基于角色的访问控制

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

目录

基于角色的访问控制

适用于VMware vSphere的ONTAP工具中基于角色的访问控制概述

vCenter Server 提供了基于角色的访问控制（ Role-Based Access Control ， RBAC ），可用于控制对 vSphere 对象的访问。vCenter Server可使用用户和组权限以及角色和特权、在清单中的许多不同级别提供集中式身份验证和授权服务。vCenter Server具有五个用于管理RBAC的主要组件：

组件	Description
特权	通过权限可以启用或拒绝在vSphere中执行操作的访问。
角色	一个角色包含一个或多个系统权限、其中每个权限定义了对系统中某个对象或某种类型的对象的管理权限。通过为用户分配角色、该用户将继承在该角色中定义的权限的功能。
用户和组	用户和组在权限中用于从Active Directory (AD)分配角色。vCenter Server具有自己的本地用户和组、您可以使用这些用户和组。
权限	通过权限、您可以为用户或组分配权限、以便在vCenter Server中执行某些操作并对对象进行更改。vCenter Server权限仅会影响登录到vCenter Server的用户、而不会影响直接登录到ESXi主机的用户。
对象	执行操作的实体。VMware vCenter对象包括数据中心、文件夹、资源池、集群、主机、 和VM

要成功完成任务、您应具有适当的vCenter Server RBAC角色。执行任务期间、适用于VMware vSphere的ONTAP工具会先检查用户的vCenter Server角色、然后再检查用户的ONTAP权限。

vCenter Server角色适用于适用于VMware vSphere vCenter用户的ONTAP工具、而不适用于管理员。默认情况下、管理员对产品具有完全访问权限、不需要为其分配角色。

用户和组通过加入vCenter Server角色获得对某个角色的访问权限。

有关分配和修改vCenter Server角色的要点

只有在希望限制对vSphere对象和任务的访问时、才需要设置vCenter Server角色。否则，您可以以管理员身份登录。通过此登录，您可以自动访问所有 vSphere 对象。

您分配角色的位置决定了用户可以执行的适用于VMware vSphere的ONTAP工具任务。您可以随时修改一个角色。 如果更改了某个角色中的特权、则与该角色关联的用户应先注销、然后重新登录、以启用更新后的角色。

适用于**VMware vSphere**的**ONTAP**工具附带的标准角色

为了简化vCenter Server特权和RBAC的使用、适用于VMware vSphere的ONTAP工具为VMware vSphere角色提供了标准的ONTAP工具、可用于对VMware vSphere任务执行关键的ONTAP工具。此外、还有一个只读角色、可用于查看信息、但不能执行任何任务。

您可以通过单击vSphere Client主页上的*角色*来查看适用于VMware vSphere的ONTAP工具标准角色。通过适用于VMware vSphere的ONTAP工具提供的角色、您可以执行以下任务：

* 角色 *	* 问题描述 *
适用于VMware vSphere管理员的NetApp ONTAP工具	提供执行某些适用于VMware vSphere的ONTAP工具任务所需的所有本机vCenter Server特权和ONTAP工具专用特权。
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

未向vCenter Server注册ONTAP工具管理器管理员角色。此角色特定于ONTAP工具管理器。

如果贵公司要求您实施的角色比适用于VMware vSphere的标准ONTAP工具角色限制性更强、则可以使用适用于VMware vSphere的ONTAP工具创建新角色。

在这种情况下、您可以克隆VMware vSphere角色所需的ONTAP工具、然后编辑克隆的角色、使其仅具有用户所需的权限。

ONTAP存储后端和**vSphere**对象的权限

如果vCenter Server权限足够、则适用于VMware vSphere的ONTAP工具会检查与存储后端凭据(用户名和密码)关联的ONTAP RBAC特权(您的ONTAP角色)。 确定您是否有足够的权限对该存储后端执行适用于VMware vSphere的ONTAP工具任务所需的存储操作。如果您具有正确的ONTAP权限、则可以访问 存储后端并执行适用于VMware vSphere的ONTAP工具任务。ONTAP角色决定了可对存储后端执行的适用于VMware vSphere的ONTAP工具任务。

vCenter Server 权限的组成部分

vCenter Server 可识别权限，而不是权限。每个 vCenter Server 权限都包含三个组件。

vCenter Server 包含以下组件：

- 一个或多个权限（角色）

  这些权限定义了用户可以执行的任务。

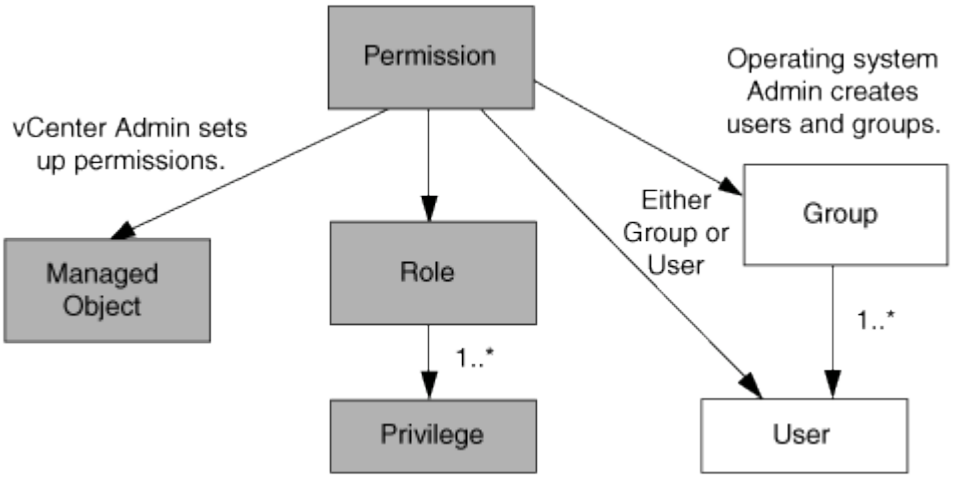
- vSphere 对象

  对象是任务的目标。

- 用户或组

  用户或组定义了谁可以执行此任务。

在此图中，灰色方框表示 vCenter Server 中的组件，白色方框表示运行 vCenter Server 的操作系统中的组件。



特权

适用于 VMware vSphere 的 ONTAP 工具具有两种特权：

- 原生 vCenter Server 特权

  这些特权随 vCenter Server 一起提供。

- ONTAP工具专用特权

  这些特权是为适用于VMware vSphere的特定ONTAP工具任务定义的。它们是适用于VMware vSphere的ONTAP工具所特有的。

适用于VMware vSphere的ONTAP工具任务需要ONTAP工具专用特权和vCenter Server本机特权。这些权限构成用户的 "`role` " 。一个权限可以具有多个权限。这些特权适用于已登录到 vCenter Server 的用户。

为了简化vCenter Server RBAC的使用、适用于VMware vSphere的ONTAP工具提供了多个标准角色、这些角色包含执行适用于VMware vSphere的ONTAP工具任务所需的所有ONTAP工具专用特权和本机特权。

如果更改了某个权限中的权限，则与该权限关联的用户应先注销，然后再登录以启用更新后的权限。

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。您可以为任何 vSphere 对象分配权限。根据分配给 vSphere 对象的权限， vCenter Server 可确定谁可以对该对象执行哪些任务。对于适用于VMware vSphere的ONTAP工具的特定任务、只会在根文件夹级别(vCenter Server)分配和验证权限、而不会在任何其他实体上分配和验证权限。但VAAI插件操作除外、在该插件操作中、系统会对相关ESXi主机验证权限。

用户和组

您可以使用 Active Directory （或本地 vCenter Server 计算机）设置用户和用户组。然后、您可以使用vCenter Server权限为这些用户或组授予访问权限、使其能够对VMware vSphere任务执行特定的ONTAP工具。

这些vCenter Server权限适用于适用于VMware vSphere vCenter用户的ONTAP工具、而不适用于适用于VMware vSphere管理员的ONTAP工具。默认情况下、适用于VMware vSphere管理员的ONTAP工具对产品具有完全访问权限、不需要为其分配权限。

没有为用户和组分配角色。他们通过加入 vCenter Server 权限来获得某个角色的访问权限。

分配和修改vCenter Server的权限

在使用 vCenter Server 权限时，需要牢记几个要点。适用于 VMware vSphere 的 ONTAP 工具任务是否成功取决于您分配权限的位置或用户在修改权限后执行的操作。

分配权限

只有在希望限制对 vSphere 对象和任务的访问时，才需要设置 vCenter Server 权限。否则，您可以以管理员身份登录。通过此登录，您可以自动访问所有 vSphere 对象。

您分配权限的位置决定了用户可以执行的适用于VMware vSphere的ONTAP工具任务。

有时、为了确保任务完成、您应在更高级别(如根对象)分配权限。如果任务需要的权限不适用于特定 vSphere 对象（例如跟踪任务），或者所需权限适用场景非 vSphere 对象（例如存储系统），则会出现这种情况。

在这种情况下，您可以设置权限，使其由子实体继承。您还可以为子实体分配其他权限。分配给子实体的权限始终会覆盖从父实体继承的权限。这意味着、您可以为子实体授予权限、以限制分配给根对象并由子实体继承的权限的范围。

除非贵公司的安全策略要求限制性更强的权限，否则最好为根对象（也称为根文件夹）分配权限。

权限和非 vSphere 对象

您创建的权限将应用于非vSphere对象。例如，存储系统不是 vSphere 对象。如果您拥有对存储系统执行适用场景的权限、则应将包含此权限的权限分配给适用于VMware vSphere的ONTAP工具根对象、因为没有可分配此权限的vSphere对象。

例如、任何包含适用于VMware vSphere的ONTAP工具等特权的权限"添加/修改/跳过存储系统"都应分配给根对象级别。

修改权限

您可以随时修改一个权限。

如果更改了某个权限中的权限，则与该权限关联的用户应先注销，然后重新登录，以启用更新后的权限。

适用于**VMware vSphere**的**ONTAP**工具任务所需的特权

不同的适用于VMware vSphere的ONTAP工具任务需要不同的特权组合、这些特权组合特定于适用于VMware vSphere的ONTAP工具、而本机vCenter Server特权则不同。

要访问适用于VMware vSphere的ONTAP工具图形用户界面、您应在正确的vSphere对象级别分配产品级的ONTAP工具专用查看特权。如果您不使用此权限登录、则在单击NetApp图标时、适用于VMware vSphere的ONTAP工具会显示一条错误消息、并阻止您访问ONTAP工具。

以*view*权限，您可以访问适用于VMware vSphere的ONTAP工具。此权限不允许您在适用于VMware vSphere的ONTAP工具中执行任务。要执行适用于VMware vSphere的任何ONTAP工具任务、您应具有执行这些任务所需的正确ONTAP工具专用特权和本机vCenter Server特权。

分配级别决定了您可以查看的 UI 部分。通过为根对象(文件夹)分配查看权限、您可以通过单击NetApp图标进入适用于VMware vSphere的ONTAP工具。

您可以将查看权限分配给其他vSphere对象级别、但这样做会限制适用于VMware vSphere的ONTAP工具菜单的显示和使用。

建议将根对象分配给包含查看权限的任何权限。

适用于**VMware vSphere**的**ONTAP**工具的建议**ONTAP**角色

您可以设置多个建议的 ONTAP 角色，以便使用适用于 VMware vSphere 的 ONTAP 工具和基于角色的访问控制（ Role-Based Access Control ， RBAC ）。这些角色包含通过适用于VMware vSphere的ONTAP工具执行存储操作所需的ONTAP特权。

要创建新用户角色、您应以运行ONTAP的存储系统的管理员身份登录。您可以使用ONTAP System Manager 9.8P1或更高版本创建ONTAP 角色。

每个ONTAP角色都有一个关联的用户名和密码对、这些用户名和密码对构成该角色的凭据。如果不使用这些凭据登录，则无法访问与此角色关联的存储操作。

作为一项安全措施、适用于VMware vSphere的ONTAP工具的特定ONTAP角色会按分层结构进行排序。这意味着、第一个角色的限制性最强、并且只具有与用于VMware vSphere存储操作的一组最基本的ONTAP工具关联的特权。下一个角色包括其自身的特权以及与上一个角色关联的所有特权。对于支持的存储操作、每个附加角色的限制都较小。

以下是使用适用于VMware vSphere的ONTAP工具时建议使用的一些ONTAP RBAC角色。创建这些角色后、您可以将其分配给必须执行与存储相关的任务(例如配置虚拟机)的用户。

* 角色 *	特权
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。此角色还包括与发现角色关联的所有特权。
修改存储	使用此角色可以修改存储。此角色还包括与"发现"角色和"创建存储"角色关联的所有特权。
销毁存储	使用此角色可以销毁存储。此角色还包括与"发现"角色、"创建存储"角色和"修改存储"角色关联的所有特权。

如果您要使用适用于VMware vSphere的ONTAP工具、则还应设置基于策略的管理(PBM)角色。通过此角色，您可以使用存储策略管理存储。此角色还要求您设置 `Discovery` 角色。