



AWS

Cloud Manager

NetApp
October 19, 2021

目 录

AWS	1
AWS 凭据和权限	1
管理 Cloud Manager 的 AWS 凭据和权限	3

AWS

AWS 凭据和权限

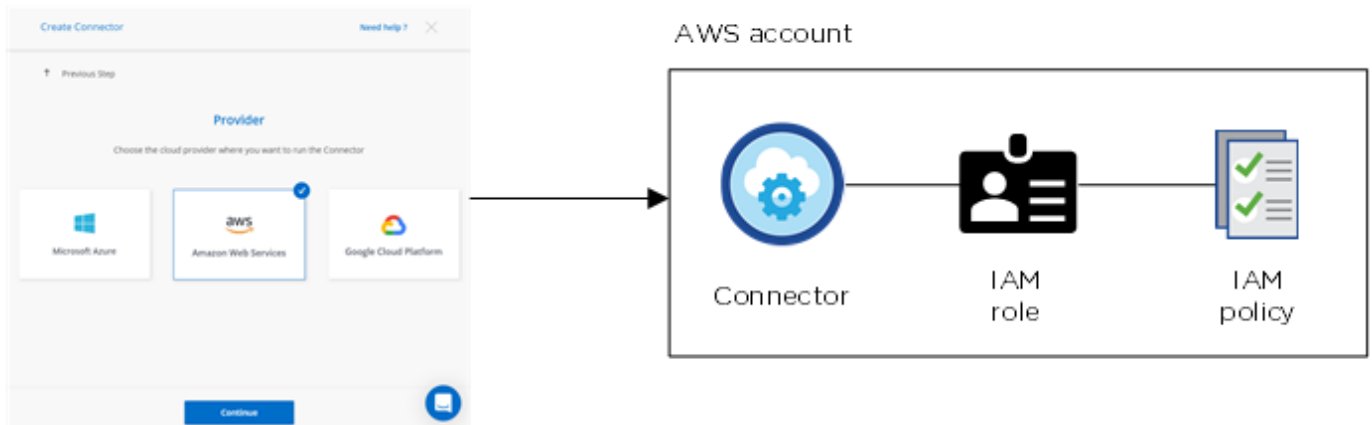
通过 Cloud Manager，您可以部署 Cloud Volumes ONTAP 要使用的 AWS 凭据。您可以使用初始 AWS 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭据。

初始 AWS 凭据

从 Cloud Manager 部署 Connector 时，需要使用有 Connector 实例的 AWS 账户。中列出了所需的权限 ["AWS 的连接器部署策略"](#)。

当 Cloud Manager 在 AWS 中部署 Connector 实例时，它会为此实例创建 IAM 角色和实例配置文件。它会附加一个策略，Cloud Manager 提供管理 AWS 账户中资源和程序的权限。 ["查看 Cloud Manager 如何使用权限"](#)。

Cloud Manager

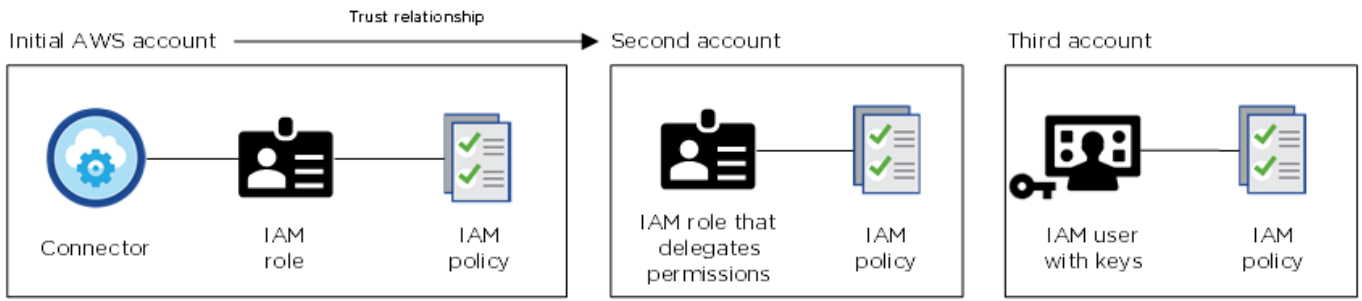


在 Cloud Volumes ONTAP 新建工作区时，Cloud Manager 会默认使用以下 AWS 凭据：

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

其他 AWS 凭据

如果您要在不同的 AWS 账户中部署 Cloud Volumes ONTAP，您可以提供一个 ["IAM 用户或信任策略中某个角色的 ARN 提供 AWS 密钥"](#)。下图显示了另外两个选项，一个通过可信策略中的 IAM 角色提供权限，一个通过 IAM 用户的 AWS 密钥提供权限：



您可以做 "将凭据添加到 Cloud Manager" 指定 IAM 角色的 Amazon 源名称（ARN）或 IAM 用户的 AWS 密钥。

添加凭据后，您可以在新建的工作环境中切换到这些凭据：

Edit Account & Add Subscription

Credentials

- Keys | Account ID: [blurred]
- Instance Profile | Account ID: [blurred]**
- QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

[+ Add Subscription](#)

Apply **Cancel**

市部署和内部部署如何？

以上各介绍了 Cloud Manager 中建的 Connector 部署方法。也可以从在 AWS 中部署连接器 "AWS Marketplace" 可以做到。

如果使用 Marketplace，会以相同方式提供。只需手动建和置 IAM 角色，然后任何其他提供即可。

于内部部署，不能 Cloud Manager 系置 IAM 角色，但可以像其他 AWS 提供限一提供限。

如何安全地 AWS 凭据？

如上所述，Cloud Manager 支持通以下几种方式提供 AWS 凭据：与 Connector 例的 IAM 角色，在可信中承担 IAM 角色或提供 AWS 密。

于前个，Cloud Manager 使用 AWS 安全令牌服取持的凭据。是最佳践—它是自的，安全的。

如果 Cloud Manager 提供了 AWS 密，定期在 Cloud Manager 中更新些密以使用。是一个完全手的程。

管理 Cloud Manager 的 AWS 凭据和

建 Cloud Volumes ONTAP 系，需要要用于系的 AWS 凭据和。如果管理多个 AWS ，可以从凭据面将其中个分配不同的 AWS 凭据。

在将 AWS 凭据添加到 Cloud Manager 之前，需要提供提供所需的限。通些限，Cloud Manager 可以管理 AWS 中的源和程。如何提供限取决于是要 Cloud Manager 提供 AWS 密是要受信任中某个角色提供 ARN。



从 Cloud Manager 部署 Connector，Cloud Manager 会自部署此 Connector 的添加 AWS 凭据。如果在有系上手安装了 Connector 件，不会添加此初始。"[了解 AWS 凭据和限](#)"。

- *
- [\[Granting permissions by providing AWS keys\]](#)
- [\[Granting permissions by assuming IAM roles in other accounts\]](#)

如何安全地 AWS 凭据？

可以通 Cloud Manager 通以下几种方式提供 AWS 凭据：与 Connector 例的 IAM 角色，在可信中担任 IAM 角色或提供 AWS 密。"[了解 AWS 凭据和限](#)"。

于前个，Cloud Manager 使用 AWS 安全令牌服取持的凭据。此程是最佳践，它是自的，并且安全。

如果 Cloud Manager 提供了 AWS 密，定期在 Cloud Manager 中更新些密以使用。是一个完全手的程。

通过提供 AWS 密钥授予权限

如果要 IAM 用户通过提供 Cloud Manager 的 AWS 密钥，则需要向用户授予所需的权限。Cloud Manager IAM 策略定义了允许云管理器使用的 AWS 操作和源。

□□

1. 从下方 Cloud Manager IAM 策略 "[Cloud Manager 策略页面](#)"。
2. 从 IAM 控制台，通过从 Cloud Manager IAM 策略控制粘文本来自建自己的策略。

"AWS 文档：创建 IAM 策略"

3. 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"

□在，此□□具有所需□限。□在，□可以将其添加到 [Cloud Manager 中](#)。

在其他□□中使用 IAM 角色来授予□限

□可以使用 IAM 角色在部署 Connector □例的源 AWS □□与其他 AWS □□之□□置信任□系。然后，□可以□ Cloud Manager 提供可信□□中 IAM 角色的 ARN 。

□□

1. □到要部署 Cloud Volumes ONTAP 的目□□□，然后□□ * 其他 AWS □□ * 来□建 IAM 角色。





□□必□行以下操作：

- □入 Connector □例所在□□的 ID 。
- 附加 Cloud Manager IAM 策略，□策略可从□得 "[Cloud Manager 策略页面](#)"。

Create role

1 2 3 4

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options Require external ID (Best practice when a third party will assume this role)
 Require MFA ⓘ

2. □到 Connector □例所在的源□□，然后□□附加到□□例的 IAM 角色。
 - a. □□ * 附加策略 *，然后□□ * □建策略 *。

b. 创建一个策略，其中包含 "STS : AssumeRole" 操作以及在目标 IAM 角色中创建的角色 ARN。

▪ 示例 *

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

在，此策略具有所需权限。在，您可以将其添加到 Cloud Manager 中。

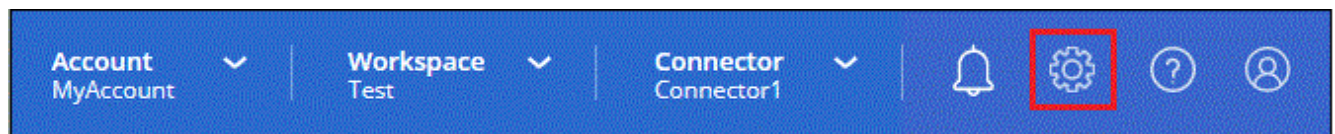
将 AWS 凭据添加到 Cloud Manager

在 AWS IAM 提供所需权限后，您可以将 IAM 角色的凭据添加到 Cloud Manager 中。一旦完成，您就可以在 Cloud Manager 中配置 Cloud Volumes ONTAP 系统。

如果您在云提供商中创建了某些凭据，您可能需要几分钟的时间才能使用这些凭据。等待几分钟，然后再将凭据添加到 Cloud Manager。

□□

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后单击 * 凭据 *。



2. 单击 * 添加凭据 * 并单击 * AWS *。

3. 提供 AWS 密钥或可信 IAM 角色的 ARN。

4. 单击已满足策略要求，然后单击 * 完成 *。

5. 单击要与凭据关联的实例，如果没有实例，单击 * 添加实例 *。


要按小时费率 (PAYGO) 或按年度合同支付 Cloud Volumes ONTAP 费用，AWS 凭据必须与 AWS Marketplace 中的 Cloud Volumes ONTAP 实例相关联。

6. 单击 * 添加 *。

在，在创建新的工作区时，您可以从 " 实例信息和凭据 " 页面切换到任一凭据：

Edit Account & Add Subscription

Credentials

Keys | Account ID: [redacted] 
Instance Profile | Account ID: [redacted]
● QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

 [Add Subscription](#)

Apply

Cancel

将 AWS 凭据与凭据

将 AWS 凭据添加到 Cloud Manager 后，您可以将 AWS Marketplace 凭据与某些凭据相关联。通常，您可以按小时率（PAYGO）或使用年度合同 Cloud Volumes ONTAP 付款，并使用其他 NetApp 云服务。

在以下情况下，您可能在将凭据添加到 Cloud Manager 后从 AWS Marketplace 删除：

- 最初将凭据添加到 Cloud Manager 时，您未选择。
- 您希望将现有 AWS Marketplace 凭据替换为新凭据。

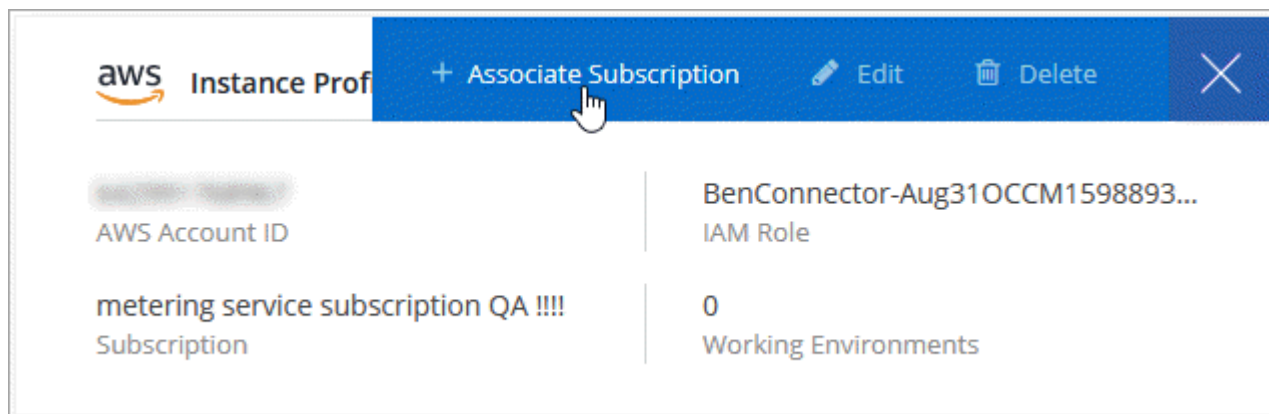
您需要先创建 Connector，然后才能更改 Cloud Manager 配置。 ["了解如何操作"](#)。

□□

1. 在 Cloud Manager 控制台的右上角，单击配置，然后单击 * 凭据 *。

2. 将鼠标停在一凭据上，然后操作菜单。

3. 从菜单中， * * 。



4. 从下拉列表中 * 或 * 添加 * ，然后按照 * 建新 * 。

► https://docs.netapp.com/zh-cn/occm//media/video_subscribing_aws.mp4 (video)

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.