



AWS

Setup and administration

NetApp
April 26, 2024

目錄

- AWS 1
 - 深入瞭解 AWS 認證與權限 1
 - 管理 BlueXP 的 AWS 認證和市場訂閱 4

AWS

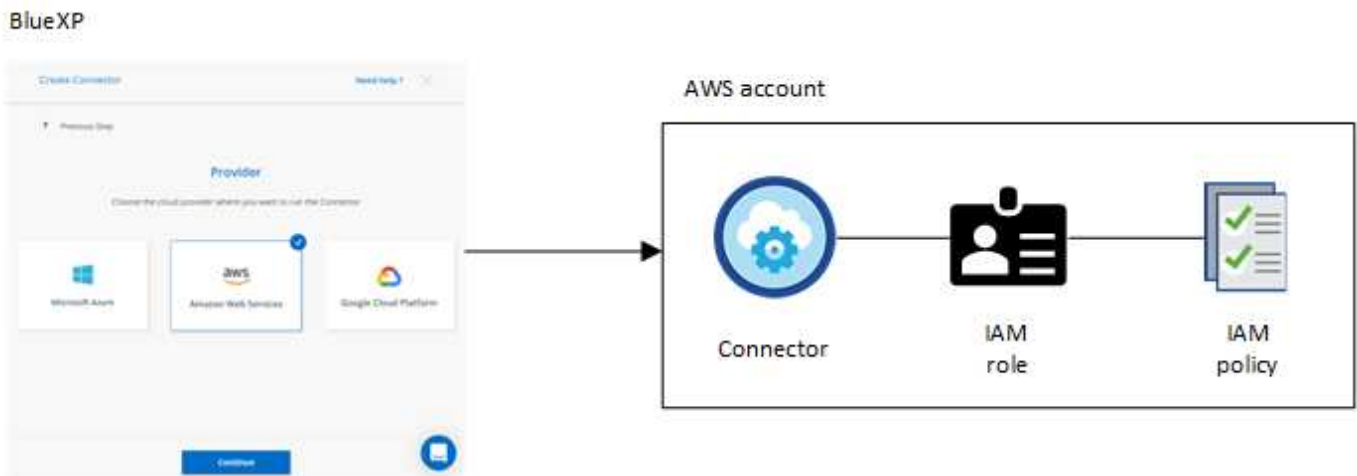
深入瞭解 AWS 認證與權限

瞭解 BlueXP 如何使用 AWS 認證來代表您執行動作、以及這些認證如何與市場訂閱相關聯。在 BlueXP 中管理一或多個 AWS 帳戶的認證時、瞭解這些詳細資料可能很有幫助。例如、您可能想要瞭解何時將額外的 AWS 認證新增至 BlueXP。

初始 AWS 認證資料

從BlueXP部署連接器時、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 Connector 部署原則"](#)。

當BlueXP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BlueXP如何使用權限"](#)。



如果您為 Cloud Volumes ONTAP 建立新的工作環境、BlueXP 預設會選取這些 AWS 認證：

Details & Credentials			
Instance Profile	Account ID	QA Subscription	Edit Credentials
Credentials		Marketplace Subscription	

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。

其他 AWS 認證資料

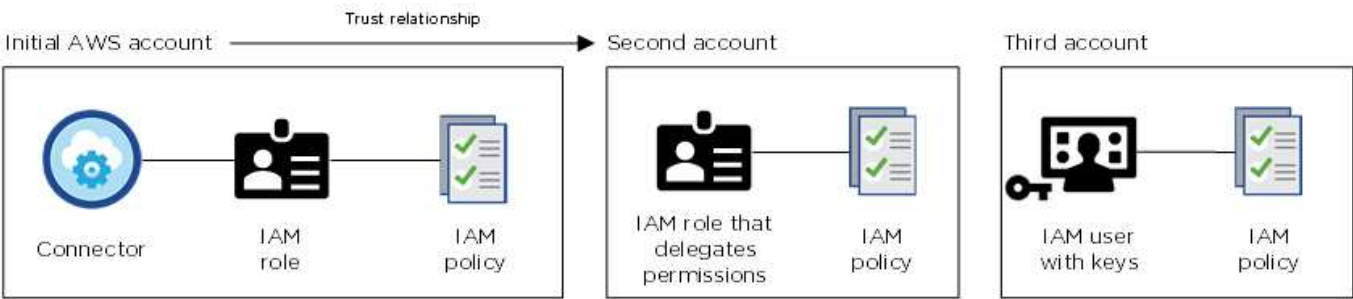
有兩種方法可以新增額外的 AWS 認證：

- 您可以將 AWS 認證新增至現有的 Connector
- 您可以直接將 AWS 認證新增至 BlueXP

請參閱以下各節以取得更多詳細資料。

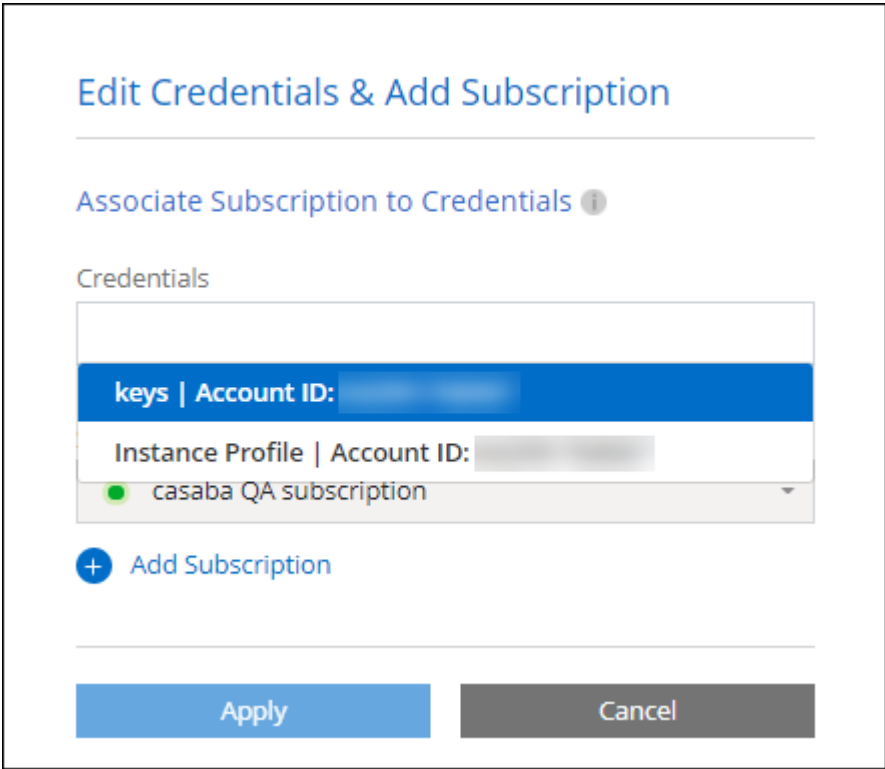
將**AWS**認證資料新增至現有的**Connector**

如果您想要將 BlueXP 與其他 AWS 帳戶搭配使用、則可以為 IAM 使用者提供 AWS 金鑰、或是在信任的帳戶中提供角色的 ARN。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：



然後您可以指定 IAM 角色的 Amazon 資源名稱（ARN）或 IAM 使用者的 AWS 金鑰、將帳戶認證新增至 BlueXP。

例如、您可以在建立新的 Cloud Volumes ONTAP 工作環境時、在認證之間切換：



"瞭解如何將 AWS 認證新增至現有的 Connector。"

直接將**AWS**認證資料新增至**BlueXP**

新增AWS認證資料至藍圖XP、可提供必要的權限來建立及管理適用於ONTAP 整個作業環境的FSX、或是建立Connector。

- ["瞭解如何將 AWS 認證新增至 BlueXP for Amazon FSX for ONTAP"](#)
- ["瞭解如何將 AWS 認證新增至 BlueXP 以建立 Connector"](#)

認證與市場訂閱

您新增至 Connector 的認證必須與 AWS Marketplace 訂閱相關聯、以便您可以按小時費率（PAYGO）或透過年度合約支付 Cloud Volumes ONTAP 費用、以及使用其他 BlueXP 服務。

["瞭解如何建立AWS訂閱的關聯"](#)。

請注意下列關於 AWS 認證和市場訂閱的資訊：

- 您只能將一項 AWS Marketplace 訂閱與一組 AWS 認證建立關聯
- 您可以使用新訂閱來取代現有的市場訂閱

常見問題集

下列問題與認證和訂閱有關。

我該如何安全地旋轉 **AWS** 認證資料？

如前節所述、BlueXP 可讓您以幾種方式提供 AWS 認證：與 Connector 執行個體相關聯的 IAM 角色、在信任的帳戶中擔任 IAM 角色、或提供 AWS 存取金鑰。

在前兩個選項中、BlueXP 會使用 AWS 安全性權杖服務來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 BlueXP 提供 AWS 存取金鑰、您應該定期在 BlueXP 中更新金鑰、以旋轉金鑰。這是完全手動的程序。

我可以變更適用於 **Cloud Volumes ONTAP** 工作環境的 **AWS Marketplace** 訂閱嗎？

是的、您可以。當您變更與一組認證相關聯的 AWS Marketplace 訂閱時、所有現有和新的 Cloud Volumes ONTAP 工作環境都會被收取新訂閱的費用。

["瞭解如何建立AWS訂閱的關聯"](#)。

我是否可以新增多個 **AWS** 認證、每個認證都有不同的市場訂閱？

屬於同一個 AWS 帳戶的所有 AWS 認證都會與相同的 AWS Marketplace 訂閱相關聯。

如果您有多個 AWS 認證屬於不同的 AWS 帳戶、則這些認證可以與相同的 AWS Marketplace 訂閱或不同的訂閱相關聯。

我可以將現有的 **Cloud Volumes ONTAP** 工作環境移至不同的 **AWS** 帳戶嗎？

否、您無法將與 Cloud Volumes ONTAP 工作環境相關的 AWS 資源移至不同的 AWS 帳戶。

認證如何適用於市場部署和內部部署？

以上各節說明建議的連接器部署方法、該方法來自於 BlueXP。您也可以從 AWS Marketplace 在 AWS 中部署

Connector、然後在自己的 Linux 主機上手動安裝 Connector 軟體。

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 BlueXP 系統設定 IAM 角色、但可以使用 AWS 存取金鑰提供權限。

若要瞭解如何設定權限、請參閱下列頁面：

- 標準模式
 - ["設定 AWS Marketplace 部署的權限"](#)
 - ["設定內部部署的權限"](#)
- ["設定受限模式的權限"](#)
- ["設定私有模式的權限"](#)

管理 BlueXP 的 AWS 認證和市場訂閱

新增及管理AWS認證資料、讓BlueXP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 Marketplace 訂閱、您可以從「認證」頁面將每個訂閱指派給不同的 AWS 認證。

總覽

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

- 將額外的AWS認證資料新增至現有的Connector

將AWS認證資料新增至現有的Connector、可提供必要的權限、以管理公有雲環境中的資源和程序。 [瞭解如何將AWS認證資料新增至Connector](#)。

- 將AWS認證資料新增至BlueXP以建立連接器

將新的AWS認證資料新增至藍圖XP、即可賦予藍圖XP建立Connector所需的權限。 [瞭解如何將AWS認證資料新增至藍圖XP](#)。

- 將AWS認證資料新增至適用於FSX ONTAP for Sf更新的BlueXP

新增AWS認證資料至藍圖XP、可讓藍圖XP擁有建立及管理FSXfor ONTAP Sfor的必要權限。 ["瞭解如何設定FSX for ONTAP Sfor Sfor Sfor的權限"](#)

如何旋轉認證資料

BlueXP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"](#)。

在前兩個選項中、BlueXP會使用AWS安全性權杖服務來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BlueXP提供AWS存取金鑰、您應該定期在BlueXP中更新金鑰、以旋轉金鑰。這是完全手動的程序。

新增其他認證資料至Connector

將額外的 AWS 認證新增至 Connector、讓它擁有在公有雲環境中管理資源和程序所需的權限。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。

如果您剛開始使用 BlueXP、["瞭解 BlueXP 如何使用 AWS 認證和權限"](#)。

授予權限

將AWS認證資料新增至Connector之前、您必須先提供必要的權限。這些權限可讓BlueXP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BlueXP提供信任帳戶或AWS金鑰中角色的ARN。



如果您從BlueXP部署Connector、則BlueXP會自動為您部署Connector的帳戶新增AWS認證資料。如果您從AWS Marketplace部署Connector、或是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 *
- [在另一個帳戶中擔任IAM角色、藉此授予權限](#)
- [提供AWS金鑰來授予權限](#)

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、您會向BlueXP提供來自信任帳戶的IAM角色ARN。

如果連接器安裝在內部部署環境中、您就無法使用此驗證方法。您必須使用AWS金鑰。

步驟

1. 前往您要為Connector提供權限的目標帳戶中的IAM主控台。
2. 在「存取管理」下、選取 * 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。
- 複製並貼上的內容、以建立所需的原則 ["連接器的IAM原則"](#)。

3. 複製IAM角色的角色ARN、以便稍後將其貼到BlueXP中。

結果

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

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

如果連接器安裝在內部部署環境中、則必須使用此驗證方法。您無法使用IAM角色。

步驟

1. 從IAM主控台複製並貼上的內容、以建立原則 "連接器的IAM原則"。

"AWS 文件：建立 IAM 原則"

2. 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"

結果

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。

開始之前

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BlueXP。

步驟

1. 確定目前在BlueXP中選取正確的連接器。
2. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。



3. 在 * 帳戶認證 * 頁面上、選取 * 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。

若要以每小時費率（PAYGO）或每年合約來支付 BlueXP 服務、AWS 認證必須與 AWS Marketplace 訂閱相關聯。

- d. * 審查 *：確認新認證的詳細資料、然後選取 * 新增 *。

結果

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BlueXP以建立連接器

提供IAM角色的ARN、為BlueXP提供建立Connector所需的權限、將AWS認證新增至BlueXP。您可以在建立新的Connector時選擇這些認證資料。

設定IAM角色

設定 IAM 角色、讓 BlueXP SaaS 層能夠擔任此角色。

步驟

1. 前往目標帳戶中的IAM主控台。
2. 在「存取管理」下、選取 * 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BlueXP SaaS的ID：952013314444.
- 建立包含建立Connector所需權限的原則。
 - "檢視FSXfor ONTAP Sfor Sf哪些 權限"
 - "檢視Connector部署原則"

3. 複製IAM角色的角色ARN、以便在下一步將其貼到BlueXP中。

結果

IAM角色現在擁有所需的權限。 [您現在可以將它新增至藍圖XP。](#)

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BlueXP。

開始之前

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BlueXP。

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。



2. 在 * 帳戶認證 * 頁面上、選取 * 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 > BlueXP*。
 - b. 定義認證資料：提供IAM角色的ARN（Amazon資源名稱）。
 - c. * 審查 *：確認新認證的詳細資料、然後選取 * 新增 *。

結果

您現在可以在建立新的Connector時使用認證資料。

將認證新增至適用於 Amazon FSX for ONTAP 的 BlueXP

如需詳細資訊、請參閱 ["適用於 Amazon FSX for ONTAP 的 BlueXP 文件"](#)

建立AWS訂閱的關聯

將AWS認證資料新增至BlueXP之後、您可以將AWS Marketplace訂閱與這些認證資料建立關聯。訂閱可讓您以每小時費率（PAYGO）或使用年度合約支付 Cloud Volumes ONTAP 費用、並使用其他 BlueXP 服務。

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

- 當您初次將認證新增至BlueXP時、並未建立訂閱關聯。
- 您想要變更與 AWS 認證相關的 AWS Marketplace 訂閱。

以新訂閱取代目前的市場訂閱、可變更任何現有 Cloud Volumes ONTAP 工作環境和所有新工作環境的市場訂閱。

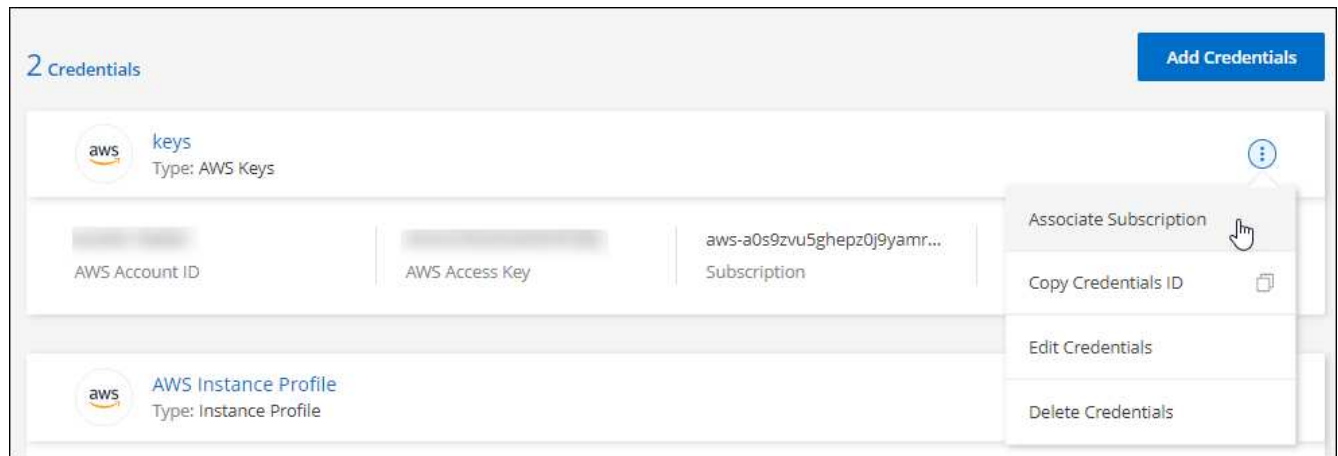
開始之前

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

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。
2. 選取一組認證的動作功能表、然後選取 * 關聯訂閱 *。

您必須選取與 Connector 相關聯的認證。您無法將市場訂閱與 BlueXP 相關的認證建立關聯。



3. 若要將認證與現有訂閱建立關聯、請從下拉式清單中選取訂閱、然後選取 * 關聯 * 。
4. 若要將認證與新訂閱建立關聯、請選取 * 新增訂閱 > 繼續 * 、然後依照 AWS Marketplace 中的步驟進行：
 - a. 選取 * 檢視購買選項 * 。
 - b. 選取 * 訂閱 * 。
 - c. 選取 * 設定您的帳戶 * 。

您將被重新導向至BlueXP網站。

- d. 從*訂閱指派*頁面：

- 選取您要與此訂閱建立關聯的 BlueXP 帳戶。
- 在「取代現有訂閱」欄位中、選擇您是否要使用此新訂閱來自動取代現有的單一帳戶訂閱。

此新訂閱取代現有的帳戶所有認證訂閱。如果一組認證資料從未與訂閱建立關聯、則此新訂閱將不會與這些認證資料建立關聯。

對於所有其他帳戶、您必須重複這些步驟、手動建立訂閱的關聯。

- 選擇*保存*。

下列影片顯示從 AWS Marketplace 訂閱的步驟：

從 AWS Marketplace 訂閱 BlueXP

將現有訂閱與您的帳戶建立關聯

當您從 AWS Marketplace 訂閱 BlueXP 時、程序的最後一個步驟是從 BlueXP 網站將訂閱與您的 BlueXP 帳戶建立關聯。如果您未完成此步驟、則無法將訂閱與 BlueXP 帳戶搭配使用。

如果您是從 AWS Marketplace 訂閱 BlueXP 、但您錯過了將訂閱與帳戶關聯的步驟、請遵循下列步驟。

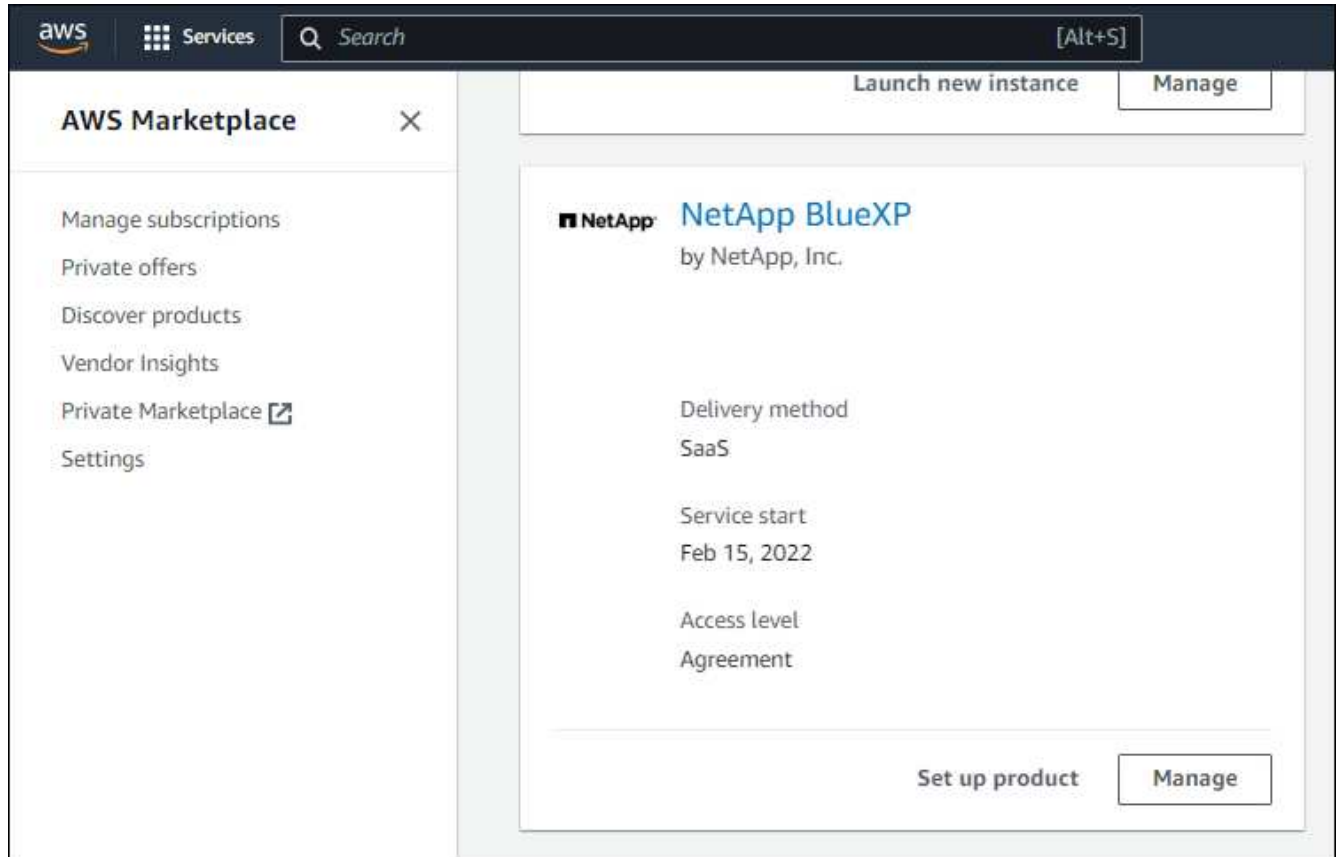
步驟

1. 請前往 BlueXP 數位錢包、確認您的訂閱並未與 BlueXP 帳戶建立關聯。

- a. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
- b. 選擇*訂閱*。
- c. 確認您的 BlueXP 訂閱未出現。

您只會看到與您目前檢視的帳戶相關聯的訂閱內容。如果您沒有看到您的訂閱、請繼續執行下列步驟。

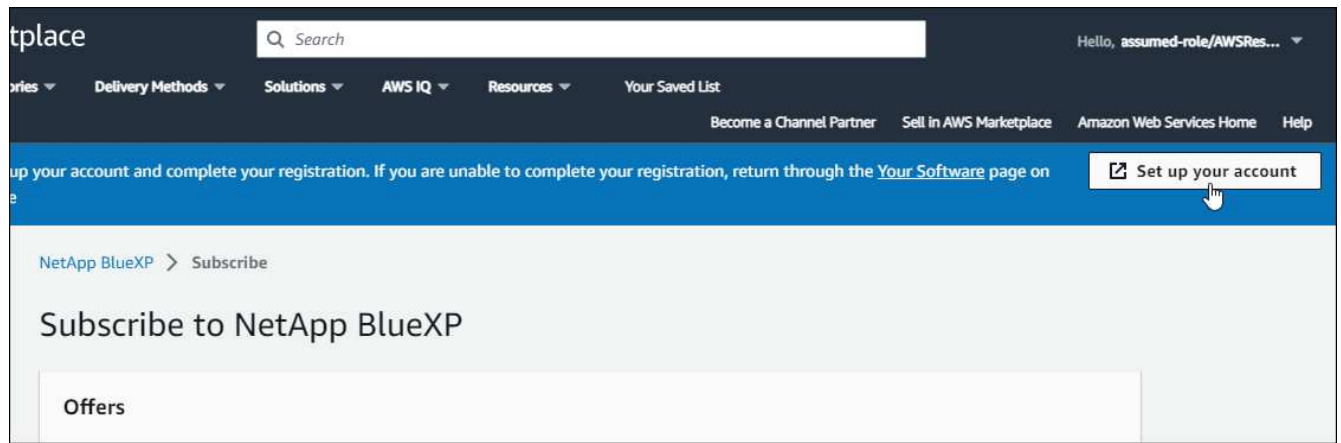
2. 登入 AWS 主控台並瀏覽至 * AWS Marketplace Subscriptions *。
3. 尋找 NetApp BlueXP 訂閱。



4. 選取 * 設定產品 *。

訂閱優惠頁面應載入新的瀏覽器索引標籤或視窗。

5. 選取 * 設定您的帳戶 *。



netapp.com 上的 * 訂閱指派 * 頁面應載入新的瀏覽器索引標籤或視窗。

請注意、系統可能會提示您先登入 BlueXP 。

6. 從*訂閱指派*頁面：

- 選取您要與此訂閱建立關聯的 BlueXP 帳戶。
- 在「取代現有訂閱」欄位中、選擇您是否要使用此新訂閱來自動取代現有的單一帳戶訂閱。

此新訂閱取代現有的帳戶所有認證訂閱。如果一組認證資料從未與訂閱建立關聯、則此新訂閱將不會與這些認證資料建立關聯。

對於所有其他帳戶、您必須重複這些步驟、手動建立訂閱的關聯。

Subscription Assignment

✓

Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name

PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with.

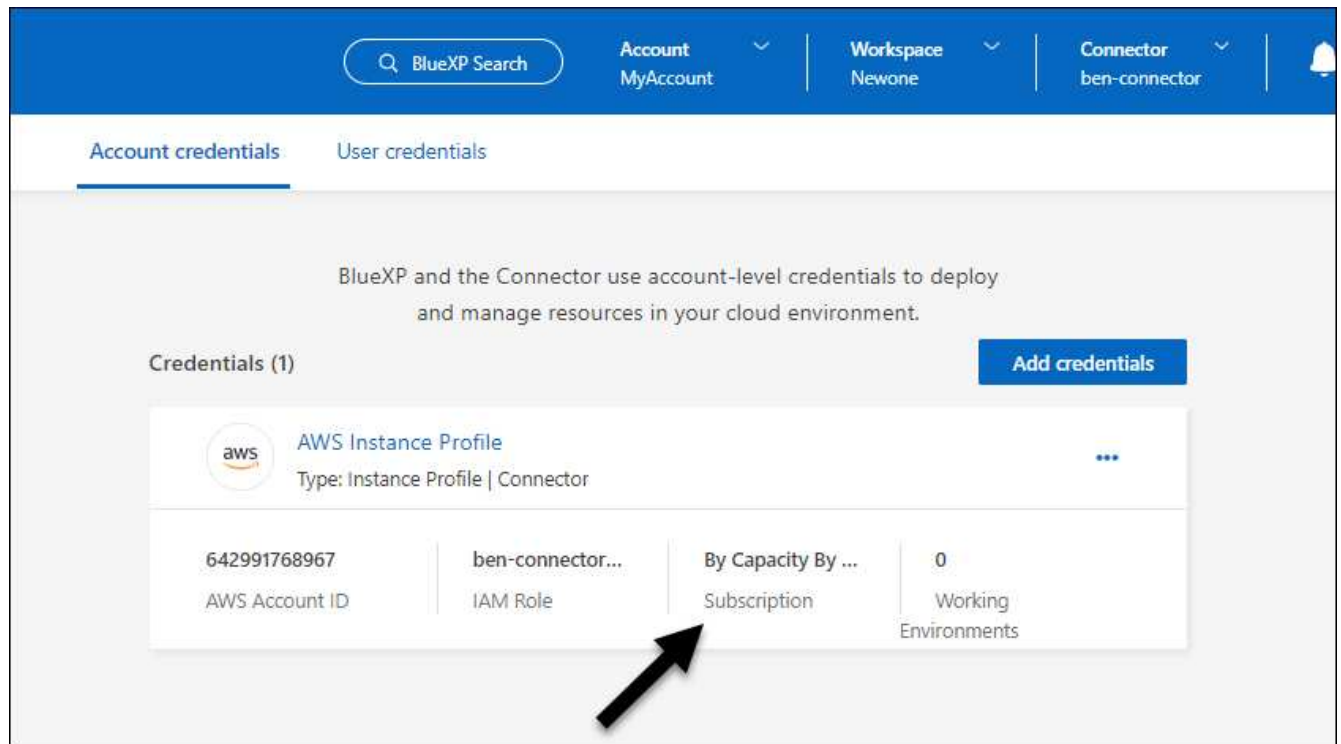
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

7. 請前往 BlueXP 數位錢包、確認訂閱內容已與您的 BlueXP 帳戶建立關聯。
 - a. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
 - b. 選擇*訂閱*。
 - c. 確認您的 BlueXP 訂閱已出現。
8. 確認訂閱已與您的 AWS 認證建立關聯。
 - a. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。
 - b. 在 * 帳戶認證 * 頁面上、確認訂閱與 AWS 認證相關聯。

以下是範例。



編輯認證資料

在BlueXP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 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。
2. 在 * 帳戶認證 * 頁面上、選取一組認證的動作功能表、然後選取 * 編輯認證 *。
3. 進行必要的變更、然後選取 * 套用 *。

刪除認證

如果您不再需要一組認證資料、可以從BlueXP中刪除。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 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。
2. 在 * 帳戶認證 * 頁面上、選取一組認證的動作功能表、然後選取 * 刪除認證 *。
3. 選擇 * 刪除 * 進行確認。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。