基于角色的访问控制

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

目录

基于角色的访问控制

了解适用于VMware vSphere 10 RBAC的ONTAP工具

基于角色的访问控制(Role-Based Access Control、RBAC)是一种用于控制对组织内资源访问的安全框架。RBAC通过定义具有特定权限级别的角色来执行操作、而不是为单个用户分配授权、从而简化了管理。定义的角色会分配给用户、这有助于降低出错风险并简化整个组织的访问控制管理。

RBAC标准模型由多种实施技术或阶段组成、这些技术或阶段的复杂性不断增加。因此、根据软件供应商及其客户的需求、实际RBAC部署可能会有所不同、从相对简单到非常复杂不等。

RBAC组件

概括地说、每个RBAC实施通常都包含多个组件。在定义授权流程时、这些组件以不同方式绑定在一起。

特权

特权是指可以允许或拒绝的操作或能力。它可能是简单的操作，例如读取文件的能力，也可能是特定于特定软件系统的更抽象的操作。Privileges还可以用于限制对 REST API 端点和 CLI 命令的访问。每个 RBAC 实现都包含预定义的特权，也可能允许管理员创建自定义特权。

角色

_Role__是包含一个或多个Privileges的容器。角色通常根据特定任务或工作职能进行定义。将角色分配给用户后、系统会为该用户授予该角色中包含的所有Privileges。与Privileges一样、实施也包括预定义角色、通常允许创建自定义角色。

对象

object_表示在RBAC环境中标识的实际资源或抽象资源。通过Privileges定义的操作将在关联对象上或与关联对象一起执行。根据实施情况、可以将Privileges授予某个对象类型或特定对象实例。

用户和组

_USERS_被分配或关联到身份验证后应用的角色。某些RBAC实施仅允许为一个用户分配一个角色、而另一些则允许为每个用户分配多个角色、可能一次只允许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是将用户或组与角色绑定到对象的定义。权限对于分层对象模型非常有用、在该模型中、可以选择由层次结构中的子级继承权限。

两个RBAC环境

使用适用于VMware vSphere 10的ONTAP工具时、需要考虑两种不同的RBAC环境。

VMware vCenter Server

VMware vCenter Server中的RBAC实施用于限制对通过vSphere Client用户界面公开的对象的访问。在安装适用于VMware vSphere 10的ONTAP工具过程中、RBAC环境进行了扩展、以包括表示ONTAP工具功能的其他对象。可通过远程插件访问这些对象。有关详细信息、请参见。"vCenter Server RBAC环境"

ONTAP 集群

适用于VMware vSphere 10的ONTAP工具可通过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身份验证期间提供的与ONTAP用户关联的ONTAP角色进行控制。有关详细信息、请参见 "ONTAP RBAC环境" 。

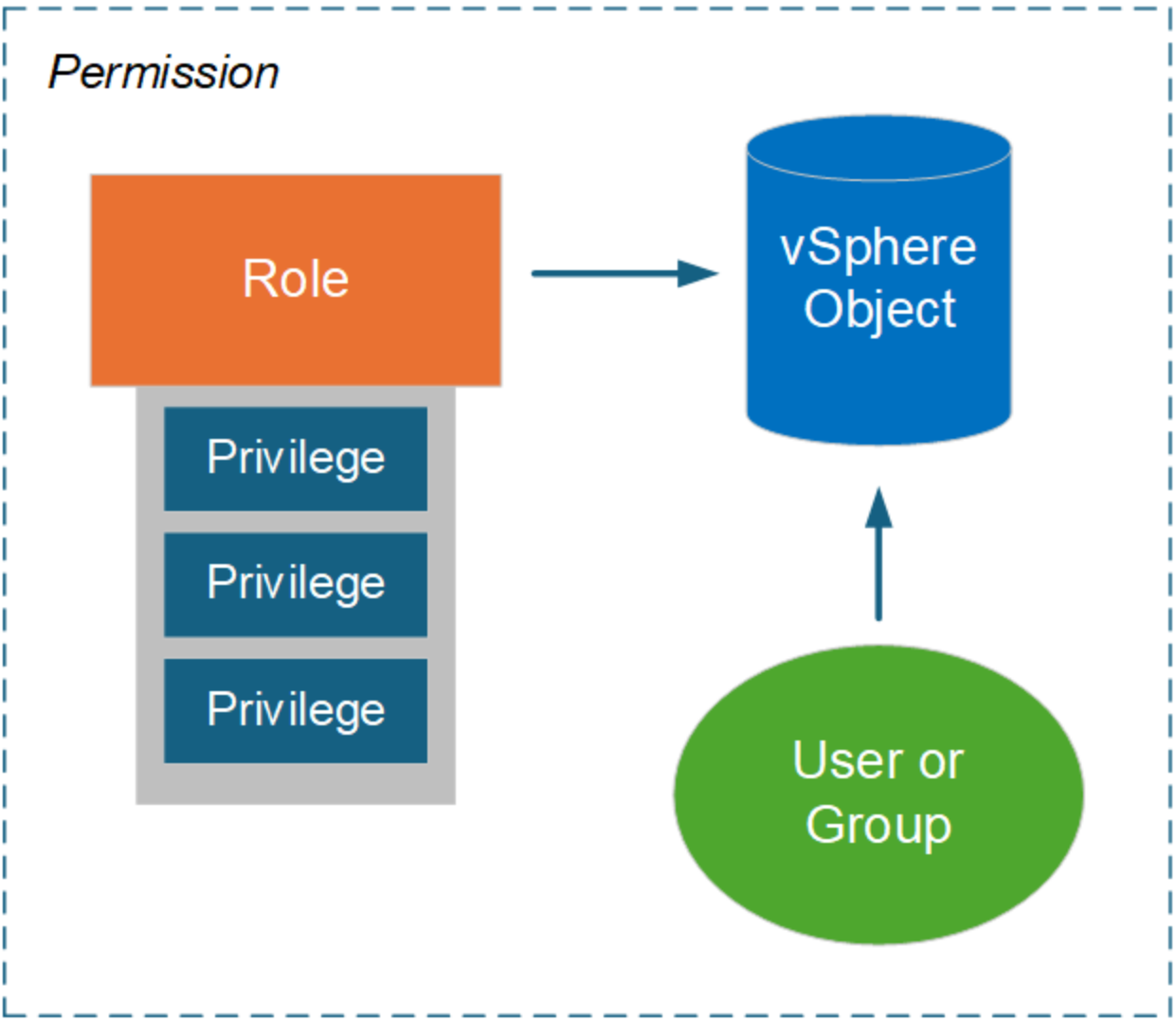
VMware vSphere中的RBAC

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。

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专为存储环境量身定制、比vCenter Server提供的RBAC实施更简单。通过ONTAP、您可以直接为用户分配角色。ONTAP RBAC不需要配置显式权限、例如用于vCenter Server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

适用于VMware vSphere 10的ONTAP工具支持创建具有自定义角色的ONTAP用户。这些定义会打包在一个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环境和安全需求定制角色。

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。