



采用 **ONTAP** 的 **RBAC**

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目录

- 采用 ONTAP 的 RBAC 1
 - ONTAP RBAC 如何与 ONTAP tools 配合使用 1
 - 管理选项概述 1
 - 使用 ONTAP REST 角色 1
 - ONTAP tools 的 ONTAP RBAC 注意事项 2
 - 配置流程概述 2
 - 使用 System Manager 配置角色 2

采用 ONTAP 的 RBAC

ONTAP RBAC 如何与 ONTAP tools 配合使用

ONTAP 提供强大且可扩展的 RBAC 环境。您可以使用 RBAC 功能来控制对通过 REST API 和 CLI 公开的存储及系统操作的访问。在将其用于 ONTAP tools for VMware vSphere 10 部署之前，熟悉该环境很有帮助。

管理选项概述

使用 ONTAP RBAC 时有几种可用选项，具体取决于您的环境和目标。以下是主要管理决策的概述。另请参见 ["ONTAP 自动化：RBAC 安全概述"](#) 以了解更多信息。



ONTAP RBAC 是针对存储环境量身定制的，比 vCenter Server 提供的 RBAC 实现更简单。使用 ONTAP，您可以将角色直接分配给用户。ONTAP RBAC 不需要配置显式权限，例如与 vCenter Server 一起使用的权限。

角色类型和权限

定义 ONTAP 用户时需要 ONTAP 角色。ONTAP 角色有两种类型：

- REST

REST 角色是在 ONTAP 9.6 中引入的，通常应用于通过 REST API 访问 ONTAP 的用户。这些角色中包含的权限是根据对 ONTAP REST API 端点和相关操作的访问权限来定义的。

- 传统

这些是 ONTAP 9.6 之前存在的旧角色。它们仍然是 RBAC 的基础方面。权限是根据对 ONTAP CLI 命令的访问来定义的。

虽然 REST 角色是最近引入的，但传统角色提供了一些优势。例如，可以包括其他查询参数，以便让 Privileges 更准确地定义它们应用的对象。

范围

ONTAP 角色可以使用两种不同的作用域之一进行定义。它们可以应用于特定的数据 SVM（SVM 级别）或整个 ONTAP 集群（集群级别）。

角色定义

ONTAP 在集群和 SVM 级别提供了一组预定义的角色。您还可以定义自定义角色。

使用 ONTAP REST 角色

使用 ONTAP tools for VMware vSphere 10 附带的 ONTAP REST 角色时，需要考虑以下几点。

角色映射

无论是使用传统角色还是 REST 角色，所有 ONTAP 访问决策都是基于底层 CLI 命令做出的。但是，由于 REST 角色中的权限是根据 REST API 端点定义的，因此 ONTAP 需要为每个 REST 角色创建一个 `_mapped_` 传统角色。因此，每个 REST 角色都映射到一个底层传统角色。这使 ONTAP 能够以一致的方式做出访问控制决

策，而不受角色类型的影响。您无法修改并行映射的角色。

使用 CLI 权限定义 REST 角色

由于 ONTAP 始终使用 CLI 命令来确定基本级别的访问，因此可以使用 CLI 命令权限而不是 REST 端点来表示 REST 角色。此方法的一个好处是传统角色具有额外的粒度。

定义 ONTAP 角色时的管理界面

您可以使用 ONTAP CLI 和 REST API 创建用户和角色。但是，使用 System Manager 界面以及通过 ONTAP tools Manager 提供的 JSON 文件更为方便。有关详细信息，请参见 ["将 ONTAP RBAC 与 ONTAP tools for VMware vSphere 10 结合使用"](#)。

ONTAP tools 的 ONTAP RBAC 注意事项

在生产环境中使用 ONTAP tools for VMware vSphere 10 与 ONTAP 的 RBAC 实现之前，您应该考虑以下几个方面。

配置流程概述

ONTAP tools for VMware vSphere 支持创建具有自定义角色的 ONTAP 用户。这些定义打包在一个 JSON 文件中，您可以将其上传到 ONTAP 集群。您可以创建用户并根据您的环境 and 安全需求定制角色。

主要配置步骤在下文中进行了高层次的描述。有关更多详细信息，请参见 ["配置 ONTAP 用户角色和权限"](#)。

1. 准备

您需要具有 ONTAP tools Manager 和 ONTAP 集群的管理凭据。

2. 下载 JSON 定义文件

登录到 ONTAP tools Manager 用户界面后，您可以下载包含 RBAC 定义的 JSON 文件。

3. 创建具有角色的 ONTAP 用户

登录到 System Manager 后，可以创建用户和角色：

1. 在左侧选择 **Cluster**，然后选择 **Settings**。
2. 向下滚动到*用户和角色*，然后单击 **→**。
3. 选择*用户*下的*添加*，然后选择*虚拟化产品*。
4. 选择本地工作站上的 JSON 文件并上传。

4. 配置角色

作为定义角色的一部分，您需要做出几个管理决策。有关更多详细信息，请参见 [使用 System Manager 配置角色](#)。

使用 System Manager 配置角色

开始使用 System Manager 创建新用户和角色并上传 JSON 文件后，您可以根据环境和需求自定义角色。

核心用户和角色配置

RBAC 定义被打包为多种产品功能，包括 VSC、VASA Provider 和 SRA 的组合。您应该选择需要 RBAC 支持的一个或多个环境。例如，如果希望角色支持远程插件功能，请选择 VSC。您还需要选择用户名和相关密码。

权限

角色权限根据 ONTAP 存储所需的访问级别分为四组。角色所基于的权限包括：

- 发现

通过此角色，您可以添加存储系统。

- 创建存储

此角色使您能够创建存储。它还包括与发现角色相关联的所有 Privileges。

- 修改存储

此角色使您能够修改存储。它还包括与发现和创建存储角色关联的所有 Privileges。

- 销毁存储

此角色使您能够销毁存储。它还包括与发现、创建存储和修改存储角色关联的所有 Privileges。

生成具有角色的用户

为您的环境选择配置选项后，单击 **Add**，ONTAP 将创建用户和角色。所生成角色的名称是以下值的串联：

- JSON 文件中定义的常量前缀值（例如"OTV_10"）
- 您选择的产品功能
- 权限集列表。

示例

OTV_10_VSC_Discovery_Create

新用户将被添加到"用户和角色"页面上的列表中。请注意，HTTP 和 ONTAPI 用户登录方法均受支持。

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。