray",
          "location": ["/EffectEvidenceSynthesis/name"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@telecom'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@gender'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@birthDate'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@address'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@maritalStatus'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@multipleBirthBoolean'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Unrecognised property '@communication'",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "warning",
          "code": "processing",
          "diagnostics": "Name should be usable as an identifier for the module by machine processing applications such as code generation [name.matches('[A-Z]([A-Za-z0-9_]){0,254}')]",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Profile http://hl7.org/fhir/StructureDefinition/EffectEvidenceSynthesis, Element 'EffectEvidenceSynthesis.status': minimum required = 1, but only found 0",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Profile http://hl7.org/fhir/StructureDefinition/EffectEvidenceSynthesis, Element 'EffectEvidenceSynthesis.population': minimum required = 1, but only found 0",
          "location": ["/EffectEvidenceSynthesis"],
          "severity": "error",
          "code": "processing",
          "diagnostics": "Profile http://hl7.org/fhir/StructureDefinition/EffectEvidenceSynthesis, Element 'EffectEvidenceSynthesis.exposure': minimum required = 1, but only found 0",
          "location": ["/EffectEvidenceSynthesis"]
        }
      ]
    }
  }
}
```

```

1, but only found 0", "location": ["EffectEvidenceSynthesis"]},
{"severity": "error", "code": "processing", "diagnostics": "Profile http://
hl7.org/fhir/StructureDefinition/EffectEvidenceSynthesis, Element
'EffectEvidenceSynthesis.exposureAlternative': minimum required
= 1, but only found 0", "location": ["EffectEvidenceSynthesis"]},
{"severity": "error", "code": "processing", "diagnostics": "Profile http://hl7.org/fhir/
StructureDefinition/EffectEvidenceSynthesis, Element 'EffectEvidenceSynthesis.outcome':
minimum required = 1, but only found 0", "location": ["EffectEvidenceSynthesis"]},
{"severity": "information", "code": "processing", "diagnostics": "Unknown
extension http://synthetichealth.github.io/synthea/disability-adjusted-
life-years", "location": ["EffectEvidenceSynthesis.extension[3]"]},
{"severity": "information", "code": "processing", "diagnostics": "Unknown extension
http://synthetichealth.github.io/synthea/quality-adjusted-life-years", "location":
["EffectEvidenceSynthesis.extension[4]"]}], "statusCode": 400}
{"lineId": 7, UpdateResourceResponse: {"jsonBlob":
{"resourceType": "OperationOutcome", "issue":
[{"severity": "error", "code": "processing", "diagnostics": "2 validation errors detected:
Value at 'resourceId' failed to satisfy constraint: Member must satisfy regular
expression pattern: [A-Za-z0-9-]{1,64}; Value at 'resourceId' failed to satisfy
constraint: Member must have length greater than or equal to 1"}]}, "statusCode": 400}
{"lineId": 9, UpdateResourceResponse: {"jsonBlob":
{"resourceType": "OperationOutcome", "issue":
[{"severity": "error", "code": "processing", "diagnostics": "Missing required id field in
resource json"]}], "statusCode": 400}
{"lineId": 15, UpdateResourceResponse: {"jsonBlob":
{"resourceType": "OperationOutcome", "issue":
[{"severity": "error", "code": "processing", "diagnostics": "Invalid JSON found in input
file"}]}, "statusCode": 400}

```

範例顯示輸入檔案中對應的輸入列第 3、4、7、9、15 行發生故障。對於這些行，說明如下：

- 在第 3 行，回應說明輸入檔案第 3 行 resourceType 所提供的 是無效的。
- 在第 5 行，回應說明輸入檔案的第 5 行中存在 FHIR 驗證錯誤。
- 在第 7 行中，回應會說明以輸入方式 resourceId 提供的 存在驗證問題。
- 在第 9 行，回應說明輸入檔案必須包含有效的資源 ID。
- 在第 15 行，輸入檔案的回應是檔案不是有效的 JSON 格式。

如何尋找 DocumentReference無法處理的資源？

如果 DocumentReference 資源無效，HealthLake 將提供表示驗證錯誤的延伸，而不是整合的醫療NLP輸出。為了尋找在NLP處理期間導致驗證錯誤 DocumentReference 的資源，客戶可以使用 HealthLake的搜尋函數搭配搜尋索引鍵cm-decoration-status和搜尋值 VALIDATION_ERROR。此搜尋會列出導致驗證錯誤的所有 DocumentReference 資源，以及描述錯誤性質的錯誤訊息。這些 DocumentReference 資源中具有驗證錯誤的延伸欄位結構將類似下列範例。

```
"extension": [
  {
    "extension": [
      {
        "url": "http://healthlake.amazonaws.com/aws-cm/status/",
        "valueString": "VALIDATION_ERROR"
      },
      {
        "url": "http://healthlake.amazonaws.com/aws-cm/message/",
        "valueString": "Resource led to too many nested objects after NLP
operation processed the document. 10937 nested objects exceeds the limit of 10000."
      }
    ],
    "url": "http://healthlake.amazonaws.com/aws-cm/"
  }
]
```

如果NLP裝飾建立超過 10,000 個巢狀物件，也可能發生 VALIDATION_ERROR。發生這種情況時，必須先將文件分割成較小的文件，才能進行處理。

遷移現有資料存放區以使用 Amazon Athena

2022 年 11 月 14 日之前建立的資料存放區可正常運作，但無法在 Athena 中使用進行查詢SQL。若需要使用 Athena 查詢預先存在的資料存放區，您必須先將其遷移至新的資料存放區。

將資料遷移至新的資料存放區

1. 建立新的資料存放區。
2. 將資料從預先存在的資料匯出至 Amazon S3 儲存貯體。
3. 從 Amazon S3 儲存貯體將資料匯入新的資料存放區。

將資料匯出至 Amazon S3 儲存貯體會產生額外費用。額外費用取決於您匯出的資料大小。

將 Athena 中的搜尋結果連接到其他 AWS 服務

與其他 AWS 服務共用 Athena 的搜尋結果時，您可能會遇到問題。

當您使用 `json_extract[1]` 做為 SQL 搜尋查詢的一部分時，可能會發生問題。

若要修正此問題，您必須更新至 CATVAR。

嘗試建立儲存結果、資料表（靜態）或檢視（動態）時，您可能會遇到此問題。

Athena 主控台在將資料匯入新資料存放區後無法運作

將資料匯入新的資料存放區後，資料可能無法立即使用。這是為了讓資料有時間擷取到 iceberg 資料表。稍後再試一次。

為什麼我會收到 Lake Formation 許可錯誤：lakeformation：新增資料湖管理員PutDataLakeSettings 時？

如果您的 IAM 使用者或角色包含 `AWSLakeFormationDataAdmin` AWS 受管政策，則無法新增資料湖管理員。您會收到包含下列項目的錯誤：

```
User arn:aws:sts::111122223333:assumed-role/lakeformation-admin-user is not authorized to perform: lakeformation:PutDataLakeSettings on resource: arn:aws:lakeformation:us-east-2:111122223333:catalog:111122223333 with an explicit deny in an identity-based policy
```

`AdministratorAccess` 需要 AWS 受管政策，才能將 IAM 使用者或角色新增為 AWS Lake Formation 資料湖管理員。如果您的 IAM 使用者或角色也包含 `AWSLakeFormationDataAdmin` 動作將會失敗。`AWSLakeFormationDataAdmin` AWS 受管政策包含 AWS Lake Formation API 操作的明確拒絕 `PutDataLakeSetting`。

即使是具有 AWS 使用 `AdministratorAccess` AWS 受管政策之完整存取權的管理員，也會受到 `AWSLakeFormationDataAdmin` 政策的限制。

如何開啟 HealthLake 整合的自然語言處理功能？

截至 2023 年 2 月 20 日，HealthLake 資料存放區的預設行為已變更。

目前的資料存放區：所有目前的 HealthLake 資料存放區都將停止使用 base64 編碼 DocumentReference 資源上的自然語言處理 (NLP)。這表示將不會使用分析新 DocumentReference 資源 NLP，也不會根據資源類型中的文字產生新 DocumentReference 資源。對於現有 DocumentReference 資源，透過產生的資料和資源會 NLP 保留，但不會在 2023 年 2 月 20 日之後更新。

新資料存放區：在 2023 年 2 月 20 日之後建立 HealthLake 的資料存放區將不會對 base64 編碼 DocumentReference 的資源執行自然語言處理 (NLP)。

若要開啟此功能，您必須使用 建立案例 [AWS Support Center Console](#)。若要建立案例，請登入您的 AWS 帳戶，然後選擇建立案例。若要進一步了解如何建立案例和案例管理，請參閱支援《使用者指南》中的 [建立支援案例和案例管理](#)。

我的資料存放區狀態不會從建立中變更

如果您嘗試建立新的 HealthLake 資料存放區，且資料存放區狀態並未從建立中變更，則需要更新 Athena 才能使用 AWS Glue Data Catalog。

若要進一步了解，請參閱《Amazon Athena 使用者指南》中的 [升級至 AWS Glue Data Catalog step-by-step](#)。

成功升級後 AWS Glue Data Catalog，您現在可以建立資料存放區。

若要移除舊的資料存放區，請使用 建立案例以開始使用 [AWS Support Center Console](#)。若要建立案例，請登入您的 AWS 帳戶，然後選擇建立案例。若要進一步了解，請參閱支援《使用者指南》中的 [建立支援案例和案例管理](#)。

我的 SDK 資料存放區建立狀態會傳回例外狀況或未知狀態

如果您的清單資料存放區或描述資料存放區 API 呼叫傳回例外狀況或未知的資料存放區狀態，請將您的更新 SDK 為最新版本。

使用 10MB 文件 FHIR POST API 進行操作，HealthLake 以取得 413 Request 實體過大錯誤。

AWS HealthLake 同步建立和更新 API 限制為 5MB，以避免增加延遲和逾時。

您可以使用 大量匯入，使用二進位來擷取高達 164MB ResourceType 的大型文件 API。

AWS HealthLake 開發人員指南的文件歷史記錄

下表說明 AWS HealthLake 版本的文件變更。

- API 版本：最新
- 文件最近更新時間：10/25/2024

變更	描述	日期
HealthLake 現在支援 FHIRhistory 和 vread 互動	HealthLake 現在支援擷取特定資源歷史記錄FHIRhistory的互動，以及執行特定版本資源讀取vread的互動。	2024 年 10 月 25 日
HealthLake 現在支援新的FHIR搜尋參數、延伸模組和資源類型。	HealthLake 現在支援新的FHIR搜尋參數、延伸模組和資源類型。	2023 年 12 月 9 日
HealthLake 現在支援 FHIR架構SMART上的	HealthLake 現在支援在FHIR已啟用 HealthLake 的資料存放區SMART上建立。	2023 年 5 月 31 日
HealthLake 現在支援設定檔驗證	HealthLake 現在支援FHIR設定檔驗證。	2023 年 5 月 31 日
HealthLake 現在支援 export	HealthLake 現在支援使用 FHIRRESTAPI操作 匯出檔案export。	2023 年 5 月 31 日
亞太區域（孟買）區域	AWS HealthLake 現可於亞太區域（孟買）區域使用。	2023 年 4 月 4 日
整合自然語言處理已關閉	HealthLake 自 2023 年 2 月 20 日起，在所有資料存放區上關閉整合的自然語言處理 (NLP)。	2023 年 2 月 20 日

HealthLake 與 Amazon Athena 整合	您現在可以使用 Athena 查詢 2022 年 11 月 14 日之後建立的資料存放區。	2022 年 11 月 14 日
總匯入任務大小增加	StartFHIRImport 任務請求中所有檔案的總大小上限為 500 GB。	2022 年 10 月 3 日
套件支援	HealthLake 現在支援用於擷取多個資源的套件資源類型。	2022 年 8 月 5 日
中 CRUD 操作的更新配額 HealthLake	HealthLake 現在支援更高的 CRUD 請求限制。	2022 年 7 月 14 日
包含支援	HealthLake 現在支援_include 資料存放區查詢。	2022 年 7 月 14 日
AWS HealthLake 現已正式推出	HealthLake 現已正式推出。	2020 年 7 月 30 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的[AWS 詞彙表](#)。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。