



Informationen zum SnapDrive for UNIX Daemon

Snapdrive for Unix

NetApp
February 20, 2023

Inhaltsverzeichnis

- Informationen zum SnapDrive for UNIX Daemon 1
 - Was der Webdienst und der Daemon sind 1
 - Überprüfen des Status des Daemon 2
 - Starten des SnapDrive for UNIX Daemon 2
 - Ändern des Standard-Daemon-Passworts 2
 - Beenden des Daemon 2
 - Starten Sie den Daemon neu 3
 - Erzwingen des Neustarts des Daemon 4
 - Sichere Daemon Kommunikation mit HTTPS 4
 - Selbstsignierte Zertifikate werden generiert 4
 - Erstellen eines CA-signierten Zertifikats 6

Informationen zum SnapDrive for UNIX Daemon

Bevor Sie einen SnapDrive for UNIX-Befehl ausführen, müssen Sie die Web-Services und den Daemon verstehen und wie Sie diese verwenden. Alle Befehle von SnapDrive für UNIX verwenden den Daemon Service. Bevor Sie SnapDrive für UNIX auf Ihrem AIX Host verwenden können, müssen Sie den Daemon starten, um SnapDrive für UNIX nahtlos und sicher mit anderen Produkten von NetApp und anderen Herstellern integrieren zu können.

Was der Webdienst und der Daemon sind

Der SnapDrive für UNIX Webservice bietet eine einheitliche Schnittstelle für alle NetApp SnapManager und Produkte von Drittanbietern zur nahtlosen Integration mit SnapDrive für UNIX. Um die Befehle der Befehlszeilenschnittstelle (CLI) in SnapDrive für UNIX zu verwenden, müssen Sie den Daemon starten.

Verschiedene NetApp SnapManager Produkte verwenden die Befehlszeilenschnittstelle (CLI) zur Kommunikation mit SnapDrive für UNIX. Die Verwendung der CLI schränkt die Performance und Managebarkeit von SnapManager und SnapDrive für UNIX ein. Wenn Sie den SnapDrive for UNIX Daemon verwenden, arbeiten alle Befehle als eindeutigen Prozess. Der Daemon Service hat keine Auswirkungen auf die Verwendung von SnapDrive für UNIX Befehlen.

Der Webservice SnapDrive für UNIX ermöglicht die nahtlose Integration von Drittanbieterapplikationen mit SnapDrive für UNIX. Sie arbeiten mithilfe von APIs mit SnapDrive für UNIX zusammen.

Beim Starten des Daemon überprüft SnapDrive for UNIX Daemon zunächst, ob der Daemon ausgeführt wird. Wenn der Daemon nicht ausgeführt wird, startet er den Daemon. Wenn der Daemon bereits ausgeführt wird und Sie versuchen, ihn zu starten, zeigt SnapDrive für UNIX die Meldung an:

```
snapdrive daemon is already running
```

Sie können den Status des Daemon überprüfen, um zu ermitteln, ob SnapDrive für UNIX ausgeführt wird oder nicht. Sie sollten den Status überprüfen, bevor Sie sich entscheiden, den Daemon zu starten. Wenn ein anderer Benutzer als der Root-Benutzer versucht, den Status zu überprüfen, prüft SnapDrive für UNIX die Anmeldeinformationen des Benutzers und zeigt die Meldung an:

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

Wenn Sie versuchen, den Daemon zu stoppen, überprüft SnapDrive für UNIX Ihre Anmeldedaten. Wenn Sie ein anderer Benutzer als Root-Benutzer sind, zeigt SnapDrive für UNIX die Meldung an

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

Nachdem Sie den Daemon angehalten haben, müssen Sie den SnapDrive for UNIX Daemon neu starten, damit Änderungen an der Konfigurationsdatei oder an einem beliebigen Modul wirksam werden. Wenn ein anderer Benutzer als der Root-Benutzer versucht, den SnapDrive für UNIX Daemon neu zu starten, überprüft SnapDrive für UNIX die Anmeldeinformationen des Benutzers und zeigt die Meldung an

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

Überprüfen des Status des Daemon

Sie können den Status des Daemon überprüfen, um zu sehen, ob der Daemon ausgeführt wird. Wenn der Daemon bereits ausgeführt wird, müssen Sie ihn erst neu starten, wenn die Konfigurationsdatei SnapDrive für UNIX aktualisiert wurde.

Sie müssen als Root-Benutzer angemeldet sein.

Schritte

1. Überprüfen Sie den Status des Daemon:

```
snapdrived status
```

Starten des SnapDrive for UNIX Daemon

Sie müssen den SnapDrive for UNIX Daemon starten und ausführen, bevor Sie jeden SnapDrive for UNIX Befehl verwenden können.

Sie müssen als Root-Benutzer angemeldet sein.

Schritte

1. Starten Sie den Daemon:

```
snapdrived start
```

Ändern des Standard-Daemon-Passworts

SnapDrive für UNIX wird einem Standard-Daemon-Passwort zugewiesen, das Sie später ändern können. Dieses Passwort wird in einer verschlüsselten Datei gespeichert, deren Lese- und Schreibberechtigungen nur dem Root-Benutzer zugewiesen sind. Nach der Kennwortänderung müssen alle Client-Anwendungen manuell benachrichtigt werden.

Sie müssen als Root-Benutzer angemeldet sein.

Schritte

1. Ändern Sie das Standardpasswort:

```
snapdrived passwd
```

2. Geben Sie das Passwort ein.
3. Bestätigen Sie das Passwort.

Beenden des Daemon

Wenn Sie die Konfigurationsdatei SnapDrive für UNIX ändern, müssen Sie den Daemon anhalten und neu starten. Sie können den Dämon gewaltsam oder gewaltsam stoppen.

Den Dämon gewaltsam stoppen

Wenn Ihre SnapDrive für UNIX-Konfigurationsdatei geändert wird, müssen Sie den Daemon stoppen, damit die Änderungen der Konfigurationsdatei wirksam werden. Nachdem der Daemon angehalten und neu gestartet wurde, werden die Änderungen in der Konfigurationsdatei wirksam. Der Daemon kann nicht erzwungenbar angehalten werden, damit alle Befehle in der Warteschlange ausgeführt werden können. Nachdem die Stopp-Anforderung empfangen wurde, werden keine neuen Befehle ausgeführt.

Sie müssen als Root-Benutzer angemeldet sein.

1. Geben Sie den folgenden Befehl ein, um den Daemon nicht gewaltsam zu beenden:

```
snapdrived stop
```

Gewaltsam das Anhalten des Dämons

Sie können den Daemon gewaltsam anhalten, wenn Sie nicht darauf warten möchten, dass alle Befehle ausgeführt werden. Nachdem die Anforderung zum gewaltsamen Stoppen des Daemon empfangen wurde, storniert der SnapDrive for UNIX Daemon alle Befehle, die ausgeführt werden oder sich in der Warteschlange befinden. Wenn Sie den Dämon gewaltsam stoppen, ist der Zustand Ihres Systems möglicherweise undefiniert. Diese Methode wird nicht empfohlen.

Sie müssen als Root-Benutzer angemeldet sein.

Schritte

1. Beenden Sie den Dämon gewaltsam:

```
snapdrived -force stop
```

Starten Sie den Daemon neu

Sie müssen den Daemon neu starten, nachdem Sie ihn angehalten haben, damit Änderungen an der Konfigurationsdatei oder an den anderen Modulen wirksam werden. Der SnapDrive for UNIX Daemon wird erst neu gestartet, nachdem alle Befehle ausgeführt und in der Warteschlange ausgeführt wurden. Nachdem die Anforderung für einen Neustart empfangen wurde, werden keine neuen Befehle ausgeführt.

- Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.
- Stellen Sie sicher, dass keine anderen Sitzungen parallel auf demselben Host ausgeführt werden. Der `snapdrived restart` Befehl hängt das System in solchen Situationen an.

Schritte

1. Geben Sie den folgenden Befehl ein, um den Daemon neu zu starten:

```
snapdrived restart
```

Erzwingen des Neustarts des Daemon

Sie können den Daemon zwingen, neu zu starten. Ein kraftvoller Neustart des Dämons stoppt die Ausführung aller ausgeführten Befehle.

Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.

Schritte

1. Geben Sie den folgenden Befehl ein, um den Daemon gewaltsam neu zu starten:

```
snapdrived -force restart
```

Nachdem die Anforderung zum Neustart erzwingen empfangen wurde, werden alle Befehle in der Ausführung und in der Warteschlange angehalten. Der Daemon wird erst neu gestartet, nachdem die Ausführung aller ausgeführten Befehle abgebrochen wurde.

Sichere Daemon Kommunikation mit HTTPS

Sie können HTTPS für sichere Webdienste und Daemon-Kommunikation verwenden. Die sichere Kommunikation wird durch das Festlegen einiger Konfigurationsvariablen im aktiviert `snapdrive.conf` Erstellen und Installieren des selbstsignierten oder CA-signierten Zertifikats.

Sie müssen das selbstsignierte oder CA-signierte Zertifikat an dem Pfad angeben, der im angegeben ist `snapdrive.conf` Datei: Um HTTPS für die Kommunikation zu verwenden, müssen Sie die folgenden Parameter in festlegen `snapdrive.conf` Datei:

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



SnapDrive 5.0 für UNIX und neuere Versionen unterstützen HTTPS für die Kommunikation mit dem Daemon. Standardmäßig ist die Option auf festgelegt `off`.

Selbstsignierte Zertifikate werden generiert

Der SnapDrive für UNIX Daemon Service erfordert, dass Sie ein selbstsigniertes Zertifikat für die Authentifizierung erstellen. Diese Authentifizierung ist bei der Kommunikation mit der CLI erforderlich.

Schritte

1. Generieren eines RSA-Schlüssels:

```
$ 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. Erstellen Sie das Zertifikat:

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

Der `-new`, `-x509`, und `-nodes` Die Optionen werden verwendet, um ein unverschlüsseltes Zertifikat zu erstellen. Der `-days` Option gibt die Anzahl der Tage an, in denen das Zertifikat gültig bleibt.

3. Wenn Sie aufgefordert werden, die x509-Daten des Zertifikats auszufüllen, geben Sie Ihre lokalen Daten ein:

```
# 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
```



Der Common Name Wert muss *localhost* sein.

4. Metadaten extrahieren (optional).

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

Sie können die Zertifikatmetadaten für eine schnelle Referenz später speichern.

5. Kombinieren Sie Schlüssel- und Zertifikatdaten.

Für SnapDrive für UNIX müssen sich die Schlüssel- und Zertifikatdaten in derselben Datei befinden. Die kombinierte Datei muss als Schlüsseldatei geschützt werden.

```
$ 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. Fügen Sie dem den vollständigen Pfad des Daemon-Zertifikats hinzu *sdu-daemon-certificate-path* Variable des *snapdrive.conf* Datei:

Erstellen eines CA-signierten Zertifikats

Der SnapDrive für UNIX Daemon Service erfordert, dass Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für die erfolgreiche Daemon Kommunikation erstellen. Sie müssen das CA-signierte Zertifikat an dem Pfad angeben, der im angegeben ist *snapdrive.conf* Datei:

- Sie müssen als Root-Benutzer angemeldet sein.
- Sie müssen die folgenden Parameter in festgelegt haben *snapdrive.conf* Datei zur Verwendung von HTTPS für die Kommunikation:
 - Use-https-to-sdu-daemon=on
 - Contact-https-Port-sdu-Daemon=4095
 - sdu-Daemon-Certificate-Path=/opt/NetApp/snapdrive/snapdrive.pem

Schritte

1. Generieren eines neuen unverschlüsselten RSA-privaten Schlüssels im Pem-Format:

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

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

2. Konfigurieren */etc/ssl/openssl.cnf* So erstellen Sie den privaten CA-Schlüssel und das Zertifikat vi */etc/ssl/openssl.cnf*.
3. Erstellen Sie ein nicht signiertes Zertifikat mit Ihrem RSA-privaten Schlüssel:

```
$ 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. Verwenden Sie Ihren privaten Schlüssel und Ihr Zertifikat, um einen CSR zu erstellen:

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

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

5. Unterschreiben Sie das Zertifikat mit dem privaten CA-Schlüssel, indem Sie die CSR verwenden, die Sie gerade erstellt haben:

```
$ 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. Installieren Sie das signierte Zertifikat und den privaten Schlüssel, der von einem SSL-Server verwendet werden soll.

```

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)

```

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.