



# **AWS**認證資料

## Set up and administration

NetApp  
June 28, 2022

# 目錄

AWS認證資料 .....	1
AWS 認證與權限 .....	1
管理AWS認證資料和Cloud Manager訂閱 .....	3

# AWS認證資料

## AWS 認證與權限

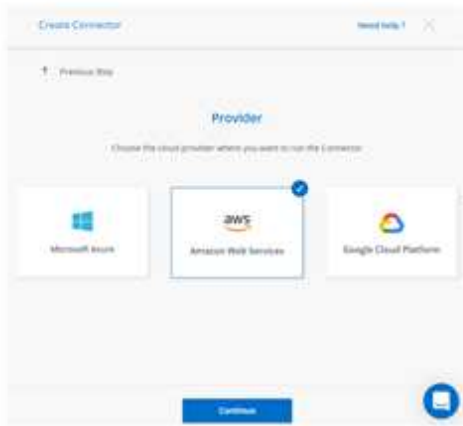
Cloud Manager 可讓您選擇部署 Cloud Volumes ONTAP 時要使用的 AWS 認證資料。您可以 Cloud Volumes ONTAP 使用初始 AWS 認證來部署所有的資訊系統、也可以新增其他認證資料。

### 初始 AWS 認證資料

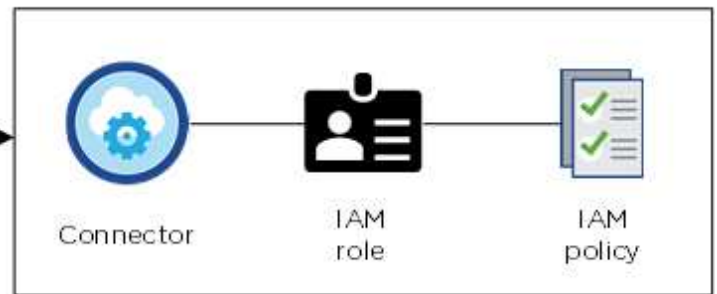
從Cloud Manager部署Connector時、您需要為IAM使用者提供IAM角色或存取金鑰的ARN。您使用的驗證方法必須具有必要的權限、才能在AWS中部署Connector執行個體。所需權限列於 "[AWS 的連接器部署原則](#)"。

Cloud Manager 在 AWS 中啟動 Connector 執行個體時、會為執行個體建立 IAM 角色和執行個體設定檔。它也附加原則、讓Connector有權限管理該AWS帳戶內的資源和程序。"[檢閱 Cloud Manager 如何使用權限](#)"。

#### Cloud Manager



#### AWS account



Cloud Manager 會在您為 Cloud Volumes ONTAP 下列項目建立新的工作環境時、依預設選取這些 AWS 認證資料：

Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

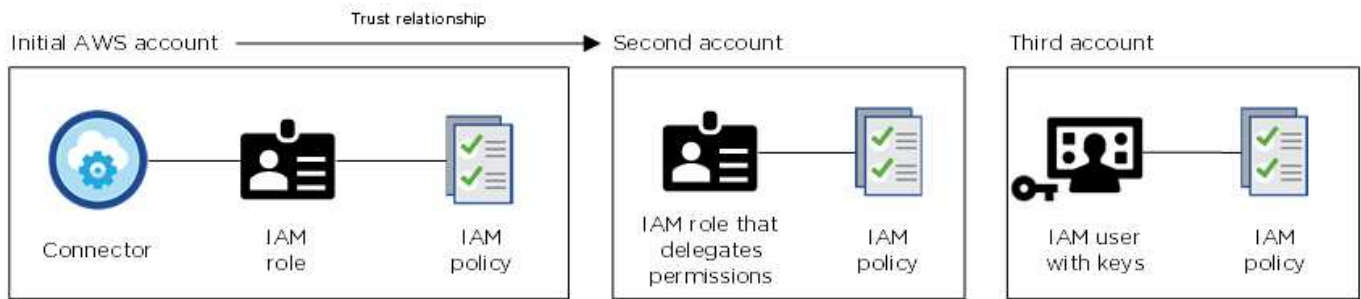
### 其他 AWS 認證資料

有兩種方法可以新增額外的AWS認證資料。

#### 將AWS認證資料新增至現有的Connector

如果您想要在 Cloud Volumes ONTAP 不同的 AWS 帳戶中啟動功能、您也可以選擇 "[為 IAM 使用者或信任帳戶中角色的 ARN 提供 AWS 金鑰](#)"。下圖顯示兩個額外的帳戶、一個透過信任帳戶中的 IAM 角色提供權限、另一

個則透過 IAM 使用者的 AWS 金鑰提供權限：



您可以 "將帳戶認證新增至 Cloud Manager" 指定 IAM 角色的 Amazon 資源名稱（ARN）或 IAM 使用者的 AWS 金鑰。

新增一組認證資料之後、您可以在建立新的工作環境時切換至這些認證資料：

直接將AWS認證資料新增至Cloud Manager

將新的AWS認證資料新增至Cloud Manager、可讓Cloud Manager擁有必要的權限、以建立和管理適用於ONTAP 整個作業環境的FSX、或是建立Connector。

## Marketplace 部署和內部部署呢？

以上各節說明建議的連接器部署方法、該方法來自 Cloud Manager。您也可以從部署 AWS 中的 Connector "AWS Marketplace" 您也可以 "在內部部署安裝連接器"。

如果您使用 Marketplace、則會以相同方式提供權限。您只需要手動建立和設定 IAM 角色、然後為任何其他帳戶提供權限。

對於內部部署、您無法為 Cloud Manager 系統設定 IAM 角色、但您可以像提供額外 AWS 帳戶一樣提供權限。

## 我該如何安全地旋轉 **AWS** 認證資料？

如上所述、Cloud Manager 可讓您以幾種方式提供 AWS 認證資料：與 Connector 執行個體相關的 IAM 角色、在信任的帳戶中擔任 IAM 角色、或提供 AWS 存取金鑰。

Cloud Manager 採用前兩個選項、使用 AWS 安全性權杖服務取得持續循環的暫用認證資料。此程序是最佳實務做法、它是自動且安全的。

如果您為 Cloud Manager 提供 AWS 存取金鑰、您應該定期在 Cloud Manager 中更新金鑰、藉此旋轉金鑰。這是完全手動的程序。

## 管理**AWS**認證資料和**Cloud Manager**訂閱

新增及管理AWS認證資料、讓Cloud Manager擁有在AWS帳戶中部署及管理雲端資源所需的權限。如果您管理多個 AWS 訂閱、您可以從「認證」頁面將每個訂閱指派給不同的 AWS 認證資料。

### 總覽

您可以將AWS認證資料新增至現有的Connector、或直接新增至Cloud Manager：

- 將AWS認證資料新增至現有的Connector

將新的AWS認證資料新增至現有的Connector、可讓您Cloud Volumes ONTAP 使用相同的Connector在另一個AWS帳戶中部署。 [瞭解如何將AWS認證資料新增至Connector](#)。

- 直接將AWS認證資料新增至Cloud Manager

將新的AWS認證資料新增至Cloud Manager、可讓Cloud Manager擁有必要的權限、以建立和管理適用於ONTAP 整個作業環境的FSX、或是建立Connector。 [瞭解如何將AWS認證資料新增至Cloud Manager](#)。

### 如何旋轉認證資料

Cloud Manager 可讓您以幾種方式提供 AWS 認證資料：與 Connector 執行個體相關的 IAM 角色、在信任的帳戶中擔任 IAM 角色、或提供 AWS 存取金鑰。 ["深入瞭解 AWS 認證與權限"](#)。

Cloud Manager 採用前兩個選項、使用 AWS 安全性權杖服務取得持續循環的暫用認證資料。此程序是最佳實務做法、因為它是自動且安全的。

如果您為 Cloud Manager 提供 AWS 存取金鑰、您應該定期在 Cloud Manager 中更新金鑰、藉此旋轉金鑰。這是完全手動的程序。

### 新增認證到**Connector**

將AWS認證資料新增至Connector、以便在Cloud Volumes ONTAP 其他AWS帳戶中部署及管理功能。您可以在其他帳戶中提供IAM角色的ARN、或是提供AWS存取金鑰。

## 授予權限

在您新增額外的AWS認證資料至Connector之前、您必須先提供必要的權限。這些權限可讓 Cloud Manager 管理該 AWS 帳戶內的資源和程序。您提供權限的方式取決於您是否要為Cloud Manager提供信任帳戶或AWS金鑰中角色的ARN。



當您從 Cloud Manager 部署 Connector 時、Cloud Manager 會自動為您部署 Connector 的帳戶新增 AWS 認證資料。如果您在現有系統上手動安裝 Connector 軟體、則不會新增此初始帳戶。"[深入瞭解 AWS 認證與權限](#)"。

- 選項 \*
- [\[Grant permissions by assuming an IAM role in another account\]](#)
- [\[Grant permissions by providing AWS keys\]](#)

在另一個帳戶中擔任IAM角色、藉此授予權限

您可以使用 IAM 角色、在部署 Connector 執行個體的來源 AWS 帳戶與其他 AWS 帳戶之間建立信任關係。接著、您將從信任的帳戶中、為 Cloud Manager 提供 IAM 角色的 ARN。

### 步驟

1. 前往您要部署Cloud Volumes ONTAP 的目標帳戶中的IAM主控台。
2. 在「存取管理」下、按一下\*「角色」>「建立角色」\*、然後依照步驟建立角色。

請務必執行下列動作：

- 在\*信任的實體類型\*下、選取\* AWS帳戶\*。
  - 選取\*其他AWS帳戶\*、然後輸入連接器執行個體所在帳戶的ID。
  - 使用Cloud Manager IAM原則建立原則、可從取得 "[Cloud Manager 原則頁面](#)"。
3. 複製IAM角色的角色ARN、以便稍後將其貼到Cloud Manager中。

帳戶現在擁有必要的權限。 [您現在可以將認證資料新增至Connector](#)。

### 提供AWS金鑰來授予權限

如果您想要為 IAM 使用者提供 AWS 金鑰給 Cloud Manager、則必須將必要的權限授予該使用者。Cloud Manager IAM 原則定義了允許 Cloud Manager 使用的 AWS 動作和資源。

### 步驟

1. 請從下載 Cloud Manager IAM 原則 "[Cloud Manager 原則頁面](#)"。
2. 從 IAM 主控台複製並貼上 Cloud Manager IAM 原則中的文字、以建立您自己的原則。

"[AWS 文件：建立 IAM 原則](#)"

3. 將原則附加至 IAM 角色或 IAM 使用者。
  - "[AWS 文件：建立 IAM 角色](#)"
  - "[AWS 文件：新增和移除 IAM 原則](#)"

帳戶現在擁有必要的權限。 [您現在可以將認證資料新增至Connector。](#)

## 新增認證資料

在您提供具備所需權限的AWS帳戶之後、您可以將該帳戶的認證資料新增至現有的Connector。這可讓您Cloud Volumes ONTAP 使用相同的Connector在該帳戶中啟動支援功能。

如果您剛在雲端供應商中建立這些認證資料、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

### 步驟

1. 請確定Cloud Manager目前已選取正確的Connector。
2. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。



3. 按一下\*「Add Credential\*（新增認證\*）」、然後依照精靈中的步驟進行。
  - a. 認證資料位置：選取\* Amazon Web Services > Connector\*。
  - b. 定義認證資料：提供可信IAM角色的ARN（Amazon資源名稱）、或輸入AWS存取金鑰和秘密金鑰。
  - c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。

若要以Cloud Volumes ONTAP 每小時費率（PAYGO）或是以年度合約支付、AWS認證資料必須與Cloud Volumes ONTAP 從AWS Marketplace訂閱的功能相關聯。
  - d. 審查：確認新認證資料的詳細資料、然後按一下\*新增\*。

現在、您可以在建立新的工作環境時、從「詳細資料與認證」頁面切換至不同的認證資料集：

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

## 新增認證資料至Cloud Manager

為Cloud Manager提供IAM角色的ARN、讓Cloud Manager擁有必要的權限、可為ONTAP 工作環境建立FSX或建立連接器、藉此將AWS認證新增至Cloud Manager。

您可以在建立FSXfor ONTAP the Sfor the Sfor the Sfor the Sfuse環境或建立新的Connector時、使用認證資料。

### 設定IAM角色

設定IAM角色、讓Cloud Manager SaaS能夠承擔角色。

#### 步驟

1. 前往目標帳戶中的IAM主控台。
2. 在「存取管理」下、按一下\*「角色」>「建立角色」\*、然後依照步驟建立角色。

請務必執行下列動作：

- 在\*信任的實體類型\*下、選取\* AWS帳戶\*。
- 選取\*其他AWS帳戶\*、然後輸入Cloud Manager SaaS的ID：952013314444。
- 建立一個原則、其中包含建立FSXfor ONTAP the S作業 環境或建立連接器所需的權限。
  - "檢視FSXfor ONTAP Sfor Sf哪些 權限"
  - 從檢視Connector部署原則 "Cloud Manager 原則頁面"

3. 複製IAM角色的角色ARN、以便在下一步將其貼到Cloud Manager中。

IAM角色現在擁有所需的權限。 [您現在可以將它新增至 Cloud Manager](#)。



## 新增認證資料

在您提供IAM角色所需的權限之後、請將角色ARN新增至Cloud Manager。

如果您剛建立IAM角色、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。



2. 按一下\*「Add Credential\*（新增認證\*）」、然後依照精靈中的步驟進行。
  - a. 認證資料位置：選取\* Amazon Web Services > Cloud Manager\*。
  - b. 定義認證資料：提供IAM角色的ARN（Amazon資源名稱）。
  - c. 審查：確認新認證資料的詳細資料、然後按一下\*新增\*。

現在您可以在建立FSXfor ONTAP the Sfor the Sfor the Sfor the fuse環境或建立新的Connector時、使用認證資料。

## 建立AWS訂閱的關聯

將 AWS 認證資料新增至 Cloud Manager 之後、您可以將 AWS Marketplace 訂閱與這些認證資料建立關聯。訂閱可讓您以Cloud Volumes ONTAP 小時費率（PAYGO）或使用年度合約來支付報銷費用、並使用其他NetApp雲端服務。

您可能會在將認證新增至 Cloud Manager 之後、在兩種情況下建立 AWS Marketplace 訂閱的關聯：

- 初次將認證新增至 Cloud Manager 時、您並未建立訂閱關聯。
- 您想要以新的訂閱取代現有的 AWS Marketplace 訂閱。

您必須先建立連接器、才能變更 Cloud Manager 設定。 ["瞭解如何建立連接器"](#)。

### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。
2. 按一下動作功能表以取得一組認證資料、然後選取「建立訂閱關聯」。



3. 從下拉式清單中選取現有的訂閱、或按一下「新增訂閱」、然後依照步驟建立新的訂閱。

▶ [https://docs.netapp.com/zh-tw/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-tw/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

## 編輯認證資料

在Cloud Manager中編輯AWS認證資料、方法是變更帳戶類型（AWS金鑰或承擔角色）、編輯名稱、或自行更新認證資料（金鑰或角色ARN）。



您無法編輯與Connector執行個體相關聯之執行個體設定檔的認證資料。

### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。
2. 按一下動作功能表以取得一組認證資料、然後選取\*編輯認證\*。
3. 進行必要的變更、然後按一下「套用」。

## 刪除認證資料

如果您不再需要一組認證資料、可以從Cloud Manager刪除。您只能刪除與工作環境無關的認證資料。



您無法刪除與連接器執行個體相關聯之執行個體設定檔的認證。

### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。
2. 按一下動作功能表以取得一組認證資料、然後選取\*刪除認證資料\*。
3. 按一下\*刪除\*以確認。

## 版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

NetApp保留隨時變更本文所述之任何產品的權利、恕不另行通知。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

## 商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。