ユーザおよびグループとクォータ

ONTAP 9

NetApp
April 24, 2024

目次

ユーザおよびグループとクォータ

クォータとユーザおよびグループとの連携の概要

ユーザまたはグループをクォータのターゲットとして指定すると、そのクォータの制限がそのユーザまたはグループに適用されます。ただし、一部の特殊なグループとユーザについては処理が異なります。ユーザの ID を指定する方法は環境によって異なります。

クォータに **UNIX** ユーザを指定する方法

クォータに UNIX ユーザを指定するには、ユーザ名、 UID 、またはユーザによって所有されているファイルまたはディレクトリの 3 つの形式のいずれかを使用します。

クォータに UNIX ユーザを指定するには、次のいずれかの形式を使用します。

- jsmith などのユーザ名

> UNIX ユーザ名にバックスラッシュ（ \ ）または @ 記号が含まれている場合、その名前を使用してクォータを指定することはできません。ONTAP では、これらの文字を含む名前は Windows 名として処理されます。

- UID （ 20 など）。
- ユーザが所有するファイルまたはディレクトリのパス。ファイルの UID がユーザと一致するように設定されます。

> ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。
>
> UID のファイルまたはディレクトリ名原因 ONTAP を指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

クォータに **Windows** ユーザを指定する方法

クォータに Windows ユーザを指定するには、 Windows 2000 より前の形式の Windows ユーザ名、 SID 、ユーザの SID によって所有されているファイルまたはディレクトリの 3 つの形式のいずれかを使用します。

クォータに Windows ユーザを指定するには、次のいずれかの形式を使用します。

- Windows 2000 より前の形式の Windows 名。
- S-1-5-32-544 など、 Windows によってテキスト形式で表示される Security ID （ SID ；セキュリティ ID ）。
- ユーザの SID によって所有されている ACL を持つファイルまたはディレクトリの名前。

ファイル名またはディレクトリ名を指定する場合は、システム上で対象のユーザアカウントを使用するかぎり削除されることのないファイルまたはディレクトリを選択する必要があります。

ONTAP が ACL から SID を取得するには、その ACL が有効である必要があります。

ファイルまたはディレクトリが UNIX 形式の qtree に存在する場合、またはストレージシステムでユーザ認証に UNIX モードが使用されている場合、 ONTAP は、 SID ではなく UID * がファイルまたはディレクトリの UID に一致するユーザにユーザクォータを適用します。

ファイルまたはディレクトリ原因 ONTAP の名前でクォータのユーザを指定しても、そのファイルまたはディレクトリにクォータを適用されるわけではありません。

デフォルトのユーザクォータおよびグループクォータで派生クォータを作成する方法

デフォルトのユーザクォータまたはグループクォータを作成すると、同じレベルでファイルを所有するユーザまたはグループごとに、対応する派生ユーザクォータまたは派生グループクォータが自動的に作成されます。

派生ユーザクォータと派生グループクォータは、次のように作成されます。

- FlexVol 上のデフォルトユーザクォータによって、ボリューム上のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- qtree 上のデフォルトユーザクォータによって、 qtree 内のファイルを所有するすべてのユーザに派生ユーザクォータが作成されます。
- FlexVol 上のデフォルトグループクォータによって、ボリューム上の任意の場所のファイルを所有するすべてのグループに派生グループクォータが作成されます。
- qtree 上のデフォルトグループクォータによって、 qtree 内のファイルを所有するすべてのグループに派生グループクォータが作成されます。

デフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有していないユーザまたはグループには、派生クォータは作成されません。たとえば、 qtree proj1 にデフォルトユーザクォータが作成され、ユーザ jsmith が異なる qtree 上のファイルを所有している場合、 jsmith には派生ユーザクォータが作成されません。

派生クォータの設定は、制限やユーザマッピングなど、デフォルトクォータと同じです。たとえば、デフォルトユーザクォータのディスク制限が 50MB でユーザマッピングが有効の場合、作成される派生クォータもディスク制限が 50MB でユーザマッピングが有効になります。

ただし、 3 つの特殊なユーザとグループの場合、派生クォータに制限はありません。次のユーザとグループがデフォルトのユーザクォータまたはグループクォータのレベルでファイルを所有している場合、派生クォータはデフォルトのユーザクォータまたはグループクォータと同じユーザマッピング設定で作成されますが、単なる追跡クォータになります（制限なし）。

- UNIX root ユーザ（ UID 0 ）
- UNIX ルートグループ（ GID 0 ）

- Windows BUILTIN\Administrators グループ

  Windows グループのクォータはユーザクォータとして追跡されるため、このグループの派生クォータは、デフォルトグループクォータではなくデフォルトユーザクォータから派生するユーザクォータになります。

派生ユーザクォータの例

root 、 jsmith 、および bob -own の 3 人のファイルが格納されているボリュームにデフォルトユーザクォータを作成すると、 ONTAP によって自動的に 3 つの派生ユーザクォータが作成されます。このため、このボリュームのクォータを再初期化すると、次の 4 つの新しいクォータがクォータレポートに表示されます。

```
cluster1::> volume quota report
  Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
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.
```

最初の新しい行は作成したデフォルトユーザクォータで、 ID がアスタリスク（ * ）であることから判別できます。ほかの新しい行は派生ユーザクォータです。jsmith と bob の派生クォータのディスク制限は、デフォルトクォータと同じく 50MB です。root ユーザの派生クォータは、制限のない追跡クォータです。

root ユーザへのクォータの適用方法

UNIX クライアント上の root ユーザ（ UID=0 ）はツリークォータの影響を受けますが、ユーザクォータまたはグループクォータの影響は受けません。これにより、 root ユーザは、通常ならクォータによって妨げられるような操作を他のユーザに代わって実行できます。

rootがファイルまたはディレクトリの所有権の変更、またはその他の操作（UNIXなど）を実行する場合 `chown` コマンド）権限の少ないユーザに代わって、ONTAP は新しい所有者に基づいてクォータをチェックしますが、新しい所有者のハードクォータ制限を超えてもエラーを報告したり処理を停止したりすることはありません。これは、消失データのリカバリなど、管理作業のために一時的にクォータを超過する場合に役立ちます。

> ただし、所有権の変更後、クォータの超過中にユーザがディスクスペースの割り当てサイズを増やそうとすると、クライアントシステムによりディスクスペースエラーが報告されます。

特殊な Windows グループとクォータ

Everyone グループおよび BUILTIN\Administrators グループと、その他の Windows グループでは、クォータの適用方法が異なります。

次のリストは、クォータターゲットが特別な Windows GID である場合の処理を示しています。

- クォータターゲットが Everyone グループである場合、 ACL で所有者が Everyone になっているファイルには Everyone の SID で処理されます。
- クォータターゲットが BUILTIN\Administrators である場合、そのエントリは追跡だけを目的としたユーザクォータであるとみなされます。

  BUILTIN\Administrators には制限を適用できません。

  BUILTIN\Administrators のメンバーがファイルを作成した場合、そのファイルは BUILTIN\Administrators によって所有され、そのユーザの個人 SID ではなく、 BUILTIN\Administrators の SID にカウントされます。

> ONTAP では、 Windows GID に基づいたグループクォータはサポートされません。Windows GID をクォータターゲットとして指定した場合、そのクォータはユーザクォータとみなされます。

複数の ID を持つユーザにクォータを適用する方法

ユーザは複数の ID で表すことができます。ID のリストをクォータターゲットとして指定して、このようなユーザに対して単一のユーザクォータを設定できます。これらの ID のいずれかによって所有されるファイルには、ユーザクォータの制限が適用されます。

ユーザが UNIX の UID 20 と、 Windows ID の corp\john_smith および engineering\jsmith を持っているとします。このユーザに対して、 UID および Windows ID のリストをクォータターゲットとするクォータを指定できます。このユーザがストレージシステムに書き込むと、その書き込み元が UID 20 、 corp\john_smith 、あるいは enginieering\jsmith のいずれの場合でも、指定されたクォータが適用されます。

> 複数のIDが同じユーザに属している場合でも、別 々 のクォータルールは別 々 のターゲットとみなされます。たとえば、 UID 20 と corp\john_smith が同一のユーザを表す場合でも、 UID 20 のディスクスペースを 1GB に制限するクォータを指定し、 corp\john_smith のディスクスペースを 2GB に制限する別のクォータを指定できます。ONTAP は UID 20 と corp\john_smith に対して個別にクォータを適用します。
>
> この場合、同じユーザが使用する他の ID に制限が適用される場合でも、 engineering\jsmith には制限が適用されません。

ONTAP が混在環境でユーザ ID を決定する方法

ユーザが Windows クライアントと UNIX クライアントの両方から ONTAP ストレージにアクセスする場合は、ファイルの所有権を決定するために、 Windows セキュリティと UNIX セキュリティの両方のセキュリティ形式が使用されます。ONTAP では、ユーザク

ォータの適用時に UNIX ID と Windows ID のどちらを使用するかを、複数の条件から決定します。

ファイルを含む qtree または FlexVol ボリュームのセキュリティ形式が NTFS のみまたは UNIX のみである場合、そのセキュリティ形式によって、ユーザクォータの適用時に使用される ID の種類が決定されます。mixed セキュリティ形式の qtree の場合、使用される ID の種類は、ファイルに ACL が設定されているかどうかによって決まります。

次の表に、使用される ID の種類を示します。

セキュリティ形式	アクセスできます	**ACL** はありません
「 UNIX 」	UNIX ID	UNIX ID
混在	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

複数のユーザがターゲットであるクォータ

複数のユーザを同じクォータターゲットに指定した場合、そのクォータで定義されているクォータ制限は各ユーザに個別に適用されるのではなく、クォータターゲットにリストされているすべてのユーザ間でクォータ制限が共有されます。

ボリュームや qtree などのオブジェクトを管理するコマンドとは異なり、マルチユーザクォータなどのクォータターゲットの名前は変更できません。つまり、マルチユーザクォータが定義されたあとで、クォータターゲット内のユーザを変更することはできず、ターゲットへのユーザの追加やターゲットからのユーザの削除もできません。マルチユーザクォータに対してユーザを追加または削除する場合は、そのユーザを含むクォータを削除し、ターゲットに定義されているユーザを使用して新しいクォータルールを定義する必要があります。

> 複数のユーザクォータを 1 つのマルチユーザクォータに結合する場合、クォータのサイズを変更することで変更をアクティブ化できます。ただし、複数のユーザを含むクォータターゲットからユーザを削除する場合、またはすでに複数のユーザを含むターゲットにユーザを追加する場合は、変更を有効にするためにクォータを再初期化する必要があります。

クォータルールに複数のユーザが含まれる例

次の例では、クォータエントリに 2 人のユーザがリストされています。2人のユーザーは、合計で最大80MBのスペースを使用できます。一方が75MBを使用している場合、もう一方は5MBしか使用できません。

```
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        -       -        -
-
```

クォータの UNIX 名と Windows 名をリンクさせる方法

混在環境では、ユーザは Windows ユーザまたは UNIX ユーザとしてログインできます。クォータは、ユーザの UNIX ID と Windows ID が同じユーザを表すことを認識するように設定できます。

次の両方の条件が満たされると、 Windows ユーザ名のクォータは UNIX ユーザ名にマッピングされ、 UNIX ユーザ名のクォータは Windows ユーザ名にマッピングされます。

- 。 `user-mapping` ユーザのクォータルールでパラメータが「on」に設定されている。
- ユーザ名がにマッピングされている `vserver name-mapping` コマンド

マッピングされた UNIX 名と Windows 名は同じユーザとして扱われ、クォータ使用量の算定に使用されます。