



使用 **VMware vSphere** 的 **RBAC**

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目录

- 使用 VMware vSphere 的 RBAC 1
 - vCenter 服务器 RBAC 如何与 ONTAP tools 配合使用 1
 - vCenter Server 权限的图示 1
 - vCenter Server 权限的组成部分 1
- ONTAP tools 的 vCenter Server RBAC 注意事项 2
 - vCenter 角色和管理员帐户 2
 - vSphere 对象层次结构 2
 - ONTAP tools for VMware vSphere 10 中包含的角色 2
 - vSphere 对象和 ONTAP 存储后端 6
 - 使用 vCenter Server RBAC 6

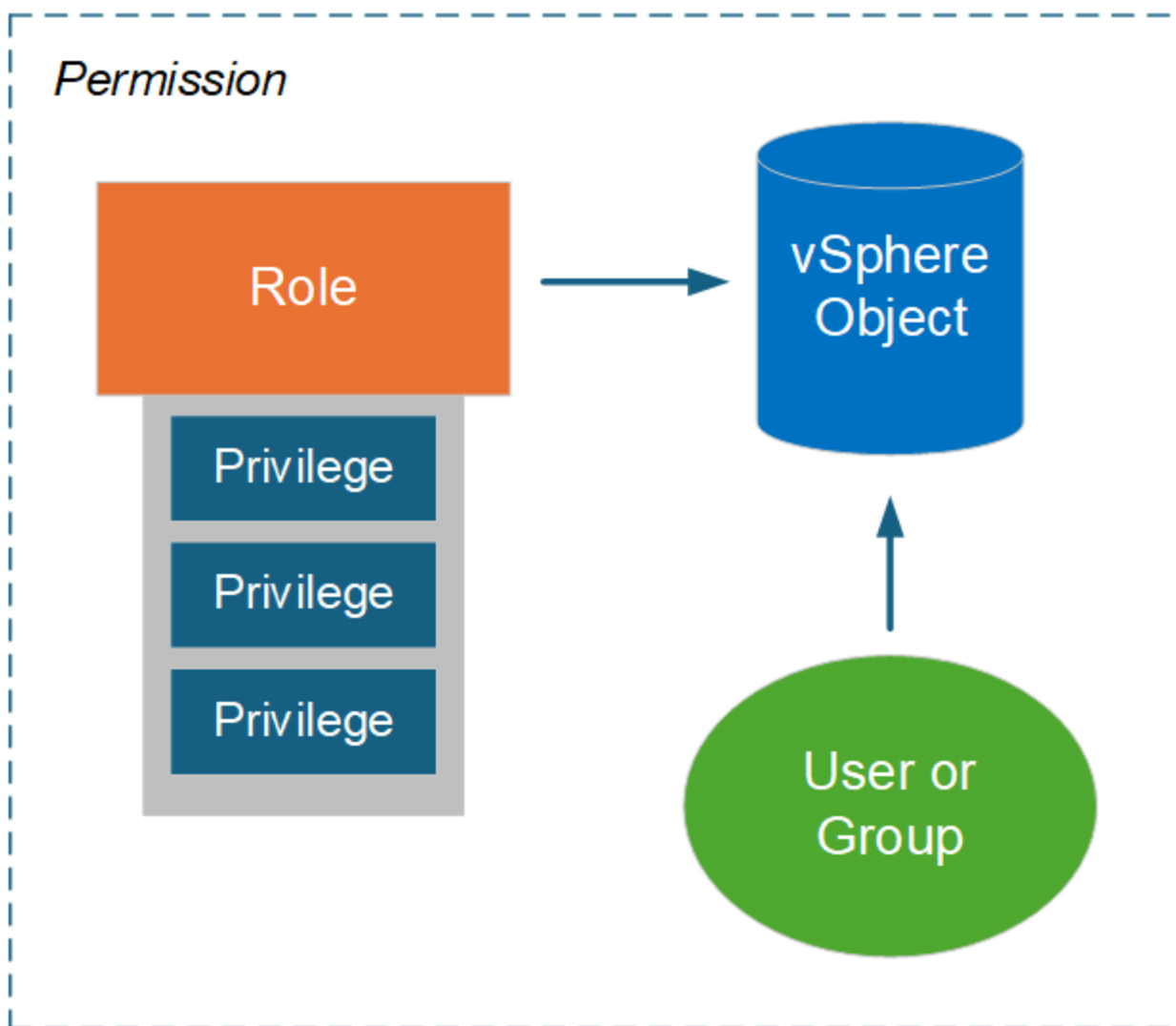
使用 VMware vSphere 的 RBAC

vCenter 服务器 RBAC 如何与 ONTAP tools 配合使用

VMware vCenter Server 提供 RBAC 功能，使您能够控制对 vSphere 对象的访问。它是 vCenter 集中式身份验证和授权安全服务的重要组成部分。

vCenter Server 权限的图示

权限是在 vCenter Server 环境中实施访问控制的基础。它应用于权限定义中包含用户或组的 vSphere 对象。下图提供了 vCenter 权限的高级示意图。



vCenter Server 权限的组成部分

A vCenter Server 权限是创建权限时绑定在一起的多个组件的集合。

vSphere 对象

权限与 vSphere 对象相关联，例如 vCenter Server、ESXi 主机、虚拟机、数据存储区、数据中心和文件夹。根据对象分配的权限，vCenter Server 确定每个用户或组可以对该对象执行哪些操作或任务。对于 ONTAP tools for VMware vSphere 的特定任务，所有权限均在 vCenter Server 的根或根文件夹级别进行分配和验证。有关详细信息，请参见 ["将 RBAC 与 vCenter 服务器结合使用"](#)。

Privileges 和角色

与 ONTAP tools for VMware vSphere 10 配合使用的 vSphere Privileges 有两种类型。为了简化在此环境中使用 RBAC，ONTAP tools 提供了包含所需本机和自定义 Privileges 的角色。这些 Privileges 包括：

- 原生 vCenter Server Privileges

这些是 vCenter Server 提供的 Privileges。

- ONTAP tools 特定 Privileges

这些是 ONTAP tools for VMware vSphere 特有的自定义 Privileges。

用户和组

可以使用 Active Directory 或本地 vCenter Server 实例定义用户和组。结合角色，可以在 vSphere 对象层次结构中的对象上创建权限。权限根据关联角色中的权限授予访问权限。请注意，角色不会单独直接分配给用户。相反，作为更大的 vCenter Server 权限的一部分，用户和组通过角色权限获得对对象的访问权限。

ONTAP tools 的 vCenter Server RBAC 注意事项

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

vCenter 角色和管理员帐户

只有在需要限制对 vSphere 对象和相关管理任务的访问时，才需要定义和使用自定义 vCenter Server 角色。如果不需要限制访问，则可以使用管理员帐户。每个管理员帐户都在对象层次结构的顶级定义了 Administrator 角色。这提供了对 vSphere 对象的完全访问权限，包括由 ONTAP tools for VMware vSphere 10 添加的对象。

vSphere 对象层次结构

vSphere 对象清单按层次结构组织。例如，您可以按如下方式向下移动层次结构：

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

所有权限均在 vSphere 对象层次结构中进行验证，但 VAAI 插件操作除外，这些操作针对目标 ESXi 主机进行验证。

ONTAP tools for VMware vSphere 10 中包含的角色

为了简化与 vCenter Server RBAC 的工作，ONTAP tools for VMware vSphere 提供了针对各种管理任务的预定义角色。



如果需要，您可以创建新的自定义角色。为此，请克隆现有的 ONTAP tools 角色之一并根据需要对其进行编辑。进行配置更改后，受影响的 vSphere 客户端用户需要注销并重新登录以激活更改。

要查看 ONTAP tools for VMware vSphere 角色，请在 vSphere Client 顶部选择 **Menu**，然后单击 **Administration**，再单击左侧的 **Roles**。分配给负责部署或载入 vCenter Server 的 vCenter 用户的角色中必须包含以下 Privileges。确保将这些 Privileges 配置为部署或载入流程的先决条件。

- 报警
 - 确认报警
- 内容库
 - 添加库项
 - 签入模板
 - 查看模板
 - 下载文件
 - 导入存储
 - 读取存储
 - 同步库项
 - 同步已订阅的库
 - 查看配置设置
- 数据存储库
 - 分配空间
 - 浏览数据存储库
 - 低级别的文件操作
 - 删除文件
 - 更新虚拟机文件
 - 更新虚拟机元数据
- ESX Agent Manager
 - 查看
- 文件夹
 - 创建文件夹
- 主机
 - 配置
 - 高级设置
 - 更改设置
 - 网络配置
 - 系统资源

- 虚拟机自动启动配置
- 本地操作
 - 创建虚拟机
 - 删除虚拟机
 - 重新配置虚拟机
- 网络
 - 分配网络
 - 配置
- OvfManager
 - OvfConsumer 访问
- 主机配置文件
 - 查看
- 资源
 - 向资源池分配虚拟机
- 计划任务
 - 创建任务
 - 修改任务
 - 运行任务
- Tasks
 - 创建任务
 - 更新任务
- vApp
 - 添加虚拟机
 - 分配资源池
 - 分配 vApp
 - 创建
 - 导入
 - 移动
 - 关闭
 - 启动
 - 从 URL 拉取
 - 查看 OVF 环境
- 虚拟机
 - 更改配置

- 添加现有磁盘
- 添加新磁盘
- 添加或删除设备
- 高级配置
- 更改 CPU 计数
- 更改内存
- 更改设置
- 更改资源
- 扩展虚拟磁盘
- 修改设备设置
- 删除磁盘
- 重置访客信息
- 升级虚拟机兼容性
- 编辑清单
 - 基于现有清单创建
 - 新建
 - 移动
 - 注册
 - 删除
 - 注销
- 交互
 - 在虚拟机上执行备份操作
 - 配置 CD 介质
 - 配置软盘介质
 - 连接设备
 - 控制台交互
 - 通过 VIX API 进行访客操作系统管理
 - 关闭
 - 启动
 - 重置
 - 暂停
- 配置
 - 允许磁盘访问
 - 克隆模板

- 自定义来宾
- 部署模板
- 修改自定义规范
- 读取自定义规范
- Snapshot 管理
 - 创建 Snapshot
 - 删除快照
 - 重命名 snapshot
 - 还原为快照

有三个预定义的角色，如下所述。

NetApp ONTAP tools for VMware vSphere 管理员

提供执行核心 ONTAP tools for VMware vSphere 管理员任务所需的所有原生 vCenter Server 权限和 ONTAP tools 专属权限。

NetApp ONTAP tools for VMware vSphere 只读

提供对 ONTAP tools 的只读访问权限。这些用户无法执行任何受访问控制的 ONTAP tools for VMware vSphere 操作。

NetApp ONTAP tools for VMware vSphere 置备

提供配置存储所需的一些本机 vCenter Server Privileges 和 ONTAP tools 专用 Privileges。您可以执行以下任务：

- 创建新数据存储区
- 管理数据存储库

vSphere 对象和 ONTAP 存储后端

两个 RBAC 环境协同工作。在 vSphere 客户端界面中执行任务时，首先检查定义给 vCenter 服务器的 ONTAP tools 角色。如果 vSphere 允许该操作，则会检查 ONTAP 角色权限。第二步是根据创建和配置存储后端时分配给用户的 ONTAP 角色执行的。

使用 vCenter Server RBAC

使用 vCenter Server 权限时需要考虑以下几点。

所需权限

要访问 ONTAP tools for VMware vSphere 10 用户界面，您需要具有 ONTAP tools 专用的 *View Privileges*。如果您在未拥有此 Privileges 的情况下登录 vSphere 并单击 NetApp 图标，ONTAP tools for VMware vSphere 将显示错误消息并阻止您访问用户界面。

vSphere 对象层次结构中的分配级别决定了您可以访问用户界面的哪些部分。将 View（视图）权限分配给根对象后，您可以通过单击 NetApp 图标来访问 ONTAP tools for VMware vSphere。

您可以将"查看"权限分配给另一个较低的 vSphere 对象级别。但是，这将限制您可以访问和使用的 ONTAP tools for VMware vSphere 菜单。

正在分配权限

如果您想限制对 vSphere 对象和任务的访问，则需要使用 vCenter Server 权限。在 vSphere 对象层次结构中分配权限的位置决定了用户可以执行的 ONTAP tools for VMware vSphere 10 任务。



除非需要定义更严格的访问限制，否则通常最好在根对象或根文件夹级别分配权限。

ONTAP tools for VMware vSphere 10 提供的权限适用于自定义非 vSphere 对象，例如存储系统。如果可能，您应将这些权限分配给 ONTAP tools for VMware vSphere 根对象，因为没有可以分配给它的 vSphere 对象。例如，任何包含 ONTAP tools for VMware vSphere "添加/修改/删除存储系统" Privileges 的权限都应在根对象级别分配。

在对象层次结构中更高级别定义权限时，可以配置权限，使其传递并由子对象继承。如果需要，您可以为子对象分配其他权限，以覆盖从父对象继承的权限。

您可以随时修改权限。如果更改权限中的任何 Privileges，则与该权限关联的用户需要从 vSphere 注销并重新登录以使更改生效。

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。