Comprender el daemon SnapDrive para UNIX

Snapdrive for Unix

NetApp
June 20, 2025

Tabla de contenidos

Comprender el daemon SnapDrive para UNIX

Antes de ejecutar cualquier comando de SnapDrive para UNIX, debe comprender los servicios web y el demonio y cómo utilizarlos. Todos los comandos de la SnapDrive para UNIX funcionan utilizando el servicio daemon. Antes de poder utilizar SnapDrive para UNIX en el host AIX, debe iniciar el daemon, que permite que SnapDrive para UNIX se integre de forma segura y sin problemas con otros productos NetApp y que no sean de NetApp.

Qué son el servicio Web y el demonio

El servicio web de SnapDrive para UNIX proporciona una interfaz uniforme para que todos los productos SnapManager y de terceros de NetApp se integren sin problemas con SnapDrive para UNIX. Para utilizar los comandos de la interfaz de línea de comandos (CLI) en SnapDrive para UNIX, tiene que iniciar el daemon.

Varios productos SnapManager de NetApp utilizan la interfaz de línea de comandos (CLI) para comunicarse con SnapDrive para UNIX. El uso de la CLI limita el rendimiento y la capacidad de gestión de SnapManager y SnapDrive para UNIX. Cuando utiliza el daemon SnapDrive para UNIX, todos los comandos funcionan como un proceso único. Daemon Service no afecta a la forma en que se utilizan los comandos de SnapDrive para UNIX.

El servicio web de SnapDrive para UNIX permite que las aplicaciones de terceros se integren perfectamente con SnapDrive para UNIX. Interactúan con SnapDrive para UNIX mediante API.

Al iniciar el daemon, el daemon de SnapDrive para UNIX comprueba primero si el daemon se está ejecutando. Si el daemon no se está ejecutando, se inicia el daemon. Si el daemon ya se está ejecutando e intenta iniciarlo, SnapDrive for UNIX muestra el mensaje:

```
snapdrive daemon is already running
```

Puede comprobar el estado del daemon para ver si SnapDrive para UNIX está en ejecución o no. Debe comprobar el estado antes de decidir iniciar el daemon. Si un usuario que no sea el usuario raíz intenta comprobar el estado, SnapDrive para UNIX comprueba las credenciales del usuario y muestra el mensaje:

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

Cuando intenta detener el daemon, SnapDrive para UNIX comprueba sus credenciales. Si es un usuario distinto de root, SnapDrive for UNIX muestra el mensaje

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

Después de detener el daemon, debe reiniciar el daemon SnapDrive for UNIX para que se apliquen los cambios que se realicen en el archivo de configuración o en cualquier módulo. Si un usuario que no sea el usuario raíz intenta reiniciar el daemon SnapDrive for UNIX, SnapDrive para UNIX comprueba las credenciales del usuario y muestra el mensaje

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

Comprobar el estado del demonio

Puede comprobar el estado del daemon para ver si se está ejecutando. Si el daemon ya se está ejecutando, no es necesario reiniciarlo hasta que se haya actualizado el archivo de configuración de SnapDrive para UNIX.

Debe iniciar sesión como usuario raíz.

Pasos

1. Compruebe el estado del demonio:

   ```
   snapdrived status
   ```

Iniciar el daemon SnapDrive para UNIX

Debe iniciar y ejecutar el daemon SnapDrive para UNIX antes de poder utilizar cualquier comando de SnapDrive para UNIX.

Debe iniciar sesión como usuario raíz.

Pasos

1. Inicie el daemon:

   ```
   snapdrived start
   ```

Cambiando la contraseña predeterminada del demonio

A SnapDrive para UNIX se le asigna una contraseña de daemon predeterminada, que puede cambiar posteriormente. Esta contraseña se almacena en un archivo cifrado con permisos de lectura y escritura asignados únicamente al usuario raíz. Después de cambiar la contraseña, todas las aplicaciones cliente deben ser notificadas manualmente.

Debe iniciar sesión como usuario raíz.

Pasos

1. Cambie la contraseña predeterminada:

   ```
   snapdrived passwd
   ```

2. Introduzca la contraseña.
3. Confirme la contraseña.

Detener el daemon

Si cambia el archivo de configuración de SnapDrive para UNIX, debe detener y reiniciar el daemon. Puede detener el demonio de manera no forzada o forzada.

Detener al demonio de manera no forzada

Si se cambia el archivo de configuración de SnapDrive para UNIX, debe detener el daemon para que el archivo de configuración tenga efecto. Después de que el daemon se detenga y se reinicie, los cambios en el archivo de configuración tienen efecto. Al detener el daemon de forma no forzada, todos los comandos en la cola pueden completar la ejecución. Una vez recibida la solicitud de detención, no se ejecutan nuevos comandos.

Debe iniciar sesión como usuario raíz.

1. Introduzca el siguiente comando para detener el demonio de forma no forzada:

   ```
   snapdrived stop
   ```

Detener al demonio por la fuerza

Puede detener el daemon de manera forzada si no desea esperar a que todos los comandos completen la ejecución. Tras recibir la solicitud de detener el daemon de manera forzada, el daemon SnapDrive for UNIX cancela cualquier comando que se encuentre en ejecución o en cola. Cuando detenga el daemon de manera forzada, el estado de su sistema podría no estar definido. No se recomienda utilizar este método.

Debe iniciar sesión como usuario raíz.

Pasos

1. Detenga forzosamente el demonio:

   ```
   snapdrived -force stop
   ```

Reiniciar el daemon

Debe reiniciar el daemon después de detenerlo para que los cambios que realice en el archivo de configuración o en los demás módulos surtan efecto. El daemon SnapDrive para UNIX sólo se reinicia después de completar todos los comandos que se encuentran en ejecución y en cola. Una vez recibida la solicitud de reinicio, no se ejecutan nuevos comandos.

- Asegúrese de que ha iniciado sesión como usuario raíz.
- Asegúrese de que no existan otras sesiones en ejecución en el mismo host en paralelo. La `snapdrived restart` el comando bloquea el sistema en estas situaciones.

Pasos

1. Introduzca el siguiente comando para reiniciar el daemon:

   ```
   snapdrived restart
   ```

Forzado del reinicio del demonio

Puede forzar el reinicio del demonio. Un reinicio enérgico del daemon detiene la ejecución de todos los comandos en ejecución.

Asegúrese de que ha iniciado sesión como usuario raíz.

Pasos

1. Introduzca el siguiente comando para reiniciar el daemon de forma forzada:

   ```
   snapdrived -force restart
   ```

   Una vez recibida la solicitud de reinicio de fuerza, el daemon detiene todos los comandos en ejecución y en cola. El daemon se reinicia sólo después de cancelar la ejecución de todos los comandos en ejecución.

Comunicación de demonio segura mediante HTTPS

Puede utilizar HTTPS para proteger los servicios web y la comunicación del demonio. La comunicación segura se habilita mediante el establecimiento de algunas variables de configuración en `snapdrive.conf` Archivo, y generar e instalar el certificado autofirmado o firmado por CA.

Debe proporcionar el certificado autofirmado o firmado por CA en la ruta especificada en el `snapdrive.conf` archivo. Para usar HTTPS para la comunicación, debe configurar los parámetros siguientes en el `snapdrive.conf` archivo:

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

SnapDrive 5.0 para UNIX y las versiones posteriores admiten HTTPS para la comunicación del demonio. De forma predeterminada, la opción se establece en `off`.

Generación de certificados autofirmados

El servicio del demonio de SnapDrive para UNIX requiere que genere un certificado autofirmado para la autenticación. Es necesario esta autenticación mientras se comunica con la CLI.

Pasos

1. Genere una clave 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. Cree el certificado:

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

La `-new`, `-x509`, y. `-nodes` las opciones se utilizan para crear un certificado no cifrado. La `-days` la opción especifica la cantidad de días que el certificado sigue siendo válido.

3. Cuando se le solicite que rellene los datos x509 del certificado, introduzca los datos 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
```

La `Common Name` el valor debe ser *localhost*.

4. Extraer metadatos (opcional).

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

Es posible guardar los metadatos del certificado para consultarlo más adelante.

5. Combinar datos de clave y certificado.

SnapDrive para UNIX requiere que los datos de la clave y del certificado estén en el mismo archivo. Debe protegerse el archivo combinado como archivo de claves.

**$ 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. Agregue la ruta completa del certificado del daemon al *sdu-daemon-certificate-path* variable de `snapdrive.conf` archivo.

Generar un certificado firmado por CA

El servicio de daemon SnapDrive para UNIX requiere que se genere un certificado firmado por CA para que la comunicación se realice correctamente. Debe proporcionar el certificado firmado por CA en la ruta especificada en `snapdrive.conf` archivo.

- Debe iniciar sesión como usuario raíz.
- Debe haber configurado los siguientes parámetros en el `snapdrive.conf` Archivo que se va a utilizar HTTPS para la comunicación:
  - use-https-to-sdu-daemon=on
  - contact-https-port-sdu-daemon=4095
  - sdu-daemon-certificate-path=`/opt/NetApp/snapdrive/snapdrive.pem`

Pasos

1. Generar una nueva clave privada RSA sin cifrar en formato pem:

   $ openssl genrsa -out privkey.pem 1024

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

2. Configurar `/etc/ssl/openssl.cnf` Para crear la clave privada de CA y el certificado vi `/etc/ssl/openssl.cnf`.
3. Cree un certificado sin firmar utilizando su clave privada 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. Utilice su clave privada y su certificado para crear una CSR:

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

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

5. Firme el certificado con la clave privada de CA mediante la CSR que acaba de crear:

   $ 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. Instale el certificado firmado y la clave privada que utilizará un servidor 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)
```

Información de copyright

Información de la marca comercial