基于角色的访问控制 (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目录

基于角色的访问控制 (RBAC)

了解 ONTAP tools RBAC

基于角色的访问控制 (RBAC) 是用于控制组织内资源访问的安全框架。RBAC 通过定义具有执行操作的特定权限级别的角色来简化管理，而不是将授权分配给单个用户。定义的角色被分配给用户，这有助于降低错误风险并简化整个组织的访问控制管理。

RBAC 标准模型由几种实施技术或日益复杂的阶段组成。因此，根据软件供应商及其客户的需求，实际的 RBAC 部署可能会有所不同，范围从相对简单到非常复杂。

RBAC组件

在高层次上，每个 RBAC 实施中通常包含几个组件。作为定义授权流程的一部分，这些组件以不同的方式绑定在一起。

权限

privilege 是可以允许或拒绝的操作或功能。它可能是一些简单的东西，例如读取文件的能力，或特定于给定软件系统的更抽象的操作。还可以定义 Privileges 来限制对 REST API 端点和 CLI 命令的访问。每个 RBAC 实现都包含预定义的 privileges，并且可能还允许管理员创建自定义 privileges。

角色

role 是包含一个或多个权限的容器。角色通常根据特定任务或工作职能来定义。将角色分配给用户时，用户将被授予该角色中包含的所有权限。与权限一样，实现包括预定义的角色，并且通常允许创建自定义角色。

对象

object 表示在 RBAC 环境中标识的真实或抽象资源。通过权限定义的操作在关联对象上执行，或与关联对象一起执行。根据实现情况，可以向对象类型或特定对象实例授予权限。

用户和组

Users 被分配或与身份验证后应用的角色相关联。某些 RBAC 实现仅允许将一个角色分配给用户，而其他实现则允许为每个用户分配多个角色，一次可能只有一个角色处于活动状态。将角色分配给 *groups* 可以进一步简化安全管理。

权限

permission 是将用户或组以及角色绑定到对象的定义。权限对于分层对象模型非常有用，其中权限可以由层次结构中的子级选择性地继承。

两个 RBAC 环境

在使用 ONTAP tools for VMware vSphere 10 时，您需要考虑两个不同的 RBAC 环境。ONTAP tools for VMware vSphere 10 需要在 vCenter 和 ONTAP 中具有特定权限才能执行其操作。虽然 ONTAP tools 可自动执行存储管理任务，但它不会在 vCenter 或 ONTAP 中创建用户帐户。服务帐户必须由 vSphere 管理员根据需要创建。本文档为管理员分配有效管理 ONTAP tools 所需的角色和权限提供了指导。

VMware vCenter Server

VMware vCenter Server 中的 RBAC 实现用于限制对通过 vSphere 客户端用户界面公开的对象的访问。作为安装 ONTAP tools for VMware vSphere 10 的一部分，RBAC 环境已扩展为包含代表 ONTAP tools 功能的其他对

象。对这些对象的访问通过远程插件提供。有关详细信息，请参见 "vCenter Server RBAC 环境"。

ONTAP集群

ONTAP tools for VMware vSphere 10 通过 ONTAP REST API 连接到 ONTAP 集群，以执行与存储相关的操作。对存储资源的访问通过与身份验证期间提供的 ONTAP 用户相关联的 ONTAP 角色来控制。有关详细信息，请参见 "ONTAP RBAC 环境"。

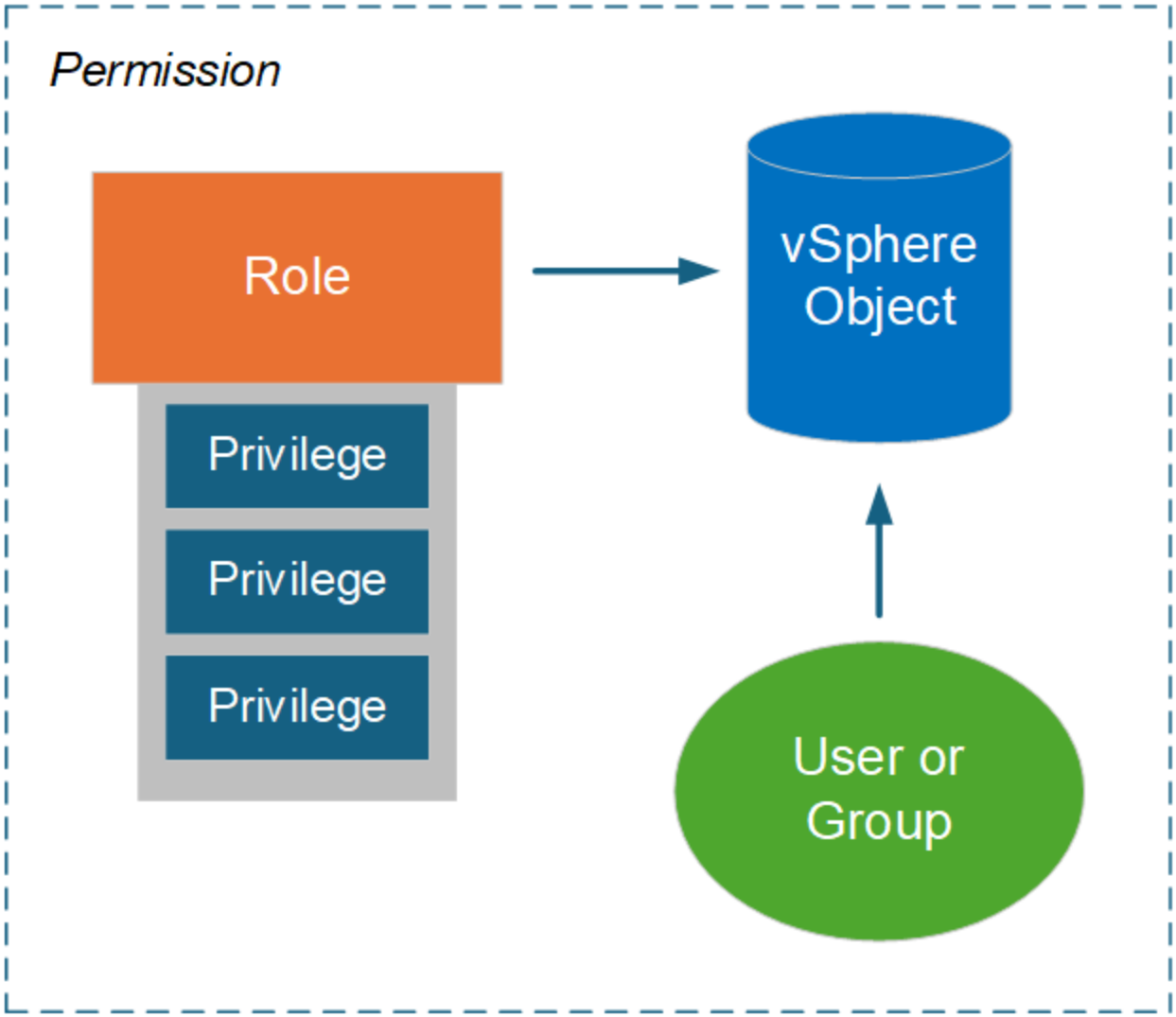
使用 VMware vSphere 的 RBAC

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。

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和安全需求定制角色。

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

商标信息