



配额如何与用户和组配合使用 ONTAP 9

NetApp
September 12, 2024

目录

- 配额如何与用户和组配合使用 1
 - 概述如何对用户和组使用配额 1
 - 为配额指定UNIX用户 1
 - 为配额指定Windows用户 1
 - 默认用户配额和组配额如何创建派生配额 2
 - 如何将配额应用于 root 用户 3
 - 配额如何与特殊 Windows 组配合使用 3
 - 如何将配额应用于具有多个 ID 的用户 4
 - ONTAP 如何在混合环境中确定用户 ID 4
 - 配额如何与多个用户配合使用 4
 - 配额的UNIX和Windows名称链接 5

配额如何与用户和组配合使用

概述如何对用户和组使用配额

您可以将用户或组指定为配额的目标。定义配额时、需要考虑几个实施差异。

您需要注意的一些差异包括：

- 用户或组
- UNIX或Windows
- 特殊用户和组
- 是否包含多个ID

根据您的环境、还可以通过不同的方式为用户指定ID。

为配额指定UNIX用户

您可以使用多种不同格式之一为配额指定UNIX用户。

为配额指定UNIX用户时、可以使用以下三种格式：

- 用户名(例如jsmith)。



如果 UNIX 用户名包含反斜杠 (\) 或 @ 符号，则不能使用该用户名来指定配额。这是因为 ONTAP 会将包含这些字符的名称视为 Windows 名称。

- 用户ID或UID (例如20)。
- 该用户所拥有的文件或目录的路径，以使该文件的 UID 与该用户匹配。



如果指定文件或目录名称，则必须选择一个文件或目录，只要用户帐户仍在系统上，该文件或目录就会持续。

为 UID 指定文件或目录名称不会通过发生原因 ONTAP 将配额应用于该文件或目录。

为配额指定Windows用户

您可以使用多种不同格式之一为配额指定Windows用户。

为配额指定Windows用户时、可以使用以下三种格式：

- Windows 2000 之前格式的 Windows 名称。
- Windows以文本形式显示的安全ID (SID)，例如 S-1-5-32-544。
- 此用户的 SID 拥有 ACL 的文件或目录的名称。

如果指定文件或目录名称，则必须选择一个文件或目录，只要用户帐户仍在系统上，该文件或目录就会持续。



要使 ONTAP 从 ACL 获取 SID，ACL 必须有效。

如果文件或目录位于 UNIX 模式的 qtree 中，或者存储系统使用 UNIX 模式进行用户身份验证，则 ONTAP 会将用户配额应用于其 * UID * 而非 SID 与文件或目录匹配的用户。

为配额指定文件或目录名称以标识用户不会通过发生原因 ONTAP 将配额应用于该文件或目录。

默认用户配额和组配额如何创建派生配额

创建默认用户或组配额时，系统会自动为在同一级别拥有文件的每个用户或组创建相应的派生用户或组配额。

派生用户配额和组配额可通过以下方式创建：

- FlexVol 卷上的默认用户配额会为在卷上任何位置拥有文件的每个用户创建派生用户配额。
- qtree 上的默认用户配额会为在 qtree 中拥有文件的每个用户创建派生用户配额。
- FlexVol 卷上的默认组配额会为在卷上任何位置拥有文件的每个组创建派生组配额。
- qtree 上的默认组配额会为在 qtree 中拥有文件的每个组创建派生组配额。

如果用户或组在默认用户或组配额级别不拥有文件，则不会为该用户或组创建派生配额。例如，如果为 qtree proj1 创建了默认用户配额，而用户 jsmith 拥有其他 qtree 上的文件，则不会为 jsmith 创建派生用户配额。

派生配额与默认配额具有相同的设置，包括限制和用户映射。例如，如果默认用户配额具有 50 MB 的磁盘限制并启用了用户映射，则生成的任何派生配额也会设置 50 MB 的磁盘限制并启用用户映射。

但是，对于三个特殊用户和组，派生配额不存在任何限制。如果以下用户和组在默认用户或组配额级别拥有文件，则会使用与默认用户或组配额相同的用户映射设置创建派生配额，但它只是一个跟踪配额（无限制）：

- UNIX root 用户（UID 0）
- UNIX 根组（GID 0）
- Windows BUILTIN\Administrators 组

由于 Windows 组的配额作为用户配额进行跟踪，因此此组的派生配额是从默认用户配额派生的用户配额，而不是从默认组配额派生的。

派生用户配额示例

如果您的卷包含三个用户（root，jsmith 和 bob）拥有的文件，并且您在该卷上创建了默认用户配额，则 ONTAP 会自动创建三个派生用户配额。因此，重新初始化卷上的配额后，配额报告中将显示四个新配额：

```
cluster1::> volume quota report
```

```
Vserver: vs1
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
vol1		user	*	0B	50MB	0	-	*
vol1		user	root	5B	-	1	-	
vol1		user	jsmith	30B	50MB	10	-	*
vol1		user	bob	40B	50MB	15	-	*

4 entries were displayed.

第一个新行是您创建的默认用户配额，可通过星号（*）标识为 ID。其他新行是派生用户配额。jsmith 和 bob 的派生配额与默认配额具有相同的 50 MB 磁盘限制。root 用户的派生配额是一个无限制的跟踪配额。

如何将配额应用于 root 用户

UNIX客户端上的root用户(UID=0)受树配额限制、但不受用户或组配额限制。这样，root 用户就可以代表其他用户执行操作，否则配额会阻止这些操作。

当root用户`chown`代表Privileges较低的用户执行文件或目录所有权更改或其他操作(例如UNIX命令)时、ONTAP会根据新所有者检查配额、但不会报告错误或停止此操作、即使超出了新所有者的硬配额限制也是如此。当恢复丢失的数据等管理操作导致临时超过配额时，此功能非常有用。



但是，在执行所有权传输后，如果用户在仍超过配额的情况下尝试分配更多磁盘空间，则客户端系统将报告磁盘空间错误。

相关信息

- ["如何应用配额"](#)
- ["如何将配额应用于具有多个 ID 的用户"](#)

配额如何与特殊 Windows 组配合使用

有几个特殊的Windows组处理配额的方式与其他Windows组不同。您应了解如何为这些特殊组应用配额。



ONTAP 不支持基于 Windows 组 ID 的组配额。如果指定 Windows 组 ID 作为配额目标，则此配额将视为用户配额。

每个人

如果配额目标为Everyone组、则ACL显示所有者为Everyone的文件将计入Everyone的SID。

BUILTIN\Administrators

如果配额目标是BUILTIFiles\Administrators组、则该条目将被视为用户配额、并且仅用于跟踪。您不能对BUILTIN\Administrators 实施限制。如果BUILWIN\Administrators的成员创建了一个文件、则该文件属于BUILWIN\Administrators、并计入BUILWIN\Administrators的SID (而不是用户的个人SID)。

如何将配额应用于具有多个 ID 的用户

一个用户可以由多个 ID 表示。您可以通过将ID列表指定为配额目标来为此类用户定义单个用户配额。这些 ID 中的任何一个所拥有的文件都受用户配额限制。

假设用户具有UNIX UID 20`以及Windows ID `corp\john_smith`和 `engineering\jsmith。对于此用户，您可以指定一个配额，其中配额目标是 UID 和 Windows ID 的列表。当此用户向存储系统写入数据时，无论写入来自UID 20、还是，都会应用指定的配额 corp\john_smith engineering\jsmith。

请注意、即使ID属于同一用户、单独的配额规则也会被视为单独的目标。例如、对于同一个用户、您可以指定一个配额将UID限制 20`为1 GB磁盘空间、而指定另一个配额则将corp\John_Smith限制为2 GB磁盘空间、即使这两个ID代表同一个用户也是如此。ONTAP会 `20 corp\john_smith`分别将配额应用于UID和。在这种情况下，不会对应用任何限制 `engineering\jsmith，即使对同一用户使用的其他ID应用了限制。

相关信息

- ["如何应用配额"](#)
- ["如何将配额应用于 root 用户"](#)

ONTAP 如何在混合环境中确定用户 ID

如果您的用户同时从Windows和UNIX客户端访问ONTAP存储、则会同时使用Windows和UNIX安全性来确定文件所有权。多个因素决定了 ONTAP 在应用用户配额时是使用 UNIX 还是 Windows ID 。

如果包含文件的 qtree 或 FlexVol 卷的安全模式仅为 NTFS 或 UNIX ，则此安全模式将确定应用用户配额时使用的 ID 类型。对于采用混合安全模式的 qtree ，使用的 ID 类型取决于文件是否具有 ACL 。

下表总结了所使用的ID类型。

安全风格	ACL	无 ACL
"unix"	UNIX ID	UNIX ID
混合	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

配额如何与多个用户配合使用

如果在同一个配额目标中放置多个用户、则配额定义的限制不会应用于每个用户。而是在配额目标中的所有用户之间共享配额限制。

与用于管理卷和 qtree 等对象的命令不同，您不能重命名配额目标，包括多用户配额。这意味着，定义多用户配额后，您将无法修改配额目标中的用户，也无法向目标添加用户或从目标中删除用户。如果要在多用户配额中添加或删除用户，则必须删除包含该用户的配额，并定义一个包含目标中的一组用户的新配额规则。



如果将单独的用户配额合并为一个多用户配额，则可以通过调整配额大小来激活更改。但是，如果要从包含多个用户的配额目标中删除用户，或者将用户添加到已包含多个用户的目标中，则必须在更改生效之前重新初始化配额。

一个配额规则包含多个用户的示例

在以下示例中，配额条目中列出了两个用户。这两个用户合计最多可使用80 MB的空间。如果一个使用75 MB、则另一个只能使用5 MB。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default			Volume: vol1	
					Soft	Soft	
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							

user	"jsmith,chen"	""	off	80MB	-	-	-
-							

配额的UNIX和Windows名称链接

在混合环境中，用户可以以 Windows 用户或 UNIX 用户身份登录。您可以配置配额以识别用户的 UNIX ID 和 Windows ID 代表同一个用户。

当同时满足以下两个条件时，Windows 用户名的配额会映射到 UNIX 用户名，反之亦然：

- 。 user-mapping 参数在用户的配额规则中设置为"on"。
- 用户名已映射到 vsserver name-mapping 命令

当 UNIX 名称和 Windows 名称映射在一起时，在确定配额使用量时，它们会被视为同一个人。

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。