RBAC与ONTAP

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

目录

RBAC与ONTAP

ONTAP RBAC 如何与 ONTAP tools 配合使用

ONTAP提供了一个强大且可扩展的RBAC环境。您可以使用RBAC功能控制对通过REST API和命令行界面公开的存储和系统操作的访问。在将该环境与适用于VMware vSphere 10的ONTAP工具结合使用之前、熟悉该环境会很有帮助。

管理选项概述

根据您的环境和目标、使用ONTAP RBAC时有多种选项可供选择。主要行政决定概述如下。有关详细信息、另请参见 "ONTAP自动化：RBAC安全性概述"。

> ONTAP RBAC 针对存储环境进行了定制，并且比 vCenter Server 提供的 RBAC 实现更简单。使用ONTAP，您可以直接向用户分配角色。 ONTAP RBAC 不需要配置明确的权限（例如与 vCenter Server 一起使用的权限）。

角色类型和**Privileges**

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、通常适用于通过REST API访问ONTAP 的用户。这些角色中包含的Privileges是根据对ONTAP REST API端点的访问权限以及关联操作定义的。

- 传统

  这些角色是ONTAP 9.6之前的旧角色。它们仍然是RBAC的基本方面。Privileges是在访问ONTAP命令行界面命令时定义的。

虽然最近才引入了REST角色、但传统角色具有一些优势。例如、可以选择包括其他查询参数、以便Privileges更精确地定义应用这些参数的对象。

范围

可以使用两个不同的范围之一定义ONTAP角色。它们可以应用于特定数据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角色。您还可以定义自定义角色。

使用**ONTAP REST**角色

在使用适用于VMware vSphere 10的ONTAP工具附带的ONTAP REST角色时、需要注意几个事项。

角色映射

无论是使用传统角色还是REST角色、所有ONTAP访问决策都是根据底层命令行界面命令做出的。但是、由于REST角色中的Privileges是根据REST API端点定义的、因此ONTAP需要为每个REST角色创建_Mapped_传统角色。因此、每个REST角色都会映射到一个底层传统角色。这样、无论角色类型如何、ONTAP都能以一致的

方式做出访问控制决策。您不能修改并行映射的角色。

使用命令行界面**Privileges**定义**REST**角色

由于ONTAP始终使用命令行界面命令来确定基本级别的访问权限、因此可以使用命令行界面命令Privileges来表示REST角色、而不是使用REST端点。这种方法的一个优势是、可以为传统角色提供更多粒度。

定义**ONTAP**角色时的管理界面

您可以使用ONTAP命令行界面和REST API创建用户和角色。但是、使用System Manager界面以及通过ONTAP工具管理器提供的JSON文件会更方便。有关详细信息、请参见 "将ONTAP RBAC与适用于VMware vSphere 10的ONTAP工具结合使用" 。

ONTAP tools 的 ONTAP 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、您应考虑在ONTAP中实施RBAC的几个方面。

配置过程概述

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。您可以根据您的环境和安全需求创建用户并定制角色。

下面将简要介绍主要配置步骤。"配置ONTAP用户角色和权限"有关详细信息、请参见。

1.准备

您需要具有ONTAP工具管理器和ONTAP集群的管理凭据。

2.下载**JSON**定义文件

登录到ONTAP工具管理器用户界面后、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、您可以创建用户和角色：

1. 选择左侧的*Cluster*，然后选择*Settings*。
2. 向下滚动至*用户和角色*，然后单击 -→。
3. 在*USERS*下选择*ADD*，然后选择*Virtualization products*。
4. 在本地工作站上选择JSON文件并上传。

4.配置角色

在定义角色时、您需要做出多项管理决策。有关详细信息、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此角色。

核心用户和角色配置

RBAC定义会打包为多种产品功能、包括VSC、VASA Provider和SRA的组合。您应选择需要RBAC支持的环

境。例如、如果您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关联密码。

特权

根据ONTAP存储所需的访问级别、角色Privileges分为四组。这些角色所基于的Privileges包括：

- 发现

  通过此角色，您可以添加存储系统。

- 创建存储

  使用此角色可以创建存储。它还包括与发现角色关联的所有Privileges。

- 修改存储

  使用此角色可以修改存储。它还包括与发现和创建存储角色关联的所有Privileges。

- 销毁存储

  使用此角色可以销毁存储。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

选择环境的配置选项后，单击*Add*，ONTAP将创建用户和角色。生成的角色的名称由以下值串联而成：

- 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
```

新用户将添加到"用户和角色"页面的列表中。请注意、HTTP和ONTAPI用户登录方法均受支持。