



VSC 任务所需的特权

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/zh-cn/vsc-vasa-provider-sra-97/deploy/reference-product-level-privilege-required-by-vsc-for-vmware-vsphere.html> on March 21, 2024. Always check docs.netapp.com for the latest.

目录

- VSC 任务所需的特权 1
 - 适用于VMware vSphere的VSC所需的产品级特权 1
 - VSC、VASA Provider和SRA虚拟设备的ONTAP 基于角色的访问控制 1
 - 使用适用于VMware vSphere的VSC时的建议ONTAP 角色 2
 - 如何为适用于VMware vSphere的VSC配置基于ONTAP 角色的访问控制 3
 - 配置用户角色和权限 5

VSC 任务所需的特权

不同的适用于VMware vSphere的Virtual Storage Console任务需要不同的(VSC)特权和原生 vCenter Server特权组合。

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VSC所需的产品级特权

要访问适用于VMware vSphere的Virtual Storage Console图形用户界面、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	Description	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。</p> <p>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>

VSC、VASA Provider和SRA虚拟设备的ONTAP 基于角色的访问控制

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的虚拟存储控制台中、ONTAP RBAC与vCenter Server RBAC结合使用来确定特定用户可以对特定存储系统上的对象执行的虚拟存储控制台(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VSC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Virtual Storage Console和基于角色的访问控制(Role-Based Access Control、RBAC)。这些角色包含执行(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：

- 9.7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）

"适用于适用于 VMware vSphere 的 VSC， VASA Provider 和 Storage Replication Adapter 7.0 的 RBAC User Creator 工具"

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VSC配置基于ONTAP 角色的访问控制

如果要对适用于VMware vSphere的虚拟存储控制台(VSC)使用基于角色的访问控制、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连接到VSC、VASA Provider和SRA、您应执行以下操作：

- 创建集群管理员或管理员角色

您可以使用以下方法之一创建这些角色：

- ONTAP System Manager 9.7 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）

"适用于适用于 VMware vSphere 的 VSC， VASA Provider 和 Storage Replication Adapter 7.0 的 RBAC User Creator 工具"

- 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。



如果要使用 ONTAP 命令手动配置角色和权限，必须参考知识库文章。

- "VSC , VASA 和 SRA 7.0 ONTAP RBAC 配置"
- "在 SVM 级别汇总 VSC 和 SRA 的所有命令"

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。

配置用户角色和权限

您可以使用随VSC、VASA Provider以及SRA和ONTAP System Manager虚拟设备提供的JSON文件配置新的用户角色来管理存储系统。

开始之前

- 您应已使用`+ https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`从VSC、VASA Provider和SRA虚拟设备下载ONTAP 特权文件。
- 您应已配置ONTAP 9.7系统管理器。
- 您应已使用存储系统的管理员权限登录。

步骤

1. 解压缩下载的`https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`文件。
2. 访问 ONTAP 系统管理器。
3. 单击菜单：集群[设置>用户和角色]。
4. 单击 * 添加用户 *。
5. 在*添加用户*对话框中、选择*虚拟化产品*。
6. 单击 * 浏览 * 以选择并上传 ONTAP 权限 JSON 文件。

产品字段会自动填充。

7. 从*产品功能*下拉菜单中选择所需功能。

系统会根据选定产品功能自动填充 * 角色 * 字段。

8. 输入所需的用户名和密码。
9. 选择用户所需的权限（发现，创建存储，修改存储，销毁存储），然后单击 * 添加 *。

结果

此时将添加新角色和用户，您可以在已配置的角色下查看详细权限。

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。