VMware vSphere中的RBAC

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

目录

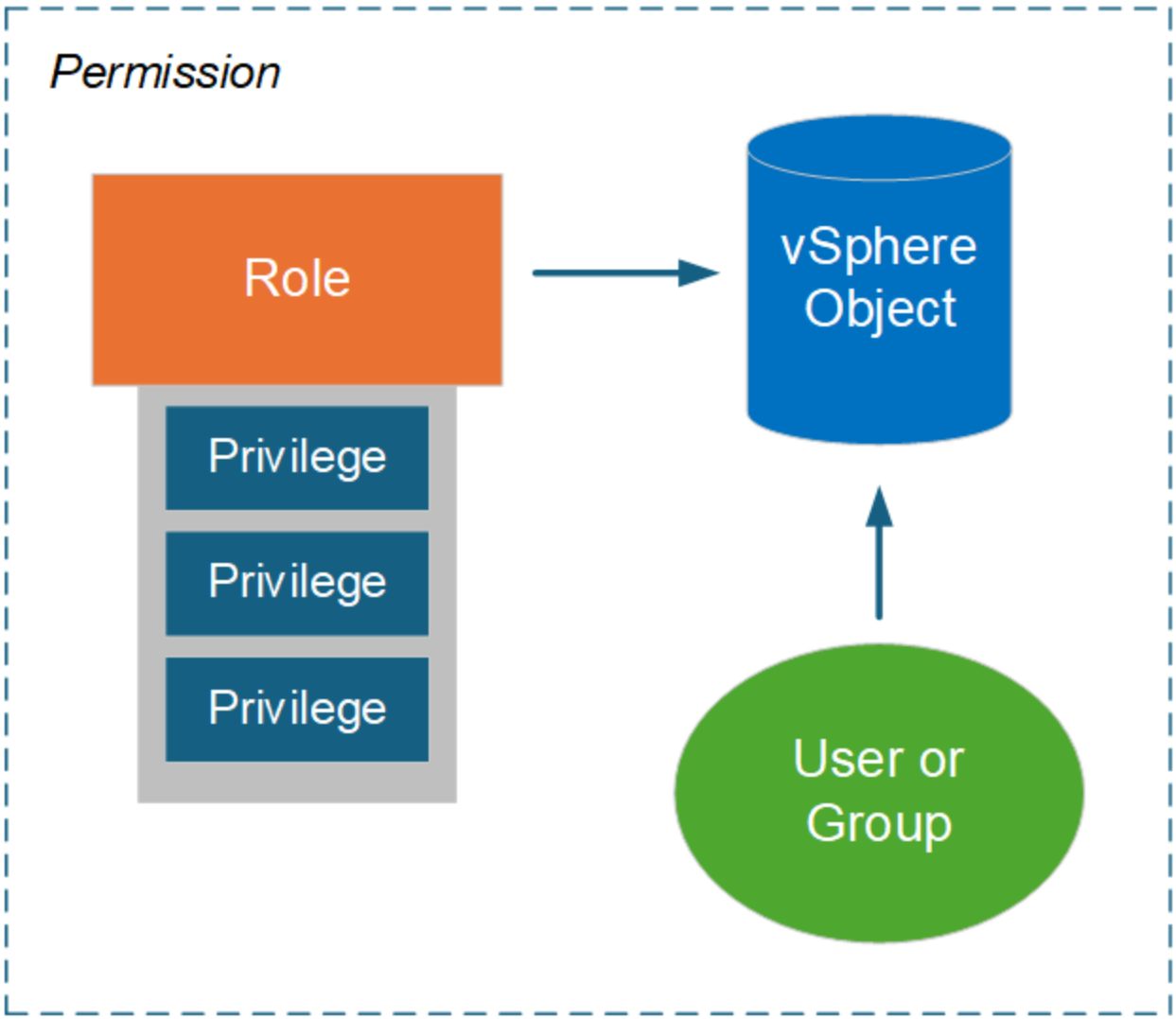
VMware vSphere中的RBAC

vCenter 服务器 RBAC 如何与 ONTAP tools 配合使用

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。

ONTAP tools 的 vCenter Server RBAC 注意事项

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ONTAP tools for VMware vSphere，请在 vSphere Client 顶部选择“菜单”，然后单击左侧的“管理”，再单击“角色”。分配给负责部署或启用 vCenter 的 vCenter 用户的角色必须包含以下权限。请确保将这些权限配置为部署或入职流程的先决条件。

- 警报
  - 确认警报
- 内容库
  - 添加库项目
  - 请在模板中签到
  - 查看模板
  - 下载文件
  - 进口存储
  - 读取存储
  - 同步库项目
  - 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 代理管理器
  - 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
    - Ovf消费者访问
- 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
    - 分配虚拟应用程序
    - 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
        - 记忆
        - 更改设置
        - 更改资源
        - 扩展虚拟磁盘
        - 修改设备设置
        - 删除磁盘
        - 重置宾客信息
        - 升级虚拟机兼容性
    - 编辑库存
        - 基于现有清单创建
        - 新建
        - 移动
        - 注册
        - 删除
        - 注销
    - 相互作用
        - 虚拟机备份操作
        - 配置 CD 介质
        - 配置软盘介质
        - 连接设备
        - 控制台交互
        - 通过 VIX API 进行客户操作系统管理
        - 关闭
        - 启动
        - 重置
        - 暂停
    - 配置
        - 允许磁盘访问
        - 克隆模板

        - 定制宾客
        - 部署模板
        - 修改定制规范
        - 读取自定义规范
    - Snapshot 管理
        - 创建 Snapshot
        - 删除快照
        - 重命名快照
        - 还原为快照

有三个预定义的角色，如下所述。

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。