瞭SnapDrive 解適用於UNIX精靈的功能

Snapdrive for Unix

NetApp
October 04, 2023

目錄

瞭SnapDrive 解適用於UNIX精靈的功能 1
Web服務和精靈的意義 1
檢查精靈的狀態 1
啟動SnapDrive UNIX精靈的功能 2
變更預設的精靈密碼 2
停止精靈 2
重新啟動精靈 3
強制重新啟動精靈 3
使用HTTPS進行安全監控通訊 4
產生自我簽署的憑證 4
產生CA簽署的憑證 5

瞭SnapDrive 解適用於UNIX精靈的功能

在執行SnapDrive 任何適用於UNIX的功能之前、您必須先瞭解Web服務和精靈、以及如何使用它們。所有SnapDrive 的UNIX指令都能使用精靈服務來運作。在SnapDrive AIX主機上使用適用於UNIX的功能之前、您必須先啟動此精靈、使SnapDrive UNIX版的支援功能能與其他NetApp和非NetApp產品無縫且安全地整合。

Web服務和精靈的意義

適用於UNIX的支援服務提供統一介面、可讓所有NetApp產品和第三方產品無縫整合適用於UNIX的支援功能。SnapDrive SnapManager SnapDrive若要在SnapDrive 適用於UNIX的方面使用命令列介面（CLI）命令、您需要啟動精靈。

各種NetApp SnapManager 產品使用命令列介面（CLI）與SnapDrive 適用於UNIX的解決方案進行通訊。使用CLI會限制SnapManager UNIX版的效能和可管理性。SnapDrive當您使用SnapDrive for UNIX精靈時、所有命令都會以獨特的程序運作。監控程式服務不會影響SnapDrive 使用UNIX指令的方式。

適用於UNIX的支援服務可讓第三方應用程式與適用於UNIX的支援無縫整合。SnapDrive SnapDrive他們使用SnapDrive API與UNIX版的for UNIX互動。

當您啟動精靈時、SnapDrive for UNIX精靈會先檢查精靈是否正在執行。如果精靈未執行、則會啟動精靈。如果精靈已經在執行中、而您嘗試啟動它、SnapDrive 則適用於UNIX的畫面會顯示訊息：

《不只是執行的程式》SnapDrive

您可以檢查監控程式的狀態、查看SnapDrive 是否正在執行UNIX的功能。在決定啟動精靈之前、您應該先檢查狀態。如果root使用者以外的使用者嘗試檢查狀態、SnapDrive 則UNIX版的for UNIX會檢查使用者的認證資料、並顯示訊息：

「SnapDrive 只有root使用者才能看到此功能的狀態」

當您嘗試停止精靈時、SnapDrive 適用於UNIX的功能會檢查您的認證資料。如果您是root使用者以外的使用者、SnapDrive 則會顯示訊息「適用於UNIX」

只有root使用者才能停止執行此功能SnapDrive

停止精靈之後、您必須重新啟動SnapDrive UNIX的funcfor daemon.、才能使組態檔或任何模組的任何變更生效。如果root使用者以外的使用者嘗試重新啟動SnapDrive UNIX版的程式、SnapDrive 則適用於UNIX的顯示器會檢查使用者的認證資料、並顯示訊息

只有root使用者才能重新啟動此程式SnapDrive

檢查精靈的狀態

您可以檢查精靈的狀態、查看精靈是否正在執行。如果精靈已經在執行中、您不需要重新啟動它、直到SnapDrive 更新完for UNIX組態檔為止。

您必須以root使用者的身分登入。

步驟

1. 檢查精靈的狀態：

   快照狀態*

啟動SnapDrive UNIX精靈的功能

您必須先啟動並執行SnapDrive for UNIX精靈、才能使用SnapDrive 任何適用於UNIX的指令。

您必須以root使用者的身分登入。

步驟

1. 啟動精靈：

   快照的start*

變更預設的精靈密碼

UNIX版的預設精靈密碼已指派給您、您可以稍後再變更。SnapDrive此密碼儲存在加密檔案中、並只指派給root使用者讀取和寫入權限。變更密碼之後、必須手動通知所有用戶端應用程式。

您必須以root使用者的身分登入。

步驟

1. 變更預設密碼：

   快照的passwd*

2. 輸入密碼。
3. 確認密碼。

停止精靈

如果您變更SnapDrive UNIX版的功能檔、則必須停止並重新啟動精靈。您可以不強制或強制地停止精靈。

不強制停止精靈

如果SnapDrive 您的UNIX版組態檔已變更、您必須停止精靈、才能使組態檔變更生效。在精靈停止並重新啟動之後、組態檔中的變更會生效。非強制停止精靈會允許所有佇列的命令完成執行。收到停止要求後、不會執行任何新命令。

您必須以root使用者的身分登入。

1. 輸入下列命令以不強制停止精靈：

   快照停止*

強制停止精靈

當您不想等待所有命令完成執行時、可以強制停止精靈。收到強制停止精靈的要求後、SnapDrive for UNIX精靈會取消執行中或佇列中的任何命令。當您強制停止精靈時、系統狀態可能未定義。不建議使用此方法。

您必須以root使用者的身分登入。

步驟

1. 強制停止精靈：

   快照的-force stop（停止）*

重新啟動精靈

您必須在停止後重新啟動精靈、如此您對組態檔或其他模組所做的變更才會生效。僅在完成執行中和佇列中的所有命令後、才能重新啟動for UNIX精靈。SnapDrive收到重新啟動要求後、不會執行任何新命令。

- 請確定您以root使用者身分登入。
- 確保同一主機上沒有其他工作階段同時執行。在這種情況下、「磁碟重新啟動」命令會使系統當機。

步驟

1. 輸入下列命令以重新啟動精靈：

   快照重新啟動*

強制重新啟動精靈

您可以強制精靈重新啟動。強制重新啟動精靈會停止執行所有執行中的命令。

請確定您以root使用者身分登入。

步驟

1. 輸入下列命令以強制重新啟動精靈：

   快照-強制重新啟動*

   收到強制重新啟動要求之後、精靈會停止執行中和佇列中的所有命令。只有在取消執行所有執行中的命令之後、精靈才會重新啟動。

使用HTTPS進行安全監控通訊

您可以使用HTTPS進行安全的Web服務和監控程式通訊。安全通訊是透過在「snapdrive.conf」檔案中設定一些組態變數、以及產生和安裝自我簽署或CA簽署的憑證來啟用的。

您必須在「snapdrive.conf」檔案中指定的路徑提供自我簽署或CA簽署的憑證。若要使用HTTPS進行通訊、您必須在「snapdrive.conf」檔案中設定下列參數：

- 「use-https-to -SDU-daemon=on」
- 「contact-https-port-sdU-daemon=4095」
- 「du-daem-Certificate path=/opt/NetApp/SnapDrive / SnapDrive。pem」

適用於UNIX及更新版本的支援HTTPS以進行精靈通訊。SnapDrive依預設、此選項設為「關」。

產生自我簽署的憑證

for UNIX精靈服務需要您產生自我簽署的憑證來進行驗證。SnapDrive與CLI進行通訊時、必須進行此驗證。

步驟

1. 產生RSA金鑰：

   「$openssl genrsa 1024 > host.key $ chmod400 host.key*」

   ```
   # openssl genrsa 1024 > host.key Generating
   RSA private key, 1024 bit long modulus
   ..............................++++++ ...++++++ e is 65537(0x10001)
   # chmod 400 host.key
   ```

2. 建立憑證：

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

   「-new」、「-x509」及「-nodes」選項可用來建立未加密的憑證。"-days（天數）"選項指定證書保持有效的天數。

3. 當系統要求您填寫憑證的x509資料時、請輸入您的本機資料：

```
# 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
```

「Common Name（一般名稱）」值必須是_localhost_。

4. 擷取中繼資料（選用）。

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

您可以儲存憑證中繼資料、以便稍後快速參考。

5. 結合金鑰與憑證資料。

UNIX版要求金鑰和憑證資料必須位於同一個檔案中。SnapDrive組合檔案必須以金鑰檔案的形式加以保護。

「**$ CAT host.cert host.key > host.pem **」

"&&rm host.key*

「$chmod400 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. 將精靈憑證的完整路徑新增至「snapdrive.conf」檔案的「*SDU-daeme-Certificate path*」變數。

產生CA簽署的憑證

for UNIX精靈服務需要您產生CA簽署的憑證、才能成功進行精靈通訊。SnapDrive您必須

在「snapdrive.conf」檔案中指定的路徑提供CA簽署的憑證。

- 您必須以root使用者的身分登入。
- 您必須在「snapdrive.conf」檔案中設定下列參數、才能使用HTTPS進行通訊：
  - use-https-to -SDU-daemon=on
  - contact-https-port-sdU-daemon=4095
  - SDU-daeme-Certificate路徑=（或）/opt/NetApp/SnapDrive / SnapDrive（磁碟機）.pem

步驟

1. 以pem格式產生新的未加密RSA私密金鑰：

   「$openssl genrsa -out privkey.pem 10410*」

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

2. 設定「/etc/ssl/openssl.cnf」以建立CA私密金鑰和憑證VI（如/etc/ssl/openssl.cnf）。
3. 使用您的RSA私密金鑰建立未簽署的憑證：

   「$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. 使用您的私密金鑰和憑證來建立CSR：

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

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

5. 使用您剛建立的CSR、以CA私密金鑰簽署憑證：

「$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. 安裝SSL伺服器所使用的簽署憑證和私密金鑰。

```
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)
```