



基于角色的访问控制

ONTAP tools for VMware vSphere 9.10

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-tools-vmware-vsphere-910/concepts/concept_vcenter_server_role_based_access_control_features_in_vsc_for_vmware_vsphere.html on January 18, 2024. Always check docs.netapp.com for the latest.

目录

- 基于角色的访问控制..... 1
 - ONTAP 工具中基于角色的访问控制概述..... 1
 - vCenter Server 权限的组成部分..... 1
 - 有关为 vCenter Server 分配和修改权限的要点..... 3
 - ONTAP 工具附带的标准角色..... 4
 - VSC 任务所需的特权..... 5
 - ONTAP 存储系统和 vSphere 对象的权限..... 5
 - 如何为适用于 VMware vSphere 的 ONTAP 工具配置 ONTAP 基于角色的访问控制..... 7

基于角色的访问控制

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。在适用于 VMware vSphere 的 ONTAP ® 工具中，vCenter Server RBAC 可与 ONTAP RBAC 结合使用，以确定特定用户可以对特定存储系统上的对象执行哪些 VSC 任务。

要成功完成任务，您必须具有适当的 vCenter Server RBAC 权限。在执行任务期间，VSC 会先检查用户的 vCenter Server 权限，然后再检查用户的 ONTAP 权限。

您可以对根对象（也称为根文件夹）设置 vCenter Server 权限。然后，您可以通过限制不需要这些权限的子实体来细化安全性。

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。

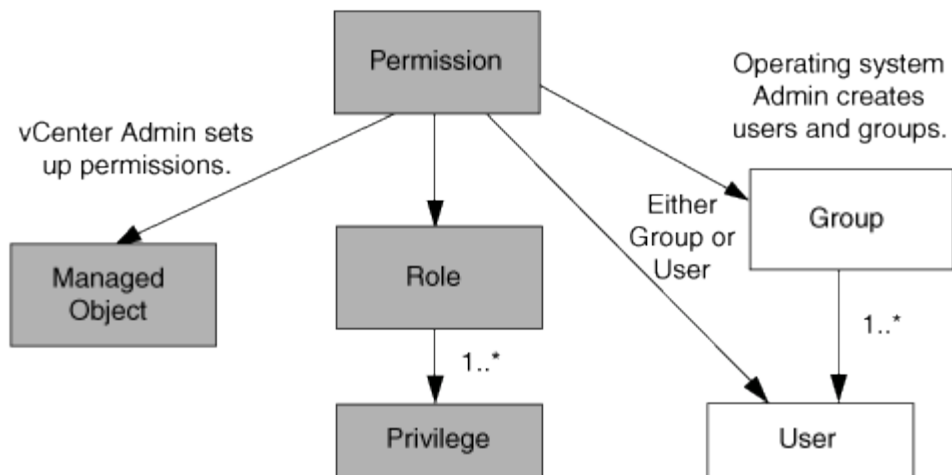
- 用户或组

用户或组定义了谁可以执行此任务。

如下图所示，要获得权限，您必须具备所有三个要素。



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 工具有两种特权：

- 原生 vCenter Server 特权

这些特权随 vCenter Server 一起提供。

- VSC 专用特权

这些特权是为特定 VSC 任务定义的。它们是 VSC 特有的。

VSC 任务既需要 VSC 专用特权，也需要 vCenter Server 原生特权。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，VSC 提供了几个标准角色，其中包含执行 VSC 任务所需的所有 VSC 专用特权和原生特权。

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。

* 权限 *	* 角色 *	* 任务 *
NetApp ONTAP Tools 控制台 > 查看	<ul style="list-style-type: none"> • VSC 管理员 • VSC 配置 • VSC 只读 	所有 VSC 和 VASA Provider 专用任务都需要查看权限。
NetApp Virtual Storage Console > 基于策略的管理 > 管理或 privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > 管理	VSC 管理员	与存储功能配置文件和阈值设置相关的 VSC 和 VASA Provider 任务。

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 VSC 专用任务，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。VAAI 插件操作除外，其中会针对相关 ESXi 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，使其能够执行特定的 VSC 任务。



这些 vCenter Server 权限适用于 VSC vCenter 用户，而不适用于 VSC 管理员。默认情况下，VSC 管理员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。

有关为 vCenter Server 分配和修改权限的要点

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 VSC 任务。

有时，为了确保任务完成，您必须在更高的级别分配权限，例如根对象。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，您可以通过对子实体的权限来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。如果某个权限适用场景存储系统，则必须将包含该权限的权限分配给 VSC 根对象，因为没有可分配给它的 vSphere 对象。

例如，任何包含 VSC 权限 "添加 / 修改 / 跳过存储系统" 等权限的权限都必须在根对象级别分配。

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。

ONTAP 工具附带的标准角色

为了简化 vCenter Server 特权和基于角色的访问控制（ Role-Based Access Control ， RBAC ）的使用， Virtual Storage Console （ VSC ）提供了标准 VSC 角色，可用于执行关键 VSC 任务。此外，您还可以使用只读角色查看 VSC 信息，但不能执行任何任务。

标准 VSC 角色具有用户执行 VSC 任务所需的 VSC 专用特权和原生 vCenter Server 特权。此外，这些角色会进行设置，以便在所有受支持的 vCenter Server 版本中具有所需的特权。

作为管理员，您可以根据需要将这些角色分配给用户。



将 VSC 升级到最新版本时，标准角色会自动升级以使用新版本的 VSC 。

您可以单击 vSphere Client 主页页面上的 * 角色 * 来查看 VSC 标准角色。

通过 VSC 提供的角色，您可以执行以下任务：

* 角色 *	* 问题描述 *
VSC 管理员	提供执行所有 VSC 任务所需的所有原生 vCenter Server 特权和 VSC 专用特权。
VSC 只读	提供对 VSC 的只读访问权限。这些用户无法执行任何受访问控制的 VSC 操作。
VSC 配置	提供配置存储所需的所有原生 vCenter Server 特权和 VSC 专用特权。您可以执行以下任务： <ul style="list-style-type: none">• 创建新数据存储库• 销毁数据存储库• 查看有关存储功能配置文件的信息

使用 VSC 标准角色的准则

使用适用于 VMware vSphere 角色的标准 ONTAP 工具时，应遵循特定准则。

您不应直接修改标准角色。否则，每次升级 VSC 时，VSC 都会覆盖您所做的更改。每次升级 VSC 时，安装程序都会更新标准角色定义。这样可以确保角色对于您的 VSC 版本以及所有受支持的 vCenter Server 版本均为最新角色。

但是，您可以使用标准角色创建根据您的环境量身定制的角色。为此，您应复制 VSC 标准角色，然后编辑复制的角色。通过创建新角色，即使重新启动或升级 VSC Windows 服务，您也可以保持此角色。

使用 VSC 标准角色的一些方法包括：

- 对所有 VSC 任务使用标准 VSC 角色。

在这种情况下，标准角色可提供用户执行 VSC 任务所需的所有特权。

- 合并角色以扩展用户可以执行的任务。

如果标准 VSC 角色为您的环境提供的粒度过高，您可以通过创建包含多个角色的更高级别组来扩展角色。

如果用户需要执行其他需要额外原生 vCenter Server 特权的非 VSC 任务，您可以创建一个提供这些特权的角色，并将其添加到组中。

- 创建更细化的角色。

如果您的公司要求您实施比标准 VSC 角色限制性更强的角色，则可以使用 VSC 角色创建新角色。

在这种情况下，您需要克隆所需的 VSC 角色，然后编辑克隆的角色，使其仅具有用户所需的权限。

VSC 任务所需的特权

适用于 VMware vSphere 任务的不同 ONTAP 工具需要使用不同的特权组合来处理 Virtual Storage Console （VSC）和原生 vCenter Server 特权。

有关 VSC 任务所需特权的信息，请参见 NetApp 知识库文章 1032542。

["如何为 Virtual Storage Console 配置 RBAC"](#)

适用于 VMware vSphere 的 ONTAP 工具所需的产品级特权

要访问适用于 VMware vSphere GUI 的 ONTAP 工具，您必须在正确的 vSphere 对象级别分配产品级 VSC 专用的查看权限。如果您在没有此权限的情况下登录，则在单击 NetApp 图标时，VSC 会显示一条错误消息，并阻止您访问 VSC。

以下信息介绍了 VSC 产品级查看权限：

* 权限 *	* 问题描述 *	* 分配级别 *
查看	您可以访问 VSC 图形用户界面。此权限不允许您在 VSC 中执行任务。要执行任何 VSC 任务，您必须具有执行这些任务的正确 VSC 专用特权和原生 vCenter Server 特权。	<p>分配级别决定了您可以查看的 UI 部分。通过在根对象（文件夹）上分配查看权限，您可以通过单击 NetApp 图标进入 VSC。</p> <p>您可以将查看权限分配给其他 vSphere 对象级别；但是，这样做会限制您可以查看和使用的 VSC 菜单。</p> <p>建议将根对象分配给包含查看权限的任何权限。</p>

ONTAP 存储系统和 vSphere 对象的权限

通过 ONTAP 基于角色的访问控制（Role-Based Access Control，RBAC），您可以控制对特定存储系统的访问，并控制用户可以对这些存储系统执行的操作。在适用于

VMware vSphere 的 ONTAP® 工具中，ONTAP RBAC 可与 vCenter Server RBAC 结合使用，以确定特定用户可以对特定存储系统上的对象执行哪些虚拟存储控制台（VSC）任务。

VSC 使用您在 VSC 中设置的凭据（用户名和密码）对每个存储系统进行身份验证，并确定可以对该存储系统执行哪些存储操作。VSC 会为每个存储系统使用一组凭据。这些凭据决定了可以对该存储系统执行哪些 VSC 任务；换言之，这些凭据适用于 VSC，而不是适用于单个 VSC 用户。

ONTAP RBAC 仅适用于访问存储系统以及执行与存储相关的 VSC 任务，例如配置虚拟机。如果您对特定存储系统没有适当的 ONTAP RBAC 特权，则无法对该存储系统上托管的 vSphere 对象执行任何任务。您可以将 ONTAP RBAC 与 VSC 专用特权结合使用来控制用户可以执行的 VSC 任务：

- 监控和配置存储系统上的存储或 vCenter Server 对象
- 配置存储系统上的 vSphere 对象

使用具有 VSC 专用权限的 ONTAP RBAC 可提供一个面向存储的安全层，存储管理员可以对其进行管理。因此，与单独的 ONTAP RBAC 或单独的 vCenter Server RBAC 相比，您可以更精细地控制访问。例如，使用 vCenter Server RBAC 时，您可以允许 vCenterUserB 在 NetApp 存储上配置数据存储空间，同时防止 vCenterUserA 配置数据存储空间。如果特定存储系统的存储系统凭据不支持创建存储，则 vCenterUserB 和 vCenterUserA 都无法在该存储系统上配置数据存储空间。

启动 VSC 任务时，VSC 会首先验证您是否具有执行此任务的正确 vCenter Server 权限。如果 vCenter Server 权限不足以执行此任务，则 VSC 不必检查该存储系统的 ONTAP 权限，因为您未通过初始 vCenter Server 安全检查。因此，您无法访问存储系统。

如果 vCenter Server 权限足够，则 VSC 会检查与存储系统凭据（用户名和密码）关联的 ONTAP RBAC 特权（您的 ONTAP 角色）确定您是否具有足够的权限来对该存储系统执行该 VSC 任务所需的存储操作。如果您具有正确的 ONTAP 权限，则可以访问存储系统并执行 VSC 任务。ONTAP 角色决定了您可以对存储系统执行的 VSC 任务。

每个存储系统都有一组关联的 ONTAP 特权。

同时使用 ONTAP RBAC 和 vCenter Server RBAC 具有以下优势：

- 安全性

管理员可以控制哪些用户可以在细化的 vCenter Server 对象级别和存储系统级别执行哪些任务。

- 审核信息

在许多情况下，VSC 会在存储系统上提供审核跟踪，使您能够将事件追溯到执行存储修改的 vCenter Server 用户。

- 可用性

您可以在一个位置维护所有控制器凭据。

使用适用于 VMware vSphere 的 ONTAP 工具时的建议 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）。这些角色包含执行虚拟存储控制台（VSC）任务所需的存储操

作所需的 ONTAP 特权。

要创建新的用户角色，您必须以管理员身份登录到运行 ONTAP 的存储系统。您可以使用以下方法之一创建 ONTAP 角色：

- ONTAP System Manager 9.8P1 或更高版本

"配置用户角色和权限"

- 适用于 ONTAP 的 RBAC User Creator 工具（如果使用的是 ONTAP 9.6 或更早版本）

每个 ONTAP 角色都有一个关联的用户名和密码对，这两个用户名和密码对构成了该角色的凭据。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，VSC 专用的 ONTAP 角色按分层结构排序。这意味着，第一个角色的限制性最强，并且只具有与一组最基本的 VSC 存储操作关联的特权。下一个角色既包括自己的特权，也包括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性都较低。

以下是使用 VSC 时建议使用的一些 ONTAP RBAC 角色。创建这些角色后，您可以将这些角色分配给必须执行与存储相关的任务的用户，例如配置虚拟机。

1. 发现

通过此角色，您可以添加存储系统。

2. 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。

3. 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。

4. 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。

如果您使用的是适用于 ONTAP 的 VASA Provider，则还应设置基于策略的管理（Policy-Based Management，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。

如何为适用于 VMware vSphere 的 ONTAP 工具配置 ONTAP 基于角色的访问控制

如果要将基于角色的访问控制与适用于 VMware vSphere 的 ONTAP 工具结合使用，则必须在存储系统上配置 ONTAP 基于角色的访问控制（Role-Based Access Control，RBAC）。您可以使用 ONTAP RBAC 功能创建一个或多个具有有限访问权限的自定义用户帐户。

VSC 和 SRA 可以在集群级别或 Storage Virtual Machine（SVM）SVM 级别访问存储系统。如果要在集群级别添加存储系统，则必须提供管理员用户的凭据，以提供所有必需的功能。如果您要通过直接添加 SVM 详细信

息来添加存储系统，则必须注意 "vsadmin" 用户没有执行某些任务所需的所有角色和功能。

VASA Provider 只能在集群级别访问存储系统。如果特定存储控制器需要 VASA Provider，则必须在集群级别将存储系统添加到 VSC 中，即使您使用的是 VSC 或 SRA 也是如此。

要创建新用户并将集群或 SVM 连接到 ONTAP 工具，应执行以下操作：

- 创建集群管理员或 SVM 管理员角色



您可以使用以下方法之一创建这些角色：

- ONTAP System Manager 9.8P1 或更高版本

["配置用户角色和权限"](#)

- 适用于 ONTAP 的 RBAC User Creator 工具（如果使用的是 ONTAP 9.6 或更早版本）

- 使用 ONTAP 创建已分配角色并设置了相应应用程序的用户

要为 VSC 配置存储系统，您需要这些存储系统凭据。您可以通过在 VSC 中输入凭据来为 VSC 配置存储系统。每次使用这些凭据登录到存储系统时，您都将有权访问在创建凭据时在 ONTAP 中设置的 VSC 功能。

- 将存储系统添加到 VSC 中，并提供您刚刚创建的用户凭据

VSC 角色

VSC 会将 ONTAP 特权分为以下几组 VSC 角色：

- 发现

用于发现所有已连接的存储控制器

- 创建存储

用于创建卷和逻辑单元号（LUN）

- 修改存储

启用存储系统的大小调整和重复数据删除

- 销毁存储

用于销毁卷和 LUN

VASA Provider 角色

您只能在集群级别创建基于策略的管理。此角色支持使用存储功能配置文件对存储进行基于策略的管理。

SRA 角色

SRA 会在集群级别或 SVM 级别将 ONTAP 权限分为 SAN 或 NAS 角色。这样，用户就可以运行 SRM 操作。

将集群添加到 VSC 时，VSC 会对 ONTAP RBAC 角色执行初始权限验证。如果添加了直接 SVM 存储 IP，则 VSC 不会执行初始验证。VSC 会稍后在任务工作流中检查并强制实施这些特权。

版权信息

版权所有 © 2024 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。