RBAC与ONTAP

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-tools-vmware-vsphere-10/concepts/rbac-ontap-environment.html on September 29, 2025. Always check docs.netapp.com for the latest.

目录

RBAC与ONTAP . . . 1
使用适用于VMware vSphere 10的ONTAP工具的ONTAP RBAC环境 . . . 1
管理选项概述 . . . 1
使用ONTAP REST角色 . . . 1
将ONTAP RBAC与适用于VMware vSphere 10的ONTAP工具结合使用 . . . 2
配置过程概述 . . . 2
使用System Manager配置角色 . . . 2

RBAC与ONTAP

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

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" 。

将**ONTAP 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、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。

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。