



# 身份和访问管理

## BlueXP setup and administration

NetApp  
December 16, 2024

# 目录

|                                |    |
|--------------------------------|----|
| 身份和访问管理 .....                  | 1  |
| 了解BlueXP 身份和访问管理 .....         | 1  |
| 开始使用BlueXP 身份和访问管理 .....       | 8  |
| 使用文件夹和项目组织BlueXP IAM中的资源 ..... | 9  |
| 添加BlueXP IAM成员并管理其权限 .....     | 15 |
| 管理BlueXP 组织中的资源层次结构 .....      | 22 |
| 将BlueXP 连接器与其他文件夹和项目相关联 .....  | 24 |
| 在BlueXP 组织、项目和连接器之间切换 .....    | 25 |
| 重命名BlueXP 组织 .....             | 28 |
| 通过BlueXP 时间表监控或审核IAM活动 .....   | 28 |
| 预定义的BlueXP IAM角色和权限 .....      | 29 |

# 身份和访问管理

## 了解BlueXP 身份和访问管理

通过BlueXP 身份和访问管理(IAM)、您可以组织和控制对NetApp资源的访问。您可以根据组织的层次结构来组织资源。例如、您可以按地理位置、站点或业务单位来组织资源。然后、您可以将权限分配给层次结构特定部分的成员、从而阻止访问层次结构其他部分中的资源。

BlueXP IAM取代并增强了BlueXP 帐户先前提提供的功能。["详细了解BlueXP IAM的推出"\(英文\)](#)

在标准模式下使用BlueXP 时、支持BlueXP IAM。如果在受限模式或私用模式下使用BlueXP 、则使用BlueXP \_account\_来管理用户和资源。

- ["了解有关BlueXP帐户的信息"](#)
- ["了解BlueXP部署模式"](#)

## BlueXP IAM的工作原理

通过BlueXP IAM、您可以通过定义哪些成员对组织层次结构的特定部分具有权限来授予对组织资源的访问权限。例如、成员可以对具有五个关联资源的项目拥有项目管理员权限。

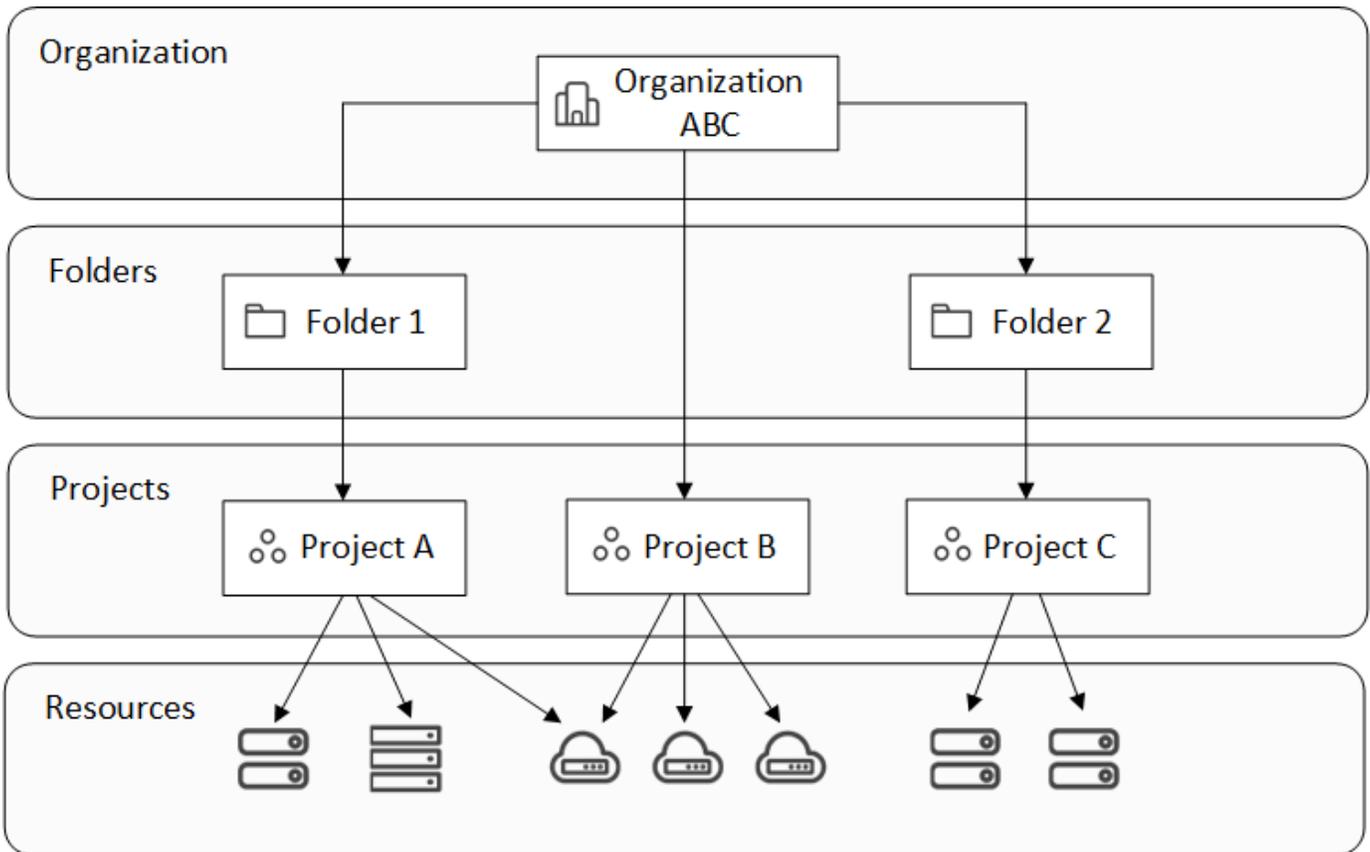
使用BlueXP IAM时、您将管理以下组件：

- 组织
- 文件夹
- 项目
- 资源
- 成员
- 角色和权限
- 连接器

BlueXP 资源按分层结构进行组织：

- 组织是层次结构的顶端。
- 文件夹是组织或其他文件夹的子文件夹。
- 项目是组织或文件夹的子项目。
- 资源与一个或多个文件夹或项目相关联。

下图从基本层面展示了此层次结构。



## 组织

一个组织是BlueXP IAM系统的顶级组织、通常代表您的公司。您的组织由文件夹、项目、成员、角色和资源组成。连接器与组织中的特定项目相关联。

注册BlueXP 时、系统会提示您创建新组织。

## 文件夹

使用 `FOLDER` 可以将相关项目分组在一起、并将其与组织中的其他项目分开。例如、文件夹可能表示地理位置(欧盟或美国东部)、站点(伦敦或多伦多)或业务单位(工程或市场营销)。

文件夹可以包含项目、其他文件夹或两者的组合。

您不需要创建文件夹。它们是可选的。

## 项目

`_project_` 表示BlueXP 中的一个工作空间、组织成员可以从BlueXP 画布访问此工作空间来管理资源。例如、项目可以包括Cloud Volumes ONTAP系统、内部ONTAP集群或FSx for ONTAP文件系统。

一个组织可以有一个或多个项目。项目可以直接驻留在组织的下面或文件夹中。

## 资源

资源是您在BlueXP 中创建或发现的工作环境。

创建或发现资源时、该资源将与当前选定的项目相关联。这可能是唯一要与此资源关联的项目。但是、您可以选择将资源与组织中的其他项目相关联。

例如、您可以将一个Cloud Volumes ONTAP系统与一个其他项目或组织中的所有项目相关联。如何关联资源取决于组织的需求。



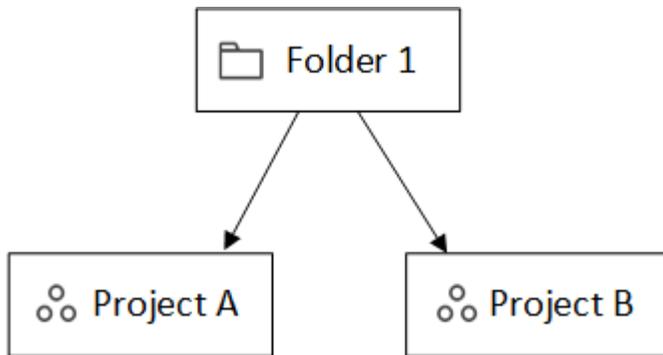
您还可以将Connector与组织中的其他文件夹或项目相关联。[详细了解如何将连接器与BlueXP IAM结合使用\(英文\)](#)

何时将资源与文件夹相关联

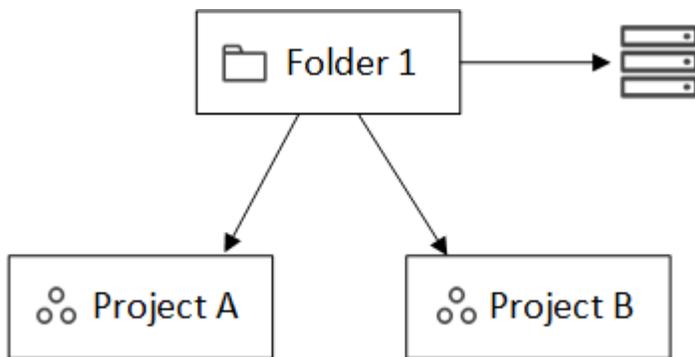
您还可以选择将资源与文件夹相关联、但这是可选操作、可满足特定使用情形的需求。

Organization admin\_可以将资源与文件夹相关联、以便\_Folder或项目admin\_可以将该资源与驻留在该文件夹中的相应项目相关联。

例如、假设您有一个包含两个项目的文件夹：

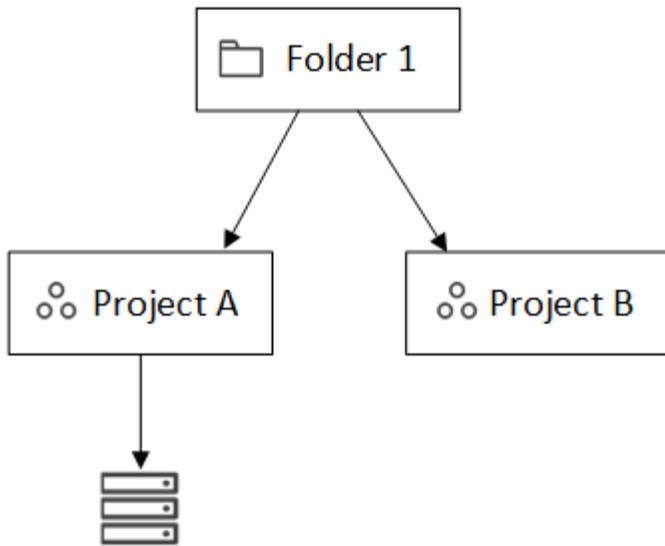


Organization admin\_可以将资源与文件夹相关联：



将资源与文件夹关联不会自动使该资源可从文件夹中的所有项目访问。但是、文件夹或项目管理可以决定应将该资源提供给哪些项目。做出此决定后、管理员可以将该资源与正确的项目相关联。

在此示例中、管理员将资源与Project A相关联：



拥有项目A权限的成员现在可以访问该资源。

## 成员

您的组织成员是用户帐户或服务帐户。服务帐户通常由应用程序使用来完成指定的任务、而无需人为干预。

一个组织至少有一个具有 `_Organization admin_` 角色的用户(系统会自动为创建该组织的用户分配此角色)。您可以向组织添加其他成员、并在资源层次结构的不同级别分配不同的权限。

## 角色和权限

在BlueXP IAM中、您不会直接向组织成员授予权限。而是为每个成员授予一个角色。角色包含一组权限、使成员能够在资源层次结构的特定级别执行特定操作。

通过在资源层次结构的特定部分提供权限、您可以将访问权限限制为只能访问成员完成其任务所需的资源。

您可以在其中分配层次结构中的角色

将成员与角色关联时、需要选择整个组织、特定文件夹或特定项目。您选择的角色会为成员授予对层次结构选定部分中资源的权限。

## 角色继承

分配角色时、该角色将继承到组织层次结构中：

### 组织

您在组织级别授予的角色将由组织中的所有文件夹、项目和资源继承。这意味着该成员对组织中的所有内容都有权限。

### 文件夹

文件夹中的所有文件夹、项目和资源都会继承您在文件夹级别授予的角色。

例如、如果您在文件夹级别分配了一个角色、并且该文件夹包含三个项目、则该成员将有权访问这三个项目以及任何关联资源。

## 项目

您在项目级别授予的角色将由与该项目关联的所有资源继承。

## 多个角色

您可以在组织层次结构的不同级别为每个组织成员分配一个角色。它可以是同一个角色、也可以是不同的角色。例如、您可以为项目1和项目2分配成员角色A。或者、您也可以为项目1分配成员角色A、为项目2分配角色B。

## 预定义角色

BlueXP 支持多个预定义角色、您可以将这些角色分配给组织的成员。

["了解IAM预定义角色"\(英文\)](#)

## 连接器

当 `_Organization admin_` 创建Connector时，BlueXP 会自动将该Connector与组织和当前选定的项目相关联。`_Organization admin_`可自动从组织中的任何位置访问该Connector。但是、如果您的组织中有其他成员具有不同的角色、这些成员只能从创建连接器的项目访问该连接器、除非您将该连接器与其他项目相关联。

在以下情况下、您可能需要使Connector可用于其他项目：

- 您希望允许组织中的成员使用现有Connector在另一个项目中创建或发现其他工作环境
- 您已将现有资源与另一个项目相关联、该资源由Connector管理

如果使用BlueXP 连接器发现了与其他项目关联的资源、则还需要将该连接器与该资源现在关联的项目关联。否则、没有 `_Organization admin_` 角色的成员将无法从BlueXP 画布访问连接器及其关联的资源。

您可以从BlueXP IAM中的\*Connectors \*页面创建关联：

- 将连接器与项目相关联

将连接器与项目关联后、可以在查看项目时从BlueXP 画布访问该连接器。

- 将连接器与文件夹相关联

将连接器与文件夹关联不会自动使该连接器可从文件夹中的所有项目访问。在将某个连接器与该特定项目关联之前、组织成员无法从该项目访问该连接器。

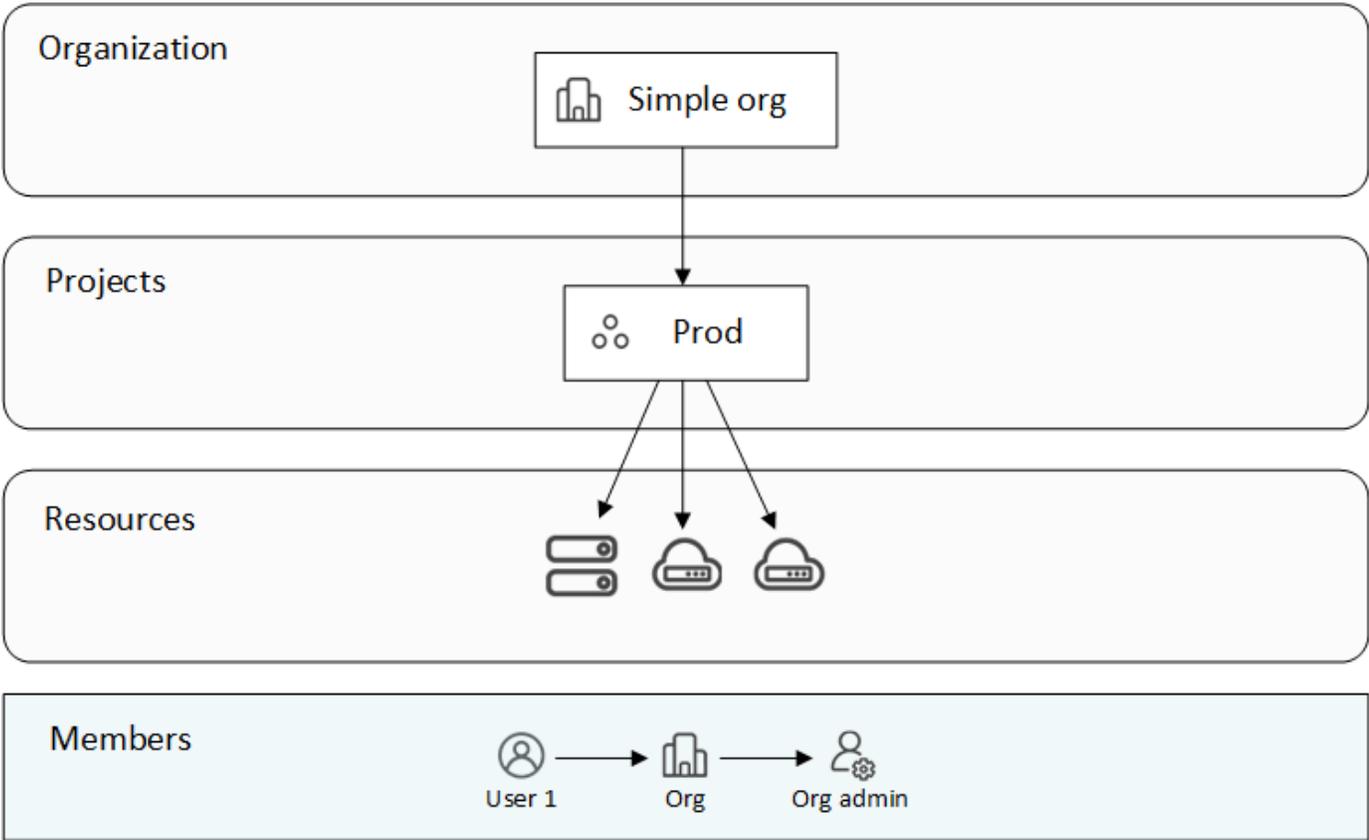
`_Organization admin_`可能会将Connector与文件夹相关联、以便 `_Folder`或项目 `admin_`可以决定将该Connector与文件夹中的相应项目相关联。

## IAM示例

以下示例显示了如何设置您的组织。

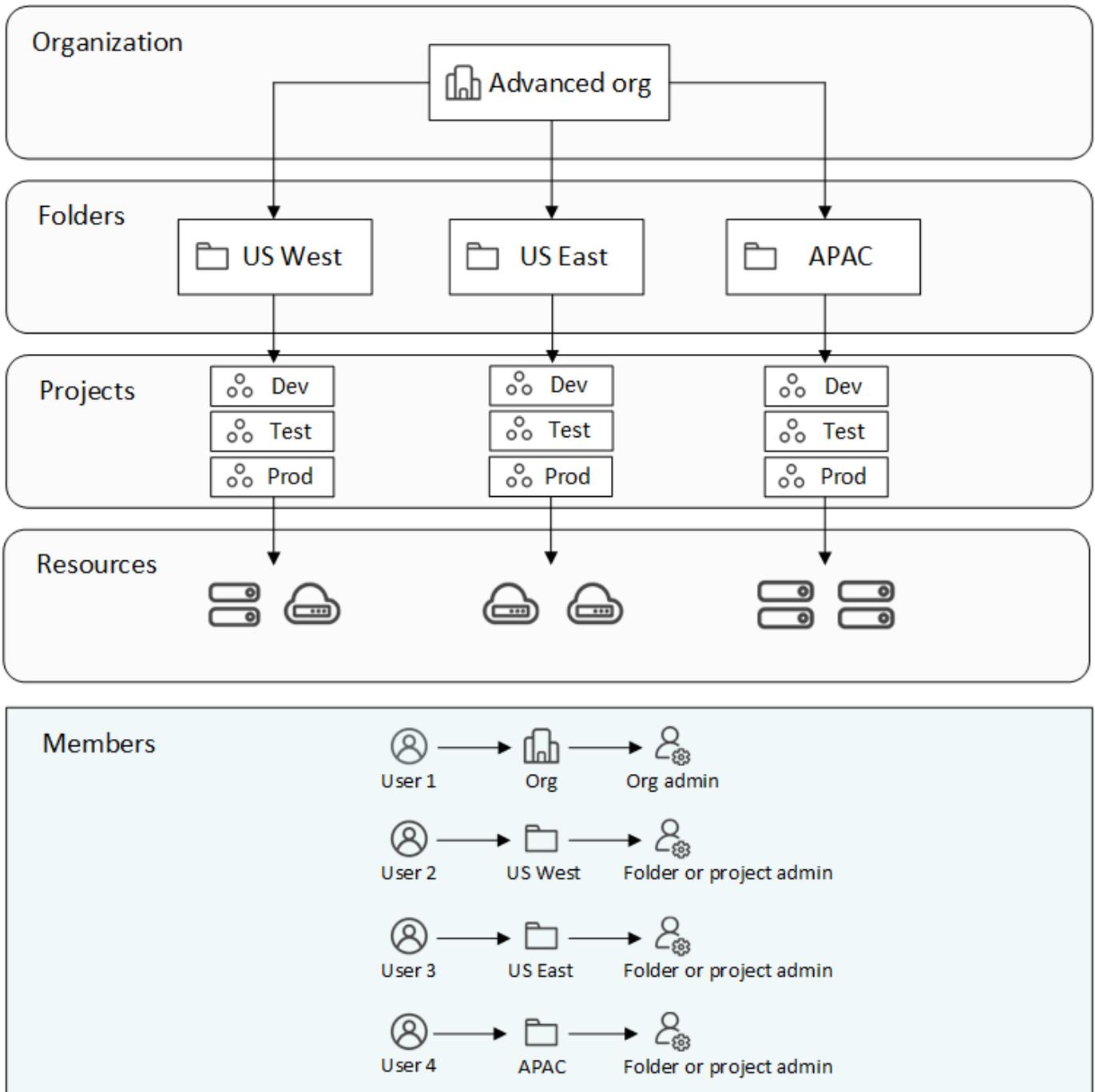
### 简单的组织

下图显示了一个使用默认项目而不使用文件夹的组织的简单示例。一个成员负责管理整个组织。



高级组织

下图显示了一个使用文件夹组织业务中每个地理位置的项目的组织。每个项目都有自己的一组关联资源。成员包括组织管理员和组织中每个文件夹的管理员。



## 您可以使用BlueXP IAM执行哪些操作

以下示例介绍了如何使用IAM管理BlueXP 组织：

- 为特定成员授予特定角色、使其只能完成所需的任务。
- 修改成员权限、因为他们移动了部门或承担了其他职责。
- 删除离开公司的用户。
- 将文件夹或项目添加到层次结构中、因为新业务单位已添加NetApp存储。
- 将资源与另一个项目相关联、因为该资源具有其他团队可以利用的容量。
- 查看成员可以访问的资源。

- 查看与特定项目关联的成员和资源。

## 下一步行动

- ["开始使用BlueXP IAM"](#)
- ["使用文件夹和项目组织BlueXP 中的资源"](#)
- ["管理BlueXP 成员及其权限"](#)
- ["管理BlueXP 组织中的资源层次结构"](#)
- ["将接头与文件夹和项目相关联"](#)
- ["在BlueXP 项目和组织之间切换"](#)
- ["重命名BlueXP 组织"](#)
- ["监控或审核IAM活动"](#)
- ["预定义的BlueXP IAM角色"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 开始使用BlueXP 身份和访问管理

注册BlueXP 时、系统会提示您创建新组织。该组织包括一个成员(组织管理员)和一个默认项目。要设置BlueXP 身份和访问管理(IAM)以满足您的业务需求、您需要自定义组织的层次结构、添加其他成员、添加或发现资源、并在整个层次结构中关联这些资源。

您必须具有\*组织管理员\*权限才能从BlueXP IAM管理整个组织。如果您拥有\*文件夹或项目管理员\*权限，则只能管理您拥有权限的文件夹和项目。

按照以下步骤设置新的BlueXP 组织。根据组织的需求、完成这些步骤的顺序可能有所不同。

1

编辑默认项目或添加到组织的层次结构中

您只需使用默认项目、也可以创建与业务层次结构匹配的其他项目和文件夹。

["了解如何使用文件夹和项目组织资源"\(英文\)](#)

2

将成员与您的组织关联起来

如果您的企业中有多个人需要从BlueXP 访问和管理资源、您需要将其用户帐户与您的组织关联起来、并在资源层次结构中提供适当的权限。您还可以选择向组织添加服务帐户。

["了解如何管理成员及其权限"\(英文\)](#)

3

添加或发现资源

在BlueXP 中将资源添加或发现为\_working workenapp环境\_。工作环境表示组织成员从项目中管理的存储系统。例如、Cloud Volumes ONTAP系统或内部ONTAP集群。

了解如何从BlueXP 画布创建或发现资源：

- ["适用于 NetApp ONTAP 的 Amazon FSX"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes ONTAP"](#)
- ["E系列系统"](#)
- ["内部 ONTAP 集群"](#)
- ["StorageGRID"](#)

## 4

### 将资源与其他项目相关联

在BlueXP 中创建或发现资源时、该资源将自动与创建或发现工作环境时选择的项目相关联。如果要使该资源可供组织中的其他项目使用、则需要在它们之间创建关联。如果资源由连接器管理，则还需要在项目和关联连接器之间创建关联。

- ["了解如何管理组织的资源层次结构"\(英文\)](#)
- ["了解如何将Connector与文件夹或项目相关联"\(英文\)](#)

#### 相关信息

- ["了解BlueXP 身份和访问管理"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 使用文件夹和项目组织BlueXP IAM中的资源

通过BlueXP 身份和访问管理(IAM)、您可以使用项目和文件夹来组织NetApp资源。*project\_*表示BlueXP 中的一个工作空间、组织成员可以访问该工作空间来管理 *\_Res*型(例如、Cloud Volumes ONTAP系统)。一个 *\_FOLDER\_* 将相关项目分组在一起。将资源组织到文件夹和项目中之后、您可以通过为组织成员提供对特定文件夹和项目的权限来授予对资源的粒度访问权限。

### 添加文件夹或项目

创建BlueXP 组织时、它包含一个项目。您可以创建其他项目来管理组织的资源。您可以选择创建文件夹以将相关项目分组在一起。

#### 关于此任务

您的组织的层次结构的深度可向下划分为7个级别。因此、您可以创建6个级别的嵌套文件夹。最后一个嵌套文件夹可以包括层次结构第七级的项目。

下图说明了组织层次结构的最大深度：

| Name             | ↑   |
|------------------|-----|
| ^ MyOrganization | ... |
| ^ Folder1        | ... |
| ^ Folder2        | ... |
| ^ Folder3        | ... |
| ^ Folder4        | ... |
| ^ Folder5        | ... |
| ^ Folder6        | ... |
| Project          | ... |

### 步骤

1. 在BlueXP 控制台的右上角，选择  > \*身份和访问管理\*。
2. 从“组织”页中，选择“添加文件夹或项目”。
3. 选择\*文件夹\*或\*项目\*。
4. 提供有关文件夹或项目的详细信息：

- 名称和位置：输入名称并在层次结构中为文件夹或项目选择一个位置。文件夹或项目可以直接位于组织的下方或文件夹内。
- 资源：选择要与此文件夹或项目关联的资源。

您只能从与文件夹或项目的父级关联的资源中进行选择。如果父级是组织、则可以从组织中的任何资源中进行选择。如果父级是文件夹、则只能从与该文件夹关联的资源中进行选择。

["了解何时可以将资源与文件夹相关联"\(英文\)](#)

- 访问：根据您的资源层次结构中已定义的现有权限查看将有权访问文件夹或项目的成员。

如果需要，请选择\*添加成员\*以指定应具有文件夹或项目访问权限的其他组织成员，然后选择角色。角色用于定义成员对文件夹或项目拥有的权限。

["了解预定义的IAM角色"\(英文\)](#)

5. 选择 \* 添加 \*。

### 结果

BlueXP 将创建文件夹或项目并关联指定的资源和成员。

## 查看与文件夹或项目关联的资源 and 成员

要验证您的资源是否已正确组织并可供组织中的适当成员访问、您可以查看哪些资源和成员与文件夹或项目相关联。

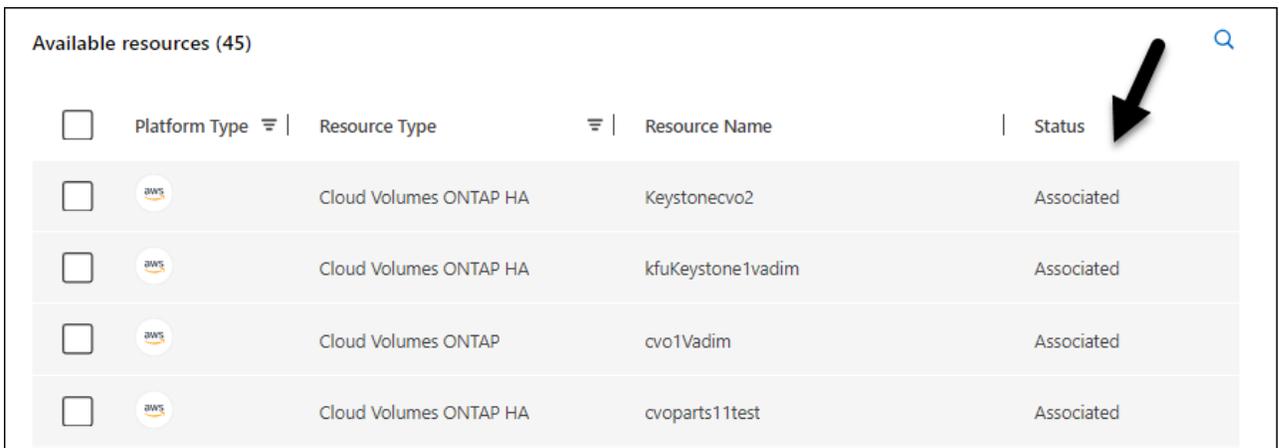
### 步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择，然后选择 **...** 编辑文件夹\*或\*编辑项目。

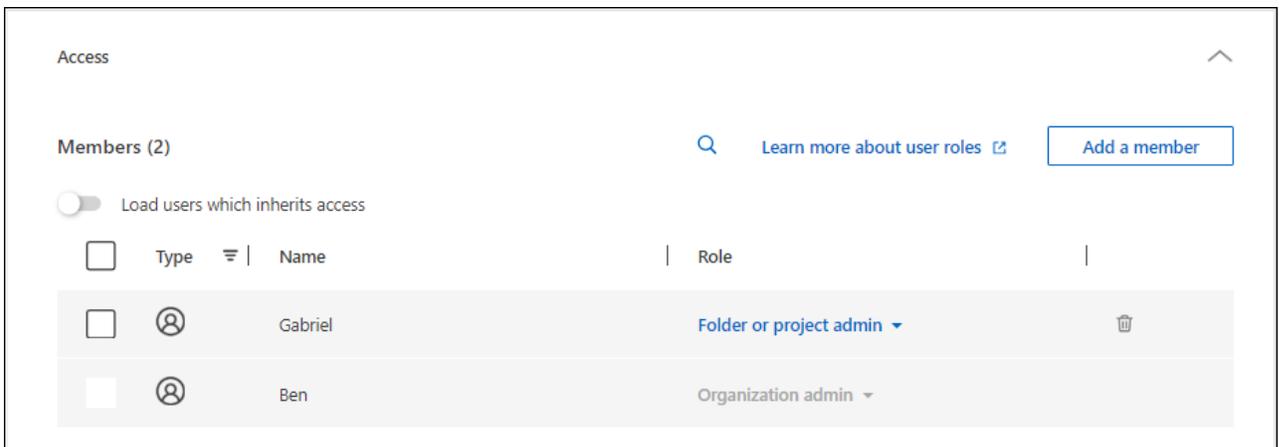


2. 在\*Edit\*页面上，查看有关关联资源和成员访问权限的详细信息：

- 选择\*资源\*以查看关联的资源。在表中，\*Status\*列标识与文件夹或项目关联的资源。



- 选择\*Access\*以查看有权访问文件夹或项目的成员。



下一步是什么？

如果需要，您可以[修改关联的资源](#)或[修改成员访问权限](#)。

## 修改与文件夹或项目关联的资源

您可以通过关联或解除关联资源来修改与文件夹或项目关联的资源。例如、您可能希望将某个资源与另一个项目相关联、因为该资源具有其他团队可以利用的容量。

开始之前

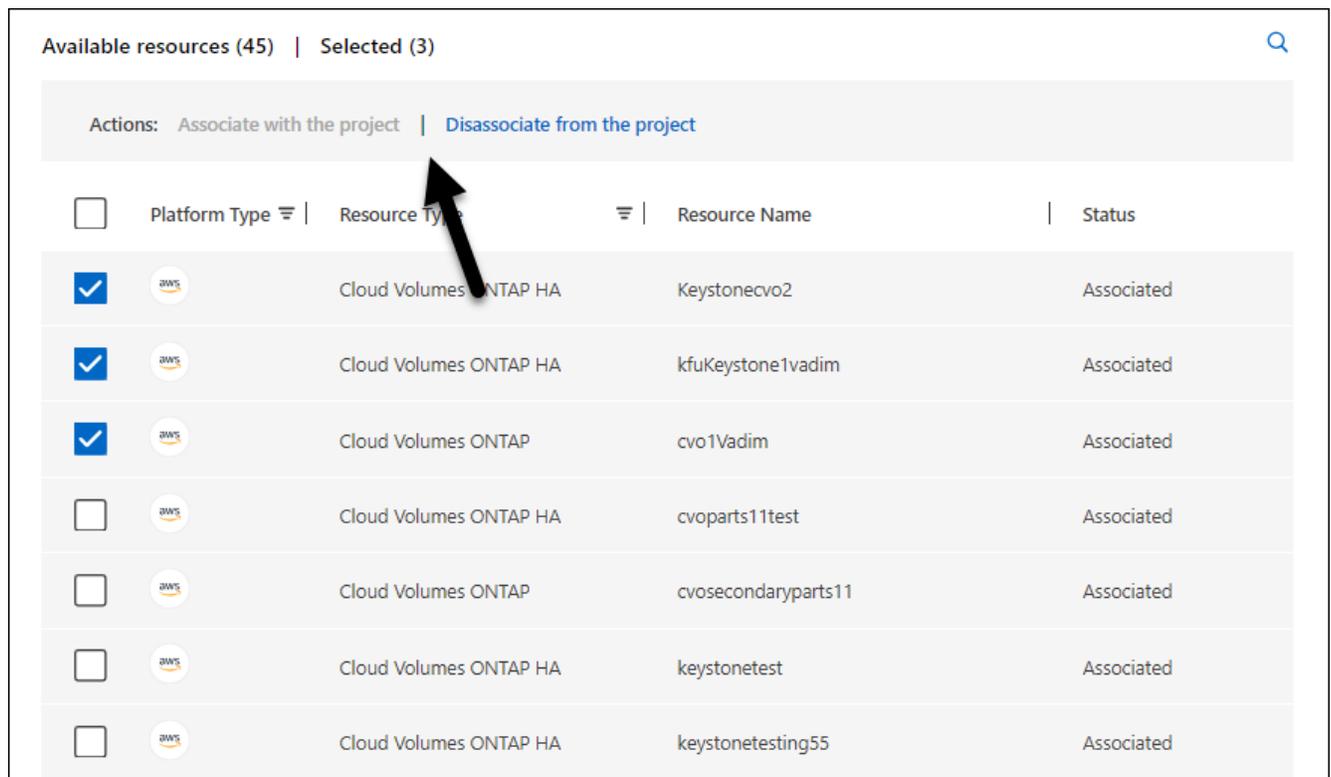
["了解何时可以将资源与文件夹相关联"](#)(英文)

步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择，然后选择 **编辑文件夹\***或\***编辑项目**。
2. 在\*Edit\*页面上，选择\*Res并且 选择\*。

在表中，\*Status\*列标识与文件夹或项目关联的资源。

3. 选择要关联或解除关联的资源。
4. 根据您选择的资源，选择\*与项目关联\*或\*与项目解除关联\*。



Available resources (45) | Selected (3)

Actions: Associate with the project | Disassociate from the project

| <input type="checkbox"/>            | Platform Type | Resource Type          | Resource Name       | Status     |
|-------------------------------------|---------------|------------------------|---------------------|------------|
| <input checked="" type="checkbox"/> | Amazon        | Cloud Volumes ONTAP HA | Keystonecvo2        | Associated |
| <input checked="" type="checkbox"/> | Amazon        | Cloud Volumes ONTAP HA | kfuKeystone1vadim   | Associated |
| <input checked="" type="checkbox"/> | Amazon        | Cloud Volumes ONTAP    | cvo1Vadim           | Associated |
| <input type="checkbox"/>            | Amazon        | Cloud Volumes ONTAP HA | cvoparts11test      | Associated |
| <input type="checkbox"/>            | Amazon        | Cloud Volumes ONTAP    | cvosecondaryparts11 | Associated |
| <input type="checkbox"/>            | Amazon        | Cloud Volumes ONTAP HA | keystonetest        | Associated |
| <input type="checkbox"/>            | Amazon        | Cloud Volumes ONTAP HA | keystonetesting55   | Associated |

5. 选择\*应用\*

结果

BlueXP 将资源与文件夹或项目相关联。拥有该文件夹或项目权限的组织成员现在可以访问关联的资源。

## 修改成员对文件夹或项目的访问权限

修改成员对文件夹或项目的访问权限、以确保正确的成员能够访问与文件夹或项目关联的资源。

## 步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择，然后选择 **...** 编辑文件夹\*或\*编辑项目。
2. 在\*Edit\*页面上，选择\*Access\*。

BlueXP 显示有权访问文件夹或项目的成员列表。

### 3. 修改成员访问权限：

- 添加成员：选择要添加到文件夹或项目中的成员并为其分配角色。
- 更改成员的角色：对于具有组织管理员以外角色的任何成员，请选择其现有角色，然后选择新角色。

如果角色是在较高级别(文件夹或组织级别)提供的、则应考虑是在较低级别还是更高级别上提供。例如、如果您在文件夹级别分配了\_Folder或项目管理员角色、则将项目级别的角色更改为更低级别的权限不会更改成员的权限。由于角色是在组织层次结构中继承的、因此该成员仍具有项目级别的管理员权限。

### "详细了解角色继承"(英文)

- 删除成员访问权限：对于在您正在查看的文件夹或项目中定义了角色的成员，您可以删除其访问权限。

如果成员访问权限是在更高级别(文件夹或组织级别)提供的、则在查看此文件夹或项目时、您无法删除成员访问权限。您需要切换到层次结构的该部分。或者，您也可以"[从成员页面管理权限](#)"。

### 4. 选择 \* 应用 \*。

## 结果

BlueXP 将更新有权访问文件夹或项目的成员。

## 获取项目的ID

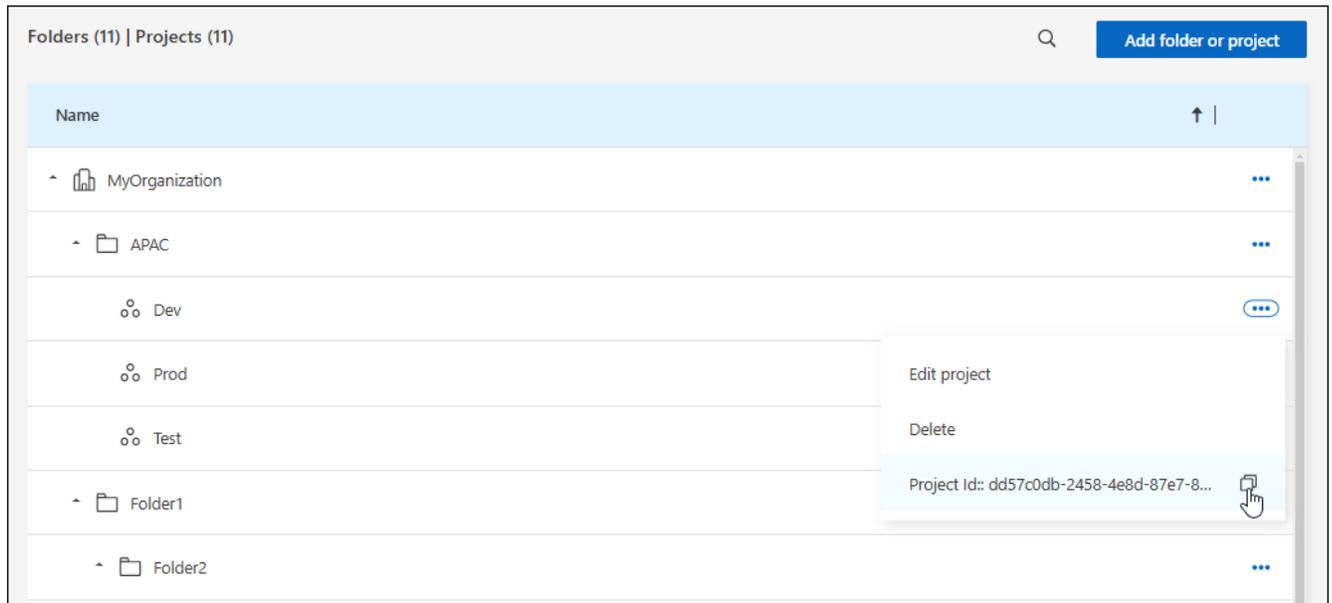
如果您使用的是BlueXP API、则可能需要获取项目的ID。例如、在创建Cloud Volumes ONTAP工作环境时。

## 步骤

1. 在“组织”页面中，导航到表中的项目，然后选择 **...**

此时将显示项目ID。

2. 要复制ID、请选择复制按钮。



## 重命名文件夹或项目

如果需要、您可以更改文件夹和项目的名称。

### 步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择，然后选择 **...** 编辑文件夹\*或\*编辑项目。
2. 在\*Edit\*页面上，输入新名称并选择\*Apply\*。

### 结果

BlueXP 将更新文件夹或项目的名称。

## 删除文件夹或项目

您可以删除不再需要的文件夹和项目。

### 开始之前

- 文件夹或项目不能具有任何关联资源。 [了解如何解除资源关联\(英文\)](#)
- 文件夹不得包含任何子文件夹或项目。您需要先删除这些文件夹和项目。

### 步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择，然后选择 **...** 删除。
2. 确认您要删除文件夹或项目。

### 结果

BlueXP 将删除文件夹或项目。组织成员无法再使用该文件夹或项目。

## 相关信息

- ["了解BlueXP 身份和访问管理"](#)

- ["开始使用BlueXP IAM"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 添加BlueXP IAM成员并管理其权限

通过BlueXP 身份和访问管理(IAM)、您可以向组织添加成员、并在资源层次结构中为其分配一个或多个角色。\_Role\_\_包含一组权限、通过这些权限、成员可以在资源层次结构的特定级别执行特定操作。您可以关联新用户帐户和服务帐户、管理成员角色等。



为确保您不会失去对BlueXP 组织的访问权限、最佳做法是让两个成员具有组织管理员角色。

### 关于此任务

当\_Folder或项目admin\_查看\*成员\*页面时，该页面将显示组织中的所有成员。但是、具有此角色的成员只能查看和管理其拥有权限的文件夹和项目的成员权限。["详细了解\\_Folder或项目admin\\_可以完成的操作"](#)(英文)

### 向您的组织添加成员

您可以向组织添加两种类型的成员：用户帐户和服务帐户。服务帐户通常由应用程序使用来完成指定的任务、而无需人为干预。

## 用户帐户

### 步骤

1. 如果用户尚未执行此操作、请要求他们转到 "[NetApp BlueXP网站](#)"并注册。

用户注册时，应完成\*Sign Up页面，验证其电子邮件地址，然后登录。当系统提示创建组织时，用户应关闭BlueXP 并告知您他们已创建其用户帐户。然后、您可以将此用户添加到现有BlueXP 组织中。

### ["了解如何注册BlueXP "\(英文\)](#)

2. 在BlueXP 控制台的右上角，选择 > \*身份和访问管理\*。
3. 选择\*成员\*。
4. 选择\*添加成员\*。
5. 要添加成员、请完成对话框中的步骤：
  - 实体类型：保持\*用户\*处于选中状态。
  - 用户的电子邮件：输入与用户创建的BlueXP 登录关联的用户电子邮件地址。
  - 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

请注意以下事项：

- 您只能从拥有管理员权限的文件夹和项目中进行选择。
- 如果选择组织或文件夹、则成员将有权访问组织或文件夹中的所有内容。
- 选择角色：选择一个角色，为成员提供与所选组织、文件夹或项目关联的资源的权限。
  - 如果选择了组织，则可以从\*文件夹或项目管理员\*以外的任何角色中进行选择。
  - 如果您选择了文件夹或项目，则可以从\*组织管理员\*以外的任何角色中进行选择。

### ["了解预定义的IAM角色"\(英文\)](#)

- 添加角色：如果要提供对组织中其他文件夹或项目的访问权限，请选择\*添加角色\*，指定其他文件夹或项目，然后选择角色。
6. 选择 \* 添加 \*。

### 结果

BlueXP 将用户添加到组织中。

### 下一步是什么？

用户应收到来自NetApp BlueXP 的电子邮件。此电子邮件包含成员可用于访问BlueXP 的信息。

## 服务帐户

### 步骤

1. 在BlueXP 控制台的右上角，选择 > \*身份和访问管理\*。
2. 选择\*成员\*。
3. 选择\*添加成员\*。

#### 4. 要添加成员、请完成对话框中的步骤：

- 实体类型：选择\*服务帐户\*。
- 服务帐户名称：输入服务帐户的名称。
- 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

请注意以下事项：

- 您只能从拥有管理员权限的文件夹和项目中进行选择。
- 如果选择组织或文件夹、则成员将有权访问组织或文件夹中的所有内容。
- 选择角色：选择一个角色，为成员提供与所选组织、文件夹或项目关联的资源的权限。
  - 如果选择了组织，则可以从\*文件夹或项目管理员\*以外的任何角色中进行选择。
  - 如果您选择了文件夹或项目，则可以从\*组织管理员\*以外的任何角色中进行选择。

#### ["了解预定义的IAM角色"\(英文\)](#)

- 添加角色：如果要提供对组织中其他文件夹或项目的访问权限，请选择\*添加角色\*，指定其他文件夹或项目，然后选择角色。

#### 5. 选择 \* 添加 \*。

#### 6. 下载或复制客户端ID和客户端密钥。

客户端密钥只能显示一次、不会由BlueXP存储在任何位置。复制或下载密钥并将其安全存储。请注意、您可以稍后根据需要重新创建客户端ID和客户端密钥。

#### 7. 选择 \* 关闭 \*。

#### 结果

BlueXP 会将服务帐户添加到您的组织中。

## 查看组织成员

您可以查看BlueXP 组织中所有成员的列表。要了解某个成员可以使用哪些资源和权限、您可以查看在组织的资源层次结构的不同级别分配给该成员的角色。

#### 关于此任务

“成员”页面显示了有关两种类型成员的详细信息：用户帐户和服务帐户。

#### 步骤

1. 在BlueXP 控制台的右上角，选择 > \*身份和访问管理\*。
2. 选择\*成员\*。

您的组织成员出现在“成员”表中。

3. 从\*成员\*页面导航到表中的成员，选择，然后选择... 查看详细信息。

#### 结果

BlueXP 显示有关成员的详细信息、其中包括成员在组织的资源层次结构中拥有权限的文件夹和项目。

下面是一个成员的示例、该成员被分配了文件夹的\_Folder或项目管理\_角色、该角色为文件夹中的三个项目提供权限。

The screenshot displays the BlueXP interface for a member. On the left, under 'Folders and projects', there are 1 Folder and 3 Projects. On the right, under 'Prominent roles', there is 1 role: 'Folder Or Project Admin'. Below this, a table lists the associated organization, folders, and projects. The table has columns for 'Type', 'Associated Organization, folders or projects', and 'Role'. One entry is shown: 'MyOrganization > USWest' with the role 'Folder or project admin'.

以下是另一个示例、其中显示了具有组织管理员角色的成员、该角色为用户授予了对组织中所有资源的访问权限。

The screenshot displays the BlueXP interface for a member with an 'Organization-Admin' role. On the left, under 'Folders and projects', there are 2 Folders and 5 Projects. On the right, under 'Prominent roles', there is 1 role: 'Organization-Admin'. Below this, a table lists the associated organization, folders, and projects. The table has columns for 'Type', 'Associated Scope', and 'Role'. One entry is shown: 'MyOrganization' with the role 'Organization-Admin'.

## 相关信息

["查看与特定文件夹或项目关联的所有成员"\(英文\)](#)

## 管理成员的权限

角色用于定义在组织、文件夹或项目级别分配给成员的权限。每个组织成员可以在组织层次结构的不同级别分配一个角色。它可以是同一个角色、也可以是不同的角色。例如、您可以为项目1分配成员角色A、为项目2分配角色B。



不能为分配了组织管理员角色的成员分配任何其他角色。他们已经拥有整个组织的权限。

## 向成员添加角色

通过添加适用于组织、文件夹或项目级别的角色、为成员提供组织中的其他权限。

## 步骤

1. 从\*成员\*页面导航到表中的成员，选择，然后选择  添加角色。
2. 要添加角色、请完成对话框中的步骤：
  - 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。  
如果选择组织或文件夹、则成员将有权访问组织或文件夹中的所有内容。
  - 选择角色：选择一个角色，为成员提供与所选组织、文件夹或项目关联的资源的权限。
    - 如果选择了组织，则可以从\*文件夹或项目管理员\*以外的任何角色中进行选择。
    - 如果您选择了文件夹或项目，则可以从\*组织管理员\*以外的任何角色中进行选择。

### ["了解预定义的IAM角色"\(英文\)](#)

- 添加角色：如果要提供对组织中其他文件夹或项目的访问权限，请选择\*添加角色\*，指定其他文件夹或项目，然后选择角色。
3. 选择\*添加新角色\*。

## 结果

BlueXP 将添加这些角色。现在、该成员对您选择的组织、文件夹或项目中的资源具有权限。

从一个角色更改为另一个角色

如果需要修改成员的权限、可以在组织、文件夹或项目级别更改与该成员关联的角色。

如果您需要更改组织中多个成员的角色、可以使用批量操作一次性完成所有更改。

一名成员

步骤

1. 从\*成员\*页面导航到表中的成员，选择，然后选择 **...** 查看详细信息。
2. 在表中、导航到组织、文件夹或项目、然后选择新角色。

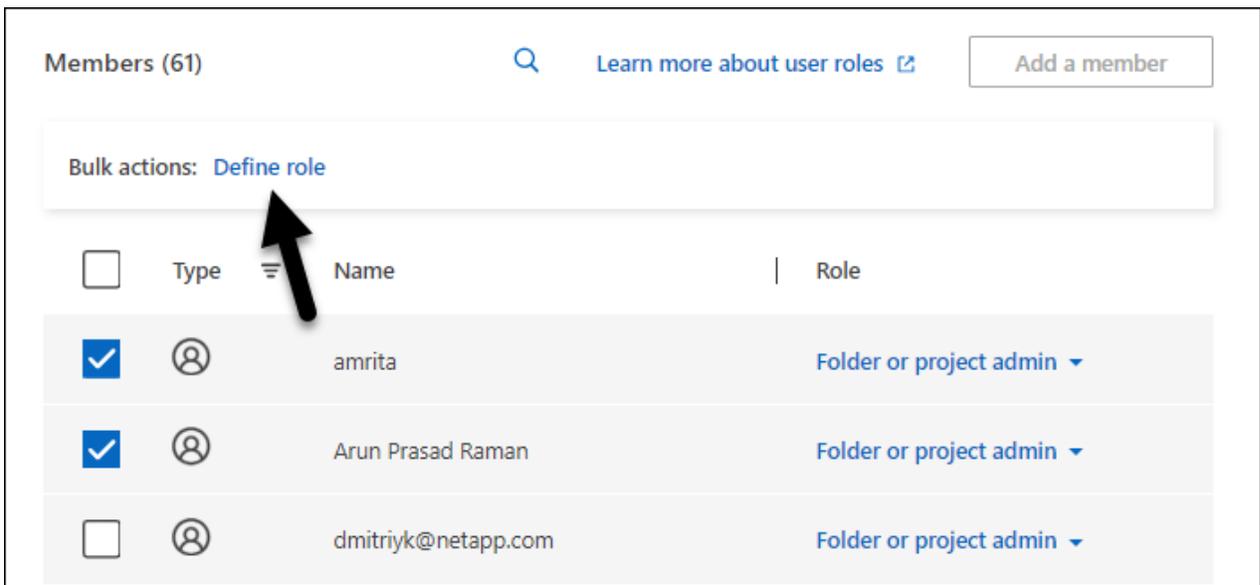
结果

BlueXP 会在组织、文件夹和项目级别更新与该成员关联的角色。

多个成员

步骤

1. 在\*组织\*页中，导航到表中的项目或文件夹，选择， **...** 然后选择\*编辑组织\*、编辑文件夹\*或\*编辑项目。
2. 在\*Edit\*页面上，选择\*Access\*。
3. 选择所有成员或单独选择两个或更多成员。
4. 选择\*Define Role\*。



5. 选择要分配给成员的角色，然后选择\*Define (定义)\*。

结果

BlueXP 会更新您选择的所有成员的角色。

## 删除文件夹或项目的权限

您可以通过删除成员角色来删除其对特定文件夹或项目的权限。

关于此任务

如果某个成员在您的组织中对 `_only_` 个文件夹或项目具有权限、则无法删除此角色。您有两种选择：

- 如果您希望成员对资源层次结构的另一部分具有权限、则需要先添加该角色、然后再删除现有角色。

- 如果您不希望成员拥有任何内容的权限、则只需从您的组织中删除该成员即可。

#### 步骤

1. 从\*成员\*页面导航到表中的成员, 选择, 然后选择... 查看详细信息。
2. 在表中、导航到文件夹或项目级别、然后选择

#### 结果

BlueXP 将在文件夹或项目级别删除该成员的权限。

## 重新创建服务帐户的凭据

您可以随时为服务帐户重新创建凭据(客户端ID和客户端密钥)。如果您丢失了这些凭据、或者您的企业要求您在一段时间后轮换安全凭据、您可以重新创建这些凭据。

#### 关于此任务

重新创建凭据将删除服务帐户的现有凭据、然后创建新凭据。您将无法使用先前的凭据。

#### 步骤

1. 在BlueXP 控制台的右上角, 选择 > \*身份和访问管理\*。
2. 选择\*成员\*。
3. 在\*成员\*表中, 导航到服务帐户, 选择, 然后选择... 重新创建密码。
4. 选择\*重新创建\*。
5. 下载或复制客户端ID和客户端密钥。

客户端密钥只能显示一次、不会由BlueXP存储在任何位置。复制或下载密钥并将其安全存储。

6. 选择 \* 关闭 \*。

#### 结果

此时、新的客户端ID和客户端密钥将与服务帐户关联。

## 从组织中删除成员

您可能需要从您的组织中删除成员, 例如, 如果他们离开了您的公司。

#### 关于此任务

此任务不会删除成员的BlueXP 帐户或NetApp支持站点帐户。它只会从您的组织中删除成员及其关联的权限。

#### 步骤

1. 从\*成员\*页面导航到表中的成员, 选择, 然后选择... 删除用户。
2. 确认要从组织中删除该成员。

#### 结果

BlueXP 将删除该成员。如果该成员再次登录到BlueXP、他们将无法再访问您的BlueXP 组织。

## 相关信息

- ["了解BlueXP 身份和访问管理"](#)
- ["开始使用BlueXP IAM"](#)
- ["预定义的BlueXP IAM角色"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 管理BlueXP 组织中的资源层次结构

当您使用BlueXP 身份和访问管理(IAM)将成员与您的组织关联时、您可以在组织、文件夹或项目级别提供权限。要确保这些成员有权访问适当的资源、您需要通过将资源与特定项目和文件夹关联来管理组织的资源层次结构。资源是BlueXP 已管理的工作环境。

### 查看组织中的资源

要开始管理资源层次结构、您应了解与您的组织关联的资源。

#### 步骤

1. 在BlueXP 控制台的右上角，选择 > \*身份和访问管理\*。
2. 选择\*资源\*。

#### 结果

与您的组织关联的资源显示在\*资源\*表中。

#### 下一步是什么？

要查找特定资源，您可以[搜索和筛选表的内容](#)。

找到要查找的资源后、您可以完成以下任一操作：

- [查看与资源关联的文件夹和项目](#)
- [将资源与其他文件夹和项目相关联](#)
- [从文件夹或项目中删除资源](#)

### 查找组织中的特定资源

如果您的组织中有大量资源、则可以使用搜索和筛选选项来查找特定资源。

#### 步骤

1. 从“资源”页面中，选择“高级搜索和筛选”。
2. 使用任何可用选项查找您要查找的资源：
  - 按资源名称搜索：输入文本字符串并选择\*Add\*。
  - 平台：选择一个或多个平台、例如Amazon Web Services。
  - 资源：选择一个或多个资源，如Cloud Volumes ONTAP。

- 组织、文件夹或项目：选择整个组织、特定文件夹或特定项目。

### 3. 选择\*搜索\*。

#### 结果

资源表的内容将刷新、以显示与您的搜索和筛选选择匹配的资源。

## 将资源与文件夹和项目相关联

如果要使某个资源可供组织中的其他文件夹或项目使用、则需要在该文件夹或项目与该资源之间创建关联。

#### 开始之前

您应了解资源关联的工作原理。"[了解有关资源的信息、包括何时将资源与文件夹相关联](#)"(英文)

#### 步骤

1. 从\*Resources\*页中，导航到表中的资源，选择 **...**，然后选择\*Associate to folder or Projects\*。
2. 选择文件夹或项目，然后选择\*accept\*。
3. 要关联其他文件夹或项目，请选择\*添加文件夹或项目\*，然后选择文件夹或项目。

请注意、您只能从具有管理员权限的文件夹和项目中进行选择。

4. 选择\*关联资源\*。

#### 结果

BlueXP 会将资源与选定的文件夹和项目相关联。

- 如果将资源与项目相关联、则对这些项目具有权限的成员现在可以在BlueXP 中访问该资源。
- 如果将资源与文件夹相关联、则 \_Folder或项目admin\_ 现在可以从BlueXP IAM中访问资源。"[了解如何将资源与文件夹相关联](#)"(英文)

#### 完成后

如果您关联的资源是使用BlueXP 连接器发现的、并且您的组织中还有其他成员、则还需要将该连接器与该资源现在关联的项目相关联。否则、没有 \_Organization admin\_ 角色的成员将无法从BlueXP 画布访问连接器及其关联的资源。

"[了解如何将Connector与文件夹或项目相关联](#)"(英文)

## 查看与资源关联的文件夹和项目

要确定某个资源在组织层次结构中的可用位置、您可以查看与该资源关联的文件夹和项目。

#### 步骤

1. 在\*Resources\*页面中，导航到表中的某个资源，选择，然后选择 **...View DEGRAMENTS**。

#### 结果

BlueXP 将显示与资源关联的文件夹和项目。

以下示例显示了与一个项目关联的资源。

| Folders (0)   Project (1)   |                                      | Associate to folder or project  |
|---|--------------------------------------|---|
| Type  | ☰ ↑   Associated folders or projects | ↕   |
|  | MyOrganization                       |   |
|  | MyOrganization > Project1            |  |

下一步是什么？

- 您可以[将资源与其他项目或文件夹相关联](#)。
- 您可以[从特定文件夹或项目中删除资源](#)。
- 如果需要确定哪些组织成员有权访问资源，可以["查看有权访问与资源关联的文件夹和项目的成员"](#)。

## 从文件夹或项目中删除资源

要从文件夹或项目中删除资源，需要删除文件夹或项目与资源之间的关联。删除关联后、组织成员将无法再管理文件夹或项目中的资源。

关于此任务

如果要从整个组织中删除已发现的资源、则需要从BlueXP 画布中删除工作环境。

步骤

1. 在\*Resources\*页面中，导航到表中的某个资源，选择，然后选择 **...View DEGRAMENTS**。
2. 对于要删除其资源的文件夹或项目、请选择 
3. 通过选择\*Delete\*确认要删除关联。

结果

BlueXP 将删除此关联。成员无法再从该文件夹或项目访问资源。

## 相关信息

- ["了解BlueXP 身份和访问管理"](#)
- ["开始使用BlueXP IAM"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 将BlueXP 连接器与其他文件夹和项目相关联

要从BlueXP 管理多种类型的工作环境、需要使用Connector。当\_Organization admin\_创建Connector时，BlueXP 会自动将该Connector与组织和当前选定的项目相关联。Organization admin\_可自动从组织中的任何位置访问该Connector。组织中的其他成员只能从创建连接器的项目访问该连接器、除非您将该连接器与BlueXP 身份和访问管理(IAM)中的其他项目相关联。

## 开始之前

您应了解连接器关联的工作原理。"[了解如何将连接器与BlueXP IAM结合使用](#)"(英文)

## 关于此任务

- 当 `_Folder` 或项目 `admin_查看*Connectors*` 页时，该页将显示组织中的所有 `Connectors*`。但是、具有此角色的成员只能查看连接器并将其与它们具有权限的文件夹和项目相关联。"[详细了解\\_Folder或项目admin\\_可以完成的操作](#)"(英文)

## 步骤

1. 在BlueXP 控制台的右上角，选择  > \*身份和访问管理\*。
2. 选择\*连接器\*。
3. 从表中、找到要关联的连接器。

要查找特定连接器、您可以使用表上方的搜索、并通过选择资源层次结构的特定部分来筛选表的内容。

4. 要首先查看与连接器关联的文件夹和项目，请选择，然后选择  查看详细信息。

BlueXP 显示与连接器关联的文件夹和项目的详细信息。

5. 选择\*关联到文件夹或项目\*。
6. 选择文件夹或项目，然后选择\*accept\*。
7. 要将连接器与其它文件夹或项目相关联，请选择\*添加文件夹或项目\*，然后选择文件夹或项目。
8. 选择\*关联连接器\*。

## 结果

BlueXP 将连接器与选定的文件夹和项目相关联。现在、对这些文件夹和项目具有权限的成员可以选择该Connector。

## 完成后

如果要将Connector管理的资源与相同的文件夹和项目相关联，可以从资源页执行此操作。

"[了解如何将资源与文件夹和项目相关联](#)"(英文)

## 相关信息

- "[了解BlueXP 连接器](#)"
- "[了解BlueXP 身份和访问管理](#)"
- "[开始使用BlueXP IAM](#)"
- "[了解适用于BlueXP IAM的API](#)"

## 在BlueXP 组织、项目和连接器之间切换

您可能属于多个BlueXP 组织、或者有权访问BlueXP 组织中的多个项目或连接器。如果需要、您可以轻松地在组织、项目和连接器之间切换、以访问与该组织、项目或连接器关联的资源。



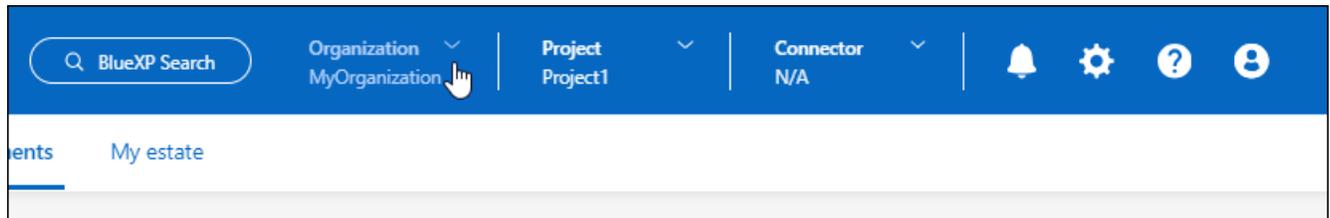
如果您被邀请加入另一个组织、或者您自己创建了一个额外的组织、则您可能属于多个组织。您可以使用API创建其他组织。["了解如何创建新组织"](#)

## 在组织之间切换

如果您是多个组织的成员、您可以随时在这些组织之间切换。

### 步骤

1. 在BlueXP 的顶部，选择\*组织\*。



2. 选择其他组织，然后选择\*Switch\*。

### 结果

BlueXP 将切换到选定组织并显示与该组织关联的资源。

## 在项目之间切换

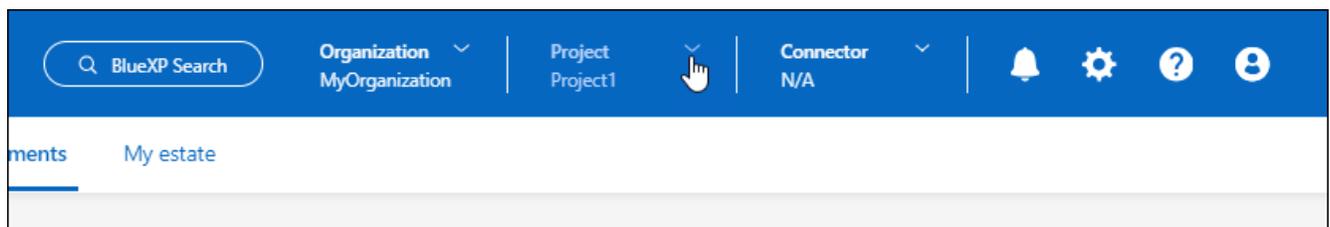
如果您的组织包含多个项目、并且您有权访问这些项目、您可以随时在这些项目之间切换。

### 开始之前

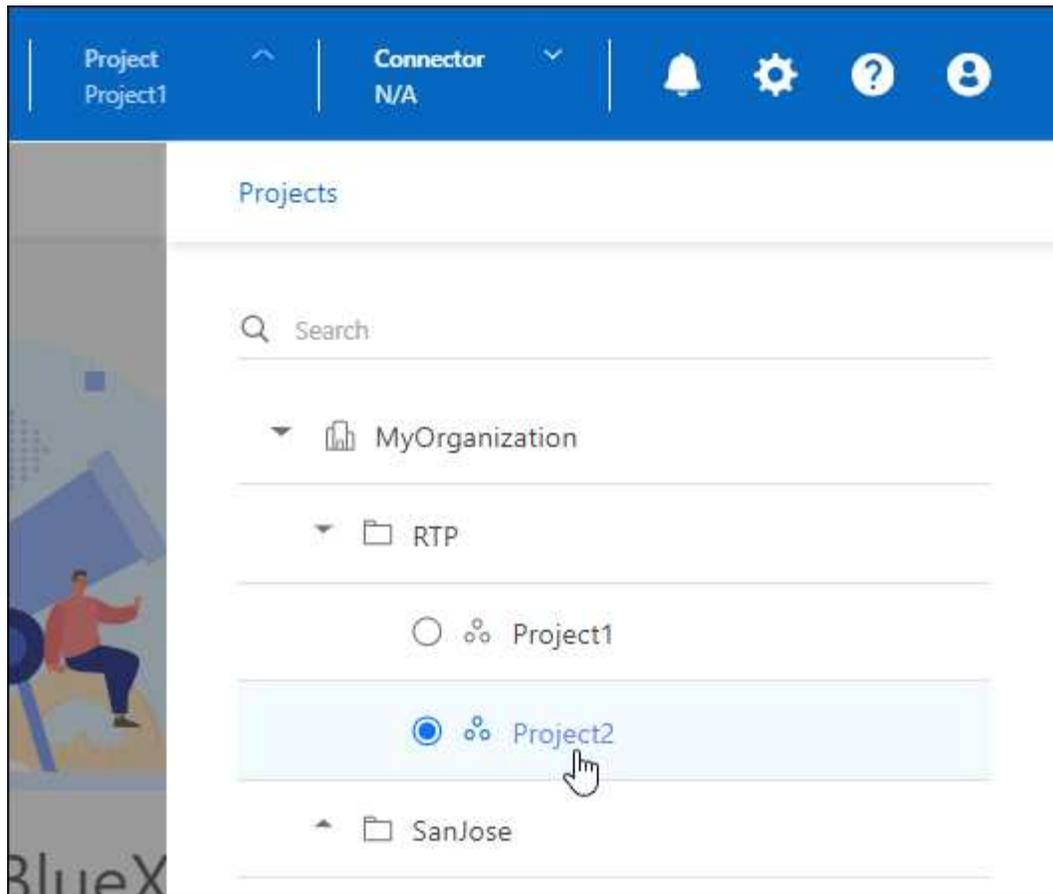
您必须位于BlueXP 控制台中除BlueXP 身份和访问管理(IAM)页面以外的任何页面上。查看任何IAM页面时、您无法切换到其他项目。

### 步骤

1. 在BlueXP 顶部，选择\*Project\*。



2. 浏览组织中的文件夹和项目，选择所需项目，然后选择\*Switch\*。



结果

BlueXP 将切换到选定项目并显示与该项目关联的资源。

## 在连接器之间切换

如果您有多个连接器、则可以在它们之间切换、以查看与特定连接器关联的工作环境。

步骤

1. 在BlueXP 的顶部，选择\*Connector\*。
2. 选择另一个连接器，然后选择\*Switch\*。

结果

BlueXP 将刷新并显示与选定连接器关联的工作环境。

相关链接

["将接头与文件夹和项目相关联"\(英文\)](#)

## 相关信息

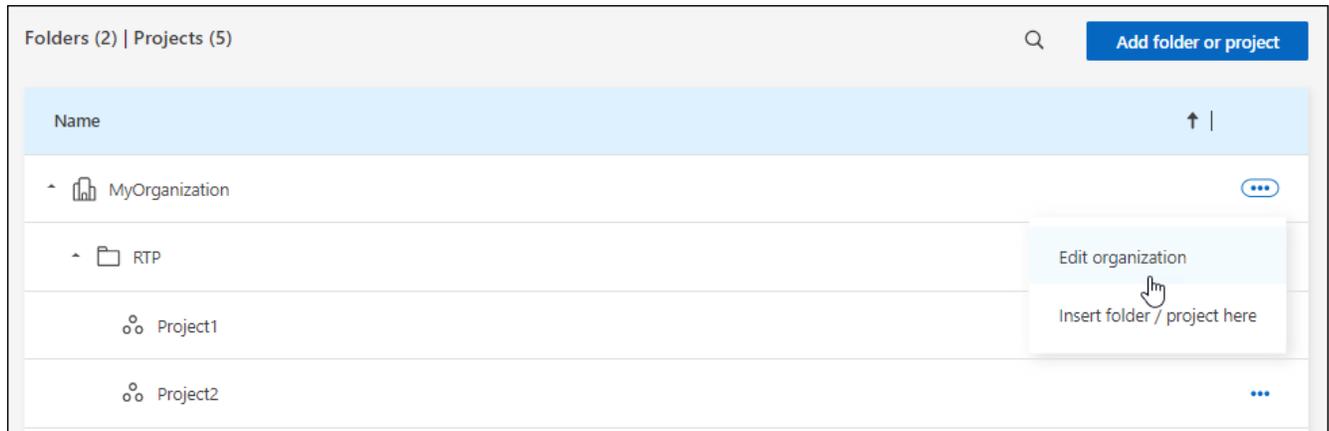
- ["了解BlueXP 身份和访问管理"](#)
- ["开始使用BlueXP IAM"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 重命名BlueXP 组织

如果需要、您可以从BlueXP 身份和访问管理(Identity and Access Management、IAM)中更改BlueXP 组织的名称。组织名称显示在BlueXP 基于Web的控制台顶部和IAM页面中。

### 步骤

1. 在BlueXP 控制台的右上角，选择 > \*身份和访问管理\*。
2. 从\*组织\*页面导航到表中的第一行，选择，然后选择 编辑组织。



3. 输入新的组织名称并选择\*Apply\*。

### 结果

BlueXP 将更新您的组织名称。您应立即在BlueXP 控制台顶部看到更新后的名称。

### 相关信息

- ["了解BlueXP 身份和访问管理"](#)
- ["开始使用BlueXP IAM"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 通过BlueXP 时间表监控或审核IAM活动

如果您需要监控或审核通过BlueXP 身份和访问管理(IAM)完成的操作、则可以从BlueXP 时间线查看详细信息。例如、您可能希望验证谁向组织添加了成员或项目是否已成功删除。

### 步骤

1. 在BlueXP 控制台的右上角，选择 > \*时间线\*。
2. 从过滤器中选择\*Service\*，然后选择\*Tenancy\*。
3. 使用任何其他筛选器更改表中显示的操作。

例如，可以使用\*User\*过滤器显示与特定用户帐户相关的操作。

结果

时间线将更新、以显示已完成的与BlueXP IAM相关的管理操作。

## 预定义的BlueXP IAM角色和权限

BlueXP 身份和访问管理(IAM)包括多个预定义角色、您可以将这些角色分配给组织中不同级别的资源层次结构成员。在分配这些角色之前、您应了解每个角色包含的权限。

### 平台角色

BlueXP IAM包括两个平台角色：组织管理员和文件夹管理员或项目管理员。两个BlueXP IAM平台角色之间的主要区别是范围。组织管理员角色在所有文件夹和项目中都拥有权限；而文件夹或项目管理员只在其所分配到的文件夹或项目中拥有权限。

文件夹或项目管理员角色无法创建连接器。

### 权限

| 任务                                | 组织管理员 | 文件夹或项目管理员 |
|-----------------------------------|-------|-----------|
| 生成接头                              | 是的。   | 否         |
| 创建、修改或删除工作环境(使用BlueXP 画布添加或发现新资源) | 是的。   | 是的。       |
| 创建项目/文件夹、包括重命名、删除和编辑              | 是的。   | 是的。       |
| 分配角色和添加用户                         | 是的。   | 是的。       |
| 将资源和连接器与文件夹和项目相关联                 | 是的。   | 是的。       |
| 通过设置>凭据管理凭据                       | 是的。   | 是的。       |
| 查看BlueXP 时间线                      | 是的。   | 是的。       |
| 使用BlueXP 服务                       | 是的。   | 是的。       |
| 注册BlueXP 以获得支持并提交案例               | 是的。   | 是的。       |

### 大型跨国组织在BlueXP 中的组织角色示例

XYZ Corporation是一家跨国公司、其目标是根据地理区域(北美、欧洲和亚太地区)隔离对数据存储资源的访问。他们希望每个区域在保持集中监督的同时，对其资源实行专属控制。

为此、在XYZ公司的BlueXP 中分配了组织管理员角色的人员会创建一个初始工作环境、然后在BlueXP 中为每个区域创建单独的文件夹。每个区域的文件夹都包含与该区域相关的项目(以及相关资源)。组织管理员为每个区域的BlueXP 用户分配文件夹/项目管理员角色。

完成初始设置后、具有文件夹或项目管理员角色的区域管理员可以创建新的工作环境并在其区域内添加用户。这些区域管理员还可以添加/删除/重命名为其分配的文件夹和项目。组织管理员可以继承任何新工作环境或资源的权限、从而保持整个组织内存使用情况的可见性。

## 数据服务角色

数据服务角色可以在任何项目或文件夹中完成其任务。

### SnapCenter管理员

#### Description

能够使用适用于应用程序的BlueXP 备份和恢复功能从内部ONTAP集群备份快照。

#### 权限

具有此角色的成员可以在BlueXP 中完成以下操作：

- 从备份和恢复>应用程序完成任何操作
- 管理他们拥有权限的项目和文件夹中的所有工作环境
- 使用所有BlueXP 服务

### 分类查看器

#### Description

提供查看BlueXP 分类扫描结果的功能。

#### 权限

查看合规性信息并为其有权访问的资源生成报告。这些用户无法启用或禁用对卷、分段或数据库架构的扫描。

具有此角色的成员不能执行任何其他操作。

## 相关链接

- ["了解BlueXP 身份和访问管理"](#)
- ["开始使用BlueXP IAM"](#)
- ["管理BlueXP 成员及其权限"](#)
- ["了解适用于BlueXP IAM的API"](#)

## 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。