UNIX용 SnapDrive 데몬 이해

Snapdrive for Unix

NetApp
June 20, 2025

목차

UNIX용 SnapDrive 데몬 이해

UNIX용 SnapDrive 명령을 실행하기 전에 웹 서비스 및 데몬과 그 사용 방법을 이해해야 합니다. 모든 UNIX용 SnapDrive 명령은 데몬 서비스를 사용하여 작동합니다. AIX 호스트에서 UNIX용 SnapDrive를 사용하려면 먼저 데몬을 시작해야 합니다. 그러면 SnapDrive for UNIX가 다른 NetApp 제품 및 비 NetApp 제품과 원활하고 안전하게 통합될 수 있습니다.

웹 서비스 및 데몬은 무엇입니까

UNIX용 SnapDrive 웹 서비스는 모든 NetApp SnapManager 및 타사 제품에 대해 일관된 인터페이스를 제공하므로 UNIX용 SnapDrive와 원활하게 통합할 수 있습니다. SnapDrive for UNIX에서 CLI(Command-Line Interface) 명령을 사용하려면 데몬을 시작해야 합니다.

다양한 NetApp SnapManager 제품은 CLI(Command-Line Interface)를 사용하여 UNIX용 SnapDrive와 통신합니다. CLI를 사용하면 SnapManager 및 UNIX용 SnapDrive의 성능과 관리 편의성에 제약이 있습니다. UNIX용 SnapDrive 데몬을 사용하는 경우 모든 명령이 고유한 프로세스로 작동합니다. 데몬 서비스는 SnapDrive for UNIX 명령 사용 방법에 영향을 주지 않습니다.

UNIX용 SnapDrive 웹 서비스를 사용하면 타사 애플리케이션을 UNIX용 SnapDrive와 원활하게 통합할 수 있습니다. API를 사용하여 UNIX용 SnapDrive와 상호 작용합니다.

데몬을 시작하면 SnapDrive for UNIX 데몬이 먼저 데몬이 실행 중인지 확인합니다. 데몬이 실행되고 있지 않으면 데몬을 시작합니다. 데몬이 이미 실행 중이고 데몬을 시작하려고 하면 SnapDrive for UNIX에 다음 메시지가 표시됩니다.

SnapDrive 디먼이 이미 실행 중입니다

데몬의 상태를 확인하여 SnapDrive for UNIX가 실행 중인지 여부를 확인할 수 있습니다. 데몬을 시작하기로 결정하기 전에 상태를 확인해야 합니다. 루트 사용자 이외의 사용자가 상태를 확인하려고 하면 SnapDrive for UNIX는 사용자의 자격 증명을 확인하고 다음 메시지를 표시합니다.

SnapDrive 디몬 상태는 루트 사용자만 볼 수 있습니다

데몬을 중지하려고 하면 SnapDrive for UNIX에서 자격 증명을 확인합니다. 루트 사용자가 아닌 사용자인 경우 UNIX용 SnapDrive에서 메시지를 표시합니다

SnapDrive 데몬은 루트 사용자만 중지할 수 있습니다

데몬을 중지한 후 구성 파일 또는 모듈의 변경 내용을 적용하려면 UNIX용 SnapDrive 데몬을 다시 시작해야 합니다. 루트 사용자 이외의 사용자가 SnapDrive for UNIX 데몬을 다시 시작하려고 하면 SnapDrive for UNIX는 사용자의 자격 증명을 확인하고 메시지를 표시합니다

SnapDrive 데몬은 루트 사용자만 재시작할 수 있습니다

데몬의 상태를 확인하는 중입니다

데몬의 상태를 확인하여 데몬이 실행 중인지 확인할 수 있습니다. 데몬이 이미 실행 중인 경우에는 SnapDrive for UNIX 구성 파일이 업데이트될 때까지 데몬을 다시 시작할 필요가

없습니다.

루트 사용자로 로그인해야 합니다.

단계

1. 데몬의 상태를 확인합니다.

   '* 스냅샷 상태 * '

UNIX용 SnapDrive 데몬을 시작합니다

UNIX용 SnapDrive 명령을 사용하려면 먼저 UNIX용 SnapDrive 데몬을 시작하고 실행해야 합니다.

루트 사용자로 로그인해야 합니다.

단계

1. 데몬을 시작합니다.

   ``스냅드라이브 시작 *'

기본 데몬 암호를 변경하는 중입니다

SnapDrive for UNIX에는 나중에 변경할 수 있는 기본 데몬 암호가 할당되어 있습니다. 이 암호는 암호화된 파일에 저장되며 읽기 및 쓰기 권한이 루트 사용자만 할당됩니다. 암호를 변경한 후에는 모든 클라이언트 응용 프로그램에 수동으로 알려야 합니다.

루트 사용자로 로그인해야 합니다.

단계

1. 기본 암호 변경:

   ``스냅드라이브 암호 *'

2. 암호를 입력합니다.
3. 암호를 확인합니다.

데몬을 중지하는 중입니다

UNIX용 SnapDrive 구성 파일을 변경하는 경우 데몬을 중지한 후 다시 시작해야 합니다. 데몬을 강제로 또는 강제로 중지할 수 있습니다.

데몬을 강제로 중지하지 않습니다

SnapDrive for UNIX 구성 파일이 변경된 경우 구성 파일 변경 내용을 적용하려면 데몬을

중지해야 합니다. 데몬이 중지되었다가 다시 시작된 후 구성 파일의 변경 사항이 적용됩니다. 데몬을 강제로 중지하지 않고 중지하면 대기 중인 모든 명령이 실행을 완료할 수 있습니다. STOP 요청을 수신한 후 새로운 명령어가 실행되지 않는다.

루트 사용자로 로그인해야 합니다.

1. 다음 명령을 입력하여 데몬을 강제로 중지합니다.

   ``스냅드라이브 정지*'

데몬을 강제로 중지합니다

모든 명령이 실행될 때까지 기다리지 않으려면 데몬을 강제로 중지할 수 있습니다. 데몬을 강제로 중지하라는 요청이 수신되면 SnapDrive for UNIX 데몬이 실행 중이거나 대기열에 있는 모든 명령을 취소합니다. 데몬을 강제로 중지하면 시스템의 상태가 정의되지 않을 수 있습니다. 이 방법은 권장되지 않습니다.

루트 사용자로 로그인해야 합니다.

단계

1. 데몬을 강제로 중지합니다.

   ``스냅드브드-포스 스탑 *''

데몬을 다시 시작하는 중입니다

구성 파일 또는 다른 모듈에 대한 변경 사항이 적용되도록 데몬을 중지한 후 다시 시작해야 합니다. SnapDrive for UNIX 데몬은 실행 중인 모든 명령과 대기열에 있는 명령을 모두 완료한 후에만 다시 시작됩니다. 재시작 요청이 수신되면 새로운 명령어가 실행되지 않는다.

- 루트 사용자로 로그인했는지 확인합니다.
- 동일한 호스트에서 병렬로 실행 중인 다른 세션이 없는지 확인합니다. 이 경우 '드라이브 재시작' 명령이 시스템을 중단한다.

단계

1. 다음 명령을 입력하여 데몬을 재시작합니다.

   ``스냅드라이브 재시작*'

강제 데몬 재시작

데몬을 강제로 다시 시작할 수 있습니다. 데몬을 강제로 다시 시작하면 실행 중인 모든 명령이 실행되지 않습니다.

루트 사용자로 로그인했는지 확인합니다.

단계

1. 다음 명령을 입력하여 데몬을 강제로 재시작합니다.

   ``스냅드라이브 강제 재시작*''

   강제 재시작 요청이 수신되면 데몬은 실행 중인 모든 명령과 대기열에 있는 명령을 모두 중지합니다. 데몬은 실행 중인 모든 명령의 실행을 취소한 후에만 다시 시작됩니다.

HTTPS를 사용하여 데몬 통신을 보호합니다

HTTPS를 사용하여 보안 웹 서비스 및 데몬 통신을 수행할 수 있습니다. 보안 통신은 'sapdrive.conf' 파일에 일부 구성 변수를 설정하고 자체 서명 또는 CA 서명 인증서를 생성 및 설치하여 활성화합니다.

'napdrive.conf' 파일에 지정된 경로에 자체 서명 또는 CA 서명 인증서를 제공해야 합니다. 통신에 HTTPS를 사용하려면 'napdrive.conf' 파일에서 다음 매개변수를 설정해야 합니다.

- 'use-https-to-SDU-daemon=on
- contact-https-port-SDU-daemon=4095
- 'du-daemon-certificate-path=/opt/netapp/SnapDrive/SnapDrive.pem'

SnapDrive 5.0 for UNIX 이상 버전은 데몬 통신을 위해 HTTPS를 지원합니다. 기본적으로 이 옵션은 '꺼짐'으로 설정됩니다.

자체 서명된 인증서를 생성하는 중입니다

SnapDrive for UNIX 데몬 서비스를 사용하려면 인증을 위해 자체 서명된 인증서를 생성해야 합니다. CLI와 통신하는 동안 이 인증이 필요합니다.

단계

1. RSA 키 생성:

   "*$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. 인증서 생성:

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

   암호화되지 않은 인증서를 만드는 데 '-new', -x509', -nodes 옵션이 사용됩니다. '-days' 옵션은 인증서가 유효한 상태로 유지되는 일 수를 지정합니다.

3. 인증서의 x509 데이터를 채우라는 메시지가 나타나면 로컬 데이터를 입력합니다.

```
# 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
```

공통 이름 값은 _localhost_이어야 합니다.

4. 메타데이터 추출(선택 사항)

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

나중에 빠르게 참조할 수 있도록 인증서 메타데이터를 저장할 수 있습니다.

5. 키와 인증서 데이터를 결합합니다.

UNIX용 SnapDrive를 사용하려면 키와 인증서 데이터가 같은 파일에 있어야 합니다. 결합된 파일은 키 파일로 보호해야 합니다.

"$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. daemon 인증서의 전체 경로를 sapdrive.conf 파일의 '*SDU-daemon-certificate-path*' 변수에 추가합니다.

CA 서명 인증서를 생성하는 중입니다

SnapDrive for UNIX 데몬 서비스를 사용하려면 데몬 통신에 사용할 CA 서명 인증서를 생성해야 합니다. 'napdrive.conf' 파일에 지정된 경로에 CA 서명 인증서를 제공해야 합니다.

- 루트 사용자로 로그인해야 합니다.
- 통신에 HTTPS를 사용하려면 'napdrive.conf' 파일에서 다음 매개 변수를 설정해야 합니다.
  - https-to-SDU-daemon=on을 사용합니다
  - Contact-https-port-SDU-daemon = 4095
  - SDU-daemon-certificate-path="/opt/NetApp/SnapDrive/SnapDrive.pem"

단계

1. PEM 형식으로 암호화되지 않은 새 RSA 개인 키를 생성합니다.

   '*$openssl genrsa-out privkey.pem 1024 *'

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

2. CA 개인 키와 인증서 vi '/etc/ssl/opensssl.cnf'를 생성하도록 '/etc/ssl/openssl.cnf'를 구성합니다.
3. RSA 개인 키를 사용하여 서명되지 않은 인증서를 생성합니다.

   '*$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. 개인 키와 인증서를 사용하여 CSR을 생성합니다.

   '* cat certt. pem privkey.pem|openssl x509-x509torq -signkey privkey.pem-out certreq.csr *'

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

5. 방금 만든 CSR을 사용하여 CA 개인 키로 인증서에 서명합니다.

   '*$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 서버에서 사용할 서명된 인증서와 개인 키를 설치합니다.

```
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)
```

저작권 정보

상표 정보