SnapDrive for UNIX デーモンについて

Snapdrive for Unix

NetApp
October 04, 2023

目次

SnapDrive for UNIX デーモンについて

SnapDrive for UNIX コマンドを実行する前に、 Web サービスおよびデーモンとその使用方法について理解しておく必要があります。SnapDrive for UNIX のすべてのコマンドは、デーモン・サービスを使用して機能します。AIX ホストで SnapDrive for UNIX を使用するには、まずデーモンを開始する必要があります。これにより、 SnapDrive for UNIX を、他のネットアップ製品やネットアップ以外の製品とシームレスかつセキュアに統合することができます。

Web サービスおよびデーモンとは

SnapDrive for UNIX Web サービスは、ネットアップのすべての SnapManager 製品とサードパーティ製品を統一したインターフェイスで、 SnapDrive for UNIX とシームレスに統合します。SnapDrive for UNIX でコマンドラインインターフェイス（ CLI ）コマンドを使用するには、デーモンを開始する必要があります。

各種のネットアップ SnapManager 製品は、コマンドラインインターフェイス（ CLI ）を使用して SnapDrive for UNIX と通信します。CLI を使用すると、 SnapManager および SnapDrive for UNIX のパフォーマンスと管理性に制約があります。SnapDrive for UNIX デーモンを使用する場合、すべてのコマンドは一意のプロセスとして機能します。デーモンサービスは、 SnapDrive for UNIX コマンドの使用方法には影響しません。

SnapDrive for UNIX Web サービスを使用すると、サードパーティ製アプリケーションを SnapDrive for UNIX とシームレスに統合できます。API を使用して SnapDrive for UNIX と連携します。

デーモンを開始すると、 SnapDrive for UNIX デーモンは最初にそのデーモンが実行されているかどうかを確認します。デーモンが実行されていない場合は、デーモンが開始されます。デーモンがすでに実行されている場合に起動しようとすると、 SnapDrive for UNIX のメッセージが表示されます。

SnapDrive デーモンはすでに実行されています

デーモンのステータスを確認して、 SnapDrive for UNIX が実行されているかどうかを確認できます。デーモンを開始するかどうかを決定する前に、ステータスを確認する必要があります。root ユーザ以外のユーザがステータスの確認を試みると、 SnapDrive for UNIX はユーザのクレデンシャルをチェックし、というメッセージを表示します。

SnapDrive デーモンのステータスは root ユーザのみが表示できます

デーモンを停止しようとすると、 SnapDrive for UNIX はクレデンシャルをチェックします。root ユーザ以外のユーザの場合は、 SnapDrive for UNIX のメッセージが表示されます

SnapDrive デーモンを停止できるのは root ユーザのみです

デーモンを停止したら、 SnapDrive for UNIX デーモンを再起動して、構成ファイルまたは任意のモジュールへの変更を有効にする必要があります。root ユーザ以外のユーザが SnapDrive for UNIX デーモンを再起動しようとすると、 SnapDrive for UNIX はユーザのクレデンシャルをチェックし、メッセージを表示します

SnapDrive デーモンは root ユーザによってのみ再起動できます

デーモンのステータスを確認しています

デーモンのステータスをチェックして、デーモンが実行されているかどうかを確認できます。デーモンがすでに実行されている場合は、 SnapDrive for UNIX 構成ファイルが更新されるまで、デーモンを再起動する必要はありません。

root ユーザとしてログインする必要があります。

手順

1. デーモンのステータスを確認します。

   「 * snapdrived status * 」を入力します

SnapDrive for UNIX デーモンを開始しています

SnapDrive for UNIX コマンドを使用するには、まず SnapDrive for UNIX デーモンを開始して実行する必要があります。

root ユーザとしてログインする必要があります。

手順

1. デーモンを開始します。

   ```
   snapdrived start
   ```

デフォルトのデーモンパスワードを変更する

SnapDrive for UNIX には、あとで変更できるデフォルトのデーモンパスワードが割り当てられます。このパスワードは、 root ユーザにのみ割り当てられた読み取りおよび書き込み権限を持つ暗号化されたファイルに保存されます。パスワードを変更した後は、すべてのクライアントアプリケーションに手動で通知する必要があります。

root ユーザとしてログインする必要があります。

手順

1. デフォルトのパスワードを変更します。

   ```
   snapdrived passwd
   ```

2. パスワードを入力します。
3. パスワードを確認します。

デーモンを停止しています

SnapDrive for UNIX の構成ファイルを変更した場合は、デーモンを停止して再起動する

必要があります。デーモンを強制的または強制的に停止できます。

デーモンを強制的に停止しません

SnapDrive for UNIX 構成ファイルが変更された場合、構成ファイルの変更を有効にするにはデーモンを停止する必要があります。デーモンが停止されて再起動されると、構成ファイルの変更が有効になります。デーモンを強制的に停止しないと、キューに入っているすべてのコマンドの実行が完了します。停止要求を受信すると、新しいコマンドは実行されません。

root ユーザとしてログインする必要があります。

1. デーモンを強制的に停止しない場合は、次のコマンドを入力します。

   「 * snapdrived stop * 」というエラーが表示されます

デーモンを強制的に停止します

すべてのコマンドの実行が完了しないようにするには、デーモンを強制的に停止します。デーモンを強制的に停止する要求が受信されると、 SnapDrive for UNIX デーモンは実行中またはキューにあるすべてのコマンドをキャンセルします。デーモンを強制的に停止すると、システムの状態が undefined になることがあります。この方法は推奨されません。

root ユーザとしてログインする必要があります。

手順

1. デーモンを強制的に停止します。

   ```
   snapdrived-force stop
   ```

デーモンを再起動しています

構成ファイルまたは他のモジュールに加えた変更を有効にするには、デーモンを停止したあとに再起動する必要があります。SnapDrive for UNIX デーモンは、実行中およびキューに登録されているすべてのコマンドを完了したあとにのみ再起動されます。再起動要求を受信すると、新しいコマンドは実行されません。

- root ユーザとしてログインしていることを確認します。
- 同じホスト上で他のセッションが並行して実行されていないことを確認します。このような状況では 'napdrived restart' コマンドを実行すると ' システムがハングアップします

手順

1. 次のコマンドを入力してデーモンを再起動します。

   「 * snapdrived restart * 」というメッセージが表示されます

デーモンを強制的に再起動して

デーモンを強制的に再起動できます。デーモンを強制的に再起動すると、実行中のすべてのコマンドの実行が停止します。

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. デーモンを強制的に再起動するには、次のコマンドを入力します。

   「 * snapdrived-force restart * 」を入力します

   強制再起動要求を受信すると ' デーモンは実行中およびキュー内のすべてのコマンドを停止しますデーモンは、実行中のすべてのコマンドの実行をキャンセルした後にのみ再起動されます。

HTTPS を使用したセキュアなデーモン通信

HTTPS を使用して、セキュアな Web サービスやデーモン通信を行うことができます。セキュアな通信を実現するには、「 snapdrive.conf 」ファイルにいくつかの設定変数を設定し、自己署名証明書または CA 署名証明書を生成してインストールします。

自己署名証明書または CA 署名証明書は、「 snapdrive.conf 」ファイルで指定されているパスで提供する必要があります。通信に HTTPS を使用するには 'napdrive.conf ファイルで次のパラメータを設定する必要があります

- 「 use-https-to-SDU -daemon= on 」と入力します
- 'contact-https-port-du-daemon=4095`
- 'du -daemon-certificate-path=/opt/NetApp/snapDrive/snapDrive.pem

> SnapDrive 5.0 for UNIX 以降のバージョンでは、デーモン通信用に HTTPS がサポートされています。デフォルトでは、このオプションは「 off 」に設定されています。

自己署名証明書の生成

SnapDrive for UNIX デーモンサービスでは、認証用の自己署名証明書を生成する必要があります。この認証は、 CLI との通信時に必要になります。

手順

1. RSA キーを生成します。

   *$openssl genrsa 1024> host.key $chmod 400 host.key *``

```
# openssl genrsa 1024 > host.key Generating
RSA private key, 1024 bit long modulus
.............................++++++ ...++++++ e is 65537(0x10001)
# chmod 400 host.key
```

2. 証明書を作成します。

   *$openssl req -new-x509 -nodes-sha1 -days 365 -key host.key > host.cert *

   非暗号化証明書を作成するには '-x509' および -nodes オプションを使用します「 -days 」オプションは、証明書が有効なままになる日数を指定します。

3. 証明書の x509 データを入力するように求められたら、ローカルデータを入力します。

```
# openssl req -new -x509 -nodes -sha1 -days 365 -key host.key >
host.cert
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN. There are quite a few fields
but you can leave some blank For some fields there will be a default
value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Sunnyvale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:abc.com
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:localhost
Email Address []:postmaster@example.org
```

   「 Common Name 」の値は *localhost* である必要があります。

4. メタデータを抽出します（オプション）。

```
$ openssl x509 -noout -fingerprint -text < host.cert > host.info
```

   証明書のメタデータは、あとで簡単に参照できるように保存できます。

5. キーと証明書のデータを結合します。

   SnapDrive for UNIX では、キーと証明書のデータが同じファイルに含まれている必要があります。組み合わせたファイルはキーファイルとして保護する必要があります。

   '$cat host.cert host.key > host.pem

'**&rm host.key**' と入力します

$chmod 400 host.pem

```
# cat host.cert host.key >  /opt/NetApp/snapdrive.pem
# rm host.key rm: remove regular file `host.key'? y
# chmod 400 /opt/NetApp/snapdrive.pem
```

6. デーモン証明書の完全パスを 'napdrive.conf ファイルの *sdu-daemon-certificate-path* 変数に追加します

CA 署名証明書を生成する

SnapDrive for UNIX デーモンサービスでデーモン通信を成功させるには、 CA 署名証明書を生成する必要があります。CA 署名証明書は 'napdrive.conf ファイルに指定されているパスで提供する必要があります

- root ユーザとしてログインする必要があります。
- 通信に HTTPS を使用するには 'napdrive.conf ファイルで次のパラメータを設定しておく必要があります
  - https-to-SDU -daemon = on を使用します
  - contact-https-port-SDdu-daemon = 4095
  - sdu-daemon-certificate-path = /opt/NetApp/snapDrive/snapDrive.pem のようになります

手順

1. PEM 形式の新しい暗号化されていない RSA 秘密鍵を生成します。

   $openssl genrsa-out privkey.pem 1024`

   ```
   Generating RSA private key, 1024 bit long modulus
    ....................++++++ ....................................++++++
   e is 65537 (0x10001)
   ```

2. CA 秘密鍵と証明書 vi /etc/ssl/openssl.cnf を作成するように '/etc/ssl/openssl.cnf を構成します
3. RSA 秘密鍵を使用して署名なし証明書を作成します。

   $openssl req -new-x509 -key privkey.pem-out cer.pem

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank For some
fields there will be a default value, If you enter '.', the field
will be left blank.
-----
Country Name (2 letter code) [XX]:NY
State or Province Name (full name) []:Nebraska Locality Name (eg,
city) [Default City]:Omaha Organization Name (eg, company) [Default
Company Ltd]:abc.com Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:localhost
Email Address []:abc@example.org
```

4. 秘密鍵と証明書を使用して CSR を作成します。

   *cat cert.pem privkey.pem|openssl x509 -x509toreq -signkey privkey.pem-out certreq.csr`

```
Getting request Private Key Generating certificate request
```

5. 作成した CSR を使用して、 CA 秘密鍵で証明書に署名します。

   '**$openssl ca-in certreq.csr-out newcert.pem**

```
Using configuration from /etc/pki/tls/openssl.cnf Check that the
request matches the signature Signature ok Certificate Details:
         Serial Number: 4096 (0x1000)
         Validity
            Not Before: May 17 06:02:51 2015 GMT
             Not After : May 16 06:02:51 2016 GMT
             Subject:
             countryName               = NY
             stateOrProvinceName       = Nebraska
             organizationName          = abc.com
             commonName                = localhost
             emailAddress              = abc@example.org
             X509v3 extensions:
             X509v3 Basic Constraints:
                 CA:FALSE
             X509v3 Key Usage:
                 Digital Signature, Non Repudiation, Key Encipherment
             Netscape Comment:
                 OpenSSL Generated Certificate
             X509v3 Subject Key Identifier:

FB:B0:F6:A0:9B:F2:C2:BC:50:BF:45:B2:9D:DB:AA:3B:C5:07:5B:7F
             X509v3 Authority Key Identifier:

 keyid:FB:B0:F6:A0:9B:F2:C2:BC:50:BF:45:B2:9D:DB:AA:3B:C5:07:5B:7F

 Certificate is to be certified until May 16 06:02:51 2016 GMT (365
 days) Sign the certificate? [y/n]:y


 1 out of 1 certificate requests certified, commit? [y/n]y Write out
 database with 1 new entries Data Base Updated
```

6. SSL サーバで使用する署名済み証明書と秘密鍵をインストールします。

```
The newcert.pem is the certificate signed by your local CA that you can
then use in an
ssl server:
( openssl x509 -in newcert.pem; cat privkey.pem ) > server.pem
ln -s server.pem `openssl x509 -hash -noout -in server.pem`.0 # dot-zero
( server.pem refers to location of https server certificate)
```