# Présentation du démon SnapDrive pour UNIX

Snapdrive for Unix

NetApp
October 22, 2024

# Sommaire

# Présentation du démon SnapDrive pour UNIX

Avant d'exécuter toute commande SnapDrive pour UNIX, vous devez comprendre les services Web et le démon et leur utilisation. Toutes les commandes SnapDrive pour UNIX fonctionnent avec le service démon. Avant de pouvoir utiliser SnapDrive pour UNIX sur votre hôte AIX, vous devez démarrer le démon qui permet à SnapDrive pour UNIX de s'intégrer en toute transparence et en toute sécurité avec d'autres produits NetApp et autres.

## Ce que sont le service Web et le démon

Le service Web SnapDrive pour UNIX offre une interface uniforme pour tous les produits NetApp SnapManager et tiers afin de s'intégrer en toute transparence à SnapDrive pour UNIX. Pour utiliser les commandes de l'interface de ligne de commande dans SnapDrive pour UNIX, vous devez démarrer le démon.

Divers produits NetApp SnapManager utilisent l'interface de ligne de commande pour communiquer avec SnapDrive pour UNIX. L'utilisation de l'interface de ligne de commande impose une contrainte sur les performances et la gestion de SnapManager et SnapDrive pour UNIX. Lorsque vous utilisez le démon SnapDrive pour UNIX, toutes les commandes fonctionnent comme un processus unique. Le service démon n'affecte pas la façon dont les commandes SnapDrive pour UNIX sont utilisées.

Le service Web SnapDrive pour UNIX permet aux applications tierces de s'intégrer de façon transparente à SnapDrive pour UNIX. Ils interagissent avec SnapDrive pour UNIX à l'aide d'API.

Lorsque vous démarrez le démon, SnapDrive for UNIX Daemon vérifie d'abord si ce dernier est en cours d'exécution. Si le démon n'est pas en cours d'exécution, il démarre le démon. Si le démon est déjà en cours d'exécution et que vous essayez de le démarrer, SnapDrive pour UNIX affiche le message suivant :

```
snapdrive daemon is already running
```

Vous pouvez vérifier l'état du démon pour savoir si SnapDrive pour UNIX est en cours d'exécution ou non. Vous devez vérifier l'état avant de décider de démarrer le démon. Si un utilisateur autre que l'utilisateur root tente de vérifier l'état, SnapDrive for UNIX vérifie les informations d'identification de l'utilisateur et affiche le message :

```
snapdrive daemon status can be seen only by root user
```

Lorsque vous essayez d'arrêter le démon, SnapDrive for UNIX vérifie vos informations d'identification. Si vous êtes un utilisateur autre que l'utilisateur root, SnapDrive pour UNIX affiche le message

```
snapdrive daemon can be stopped only by root user
```

Après avoir arrêté le démon, vous devez redémarrer le démon SnapDrive pour UNIX pour que les modifications apportées au fichier de configuration ou à tout module soient appliquées. Si un utilisateur autre que l'utilisateur root tente de redémarrer le démon SnapDrive for UNIX, SnapDrive for UNIX vérifie les informations d'identification de l'utilisateur et affiche le message

```
snapdrive daemon can be restarted only by root user
```

# Vérification de l’état du démon

Vous pouvez vérifier l’état du démon pour savoir si celui-ci est en cours d’exécution. Si le démon est déjà en cours d’exécution, il n’est pas nécessaire de le redémarrer tant que le fichier de configuration SnapDrive pour UNIX n’a pas été mis à jour.

Vous devez être connecté en tant qu’utilisateur racine.

**Étapes**

1. Vérifiez le statut du démon :

   ```
   snapdrived status
   ```

# Démarrage du démon SnapDrive pour UNIX

Vous devez démarrer et exécuter le démon SnapDrive pour UNIX avant de pouvoir utiliser n’importe quelle commande SnapDrive pour UNIX.

Vous devez être connecté en tant qu’utilisateur racine.

**Étapes**

1. Lancez le démon :

   ```
   snapdrived start
   ```

# Modification du mot de passe du démon par défaut

Un mot de passe de démon par défaut est attribué à SnapDrive pour UNIX, que vous pourrez modifier ultérieurement. Ce mot de passe est stocké dans un fichier chiffré avec des autorisations de lecture et d’écriture attribuées uniquement à l’utilisateur root. Une fois le mot de passe modifié, toutes les applications client doivent être notifiées manuellement.

Vous devez être connecté en tant qu’utilisateur racine.

**Étapes**

1. Modifier le mot de passe par défaut :

   ```
   snapdrived passwd
   ```

2. Saisissez le mot de passe.
3. Confirmez le mot de passe.

# Arrêt du démon

Si vous modifiez le fichier de configuration SnapDrive pour UNIX, vous devez arrêter et redémarrer le démon. Vous pouvez arrêter le démon de force ou de force.

### Arrêt non forcé du démon

Si votre fichier de configuration SnapDrive pour UNIX est modifié, vous devez arrêter le démon pour que les modifications apportées au fichier de configuration prennent effet. Une fois le démon arrêté et redémarré, les modifications du fichier de configuration prennent effet. L'arrêt non forcé du démon permet à toutes les commandes mises en file d'attente de terminer l'exécution. Une fois la demande d'arrêt reçue, aucune nouvelle commande n'est exécutée.

Vous devez être connecté en tant qu'utilisateur racine.

1. Entrez la commande suivante pour arrêter le démon de manière non forcée :

   ```
   snapdrived stop
   ```

### Arrêt forcé du démon

Vous pouvez forcer l'arrêt du démon lorsque vous ne voulez pas attendre que toutes les commandes soient terminées. Une fois la demande d'arrêt forcé du démon reçue, le démon SnapDrive pour UNIX annule toutes les commandes en cours d'exécution ou en file d'attente. Lorsque vous arrêtez le démon de force, il est possible que l'état de votre système ne soit pas défini. Cette méthode n'est pas recommandée.

Vous devez être connecté en tant qu'utilisateur racine.

**Étapes**

1. Arrêtez le démon de force :

   ```
   snapdrived -force stop
   ```

# Redémarrage du démon

Vous devez redémarrer le démon après l'avoir arrêté afin que les modifications que vous apportez au fichier de configuration ou aux autres modules prennent effet. Le démon SnapDrive pour UNIX ne redémarre qu'après avoir terminé toutes les commandes en cours d'exécution et en file d'attente. Une fois la demande de redémarrage reçue, aucune nouvelle commande n'est exécutée.

- Assurez-vous d'être connecté en tant qu'utilisateur racine.
- Assurez-vous qu'aucune autre session n'est exécutée sur le même hôte en parallèle. Le `snapdrived restart` la commande bloque le système dans de telles situations.

**Étapes**

1. Entrez la commande suivante pour redémarrer le démon :

   ```
   snapdrived restart
   ```

# Redémarrage forcé du démon

Vous pouvez forcer le redémarrage du démon. Un redémarrage puissant du démon arrête l'exécution de toutes les commandes en cours d'exécution.

Assurez-vous d'être connecté en tant qu'utilisateur racine.

**Étapes**

1. Entrez la commande suivante pour redémarrer avec force le démon :

   ```
   snapdrived -force restart
   ```

   Une fois la demande de redémarrage forcé reçue, le démon arrête toutes les commandes en cours d'exécution et en file d'attente. Le démon n'est redémarré qu'après l'annulation de l'exécution de toutes les commandes en cours d'exécution.

# Sécurisation de la communication par démon à l'aide de HTTPS

Vous pouvez utiliser HTTPS pour des services Web sécurisés et des communications par démon. La communication sécurisée est activée en définissant certaines variables de configuration dans l' `snapdrive.conf` Fichier, génération et installation du certificat auto-signé ou signé par l'autorité de certification.

Vous devez fournir le certificat auto-signé ou signé par l'autorité de certification au chemin indiqué dans le `snapdrive.conf` fichier. Pour utiliser HTTPS pour la communication, vous devez définir les paramètres suivants dans le `snapdrive.conf` fichier :

- `use-https-to-sdu-daemon=on`
- `contact-https-port-sdu-daemon=4095`
- `sdu-daemon-certificate-path=/opt/NetApp/snapdrive/snapdrive.pem`

SnapDrive 5.0 pour UNIX et les versions ultérieures prennent en charge HTTPS pour la communication des démons. Par défaut, l'option est définie sur `off`.

# Génération de certificats auto-signés

Le service démon SnapDrive pour UNIX nécessite la génération d'un certificat auto-signé pour l'authentification. Cette authentification est requise lors de la communication avec l'interface de ligne de commande.

**Étapes**

1. Générer une clé RSA :

   ```
   $ 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. Création du certificat :

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

   Le `-new`, `-x509`, et `-nodes` les options sont utilisées pour créer un certificat non chiffré. Le `-days` indique le nombre de jours pendant lesquels le certificat reste valide.

3. Lorsque vous êtes invité à remplir les données x509 du certificat, saisissez vos données locales :

```
# 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
```

   Le `Common Name` la valeur doit être *localhost*.

4. Extraction des métadonnées (facultatif)

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

   Vous pouvez enregistrer les métadonnées du certificat pour pouvoir les consulter rapidement ultérieurement.

5. Combiner les données de clé et de certificat.

   SnapDrive pour UNIX nécessite que les données de clé et de certificat soient dans le même fichier. Le fichier combiné doit être protégé en tant que fichier de clé.

```
$ cat host.cert host.key > host.pem \

&& rm host.key

$ 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. Ajoutez le chemin complet du certificat du démon au *sdu-daemon-certificate-path* variable du `snapdrive.conf` fichier.

# Génération d'un certificat signé par une autorité de certification

Le service démon SnapDrive pour UNIX nécessite la génération d'un certificat signé par une autorité de certification pour une communication réussie avec le démon. Vous devez fournir le certificat signé par l'autorité de certification au chemin spécifié dans `snapdrive.conf` fichier.

- Vous devez être connecté en tant qu'utilisateur racine.
- Vous devez avoir défini les paramètres suivants dans le `snapdrive.conf` Fichier à utiliser HTTPS pour la communication :
  - use-https-to-sdu-daemon=on
  - contact-https-port-sdu-daemon=4095
  - sdu-chemin-certificat-démon=`/opt/NetApp/snapdrive/snapdrive.pem`

**Étapes**

1. Générer une nouvelle clé privée RSA non chiffrée au format pem :

```
$ openssl genrsa -out privkey.pem 1024
```

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

2. Configurer `/etc/ssl/openssl.cnf` Pour créer la clé privée de l'autorité de certification et le certificat vi `/etc/ssl/openssl.cnf`.
3. Créez un certificat non signé à l'aide de votre clé privée RSA :

```
$ openssl req -new -x509 -key privkey.pem -out cert.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. Utilisez votre clé privée et votre certificat pour créer une RSC :

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

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

5. Signez le certificat avec la clé privée de l'autorité de certification en utilisant la RSC que vous venez de créer :

   **$ 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. Installez le certificat signé et la clé privée à utiliser par un serveur SSL.

```
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)
```