SnapDrive for UNIX のセキュリティ機能

Snapdrive for Unix

NetApp
October 04, 2023

目次

SnapDrive for UNIX のセキュリティ機能

SnapDrive for UNIX を使用する前に、 UNIX のセキュリティ機能について理解し、その機能へのアクセス方法を習得しておく必要があります。

セキュリティ機能とは

SnapDrive for UNIX には、より安全に操作できる特定の機能が用意されています。これらの機能を使用すると、ストレージシステム上でどのユーザが操作を実行できるか、およびどのホストから操作を実行できるかを、より細かく制御できます。

セキュリティ機能を使用すると、次のタスクを実行できます。

- アクセス制御権限を設定します
- ストレージシステムのログイン情報を指定してください
- SnapDrive for UNIX で HTTPS を使用するように指定します

アクセス制御機能を使用すると、 SnapDrive for UNIX を実行するホストがストレージシステムで実行できる操作を指定できます。これらの権限はホストごとに個別に設定します。また、 SnapDrive for UNIX からストレージ・システムへのアクセスを許可するには、そのストレージ・システムのログイン名およびパスワードを入力する必要があります。

HTTPS 機能を使用すると、パスワードの送信など、 Manage ONTAP インターフェイスからストレージシステムへのすべての通信に SSL 暗号化を指定できます。この動作は 'AIX ホスト用の SnapDrive 4.1 以降のリリースではデフォルトですが 'use-https-to-filer 構成変数の値を off に変更すると 'SSL 暗号化を無効にできます

SnapDrive for UNIX でのアクセス制御

SnapDrive for UNIX では、ホストの接続先の各ストレージ・システムに対する各ホストのアクセス・レベルを制御できます。

SnapDrive for UNIX のアクセスレベルは、特定のストレージシステムをターゲットとしてホストが実行できる操作を示します。show 処理と list 処理を除き、アクセス制御権限は Snapshot とストレージのすべての処理に影響する可能性があります。

アクセス制御の設定

ユーザアクセスを判別するために、 SnapDrive for UNIX は、ストレージシステムのルートボリューム内の 2 つのうちの 1 つのアクセス権ファイルをチェックします。アクセス制御を評価するには、対象のファイルに設定されているルールを確認する必要があります。

- 「 dhost-name.prbac 」ファイルは「 /vol/vol0/sdprbac 」ディレクトリ（ SnapDrive 権限ロールベースのアクセス制御）にあります。

  ファイル名は 'dbhost-name.prbac' ですここで '*host-name*' は ' アクセス権が適用されるホストの名前ですストレージシステムに接続されている各ホストのアクセス権ファイルを作成できます。SnapDrive config

access コマンドを使用すると ' 特定のストレージ・システム上のホストに使用できるアクセス権に関する情報を表示できます

「 dhost-name .prbac 」が存在しない場合は、「 dgeneric.prbac 」ファイルを使用してアクセス権を確認します。

- 「 dgeneric.prbac 」ファイルもディレクトリ「 /vol/vol0/sdprbac 」にあります。

  ファイル名「 dgeneric.prbac 」は、ストレージシステム上の「 dbhost-name .prbac 」ファイルにアクセスできない複数のホストのデフォルトアクセス設定として使用されます。

アクセス権限を確認するには、「 dbhost -name.prbac 」ファイルと「 dbgeneric.prbac 」ファイルの両方が必要です。これにより、「 dbhost -name.prbac 」ファイルに指定された値が上書きされるため、アクセス権限が確認されます。

「 dhost-name .prbac 」ファイルと「 dgeneric.prbac 」ファイルの両方がない場合は、「 'napdrive.conf 」ファイルに定義されている構成変数「 _all-access - if -rbac - unspecified _ 」を確認します。

あるホストから特定の vFiler ユニットへのアクセス制御の設定は手動で行います。特定のホストからのアクセスは、影響を受ける vFiler ユニットのルートボリュームにあるファイルによって制御されます。このファイルには '/vol/<vfiler root volume>/sdprbac/sdhost-name .prbac' が含まれていますここで '`*host-name*' は影響を受けるホストの名前で 'gethostname(3)' から返されますこのファイルにアクセスできるホストから、このファイルが読み取り可能であり、書き込み可能でないことを確認してください。

ホスト名を確認するには 'hostname コマンドを実行します

ファイルが空であるか、読み取り不能であるか、または形式が無効な場合、 SnapDrive for UNIX は処理へのホストアクセスを許可しません。

ファイルが見つからない場合、 SnapDrive for UNIX は「 napdrive.conf 」ファイルの設定変数「 _all-access if -rbac -unspecified _ 」をチェックします。この変数が on （デフォルト値）に設定されている場合 ' ホストはそのストレージ・システム上のこれらすべての操作に完全にアクセスできますこの変数が「 off 」に設定されている場合、 SnapDrive for UNIX は、そのストレージ・システムのアクセス制御によって制御されるすべての操作を実行するホスト権限を拒否します。

使用可能なアクセス制御レベル

SnapDrive for UNIX は、ユーザにさまざまなアクセス制御レベルを提供します。これらのアクセスレベルは、 Snapshot コピーとストレージシステムの処理に関連します。

次のアクセスレベルを設定できます。

- none — ホストはストレージシステムにアクセスできません
- snap create — ホストは Snapshot コピーを作成できる。
- スナップの使用 — ホストは Snapshot コピーを削除したり名前を変更したりできます
- すべてスナップ — ホストは Snapshot コピーの作成、復元、削除、および名前変更を行うことができます。
- storage create delete — ホストはストレージの作成、サイズ変更、および削除を行うことができます。
- ストレージ使用量 — ホストはストレージを接続したり切断したり ' ストレージ上でクローンスプリットの

見積もりやクローンスプリットの開始を実行したりすることができます

- Storage All ：ホストは ' ストレージの作成 ' 削除 ' 接続 ' 切断 ' クローン・スプリットの見積もり ' クローン・スプリットの開始をストレージ上で実行できます
- すべてのアクセス — ホストは 'UNIX で上記のすべての SnapDrive へのアクセス権を持っています

レベルはそれぞれ異なります。特定の処理の権限のみを指定した場合、 SnapDrive for UNIX ではそれらの処理のみを実行できます。たとえば、ストレージの使用を指定すると、ホストは SnapDrive for UNIX を使用してストレージに接続したり切断したりできますが、アクセス制御権限によって制御されるその他の処理は実行できません。

アクセス制御権限を設定しています

SnapDrive for UNIX でアクセス制御権限を設定するには、ストレージシステムのルートボリュームに特別なディレクトリとファイルを作成します。

root ユーザとしてログインしていることを確認します。

手順

1. ターゲット・ストレージ・システムのルート・ボリュームに「 dprbac 」というディレクトリを作成します。

   ルートボリュームにアクセスできるようにする方法の 1 つは、 NFS を使用してボリュームをマウントすることです。

2. 権限ファイルを 'dbprbac' ディレクトリに作成します次の記述が正しいことを確認してください。
   - このファイルには 'host-name .prbac' という名前を付ける必要があります host-name は ' アクセス権を指定するホストの名前です
   - ファイルは、 SnapDrive for UNIX がそのファイルを読み取ることができるように読み取り専用にする必要がありますが、変更することはできません。

     dev-sun1 という名前のホストにアクセス権を付与するには ' ストレージ・システム上に次のファイルを作成します `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. そのホストのファイルに権限を設定します。

   ファイルには次の形式を使用する必要があります。

   - 指定できる権限のレベルは 1 つだけです。ホストにすべての操作へのフルアクセスを許可するには、文字列 all access を入力します。
   - 権限の文字列は、ファイルの最初の文字列である必要があります。権限の文字列が 1 行目にない場合、ファイル形式は無効です。
   - 権限文字列では大文字と小文字は区別されません。
   - アクセス許可文字列の前に空白を追加することはできません。
   - コメントは許可されません。

     これらの有効な権限文字列を使用すると、次のアクセスレベルを設定できます。

   - none — ホストはストレージシステムにアクセスできません

- snap create — ホストは Snapshot コピーを作成できる。
- スナップの使用 — ホストは Snapshot コピーを削除したり名前を変更したりできます
- すべてスナップ — ホストは Snapshot コピーの作成、復元、削除、および名前変更を行うことができます。
- storage create delete — ホストはストレージの作成、サイズ変更、および削除を行うことができます。
- ストレージ使用量 — ホストはストレージを接続したり切断したり ' ストレージ上でクローンスプリットの見積もりやクローンスプリットの開始を実行したりすることができます
- Storage All ：ホストは ' ストレージの作成 ' 削除 ' 接続 ' 切断 ' クローン・スプリットの見積もり ' クローン・スプリットの開始をストレージ上で実行できます
- すべてのアクセス — ホストは 'UNIX で上記のすべての SnapDrive へのアクセス権を持っていますこれらの各権限文字列は個別です。snap use を指定すると、ホストは Snapshot コピーの削除や名前変更を実行できますが、 Snapshot コピーの作成やリストア、ストレージプロビジョニング処理の実行はできません。

設定した権限に関係なく、ホストでは表示とリスト表示の処理を実行できます。

4. 次のコマンドを入力して、アクセス権限を確認します。

   'SnapDrive config access show_filer_name_

アクセス制御権限を表示します

アクセス制御権限を表示するには、 SnapDrive config access show コマンドを実行します。

手順

1. SnapDrive config access show コマンドを実行します。

   このコマンドの形式は次のとおりです。 SnapDrive config access ｛ show | list ｝ filename `

   「 show 」または「 list 」のどちらのバージョンのコマンドを入力しても、同じパラメータを使用できます。

   このコマンド・ラインを使用すると、ストレージ・システムの toaster が、ホストに許可されているアクセス許可を判別できます。出力に基づいて、このストレージシステム上のホストに対する権限はすべて snap になります。

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

この例では ' パーミッション・ファイルはストレージ・システム上に存在しないため 'UNIX 用 SnapDrive は 'napdrive.conf ファイル内の変数 _all-access if -rbac -unspecified _ をチェックして ' ホストに付与されているパーミッションを判別しますこの変数は on に設定されます。これは、アクセスレベルが all access に設定された permissions ファイルを作成するのと同じです。

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

この例は ' ストレージ・システム toaster にアクセス権ファイルが存在しない場合に受信するメッセージの種類を示していますまた 'napdrive.conf ファイルの変数 *all-access -if-rbac -unspecified* は 'off' に設定されています

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

ストレージシステムのログイン情報

SnapDrive for UNIX が各ストレージ・システムにアクセスできるように、ユーザ名またはパスワードを設定します。また、 root としてログインしているだけでなく、SnapDrive for UNIX を実行しているユーザーが、プロンプトが表示されたときに正しいユーザー名またはパスワードを入力する必要があるため、セキュリティが確保されます。ログインが侵害された場合は、ログインを削除して、新しいユーザログインを設定できます。

ストレージシステムのセットアップ時に、ユーザログインを作成しておきます。SnapDrive for UNIX をストレージ・システムと連携させるには、このログイン情報を指定する必要があります。ストレージシステムのセットアップ時に指定した内容に応じて、各ストレージシステムは同じログインまたは一意のログインのどちらかを使用できます。

SnapDrive for UNIX では、これらのログインとパスワードが暗号化された形式で各ホストに保存されます。SnapDrive for UNIX がストレージ・システムと通信するときにこの情報を暗号化するように指定するには `*snapdrive.conf*` 構成変数 `use-https-to-filer =on` を設定します

ログイン情報を指定しています

ストレージシステムのユーザログイン情報を指定する必要があります。ストレージシステムのセットアップ時に指定した内容に応じて、各ストレージシステムは同じユーザ名またはパスワード、あるいは一意のユーザ名またはパスワードを使用できます。すべてのストレージシステムが同じユーザ名またはパスワード情報を使用する場合は、次の手順を 1 回だけ実行する必要があります。ストレージシステムで一意のユーザ名またはパスワードを使用する場合は、ストレージシステムごとに次の手順を繰り返す必要があります。

root ユーザとしてログインしていることを確認します。

手順

1. 次のコマンドを入力します。

   ```
   * SnapDrive config set_user_name filename_[_ filename…_]*
   ```

   `user_name` は最初にセットアップしたときにそのストレージ・システムに指定されたユーザー名です

   `filename` はストレージ・システムの名前です

   `*[filename…]* すべてのストレージ・システムに同じユーザ・ログインまたはパスワードが設定されている場合、 1 つのコマンド・ラインに複数のストレージ・システム名を入力できることを定義します。少なくとも 1 つのストレージシステムの名前を入力する必要があります。

2. パスワードがある場合は、プロンプトでパスワードを入力します。

   パスワードが設定されていない場合は、パスワードの入力を求められたら Enter キーを押します。

次に、 toaster というストレージ・システム用に「 root 」というユーザを設定する例を示します。

```
# snapdrive config set `root` toaster
Password for root:
Retype Password:
```

次の例では '3 つのストレージ・システム用に 'root' という名前の 1 つのユーザを設定します

```
# snapdrive config set root toaster oven broiler
Password for root:
Retype Password:
```

3. 別のユーザ名またはパスワードを持つ別のストレージ・システムを使用している場合は、この手順を繰り返します。

SnapDrive for UNIX に関連付けられているストレージシステムのユーザ名の確認

SnapDrive config list' コマンドを実行することにより 'UNIX 用の SnapDrive がストレージ・システムに関連づけられているユーザー名を確認できます

root ユーザとしてログインしておく必要があります。

手順

1. 次のコマンドを入力します。

   「 * SnapDrive config list * 」

   このコマンドは、 SnapDrive for UNIX でユーザが指定した値に一致するすべてのシステムのユーザ名またはストレージシステムのペアを表示します。ストレージシステムのパスワードは表示されません。

   次に、 rapunzel および medium ストレージシステムという名前のストレージシステムに関連付けられているユーザを表示する例を示します。

```
# snapdrive config list
user name           storage system name
-----------------------------
rumplestiltskins    rapunzel
longuser            mediumstoragesystem
```

ストレージシステムのユーザログインを削除する

SnapDrive config delete コマンドを実行すると '1 つ以上のストレージ・システムのユーザー・ログインを削除できます

root ユーザとしてログインしていることを確認します。

手順

1. 次のコマンドを入力します。

   '*SnapDrive config delete_apply_name[apply_name] _ *

   `apply_name` は ' ユーザー・ログイン情報を削除するストレージ・システムの名前です

   SnapDrive for UNIX を使用すると、指定したストレージシステムのユーザ名またはパスワードのログイン情報が削除されます。

   > SnapDrive for UNIX からストレージ・システムにアクセスできるようにするには、新しいユーザ・ログインを指定する必要があります。

HTTP をセットアップしています

ホストプラットフォームに HTTP を使用するように SnapDrive for UNIX を設定できます。

root ユーザとしてログインしていることを確認します。

手順

1. 「 snapdrive.conf 」ファイルのバックアップを作成します。
2. テキストエディタで 'napdrive.conf ファイルを開きます
3. 「 *use-https-to-filer*」 変数の値を「 off 」に変更します。

   「 napdrive.conf 」ファイルを変更する場合は、次の手順を実行することをお勧めします。

   a. 変更する行をコメントとして指定します。
   b. コメント指定した行をコピーします。
   c. コピーしたテキストのコメントを解除するには、シャープ（ # ）記号を削除します。
   d. 値を修正します。
4. 変更を行ったらファイルを保存します。

   SnapDrive for UNIX では、起動するたびにこのファイルが自動的にチェックされます。変更を有効にするには、 SnapDrive for UNIX デーモンを再起動する必要があります。