



Azure

NetApp Console setup and administration

NetApp
January 27, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/console-setup-admin/concept-accounts-azure.html> on January 27, 2026. Always check docs.netapp.com for the latest.

目录

- Azure 1
 - 了解NetApp Console中的 Azure 凭据和权限 1
 - 初始 Azure 凭据 1
 - 托管标识的其他 Azure 订阅 1
 - 其他 Azure 凭据 2
 - 凭证和市场订阅 2
 - 常见问题解答 3
 - 管理NetApp Console的 Azure 凭据和市场订阅 3
 - 概述 4
 - 将其他 Azure 订阅与托管标识关联Associate additional Azure subscriptions with a managed identity 4
 - 向NetApp Console添加其他 Azure 凭据 5
 - 管理现有凭证 13

Azure

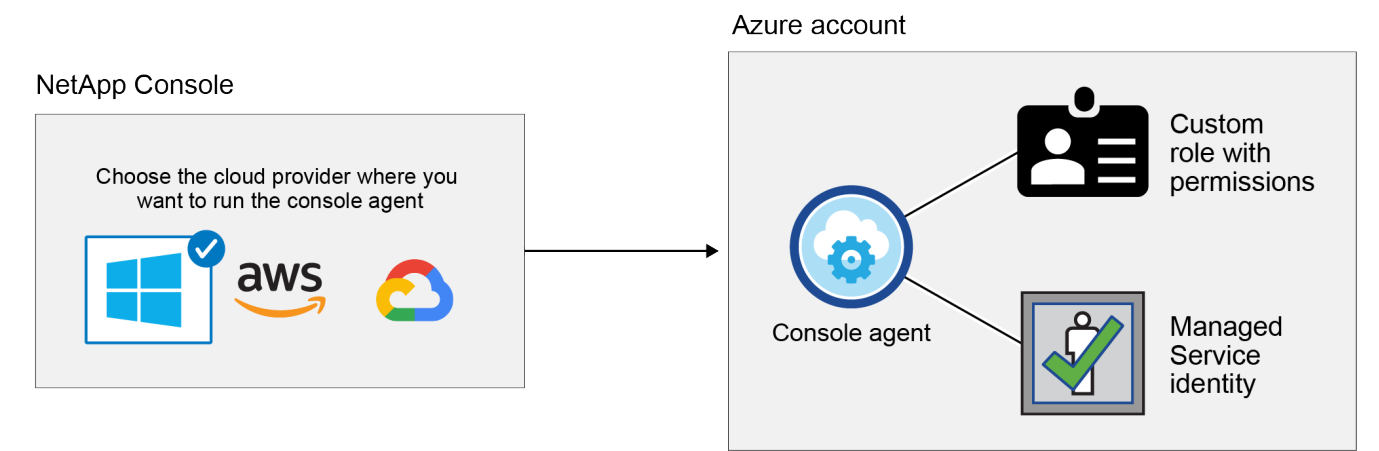
了解NetApp Console中的 Azure 凭据和权限

了解NetApp Console如何使用 Azure 凭据代表您执行操作以及这些凭据如何与市场订阅相关联。了解这些详细信息有助于您管理一个或多个 Azure 订阅的凭据。例如，您可能想了解何时向控制台添加其他 Azure 凭据。

初始 Azure 凭据

从控制台部署控制台代理时，您需要使用具有部署控制台代理虚拟机权限的 Azure 帐户或服务主体。所需权限列于["Azure 的代理部署策略"](#)。

当控制台在 Azure 中部署控制台代理虚拟机时，它会启用 ["系统分配的托管标识"](#)在虚拟机上，创建自定义角色，并将其分配给虚拟机。该角色为控制台提供管理该 Azure 订阅内的资源和流程所需的权限。["查看控制台如何使用权限"](#)。



如果您为Cloud Volumes ONTAP创建新系统，控制台将默认选择以下 Azure 凭据：

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

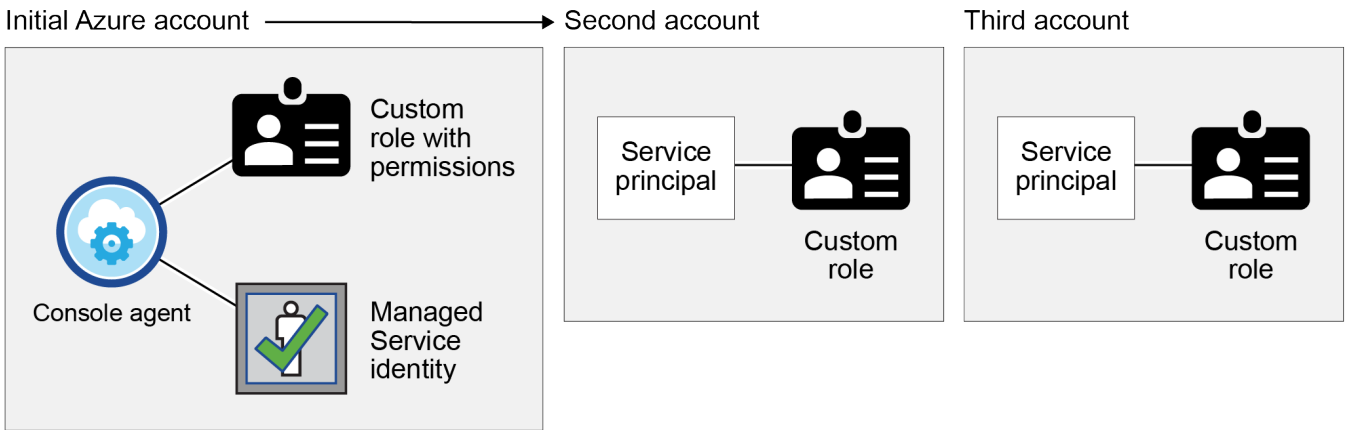
您可以使用初始 Azure 凭据部署所有Cloud Volumes ONTAP系统，也可以添加其他凭据。

托管标识的其他 Azure 订阅

分配给控制台代理 VM 的系统分配托管标识与您启动控制台代理的订阅相关联。如果您想选择不同的 Azure 订阅，则需要["将托管标识与这些订阅关联"](#)。

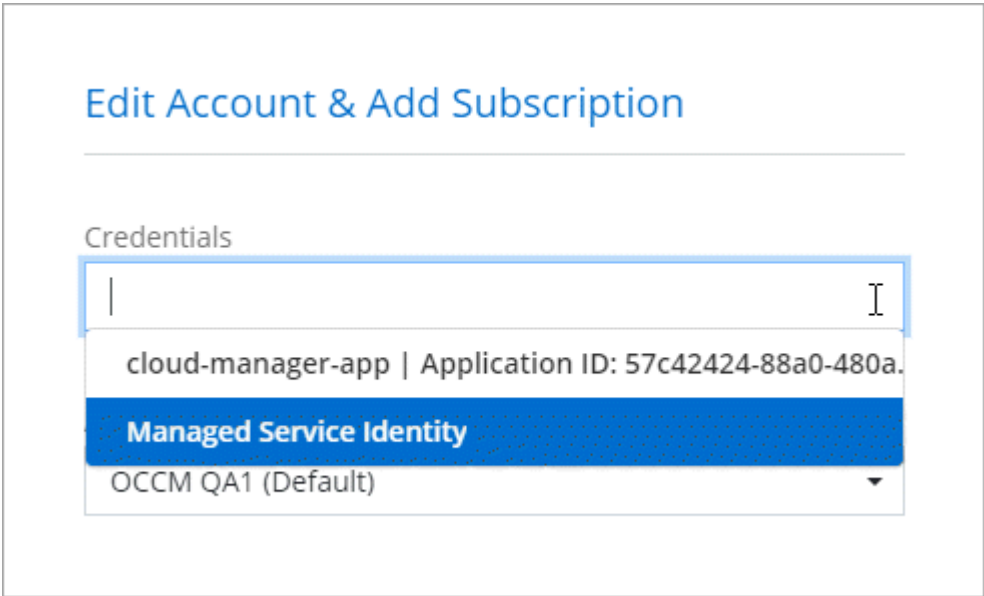
其他 Azure 凭据

如果要在控制台中使用不同的 Azure 凭据，则必须通过以下方式授予所需的权限"[在 Microsoft Entra ID 中创建和设置服务主体](#)"对于每个 Azure 帐户。下图显示了另外两个帐户，每个帐户都设置了服务主体和提供权限的自定义角色：



那么你会"[将帐户凭据添加到控制台](#)"通过提供有关 AD 服务主体的详细信息。

例如，您可以在创建新的Cloud Volumes ONTAP系统时在凭据之间切换：



凭证和市场订阅

您添加到控制台代理的凭据必须与 Azure Marketplace 订阅相关联，以便您可以按小时费率（PAYGO）或NetApp数据服务或通过年度合同支付Cloud Volumes ONTAP费用。

"[了解如何关联 Azure 订阅](#)"。

请注意有关 Azure 凭据和市场订阅的以下事项：

- 只能将一个 Azure 市场订阅与一组 Azure 凭据关联

- 您可以使用新的订阅替换现有的市场订阅

常见问题解答

以下问题与凭证和订阅有关。

我可以更改**Cloud Volumes ONTAP**系统的 **Azure Marketplace** 订阅吗？

是的，你可以。当您更改与一组 Azure 凭证关联的 Azure 市场订阅时，所有现有和新的 Cloud Volumes ONTAP 系统都将根据新订阅收费。

["了解如何关联 Azure 订阅"](#)。

我可以添加多个 **Azure** 凭证，每个凭证都有不同的市场订阅吗？

属于同一 Azure 订阅的所有 Azure 凭证都将与同一 Azure 市场订阅相关联。

如果您有属于不同 Azure 订阅的多个 Azure 凭证，则这些凭证可以与同一个 Azure 市场订阅或不同的市场订阅相关联。

我可以将现有的**Cloud Volumes ONTAP**系统移动到不同的 **Azure** 订阅吗？

不可以，无法将与您的 Cloud Volumes ONTAP 系统关联的 Azure 资源移动到其他 Azure 订阅。

凭证如何用于市场部署和本地部署？

以上部分描述了控制台代理的推荐部署方法，即从控制台部署。您还可以从 Azure 市场在 Azure 中部署控制台代理，并且可以在自己的 Linux 主机上安装控制台代理软件。

如果您使用 Marketplace，您可以通过向控制台代理 VM 和系统分配的托管身份分配自定义角色来提供权限，或者您可以使用 Microsoft Entra 服务主体。

对于本地部署，您无法为控制台代理设置托管标识，但可以使用服务主体提供权限。

要了解如何设置权限，请参阅以下页面：

- 标准模式
 - ["设置 Azure 市场部署的权限"](#)
 - ["设置本地部署的权限"](#)
- 限制模式
 - ["设置限制模式的权限"](#)

管理 NetApp Console 的 Azure 凭证和市场订阅

添加和管理 Azure 凭证，以便 NetApp Console 具有在 Azure 订阅中部署和管理云资源所需的权限。如果您管理多个 Azure 市场订阅，则可以从“凭证”页面将每个订阅分配给不同的 Azure 凭证。

概述

有两种方法可以在控制台中添加额外的 Azure 订阅和凭据。

1. 将其他 Azure 订阅与 Azure 托管标识关联。
2. 要使用不同的 Azure 凭据部署 Cloud Volumes ONTAP，请使用服务主体授予 Azure 权限并将其凭据添加到控制台。

将其他 Azure 订阅与托管标识关联 Associate additional Azure subscriptions with a managed identity

控制台使您能够选择要部署 Cloud Volumes ONTAP 的 Azure 凭据和 Azure 订阅。除非关联 ["托管标识"](#)通过这些订阅。

关于此任务

托管身份 ["初始 Azure 帐户"](#) 当您从控制台部署控制台代理时。部署控制台代理时，控制台会将控制台操作员角色分配给控制台代理虚拟机。

步骤

1. 登录 Azure 门户。
2. 打开 ["订阅"](#) 服务，然后选择要部署 Cloud Volumes ONTAP 的订阅。
3. 选择 ["访问控制 \(IAM\)"](#)。
 - a. 选择 [添加 > 添加角色分配](#)，然后添加权限：
 - 选择 ["控制台操作员"](#) 角色。

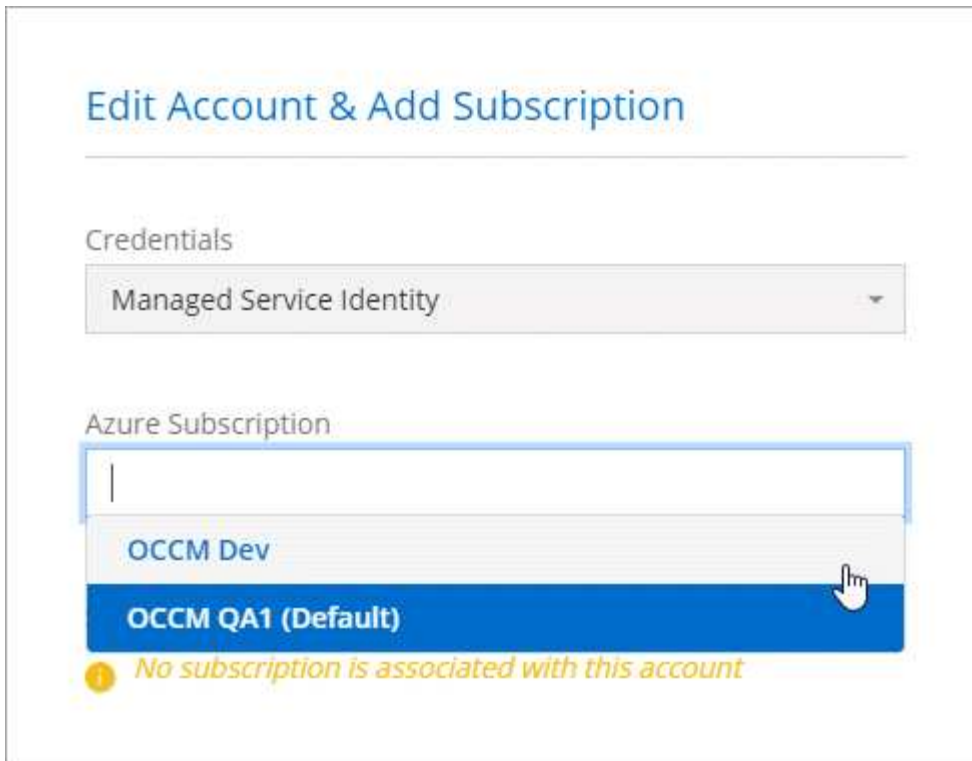


控制台操作员是控制台代理策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

- 分配对 ["虚拟机"](#) 的访问权限。
 - 选择创建控制台代理虚拟机的订阅。
 - 选择一个控制台代理虚拟机。
 - 选择 ["保存"](#)。
4. 重复这些步骤以获得更多订阅。

结果

创建新系统时，您现在可以从多个 Azure 订阅中选择托管标识配置文件。



向NetApp Console添加其他 Azure 凭据

从控制台部署控制台代理时，控制台会在具有所需权限的虚拟机上启用系统分配的托管标识。当您为Cloud Volumes ONTAP创建新系统时，控制台会默认选择这些 Azure 凭据。



如果您在现有系统上手动安装了控制台代理软件，则不会添加初始凭据集。["了解 Azure 凭据和权限"](#)。

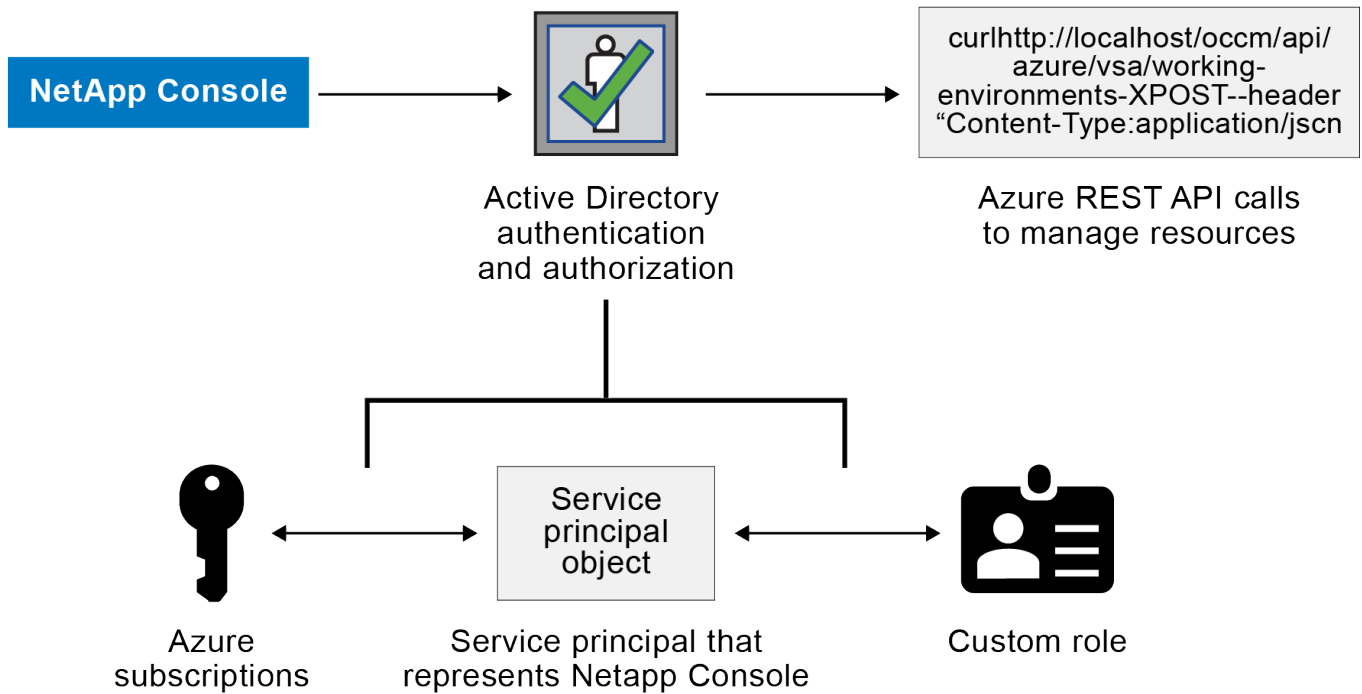
如果您想使用不同的 Azure 凭据部署Cloud Volumes ONTAP，则必须通过在 Microsoft Entra ID 中为每个 Azure 帐户创建和设置服务主体来授予所需的权限。然后，您可以将新凭据添加到控制台。

使用服务主体授予 Azure 权限

控制台需要权限才能在 Azure 中执行操作。您可以通过在 Microsoft Entra ID 中创建和设置服务主体并获取控制台所需的 Azure 凭据来向 Azure 帐户授予所需的权限。

关于此任务

下图描述了控制台如何获取在 Azure 中执行操作的权限。服务主体对象与一个或多个 Azure 订阅绑定，代表 Microsoft Entra ID 中的控制台，并分配给允许所需权限的自定义角色。



步骤

1. 创建 [Microsoft Entra 应用程序](#)。
2. [\[将应用程序分配给角色\]](#)。
3. 添加 [Windows Azure 服务管理 API 权限](#)。
4. 获取应用程序ID和目录ID。
5. [\[创建客户端机密\]](#)。

创建 **Microsoft Entra** 应用程序

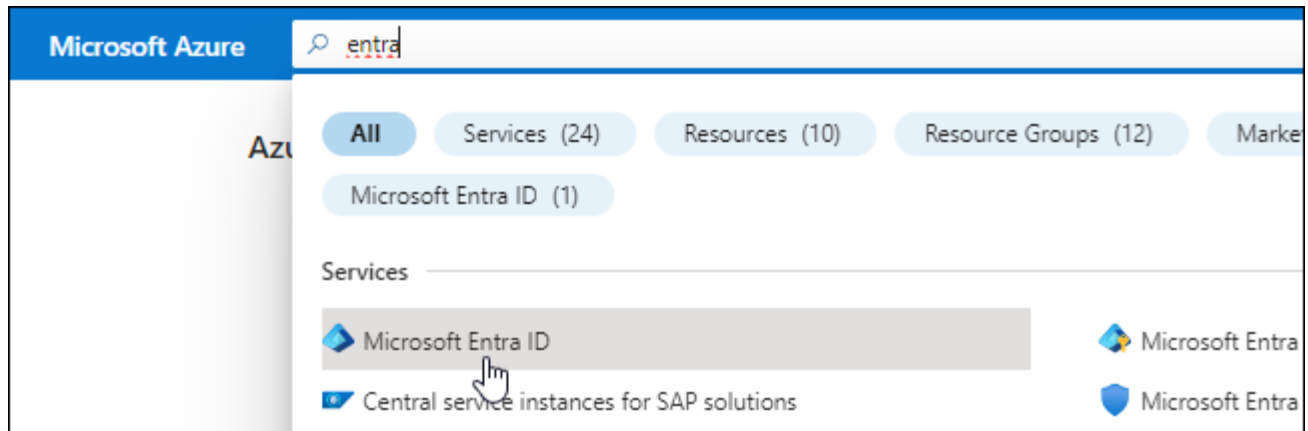
创建控制台可用于基于角色的访问控制的 **Microsoft Entra** 应用程序和服务主体。

步骤

1. 确保您在 Azure 中拥有创建 Active Directory 应用程序并将该应用程序分配给角色的权限。

有关详细信息，请参阅 ["Microsoft Azure 文档：所需权限"](#)

2. 从 Azure 门户打开 **Microsoft Entra ID** 服务。



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
 - 名称：输入应用程序的名称。
 - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
 - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

您必须将服务主体绑定到一个或多个 Azure 订阅，并为其分配自定义“控制台操作员”角色，以便控制台在 Azure 中拥有权限。

步骤

1. 创建自定义角色：

请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 ["Azure 文档"](#)

- a. 复制["控制台代理的自定义角色权限"](#)并将它们保存在 JSON 文件中。
- b. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

您应该为用户将从中创建Cloud Volumes ONTAP系统的每个 Azure 订阅添加 ID。

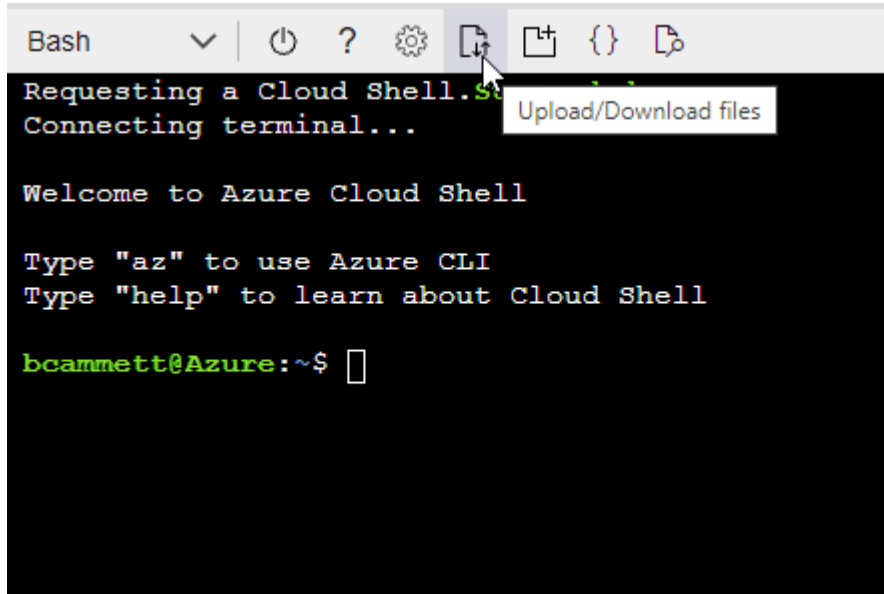
例子

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

- c. 使用 JSON 文件在 Azure 中创建自定义角色。

以下步骤介绍如何使用 Azure Cloud Shell 中的 Bash 创建角色。

- 开始 "Azure 云外壳" 并选择 Bash 环境。
- 上传 JSON 文件。



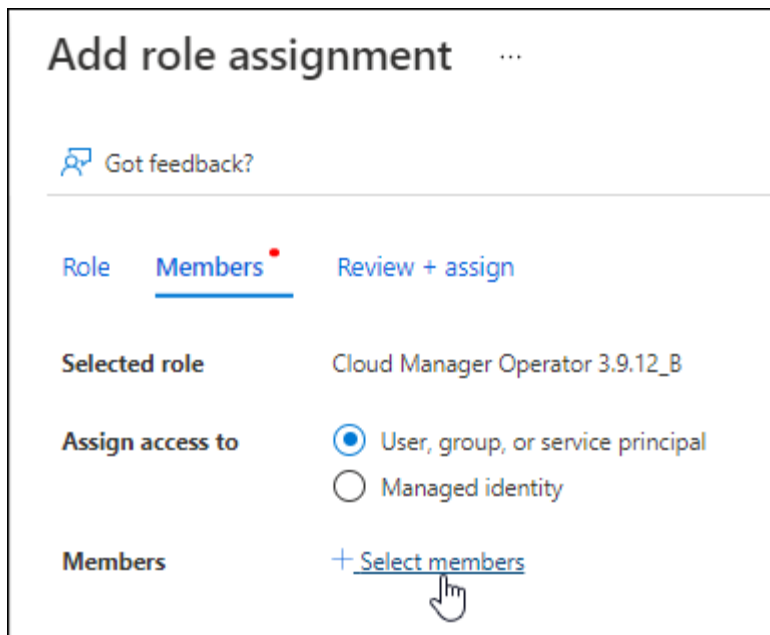
- 使用 Azure CLI 创建自定义角色：

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

现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

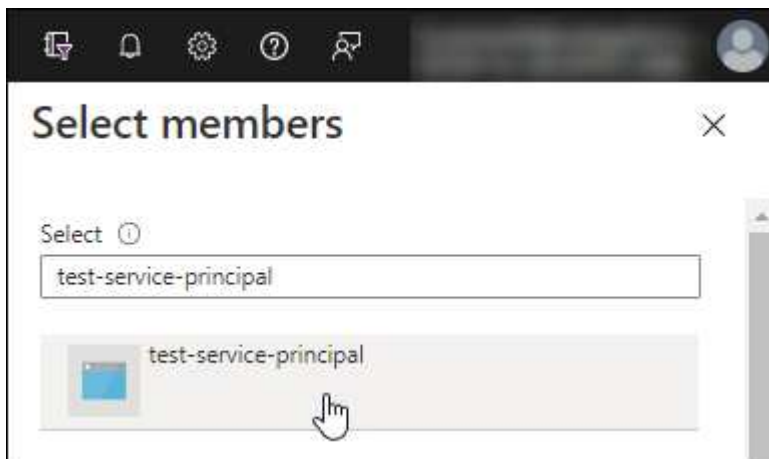
2. 将应用程序分配给角色：

- a. 从 Azure 门户打开 **Subscriptions** 服务。
- b. 选择订阅。
- c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
- d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
- e. 在“成员”选项卡中，完成以下步骤：
 - 保持选中“用户、组或服务主体”。
 - 选择*选择成员*。



- 搜索应用程序的名称。

以下是一个例子：



- 选择应用程序并选择*选择*。
 - 选择“下一步”。
- f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

如果您想从多个 Azure 订阅部署 Cloud Volumes ONTAP，则必须将服务主体绑定到每个订阅。在 NetApp Console 中，您可以选择部署 Cloud Volumes ONTAP 时要使用的订阅。

添加 **Windows Azure 服务管理 API** 权限

您必须为服务主体分配“Windows Azure 服务管理 API”权限。

步骤

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

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. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。

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](#)

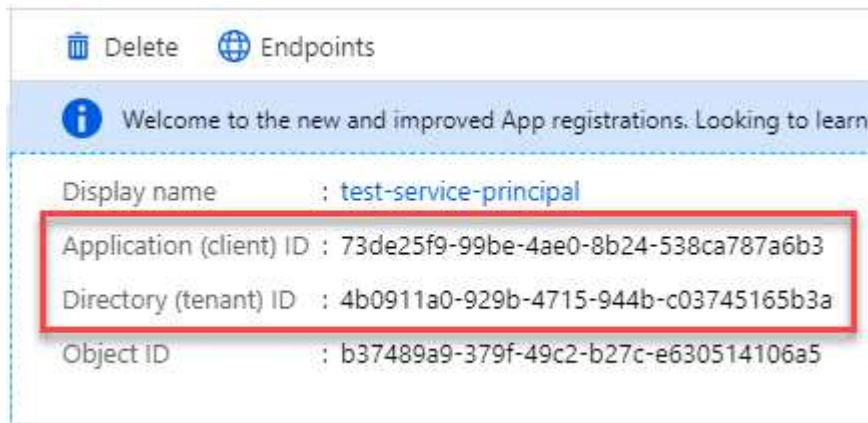
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
☒ user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

获取应用程序ID和目录ID

将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

步骤

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

创建客户端机密

创建客户端密钥并将其值提供给控制台以使用 Microsoft Entra ID 进行身份验证。

步骤

1. 开启*Microsoft Entra ID*服务。

2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。

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

结果

您的服务主体现已设置，您应该已经复制了应用程序（客户端）ID、目录（租户）ID 和客户端机密的值。添加 Azure 帐户时，您需要在控制台中输入此信息。

将凭据添加到控制台

为 Azure 帐户提供所需权限后，您可以将该帐户的凭据添加到控制台。完成此步骤后，您可以使用不同的 Azure 凭据启动 Cloud Volumes ONTAP。

开始之前

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟才能使用它们。等待几分钟，然后将凭据添加到控制台。

开始之前

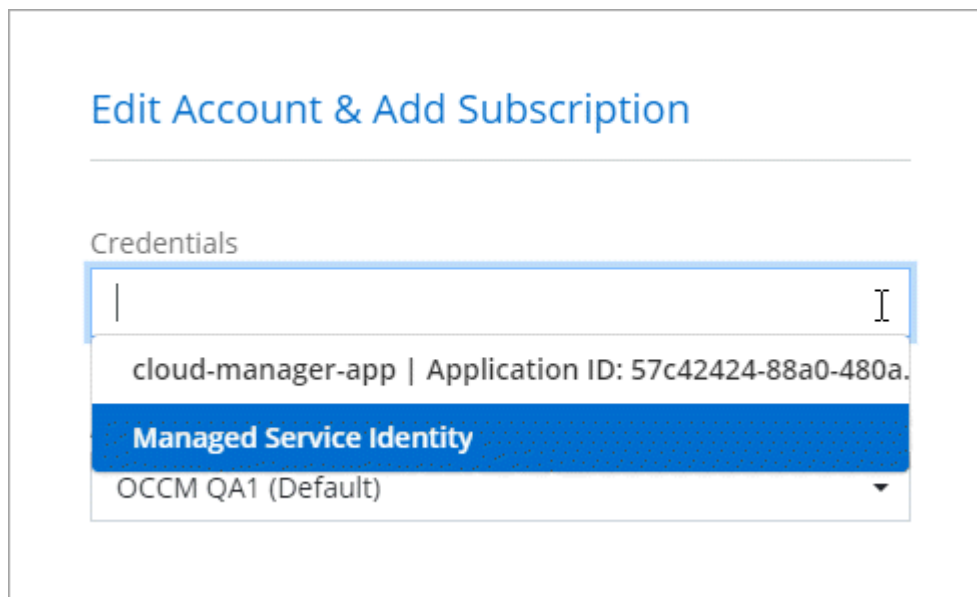
您需要先创建控制台代理，然后才能更改控制台设置。["了解如何创建控制台代理"](#)。

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
 - a. 凭证位置：选择*Microsoft Azure > 代理*。
 - b. 定义凭据：输入有关授予所需权限的 Microsoft Entra 服务主体的信息：
 - 应用程序（客户端）ID
 - 目录（租户）ID
 - 客户端密钥
 - 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证关联。
 - d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

您可以从“详细信息和凭证”页面切换到另一组凭证 ["将系统添加到控制台时"](#)



管理现有凭证

通过关联 Marketplace 订阅、编辑凭据和删除凭据来管理已添加到控制台的 Azure 凭据。

将 **Azure** 市场订阅关联到凭据

将 Azure 凭据添加到控制台后，您可以将 Azure 市场订阅与这些凭据关联。您可以使用订阅来创建按使用量付费的 Cloud Volumes ONTAP 系统并访问 NetApp 数据服务。

在将凭据添加到控制台后，可以在两种情况下关联 Azure 市场订阅：

- 当您最初将凭据添加到控制台时，您没有关联订阅。
- 您想要更改与 Azure 凭据关联的 Azure 市场订阅。

替换当前的市场订阅会针对现有和新的 Cloud Volumes ONTAP 系统进行更新。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择与控制台代理关联的一组凭据的操作菜单，然后选择*配置订阅*。

您必须选择与控制台代理关联的凭据。您无法将市场订阅与与 NetApp Console 关联的凭据关联。

4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭据与新订阅关联，请选择“添加订阅”>“继续”，然后按照 Azure 市场中的步骤操作：
 - a. 如果出现提示，请登录您的 Azure 帐户。
 - b. 选择*订阅*。

- c. 填写表格并选择*订阅*。
- d. 订阅过程完成后，选择*立即配置帐户*。

您将被重定向到NetApp Console。

- e. 从“订阅分配”页面：

- 选择您想要与此订阅关联的控制台组织或帐户。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

编辑凭据

在控制台中编辑您的 Azure 凭据。例如，如果为服务主体应用程序创建了新的密钥，您可以更新客户端密钥。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择一组凭证的操作菜单，然后选择*编辑凭证*。
4. 进行所需的更改，然后选择*应用*。

删除凭据

如果您不再需要一组凭证，您可以删除它们。您只能删除与系统无关的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 在*组织凭证*页面上，选择一组凭证的操作菜单，然后选择*删除凭证*。
4. 选择*删除*进行确认。

版权信息

版权所有 © 2026 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，本文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。