基于角色的访问控制

ONTAP tools for VMware vSphere 9.12

NetApp
December 19, 2023

目录

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ONTAP工具任务。

要成功完成任务，您必须具有适当的 vCenter Server RBAC 权限。执行任务期间、ONTAP工具会先检查用户的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

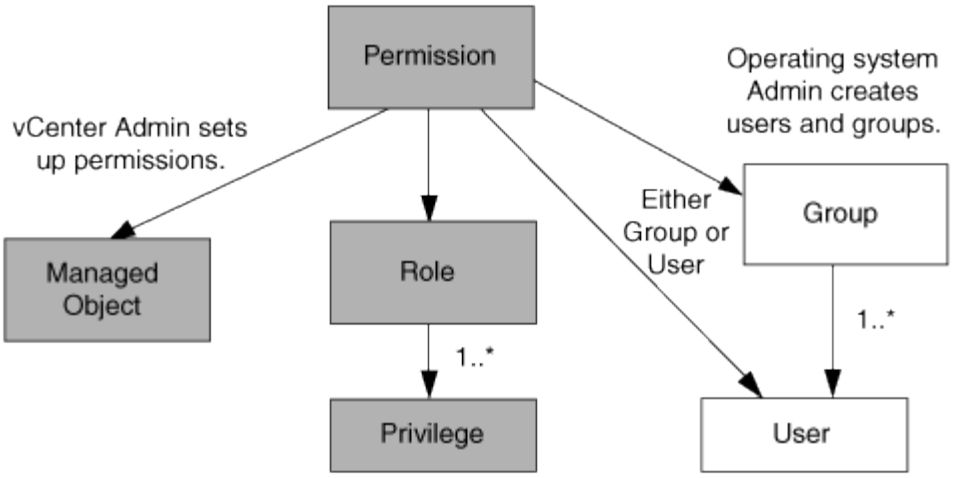
  对象是任务的目标。

- 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

  这些特权是为特定ONTAP工具任务定义的。它们是ONTAP工具所特有的。

ONTAP工具任务既需要ONTAP工具专用特权、也需要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、ONTAP工具提供了多个标准角色、这些标准角色包含执行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。

* 权限 *	* 角色 *	* 任务 *
NetApp ONTAP Tools 控制台 > 查看	• VSC管理员 • VSC 配置 • VSC 只读	所有ONTAP工具和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ONTAP工具专用任务、只能在根文件夹级别(vCenter Server)分配和验证权限、而不能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ONTAP工具任务。

这些vCenter Server权限适用于ONTAP工具vCenter用户、而不适用于ONTAP工具管理员。默认情况下、ONTAP工具管理员对产品拥有完全访问权限、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ONTAP工具任务。

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。如果您拥有对存储系统执行适用场景的权限、则必须将包含此权限的权限分配给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ONTAP工具特权"添加/修改/跳过存储系统"等特权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、ONTAP工具提供了标准ONTAP工具角色、可用于执行关键ONTAP工具任务。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。

标准ONTAP工具角色具有用户执行ONTAP工具任务所需的ONTAP工具专用特权和本机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。

在将ONTAP工具升级到最新版本时、标准角色会自动升级、以使用新版本的工具。

您可以通过单击vSphere Client主页页面上的*角色*来查看ONTAP工具标准角色。

通过ONTAP工具提供的角色、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ONTAP工具任务所需的所有本机vCenter Server特权和ONTAP工具专用特权。
VSC 只读	提供对ONTAP工具的只读访问权限。这些用户无法执行任何受访问控制的ONTAP工具操作。
VSC 配置	提供配置存储所需的所有本机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 • 销毁数据存储库 • 查看有关存储功能配置文件的信息

使用ONTAP工具标准角色的准则

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。如果这样做、ONTAP工具将在每次升级时覆盖您所做的更改。安装程序会在您每次升级ONTAP工具时更新标准角色定义。这样可以确保这些角色对于您的ONTAP工具版本以及所有受支持的vCenter Server版本都是最新的。

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。要执行此操作、您应复制ONTAP工具标准角色、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ONTAP工具Windows服务、您也可以保留此角色。

您可以通过以下方式使用ONTAP工具标准角色：

- 对所有ONTAP工具任务使用标准ONTAP工具角色。

在这种情况下、标准角色提供了用户执行ONTAP工具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ONTAP工具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非ONTAP工具任务、而这些任务需要额外的本机vCenter Server特权、您也可以创建一个角色来提供这些特权、并将其添加到组中。

- 创建更细化的角色。

  如果公司要求您实施比标准ONTAP工具角色限制性更强的角色、您可以使用ONTAP工具角色创建新角色。

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

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ONTAP工具特权和本机vCenter Server特权组合。

有关ONTAP工具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的ONTAP工具图形用户界面、您必须在正确的vSphere对象级别分配产品级的ONTAP工具专用查看特权。如果您在没有此权限的情况下登录、则在单击NetApp图标时、ONTAP工具会显示一条错误消息、并阻止您访问ONTAP工具。

在*view*权限下，您可以访问ONTAP工具图形用户界面。此权限不允许您在ONTAP工具中执行任务。要执行任何ONTAP工具任务、您必须对这些任务具有正确的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。通过在根对象(文件夹)上分配查看权限、您可以单击ONTAP图标来进入NetApp工具。

您可以将查看权限分配给其他vSphere对象级别、但这样做会限制您可以查看和使用的ONTAP工具菜单。

建议将根对象分配给包含查看权限的任何权限。

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ONTAP工具任务。

ONTAP工具使用您在ONTAP工具中设置的凭据(用户名和密码)来对每个存储系统进行身份验证、并确定可对该

存储系统执行的存储操作。ONTAP工具会为每个存储系统使用一组凭据。这些凭据决定了可在该存储系统上执行的ONTAP工具任务；换言之、这些凭据用于ONTAP工具、而不是单个ONTAP工具用户。

ONTAP RBAC仅适用于访问存储系统以及执行与存储相关的ONTAP工具任务(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ONTAP工具专用特权结合使用来控制用户可以执行的ONTAP工具任务：

- 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

将ONTAP RBAC与ONTAP工具专用的特权结合使用、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库，同时防止 vCenterUserA 配置数据存储库。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库。

启动ONTAP工具任务时、ONTAP工具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ONTAP工具无需检查该存储系统的ONTAP特权、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ONTAP工具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)。 确定您是否有足够的权限在该存储系统上执行该ONTAP工具任务所需的存储操作。如果您具有正确的ONTAP权限、则可以访问存储系统并执行ONTAP工具任务。ONTAP角色决定了您可以对存储系统执行的ONTAP工具任务。

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、ONTAP工具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ONTAP工具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ONTAP System Manager 9.8P1或更高版本创建ONTAP 角色。 请参见 "配置用户角色和权限" 有关详细信息 …

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、ONTAP工具专用的ONTAP角色按分层结构进行排序。这意味着、第一个角色的限制性最强、它只具有与一组最基本的ONTAP工具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。

下面列出了一些使用ONTAP工具时建议使用的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。

ONTAP工具和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ONTAP工具中、即使您使用的是ONTAP工具或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：

- 使用ONTAP System Manager 9.8P1或更高版本创建集群管理员或SVM管理员角色。 请参见 "配置用户角色和权限" 有关详细信息 …
- 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ONTAP工具配置存储系统、您需要这些存储系统凭据。您可以通过在ONTAP工具中输入凭据来

为ONTAP工具配置存储系统。每次使用这些凭据登录到存储系统时、您都将有权访问创建这些凭据时在ONTAP中设置的ONTAP工具功能。

- 将存储系统添加到ONTAP工具中、并提供刚刚创建的用户的凭据

ONTAP工具角色

ONTAP工具将ONTAP特权分为以下一组ONTAP工具角色：

- 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ONTAP工具时、ONTAP工具会对ONTAP RBAC角色执行初始权限验证。如果添加了直接SVM存储IP、则ONTAP工具不会执行初始验证。ONTAP工具会稍后在任务工作流中检查并强制实施特权。