



# **AWS**

## **Setup and administration**

NetApp  
June 17, 2024

# 目录

AWS .....	1
了解 AWS 凭据和权限 .....	1
管理BlueXP的AWS凭据和市场订阅 .....	4

# AWS

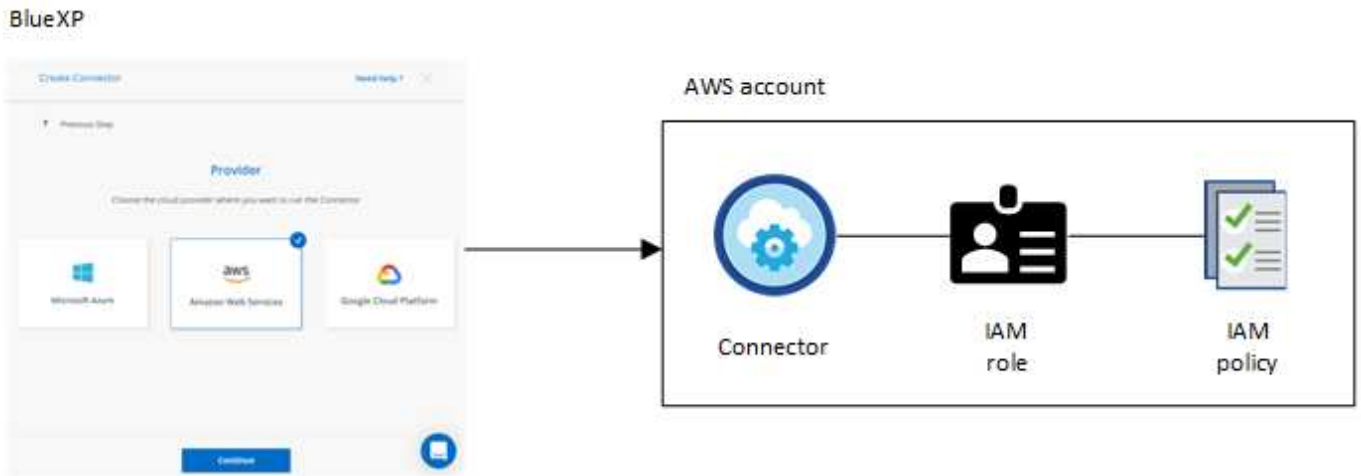
## 了解 AWS 凭据和权限

了解BlueXP如何使用AWS凭据代表您执行操作、以及这些凭据如何与商城订阅相关联。了解这些详细信息有助于您在BlueXP中管理一个或多个AWS帐户的凭据。例如、您可能希望了解何时向BlueXP添加其他AWS凭据。

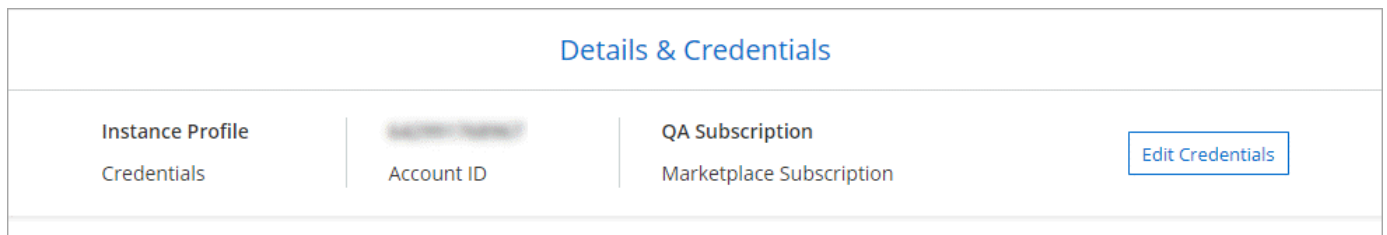
### 初始 AWS 凭据

从BlueXP部署Connector时、您需要为IAM用户提供IAM角色的ARN或访问密钥。您使用的身份验证方法必须具有在 AWS 中部署 Connector 实例所需的权限。中列出了所需的权限 "[适用于AWS的Connector部署策略](#)"。

当BlueXP在AWS中启动Connector实例时、它会为此实例创建IAM角色和实例配置文件。此外，它还会附加一个策略，为 Connector 提供管理该 AWS 帐户中资源和进程的权限。"[查看BlueXP如何使用权限](#)"。



如果为Cloud Volumes ONTAP创建新的工作环境、则BlueXP会默认选择以下AWS凭据：



您可以使用初始 AWS 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭据。

### 其他 AWS 凭据

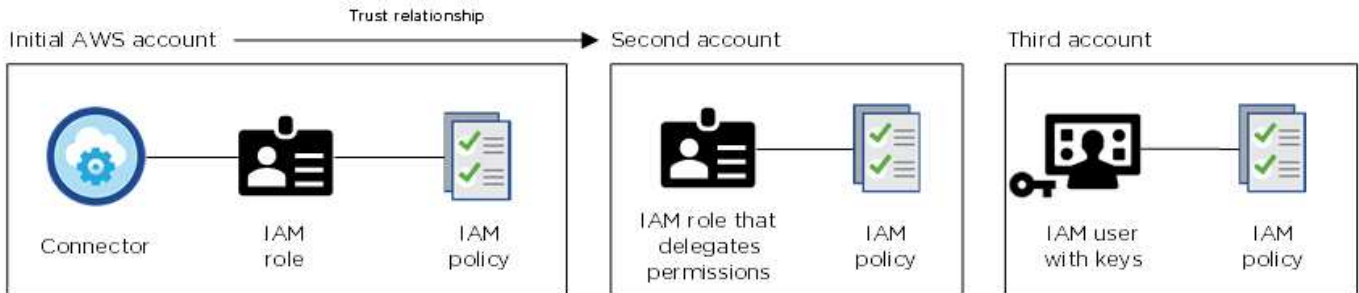
可以通过两种方式添加其他AWS凭据：

- 您可以向现有Connector添加AWS凭据
- 您可以将AWS凭据直接添加到BlueXP

有关更多详细信息、请查看以下各节。

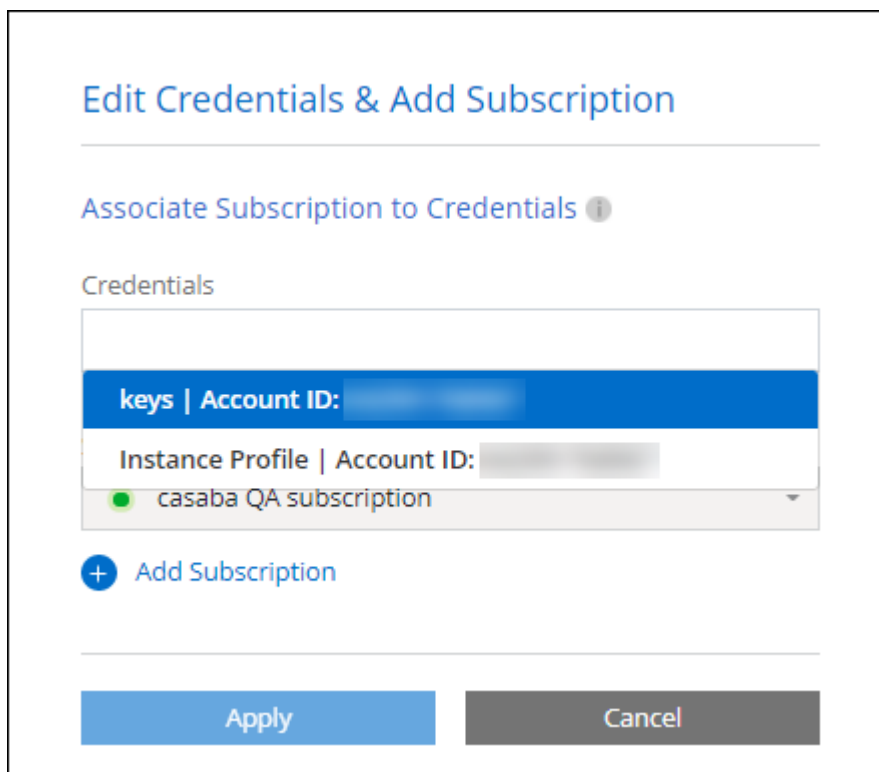
### 将 **AWS** 凭据添加到现有 **Connector**

如果要将BlueXP与其他AWS帐户结合使用、则可以为IAM用户或可信帐户中某个角色的ARN提供AWS密钥。下图显示了另外两个帐户，一个通过可信帐户中的 IAM 角色提供权限，另一个通过 IAM 用户的 AWS 密钥提供权限：



然后、您可以通过指定IAM角色的Amazon资源名称(ARN)或IAM用户的AWS密钥将帐户凭据添加到BlueXP。

例如、在创建新的Cloud Volumes ONTAP 工作环境时、您可以在凭据之间切换：



"了解如何向现有Connector添加AWS凭据。"

### 将**AWS**凭据直接添加到**BlueXP**

向BlueXP添加新的AWS凭据可提供创建和管理适用于ONTAP 的FSX工作环境或创建连接器所需的权限。

- "了解如何将AWS凭据添加到适用于Amazon FSX for ONTAP 的BlueXP中"
- "了解如何向BlueXP添加AWS凭据以创建Connector"

## 凭据和商城订阅

您添加到连接器的凭据必须与AWS Marketplace订阅相关联、以便您可以按小时费率(PAYGO)或通过年度合同支付Cloud Volumes ONTAP费用、并使用其他BlueXP服务。

["了解如何关联AWS订阅"](#)。

请注意以下有关AWS凭据和Marketplace订阅的信息：

- 您只能将一个AWS Marketplace订阅与一组AWS凭据相关联
- 您可以将现有商城订阅替换为新订阅

## 常见问题解答

以下问题与凭据和订阅相关。

如何安全地轮换 **AWS** 凭据？

如上文各节所述、BlueXP支持您通过几种方式提供AWS凭据：与连接器实例关联的IAM角色、在受信任帐户中承担IAM角色或提供AWS访问密钥。

对于前两个选项、BlueXP使用AWS安全令牌服务获取持续轮换的临时凭据。这是最佳实践—它是自动的，安全的。

如果您为BlueXP提供了AWS访问密钥、则应定期在BlueXP中更新这些密钥以轮换使用。这是一个完全手动的过程。

我是否可以更改适用于**Cloud Volumes ONTAP**工作环境的**AWS Marketplace**订阅？

可以。当您更改与一组凭据关联的AWS Marketplace订阅时、所有现有和新的Cloud Volumes ONTAP工作环境都将按新订阅收费。

["了解如何关联AWS订阅"](#)。

我是否可以添加多个**AWS**凭据、每个凭据都有不同的商城订阅？

属于同一AWS帐户的所有AWS凭据都将与同一AWS Marketplace订阅相关联。

如果您有多个属于不同AWS帐户的AWS凭据、则这些凭据可以与同一AWS Marketplace订阅或不同订阅相关联。

我是否可以将现有**Cloud Volumes ONTAP**工作环境移至其他**AWS**帐户？

不可以、不能将与您的Cloud Volumes ONTAP工作环境关联的AWS资源移动到其他AWS帐户。

凭据如何用于市场部署和内置部署？

以上各节介绍了BlueXP中建议的Connector部署方法。您还可以从AWS Marketplace在AWS中部署Connector、并在您自己的Linux主机上手动安装Connector软件。

如果您使用 Marketplace ，则会以相同方式提供权限。您只需手动创建和设置 IAM 角色，然后为任何其他帐户提供权限即可。

对于内部部署、您无法为BlueXP系统设置IAM角色、但可以使用AWS访问密钥提供权限。

要了解如何设置权限、请参见以下页面：

- 标准模式
  - ["为AWS Marketplace部署设置权限"](#)
  - ["设置对内置部署的权限"](#)
- ["设置受限模式的权限"](#)
- ["设置私有模式的权限"](#)

## 管理BlueXP的AWS凭据和市场订阅

添加和管理AWS凭据、以便BlueXP拥有在AWS帐户中部署和管理云资源所需的权限。如果您管理多个AWS Marketplace订阅、则可以从"凭据"页面将其中每个订阅分配给不同的AWS凭据。

### 概述

您可以将AWS凭据添加到现有Connector或直接添加到BlueXP：

- 向现有Connector添加其他AWS凭据

将AWS凭据添加到现有连接器可提供在公有云环境中管理资源和进程所需的权限。 [了解如何将AWS凭据添加到Connector。](#)

- 将AWS凭据添加到BlueXP以创建Connector

向BlueXP添加新的AWS凭据可为BlueXP提供创建Connector所需的权限。 [了解如何向BlueXP添加AWS凭据。](#)

- 将AWS凭据添加到BlueXP for FSX for ONTAP

向BlueXP添加新的AWS凭据可为BlueXP提供创建和管理适用于ONTAP的FSX所需的权限。 ["了解如何为适用于ONTAP的FSX设置权限"](#)

### 如何轮换凭据

通过BlueXP、您可以通过以下几种方式提供AWS凭据：与Connector实例关联的IAM角色、在可信帐户中担任IAM角色或提供AWS访问密钥。 ["详细了解AWS凭据和权限"](#)。

对于前两个选项、BlueXP使用AWS安全令牌服务获取持续轮换的临时凭据。此过程是最佳实践，因为它是自动的，并且安全。

如果您为BlueXP提供了AWS访问密钥、则应定期在BlueXP中更新这些密钥以轮换使用。这是一个完全手动的过程。

## 向Connector添加其他凭据

将其他AWS凭据添加到Connector、以便其拥有管理公共云环境中的资源和流程所需的权限。您可以在其他帐户中提供 IAM 角色的 ARN ，也可以提供 AWS 访问密钥。

如果您刚刚开始使用BlueXP、"[了解BlueXP如何使用AWS凭据和权限](#)"。

### 授予权限

在将AWS凭据添加到Connector之前、您需要提供所需的权限。通过这些权限、BlueXP可以管理该AWS帐户中的资源和进程。如何提供权限取决于您是要为BlueXP提供受信任帐户或AWS密钥中某个角色的ARN。



如果您从BlueXP部署了Connector、则BlueXP会自动为部署此Connector的帐户添加AWS凭据。如果您从AWS Marketplace部署了Connector或在现有系统上手动安装了Connector软件、则不会添加此初始帐户。"[了解 AWS 凭据和权限](#)"。

- 选项 \*
- [在另一个帐户中担任 IAM 角色以授予权限](#)
- [通过提供 AWS 密钥授予权限](#)

在另一个帐户中担任 **IAM** 角色以授予权限

您可以使用 IAM 角色在部署 Connector 实例的源 AWS 帐户与其他 AWS 帐户之间设置信任关系。然后、您可以为BlueXP提供可信帐户中IAM角色的ARN。

如果Connector安装在内部、则无法使用此身份验证方法。您必须使用AWS密钥。

### 步骤

1. 转到要为Connector提供权限的目标帐户中的IAM控制台。
2. 在访问管理下、选择\*角色>创建角色\*、然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \* 。
- 选择 \* 其他 AWS 帐户 \* ，然后输入 Connector 实例所在帐户的 ID 。
- 通过复制和粘贴内容来创建所需的策略 "[Connector的IAM策略](#)"。

3. 复制IAM角色的角色ARN、以便稍后将其粘贴到BlueXP中。

### 结果

现在，此帐户具有所需权限。 [现在，您可以将凭据添加到 Connector。](#)

### 通过提供 **AWS** 密钥授予权限

如果要为BlueXP为IAM用户提供AWS密钥、则需要向该用户授予所需的权限。BlueXP IAM策略定义了允许BlueXP使用的AWS操作和资源。

如果Connector安装在内部、则必须使用此身份验证方法。您不能使用IAM角色。

## 步骤

1. 在IAM控制台中、通过复制和粘贴内容来创建策略 "[Connector的IAM策略](#)"。

["AWS 文档：创建 IAM 策略"](#)

2. 将策略附加到IAM角色或IAM用户。
  - ["AWS 文档：创建 IAM 角色"](#)
  - ["AWS 文档：添加和删除 IAM 策略"](#)

## 结果

现在，此帐户具有所需权限。 [现在，您可以将凭据添加到 Connector。](#)

## 添加凭据

在为 AWS 帐户提供所需权限后，您可以将该帐户的凭据添加到现有 Connector 。这样，您就可以使用同一个连接器在该帐户中启动 Cloud Volumes ONTAP 系统了。

## 开始之前

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟的时间才能使用这些凭据。请等待几分钟、然后再将凭据添加到BlueXP。

## 步骤

1. 确保当前在BlueXP中选择了正确的Connector。
2. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。



3. 在\*帐户凭据\*页面上、选择\*添加凭据\*、然后按照向导中的步骤进行操作。
  - a. \* 凭据位置 \*：选择 \* Amazon Web Services > Connector\* 。
  - b. \* 定义凭据 \*：提供可信 IAM 角色的 ARN （ Amazon 资源名称），或者输入 AWS 访问密钥和机密密钥。
  - c. \* 市场订阅 \*：通过立即订阅或选择现有订阅，将市场订阅与这些凭据相关联。

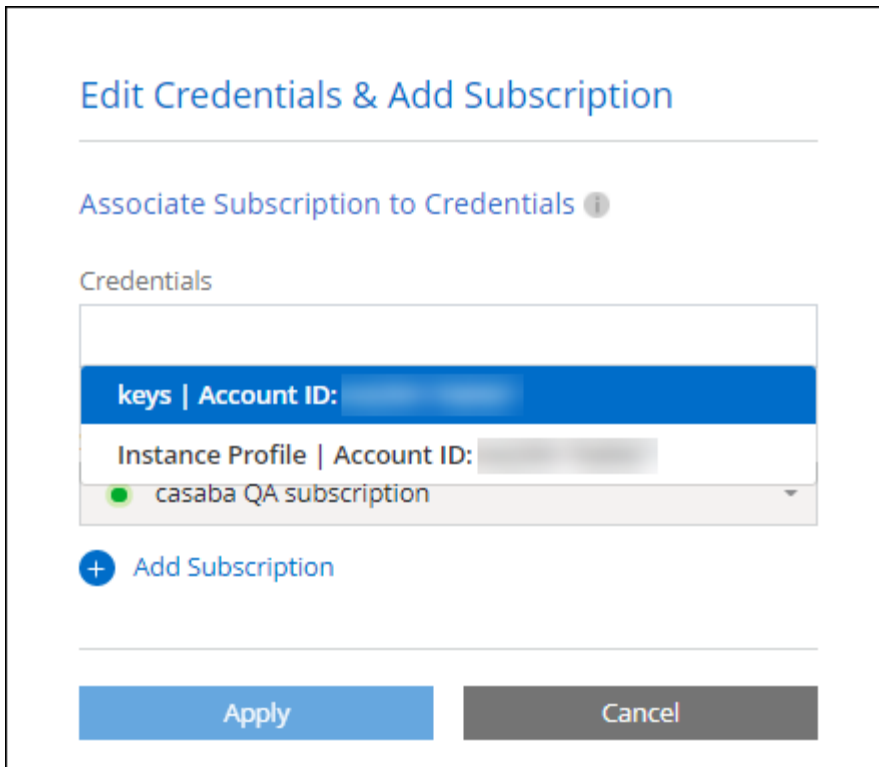
要按小时费率(PAYGO)或按年度合同支付BlueXP服务费用、AWS凭据必须与AWS Marketplace订阅相关联。

- d. 查看：确认有关新凭据的详细信息、然后选择\*添加\*。

## 结果

现在，在创建新的工作环境时，您可以从 " 详细信息和凭据 " 页面切换到另一组凭据：





## 向BlueXP添加用于创建Connector的凭据

通过提供IAM角色的ARN、为BlueXP提供创建Connector所需的权限、将AWS凭据添加到BlueXP。您可以在创建新的Connector时选择这些凭据。

### 设置 IAM 角色

设置一个IAM角色、使BlueXP SaaS层能够承担此角色。

#### 步骤

1. 转到目标帐户中的 IAM 控制台。
2. 在访问管理下、选择\*角色>创建角色\*、然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \*。
- 选择\*其他AWS帐户\*、然后输入BlueXP SaaS的ID：952013314444
- 创建包含创建Connector所需权限的策略。
  - "查看适用于 ONTAP 的 FSX 所需的权限"
  - "查看连接器部署策略"

3. 复制IAM角色的角色ARN、以便在下一步将其粘贴到BlueXP中。

#### 结果

IAM 角色现在具有所需的权限。现在、您可以将其添加到BlueXP中。

## 添加凭据

为IAM角色提供所需权限后、将角色ARN添加到BlueXP中。

### 开始之前

如果您刚刚创建了 IAM 角色，则可能需要几分钟的时间，直到这些角色可用为止。请等待几分钟、然后再将凭据添加到BlueXP。

### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。



2. 在\*帐户凭据\*页面上、选择\*添加凭据\*、然后按照向导中的步骤进行操作。
  - a. 凭据位置：选择\* Amazon Web Services > BlueX\*。
  - b. \* 定义凭据 \*：提供 IAM 角色的 ARN （ Amazon 资源名称）。
  - c. 查看：确认有关新凭据的详细信息、然后选择\*添加\*。

### 结果

现在、您可以在创建新Connector时使用这些凭据。

## 向BlueXP for Amazon FSX for ONTAP 添加凭据

有关详细信息，请参见 ["适用于ONTAP 的Amazon FSX的BlueXP文档"](#)

## 关联 AWS 订阅

将AWS凭据添加到BlueXP后、您可以将AWS Marketplace订阅与这些凭据相关联。通过订阅、您可以按每小时费率(PAYGO)或使用年度合同为Cloud Volumes ONTAP 付费、并使用其他BlueXP服务。

在以下两种情况下、您可能在将凭据添加到BlueXP后关联AWS Marketplace订阅：

- 最初将凭据添加到BlueXP时、您未关联订阅。
- 您希望更改与AWS凭据关联的AWS Marketplace订阅。

将当前市场订阅替换为新订阅会改变任何现有Cloud Volumes ONTAP工作环境和所有新工作环境的市场订阅。

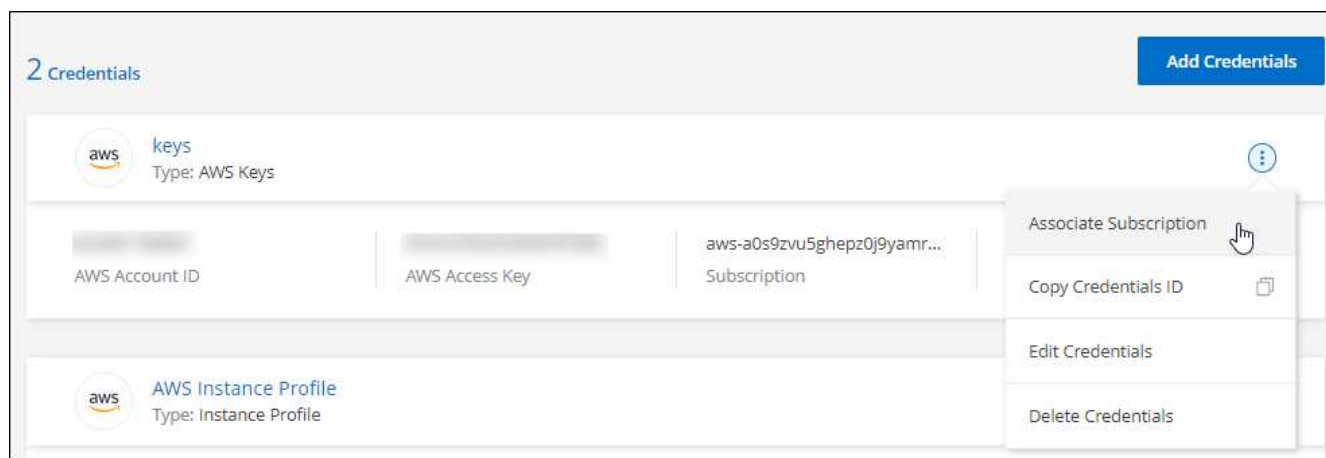
### 开始之前

您需要先创建Connector、然后才能更改BlueXP设置。 ["了解如何创建 Connector"](#)。

### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。
2. 选择一组凭据的操作菜单，然后选择\*关联订阅\*。

您必须选择与连接器关联的凭据。您不能将商城订阅与BlueXP关联的凭据关联。



3. 要将凭据与现有订阅关联、请从下拉列表中选择此订阅、然后选择\*关联\*。
4. 要将凭据与新订阅关联、请选择\*添加订阅>继续\*、然后按照AWS Marketplace中的步骤进行操作：
  - a. 选择\*查看购买选项\*。
  - b. 选择\*订阅\*。
  - c. 选择\*设置您的帐户\*。

您将重定向到BlueXP网站。

- d. 在\*订阅分配\*页面中：

- 选择要与此订阅关联的BlueXP帐户。
- 在\*替换现有订阅\*字段中、选择是否要将一个帐户的现有订阅自动替换为此新订阅。

此新订阅将取代帐户中所有凭据的现有订阅。如果一组凭据从未与订阅关联、则此新订阅将不会与这些凭据关联。

对于所有其他帐户、您需要重复上述步骤来手动关联订阅。

- 选择 \* 保存 \*。

以下视频显示了从AWS Marketplace订阅的步骤：

### [从AWS Marketplace订阅BlueXP](#)

## 将现有订阅与您的帐户关联

从AWS Marketplace订阅BlueXP后、此过程的最后一步是将此订阅与BlueXP网站上的BlueXP帐户相关联。如果您未完成此步骤、则无法通过BlueXP帐户使用订阅。

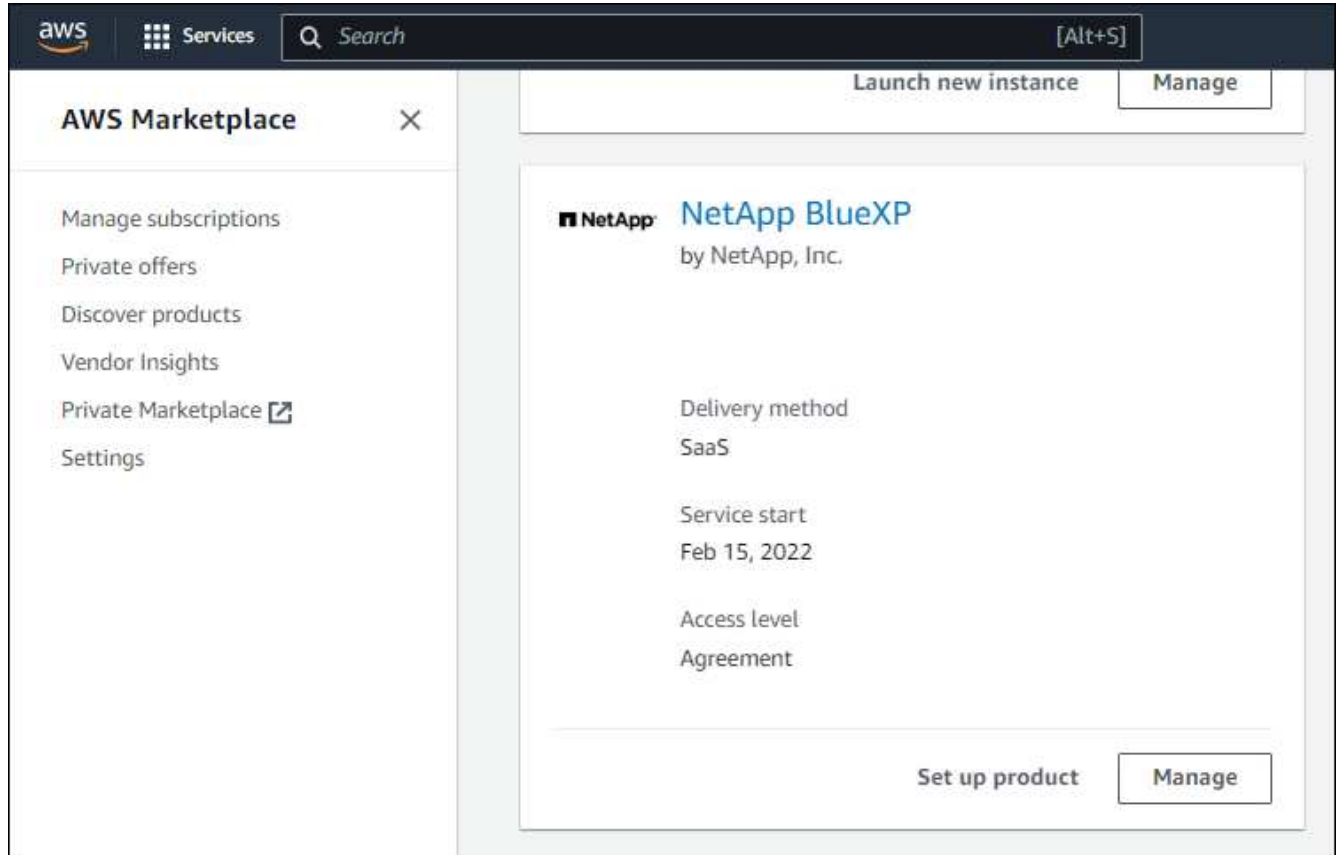
如果您从AWS Marketplace订阅了BlueXP、但错过了将订阅与您的帐户关联的步骤、请按照以下步骤进行操作。

步骤

1. 转到BlueXP数字钱包、确认您的订阅未与BlueXP帐户关联。
  - a. 从BlueXP导航菜单中、选择\*监管>数字电子钱包\*。
  - b. 选择\*订阅\*。
  - c. 确认未显示您的BlueXP订阅。

您将只看到与当前正在查看的帐户关联的订阅。如果您看不到您的订阅、请继续执行以下步骤。

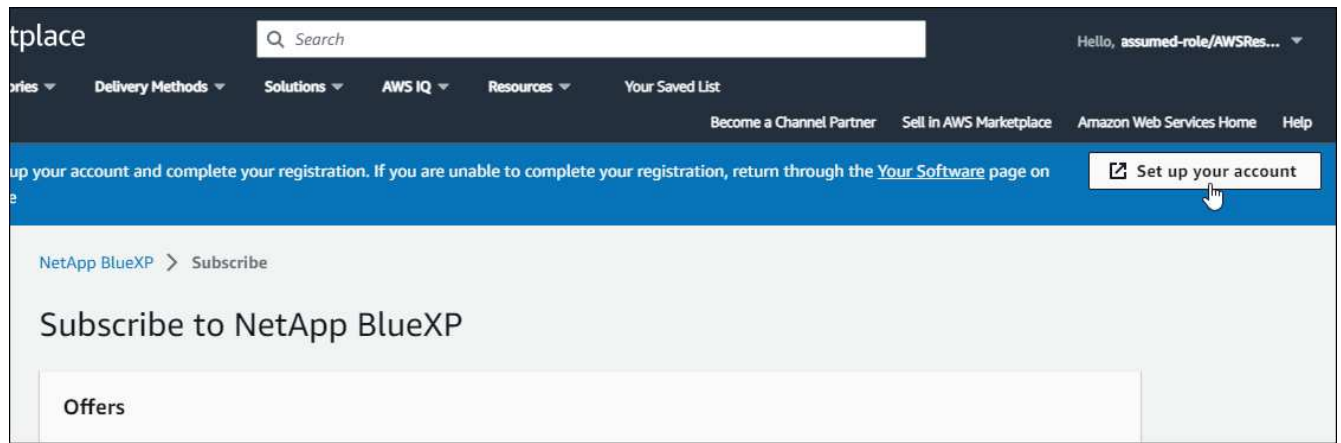
2. 登录到AWS控制台并导航到\*AWS Marketplace订阅\*。
3. 查找NetApp BlueXP订阅。



4. 选择\*设置产品\*。

订阅服务页面应加载到新的浏览器选项卡或窗口中。

5. 选择\*设置您的帐户\*。



netapp.com上的\*订阅分配\*页面应加载到新的浏览器选项卡或窗口中。

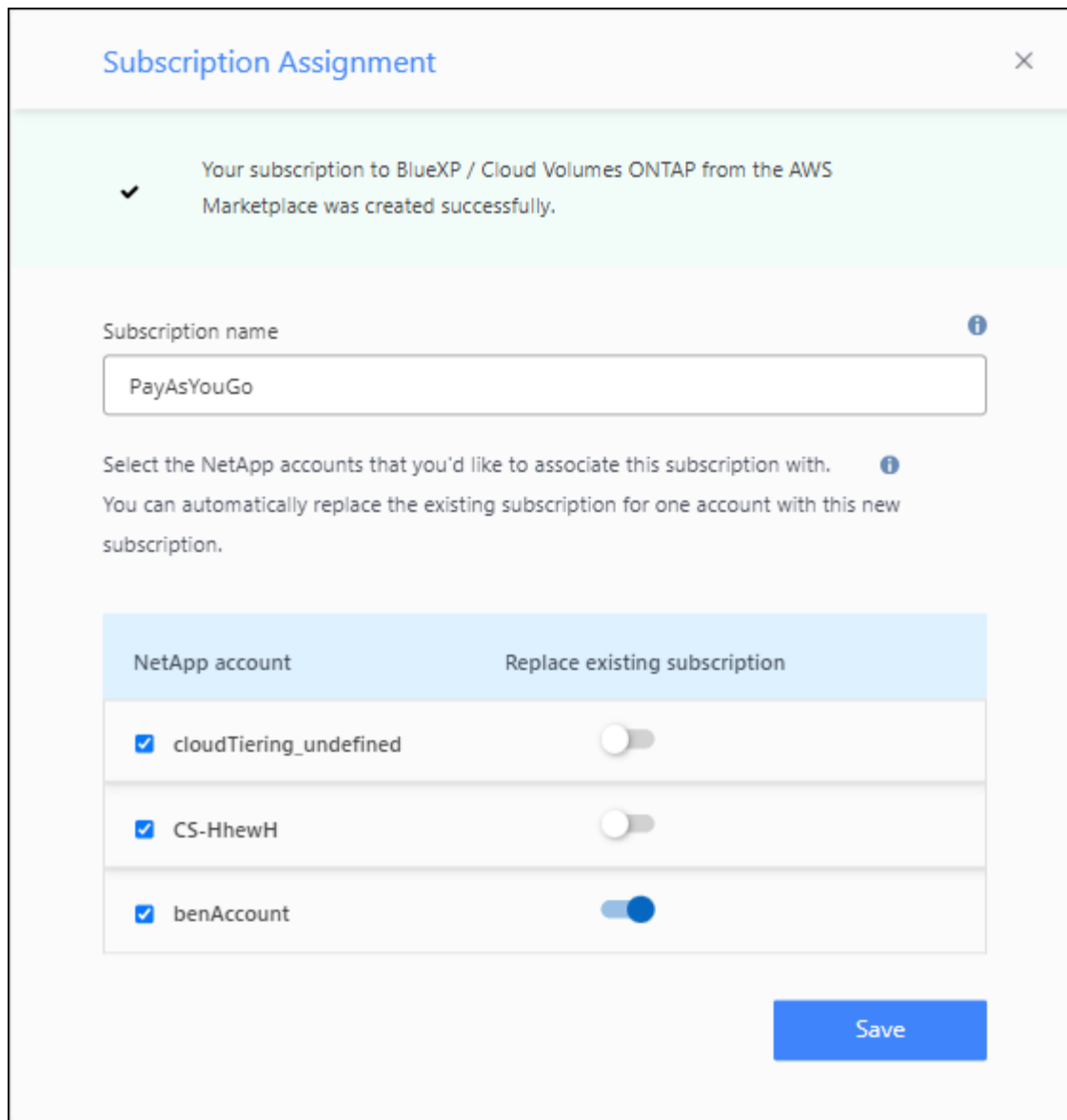
请注意、系统可能会提示您先登录BlueXP。

6. 在\*订阅分配\*页面中：

- 选择要与此订阅关联的BlueXP帐户。
- 在\*替换现有订阅\*字段中、选择是否要将一个帐户的现有订阅自动替换为此新订阅。

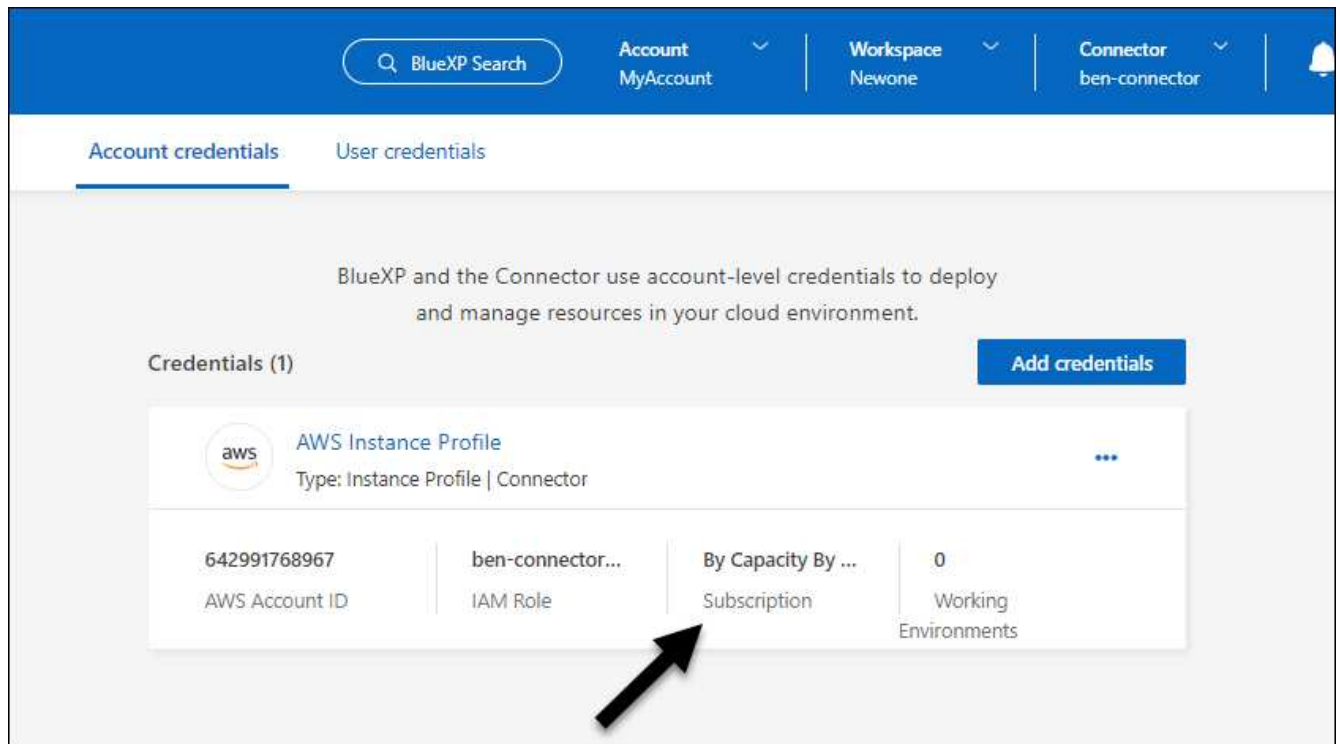
此新订阅将取代帐户中所有凭据的现有订阅。如果一组凭据从未与订阅关联、则此新订阅将不会与这些凭据关联。

对于所有其他帐户、您需要重复上述步骤来手动关联订阅。



7. 转到BlueXP数字钱包、确认订阅与您的BlueXP帐户关联。
  - a. 从BlueXP导航菜单中、选择\*监管>数字电子钱包\*。
  - b. 选择\*订阅\*。
  - c. 验证是否显示您的BlueXP订阅。
8. 确认订阅与您的AWS凭据关联。
  - a. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。
  - b. 在\*帐户凭据\*页面上、验证订阅是否与您的AWS凭据关联。

下面是一个示例。



## 编辑凭据

通过更改帐户类型(AWS密钥或承担角色)、编辑名称或更新凭据本身(密钥或角色ARN)、在BlueXP中编辑AWS凭据。



您不能编辑与 Connector 实例关联的实例配置文件的凭据。

### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。
2. 在\*帐户凭据\*页面上、选择一组凭据的操作菜单、然后选择\*编辑凭据\*。
3. 进行所需更改、然后选择\*应用\*。

## 删除凭据

如果您不再需要一组凭据、可以从BlueXP中删除这些凭据。您只能删除与工作环境无关的凭据。



您不能删除与 Connector 实例关联的实例配置文件的凭据。

### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。
2. 在\*帐户凭据\*页面上、选择一组凭据的操作菜单、然后选择\*删除凭据\*。
3. 选择\*删除\*进行确认。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。