SnapDrive for UNIX でのロールベースアクセス制御

Snapdrive for Unix

NetApp
August 08, 2024

目次

SnapDrive for UNIX でのロールベースアクセス制御

ロールベースアクセス制御（ RBAC ）はユーザログインとロールの権限に使用されます。RBAC では、管理者がロールを定義してユーザのグループを管理できます。データベースへのアクセスを特定の管理者に制限する必要がある場合は、その管理者用の管理者アカウントを設定する必要があります。また、情報を制限したり、これらの管理者が表示したり、実行できる処理を実行したりする場合は、作成した管理者アカウントにロールを適用する必要があります。

SnapDrive for UNIX では、 Operations Manager コンソールを使用して RBAC を使用します。Operations Manager コンソールを使用して、 LUN 、 qtree 、ボリューム、アグリゲート、 vFiler ユニットなどのストレージオブジェクトにきめ細かくアクセスできます。

- 関連情報 *

ボリュームベース SnapRestore の必須チェック項目です

デスティネーションストレージシステムでの Snapshot コピーのリストア

手順のスナップ切断

SnapDrive for UNIX の Role-Based Access Control （ RBAC ；ロールベースアクセス制御）とは何ですか

RBAC を使用すると、 SnapDrive 管理者は、さまざまな SnapDrive 操作によってストレージシステムへのアクセスを制限できます。ストレージ処理に関するこの制限アクセスまたはフルアクセスは、ユーザに割り当てられたロールによって異なります。

SnapDrive 4.0 for UNIX 以降では、 SnapDrive for UNIX のすべての処理に対する RBAC アクセスチェックが必要です。この動作により、ストレージ管理者は、割り当てられたロールに応じて SnapDrive ユーザが実行できる処理を制限できます。RBAC は、 Operations Manager インフラを使用して実装します。SnapDrive 4.0 for UNIX よりも前のリリースでは、アクセス制御が制限されており、 root ユーザのみが SnapDrive for UNIX の処理を実行できました。SnapDrive 4.0 for UNIX 以降では、 Operations Manager コンソールの RBAC インフラストラクチャを使用して、ルート以外のローカルユーザおよび Network Information System （ NIS ）ユーザをサポートしています。SnapDrive for UNIX では、ストレージシステムの root パスワードは必要なく、 SD-<hostname> ユーザを使用してストレージシステムと通信します。

デフォルトでは、 Operations Manager コンソールの RBAC 機能は使用されません。RBAC 機能を有効にするには 'napdrive.conf ファイルの変数 `*rbac -method=dfm*' を設定し ' SnapDrive for UNIX デーモンを再起動する必要があります

この機能を使用するには、次の要件を満たしている必要があります。

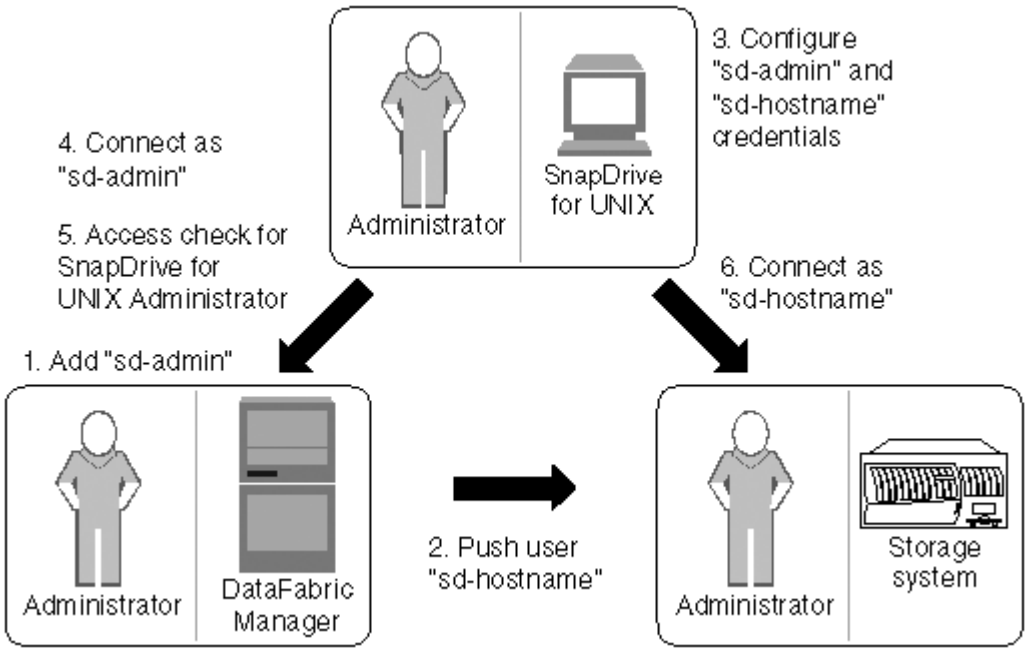
- Operations Manager コンソール 3.7 以降
- SnapDrive ホストとストレージシステムを含む IP ネットワークに、 Operations Manager コンソールサーバが存在し、設定されている必要があります。

- SnapDrive のインストール時に、 Operations Manager コンソールの通信設定を行う必要があります。
- SnapDrive for UNIX デーモンが実行されている必要があります。

SnapDrive for UNIX と Operations Manager コンソールの連携

ロールベースアクセス制御（ RBAC ）の使用は、 Operations Manager コンソールのインフラによって異なります。Operations Manager コンソール管理者は、 UNIX 用の SnapDrive のユーザ名を作成する必要があります。すべてのストレージ操作要求は、最初に Operations Manager コンソールに送信されてアクセスチェックが行われます。Operations Manager コンソールで特定の SnapDrive ユーザのストレージ操作が検証されると、処理が完了します。

次の図は、ストレージ処理用の RBAC 全体を示しています。



1. Operations Manager コンソール管理者が、 Operations Manager コンソールに SD-admin ユーザを追加しました。
2. Operations Manager コンソール管理者がストレージシステムに SD-hostname ユーザを作成します。
3. Operations Manager コンソールの管理者は、 SD-admin と SD-hostname のクレデンシャルを SnapDrive for UNIX 管理者に送信します。
4. SnapDrive 管理者が、受信したユーザクレデンシャルを使用して SnapDrive を設定し
5. SnapDrive 管理者が追加したユーザクレデンシャルを使用して、 Operations Manager コンソールで SnapDrive for UNIX のアクセスチェックが実行されます。
6. SnapDrive ユーザの認証が完了すると、ユーザはストレージシステムに接続できるようになります。

SnapDrive ユーザがストレージ操作を実行する場合は、コマンドラインで対応するコマンドを実行します。要求は、アクセスチェックのために Operations Manager コンソールに送信されます。Operations Manager コン

ソールは、要求されたユーザに SnapDrive 処理を実行するための適切な権限があるかどうかをチェックします。アクセスチェックの結果が SnapDrive に返されます。この結果に応じて、ユーザはストレージシステムに対してストレージ操作を実行できます。

アクセスチェック後にユーザが確認された場合、ユーザは SD-hostname としてストレージシステムに接続します。

> 推奨されるユーザ名は SD-hostname と SD-admin です。SnapDrive for UNIX に他のユーザ名を設定できます。

SnapDrive for UNIX でのロールベースアクセス制御の設定

SnapDrive for UNIX の Role-Based Access Control （ RBAC ；ロールベースアクセス制御）を設定するには、さまざまなタスクを完了する必要があります。このタスクは、Operations Manager コンソールまたはコマンドラインインターフェイスを使用して実行できます。

Operations Manager コンソールでの SD-admin の設定

Operations Manager コンソール管理者は、 SD-admin ユーザを作成できます。

Operations Manager コンソール管理者は、グローバルグループ（グローバル「 FM/Core.AccessCheck 」）でコアアクセスチェックを実行する機能を持つ、 SD-admin という名前のユーザを作成します。Operations Manager コンソール管理者が SD-admin ユーザを設定したら、 SnapDrive for UNIX 管理者に手動でクレデンシャル情報を送信する必要があります。Operations Manager コンソールを使用してユーザーとロールを設定する方法の詳細については、『 Operations Manager Console Administration guide 』およびオンラインヘルプを参照してください。

> SD-admin の代わりに任意の名前を使用できますが、 SD-admin を使用することをお勧めします。

Operations Manager コンソールでロールを作成するには、 * Setup * > * Roles * を選択します。SD-admin 設定ページでは、 Operations Manager コンソール管理者はグローバルグループの「 DFM-Database.Write 」機能を SD-admin-role に割り当てる必要があります。これにより、 SnapDrive for UNIX が Operations Manager コンソールでストレージエンティティを更新できるようになります。

コマンドラインインターフェイスを使用した SD-admin の設定

ストレージシステム管理者は、コマンドラインインターフェイスを使用して SD-admin ユーザを設定できます。

手順

1. SD-admin という名前のユーザーを追加します。

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. SD-admin という名前の管理者を追加します。

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. SD-admin-role という名前のロールを作成します。

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. 手順 3 で作成したロールに機能を追加します。

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. Operations Manager 管理者は、グローバルグループの「 D FM/Database.Write 」機能を「 <SD-admin> 」に付与して、 SnapDrive for UNIX が Operations Manager のストレージシステムエンティティを更新できるようにすることもできます。

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. SD-admin ユーザーに SD-admin-role ロールを追加します。

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

ストレージシステムに **SD-hostname** を追加しています

Operations Manager コンソールの管理者は、 Operations Manager コンソールを使用して、ストレージシステムに SD-hostname ユーザを作成できます。手順の完了後、Operations Manager コンソール管理者は手動で SnapDrive for UNIX 管理者にクレデンシャルを送信する必要があります。SD-hostname の代わりに任意の名前を使用できます

が、 SD-hostname を使用することをお勧めします。

手順

1. ストレージ・システムの root パスワードを取得し、パスワードを保管します。

   ストレージ・システムのパスワードを追加するには、 * Management * > * Storage System * を選択します。

2. UNIX システムごとに SD-hostname ユーザーを作成します。
3. 機能「 api- * 」と「 login- * 」を、 SD- ロールなどのロールに割り当てます。
4. このロール（ sd-role ）を、 sd-usergroup などの新しいユーザグループに含めます。
5. このユーザグループ（ sd-usergroup ）をストレージシステム上の sd-hostname ユーザに関連付けます。

CLI を使用してストレージシステムに **SD-hostname** を追加

ストレージシステム管理者は、 useradmin コマンドを使用して SD-hostname ユーザを作成し、設定できます。

手順

1. ストレージを追加します

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. ホストのパスワードを設定します。

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. ホストにロールを作成します。

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. ユーザグループを作成します。

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. ローカルユーザを作成します。

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

SnapDrive for UNIX でのユーザクレデンシャルの設定

SnapDrive for UNIX 管理者は、 Operations Manager コンソール管理者からユーザクレデンシャルを受け取ります。ストレージが適切に動作するためには、これらのユーザクレデンシャルを SnapDrive で設定する必要があります。

手順

1. ストレージシステムで SD-admin を設定します。

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. ストレージシステムで SD-hostname を設定します。

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. SnapDrive config list コマンドを使用して、手順 1 と手順 2 を確認します。

```
user name       appliance name          appliance type
-------------------------------------------------------
sd-admin        ops_mngr_server         DFM
sd-unix_host    storage_array1          StorageSystem
```

4. SnapDrive for UNIX で Operations Manager コンソールの Role Based Access Control （ RBAC ；役割ベースのアクセス制御）を使用するように設定するには 'napdrive.conf ファイルの構成変数 RBAC -method="dfm" を設定します

> ユーザ・クレデンシャルは暗号化され ' 既存の sdupw ファイルに保存されます以前のファイルのデフォルトの場所は、 /opt/NetApp/snapDrive/.sdupw' です。

Operations Manager コンソールでアクセスチェックを実行するためのユーザ名の形式

SnapDrive for UNIX では、 Operations Manager コンソールによるアクセスチェックの実行にユーザ名の形式を使用します。これらの形式は、 Network Information System （ NIS ；ネットワーク情報システム）とローカルユーザのどちらであるかによって異なります。

SnapDrive for UNIX では、次の形式を使用して、ユーザに特定のタスクの実行が許可されているかどうかを確認します。

- SnapDrive コマンドを実行している NIS ユーザの場合は 'UNIX 用 SnapDrive は '<nisdomain>\<username> の形式を使用します (たとえば 'netapp.com\marc` という形式)
- UNIX ホスト lnx197-141 のようなローカル・ユーザの場合、 SnapDrive for UNIX は「 <hostname>\<username>` 」の形式を使用します（たとえば、「 lnx197-141\john 」）。
- UNIX ホストの管理者（ root ）である場合、 SnapDrive for UNIX は常に管理者をローカルユーザとして扱い、「 lnx197-141\root 」の形式を使用します。

ロールベースアクセス制御の設定変数

ロールベースのアクセス制御に関連するさまざまな構成変数は 'napdrive.conf ファイルで設定する必要があります

変数（ **Variable** ）	説明
contact-http-dfm -port=808080	Operations Manager コンソールサーバとの通信に使用する HTTP ポートを指定します。デフォルト値は 8088. です。
contact-ssl-dfm -port=8488	Operations Manager コンソールサーバとの通信に使用する SSL ポートを指定します。デフォルト値は 8488. です。
rbac - method=dfm	アクセス制御方式を指定します。指定できる値は「 native 」と「 d fm 」です。 値が「 native 」の場合、アクセスチェックにはアクセス制御ファイル「 /vol/vol0/sdprbac/sdhost-name.prbac 」が使用されます。 値が「 d fm 」に設定されている場合、 Operations Manager コンソールが前提条件となります。この場合、 SnapDrive for UNIX は Operations Manager コンソールにアクセスチェックを送信します。

変数（ **Variable** ）	説明
rbac キャッシュ *=on*	SnapDrive for UNIX では、アクセスチェッククエリのキャッシュとそれに対応する結果が保持されます。SnapDrive for UNIX では、設定されているすべての Operations Manager コンソールサーバが停止した場合にのみ、このキャッシュを使用します。 この値を「オン」に設定してキャッシュを有効にするか、「オフ」に設定して無効にすることができます。デフォルト値は off で、 SnapDrive for UNIX で Operations Manager コンソールを使用し、「 RBAC メソッド」の設定変数を「 d fm 」に設定することができます。
rbac キャッシュ *-timeout*	RBAC キャッシュのタイムアウト時間を指定しますこれは '_rbac キャッシュが有効になっている場合にのみ適用されますデフォルト値は「 24 」時間です。 SnapDrive for UNIX では、設定されているすべての Operations Manager コンソールサーバが停止した場合にのみ、このキャッシュを使用します。
use-https-to-dfM=on	この変数を使用すると、 SnapDrive for UNIX が Operations Manager コンソールと通信するときに SSL 暗号化（ HTTPS ）を使用するように設定できます。デフォルト値は「オン」です。

SnapDrive のコマンドと機能

Role-Based Access Control （ RBAC ；ロールベースアクセス制御）では、処理が成功するためにはそれぞれ特定の機能が必要です。ユーザがストレージ操作を実行するには、適切な機能セットを割り当てられている必要があります。

次の表に、必要なコマンドと対応する機能を示します。

コマンドを実行します	機能
「 storage show 」	SD.Storage.Read on volume （ SD 、ストレージ、ボリュームの読み取り
「ストレージリスト」	SD.Storage.Read on volume （ SD 、ストレージ、ボリュームの読み取り
「 storage create 」	• ボリューム内の LUN の場合：「 D 」「 Storage 」「 Write 」 on Volume 」 • qtree 内の LUN の場合：「 D 」「 Storage.Write 」は qtree 上にあります

コマンドを実行します	機能
「ストレージのサイズ変更」	'D.Storage.Write-on LUN （ LUN に書き込み
「 storage delete 」をクリックします	LUN 上の 'D.Storage.Delete
「スナップショー」	'D.snapshot.Read' on volume （ボリューム上のスナップショットを読み取ります
「スナップリスト」	'D.snapshot.Read' on volume （ボリューム上のスナップショットを読み取ります
'snap delete `	'D.Storage.Delete' on volume （ボリュームのデータを削除
'snap rename (仮名の変更	'D.Storage.Write' on volume （ボリュームに書き込みます
'snap connect`	• ボリュームの LUN クローンの場合：ボリューム上の「スナップショット . クローン」 • qtree 内の LUN クローンの場合： qtree 上の「スナップショット . クローン」 • 従来のボリュームクローンの場合：ストレージシステム上の「スナップショット . クローン」 • FlexClone ボリュームの場合：親ボリューム上の「 D.snapshot.Clone 」 • 制限のない FlexClone ボリュームの場合：親ボリューム上の「スナップショット。制限のないクローン」

コマンドを実行します	機能
'snap connect -fit`	• LUN クローン（ LUN クローンおよびボリューム内でのスプリット）の場合：ボリューム上では「スナップショット」、ボリューム上では「スナップショット」、ボリューム上では「ストレージ」「書き込み」 • LUN クローン（ LUN クローンおよび qtree 内でのスプリット）の場合：「 D 」、「スナップショット」、「 Clone 」（ qtree 上でのクローン）、「 D 」「 Storage 」「 Write 」（ストレージ上での書き込み） • 分割された従来のボリュームクローンの場合：ストレージシステム上の「スナップショット」およびストレージシステム上の「 D ストレージ」「書き込み」 • スプリットされた Flex ボリュームクローンの場合は、親ボリューム上の「 D.snapshot.Clone 」。
「 clone split start 」を指定します	• LUN がボリュームまたは qtree に存在する LUN クローンの場合：ボリュームまたは qtree を含む「 D.snapshot.Clone 」 • ボリュームクローンの場合：親ボリューム上の「 D.snapshot.Clone 」
'Snap disconnect' （スナップ切断	• LUN がボリュームまたは qtree に存在する LUN クローンの場合：ボリュームまたは qtree を含む「 D.snapshot.Clone 」 • ボリュームクローンの場合：親ボリューム上の「 D.snapshot.Clone 」 • 無制限のボリュームクローンを削除する場合：ボリューム上の「スナップショット。 DestroyUnrestrictedClone 」
'Snap disconnect-split`	• LUN がボリュームまたは qtree に存在する LUN クローンの場合：「 D 」、「スナップショット」、「クローン」は、 LUN を含むボリュームまたは qtree 上に作成されます • ボリュームクローンの場合：親ボリューム上の「 D 」「ストレージ」「削除」 • 無制限のボリュームクローンを削除する場合：ボリューム上の「スナップショット。 DestroyUnrestrictedClone 」

コマンドを実行します	機能
'snap restore (スナップ復元	• ボリュームに存在する LUN の場合：「スナップショット」「ボリューム上でのリストア」「 D ストレージ」「 LUN 上での書き込み」 • qtree に存在する LUN の場合：「スナップショット。リストア」 qtree では「スナップショット。リストア」、「 D ストレージ . ライト」 LUN では「スナップショット . リストア」 • ボリュームにない LUN の場合：「スナップショット。ボリュームに復元」および「 S D ストレージ」。ボリュームに書き込みます • qtree にない LUN の場合：「スナップショット・リストア」 qtree では「スナップショット・リストア」、「ストレージ・ライト」 qtree では「スナップショット・リストア」 • ボリュームの場合：従来のボリュームの場合はストレージ・システム上の「スナップショット」、フレキシブル・ボリュームの場合は「スナップショット」「リストア」 • ボリュームの単一ファイルの snap restore の場合：ボリュームの「スナップショット。復元」 • qtree の単一ファイルの snap restore の場合 : `s D. snapshot. Restore ` qtree • ベースライン Snapshot コピーを無効にする場合：ボリュームの「スナップショット。ruptBaseline 」
「 host connect 」、「 host disconnect 」です	LUN に「 D.Config.Write 」と入力します
「 config access 」を選択します	ストレージ・システムの 'D.Config.Read
「 config prepare 」	少なくとも 1 つのストレージ・システムで 'D.Config.Write' を実行します
「 config check 」	1 つ以上のストレージ・システムの 'D.Config.Read
「 config show 」を参照してください	1 つ以上のストレージ・システムの 'D.Config.Read
「 config set 」のようになります	「 D.Config.Write 」をストレージシステムに書き込みます
config set-dfm 、 'config set-mgmtpath' 、	少なくとも 1 つのストレージ・システムで 'D.Config.Write' を実行します

コマンドを実行します	機能
「 config delete 」	ストレージ・システムの 'D.Config.Delete]
config delete dfm_appliance 'config delete mgmtpath	少なくとも 1 つのストレージ・システムで 'D.Config.Delete] を選択します
「 config list 」	1 つ以上のストレージ・システムの 'D.Config.Read
'config migrate set	少なくとも 1 つのストレージ・システムで 'D.Config.Write' を実行します
「 config migrate delete 」	少なくとも 1 つのストレージ・システムで 'D.Config.Delete] を選択します
「 config migrate list 」	1 つ以上のストレージ・システムの 'D.Config.Read

SnapDrive for UNIX では、管理者（ root ）の権限はチェックされません。

ユーザロールを簡単に設定できるように事前設定されたロール

事前設定されたロールにより、ユーザへのロールの割り当てが容易になります。

次の表に、事前定義されたロールを示します。

ロール名	説明
GlobalSDStorage の略	SnapDrive for UNIX を使用してストレージを管理します
GlobalSDConfig	SnapDrive for UNIX を使用して構成を管理します
GlobalSDSnapshot	SnapDrive for UNIX を使用して Snapshot コピーを管理します
GlobalSDFullControl の略	UNIX での SnapDrive のフル活用

上記の表の「グローバル」とは、 Operations Manager コンソールで管理されるすべてのストレージシステムのことです。

Operations Manager コンソールでのストレージシステムの自動更新

Operations Manager コンソールでは、ネットワークでサポートされているストレージシ

ステムを検出できます。検出されたストレージシステムから定期的に収集されたデータを監視します。データは設定された間隔で更新されます。Operations Manager コンソール管理者は、更新間隔を設定できます。

LUN の監視間隔、 qtree の監視間隔、 vFiler の監視間隔は、 LUN 、 qtree 、および vFiler の更新頻度を決定する重要なフィールドです。たとえば、ストレージシステムに新しい LUN が作成されても、 Operations Manager コンソールで新しい LUN がすぐに更新されるわけではありません。そのため、その LUN から Operations Manager コンソールへのアクセスチェックが失敗します。この状況を回避するには、要件に合わせて LUN の監視間隔を変更します。

1. 監視間隔を変更するには、 Operations Manager コンソールで * Setup * > * Options * を選択します。
2. Operations Manager コンソール管理者は、コマンドラインインターフェイスで「 d fm host discovery filename 」を実行することにより、 Operations Manager コンソールを強制的に更新することもできます。
3. また、 Operations Manager コンソール管理者は、グローバルグループの「 Dfm.Database.Write 」機能を SD-admin に付与して、 SnapDrive for UNIX が Operations Manager コンソールでストレージシステムエンティティを更新できるようにすることもできます。

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

複数の **Operations Manager** コンソールサーバ

SnapDrive for UNIX は、複数の Operations Manager コンソールサーバをサポートしています。この機能は、ストレージシステムのグループが複数の Operations Manager コンソールサーバで管理されている場合に必要です。SnapDrive for UNIX は、 Operations Manager コンソールサーバが SnapDrive for UNIX で設定されているのと同じ順序で、Operations Manager コンソールサーバにアクセスします。SnapDrive config list コマンドを実行して、設定順序を取得できます。

次に、複数の Operations Manager コンソールサーバの出力例を示します。

```
# snapdrive config list
username    appliance name     appliance type
----------------------------------------------
root        storage_array1     StorageSystem
root        storage_array2     StorageSystem
sd-admin    ops_mngr_server1   DFM
sd-admin    ops_mngr_server2   DFM
```

上記の例では、 storage_array1 は ops_mngr_server1 、 storage_array2 は ops_mngr_servers2 によって管理されています。この例では、 SnapDrive for UNIX contacts ops_mngr_server1 が最初に接続されています。ops_mngr_server1 がアクセスを判別できない場合は 'UNIX の SnapDrive は ops_mngr_server2 と通信します

SnapDrive for UNIX は、次の条件下でのみ 2 番目の Operations Manager コンソールにアクセスします。

- 最初の Operations Manager コンソールがアクセス権を判断できない場合。この状況は、最初の Operations Manager コンソールでストレージシステムが管理されていない場合に発生することがあります。
- 最初の Operations Manager コンソールが停止したとき。

Operations Manager コンソールを使用できません

SnapDrive for UNIX のアクセスチェックには、 Operations Manager コンソールが必要です。Operations Manager コンソールサーバを使用できない理由はさまざまです。

RBAC メソッド `*rbac - method=dfm*' が設定されていて、 Operations Manager コンソールが使用できない場合、 SnapDrive for UNIX では次のエラーメッセージが表示されます。

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive for UNIX では、 Operations Manager コンソールから返されるユーザアクセスチェック結果のキャッシュを保持することもできます。このキャッシュは 24 時間有効で、設定することはできません。Operations Manager コンソールを使用できない場合、 SnapDrive for UNIX はキャッシュを使用してアクセスを判断します。このキャッシュは、設定されているすべての Operations Manager コンソールサーバが応答しない場合にのみ使用されます。

SnapDrive for UNIX でアクセス・チェックにキャッシュを使用するには '_rbac キャッシュ _' 構成変数をオンにして ' アクセス結果のキャッシュを維持する必要がありますコンフィギュレーション変数 '_rbac キャッシュ _' はデフォルトでオフになっています

SnapDrive for UNIX を使用するには 'Operations Manager コンソールが使用できない場合でも ' サーバ管理者は 'napdrive.conf ファイルの role-based access control (RBAC) メソッドを `*rbac -method=native*`' にリセットする必要があります「 `snapdrive.conf` 」ファイルを変更した場合は、 `SnapDrive for UNIX` デーモンを再起動する必要があります。`*rbac -method=native* が設定されている場合 'UNIX 用の SnapDrive を使用できるのは root ユーザだけです

RBAC とストレージ処理の例

ロールベースアクセス制御を使用すると、割り当てられた機能に応じてストレージの処理を実行できます。ストレージ操作を実行するための適切な機能がない場合は、エラーメッセージが表示されます。

1 つのストレージオブジェクトに対して 1 つのファイル仕様を使用する処理

指定したボリューム上でファイル仕様を作成する権限を持つユーザでない場合、SnapDrive for UNIX でエラー・メッセージが表示されます。

_filespec ：ファイルシステム、ホストボリューム、ディスクグループ、または lun_を 指定できます。

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

この例では、 John がルート以外のユーザであり、指定されたボリューム上で filespec を作成する権限がありません。John は、 Operations Manager コンソール管理者に、ボリューム「 Storage_array1:/vol/vol1/vol1 」に対する「 D.Storage.Write 」アクセスを許可するように依頼する必要があります。

複数のストレージ・オブジェクトに対して、単一のファイル仕様を使用する処理

管理者が複数のストレージオブジェクトに対してストレージ操作の実行に必要な権限を持っていない場合、 SnapDrive for UNIX にエラーメッセージが表示されます。

_filespec ：ファイル仕様には、ファイルシステム、ホストボリューム、ディスクグループ、 LUN など、あらゆる種類があります

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2  -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mngr_server
```

この例では、ファイル仕様は、 vol1 と vol2 という 2 つのストレージ・システム・ボリュームに適用されます。UNIX_host の管理者 (root) には、両方のボリュームに対する「 D 」の「 Storage 」「 Write 」アクセス権がありません。そのため、 SnapDrive for UNIX では、ボリュームごとに 1 つのエラーメッセージが表示されます。「 storage create 」を実行するには、管理者（ root ）が Operations Manager コンソール管理者に、両方のボリュームに対する「 D 」ストレージへの書き込みアクセスを許可するように依頼する必要があります。

複数のファイル仕様およびストレージ・オブジェクトを使用する場合

次の例は、特定の操作を実行する権限を持つユーザーでない場合に表示されるエラーメッセージを示しています。

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

この例では、 vol1 と vol2 という 2 つのストレージシステムボリュームに 3 つの LUN があります。ユーザ Marc は nis_domain' および vol2 上で filespec を作成する権限がありませんSnapDrive for UNIX の場合、上記の例では 2 つのエラー・メッセージが表示されます。エラーメッセージには、ユーザには vol1 と vol2 に対する「 D.Storage.Write 」アクセス権が必要であることが示されています。

複数のストレージオブジェクトを使用する処理

次の例は、特定の操作を実行する権限を持つユーザーでない場合に表示されるエラーメッセージを示しています。

```
[john]$ snapdrive storage show -all

Connected LUNs and devices:

device filename   adapter  path  size  proto  state  clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----  -----  --------
---------------
/dev/sdao            -     -     200m  iscsi  online  No
storage_array1:/vol/vol2/passlun1           -
/dev/sda1            -     -     200m  fcp    online  No
storage_array1:/vol/vol2/passlun2           -

Host devices and file systems:

dg: testfs1_SdDg                dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv       mount point: /mnt/testfs1
(persistent) fstype jfs2

device filename   adapter  path  size  proto  state   clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----   -----  --------
---------
/dev/sdn             -      P    108m  iscsi  online   No
storage_array1:/vol/vol2/testfs1_SdLun         -
/dev/sdn1             -      P    108m  fcp  online   No
storage_array1:/vol/vol2/testfs1_SdLun1         -

0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

John は、 vol1 ではなく vol2 上のストレージエンティティのリストを表示する権限を持っています。SnapDrive for UNIX は、 vol1 のエンティティを表示し、 vol2 に関する警告メッセージを表示します。

> 「 storage list 」、「 storage show 」、「 snap list 」、「 snap show 」コマンドの場合、SnapDrive for UNIX はエラーではなく警告を表示します。

複数の **Operations Manager** コンソールサーバを使用してストレージシステムを管理する

次の出力は、ストレージシステムが複数の Operations Manager コンソールで管理されている場合に表示されるエラーメッセージを示しています。

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server1
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user
unix_host\root on Operations Manager server ops_mngr_server2
```

storage_array1 は ops_mngr_server1 、 storage_array2 は ops_mngr_server2 によって管理されます。UNIX_host の管理者は、 storage_array1 および storage_array2 でファイル指定を作成することは許可されていません。上記の SnapDrive for UNIX の例では、アクセスの判別に使用する Operations Manager コンソールを表示しています。