VMware vSphere中的RBAC

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-tools-vmware-vsphere-10/concepts/rbac-vcenter-environment.html on August 25, 2025. Always check docs.netapp.com for the latest.

目录

VMware vSphere中的RBAC . . . 1
使用适用于VMware vSphere 10的ONTAP工具的vCenter Server RBAC环境 . . . 1
vCenter Server权限图示 . . . 1
vCenter Server权限的组成部分 . . . 2
将vCenter Server RBAC与适用于VMware vSphere 10的ONTAP工具结合使用 . . . 2
vCenter角色和管理员帐户 . . . 2
vSphere对象层次结构 . . . 2
适用于VMware vSphere 10的ONTAP工具附带的角色 . . . 3
vSphere对象和ONTAP存储后端 . . . 3
使用vCenter Server RBAC . . . 3

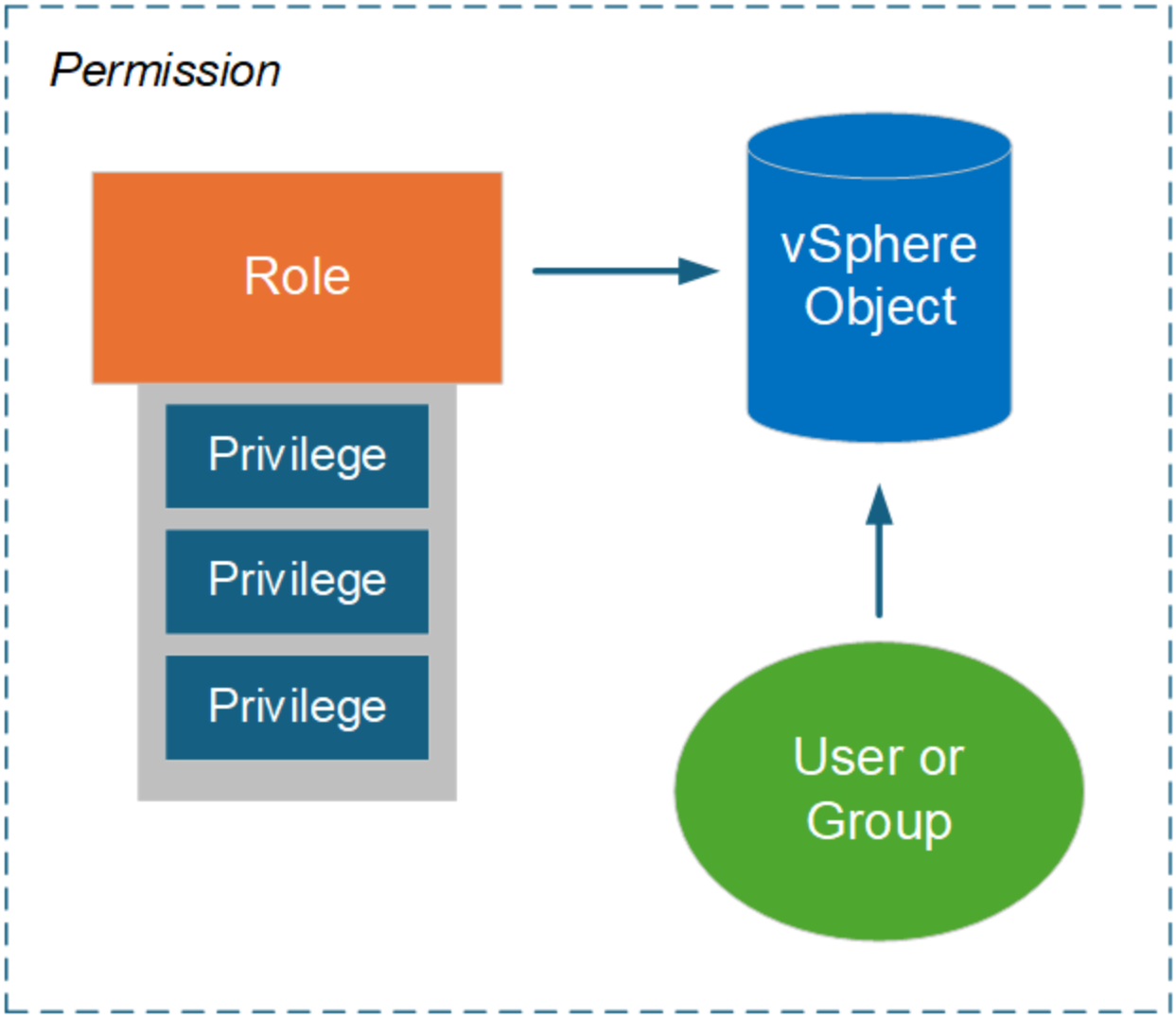
VMware vSphere中的RBAC

使用适用于VMware vSphere 10的ONTAP工具的vCenter Server RBAC环境

VMware vCenter Server提供了RBAC功能、可用于控制对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权限图示

权限是在vCenter Server环境中强制实施访问控制的基础。它将应用于权限定义中包含用户或组的vSphere对象。下图简要展示了vCenter权限。



vCenter Server权限的组成部分

vCenter Server权限是指在创建权限时绑定在一起的多个组件的软件包。

vSphere 对象

权限与vSphere对象关联、例如vCenter Server、ESXi主机、虚拟机、数据存储库、数据中心和文件夹。根据为对象分配的权限、vCenter Server可确定每个用户或组可对对象执行的操作或任务。对于适用于VMware vSphere的ONTAP工具专用的任务、所有权限都将在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 "对vCenter Server使用RBAC" 。

Privileges和角色

适用于VMware vSphere 10的ONTAP工具可使用两种类型的vSphere Privileges。为了简化在此环境中使用RBAC的过程、ONTAP工具提供了包含所需本机和自定义Privileges的角色。Privileges包括：

- 原生 vCenter Server 特权

  这些是vCenter Server提供的Privileges。

- ONTAP工具专用特权

  这些自定义Privileges是适用于VMware vSphere的ONTAP工具所特有的。

用户和组

您可以使用 Active Directory 或本地 vCenter Server 实例定义用户和组。结合角色，您可以创建对 vSphere 对象层次结构中对象的权限。该权限根据关联角色中的特权授予访问权限。请注意，角色并非直接分配给单独用户。相反，用户和组通过角色特权获得对对象的访问权限，这是更大的 vCenter Server 权限的一部分。

将vCenter Server RBAC与适用于VMware vSphere 10的ONTAP工具结合使用

在生产环境中使用适用于VMware vSphere 10的ONTAP工具之前、应考虑在vCenter Server中实施RBAC的几个方面。

vCenter角色和管理员帐户

只有在要限制对vSphere对象和关联管理任务的访问时、才需要定义和使用自定义vCenter Server角色。如果不需要限制访问、则可以改用管理员帐户。每个管理员帐户都在对象层次结构的顶层使用管理员角色进行定义。这样、您就可以完全访问vSphere对象、包括适用于VMware vSphere 10的ONTAP工具添加的对象。

vSphere对象层次结构

vSphere对象清单按层次结构进行组织。例如、您可以按如下所示向下移动层次结构：

```
vCenter Server-->-->-->-->-->-->-->-> Datacenter Cluster ESXi host-->-> Virtual Machine
```

所有权限都会在vSphere对象层次结构中进行验证、但VAAI插件操作除外、这些操作会在目标ESXi主机上进行验证。

适用于VMware vSphere 10的ONTAP工具附带的角色

为了简化vCenter Server RBAC的使用、适用于VMware vSphere的ONTAP工具提供了针对各种管理任务量身定制的预定义角色。

> 您可以根据需要创建新的自定义角色。在这种情况下、您应克隆一个现有ONTAP工具角色、并根据需要对其进行编辑。更改配置后、受影响的vSphere客户端用户需要注销并重新登录才能激活更改。

要查看适用于VMware vSphere的ONTAP工具角色、请选择vSphere Client顶部的*菜单*、然后单击*管理*、再单击左侧的*角色*。下面介绍了三种预定义角色。

适用于**VMware vSphere**管理员的**NetApp ONTAP**工具

提供执行适用于VMware vSphere的核心Privileges工具管理员任务所需的所有本机vCenter Server ONTAP和ONTAP工具专用Privileges。

适用于**VMware vSphere**的**NetApp ONTAP**工具只读

提供对ONTAP工具的只读访问权限。这些用户无法对适用于VMware vSphere的任何ONTAP工具执行受访问控制的操作。

适用于**VMware vSphere**的**NetApp ONTAP**工具配置

提供配置存储所需的一些本机vCenter Server特权和ONTAP工具专用特权。您可以执行以下任务：

- 创建新数据存储库
- 管理数据存储库

vSphere对象和ONTAP存储后端

这两个RBAC环境协同工作。在vSphere客户端界面中执行任务时、系统会首先检查为vCenter Server定义的ONTAP工具角色。如果vSphere允许执行此操作、则会检查ONTAP Role Privileges。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 Privileges和权限时、需要考虑几个事项。

所需权限

要访问适用于VMware vSphere 10的ONTAP工具用户界面、您需要具有ONTAP tools-Specific _view_权限。如果您在没有此特权的情况下登录到vSphere并单击NetApp图标、则适用于VMware vSphere的ONTAP工具将显示一条错误消息、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。通过为根对象分配查看权限、您可以单击NetApp图标来访问适用于VMware vSphere的ONTAP工具。

而是可以将查看权限分配给其他较低的vSphere对象级别。但是、这会限制您可以访问和使用的适用于VMware vSphere的ONTAP工具菜单。

分配权限

如果要限制对vSphere对象和任务的访问、您需要使用vCenter Server权限。在vSphere对象层次结构中分配权限的位置决定了适用于VMware vSphere 10的ONTAP工具用户可以执行的任务。

> 除非您需要定义限制性更强的访问、否则通常最好在根对象或根文件夹级别分配权限。

适用于VMware vSphere 10的ONTAP工具提供的权限适用于自定义的非vSphere对象、例如存储系统。如果可能、您应将这些权限分配给适用于VMware vSphere的ONTAP工具根对象、因为没有可将其分配到的vSphere对象。例如、任何包含适用于VMware vSphere的ONTAP工具"添加/修改/删除存储系统"权限的权限都应在根对象级别分配。

在对象层次结构中的较高级别定义权限时、您可以配置该权限、使其向下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。如果您更改了某个权限中的任何Privileges、则与该权限关联的用户需要从vSphere中注销并重新登录才能启用此更改。

版权信息

版权所有 © 2025 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。