SnapCenter 基于角色的访问控制（RBAC）

SnapCenter Software 5.0

NetApp
July 18, 2024

目录

SnapCenter 基于角色的访问控制（ RBAC ）

RBAC 的类型

通过 SnapCenter 基于角色的访问控制（ Role-Based Access Control ， RBAC ）和 ONTAP 权限， SnapCenter 管理员可以将 SnapCenter 资源的控制权委派给不同的用户或用户组。通过这种集中管理的访问，应用程序管理员可以在委派的环境中安全地工作。

您可以随时创建和修改角色，并向用户添加资源访问权限，但在首次设置 SnapCenter 时，您应至少将 Active Directory 用户或组添加到角色中，然后向这些用户或组添加资源访问权限。

您不能使用 SnapCenter 创建用户或组帐户。您应在操作系统或数据库的 Active Directory 中创建用户或组帐户。

SnapCenter 使用以下类型的基于角色的访问控制：

- SnapCenter RBAC
- SnapCenter 插件 RBAC （对于某些插件）
- 应用程序级 RBAC
- ONTAP权限

SnapCenter RBAC

角色和权限

SnapCenter 附带的预定义角色已分配权限。您可以将用户或用户组分配给这些角色。您还可以创建新角色并管理权限和用户。

- 为用户或组分配权限 *

您可以为用户或组分配访问主机，存储连接和资源组等 SnapCenter 对象的权限。您不能更改 SnapCenterAdmin 角色的权限。

您可以为同一林中的用户和组以及属于不同林的用户分配 RBAC 权限。您不能为属于林间嵌套组的用户分配 RBAC 权限。

如果创建自定义角色，则该角色必须包含 SnapCenter 管理员角色的所有权限。如果您仅复制某些权限，例如 Host add 或 Host remove ，则无法执行这些操作。

身份验证

用户需要在登录期间通过图形用户界面（ GUI ）或 PowerShell cmdlet 提供身份验证。如果用户是多个角色的成员，则在输入登录凭据后，系统会提示用户指定要使用的角色。用户还需要提供身份验证才能运行 API 。

应用程序级 RBAC

SnapCenter 使用凭据验证授权的 SnapCenter 用户是否也具有应用程序级别的权限。

例如、如果要在SQL Server环境中执行Snapshot和数据保护操作、则必须使用正确的Windows或SQL凭据设置凭据。SnapCenter 服务器使用任一方法对设置的凭据进行身份验证。如果要在Windows文件系统环境中对ONTAP存储执行快照和数据保护操作、SnapCenter管理员角色必须在Windows主机上具有管理员权限。

同样，如果要对 Oracle 数据库执行数据保护操作，并且在数据库主机中禁用了操作系统（ OS ）身份验证，则必须使用 Oracle 数据库或 Oracle ASM 凭据设置凭据。SnapCenter 服务器会根据操作使用以下方法之一对凭据集进行身份验证。

适用于 **VMware vSphere RBAC** 的 **SnapCenter** 插件

如果您使用 SnapCenter VMware 插件进行 VM 一致的数据保护，则 vCenter Server 可提供额外级别的 RBAC 。SnapCenter VMware 插件既支持 vCenter Server RBAC ，又支持 Data ONTAP RBAC 。

有关信息、请参见 "适用于 VMware vSphere RBAC 的 SnapCenter 插件"

ONTAP权限

您应创建具有访问存储系统所需权限的 vsadmin 帐户。

有关创建帐户和分配权限的信息、请参见 "创建具有最低权限的 ONTAP 集群角色"

RBAC 权限和角色

通过 SnapCenter 基于角色的访问控制（ Role-Based Access Control ， RBAC ），您可以创建角色并为这些角色分配权限，然后将用户或用户组分配给这些角色。这样，SnapCenter 管理员就可以创建一个集中管理的环境，而应用程序管理员则可以管理数据保护作业。SnapCenter 附带了一些预定义的角色和权限。

SnapCenter 角色

SnapCenter 附带以下预定义角色。您可以将用户和组分配给这些角色，也可以创建新角色。

将角色分配给用户时，只有与该用户相关的作业才会显示在 " 作业 " 页面中，除非您已分配 SnapCenter 管理员角色。

- 应用程序备份和克隆管理员
- 备份和克隆查看器
- 基础架构管理员
- SnapCenterAdmin

适用于 **VMware vSphere** 的 **SnapCenter** 插件角色

为了管理 VM ， VMDK 和数据存储库的 VM 一致数据保护，适用于 VMware vSphere 的 SnapCenter 插件会在 vCenter 中创建以下角色：

- 选择控制阀管理器
- SCV 视图

- SCV 备份
- SCV 恢复
- SCV 子系统文件还原

有关详细信息、请参见 "适用于 VMware vSphere 的 SnapCenter 插件用户的 RBAC 类型"

* 最佳实践： * NetApp 建议您为适用于 VMware vSphere 的 SnapCenter 插件操作创建一个 ONTAP 角色，并为其分配所有必需的特权。

SnapCenter 权限

SnapCenter 提供以下权限：

- Resource Group
- 策略
- 备份
- 主机
- 存储连接
- 克隆
- 配置（仅适用于 Microsoft SQL 数据库）
- 信息板
- 报告
- 还原
  - 完整卷还原（仅适用于自定义插件）
- 资源

  要执行资源发现操作，非管理员需要具有管理员提供的插件权限。

- 插件安装或卸载

  启用插件安装权限时，您还必须修改主机权限以启用读取和更新。

- 迁移
- 挂载（仅适用于 Oracle 数据库）
- 卸载（仅适用于 Oracle 数据库）
- 作业监控器

  通过作业监控权限，不同角色的成员可以查看其分配到的所有对象上的操作。

预定义的 SnapCenter 角色和权限

SnapCenter 附带预定义角色，每个角色都已启用一组权限。在设置和管理基于角色的访问控制（ Role-Based Access Control ， RBAC ）时，您可以使用这些预定义角色，也可以创建新角色。

SnapCenter 包括以下预定义角色：

- SnapCenter 管理员角色
- 应用程序备份和克隆管理员角色
- 备份和克隆查看器角色
- 基础架构管理员角色

将用户添加到角色时，您必须分配 StorageConnection 权限以启用 Storage Virtual Machine （ SVM ）通信，或者向用户分配 SVM 以启用使用 SVM 的权限。用户可以通过存储连接权限创建 SVM 连接。

例如，具有 SnapCenter 管理员角色的用户可以创建 SVM 连接并将其分配给具有应用程序备份和克隆管理员角色的用户，默认情况下，此用户无权创建或编辑 SVM 连接。如果没有 SVM 连接，用户将无法完成任何备份，克隆或还原操作。

SnapCenter 管理员角色

SnapCenter 管理员角色已启用所有权限。您不能修改此角色的权限。您可以将用户和组添加到角色或将其删除。

应用程序备份和克隆管理员角色

应用程序备份和克隆管理员角色具有为应用程序备份和克隆相关任务执行管理操作所需的权限。此角色不具有主机管理，配置，存储连接管理或远程安装的权限。

权限	已启用	创建	读取	更新	删除
Resource Group	不适用	是	是	是	是
策略	不适用	是	是	是	是
备份	不适用	是	是	是	是
主机	不适用	是	是	是	是
存储连接	不适用	否	是	否	否
克隆	不适用	是	是	是	是
配置	不适用	否	是	否	否

权限	已启用	创建	读取	更新	删除
信息板	是	不适用	不适用	不适用	不适用
报告	是	不适用	不适用	不适用	不适用
还原	是	不适用	不适用	不适用	不适用
资源	是	是	是	是	是
插件安装 / 卸载	否	不适用		不适用	不适用
迁移	否	不适用	不适用	不适用	不适用
挂载	是	是	不适用	不适用	不适用
卸载	是	是	不适用	不适用	不适用
完整卷还原	否	否	不适用	不适用	不适用
作业监控器	是	不适用	不适用	不适用	不适用

备份和克隆查看器角色

备份和克隆查看器角色具有所有权限的只读视图。此角色还可以启用发现，报告和访问信息板的权限。

权限	已启用	创建	读取	更新	删除
Resource Group	不适用	否	是	否	否
策略	不适用	否	是	否	否
备份	不适用	否	是	否	否
主机	不适用	否	是	否	否
存储连接	不适用	否	是	否	否
克隆	不适用	否	是	否	否
配置	不适用	否	是	否	否
信息板	是	不适用	不适用	不适用	不适用

权限	已启用	创建	读取	更新	删除
报告	是	不适用	不适用	不适用	不适用
还原	否	否	不适用	不适用	不适用
资源	否	否	是	是	否
插件安装 / 卸载	否	不适用	不适用	不适用	不适用
迁移	否	不适用	不适用	不适用	不适用
挂载	是	不适用	不适用	不适用	不适用
卸载	是	不适用	不适用	不适用	不适用
完整卷还原	否	不适用	不适用	不适用	不适用
作业监控器	是	不适用	不适用	不适用	不适用

基础架构管理员角色

基础架构管理员角色已启用主机管理，存储管理，配置，资源组，远程安装报告， 并访问信息板。

权限	已启用	创建	读取	更新	删除
Resource Group	不适用	是	是	是	是
策略	不适用	否	是	是	是
备份	不适用	是	是	是	是
主机	不适用	是	是	是	是
存储连接	不适用	是	是	是	是
克隆	不适用	否	是	否	否
配置	不适用	是	是	是	是
信息板	是	不适用	不适用	不适用	不适用
报告	是	不适用	不适用	不适用	不适用

权限	已启用	创建	读取	更新	删除
还原	是	不适用	不适用	不适用	不适用
资源	是	是	是	是	是
插件安装 / 卸载	是	不适用	不适用	不适用	不适用
迁移	否	不适用	不适用	不适用	不适用
挂载	否	不适用	不适用	不适用	不适用
卸载	否	不适用	不适用	不适用	不适用
完整卷还原	否	否	不适用	不适用	不适用
作业监控器	是	不适用	不适用	不适用	不适用