RBAC 安全性

ONTAP Automation

NetApp
May 24, 2024

目录

RBAC 安全性

RBAC安全性概述

ONTAP 具有强大且可扩展的基于角色的访问控制(Role-Based Access Control、RBAC)功能。您可以为每个帐户分配不同的角色、以控制用户对通过REST API和CLI公开的资源的访问。这些角色为各种ONTAP 用户定义了不同的管理访问级别。

ONTAP RBAC功能继续扩展、并在ONTAP 9.11.1 (及后续版本)中得到了显著增强。请参见 "RBAC演变概述" 和 "ONTAP REST API 和自动化的新增功能" 有关详细信息 …

ONTAP 角色

角色是一组特权、这些特权共同定义了用户可以执行的操作。每个权限都标识一个特定访问路径以及关联的访问级别。角色会分配给用户帐户、并由ONTAP 在做出访问控制决策时应用。

角色类型

角色有两种类型。随着ONTAP 的发展、它们会针对不同的环境进行介绍和定制。

使用每种类型的角色都有优缺点。请参见 "比较角色类型" 有关详细信息 …

Type	Description
REST	REST角色是在ONTAP 9.6中引入的、通常适用于通过REST API访问ONTAP 的用户。创建REST角色会自动创建传统的_MAPPING角色。
传统	这些角色是ONTAP 9.6之前的旧角色。它们是为ONTAP 命令行界面环境引入的、并且仍然是RBAC安全性的基础。

范围

每个角色都有一个定义和应用该角色的范围或环境。范围用于确定特定角色的使用位置和使用方式。

ONTAP 用户帐户也具有类似的范围、用于确定用户的定义和使用方式。

范围	Description
集群	具有集群范围的角色在ONTAP 集群级别定义。它们与集群级别的用户帐户关联。
SVM	具有SVM范围的角色是为特定数据SVM定义的。它们会分配给同一SVM中的用户帐户。

角色定义的来源

可以通过两种方式定义ONTAP 角色。

角色源	Description
自定义	ONTAP 管理员可以创建自定义角色。这些角色可以根据特定环境和安全要求进行定制。

角色源	Description
内置	虽然自定义角色可提供更大的灵活性、但集群和SVM级别也提供了一组内置角色。这些角色是预定义的、可用于执行许多常见的管理任务。

角色映射和ONTAP 处理

根据所使用的ONTAP 版本、所有或几乎所有REST API调用都会映射到一个或多个命令行界面命令。创建REST角色时、也会创建传统或传统角色。此*映射*传统角色基于相应的CLI命令、不能操作或更改。

不支持反向角色映射。也就是说、创建传统角色不会创建相应的REST角色。

RBAC演变概述

所有ONTAP 9版本都包含传统角色。其余角色稍后介绍、并按如下所述进行了改进。

ONTAP 9.6

REST API是在ONTAP 9.6中推出的。此版本还包括其余角色。此外、创建REST角色时、还会创建相应的传统角色。

ONTAP 9.7到9.10.1

从9.7到9.10.1的每个ONTAP 版本都对REST API进行了增强。例如、每个版本都添加了其他REST端点。但是、这两种角色类型的创建和管理仍然是分开的。此外、ONTAP 9.10.1还为快照REST端点`/api/storage/volumes/｛vol.uuid｝/snapshots`添加了REST RBAC支持、该端点是一个符合资源条件的端点。

ONTAP 9.11.1

此版本增加了使用REST API配置和管理传统角色的功能。此外、还为REST角色添加了其他访问级别。

使用角色和用户

了解基本RBAC功能后、您可以开始使用ONTAP 角色和用户。

请参见 "RBAC工作流" 有关如何在ONTAP REST API中创建和使用角色的示例。

管理访问

您可以通过REST API或命令行界面创建和管理ONTAP 角色。访问详细信息如下所述。

REST API

使用RBAC角色和用户帐户时、可以使用多个端点。表中的前四个用于创建和管理角色。最后两个用于创建和管理用户帐户。

您可以联机访问ONTAP "API 参考" 有关详细信息的文档、包括如何使用API的示例。

端点	Description
安全性/角色	使用此端点可以创建新的REST角色。从ONTAP 9.11.1开始、您还可以创建传统角色。在这种情况下、ONTAP 会根据输入参数确定角色类型。您还可以检索已定义角色的列表。
安全性/角色/ {owner.UUID} / {name}	您可以检索或删除特定集群或SVM范围的角色。UUID值用于标识定义角色的SVM (集群或数据SVM)。name值是角色的名称。
安全性/角色/ {owner.UUID} / {name} /权限	使用此端点可以为特定角色配置特权。可以检索内置角色、但不能更新。有关详细信息、请参见适用于您的ONTAP 版本的API参考文档。
安全性/角色/ {owner.UUID} / {name} /privileges/[path]	您可以检索、修改和删除特定权限的访问级别和可选查询值。有关详细信息、请参见适用于您的ONTAP 版本的API参考文档。
安全性/帐户	使用此端点可以创建新的集群或SVM范围的用户帐户。在帐户正常运行之前、必须包含或随后添加多种类型的信息。您还可以检索已定义的用户帐户列表。
/security/accouns/ {owner.UUID} / {name}	您可以检索、修改和删除特定集群或SVM范围的用户帐户。UUID值用于标识定义用户的SVM (集群或数据SVM)。name值是帐户的名称。

命令行界面

下面介绍了相关的ONTAP 命令行界面命令。所有命令均通过管理员帐户在集群级别访问。

命令	Description
s安全性登录	此目录包含创建和管理用户登录所需的命令。
s安全性登录REST角色	此目录包含创建和管理与用户登录关联的REST角色所需的命令。
s安全登录角色	此目录包含创建和管理与用户登录关联的传统角色所需的命令。

角色定义

其余角色和传统角色通过一组属性进行定义。

所有者和范围

角色可以归ONTAP 集群或集群中的特定数据SVM所有。所有者还隐式确定角色的范围。

唯一名称

每个角色在其范围内都必须具有唯一的名称。集群角色的名称在ONTAP 集群级别必须是唯一的、而SVM角色在特定SVM中必须是唯一的。

新的REST角色的名称必须在REST角色和传统角色之间是唯一的。这是因为、创建REST角色还会导致使用相同名称的新传统_MAPPING角色。

一组权限

每个角色都包含一组或多个权限。每个权限可标识特定资源或命令以及关联的访问级别。

特权

一个角色可以包含一个或多个权限。每个权限定义都是一个元组、用于建立对特定资源或操作的访问级别。

资源路径

资源路径标识为REST端点或CLI命令/命令目录路径。

REST端点

API端点确定了REST角色的目标资源。

CLI 命令

CLI命令用于标识传统角色的目标。此外、还可以指定命令目录、该目录将包括ONTAP 命令行界面层次结构中的所有下游命令。

访问级别

访问级别定义了角色对特定资源路径或命令的访问类型。访问级别通过一组预定义的关键字来标识。ONTAP 9.6引入了三种访问级别。它们既可用于传统角色、也可用于REST角色。此外、ONTAP 9.11.1增加了三个新的访问级别。这些新访问级别只能用于REST角色。

> 访问级别遵循CRUD模式。使用REST时、此方法基于主要HTTP方法(POST、GET、PATCH、DELETE)。相应的CLI操作通常会映射到REST操作(create、show、modify、delete)。

访问级别	其他基本功能	已添加	仅限**REST**角色
无	不适用	9.6	否
-readonly	获取	9.6	否
全部	获取、发布、修补、删除	9.6	否
read_create	获取、发布	9.11.1	是的。
read_modify	获取、修补	9.11.1	是的。
read_create_modify	获取、发布、修补	9.11.1	是的。

可选查询

创建传统角色时、您可以选择包含*查询*值、以确定命令或命令目录的适用对象子集。

内置角色摘要

ONTAP 中包含多个预定义角色、您可以在集群或SVM级别使用这些角色。

集群范围的角色

集群范围内提供了多个内置角色。

请参见 "集群管理员的预定义角色" 有关详细信息 …

Role	Description
管理员	具有此角色的管理员拥有不受限制的权限、可以在ONTAP 系统中执行任何操作。他们可以配置所有集群级别和SVM级别的资源。
AutoSupport	这是为AutoSupport 帐户量身定制的一个特殊角色。
backup	此特殊角色适用于需要备份系统的备份软件。
SnapLock	这是为SnapLock 帐户量身定制的一个特殊角色。
-readonly	具有此角色的管理员可以查看集群级别的所有内容、但无法进行任何更改。
无	不提供任何管理功能。

SVM范围的角色

SVM范围内提供了多个内置角色。通过* vsadmin*、您可以访问最通用且功能最强大的功能。还有几个针对特定管理任务量身定制的其他角色、其中包括：

- vsadmin-volume
- vsadmin-protocol
- vsadmin-backup
- vsadmin-SnapLock
- vsadmin-readonly

请参见 "SVM 管理员的预定义角色" 有关详细信息 …

比较角色类型

在选择"Rest"角色或"*传统"角色之前、您应了解这些差异。下面介绍了比较这两种角色类型的一些方法。

对于更高级或更复杂的RBAC使用情形、通常应使用传统角色。

用户如何访问**ONTAP**

在创建角色之前、请务必了解用户将如何访问ONTAP 系统。可以根据此情况确定角色类型。

访问	建议的类型
仅限REST API	REST角色设计为与REST API结合使用。
REST API和CLI	您可以定义一个REST角色、此角色也会创建相应的传统角色。
仅限CLI	您可以创建传统角色。

访问路径的精度

为REST角色定义的访问路径基于REST端点。传统角色的访问路径基于命令行界面命令或命令目录。此外、您还可以包括具有传统角色的可选查询参数、以便根据命令参数值进一步限制访问。