



管理BlueXP

Setup and administration

NetApp
April 26, 2024

目錄

管理BlueXP	1
使用與BlueXP的身分識別聯盟	1
BlueXP 帳戶	6
連接器	19
認證與訂閱	38

管理BlueXP

使用與BlueXP的身分識別聯盟

Identity Federation®啟用單一登入BlueXP、讓使用者可以使用公司身分的認證登入。若要開始使用、請瞭解身分識別聯盟如何與BlueXP搭配運作、然後檢閱設定程序的總覽。

與 NSS 認證的身分識別聯盟

如果您使用 NetApp 支援網站（NSS）認證登入 BlueXP、則不應遵循本頁的指示來設定身分識別聯盟。您應該改為執行下列動作：

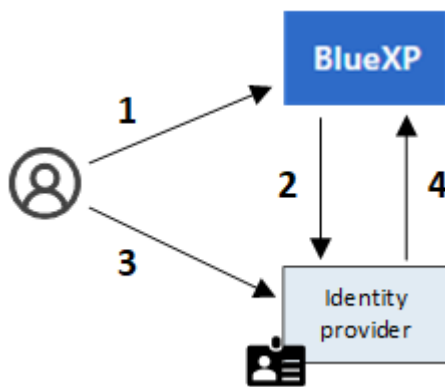
- 下載並完成 "[NetApp 聯盟申請表](#)"
- 將表單提交至表單中指定的電子郵件地址

NetApp 身分識別與存取管理團隊將審查您的申請。

身分識別聯盟的運作方式

設定身分識別聯盟會在BlueXP的驗證服務供應商（auth0）和您自己的身分識別管理供應商之間建立信任連線。

下圖說明身分識別聯盟如何與BlueXP搭配運作：



1. 使用者在BlueXP登入頁面上輸入電子郵件地址。
2. BlueXP會識別電子郵件網域是聯盟連線的一部分、並使用信任的連線將驗證要求傳送給身分識別供應商。

當您設定聯盟連線時、BlueXP一律會使用該聯盟連線進行驗證。

3. 使用者使用公司目錄中的認證資料進行驗證。
4. 您的身分識別供應商會驗證使用者的身分識別、且使用者已登入BlueXP。

身分識別聯盟使用開放式標準、例如安全聲明標記語言2.0（SAML）和OpenID Connect（OIDC）。

支援的身分識別供應商

BlueXP支援下列身分識別供應商：

- 安全聲明標記語言（SAML）身分識別供應商
- Microsoft Entra ID
- Active Directory Federation Services（ADFS）
- PingFedate

BlueXP僅支援服務供應商啟動（SP啟動）SSO。不支援身分識別供應商起始（IDP初始化）SSO。


設定程序總覽

在您建立BlueXP與身分識別管理供應商之間的連線之前、您應該先瞭解所需採取的步驟、以便做好相應的準備。

這些步驟僅適用於使用 NetApp 雲端登入登入 BlueXP 的使用者。如果您使用 NSS 認證登入 BlueXP、[瞭解如何使用 NSS 認證設定身分識別聯盟](#)。

SAML身分識別供應商

在高層級上、在BlueXP與SAML身分識別供應商之間建立聯盟連線包括下列步驟：

步驟	完成者	說明
1.	Active Directory（AD）管理員	<p>設定您的SAML身分識別供應商、以啟用與BlueXP的身分識別聯盟功能。</p> <p>檢視SAML身分識別供應商的指示：</p> <ul style="list-style-type: none">• "ADFS"• "奧塔"• "OneLogin"• "PingFedate"• "Salesforce"• "產品型資料夾"• "SSOCircle" <p>如果您的身分識別供應商未出現在上方清單中、"請遵循下列一般指示"</p> <div> 請勿完成介紹如何在驗證0中建立連線的步驟。您將在下一步建立該連線。</div>

步驟	完成者	說明
2.	BlueXP管理	<p>前往 "NetApp聯盟設定頁面" 並建立與BlueXP的連線。</p> <p>若要完成此步驟、您必須向AD管理員取得身分識別供應商的下列資訊：</p> <ul style="list-style-type: none"> • 登入URL • X509簽署憑證（PEE或CERE格式） • 登出URL（選用） <p>使用此資訊建立連線之後、「Federation Setup」頁面會列出可傳送給AD管理員的參數、以便在下一步完成組態設定。</p> <div>  <p>請記下憑證到期日。您需要返回「聯盟設定」頁面、並在憑證過期前更新憑證。這是您的責任。BlueXP 不會追蹤到期日。最好與您的AD 團隊合作、準時收到警示。</p> </div>
3.	廣告管理員	完成步驟2之後、請使用「聯盟設定」頁面上顯示的參數、在身分識別供應商上完成組態設定。
4.	BlueXP管理	<p>從測試並啟用連線 "NetApp聯盟設定頁面"</p> <p>請注意、測試連線和啟用連線之間的頁面會重新整理。</p>

Microsoft Entra ID


在高層級上、設定 BlueXP 與 Microsoft Entra ID 之間的聯盟連線包括下列步驟：

步驟	完成者	說明
1.	廣告管理員	<p>設定 Microsoft Entra ID 以啟用與 BlueXP 的身分識別聯盟。</p> <p>檢視使用 Microsoft Entra ID 登錄應用程式的指示</p> <div>  <p>請勿完成介紹如何在驗證0中建立連線的步驟。您將在下一步建立該連線。</p> </div>

步驟	完成者	說明
2.	BlueXP管理	<p>前往 "NetApp聯盟設定頁面" 並建立與BlueXP的連線。</p> <p>若要完成此步驟、您必須向AD管理員取得下列資訊：</p> <ul style="list-style-type: none"> • 用戶端ID • 用戶端機密值 • Microsoft Entra ID 網域 <p>使用此資訊建立連線之後、「Federation Setup」頁面會列出可傳送給AD管理員的參數、以便在下一步完成組態設定。</p> <div>  <p>請記下秘密金鑰到期日。您需要返回「聯盟設定」頁面、並在憑證過期前更新憑證。這是您的責任。BlueXP 不會追蹤到期日。最好與您的 AD 團隊合作、準時收到警示。</p> </div>
3.	廣告管理員	完成步驟 2 之後、請使用「聯盟設定」頁面上顯示的參數、完成 Microsoft Entra ID 的組態設定。
4.	BlueXP管理	<p>從測試並啟用連線 "NetApp聯盟設定頁面"</p> <p>請注意、測試連線和啟用連線之間的頁面會重新整理。</p>

ADFS

在高層級上、在BlueXP和ADFS之間設定聯盟連線包括下列步驟：

步驟	完成者	說明
1.	廣告管理員	<p>設定ADFS伺服器以啟用與BlueXP的身分識別聯盟。</p> <p>"檢視使用auth0設定ADFS伺服器的指示"</p>
2.	BlueXP管理	<p>前往 "NetApp聯盟設定頁面" 並建立與BlueXP的連線。</p> <p>若要完成此步驟、您必須向AD管理員取得下列資訊：ADFS伺服器的URL或同盟中繼資料檔案。</p> <p>使用此資訊建立連線之後、「Federation Setup」頁面會列出可傳送給AD管理員的參數、以便在下一步完成組態設定。</p> <div>  <p>請記下憑證到期日。您需要返回「聯盟設定」頁面、並在憑證過期前更新憑證。這是您的責任。BlueXP 不會追蹤到期日。最好與您的 AD 團隊合作、準時收到警示。</p> </div>
3.	廣告管理員	完成步驟2後、使用「Federation Setup」（聯盟設定）頁面上顯示的參數、完成ADFS伺服器上的組態。

步驟	完成者	說明
4.	BlueXP管理	從測試並啟用連線 "NetApp聯盟設定頁面" 請注意、測試連線和啟用連線之間的頁面會重新整理。

PingFedate

在高層級上、在BlueXP與PingFedate伺服器之間設定聯盟連線包括下列步驟：

步驟	完成者	說明
1.	廣告管理員	設定您的PingFederation伺服器、以啟用與BlueXP的身分識別聯盟。 "檢視建立連線的指示"  請勿完成介紹如何在驗證0中建立連線的步驟。您將在下一步建立該連線。
2.	BlueXP管理	前往 "NetApp聯盟設定頁面" 並建立與BlueXP的連線。 若要完成此步驟、您必須向AD管理員取得下列資訊： <ul style="list-style-type: none">• PingFedate伺服器的URL• X509簽署憑證（PEE或CERE格式） 使用此資訊建立連線之後、「Federation Setup」頁面會列出可傳送給AD管理員的參數、以便在下一步完成組態設定。  請記下憑證到期日。您需要返回「聯盟設定」頁面、並在憑證過期前更新憑證。這是您的責任。BlueXP 不會追蹤到期日。最好與您的AD 團隊合作、準時收到警示。
3.	廣告管理員	完成步驟2之後、請使用「聯盟設定」頁面上顯示的參數、在PingFederation伺服器上完成設定。
4.	BlueXP管理	從測試並啟用連線 "NetApp聯盟設定頁面" 請注意、測試連線和啟用連線之間的頁面會重新整理。

正在更新聯盟連線

在BlueXP管理員啟用連線之後、管理員可以隨時從更新連線 ["NetApp聯盟設定頁面"](#)

例如、您可能需要上傳新的憑證來更新連線。

建立連線的BlueXP管理員是唯一能夠更新連線的授權使用者。如果您想新增其他管理員、請聯絡NetApp支援部門。

BlueXP 帳戶

管理 BlueXP 帳戶

建立 BlueXP 帳戶時、只會包含單一管理員使用者和工作區。您可以透過新增使用者、建立自動化服務帳戶、新增工作區等方式來管理帳戶、以符合組織的需求。

["瞭解 BlueXP 帳戶的運作方式"](#)。

使用 Tenancy API 管理您的帳戶

如果您想要透過傳送API要求來管理帳戶設定、則必須使用_Tenancy API。此API與您用來建立及管理Cloud Volumes ONTAP 各種運作環境的BlueXP API不同。

["檢視Tenancy API的端點"](#)

建立及管理使用者

您帳戶中的使用者可以存取及管理特定工作區中的資源。

新增使用者

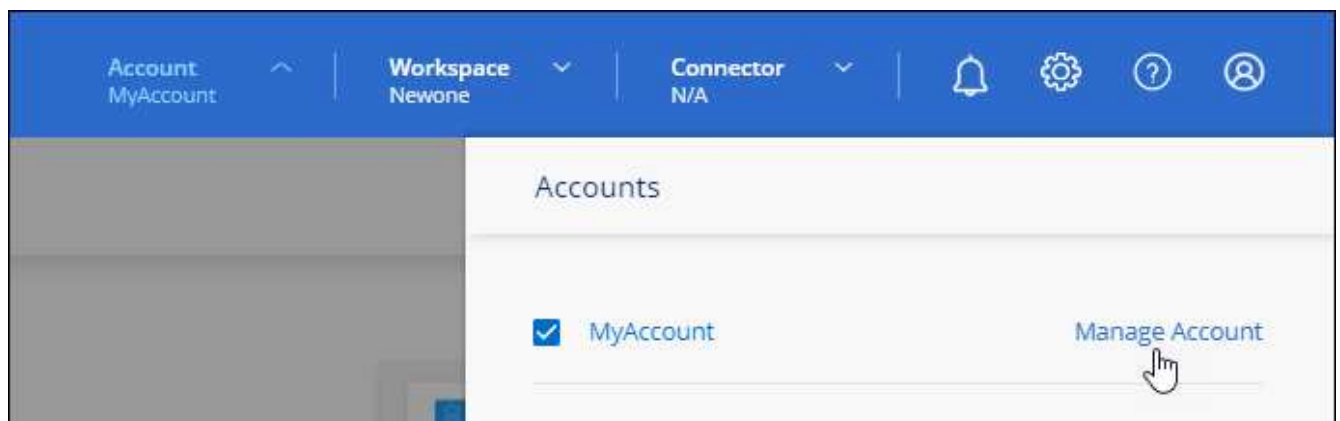
將使用者與您的 BlueXP 帳戶建立關聯、讓這些使用者能夠在 BlueXP 中建立及管理工作環境。

步驟

1. 如果使用者尚未這麼做、請要求使用者前往 ["NetApp BlueXP網站"](#) 並註冊。
2. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單。

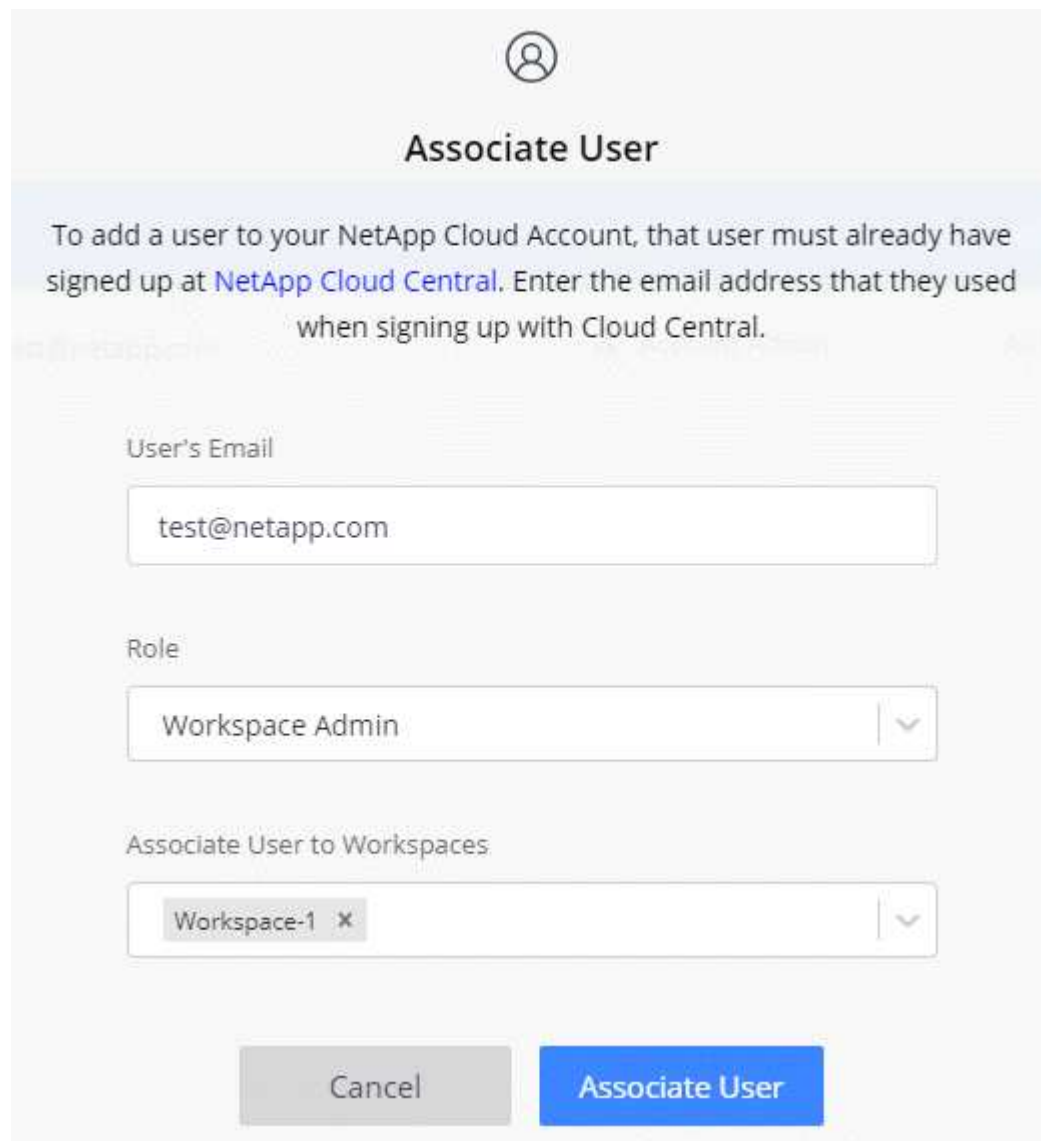


3. 選取目前所選帳戶旁的 * 管理帳戶 * 。



4. 從「成員」索引標籤中、選取 * 關聯使用者 * 。

5. 輸入使用者的電子郵件地址、然後為使用者選取角色：
 - 帳戶管理：可在BlueXP中執行任何動作。
 - * 工作區管理 *：可在指派的工作區中建立及管理資源。
 - * 法規遵循檢視器 *：只能檢視 BlueXP 分類的法規遵循資訊、並為擁有存取權限的工作區產生報告。
6. 如果您選取「工作區管理」或「法規遵循檢視器」、請選取一個或多個工作區以與該使用者建立關聯。



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this banner are three input fields: "User's Email" with the text "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close icon. At the bottom are two buttons: "Cancel" and "Associate User".

7. 選取 * 關聯 *。

結果

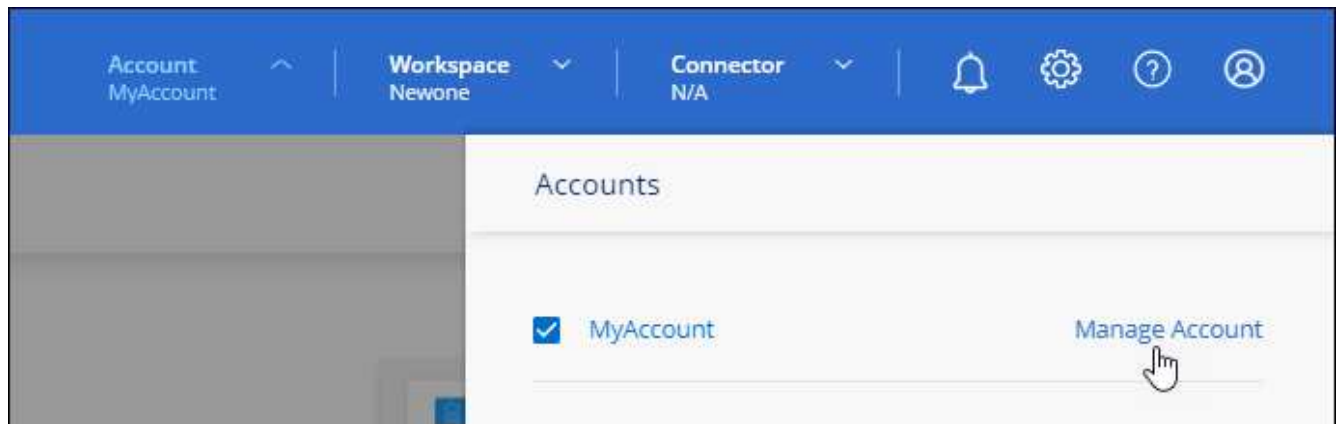
使用者應收到NetApp BlueXP寄送的電子郵件、標題為「Account Association（客戶關聯）」。電子郵件中包含存取BlueXP所需的資訊。

移除使用者

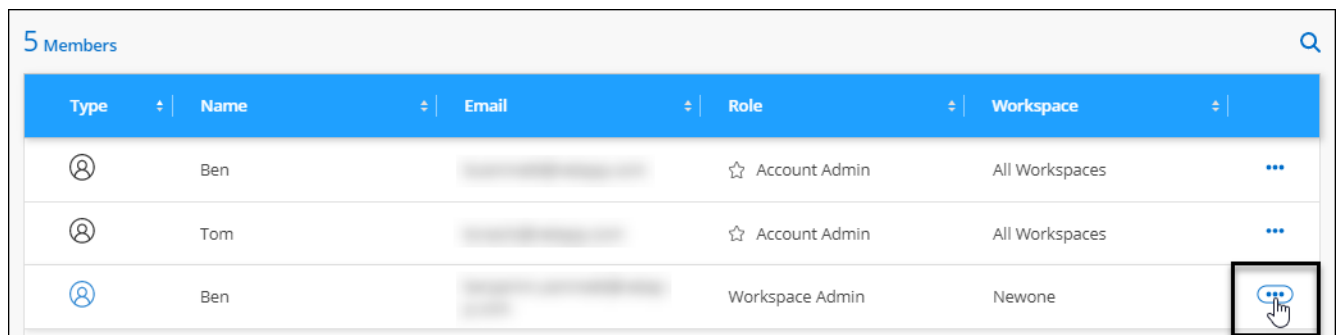
解除使用者的關聯、使其無法再存取 BlueXP 帳戶中的資源。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。



2. 從「成員」索引標籤中、選取與使用者對應的列中的動作功能表。



3. 選取 * 取消使用者關聯 *、然後選取 * 解除關聯 * 進行確認。

結果

使用者無法再存取此 BlueXP 帳戶中的資源。

管理 Workspace 管理的工作區

您可以隨時建立工作區管理員與工作區的關聯和取消關聯。建立使用者關聯可讓他們在該工作區中建立及檢視工作環境。



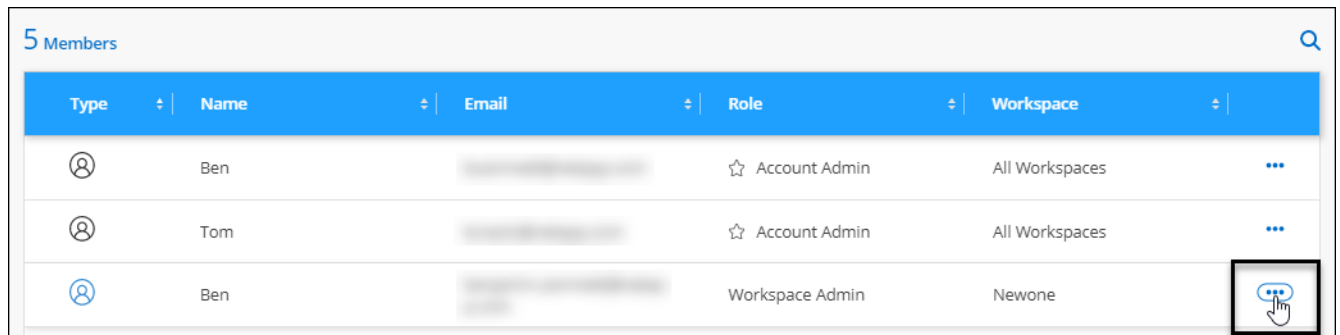
您也需要將 Connector 與工作區建立關聯、讓 Workspace 管理員可以從 BlueXP 存取這些工作區。"瞭解如何管理 Connector 的工作區"。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。



2. 從「成員」索引標籤中、選取與使用者對應的列中的動作功能表。



3. 選取 * 管理工作區 * 。

4. 選取要與使用者建立關聯的工作區、然後選取 * 套用 * 。

結果

只要Connector也與工作區相關聯、使用者就能從BlueXP存取這些工作區。

建立及管理服務帳戶

服務帳戶扮演「使用者」的角色、可撥打授權API呼叫至BlueXP以進行自動化。如此一來、您就不需要根據實際使用者帳戶建置自動化指令碼、也能隨時離開公司、因此更容易管理自動化作業。

您可以將服務帳戶指派為角色、就像其他任何BlueXP使用者一樣、為其授予權限。您也可以將服務帳戶與特定工作區建立關聯、以控制服務可以存取的工作環境（資源）。

建立服務帳戶時、BlueXP可讓您複製或下載服務帳戶的用戶端ID和用戶端密碼。此金鑰組用於驗證BlueXP。

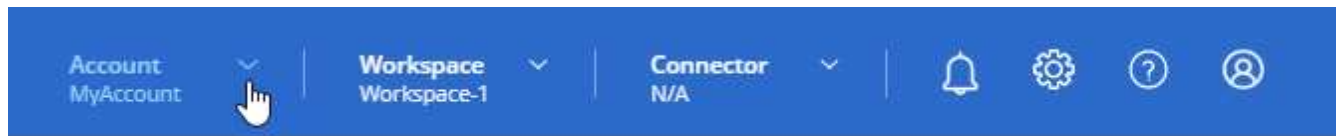
請注意、使用服務帳戶時、API 作業不需要重新整理權杖。"瞭解重新整理權杖"

建立服務帳戶

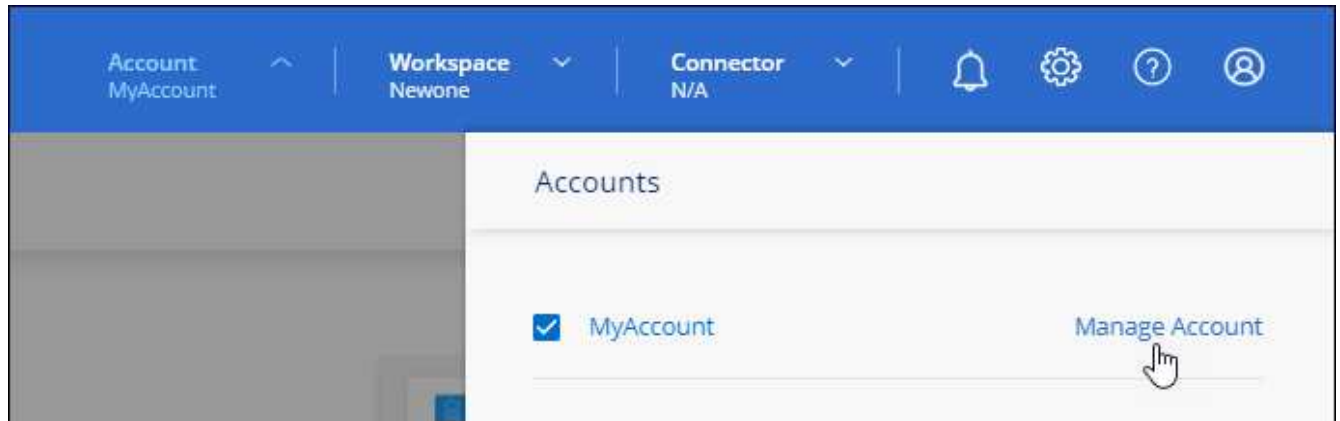
建立所需數量的服務帳戶、以管理工作環境中的資源。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單。



2. 選取目前所選帳戶旁的 * 管理帳戶 * 。



3. 從「成員」標籤中、選取 * 建立服務帳戶 * 。
4. 輸入名稱並選取角色。如果您選擇帳戶管理員以外的角色、請選擇要與此服務帳戶建立關聯的工作區。
5. 選擇 * Create （建立） 。
6. 複製或下載用戶端ID和用戶端密碼。

用戶端機密只會顯示一次、而且不會儲存在任何位置。複製或下載機密、並安全地儲存。

7. 選擇 * 關閉 * 。

取得服務帳戶的承載權杖

以便對進行API呼叫 "租戶API"、您需要取得服務帳戶的承載權杖。

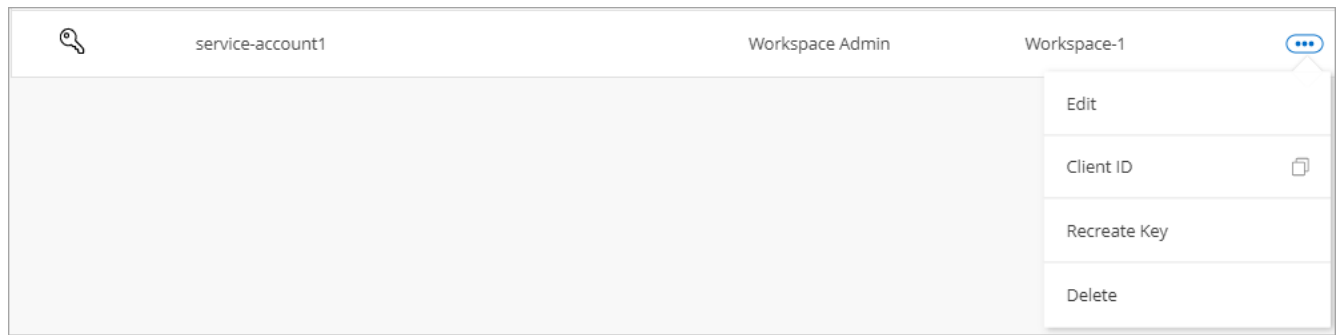
["瞭解如何建立服務帳戶權杖"](#)

複製用戶端 ID

您可以隨時複製服務帳戶的用戶端ID。

步驟

1. 從「成員」索引標籤中、選取與服務帳戶對應的列中的動作功能表。



2. 選取 * 用戶端 ID* 。

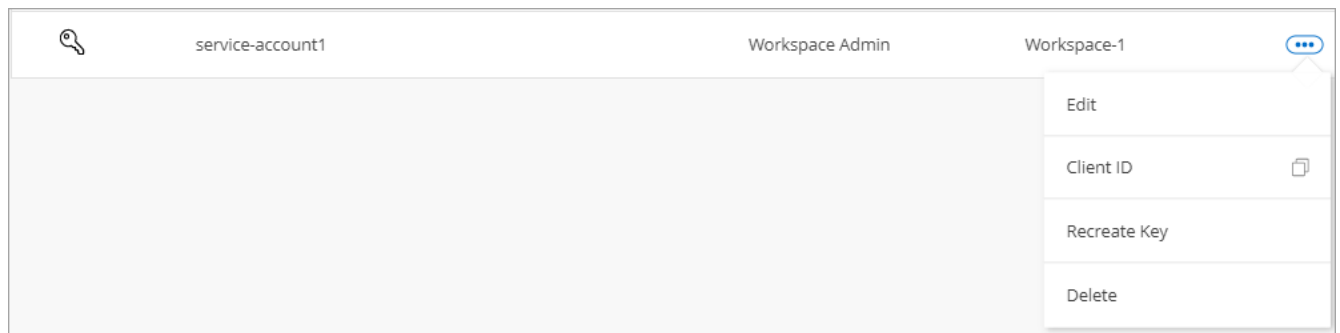
3. ID會複製到剪貼簿。

重新建立金鑰

重新建立金鑰會刪除此服務帳戶的現有金鑰、然後建立新金鑰。您將無法使用上一個按鍵。

步驟

1. 從「成員」索引標籤中、選取與服務帳戶對應的列中的動作功能表。



2. 選取 * 重新建立金鑰* 。

3. 選取 * 重新建立* 以確認。

4. 複製或下載用戶端ID和用戶端密碼。

用戶端機密只會顯示一次、而且不會儲存在任何位置。複製或下載機密、並安全地儲存。

5. 選擇*關閉*。

刪除服務帳戶

如果您不再需要使用服務帳戶、請將其刪除。

步驟

1. 從「成員」索引標籤中、選取與服務帳戶對應的列中的動作功能表。



2. 選擇*刪除*。
3. 再次選擇 * 刪除 * 進行確認。

管理工作區

透過建立、重新命名及刪除工作區來管理工作區。請注意、如果工作區包含任何資源、您就無法刪除該工作區。它必須是空的。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。
2. 選取 * 工作區 * 。
3. 請選擇下列其中一個選項：
 - 選取 * 新增工作區 * 以建立新的工作區。
 - 選取 * 重新命名 * 以重新命名工作區。
 - 選取 * 刪除 * 以刪除工作區。

如果您建立了新的工作區、也必須將 Connector 新增至該工作區。如果您未新增 Connector、則 Workspace 管理員將無法存取工作區中的任何資源。如需詳細資訊、請參閱下一節。

管理 **Connector** 的工作區

您需要將Connector與工作區建立關聯、讓Workspace Admins能夠從BlueXP存取這些工作區。

如果您只有帳戶管理員、則不需要將 Connector 與工作區建立關聯。帳戶管理員預設能夠存取BlueXP中的所有工作區。

["深入瞭解使用者、工作區和連接器"](#)。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。
2. 選取 * Connector * 。
3. 為您要關聯的 Connector 選取 * 管理 Workspace* 。
4. 選取要與 Connector 建立關聯的工作區、然後選取 * 套用 * 。

變更您的帳戶名稱

隨時變更您的帳戶名稱、將其變更為對您有意義的名稱。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。
2. 在 * 總覽 * 標籤中、選取帳戶名稱旁的編輯圖示。
3. 輸入新的帳戶名稱、然後選取 * 儲存 * 。

允許私有預覽

允許帳戶中的私人預覽、以存取 BlueXP 中的預覽形式提供的新服務。

私有預覽中的服務無法保證其行為符合預期、而且可能會持續中斷運作並喪失功能。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。
2. 在「總覽」標籤中、啟用「允許私有預覽」設定。

允許第三方服務

允許您帳戶中的第三方服務存取BlueXP中提供的第三方服務。第三方服務是類似NetApp所提供服務的雲端服務、但由第三方公司管理及支援。

步驟

1. 從 BlueXP 頂端、選取 * 帳戶 * 下拉式清單、然後選取 * 管理帳戶 * 。
2. 在「總覽」標籤中、啟用「允許協力廠商服務」設定。

監控您帳戶中的作業


您可以監控BlueXP執行的作業狀態、查看是否有任何需要解決的問題。您可以在「通知中心」、「時間表」中檢視狀態、或將通知傳送至您的電子郵件。

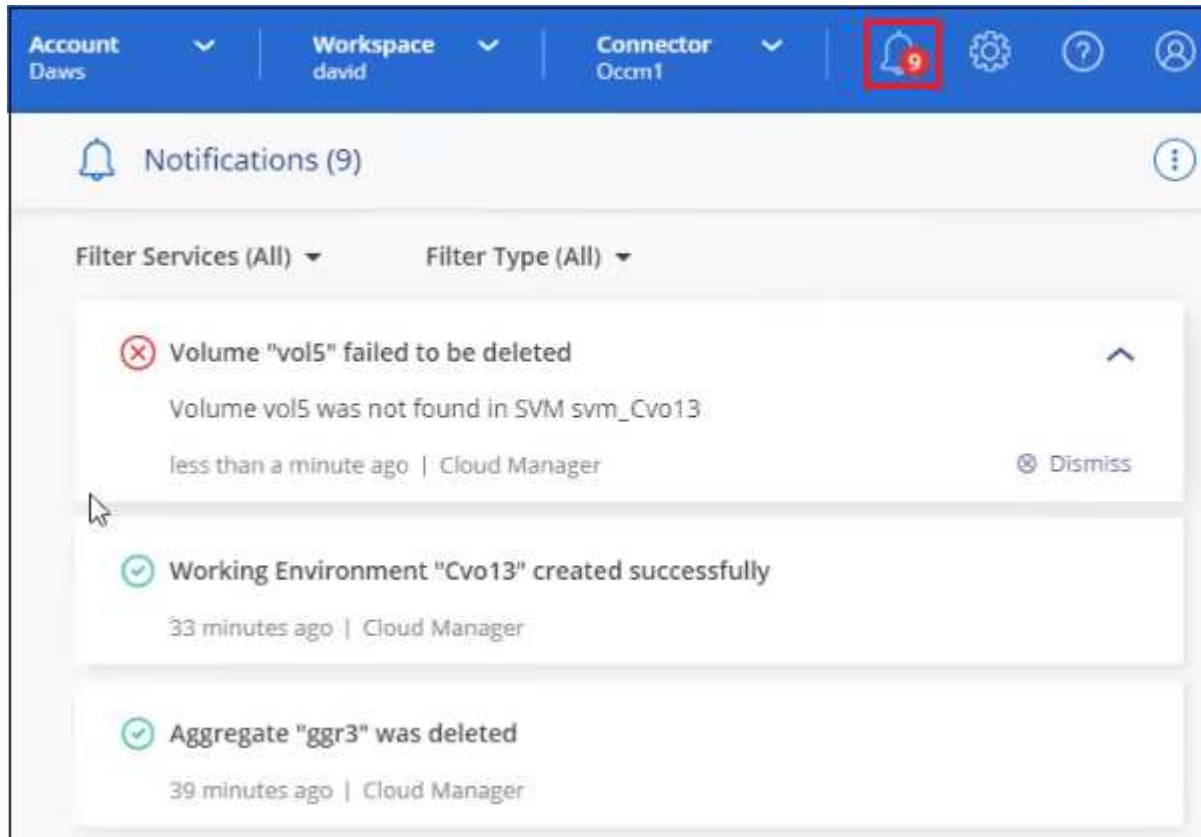
下表提供「通知中心」與「時間表」的比較、讓您瞭解每個項目的內容。

通知中心	時間表
顯示事件和行動的高層級狀態	提供每個事件或行動的詳細資料、以供進一步調查
顯示目前登入工作階段的狀態（登出後、資訊不會顯示在通知中心）	保留上個月的狀態
僅顯示在使用者介面中啟動的動作	顯示UI或API的所有動作
顯示使用者啟動的動作	顯示所有動作、無論是使用者啟動或系統啟動
依重要性篩選結果	依服務、行動、使用者、狀態及其他項目篩選
可將通知以電子郵件傳送給帳戶使用者和其他人	無電子郵件功能

使用通知中心監控活動

通知會追蹤您在BlueXP中啟動的作業進度、以便您確認作業是否成功。這些功能可讓您檢視您在目前登入工作階段期間所啟動的許多BlueXP動作狀態。目前並非所有 BlueXP 服務都會將資訊回報至通知中心。

您可以選取通知鈴（）。警示中的小球型罩顏色代表作用中的最高層級嚴重性通知。因此、如果您看到紅色的球型罩、就表示您應該查看重要通知。



您也可以將 BlueXP 設定為透過電子郵件傳送特定類型的通知、以便即使您未登入系統、也能得知重要的系統活動。您可以將電子郵件傳送給任何屬於 BlueXP 帳戶的使用者、或是任何其他需要注意特定類型系統活動的收件者。瞭解如何操作 [設定電子郵件通知設定](#)。

通知類型

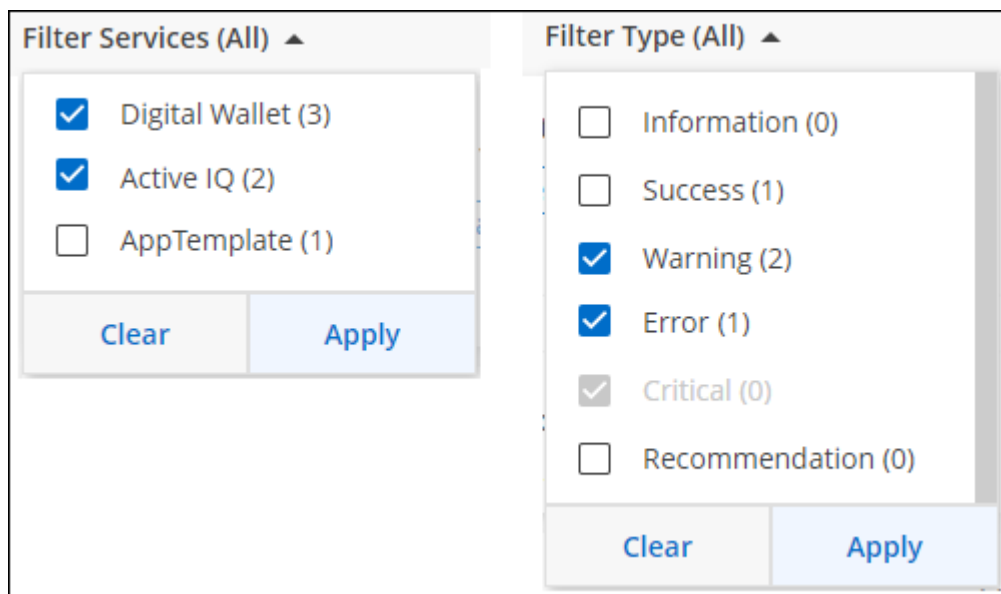
通知分為下列類別：

通知類型	說明
關鍵	如果未立即採取修正行動、可能導致服務中斷。
錯誤	某項行動或程序因故障而結束、或是在未採取修正行動時可能導致故障。
警告	您應注意的問題、以確保其未達到嚴重嚴重性。此嚴重性的通知不會造成服務中斷、因此可能不需要立即採取修正行動。
建議	系統建議您採取行動來改善系統或特定服務、例如：節省成本、建議新服務、建議的安全組態等
資訊	提供有關行動或程序的其他資訊的訊息。

通知類型	說明
成功	已成功完成行動或程序。

篩選通知

依預設、您會在通知中心看到所有作用中的通知。您可以篩選看到的通知、僅顯示對您很重要的通知。您可以依BlueXP「服務」和通知「類型」進行篩選。

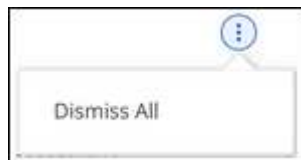


例如、如果您只想查看BlueXP作業的「錯誤」和「警告」通知、請選取這些項目、您只會看到這些類型的通知。

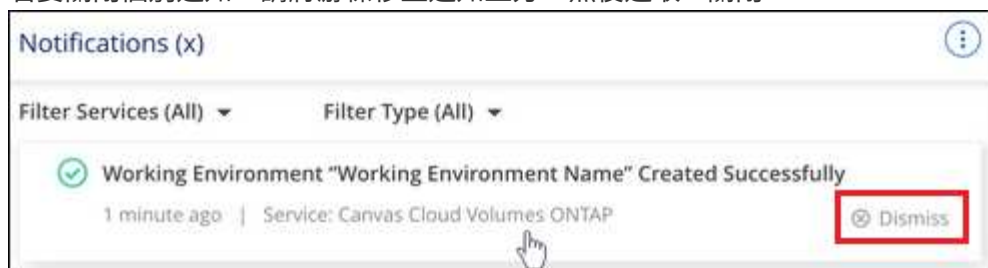
關閉通知

如果您不再需要查看通知、可以從頁面移除通知。您可以一次關閉所有通知、也可以關閉個別通知。

若要關閉所有通知、請在通知中心中選取 並選擇*全部關閉*。



若要關閉個別通知、請將游標移至通知上方、然後選取 * 關閉 * 。



設定電子郵件通知設定

您可以透過電子郵件傳送特定類型的通知、即使您尚未登入BlueXP、也能得知重要的系統活動。您可以將電子

郵件傳送給任何屬於 BlueXP 帳戶的使用者、或是任何其他需要注意特定類型系統活動的收件者。



- 目前、系統會以電子郵件傳送通知、說明下列 BlueXP 功能與服務：Connector、BlueXP 數位錢包、BlueXP 複本與同步、BlueXP 備份與還原、BlueXP 分層和 BlueXP 移轉報告。未來版本將會新增其他服務。
- 如果Connector安裝在沒有網際網路存取的網站上、則不支援傳送電子郵件通知。

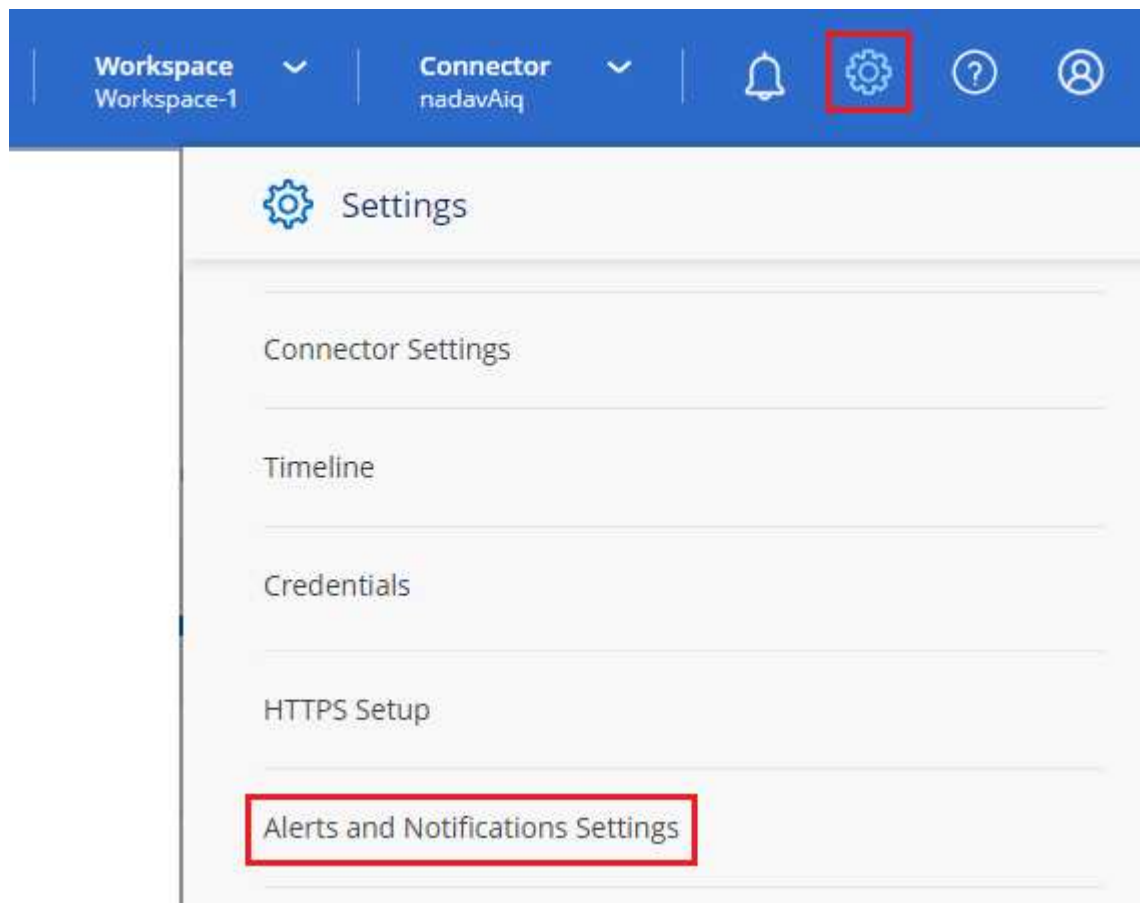
您在通知中心中設定的篩選條件並不會決定您將透過電子郵件收到的通知類型。根據預設、BlueXP帳戶管理員會收到所有「重大」和「建議」通知的電子郵件。這些通知涵蓋所有服務、您無法選擇僅接收特定服務的通知、例如 Connectors 或 BlueXP 備份與還原。

所有其他使用者和收件者均設定為不接收任何通知電子郵件、因此您需要為任何其他使用者設定通知設定。

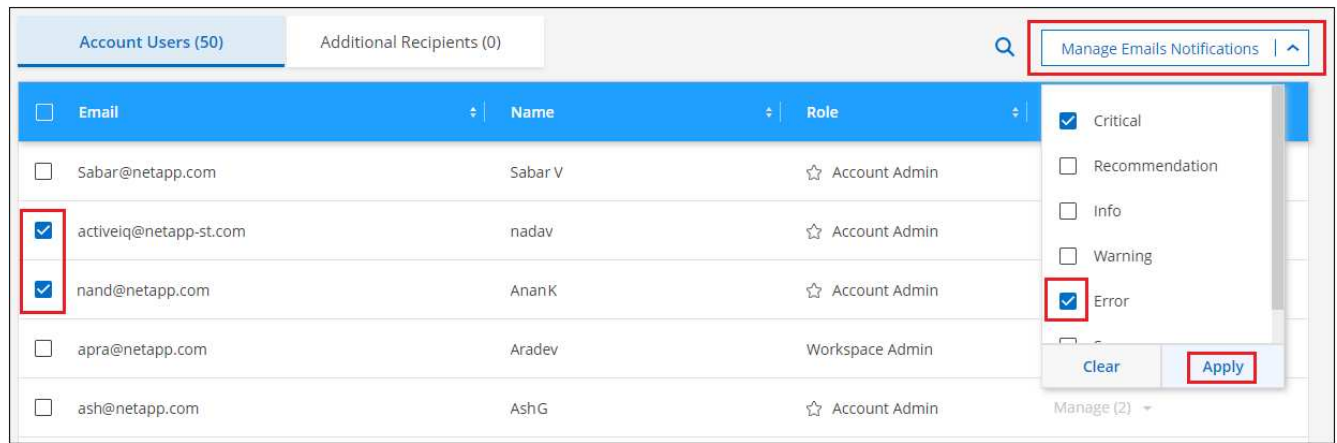
您必須是帳戶管理員、才能自訂通知設定。

步驟

1. 從 BlueXP 功能表列中、選取 * 設定 > 警示與通知設定 *。



2. 從「帳戶使用者」索引標籤或「其他收件者」索引標籤中選取一位或多位使用者、然後選擇要傳送的通知類型：
 - 若要變更單一使用者、請在該使用者的「通知」欄中選取功能表、檢查要傳送的通知類型、然後選取 * 套用 *。
 - 若要對多位使用者進行變更、請勾選每位使用者的方塊、選取 * 管理電子郵件通知 *、勾選要傳送的通知類型、然後選取 * 套用 *。



新增其他電子郵件收件者

出現在 *Account Users* 標籤中的使用者會自動從 BlueXP 帳戶中的使用者（從 "管理帳戶頁面"）。您可以在「其他收件者」索引標籤中新增電子郵件地址、以供無權存取BlueXP但需要收到特定警示和通知類型通知的其他人員或群組使用。

步驟

1. 從「警示與通知設定」頁面中、選取 * 新增收件者 * 。

The screenshot shows the 'Add New Recipient' form. It has a title 'Add New Recipient' in blue. Below the title are three input fields: 'Email' with the value 'saul.jenkin@gmail.com', 'Name' with the value 'Saul Jenkin', and 'Notification Type' which is a multi-select dropdown showing 'Critical', 'Recommendation', and 'Error'. At the bottom of the form are two buttons: 'Add New Recipient' and 'Cancel'.

2. 輸入姓名、電子郵件地址、然後選取收件者將收到的通知類型、然後選取 * 新增收件者 * 。

稽核您帳戶中的使用者活動

藍圖XP中的時間表顯示使用者為管理您的帳戶而完成的動作。這包括關聯使用者、建立工作區、建立連接器等管理動作。

如果您需要識別執行特定行動的人員、或是需要識別行動的狀態、檢查時間表會很有幫助。

步驟

1. 從 BlueXP 功能表列中、選取 * 設定 > 時間軸 * 。
2. 在篩選器下、選取 * 服務 * 、啟用 * 佔用 * 、然後選取 * 套用 * 。

結果

時間軸會更新以顯示帳戶管理動作。

建立另一個 BlueXP 帳戶

當您註冊 BlueXP 時、系統會提示您為組織建立帳戶。您可能只需要這個帳戶、但如果您的企業需要多個帳戶、則需要使用 Tenancy API 來建立其他帳戶。

使用下列 API 呼叫建立其他 BlueXP 帳戶：

貼文 /tenancy/account/{accountName}

如果您想要啟用受限模式、則需要在要求本文中包含下列項目：

```
{
  "isSaasDisabled": true
}
```



BlueXP 建立帳戶後、您無法變更限制模式設定。您稍後無法啟用受限模式、之後也無法停用。必須在建立帳戶時設定。

"瞭解如何使用此 API 呼叫"

相關連結

- ["瞭解 BlueXP 帳戶"](#)
- ["瞭解 BlueXP 部署模式"](#)

使用者角色

「帳戶管理員」、「工作區管理員」、「法規遵循檢視器」及 SnapCenter「支援對象管理員」角色、可為使用者提供特定權限。當您將新使用者與 BlueXP 帳戶建立關聯時、您可以指派其中一個角色。

Compliance Viewer 角色適用於唯讀 BlueXP 分類存取。

工作	帳戶管理員	工作區管理	法規遵循檢視器	系統管理員 SnapCenter
管理工作環境	是的	是的	否	否
在工作環境中啟用服務	是的	是的	否	否
從工作區移除工作環境	是的	是的	否	否
刪除工作環境	是的	是的	否	否

工作	帳戶管理員	工作區管理	法規遵循檢視器	系統管理員 SnapCenter
檢視資料複寫狀態	是的	是的	否	否
檢視時間表	是的	是的	否	否
在工作區之間切換	是的	是的	是的	否
檢視 BlueXP 分類掃描結果	是的	是的	是的	否
接收 Cloud Volumes ONTAP 此報告	是的	否	否	否
建立連接器	是的	否	否	否
管理 BlueXP 帳戶	是的	否	否	否
管理認證資料	是的	否	否	否
修改 BlueXP 設定	是的	否	否	否
檢視及管理支援儀表板	是的	否	否	否
安裝 HTTPS 憑證	是的	否	否	否

相關連結

- ["在 BlueXP 帳戶中設定工作區和使用者"](#)
- ["管理 BlueXP 帳戶中的工作區和使用者"](#)

連接器

尋找連接器的系統ID

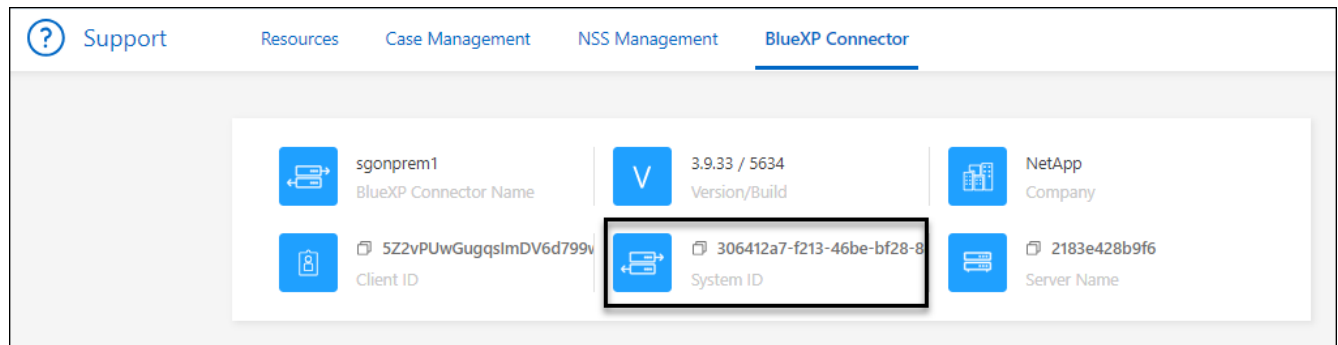
為了協助您開始使用、您的 NetApp 代表可能會要求您提供 Connector 的系統 ID。此 ID 通常用於授權和疑難排解。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示。
2. 選取 * 支援 > BlueXP Connector*。

系統 ID 會顯示在頁面頂端。

- 範例 *



管理現有的連接器

建立 Connector 之後、您可能需要隨時加以管理。例如、如果有多個連接器、您可能會想要在連接器之間切換。或者、在私有模式下使用 BlueXP 時、您可能需要手動升級 Connector。

"瞭解 Connectors 的運作方式"。



Connector 包含可從 Connector 主機存取的本機 UI。此使用者介面適用於以受限模式或私人模式使用 BlueXP 的客戶。在標準模式下使用 BlueXP 時、您應該從存取使用者介面 ["BlueXP SaaS 主控台"](#)

"瞭解 BlueXP 部署模式"。

作業系統與 VM 維護

在 Connector 主機上維護作業系統是您的責任。例如、您應該遵循公司的作業系統發佈標準程序、將安全性更新套用至 Connector 主機上的作業系統。

請注意、執行作業系統更新時、不需要停止 Connector 主機上的任何服務。

如果您需要停止然後啟動 Connector VM、您應該從雲端供應商的主控台或使用內部部署管理的標準程序來執行。

"請注意、Connector 必須隨時都能運作"。

VM 或執行個體類型

如果您直接從 BlueXP 建立 Connector、BlueXP 會使用預設組態、在雲端供應商中部署虛擬機器執行個體。建立 Connector 之後、不應變更為 CPU 或 RAM 較少的較小 VM 執行個體。

CPU 和 RAM 需求如下：

CPU

4 個核心或 4 個 vCPU

RAM

14 GB

"瞭解連接器的預設組態"。

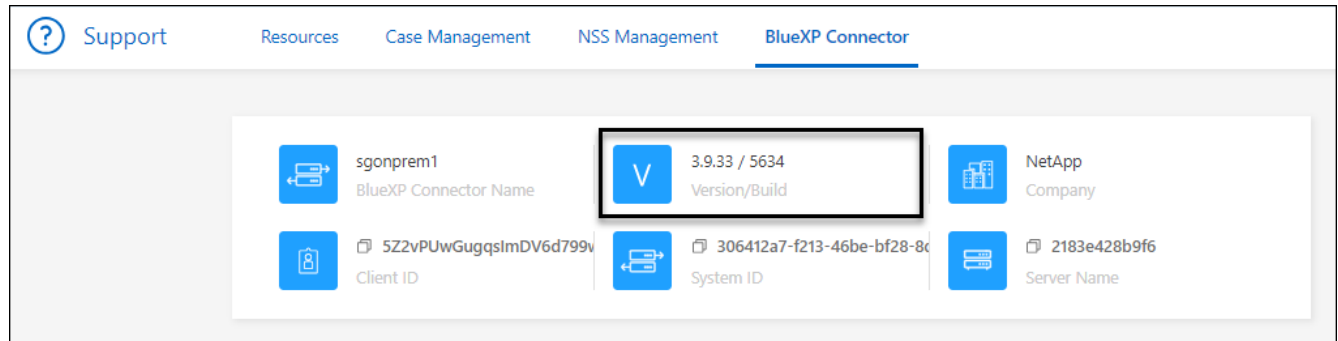
檢視 Connector 的版本

您可以檢視 Connector 的版本、以確認 Connector 已自動升級至最新版本、或是您需要與 NetApp 代表分享。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示。
2. 選取 * 支援 > BlueXP Connector* 。

版本會顯示在頁面頂端。



在連接器之間切換

如果您有多個連接器、可以在它們之間切換、以查看與特定連接器相關聯的工作環境。

例如、假設您是在多個雲端環境中工作。您可能在 AWS 中有一個 Connector、在 Google Cloud 中有一個 Connector。您必須在這些連接器之間切換、才能管理 Cloud Volumes ONTAP 在雲端上執行的各種功能。

步驟

1. 選取 * Connector * 下拉式清單、選取 Another Connector、然後選取 * Switch* 。



結果

BlueXP會重新整理並顯示與所選Connector相關的工作環境。

下載**AutoSupport** 或傳送更新訊息

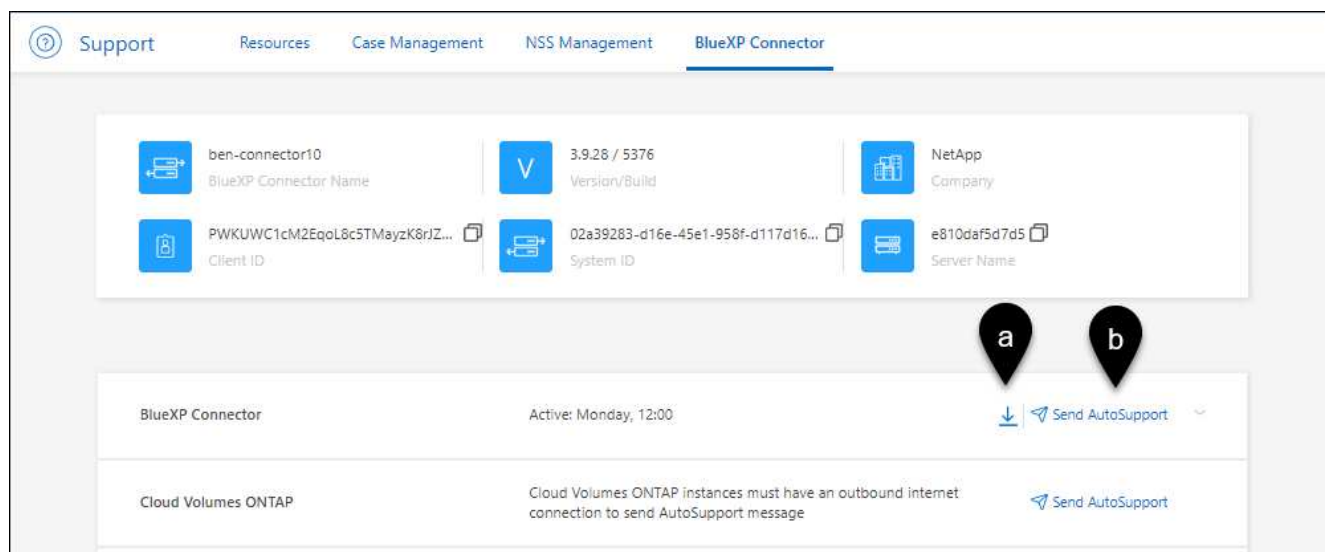
如果您有任何問題、NetApp人員可能會要求您傳送AutoSupport 一份關於解決疑難的消息給NetApp支援部門。

步驟

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



2. 選擇 * BlueXP Connector* 。
3. 根據您傳送資訊給NetApp支援部門的方式、請選擇下列其中一個選項：
 - a. 選取選項、將AutoSupport 此資訊下載到您的本機機器。然後、您可以使用偏好的方法將其傳送給NetApp支援部門。
 - b. 選擇 * 傳送 AutoSupport * 、將訊息直接傳送至 NetApp 支援部門。



連線至Linux VM

如果您需要連線至執行Connector的Linux VM、可以使用雲端供應商提供的連線選項來執行。

AWS

在AWS中建立Connector執行個體時、您提供了AWS存取金鑰和秘密金鑰。您可以將此金鑰配對用於執行個體的SSH。EC2 Linux 執行個體的使用者名稱為 Ubuntu （對於在 2023 年 5 月之前建立的 Connectors 、使

用者名稱為 EC2-user) 。

["AWS文件：連線至您的Linux執行個體"](#)

Azure

在 Azure 中建立 Connector VM 時、您指定了使用者名稱、並選擇使用密碼或 SSH 公開金鑰進行驗證。使用您選擇的驗證方法來連線至 VM。

["Azure文件：SSH進入VM"](#)

Google Cloud

在 Google Cloud 中建立 Connector 時、您無法指定驗證方法。不過、您可以使用 Google Cloud Console 或 Google Cloud CLI (gcloud) 連線至 Linux VM 執行個體。

["Google Cloud Docs：連線至Linux VM"](#)

需要在 Amazon EC2 執行個體上使用 IMDSv2

從 2024 年 3 月開始、BlueXP 現在支援 Amazon EC2 執行個體中繼資料服務版本 2 (IMDSv2) 搭配 Connector 和 Cloud Volumes ONTAP (包括 HA 部署的協調器)。在大多數情況下、會在新的 EC2 執行個體上自動設定 IMDSv2。IMDSv1 在 2024 年 3 月之前啟用。如果您的安全性原則要求、您可能需要在 EC2 執行個體上手動設定 IMDSv2。

關於這項工作

IMDSv2 提供更強大的保護功能、防範弱點。 ["從 AWS 安全性部落格深入瞭解 IMDSv2"](#)

在 EC2 執行個體上、執行個體中繼資料服務 (IMDS) 的啟用方式如下：

- 適用於從 BlueXP 或使用的新 Connector 部署 ["Terraform 指令碼"](#)、根據預設、EC2 執行個體上會啟用 IMDSv2。
- 如果您在 AWS 中啟動新的 EC2 執行個體、然後手動安裝 Connector 軟體、則預設也會啟用 IMDSv2。
- 如果您從 AWS Marketplace 啟動 Connector、則預設會啟用 IMDSv1。您可以在 EC2 執行個體上手動設定 IMDSv2。
- 對於現有的 Connectors、仍支援 IMDSv1、但您可以視需要在 EC2 執行個體上手動設定 IMDSv2。
- 對於 Cloud Volumes ONTAP、根據預設、會在新的和現有的執行個體上啟用 IMDSv1。您可以視需要在 EC2 執行個體上手動設定 IMDSv2。

開始之前

- Connector 版本必須為 3.9.38 或更新版本。
- Cloud Volumes ONTAP 必須執行下列其中一個版本：
 - 9.12.1 P2 (或任何後續修補程式)
 - 9.13.0 P4 (或任何後續修補程式)
 - 9.13.1 或本版本之後的任何版本
- 此變更需要重新啟動 Cloud Volumes ONTAP 執行個體。

關於這項工作

這些步驟需要使用 AWS CLI、因為您必須將回應躍點限制變更為 3。

步驟

1. 需要在 Connector 執行個體上使用 IMDSv2：

a. 連接至 Linux VM for the Connector。

在AWS中建立Connector執行個體時、您提供了AWS存取金鑰和秘密金鑰。您可以將此金鑰配對用於執行個體的SSH。EC2 Linux 執行個體的使用者名稱為 Ubuntu（對於在 2023 年 5 月之前建立的 Connectors、使用者名稱為 EC2-user）。

["AWS文件：連線至您的Linux執行個體"](#)

b. 安裝 AWS CLI。

["AWS 文件：安裝或更新至 AWS CLI 的最新版本"](#)

c. 使用 `aws ec2 modify-instance-metadata-options` 命令要求使用 IMDSv2、並將「輸入回應躍點」限制變更為 3。

▪ 範例 *

```
aws ec2 modify-instance-metadata-options \
  --instance-id <instance-id> \
  --http-put-response-hop-limit 3 \
  --http-tokens required \
  --http-endpoint enabled
```



。 `http-tokens` 參數會將 IMDSv2 設為必要。何時 `http-tokens` 為必填、您也必須設定 `http-endpoint` 至啟用。

2. 需要在 Cloud Volumes ONTAP 執行個體上使用 IMDSv2：

a. 前往 ["Amazon EC2 主控台"](#)

b. 從導覽窗格中、選取 * 執行個體 *。

c. 選取 Cloud Volumes ONTAP 執行個體。

d. 選取 * 「動作」 > 「執行個體設定」 > 「修改執行個體中繼資料選項」 *。

e. 在 * 修改執行個體中繼資料選項 * 對話方塊中、選取下列項目：

- 對於 * 執行個體中繼資料服務 *、請選取 * 啟用 *。
- 對於 **IMDSv2**，請選擇 * 必要 *。
- 選擇*保存*。

f. 對其他 Cloud Volumes ONTAP 執行個體（包括 HA 協調器）重複這些步驟。

g. ["停止並啟動 Cloud Volumes ONTAP 執行個體"](#)

結果

Connector 執行個體和 Cloud Volumes ONTAP 執行個體現在已設定為使用 IMDSv2。

使用私有模式時升級 Connector

如果您在私有模式下使用 BlueXP、則可在 NetApp 支援網站 提供較新版本時升級 Connector。

Connector 需要在升級過程中重新啟動、以便在升級期間無法使用網路型主控台。



當您在標準模式或受限模式下使用 BlueXP 時、只要 Connector 有外送網際網路存取權來取得軟體更新、它就會自動將其軟體更新至最新版本。

步驟

1. 從下載Connector軟體 "[NetApp 支援網站](#)"。

請務必下載無網際網路存取的私有網路離線安裝程式。

2. 將安裝程式複製到Linux主機。
3. 指派執行指令碼的權限。

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

其中、就是您下載的Connector版本<version>。

4. 執行安裝指令碼：

```
sudo /path/BlueXP-Connector-offline-<version>
```

其中、就是您下載的Connector版本<version>。

5. 升級完成後、您可以前往*「Help」（說明）>「Support」（支援）>「Connector*」（連接器*）來驗證連接器的版本。

變更連接器的IP位址

如果貴企業需要、您可以變更由雲端供應商自動指派之Connector執行個體的內部IP位址和公有IP位址。

步驟

1. 依照雲端供應商的指示、變更連接器執行個體的本機IP位址或公有IP位址（或兩者）。
2. 如果您變更了公用IP位址、而且需要連線至連接器上執行的本機使用者介面、請重新啟動連接器執行個體、以使用BlueXP登錄新的IP位址。
3. 如果您變更了私有IP位址、請更新Cloud Volumes ONTAP 支援的還原組態檔案備份位置、以便將備份傳送到Connector上的新私有IP位址。

您需要更新每個 Cloud Volumes ONTAP 系統的備份位置。

- a. 從 Cloud Volumes ONTAP CLI 執行下列命令以顯示目前的備份目標：

```
system configuration backup show
```

- b. 執行下列命令以更新備份目標的 IP 位址：

```
system configuration backup settings modify -destination <target-  
location>
```

編輯連接器的URI

新增及移除 Connector 的統一資源識別元（URI）。

步驟

1. 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
2. 選取 * 管理連接器 *。
3. 選取 Connector 的動作功能表、然後選取 * 編輯 URI*。
4. 新增並移除 URI、然後選取 * 套用 *。

修正使用Google Cloud NAT閘道時的下載失敗

Connector會自動下載Cloud Volumes ONTAP 適用於更新的軟體。如果您的組態使用Google Cloud NAT閘道、下載可能會失敗。您可以限制軟體映像分成的零件數量來修正此問題。此步驟必須使用BlueXP API完成。

步驟

1. 將PUT要求提交至/occm/config、並以下列Json做為本文：

```
{  
  "maxDownloadSessions": 32  
}
```

_MaxDownloadSessions_的值可以是1或任何大於1的整數。如果值為1、則下載的映像不會分割。

請注意、32為範例值。您應該使用的值取決於NAT組態和可同時使用的工作階段數目。

"深入瞭解/occm/config API呼叫"

從BlueXP移除連接器

如果連接器處於非作用中狀態、您可以將其從BlueXP的連接器清單中移除。如果您刪除了 Connector 虛擬機器、或是卸載了 Connector 軟體、則可以這麼做。

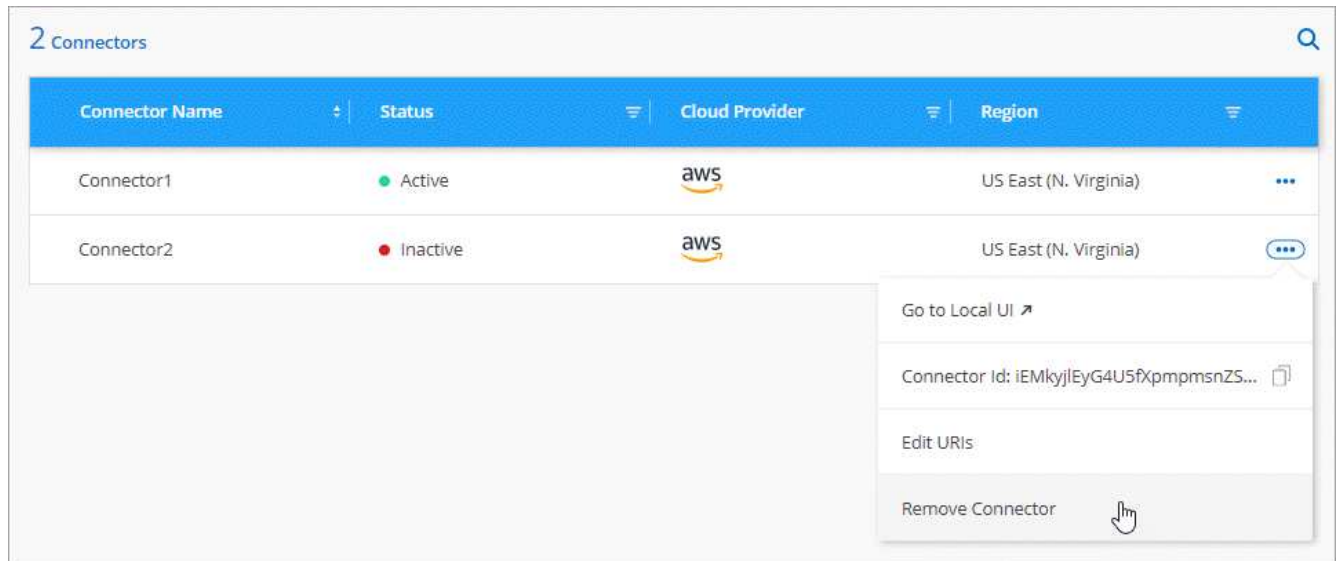
請注意下列關於移除連接器的事項：

- 此動作不會刪除虛擬機器。

- 此動作無法還原、只要從 BlueXP 移除 Connector、就無法重新新增。

步驟

1. 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
2. 選取 * 管理連接器 *。
3. 選取非作用中 Connector 的動作功能表、然後選取 * 移除 Connector*。



4. 輸入 Connector 的名稱以確認、然後選取 * 移除 *。

結果

BlueXP 會將 Connector 從記錄中移除。

解除安裝 Connector 軟體

解除安裝 Connector 軟體以疑難排解問題、或從主機上永久移除軟體。您需要使用的步驟取決於您是在具有網際網路存取（標準模式或限制模式）的主機上安裝 Connector、還是在沒有網際網路存取（私有模式）的網路中安裝 Connector。

使用標準模式或受限模式時解除安裝

下列步驟可讓您在標準模式或受限模式下使用 BlueXP 時、解除安裝 Connector 軟體。

步驟

1. 連接至 Linux VM for the Connector。
2. 從 Linux 主機執行解除安裝指令碼：

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

silon 執行指令碼時不會提示您確認。

使用私有模式時解除安裝

下列步驟可讓您在無法存取網際網路的私人模式下使用 BlueXP 時、解除安裝 Connector 軟體。

步驟

- 1. 連接至 Linux VM for the Connector 。
- 2. 從Linux主機執行下列命令：

```
./opt/application/netapp/ds/cleanup.sh  
rm -rf /opt/application/netapp/ds
```

安裝 HTTPS 憑證以進行安全存取

根據預設、BlueXP會使用自我簽署的憑證來存取Web主控台的HTTPS。如果貴企業有需要、您可以安裝由憑證授權單位（CA）簽署的憑證、以提供比自我簽署的憑證更好的安全保護。

開始之前

您必須先建立連接器、才能變更BlueXP設定。"瞭解方法"。

安裝 HTTPS 憑證

安裝由 CA 簽署的憑證、以確保安全存取。

步驟

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



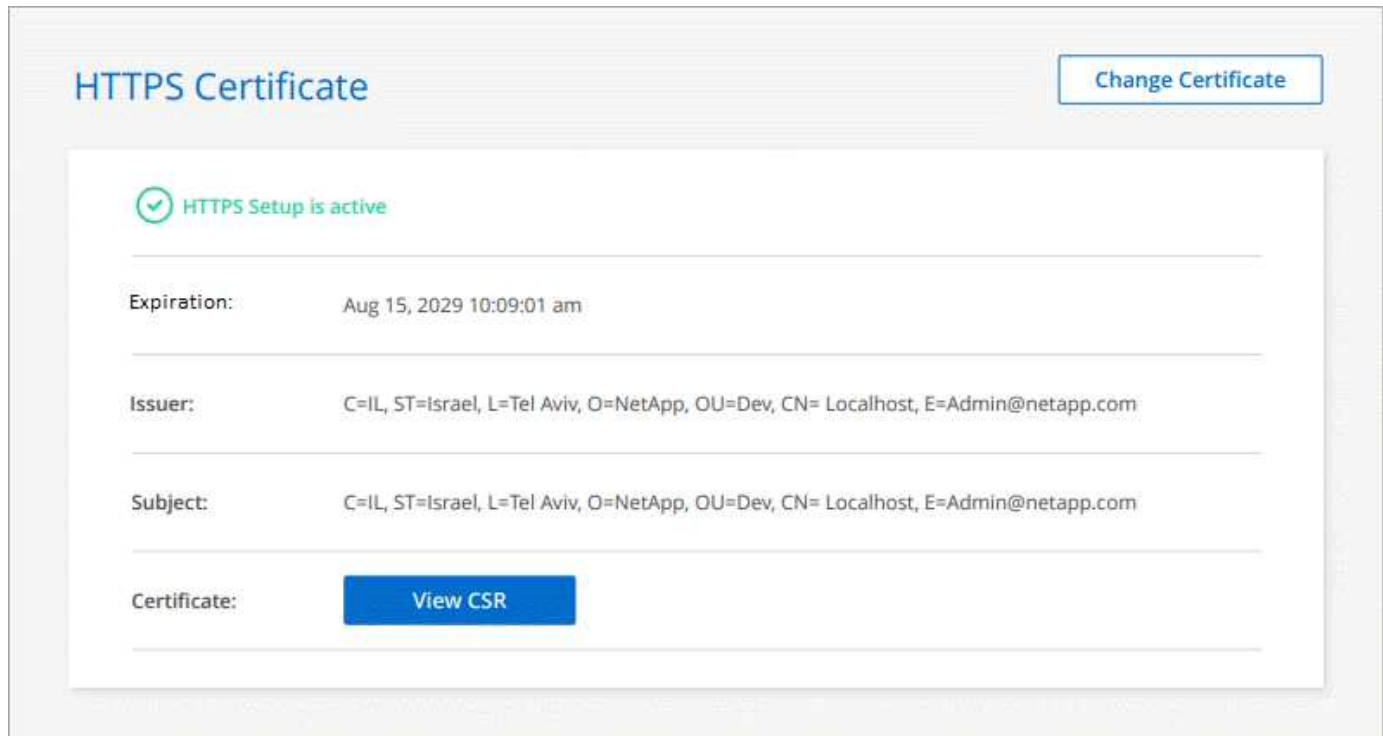
- 2. 在「HTTPS 設定」頁面中、產生憑證簽署要求（CSR）或安裝您自己的 CA 簽署憑證來安裝憑證：

選項	說明
產生 CSR	<div>a. 輸入 Connector 主機的主機名稱或 DNS （其一般名稱）、然後選取 * 產生 CSR * 。</div> <div>BlueXP會顯示憑證簽署要求。</div> <div>b. 使用 CSR 將 SSL 憑證要求提交給 CA 。</div> <div>憑證必須使用隱私增強型郵件（PEF）Base - 64 編碼的 X · 509 格式。</div> <div>c. 上傳憑證檔案、然後選取 * 安裝 * 。</div>

選項	說明
安裝您自己的 CA 簽署憑證	<p>a. 選擇 * 安裝 CA 簽署的憑證 * 。</p> <p>b. 同時載入憑證檔案和私密金鑰、然後選取 * 安裝 * 。</p> <p>憑證必須使用隱私增強型郵件（PEF）Base - 64 編碼的 X · 509 格式。</p>

結果

現在、BlueXP使用CA簽署的憑證來提供安全的HTTPS存取。下圖顯示設定為安全存取的BlueXP帳戶：



更新 BlueXP HTTPS 憑證

您應該在過期之前更新BlueXP HTTPS憑證、以確保安全存取BlueXP主控台。如果您在憑證到期之前未續約、當使用者使用HTTPS存取Web主控台時、會出現警告。

步驟

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

顯示有關BlueXP憑證的詳細資料、包括到期日。

2. 選取 * 變更憑證 * 、然後依照步驟產生 CSR 或安裝您自己的 CA 簽署憑證。

結果

BlueXP使用新的CA簽署憑證來提供安全的HTTPS存取。

設定連接器以使用Proxy伺服器

如果您的企業原則要求您使用Proxy伺服器來進行所有網際網路通訊、則您必須設定連接器以使用該Proxy伺服器。如果在安裝期間未將Connector設定為使用Proxy伺服器、則可將Connector設定為隨時使用該Proxy伺服器。

如果無法使用公用IP位址或NAT閘道、設定連接器使用Proxy伺服器可提供傳出網際網路存取。此Proxy伺服器僅提供連接器與傳出連線。它不提供Cloud Volumes ONTAP 任何連接功能給不適用的系統。

如果Cloud Volumes ONTAP 無法透過外部網際網路連線來傳送AutoSupport 各種消息、則BlueXP會自動將這些Cloud Volumes ONTAP 系統設定為使用連接器隨附的Proxy伺服器。唯一的需求是確保連接器的安全群組允許透過連接埠3128進行傳入連線。部署Connector之後、您需要開啟此連接埠。

支援的組態

- BlueXP支援HTTP和HTTPS。
- Proxy 伺服器可以位於雲端或網路中。
- BlueXP 不支援透明 Proxy 伺服器。

在連接器上啟用Proxy

當您將連接器設定為使用 Proxy 伺服器、連接器及 Cloud Volumes ONTAP 其所管理的各種系統（包括任何 HA 協調器）時、都會使用 Proxy 伺服器。

請注意、此作業會重新啟動Connector。請先確定 Connector 未執行任何作業、然後再繼續。

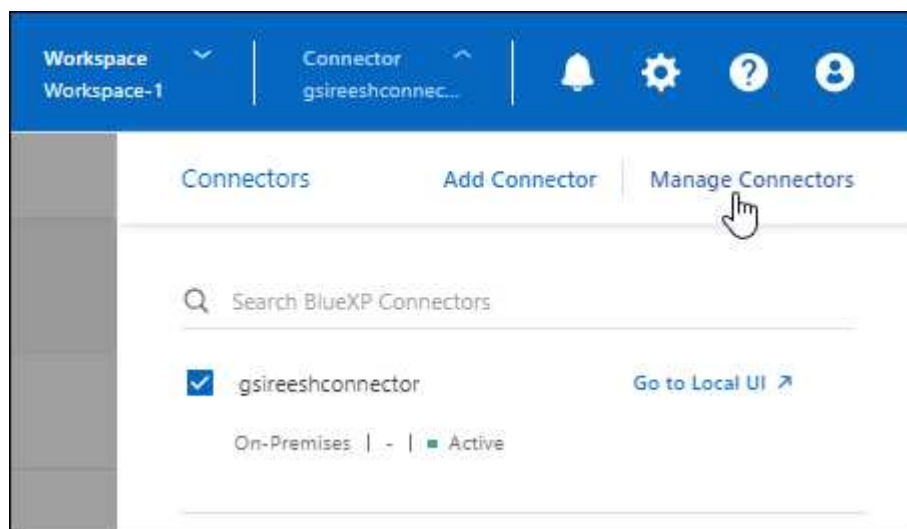
步驟

1. 瀏覽至 * 編輯 BlueXP Connector* 頁面。

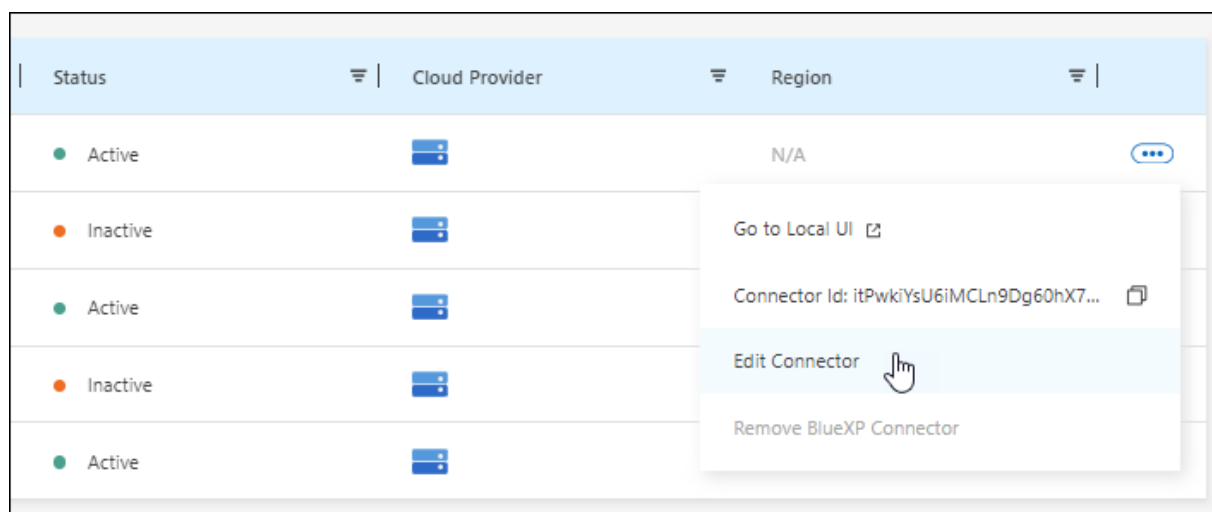
導覽方式取決於您是以標準模式使用 BlueXP （從 SaaS 網站存取 BlueXP 介面）、還是以受限模式或私有模式使用 BlueXP （從 Connector 主機本機存取 BlueXP 介面）。

標準模式

- 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
- 選取 * 管理連接器 *。

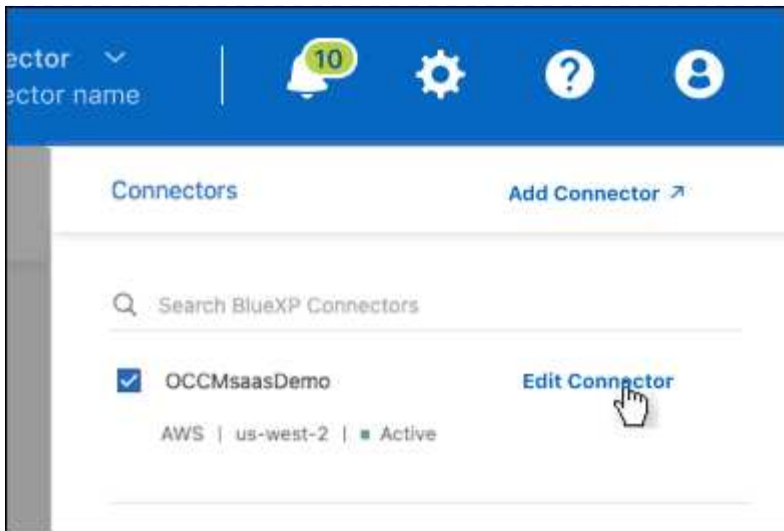


- 選取 Connector 的動作功能表、然後選取 * 編輯 Connector*。



受限或私人模式

- 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
- 選擇 * 編輯 Connector*。



選項，您可以在展開 [連接器]

功能表之後使用此選項。"]

2. 選擇 * HTTP Proxy 組態 * 。

3. 設定Proxy：

- a. 選取 * 啟用 Proxy* 。
- b. 使用語法指定伺服器 `http://address:port` 或 `https://address:port`
- c. 如果伺服器需要基本驗證、請指定使用者名稱和密碼。

請注意下列事項：

- 使用者可以是本機使用者或網域使用者。
- 對於網域使用者、您必須輸入 \ 的 ASCII 碼、如下所示： domain-name%92user-name

例如： NetApp%92Proxy

- BlueXP不支援包含@字元的密碼。

d. 選擇*保存*。

啟用直接API流量

如果您將連接器設定為使用Proxy伺服器、則可在連接器上啟用直接API流量、以便直接將API呼叫傳送至雲端供應商服務、而無需透過Proxy。此選項受AWS、Azure或Google Cloud中執行的Connectors支援。

如果您停用使用Azure私有連結Cloud Volumes ONTAP 搭配使用、並改用服務端點、則必須啟用直接API流量。否則、流量將無法正確路由傳送。

["深入瞭解如何搭配Cloud Volumes ONTAP 使用Azure Private Link或服務端點搭配使用"](#)

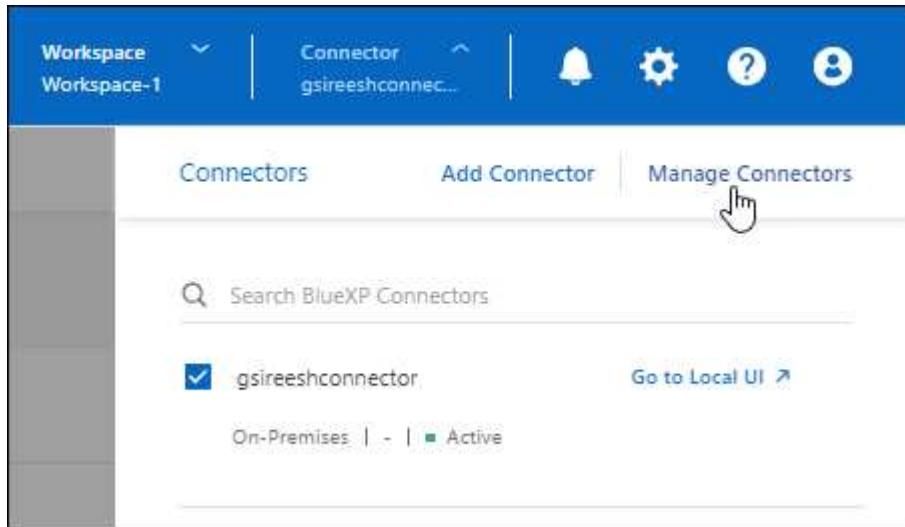
步驟

1. 瀏覽 * 編輯 BlueXP Connector* 頁面：

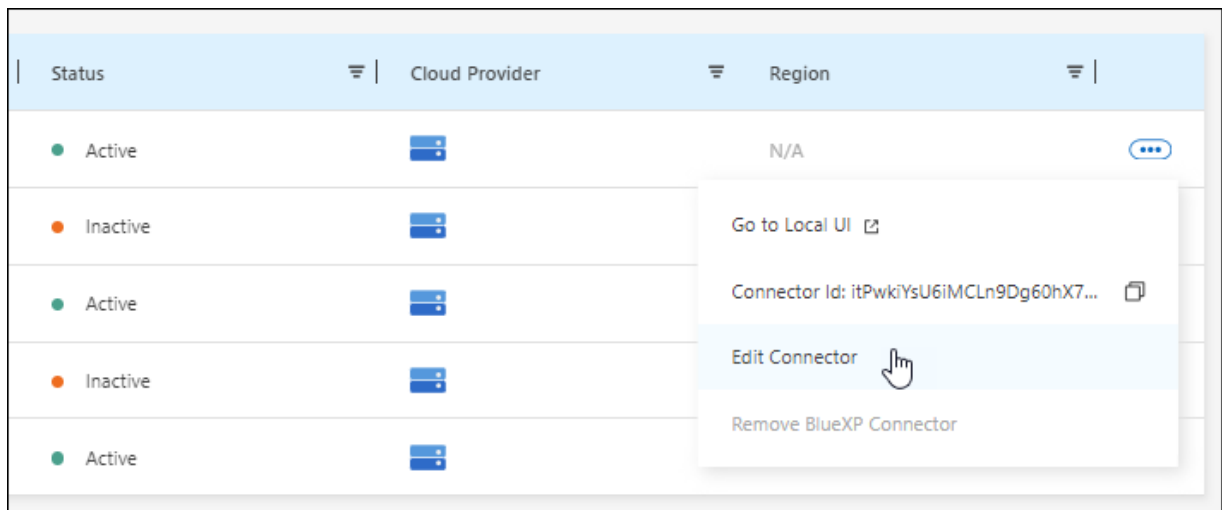
導覽方式取決於您是以標準模式使用 BlueXP（從 SaaS 網站存取 BlueXP 介面）、還是以受限模式或私有模式使用 BlueXP（從 Connector 主機本機存取 BlueXP 介面）。

標準模式

- 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
- 選取 * 管理連接器 *。

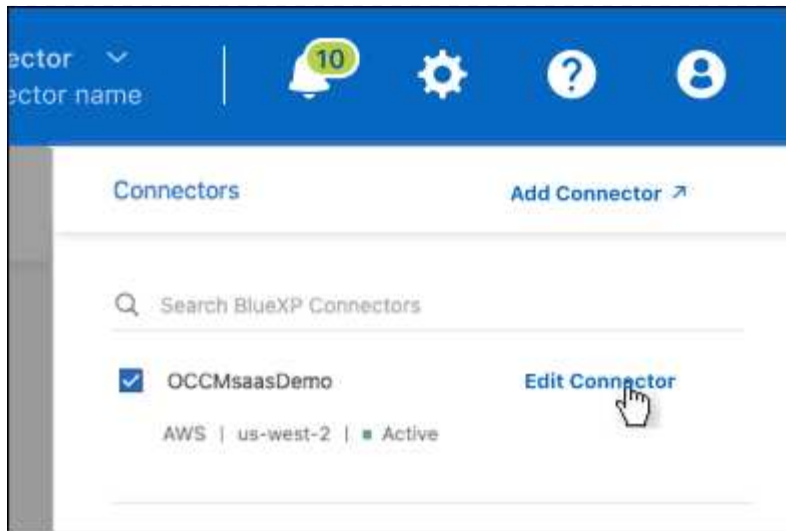


- 選取 Connector 的動作功能表、然後選取 * 編輯 Connector*。



受限或私人模式

- 從 BlueXP 標頭中選取 * Connector* 下拉式清單。
- 選擇 * 編輯 Connector*。



選項，您可以在展開 [連接器]

功能表之後使用此選項。"]

2. 選取 * 支援直接 API 流量 * 。
3. 選取核取方塊以啟用選項、然後選取 * 儲存 * 。

Connector 的預設組態

您可能想要在部署 Connector 之前、或是需要疑難排解任何問題時、深入瞭解 Connector 的組態。

具備網際網路存取的預設組態

如果您是從BlueXP、雲端供應商的市場部署Connector、或是手動將Connector安裝在可存取網際網路的內部部署Linux主機上、則適用下列組態詳細資料。

AWS 詳細資料

如果您是從BlueXP或雲端供應商的市場部署Connector、請注意下列事項：

- EC2執行個體類型為T3.xLarge。
- 映像的作業系統為 Ubuntu 22.04 LTS。

作業系統不含 GUI。您必須使用終端機來存取系統。

- EC2 Linux 執行個體的使用者名稱為 Ubuntu（對於在 2023 年 5 月之前建立的 Connectors、使用者名稱為 EC2-user）。
- 預設系統磁碟為 100 GiB gp2 磁碟。

Azure詳細資料

如果您是從BlueXP或雲端供應商的市場部署Connector、請注意下列事項：

- VM類型為DS3 v2。

- 映像的作業系統為 Ubuntu 22.04 LTS 。

作業系統不含 GUI 。您必須使用終端機來存取系統。

- 預設系統磁碟為100 GiB優質SSD磁碟。

Google Cloud詳細資料

如果您是從 BlueXP 部署 Connector 、請注意下列事項：

- VM 執行個體為 n2-Standard-4 。
- 映像的作業系統為 Ubuntu 22.04 LTS 。

作業系統不含 GUI 。您必須使用終端機來存取系統。

- 預設系統磁碟為100 GiB SSD持續磁碟。

安裝資料夾

Connector 安裝資料夾位於下列位置：

`/opt/application/NetApp/cloudmanager`

記錄檔

記錄檔包含在下列資料夾中：

- `/opt/application/NetApp/cloudmanager/log`
或
- `/opt/application/NetApp/service-manager-2/logs`（從全新3.9.23安裝開始）

這些資料夾中的記錄提供有關Connector和Docker影像的詳細資料。

- `/opt/application/netapp/cloudmanager/dock_occm/data/log`

此資料夾中的記錄提供有關在Connector上執行雲端服務和BlueXP服務的詳細資料。

連接器服務

- BlueXP服務的名稱為occm。
- occm 服務取決於 MySQL 服務。

如果 MySQL 服務當機、則 occm 服務也會停機。

連接埠

連接器在 Linux 主機上使用下列連接埠：

- 80 （用於 HTTP 存取）
- 用於 HTTPS 存取的 443

預設組態、不含網際網路存取

如果您手動將Connector安裝在無法存取網際網路的內部部署Linux主機上、則適用下列組態。 ["深入瞭解此安裝選項"](#)。

- Connector 安裝資料夾位於下列位置：

`/opt/application/NetApp/DS`

- 記錄檔包含在下列資料夾中：

`/var/lib/dock/volumes/ds_occmdata/log`

此資料夾中的記錄提供有關Connector和Docker影像的詳細資料。

- 所有服務都在Docker容器內執行

這些服務取決於執行的Docker執行時間服務

- 連接器在 Linux 主機上使用下列連接埠：

- 80 （用於 HTTP 存取）
- 用於 HTTPS 存取的 443

認證與訂閱

AWS

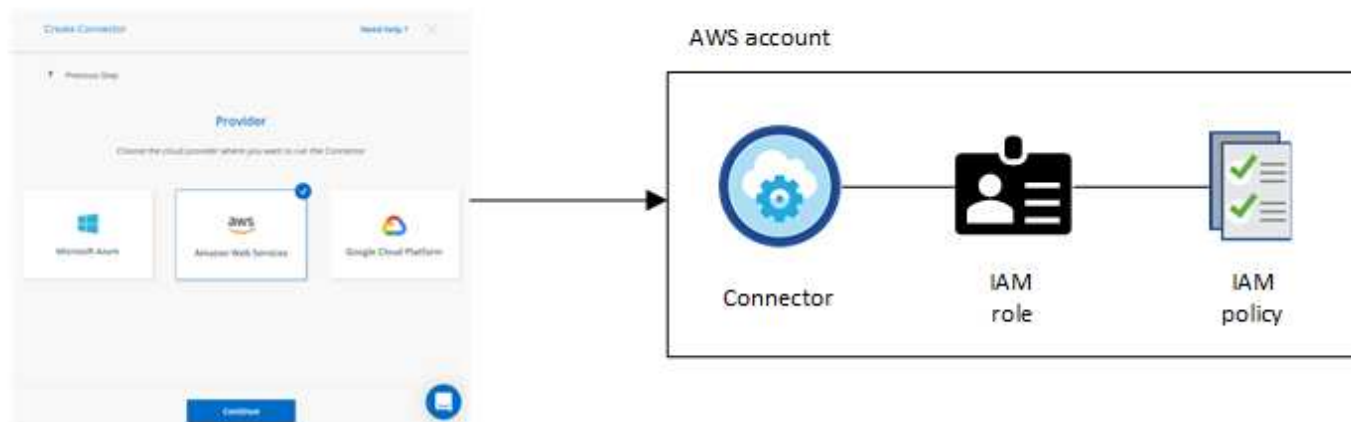
深入瞭解 **AWS** 認證與權限

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		QA Subscription	Edit Credentials
Credentials	Account ID	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

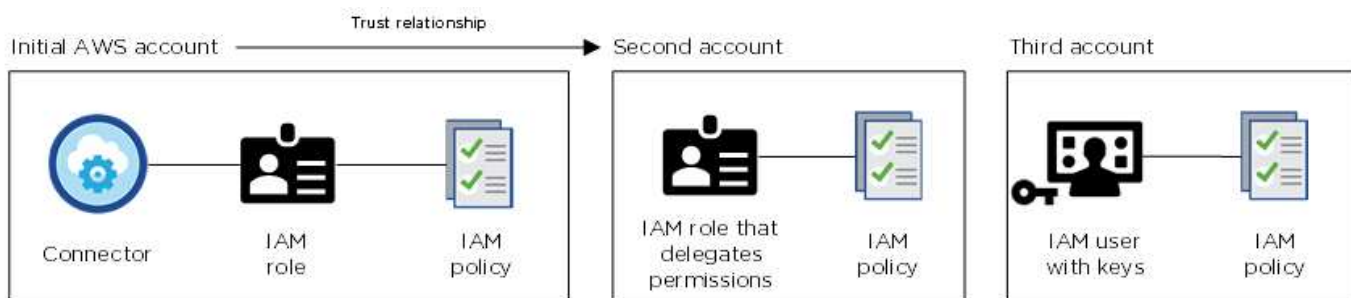
有兩種方法可以新增額外的 AWS 認證：

- 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

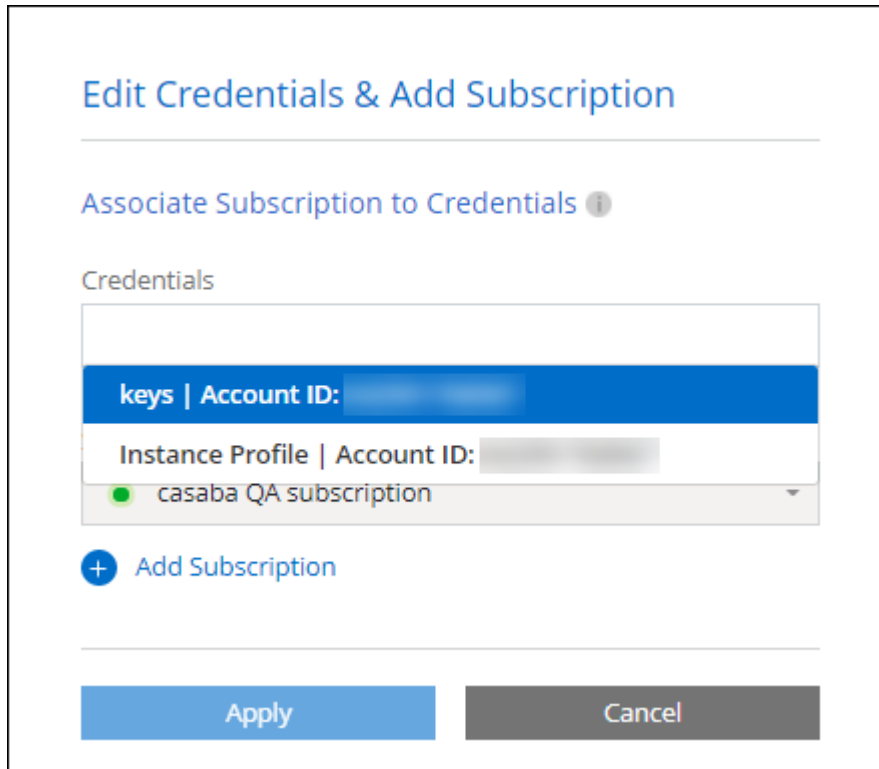
如果您想要將 BlueXP 與其他 AWS 帳戶搭配使用、則可以為 IAM 使用者提供 AWS 金鑰、或是在信任的帳戶中提供角色的 ARN。下圖顯示兩個額外的帳戶、一個透過信任帳戶中的 IAM 角色提供權限、另一個則透過 IAM 使用者的 AWS 金鑰提供權限：



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 Sfor Sfor Sfor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 Sfor 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 *。



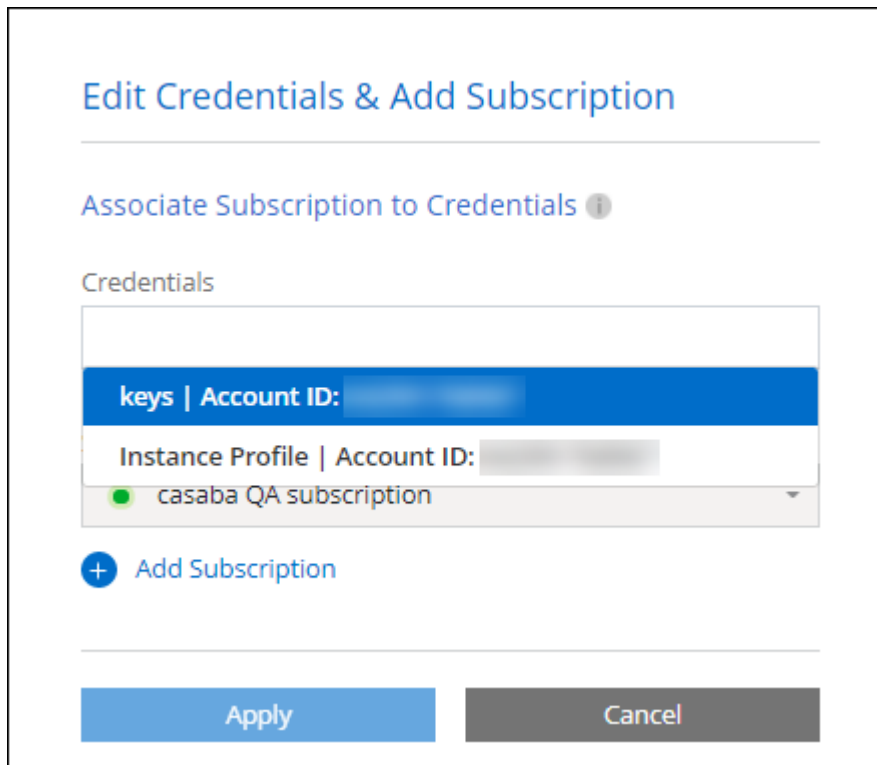
3. 在 * 帳戶認證 * 頁面上、選取 * 新增認證 *、然後依照精靈中的步驟進行。
 - a. 認證資料位置：選取 * Amazon Web Services > Connector*。
 - b. 定義認證資料：提供可信IAM角色的ARN（Amazon資源名稱）、或輸入AWS存取金鑰和秘密金鑰。
 - c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。

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：



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。

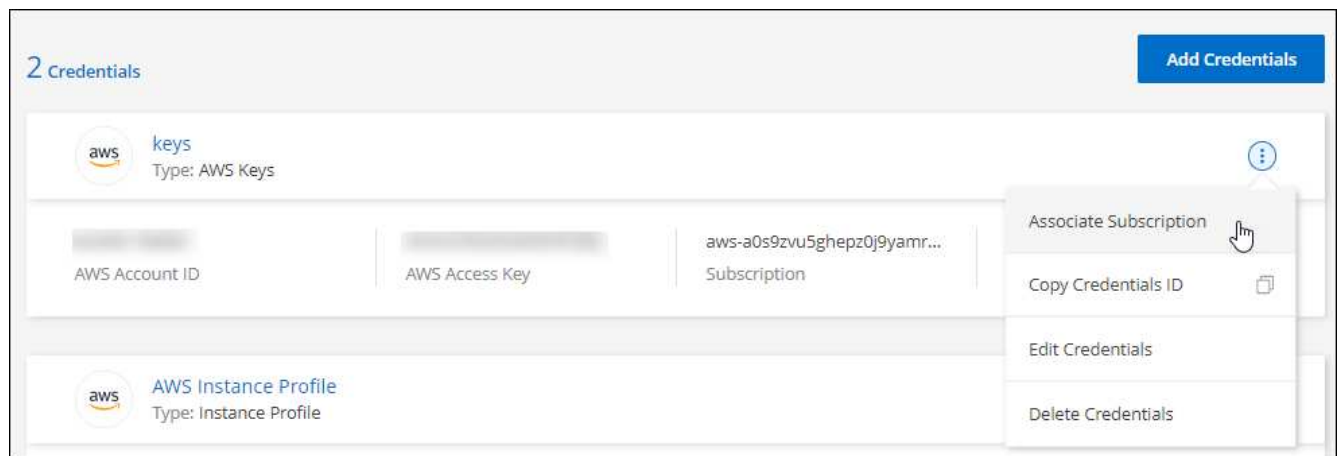
開始之前

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。

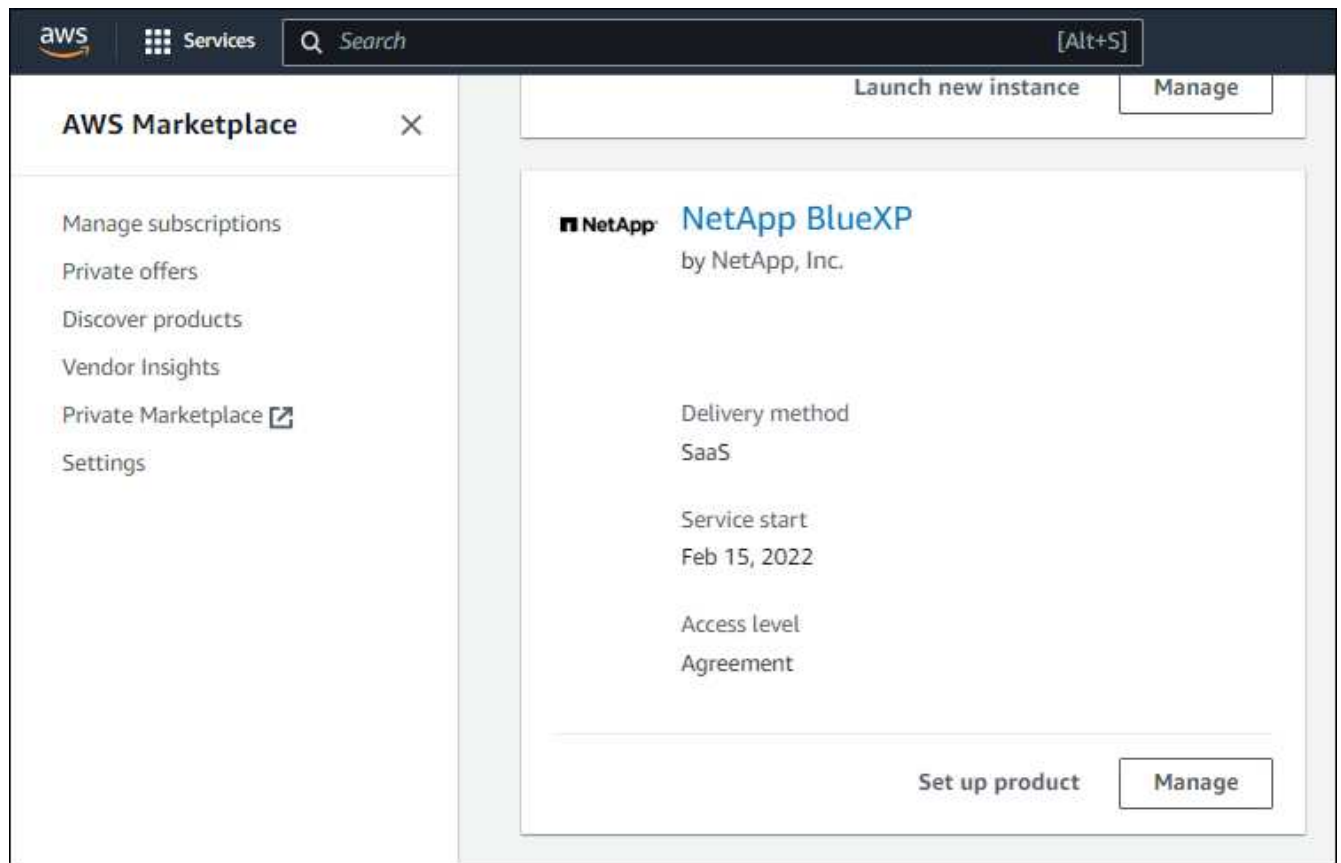
如果您是從 AWS Marketplace 訂閱 BlueXP、但您錯過了將訂閱與帳戶關聯的步驟、請遵循下列步驟。

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。

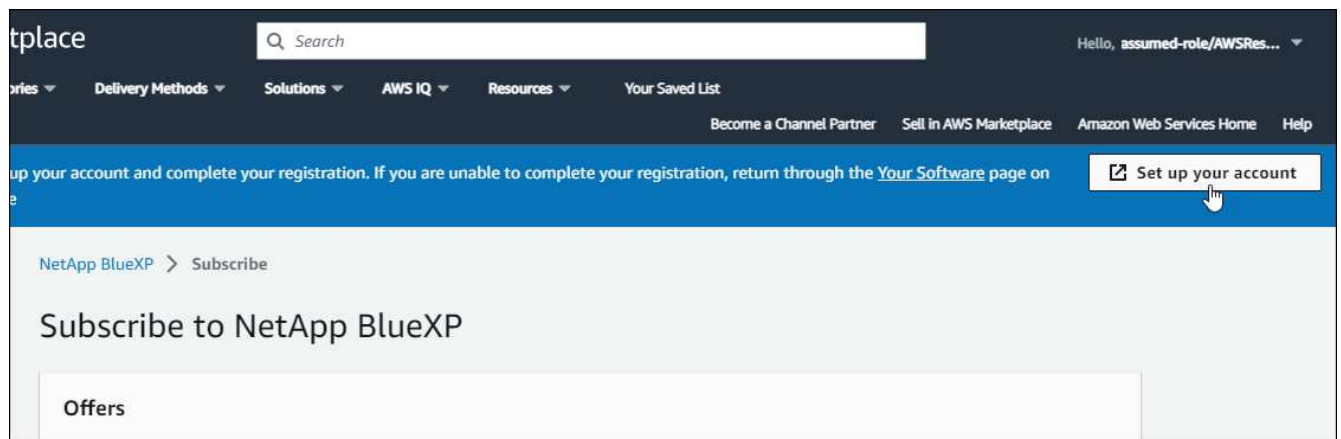
2. 登入 AWS 主控台並瀏覽至 * AWS Marketplace Subscriptions *。
3. 尋找 NetApp BlueXP 訂閱。



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 [X]

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

Subscription name i

PayAsYouGo

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

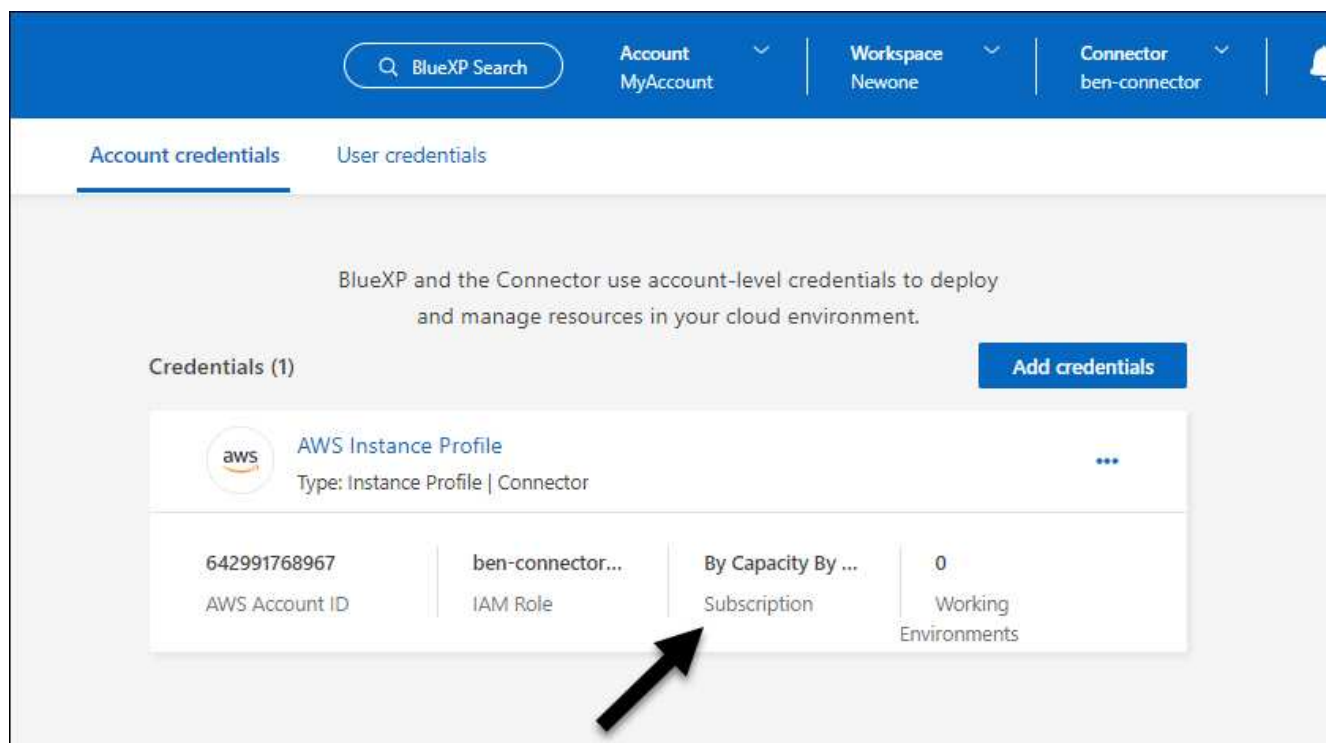
You can automatically replace the existing subscription for one account with this new subscription.

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。

Azure

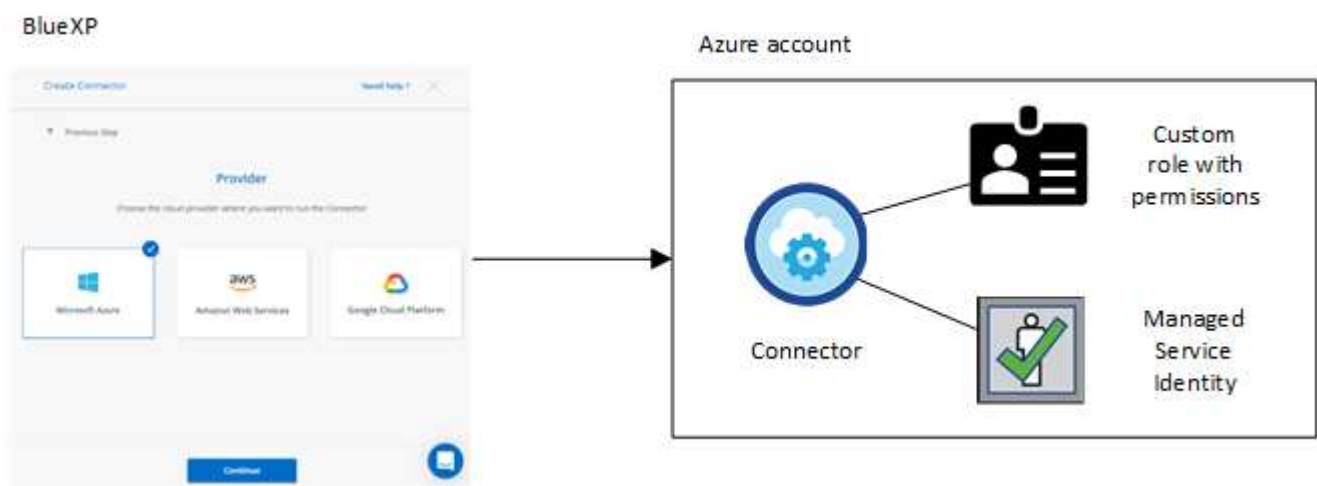
瞭解Azure認證與權限

瞭解 BlueXP 如何使用 Azure 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。瞭解這些詳細資料有助於您管理一或多個 Azure 訂閱的認證。例如、您可能想要瞭解何時將額外的 Azure 認證新增至 BlueXP。

Azure 初始認證

從BlueXP部署Connector時、您需要使用具備部署Connector虛擬機器權限的Azure帳戶或服務主體。所需權限列於 "Azure 的连接器部署原則"。

當BlueXP在Azure中部署Connector虛擬機器時、它會啟用 "系統指派的託管身分識別" 在虛擬機器上建立自訂角色、然後將其指派給虛擬機器。此角色可為BlueXP提供所需的權限、以管理該Azure訂閱中的資源和程序。"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 預設會選取以下 Azure 認證：

Details & Credentials			
Managed Service Ide...	OCCM QA1	No subscription is associated	
Credential Name	Azure Subscription	Marketplace Subscription	Edit Credentials

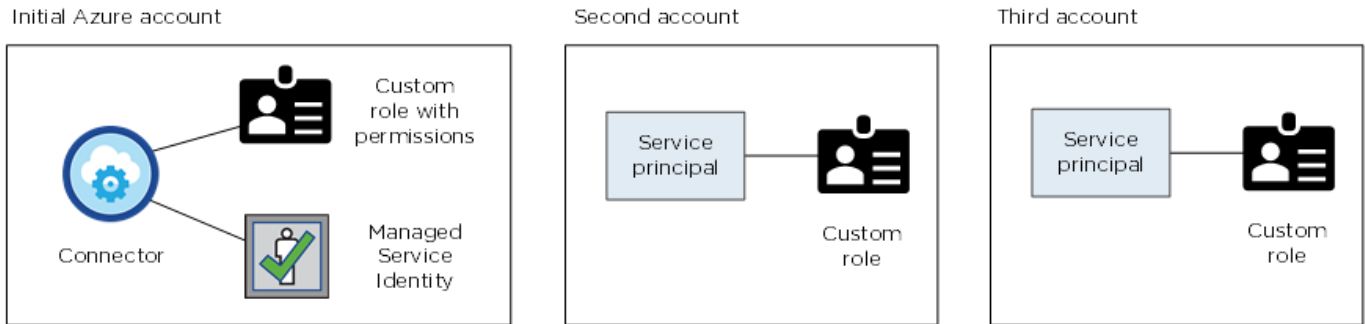
您可以 Cloud Volumes ONTAP 使用初始 Azure 認證來部署所有的整套系統、也可以新增其他認證資料。

額外的 Azure 訂閱、提供託管身分識別

指派給 Connector VM 的系統指派託管身分識別與您啟動 Connector 的訂閱相關聯。如果您想要選擇不同的 Azure 訂閱、則需要 "將託管身分識別與這些訂閱建立關聯"。

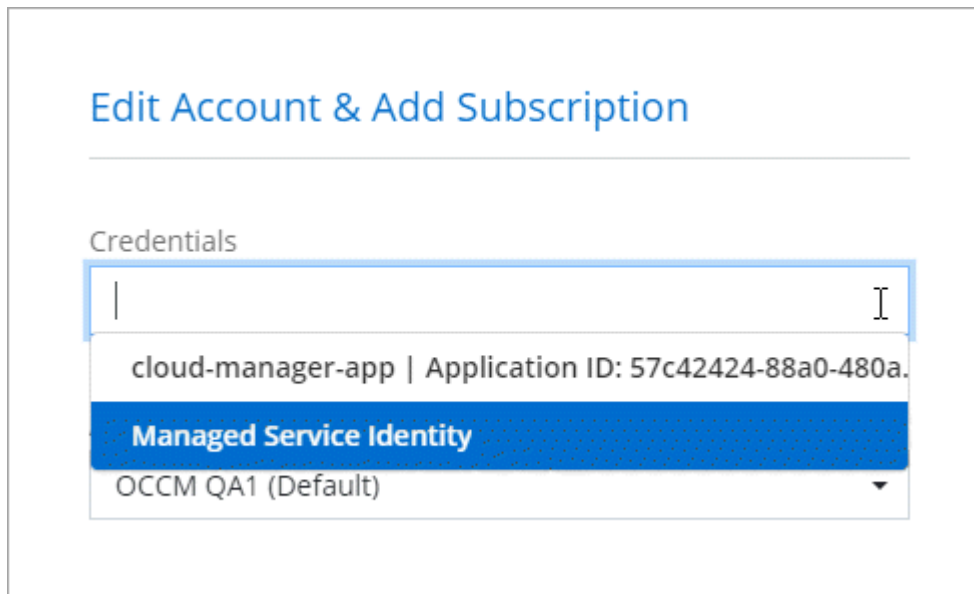
其他 Azure 認證資料

如果您想要將不同的 Azure 認證搭配 BlueXP 使用、則必須將必要的權限授予 ["在 Microsoft Entra ID 中建立及設定服務主體"](#) 針對每個 Azure 帳戶。下圖顯示兩個額外的帳戶、每個帳戶都設有提供權限的服務主體和自訂角色：



您可以 ["將帳戶認證新增至BlueXP"](#) 提供 AD 服務主體的詳細資料。

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：



認證與市場訂閱

您新增至 Connector 的認證必須與 Azure Marketplace 訂閱相關聯、才能以每小時費率（PAYGO）或每年合約支付 Cloud Volumes ONTAP 費用、以及使用其他 BlueXP 服務。

["瞭解如何建立Azure訂閱的關聯"](#)。

請注意以下關於 Azure 認證與市場訂閱的資訊：

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

下列問題與認證和訂閱有關。

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

是的、您可以。當您變更與一組 Azure 認證相關聯的 Azure Marketplace 訂閱時、所有現有和新的 Cloud Volumes ONTAP 工作環境都將從新訂閱中扣除費用。

["瞭解如何建立Azure訂閱的關聯"](#)。

我是否可以新增多個 **Azure** 認證、每個認證都有不同的市場訂閱？

屬於同一 Azure 訂閱的所有 Azure 認證資料將與同一 Azure Marketplace 訂閱相關聯。

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

我可以將現有的 **Cloud Volumes ONTAP** 工作環境移轉至不同的 **Azure** 訂閱嗎？

否、您無法將與 Cloud Volumes ONTAP 工作環境相關的 Azure 資源移轉至不同的 Azure 訂閱。

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 Azure Marketplace 在 Azure 中部署 Connector、也可以在自己的 Linux 主機上安裝 Connector 軟體。

如果您使用 Marketplace、您可以將自訂角色指派給 Connector VM 和系統指派的託管身分識別、以提供權限、或是使用 Microsoft Entra 服務主體。

對於內部部署、您無法設定 Connector 的託管身分識別、但可以使用服務主體來提供權限。

若要瞭解如何設定權限、請參閱下列頁面：

- 標準模式
 - ["設定 Azure 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 **Azure** 認證和市場訂閱

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

如果您需要使用多個Azure認證或多個Azure Marketplace訂閱Cloud Volumes ONTAP 以供使用、請依照本頁的步驟進行。

總覽

在BlueXP中新增額外Azure訂閱和認證的方法有兩種。

1. 將額外的Azure訂閱與Azure託管身分識別建立關聯。
2. 如果您要使用Cloud Volumes ONTAP 不同的Azure認證資料來部署功能、請使用服務主體來授予Azure權限、並將其認證資料新增至藍圖XP。

將額外的 **Azure** 訂閱與託管身分識別建立關聯

BlueXP可讓您選擇要部署Cloud Volumes ONTAP 的Azure認證和Azure訂閱。除非您建立關聯、否則您無法為託管身分識別設定檔選取不同的 Azure 訂閱 **"託管身分識別"** 這些訂閱。

關於這項工作

託管身分識別是 **"初始 Azure 帳戶"** 當您從BlueXP部署連接器時。部署Connector時、BlueXP會建立BlueXP運算子角色、並將其指派給Connector虛擬機器。

步驟

1. 登入 Azure 入口網站。
2. 開啟 * 訂閱 * 服務、然後選取您要部署 Cloud Volumes ONTAP 的訂閱內容。
3. 選取 * 存取控制 (IAM) * 。
 - a. 選取 * 新增 * > * 新增角色指派 * 、然後新增權限：

- 選取*藍圖操作員*角色。



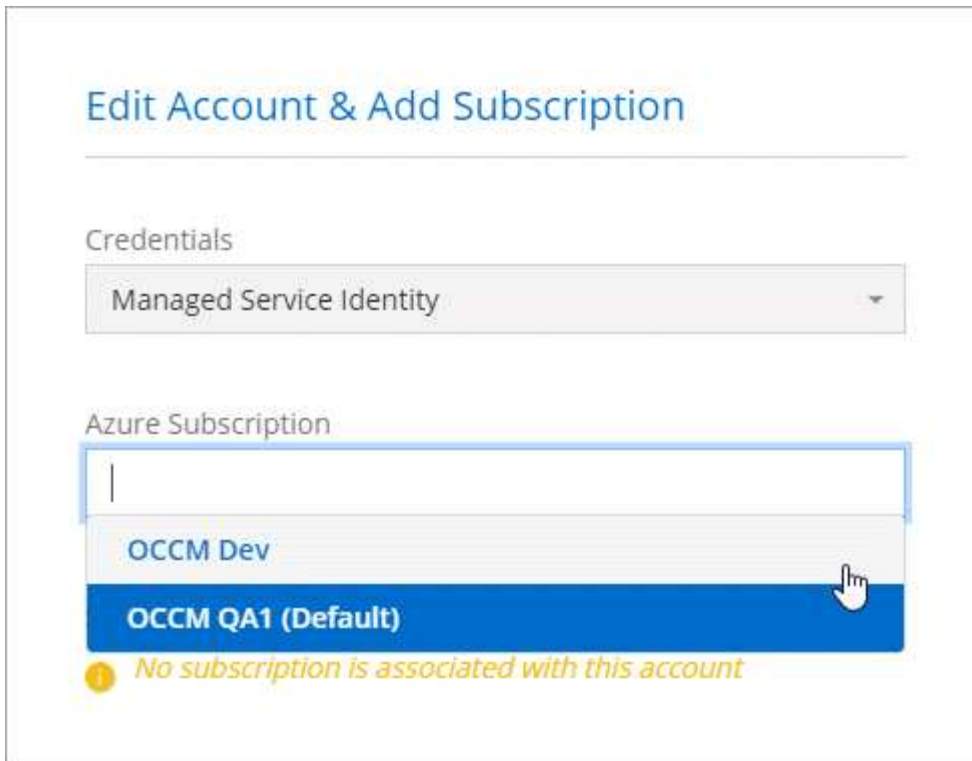
BlueXP運算子是Connector原則中提供的預設名稱。如果您為角色選擇不同的名稱、請改為選取該名稱。

- 指派 * 虛擬機器 * 的存取權。
- 選取建立 Connector 虛擬機器的訂閱。
- 選取 Connector 虛擬機器。
- 選擇*保存*。

4. 請重複這些步驟以取得額外訂閱內容。

結果

當您建立新的工作環境時、現在應該能夠從多個 Azure 訂閱中選取託管身分識別設定檔。



Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

將額外的 **Azure** 認證新增至 **BlueXP**

從BlueXP部署Connector時、BlueXP會在擁有必要權限的虛擬機器上啟用系統指派的託管身分識別。當您建立Cloud Volumes ONTAP 全新的作業系統環境時、BlueXP會預設選取這些Azure認證資料。



如果您在現有系統上手動安裝Connector軟體、則不會新增一組初始認證資料。 ["瞭解Azure認證與權限"](#)。

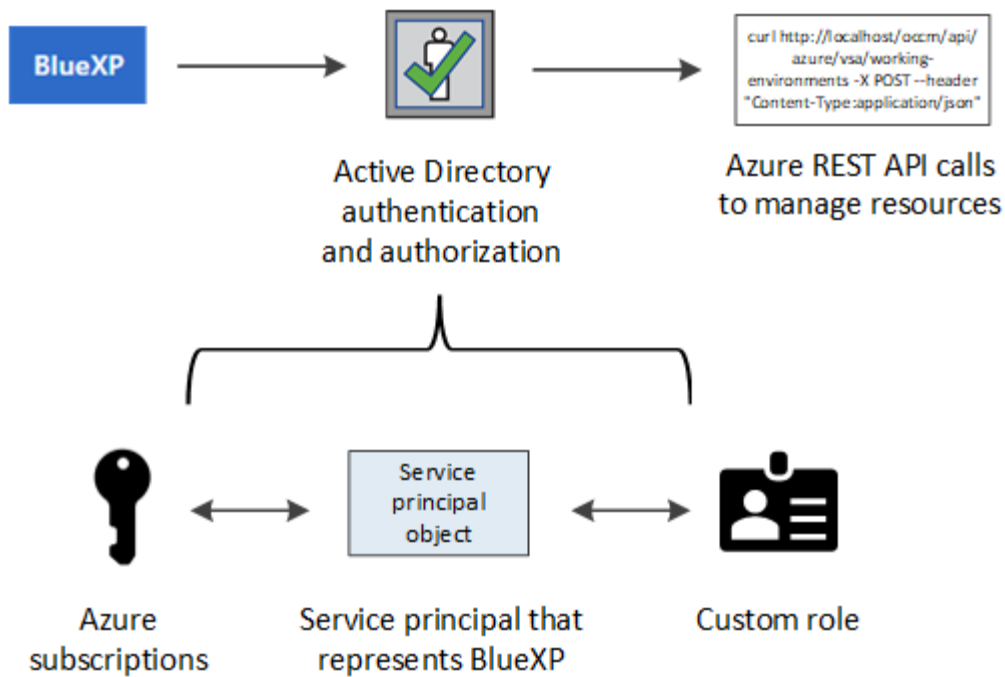
如果您想要使用 *_different* 的 Azure 認證來部署 Cloud Volumes ONTAP 、則必須在每個 Azure 帳戶的 Microsoft Entra ID 中建立及設定服務主體、以授予必要的權限。然後您可以將新認證新增至藍圖XP。

使用服務主體授與 **Azure** 權限

BlueXP需要權限才能在Azure中執行動作。您可以在 Microsoft Entra ID 中建立及設定服務主體、並取得BlueXP 所需的 Azure 認證、將必要權限授予 Azure 帳戶。

關於這項工作

下圖說明BlueXP如何取得權限在Azure中執行作業。服務主體物件與一或多個 Azure 訂閱相關、代表 Microsoft Entra ID 中的 BlueXP 、並指派給允許必要權限的自訂角色。



步驟

1. 建立 [Microsoft Entra 應用程式](#)。
2. [\[將應用程式指派給角色\]](#)。
3. 新增 [Windows Azure Service Management API 權限](#)。
4. 取得應用程式 ID 和目錄 ID。
5. [\[建立用戶端機密\]](#)。

建立 **Microsoft Entra** 應用程式

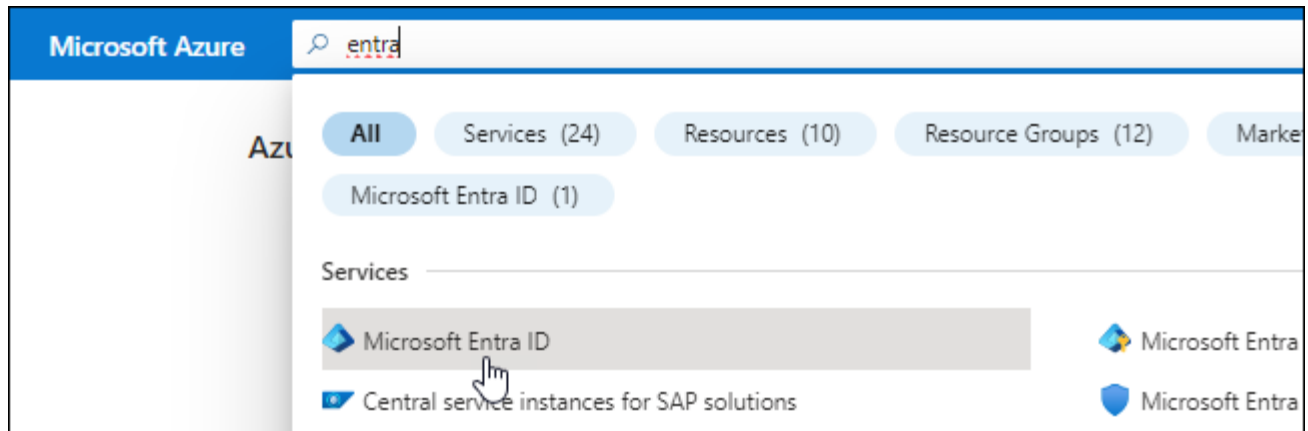
建立 Microsoft Entra 應用程式和服務主體、讓 BlueXP 用於角色型存取控制。

步驟

1. 確保您在 Azure 中擁有建立 Active Directory 應用程式及將應用程式指派給角色的權限。

如需詳細資訊、請參閱 "[Microsoft Azure 說明文件：必要權限](#)"

2. 從 Azure 入口網站開啟 * Microsoft Entra ID* 服務。



3. 在功能表中、選取 * 應用程式註冊 * 。
4. 選取 * 新登錄 * 。
5. 指定應用程式的詳細資料：
 - * 名稱 *：輸入應用程式的名稱。
 - 帳戶類型：選取帳戶類型（任何帳戶類型均可用於BlueXP）。
 - 重新導向URI：您可以將此欄位保留空白。
6. 選擇*註冊*。

您已建立 AD 應用程式和服務主體。

結果

您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

您必須將服務主體繫結至一或多個Azure訂閱、並指派自訂的「BlueXP運算子」角色給它、以便BlueXP在Azure中擁有權限。

步驟

1. 建立自訂角色：

請注意、您可以使用 Azure 入口網站、Azure PowerShell、Azure CLI 或 REST API 來建立 Azure 自訂角色。下列步驟說明如何使用 Azure CLI 建立角色。如果您想要使用不同的方法、請參閱 ["Azure文件"](#)

- a. 複製的內容 ["Connector的自訂角色權限"](#) 並將它們儲存在Json檔案中。
- b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

您應該為使用者建立 Cloud Volumes ONTAP 的各個 Azure 訂閱新增 ID 。

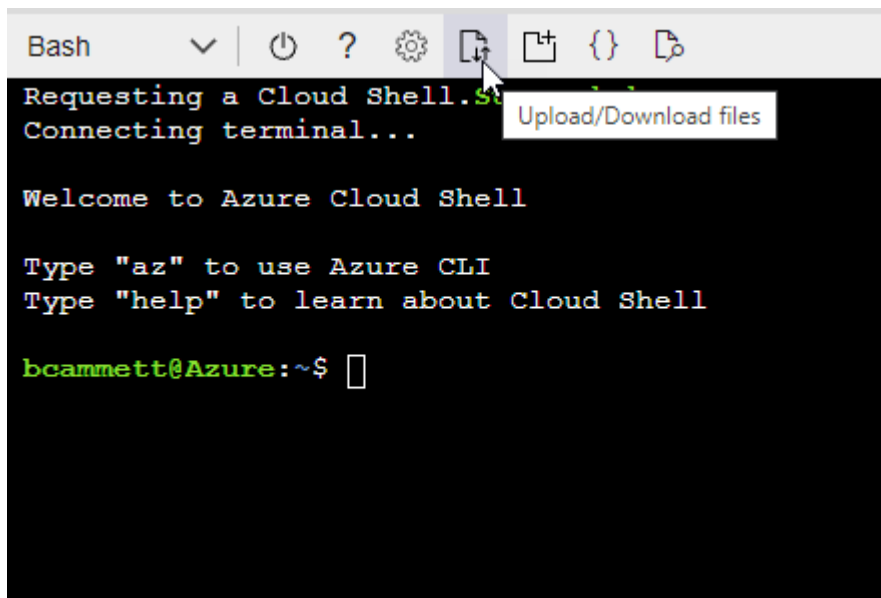
- 範例 *

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. 使用 Json 檔案在 Azure 中建立自訂角色。

下列步驟說明如何在 Azure Cloud Shell 中使用 Bash 建立角色。

- 開始 "Azure Cloud Shell" 並選擇 Bash 環境。
- 上傳 Json 檔案。



- 使用 Azure CLI 建立自訂角色：

```
az role definition create --role-definition Connector_Policy.json
```

現在您應該有一個名為 BlueXP 運算子的自訂角色、可以指派給連接器虛擬機器。

2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 * 訂閱 * 服務。
- 選取訂閱。
- 選取 * 存取控制 (IAM) > 新增 > 新增角色指派 *。
- 在 * 角色 * 索引標籤中、選取 * BlueXP 操作員 * 角色、然後選取 * 下一步 *。
- 在「成員」索引標籤中、完成下列步驟：
 - 保留 * 選取「使用者」、「群組」或「服務主體」 *。
 - 選取 * 選取成員 *。

Add role assignment ...

[Got feedback?](#)

Role **Members** [Review + assign](#)

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- 搜尋應用程式名稱。

範例如下：

Select members ×

Select ⓘ

test-service-principal

test-service-principal

- 選取應用程式、然後選取 * 選取 *。
 - 選擇*下一步*。
- f. 選取 * 檢閱 + 指派 *。

服務主體現在擁有部署Connector所需的Azure權限。

如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。BlueXP可讓您選擇部署Cloud Volumes ONTAP 時要使用的訂閱內容。

新增 **Windows Azure Service Management API** 權限

服務主體必須具有「Windows Azure Service Management API」權限。

步驟

1. 在 * Microsoft Entra ID* 服務中、選取 * 應用程式登錄 * 、然後選取應用程式。
2. 選取 * API 權限 > 新增權限 * 。
3. 在「 * Microsoft API* 」下、選取「 * Azure 服務管理 * 」。













Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

4. 選取 * 以組織使用者身分存取 Azure 服務管理 * 、然後選取 * 新增權限 * 。

Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

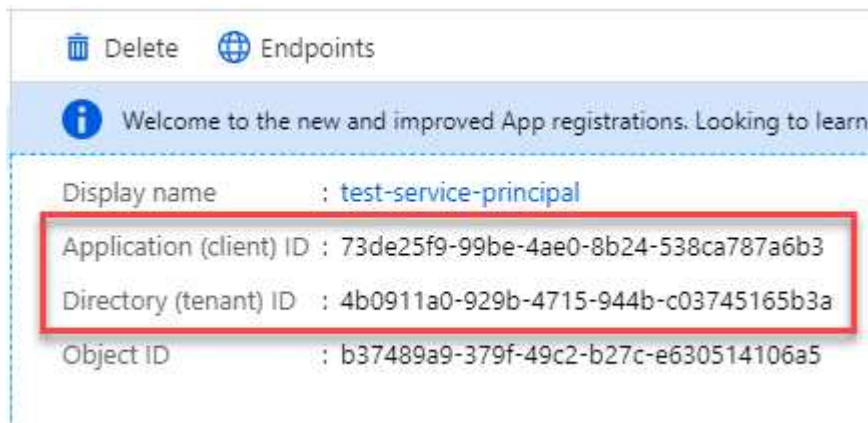
Access Azure Service Management as organization users (preview) ⓘ

取得應用程式 ID 和目錄 ID

將 Azure 帳戶新增至 BlueXP 時、您必須提供應用程式的應用程式（用戶端）ID 和目錄（租戶）ID。BlueXP 使用 ID 以程式設計方式登入。

步驟

1. 在 * Microsoft Entra ID* 服務中、選取 * 應用程式登錄 *、然後選取應用程式。
2. 複製 * 應用程式（用戶端）ID* 和 * 目錄（租戶）ID*。



將 Azure 帳戶新增至 BlueXP 時、您必須提供應用程式的應用程式（用戶端）ID 和目錄（租戶）ID。BlueXP 使用 ID 以程式設計方式登入。

建立用戶端機密

您需要建立用戶端機密、然後提供 BlueXP 的機密值、以便 BlueXP 使用它來驗證 Microsoft Entra ID。

步驟

1. 開啟 * Microsoft Entra ID* 服務。

2. 選取 * 應用程式註冊 * 、然後選取您的應用程式。
3. 選取 * 「憑證與機密」 > 「新用戶端機密」 * 。
4. 提供機密與持續時間的說明。
5. 選取 * 「Add*」 。
6. 複製用戶端機密的值。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

您現在擁有一個客戶機密、BlueXP 可以使用它來驗證 Microsoft Entra ID 。

結果

您的服務主體現在已設定完成、您應該已經複製應用程式（用戶端）ID、目錄（租戶）ID、以及用戶端機密的值。新增Azure帳戶時、您必須在BlueXP中輸入此資訊。

將認證資料新增至藍圖XP

在您提供Azure帳戶所需的權限之後、即可將該帳戶的認證資料新增至BlueXP。完成此步驟可讓您Cloud Volumes ONTAP 使用不同的Azure認證資料來啟動功能。

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。

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 * 。

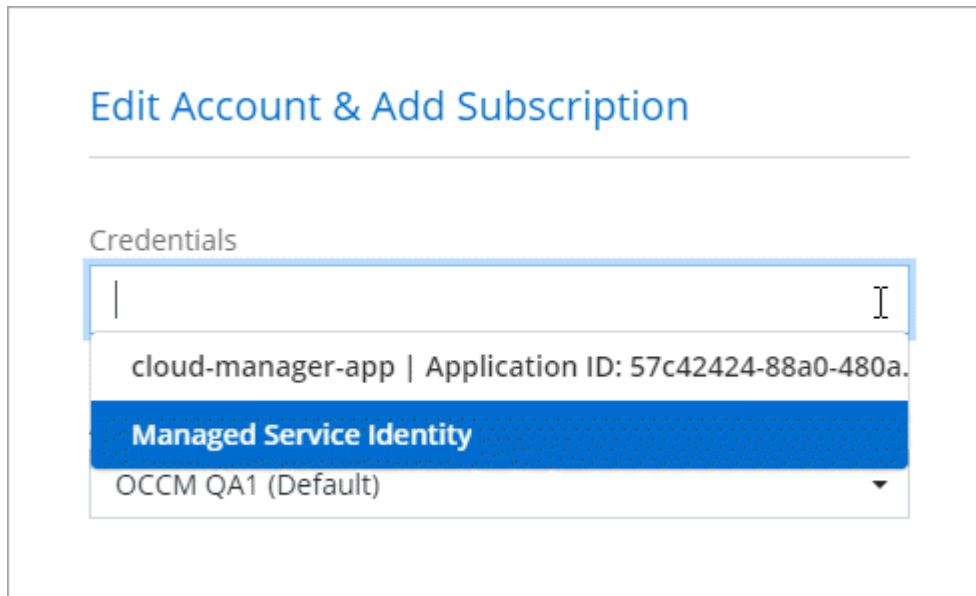


2. 選取 * 新增認證 * 、然後依照精靈中的步驟進行。
 - a. 認證位置：選擇* Microsoft Azure > Connector* 。
 - b. * 定義認證 * ：輸入 Microsoft Entra 服務授權者的相關資訊、以授予必要的權限：
 - 應用程式（用戶端）ID
 - 目錄（租戶）ID

- 用戶端機密
- 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。
- d. * 審查 *：確認新認證的詳細資料、然後選取 * 新增 *。

結果

您現在可以從「詳細資料與認證」頁面切換至不同的認證集合 ["在建立新的工作環境時"](#)



管理現有認證資料

透過建立Marketplace訂閱、編輯認證及刪除認證、來管理您已新增至BlueXP的Azure認證資料。

將 Azure Marketplace 訂閱與認證建立關聯

將Azure認證資料新增至BlueXP之後、您就可以將Azure Marketplace訂閱與這些認證資料建立關聯。訂閱可讓您建立隨用隨付的 Cloud Volumes ONTAP 系統、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Azure 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 Azure 認證相關的 Azure 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。

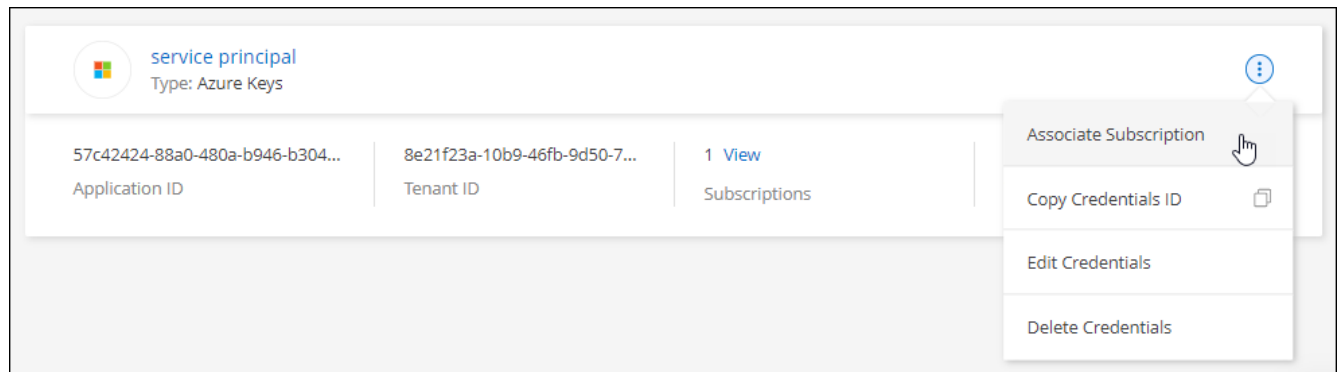
開始之前

您必須先建立連接器、才能變更BlueXP設定。 ["瞭解方法"](#)。

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 Azure Marketplace 中的步驟進行：
 - a. 出現提示時、請登入您的Azure帳戶。
 - b. 選取 * 訂閱 * 。
 - c. 填寫表單並選擇 * 訂閱 * 。
 - d. 訂閱程序完成後、請選取 * 立即設定帳戶 * 。

您將被重新導向至BlueXP網站。

- e. 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Azure Marketplace訂閱的步驟：

從 Azure Marketplace 訂閱 BlueXP

編輯認證資料

修改Azure服務認證資料的詳細資料、即可在BlueXP中編輯Azure認證資料。例如、如果為服務主體應用程式建立新的密碼、您可能需要更新用戶端密碼。

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。

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。

Google Cloud

瞭解 Google Cloud 專案和權限

瞭解 BlueXP 如何使用 Google Cloud 認證來代表您執行行動、以及這些認證如何與市場訂閱相關聯。瞭解這些詳細資料有助於您管理一或多個 Google Cloud 專案的認證。例如、您可能想要瞭解與 Connector VM 相關聯的服務帳戶。

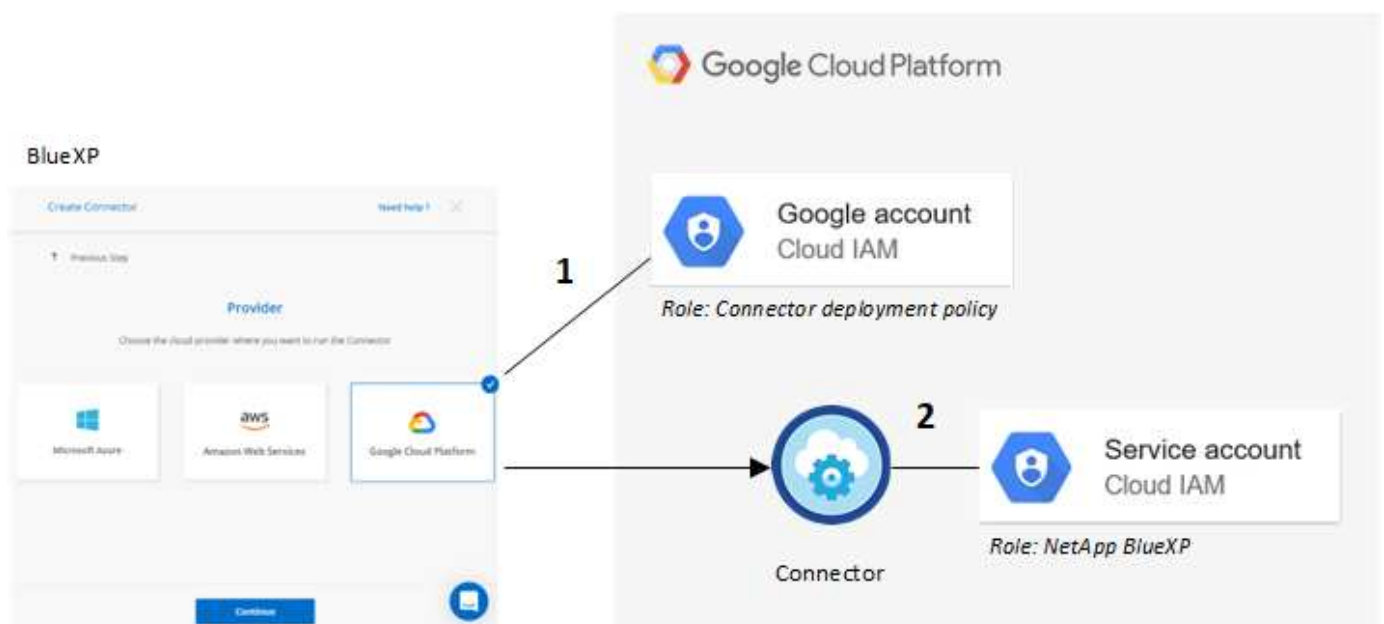
BlueXP的專案與權限

您必須先部署 Connector、才能使用 BlueXP 管理 Google Cloud 專案中的資源。Connector 無法在您的內部環境或其他雲端供應商中執行。

直接從BlueXP部署Connector之前、必須先設定兩組權限：

1. 您需要使用具有從BlueXP啟動Connector VM執行個體權限的Google帳戶來部署Connector。
2. 部署 Connector 時、系統會提示您選取 "服務帳戶" 適用於 VM 執行個體。BlueXP 可從服務帳戶取得權限來建立和管理 Cloud Volumes ONTAP 系統、使用 BlueXP 備份和還原來管理備份等。將自訂角色附加至服務帳戶、即可提供權限。

下圖說明上述第 1 和第 2 項所述的權限要求：



若要瞭解如何設定權限、請參閱下列頁面：

- ["設定標準模式的 Google Cloud 權限"](#)
- ["設定受限模式的權限"](#)
- ["設定私有模式的權限"](#)

認證與市場訂閱

當您在 Google Cloud 中部署 Connector 時、BlueXP 會在 Connector 所在的專案中、為 Google Cloud 服務帳戶建立一組預設認證。這些認證必須與 Google Cloud Marketplace 訂閱相關聯、以便您可以按小時費率（PAYGO）支付 Cloud Volumes ONTAP 費用、並使用其他 BlueXP 服務。

["瞭解如何建立 Google Cloud Marketplace 訂閱的關聯"](#)。

請注意下列關於 Google Cloud 認證和市場訂閱的資訊：

- 只能將一組 Google Cloud 認證與 Connector 建立關聯
- 您只能將一個 Google Cloud Marketplace 訂閱與認證建立關聯
- 您可以使用新訂閱來取代現有的市場訂閱

適用於此產品的專案 Cloud Volumes ONTAP

可與 Connector 位於同一個專案中、或位於不同的專案中。Cloud Volumes ONTAP 若要在 Cloud Volumes ONTAP 不同的專案中部署功能、您必須先將 Connector 服務帳戶和角色新增至該專案。

- ["瞭解如何設定服務帳戶"](#)
- ["瞭解如何在 Google Cloud 中部署 Cloud Volumes ONTAP、並選擇專案"](#)

管理 BlueXP 的 Google Cloud 認證和訂閱

您可以建立與 Connector VM 執行個體相關聯的 Google Cloud 認證、方法是建立市場訂閱的關聯、並疑難排解訂閱程序。這兩項工作都能確保您可以使用市場訂閱來支付 BlueXP 服務費用。

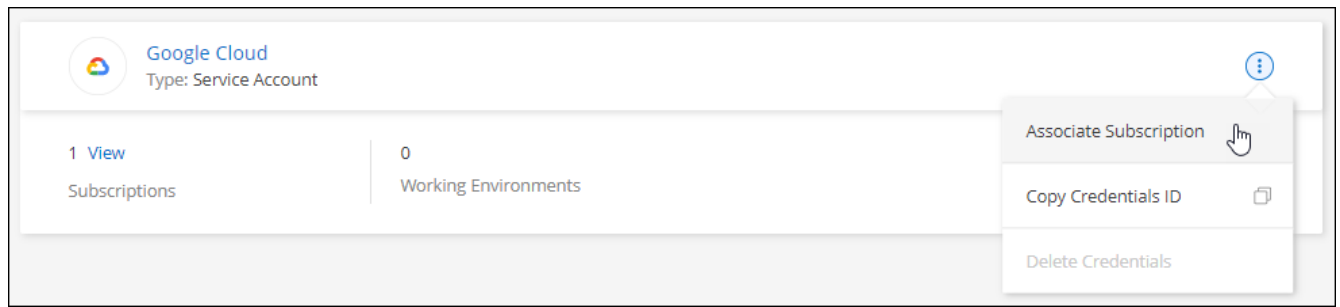
將 Marketplace 訂閱與 Google Cloud 認證建立關聯

在 Google Cloud 中部署 Connector 時、BlueXP 會建立一組與 Connector VM 執行個體相關的預設認證資料。您可以隨時變更與這些認證相關的 Google Cloud Marketplace 訂閱。訂閱可讓您建立隨用隨付的 Cloud Volumes ONTAP 系統、並使用其他 BlueXP 服務。

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。

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 *。



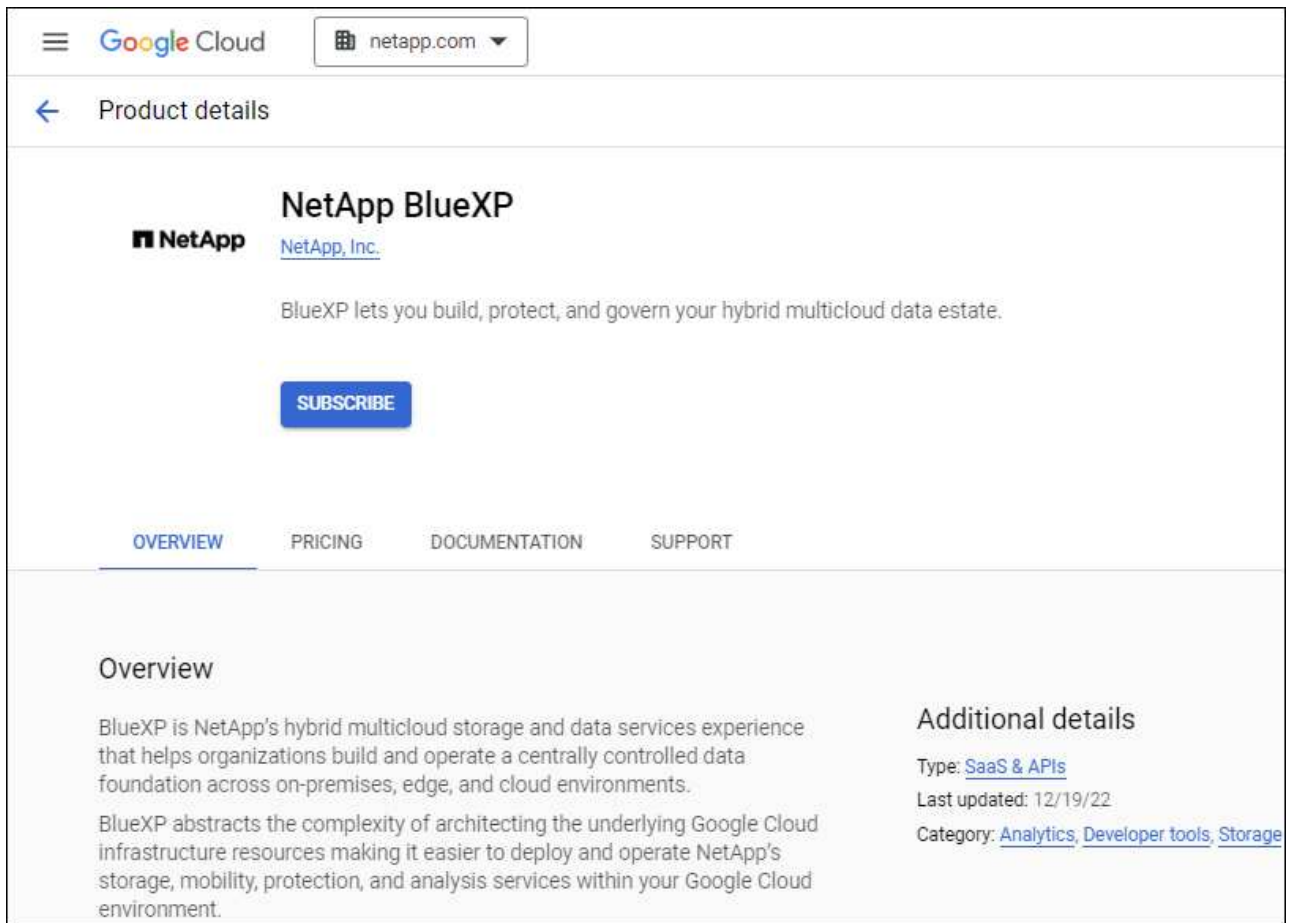
3. 若要將認證與現有訂閱建立關聯、請從下拉式清單中選取 Google Cloud 專案和訂閱、然後選取 * Associate*。

4. 如果您尚未訂閱、請選取 * 新增訂閱 > 繼續 *、然後依照 Google Cloud Marketplace 中的步驟進行。



在您完成下列步驟之前、請先確認您的Google Cloud帳戶擁有「帳單管理」權限、以及BlueXP登入權限。

- a. 重新導向至之後 "[Google Cloud Marketplace上的NetApp BlueXP頁面](#)"下、請確定在頂端導覽功能表中選取正確的專案。

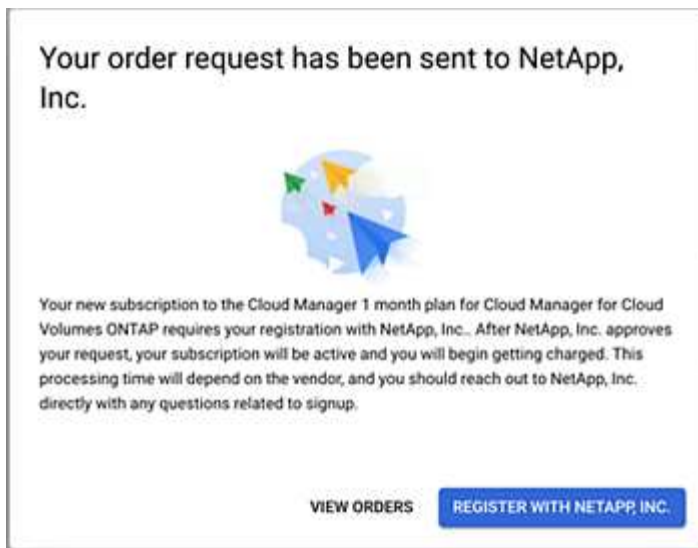


- b. 選取 * 訂閱 * 。
- c. 選擇適當的帳單帳戶、並同意條款與條件。
- d. 選取 * 訂閱 * 。

此步驟會將您的轉帳要求傳送給NetApp。

- e. 在快顯對話方塊中、選取 * 註冊 NetApp 、 Inc.*

您必須完成此步驟、才能將 Google Cloud 訂閱連結至您的 BlueXP 帳戶。連結訂閱的程序要等到您從本頁重新導向、然後登入BlueXP之後才會完成。



f. 完成「訂閱指派」頁面上的步驟：



如果貴組織的人員已從您的帳單帳戶訂閱NetApp BlueXP訂閱、您將會被重新導向至 "[BlueXP網站上的「支持」頁面Cloud Volumes ONTAP](#)" 而是。如果這是意外情況、請聯絡您的NetApp銷售團隊。Google每個Google帳單帳戶只能啟用一次訂閱。

- 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Google Cloud Marketplace訂閱的步驟：

[從 Google Cloud Marketplace 訂閱 BlueXP](#)

- a. 完成此程序後、請瀏覽至BlueXP中的「認證」頁面、然後選取此新的訂閱。

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

+ Add Subscription

疑難排解 Marketplace 訂閱程序

有時透過 Google Cloud Marketplace 訂閱 BlueXP 可能會因為權限不正確或不小心轉寄至 BlueXP 網站而變得零散。如果發生這種情況、請使用下列步驟完成訂購程序。

步驟

1. 瀏覽至 "[Google Cloud Marketplace上的NetApp BlueXP頁面](#)" 檢查訂單狀態。如果頁面顯示 * 管理供應商 *、請向下捲動並選取 * 管理訂單 *。

Pricing

The product was purchased on 12/9/20.

MANAGE ORDERS

- 如果訂單顯示綠色勾選標記、但這是意外情況、則組織中使用相同帳單帳戶的其他人可能已經訂閱。如果這是意外情況、或您需要此訂閱的詳細資料、請聯絡您的NetApp銷售團隊。

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- 如果訂單顯示時鐘和*待處理*狀態、請返回市場頁面、選擇*管理供應商*以完成上述程序。

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

管理與BlueXP帳戶相關聯的NSS認證

將 NetApp 支援網站 帳戶與 BlueXP 帳戶建立關聯、以啟用 Cloud Volumes ONTAP 的關鍵工作流程。這些NSS認證資料會與整個BlueXP帳戶建立關聯。



BlueXP也支援為每個BlueXP使用者建立一個NSS帳戶的關聯。"瞭解如何管理使用者層級認證"。

總覽

若要在BlueXP中啟用下列工作、需要將NetApp 支援網站 此認證與您的特定BlueXP帳戶ID建立關聯：

- 自帶授權（Cloud Volumes ONTAP BYOL）即可部署

您必須提供您的NSS帳戶、才能讓BlueXP上傳授權金鑰、並啟用您所購買期間的訂閱。這包括定期續約的自動更新。

- 註冊隨用隨付Cloud Volumes ONTAP 的功能系統

您必須提供您的NSS帳戶、才能啟動系統支援、並取得NetApp技術支援資源的存取權。

- 升級Cloud Volumes ONTAP 更新版的更新版

這些認證資料會與您的特定BlueXP帳戶ID建立關聯。屬於BlueXP帳戶的使用者可以從*支援> nss管理*存取這些認證資料。

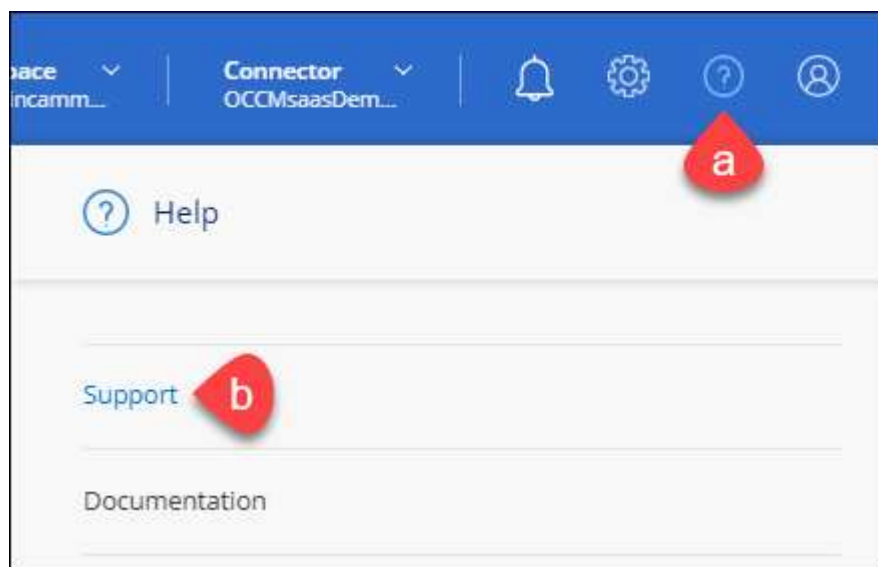
新增一個NSS帳戶

「支援儀表板」可讓您新增及管理NetApp 支援網站 適用於BlueXP帳戶層級的功能。

- 如果您有客戶層級的帳戶、可以新增一或多個NSS帳戶。
- 如果您有合作夥伴或經銷商帳戶、您可以新增一或多個NSS帳戶、但這些帳戶無法與客戶層級帳戶一起新增。

步驟

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



2. 選取 **NSS Management > Add NSS Account** 。
3. 系統提示時、請選取 * 繼續 * 以重新導向至 Microsoft 登入頁面。

NetApp 使用 Microsoft Entra ID 做為身分識別提供者、提供專為支援與授權所設計的驗證服務。

4. 在登入頁面上，提供您的 NetApp 支援網站註冊電子郵件地址和密碼，以執行身分驗證程序。

這些行動可讓BlueXP將您的nssa帳戶用於授權下載、軟體升級驗證、以及未來的支援註冊等項目。


請注意下列事項：


- NSS-帳戶必須是客戶層級的帳戶（而非來賓帳戶或暫存帳戶）。您可以擁有多個客戶層級的NSS帳戶。
- 如果該帳戶是合作夥伴層級帳戶、則只能有一個NSS帳戶。如果您嘗試新增客戶層級的NSS帳戶、但有合作夥伴層級的帳戶存在、您會收到下列錯誤訊息：

「此帳戶不允許使用新增服務客戶類型、因為已經有不同類型的新增服務使用者。」

如果您擁有預先存在的客戶層級的NSS帳戶、並嘗試新增合作夥伴層級的帳戶、情況也是如此。

- 成功登入後、NetApp會儲存NSS.使用者名稱。

這是系統產生的ID、會對應至您的電子郵件。在「* nssn*管理*」頁面上、您可以從顯示電子郵件  功能表。

- 如果您需要重新整理登入認證憑證權杖、也可以在中使用*更新認證*選項  功能表。

使用此選項會提示您重新登入。請注意、這些帳戶的權杖會在90天後過期。系統會張貼通知、提醒您注意此點。

接下來呢？

現在、使用者可以在建立新的 Cloud Volumes ONTAP 系統和註冊現有 Cloud Volumes ONTAP 系統時、選擇帳戶。


- "在 Cloud Volumes ONTAP AWS 中啟動"
- "在 Cloud Volumes ONTAP Azure 中啟動"
- "在Cloud Volumes ONTAP Google Cloud上啟動"
- "註冊隨用隨付系統"

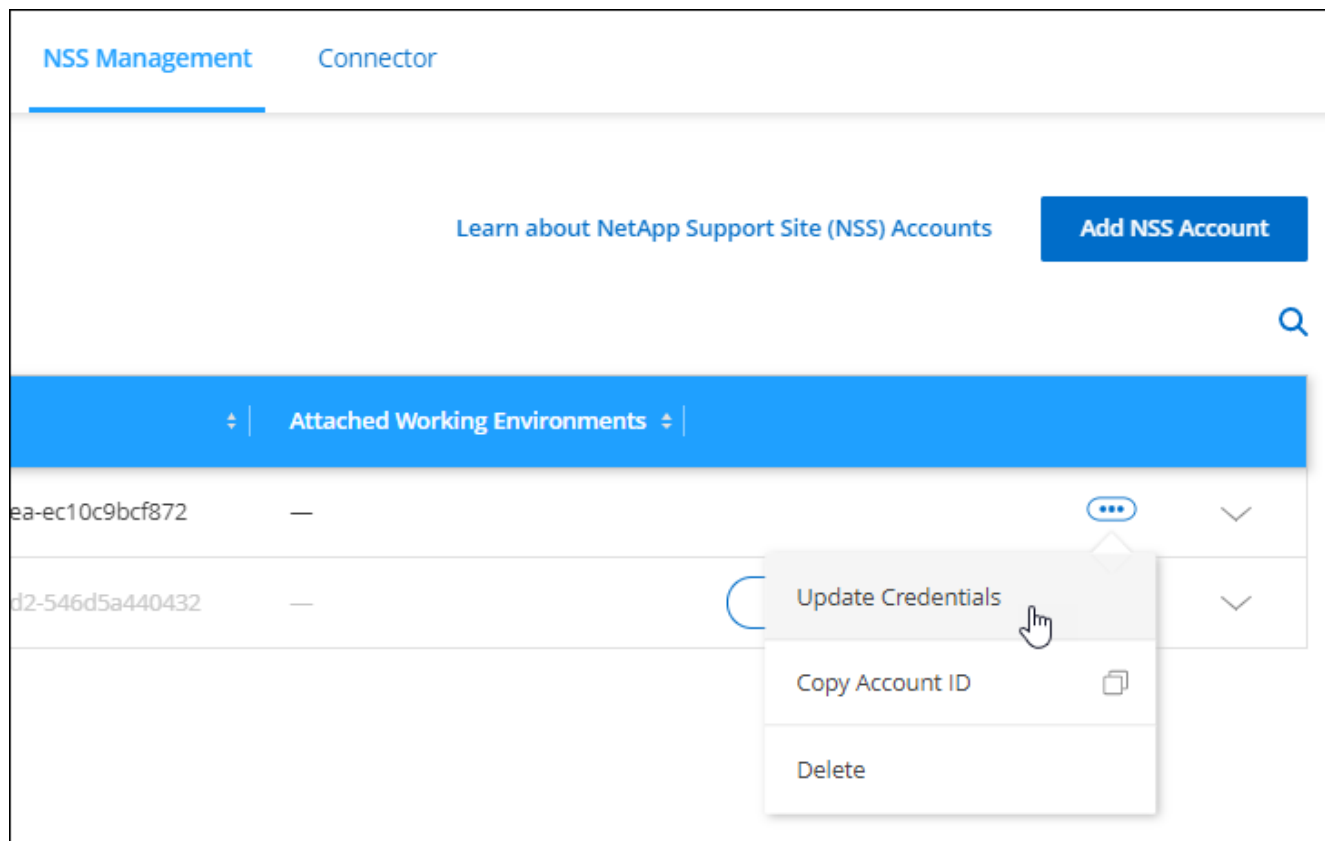
更新 NSS 認證

發生下列任一情況時、您必須更新BlueXP中的NSS帳戶認證：

- 您可以變更帳戶的認證資料
- 與您帳戶相關的更新Token會在3個月後過期

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 *」。
2. 選取 * NSS 管理 *。
3. 針對您要更新的 NSS 帳戶、選取  然後選取*更新認證*。



4. 系統提示時、請選取 * 繼續 * 以重新導向至 Microsoft 登入頁面。

NetApp 使用 Microsoft Entra ID 做為身分識別提供者、提供專為支援與授權所設計的驗證服務。

5. 在登入頁面上，提供您的 NetApp 支援網站註冊電子郵件地址和密碼，以執行身分驗證程序。

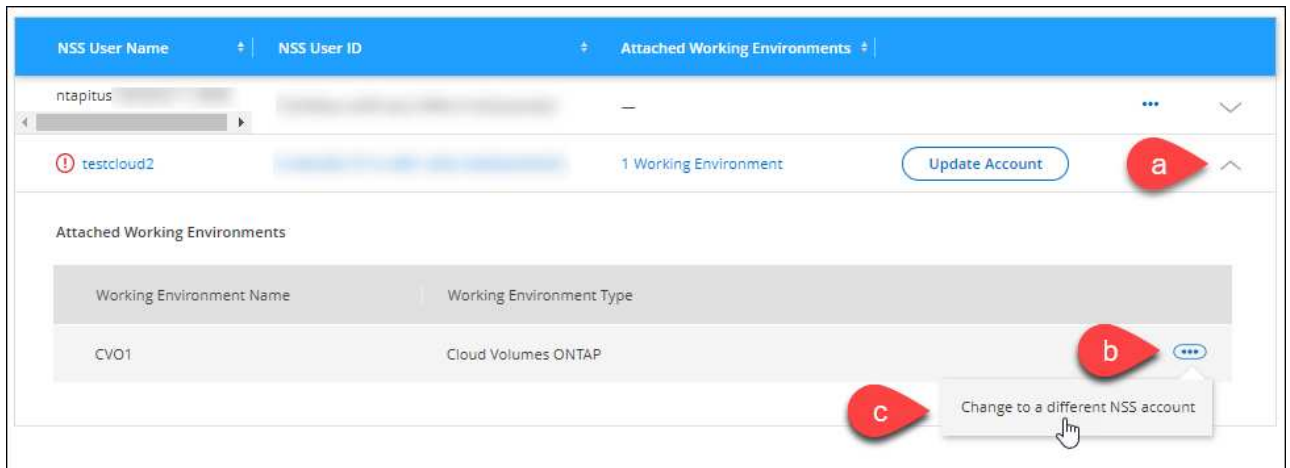
將工作環境附加至不同的NSS帳戶

如果貴組織有多個 NetApp 支援網站帳戶，您可以變更哪個帳戶要與哪個 Cloud Volumes ONTAP 系統相關聯。

此功能僅支援已設定為使用 NetApp 採用的 Microsoft Entra ID 進行身分識別管理的 NSS 帳戶。在使用此功能之前、您需要選取 * 新增 NSS 帳戶 * 或 * 更新帳戶 *。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 *」。
2. 選取 * NSS 管理 *。
3. 完成下列步驟以變更NSS帳戶：
 - a. 展開目前與工作環境相關聯的 NetApp 支援網站帳戶列。
 - b. 針對您要變更關聯的工作環境、選取 ...
 - c. 選擇*變更為不同的nss*帳戶。



d. 選取帳戶、然後選取 * 儲存 * 。

顯示NSS帳戶的電子郵件地址

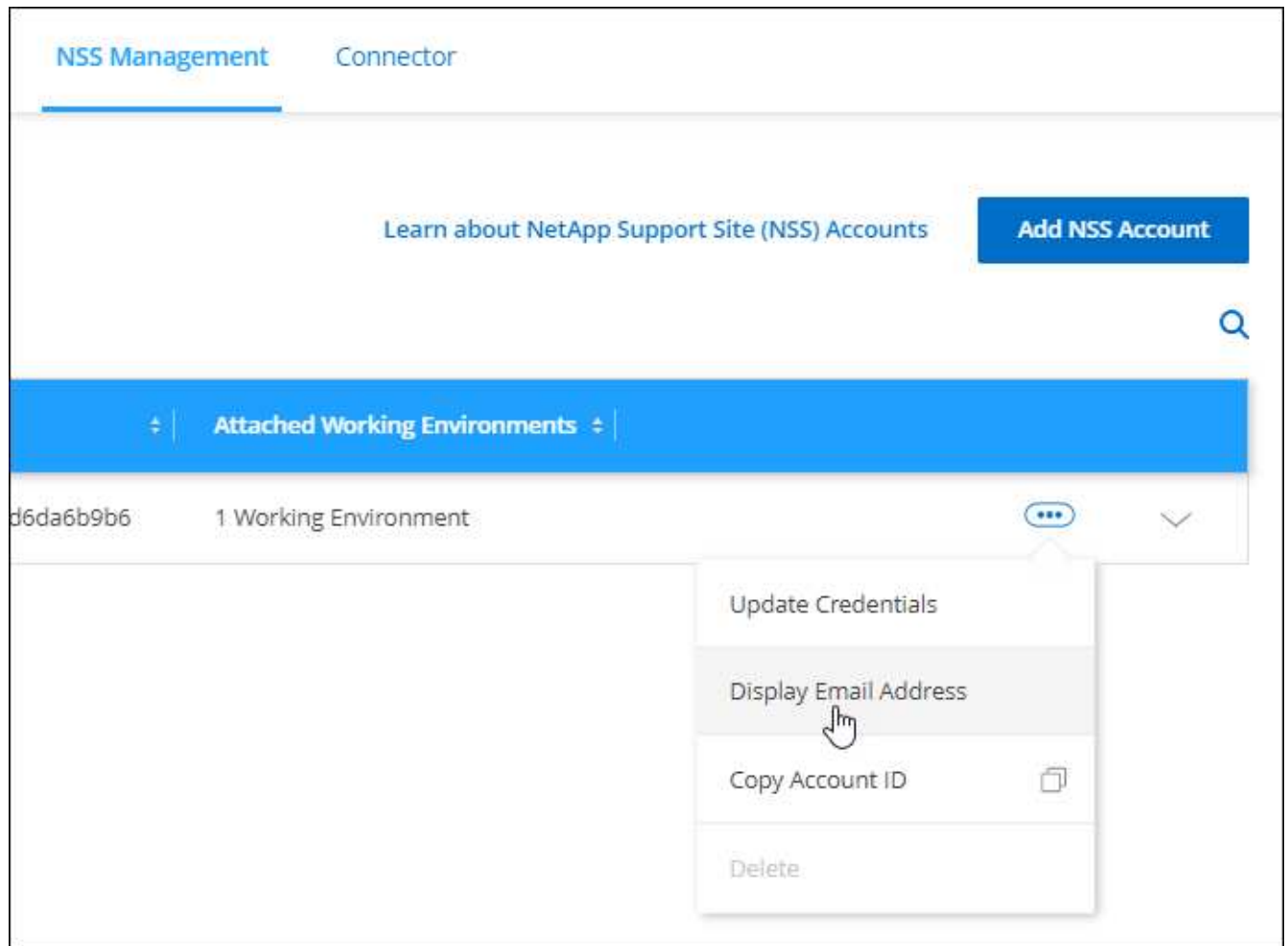
現在 NetApp 支援網站 帳戶使用 Microsoft Entra ID 進行驗證服務、BlueXP 中顯示的 NSS 使用者名稱通常是 Microsoft Entra 所產生的識別碼。因此、您可能無法立即得知與該帳戶相關的電子郵件地址。不過、BlueXP 有一個選項可以顯示相關的電子郵件地址。



當您移至「NSS管理」頁面時、BlueXP會為表格中的每個帳戶產生一個權杖。該權杖包含相關電子郵件地址的相關資訊。當您離開頁面時、便會移除權杖。這些資訊永遠不會快取、有助於保護您的隱私。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 *」。
2. 選取 * NSS 管理 * 。
3. 針對您要更新的 NSS 帳戶、選取 ... 然後選取*顯示電子郵件地址*。



結果

BlueXP會顯示NetApp 支援網站 不完整的使用者名稱及相關的電子郵件地址。您可以使用複製按鈕來複製電子郵件地址。

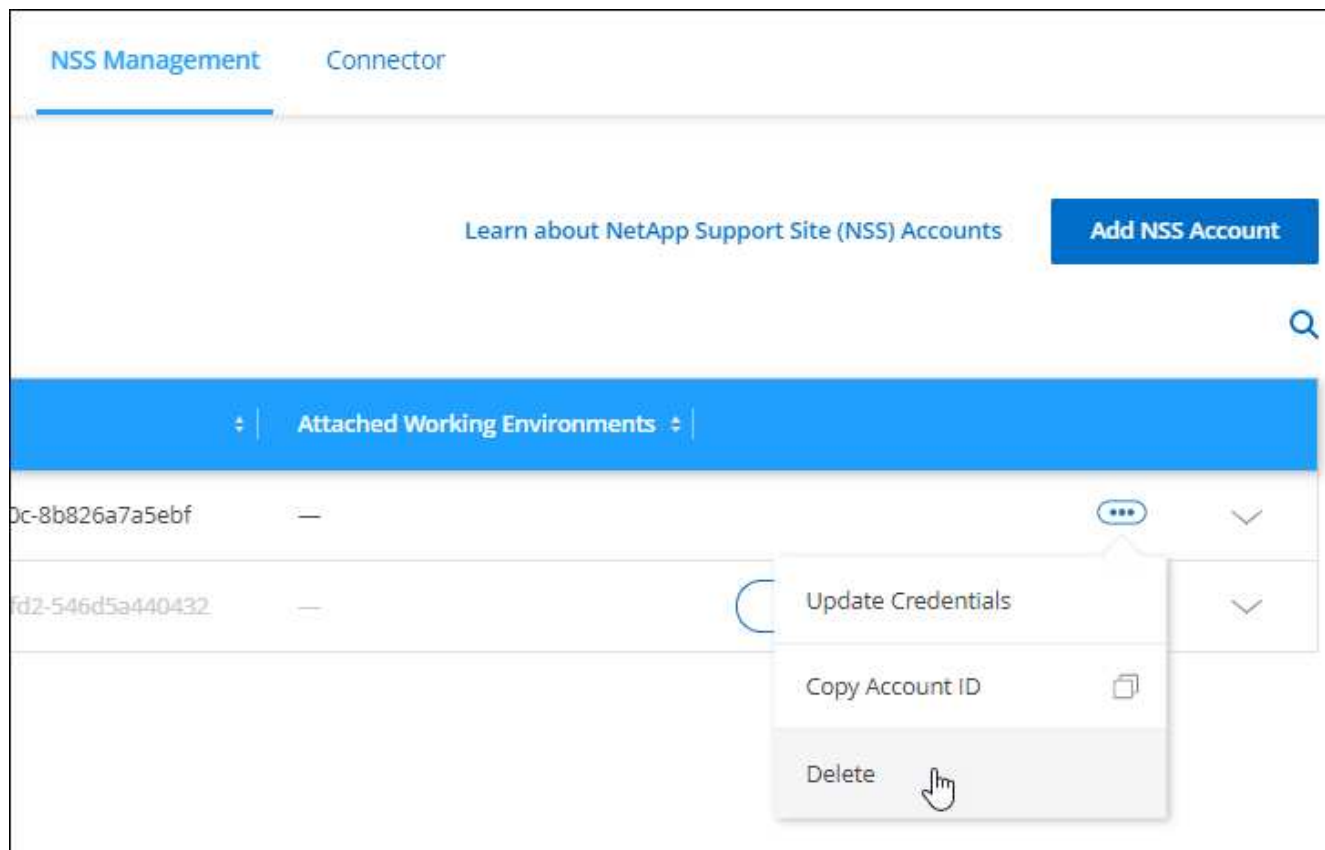
移除NSS.帳戶

刪除任何不再想與BlueXP搭配使用的NSS帳戶。

請注意、您無法刪除目前與Cloud Volumes ONTAP 某個運作環境相關聯的帳戶。您首先需要 [將這些工作環境附加至不同的NSS帳戶](#)。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 *「支援 *」。
2. 選取 * NSS 管理 *。
3. 針對您要刪除的 NSS 帳戶、選取 ... 然後選取*刪除*。



4. 選擇 * 刪除 * 進行確認。

管理與您的BlueXP登入相關的認證資料

視您在BlueXP中採取的行動而定、ONTAP 您可能會在NetApp 支援網站 使用者登入BlueXP時、擁有相關的功能驗證資料和功能驗證（NSS）認證資料。您可以在建立相關聯之後、在BlueXP中檢視及管理這些認證資料。例如、如果您變更這些認證資料的密碼、則需要更新BlueXP中的密碼。

身分證明ONTAP

當您直接探索內部部署ONTAP 的無線叢集而不使用Connector時、系統會提示您輸入ONTAP 叢集的憑據。這些認證資料是在使用者層級進行管理、這表示登入的其他使用者無法檢視這些認證資料。

NSS.認證資料

與 BlueXP 登入相關的 NSS 認證資料可支援註冊、案例管理及存取 Digital Advisor 。

- 當您存取 * 支援 > 資源 * 並註冊支援時、系統會提示您將 NSS 認證與 BlueXP 登入建立關聯。

此動作會登錄 BlueXP 帳戶以取得支援、並啟動支援權利。BlueXP 帳戶中只有一位使用者必須將 NetApp 支援網站 帳戶與其 BlueXP 登入建立關聯、才能註冊支援並啟動支援權利。完成後、「* 資源 *」頁面會顯示您的帳戶已註冊以取得支援。

["瞭解如何註冊以取得支援"](#)

- 當您存取*支援>個案管理*時、系統會提示您輸入您的NSS認證（如果您尚未輸入）。此頁面可讓您建立及管理與您的 NSS 帳戶和貴公司相關的支援案例。
- 當您在BlueXP中存取Digital Advisor時、系統會提示您輸入您的NSS認證、以登入Digital Advisor。

請注意下列與 BlueXP 登入相關的 NSS 帳戶：

- 帳戶是在使用者層級管理、這表示登入的其他使用者無法檢視。
- 每位使用者只能有一個與 Digital Advisor 相關聯的 NSS 帳戶、以及支援案例管理。
- 如果您嘗試將 NetApp 支援網站 帳戶與 Cloud Volumes ONTAP 工作環境建立關聯、則只能從新增至您所屬 BlueXP 帳戶的 NSS 帳戶中進行選擇。

NSS 帳戶層級的認證與與 BlueXP 登入相關的 NSS 帳戶不同。NSS 帳戶層級認證可讓您在攜帶自己的授權（BYOL）、註冊 PAYGO 系統、以及升級 Cloud Volumes ONTAP 軟體時、部署 Cloud Volumes ONTAP。

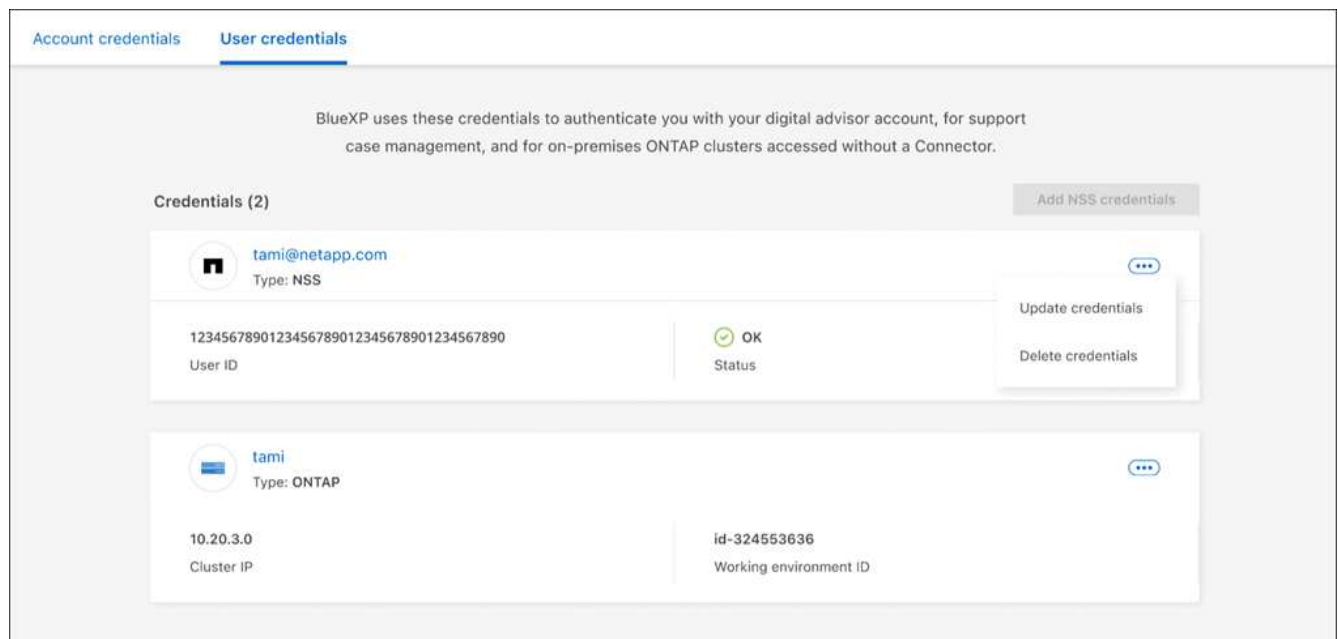
["深入瞭解如何搭配您的BlueXP帳戶使用NSS認證"](#)。

管理您的使用者認證資料

更新使用者名稱和密碼、或刪除認證資料、以管理您的使用者認證資料。

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. 選取 * 使用者認證 *。
3. 如果您還沒有任何使用者認證資料、您可以選取*新增NSS帳戶認證*來新增NetApp 支援網站 您的帳戶。
4. 選擇下列選項來管理現有認證：
 - 更新認證資料：更新帳戶的使用者名稱和密碼。
 - 刪除認證資料：移除與您的BlueXP使用者帳戶相關的帳戶。



結果

BlueXP會更新您的認證資料。當您存取ONTAP「叢集」、「數位顧問」或「案例管理」頁面時、這些變更將會反映出來。

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。