Informazioni sul daemon SnapDrive per UNIX

Snapdrive for Unix

NetApp
October 04, 2023

Sommario

Informazioni sul daemon SnapDrive per UNIX

Prima di eseguire qualsiasi comando SnapDrive per UNIX, è necessario conoscere i servizi Web e il daemon e come utilizzarli. Tutti i comandi di SnapDrive per UNIX funzionano utilizzando il servizio daemon. Prima di poter utilizzare SnapDrive per UNIX sull'host AIX, è necessario avviare il daemon, che consente a SnapDrive per UNIX di integrarsi perfettamente e in modo sicuro con altri prodotti NetApp e non.

Cosa sono il servizio Web e il daemon

Il servizio Web SnapDrive per UNIX fornisce un'interfaccia uniforme per tutti i prodotti NetApp SnapManager e di terze parti per integrarsi perfettamente con SnapDrive per UNIX. Per utilizzare i comandi dell'interfaccia a riga di comando (CLI) in SnapDrive per UNIX, è necessario avviare il daemon.

Diversi prodotti NetApp SnapManager utilizzano l'interfaccia a riga di comando (CLI) per comunicare con SnapDrive per UNIX. L'utilizzo della CLI pone un limite alle performance e alla gestibilità di SnapManager e SnapDrive per UNIX. Quando si utilizza il daemon SnapDrive per UNIX, tutti i comandi funzionano come un processo unico. Il servizio daemon non influisce sul modo in cui vengono utilizzati i comandi SnapDrive per UNIX.

Il servizio Web SnapDrive per UNIX consente alle applicazioni di terze parti di integrarsi perfettamente con SnapDrive per UNIX. Interagiscono con SnapDrive per UNIX utilizzando API.

All'avvio del daemon, SnapDrive per UNIX verifica prima se il daemon è in esecuzione. Se il daemon non è in esecuzione, avvia il daemon. Se il daemon è già in esecuzione e si tenta di avviarlo, SnapDrive per UNIX visualizza il messaggio:

```
snapdrive daemon is already running
```

È possibile controllare lo stato del daemon per verificare se SnapDrive per UNIX è in esecuzione o meno. Controllare lo stato prima di decidere di avviare il daemon. Se un utente diverso dall'utente root tenta di controllare lo stato, SnapDrive per UNIX verifica le credenziali dell'utente e visualizza il messaggio:

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

Quando si tenta di arrestare il daemon, SnapDrive per UNIX verifica le credenziali. Se si è un utente diverso da quello root, SnapDrive per UNIX visualizza il messaggio

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

Dopo aver interrotto il daemon, è necessario riavviare il daemon SnapDrive per UNIX per rendere effettive le modifiche apportate al file di configurazione o a qualsiasi modulo. Se un utente diverso dall'utente root tenta di riavviare il daemon SnapDrive per UNIX, SnapDrive per UNIX verifica le credenziali dell'utente e visualizza il messaggio

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

Verifica dello stato del daemon

È possibile controllare lo stato del daemon per verificare se il daemon è in esecuzione. Se il daemon è già in esecuzione, non è necessario riavviarlo finché il file di configurazione di SnapDrive per UNIX non è stato aggiornato.

Devi essere connesso come utente root.

Fasi

1. Controllare lo stato del daemon:

   ```
   snapdrived status
   ```

Avvio del daemon SnapDrive per UNIX

È necessario avviare ed eseguire il daemon SnapDrive per UNIX prima di poter utilizzare qualsiasi comando SnapDrive per UNIX.

Devi essere connesso come utente root.

Fasi

1. Avviare il daemon:

   ```
   snapdrived start
   ```

Modifica della password predefinita del daemon

A SnapDrive per UNIX viene assegnata una password daemon predefinita, che è possibile modificare in seguito. Questa password viene memorizzata in un file crittografato con permessi di lettura e scrittura assegnati solo all'utente root. Una volta modificata la password, tutte le applicazioni client devono essere avvisate manualmente.

Devi essere connesso come utente root.

Fasi

1. Modificare la password predefinita:

   ```
   snapdrived passwd
   ```

2. Inserire la password.
3. Confermare la password.

Arrestare il daemon

Se si modifica il file di configurazione di SnapDrive per UNIX, è necessario arrestare e riavviare il daemon. Puoi fermare il demone in modo non forzato o forzato.

Arresto non forzato del demone

Se il file di configurazione di SnapDrive per UNIX viene modificato, è necessario arrestare il daemon per rendere effettive le modifiche apportate al file di configurazione. Una volta arrestato e riavviato il daemon, le modifiche apportate al file di configurazione diventano effettive. L'arresto non forzato del daemon consente a tutti i comandi in coda di completare l'esecuzione. Una volta ricevuta la richiesta di arresto, non vengono eseguiti nuovi comandi.

Devi essere connesso come utente root.

1. Immettere il seguente comando per arrestare il daemon in modo non forzato:

   ```
   snapdrived stop
   ```

Arrestare il demone con la forza

È possibile arrestare forzatamente il daemon quando non si desidera attendere il completamento dell'esecuzione di tutti i comandi. Una volta ricevuta la richiesta di arrestare forzatamente il daemon, SnapDrive per UNIX annulla tutti i comandi in esecuzione o in coda. Quando si arresta forzatamente il daemon, lo stato del sistema potrebbe non essere definito. Questo metodo non è consigliato.

Devi essere connesso come utente root.

Fasi

1. Arrestare il demone con la forza:

   ```
   snapdrived -force stop
   ```

Riavviare il daemon

È necessario riavviare il daemon dopo averlo interrotto in modo che le modifiche apportate al file di configurazione o agli altri moduli abbiano effetto. Il daemon SnapDrive per UNIX viene riavviato solo dopo aver completato tutti i comandi in esecuzione e in coda. Una volta ricevuta la richiesta di riavvio, non vengono eseguiti nuovi comandi.

- Assicurarsi di aver effettuato l'accesso come utente root.
- Assicurarsi che sullo stesso host non siano in esecuzione altre sessioni in parallelo. Il `snapdrived restart` il comando blocca il sistema in tali situazioni.

Fasi

1. Immettere il seguente comando per riavviare il daemon:

   ```
   snapdrived restart
   ```

Forzare il riavvio del daemon

È possibile forzare il riavvio del daemon. Un riavvio forzato del daemon interrompe l'esecuzione di tutti i comandi in esecuzione.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Immettere il seguente comando per riavviare forzatamente il daemon:

   ```
   snapdrived -force restart
   ```

   Una volta ricevuta la richiesta di riavvio forzato, il daemon arresta tutti i comandi in esecuzione e in coda. Il daemon viene riavviato solo dopo aver cancellato l'esecuzione di tutti i comandi in esecuzione.

Comunicazione sicura con i daemon tramite HTTPS

È possibile utilizzare HTTPS per servizi Web sicuri e comunicazioni daemon. La comunicazione protetta viene attivata impostando alcune variabili di configurazione in `snapdrive.conf` Generare e installare il certificato autofirmato o firmato dalla CA.

È necessario fornire il certificato autofirmato o firmato dalla CA nel percorso specificato in `snapdrive.conf` file. Per utilizzare HTTPS per la comunicazione, è necessario impostare i seguenti parametri in `snapdrive.conf` file:

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

> SnapDrive 5.0 per UNIX e versioni successive supportano HTTPS per la comunicazione daemon. Per impostazione predefinita, l'opzione è impostata su `off`.

Creazione di certificati autofirmati

Il servizio daemon SnapDrive per UNIX richiede la creazione di un certificato autofirmato per l'autenticazione. Questa autenticazione è necessaria durante la comunicazione con la CLI.

Fasi

1. Generare una chiave 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. Creare il certificato:

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

   Il `-new`, `-x509`, e. `-nodes` le opzioni vengono utilizzate per creare un certificato non crittografato. Il `-days` l'opzione specifica il numero di giorni in cui il certificato rimane valido.

3. Quando viene richiesto di compilare i dati x509 del certificato, inserire i dati locali:

```
# 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
```

   Il `Common Name` il valore deve essere *localhost*.

4. Estrarre i metadati (facoltativo).

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

   È possibile salvare i metadati del certificato per un riferimento rapido in un secondo momento.

5. Combinazione di dati chiave e certificato.

   SnapDrive per UNIX richiede che i dati della chiave e del certificato siano nello stesso file. Il file combinato deve essere protetto come file chiave.

   **$ 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. Aggiungere il percorso completo del certificato daemon a *`sdu-daemon-certificate-path`* variabile di `snapdrive.conf` file.

Creazione di un certificato firmato dalla CA

Il servizio daemon SnapDrive per UNIX richiede la generazione di un certificato firmato da CA per la comunicazione daemon. È necessario fornire il certificato firmato dalla CA nel percorso specificato in `snapdrive.conf` file.

- Devi essere connesso come utente root.
- È necessario impostare i seguenti parametri in `snapdrive.conf` File per utilizzare HTTPS per la comunicazione:
  - use-https-to-sdu-daemon=on
  - contact-https-port-sdu-daemon=4095
  - sdu-daemon-certificate-path=`/opt/NetApp/snapdrive/snapdrive.pem`

Fasi

1. Generare una nuova chiave privata RSA non crittografata in un formato pem:

   $ openssl genrsa -out privkey.pem 1024

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

2. Configurare `/etc/ssl/openssl.cnf` Per creare la chiave privata della CA e il certificato vi `/etc/ssl/openssl.cnf`.
3. Creare un certificato senza firma utilizzando la chiave privata 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. Utilizzare la chiave privata e il certificato per creare una CSR:

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

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

5. Firmare il certificato con la chiave privata della CA utilizzando la CSR appena creata:

   `$ 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. Installare il certificato firmato e la chiave privata che devono essere utilizzati da un server 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)
```