UNIX용 SnapDrive의 보안 기능

Snapdrive for Unix

NetApp
October 04, 2023

목차

UNIX용 SnapDrive의 보안 기능

UNIX용 SnapDrive를 사용하기 전에 해당 보안 기능을 이해하고 이러한 기능에 액세스하는 방법을 익혀야 합니다.

보안 기능

SnapDrive for UNIX는 보다 안전하게 작업할 수 있는 특정 기능을 제공합니다. 이러한 기능을 통해 스토리지 시스템 및 호스트에서 작업을 수행할 수 있는 사용자를 보다 효과적으로 제어할 수 있습니다.

보안 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- 액세스 제어 권한을 설정합니다
- 스토리지 시스템의 로그인 정보를 지정합니다
- UNIX용 SnapDrive에서 HTTPS를 사용하도록 지정합니다

액세스 제어 기능을 사용하면 SnapDrive for UNIX를 실행하는 호스트가 스토리지 시스템에서 수행할 수 있는 작업을 지정할 수 있습니다. 각 호스트에 대해 이러한 권한을 개별적으로 설정합니다. 또한 UNIX용 SnapDrive가 스토리지 시스템에 액세스할 수 있도록 하려면 해당 스토리지 시스템의 로그인 이름과 암호를 제공해야 합니다.

HTTPS 기능을 사용하면 암호 전송을 포함하여 Manage ONTAP 인터페이스를 통해 스토리지 시스템과의 모든 상호 작용에 대해 SSL 암호화를 지정할 수 있습니다. 이 동작은 UNIX용 SnapDrive 4.1 이후 버전 AIX 호스트의 경우 기본값이지만, 'Use-https-to-filer' 구성 변수의 값을 'off'로 변경하여 SSL 암호화를 해제할 수 있습니다.

UNIX용 SnapDrive의 액세스 제어

SnapDrive for UNIX를 사용하면 호스트가 접속된 각 스토리지 시스템에 대한 각 호스트의 액세스 레벨을 제어할 수 있습니다.

UNIX용 SnapDrive의 액세스 수준은 호스트가 특정 스토리지 시스템을 대상으로 수행할 때 수행할 수 있는 작업을 나타냅니다. 표시 및 목록 작업을 제외하고 액세스 제어 권한은 모든 스냅샷 및 스토리지 작업에 영향을 줄 수 있습니다.

액세스 제어 설정은 무엇입니까

사용자 액세스를 확인하기 위해 SnapDrive for UNIX는 스토리지 시스템의 루트 볼륨에 있는 두 개의 사용 권한 파일 중 하나를 확인합니다. 액세스 제어를 평가하려면 해당 파일에 설정된 규칙을 확인해야 합니다.

- 'DHOST-NAME.prbac' 파일은 디렉토리 '/vol/vol0/sdprbac'(SnapDrive 사용 권한 역할 기반 액세스 제어)에 있습니다.

  파일 이름은 DHOST-NAME.prbac입니다. 여기서, '*host-name*'은 사용 권한이 적용되는 호스트의 이름입니다. 스토리지 시스템에 접속된 각 호스트에 대한 사용 권한 파일이 있을 수 있습니다. "SnapDrive config access" 명령을 사용하여 특정 스토리지 시스템에서 호스트에 사용할 수 있는 권한에 대한 정보를 표시할 수 있습니다.

  DHOST-NAME.prbac이 존재하지 않는 경우, 'dsgeneric.prbac' 파일을 사용하여 액세스 권한을 확인한다.

- 'sdgeneric.prbac' 파일도 '/vol/vol0/sdprbac' 디렉토리에 있습니다.

  파일 이름 'dsgeneric.prbac'은 스토리지 시스템의 DHOST-NAME.prbac 파일에 액세스할 수 없는 여러 호스트에 대한 기본 액세스 설정으로 사용됩니다.

/vol/vol0/sdprbac 경로에서 사용할 수 있는 DHOST-NAME.prbac 및 sdgeneric.prbac 파일이 모두 있는 경우, 'dsgeneric.prbac' 파일에 제공된 값을 덮어쓰므로 'DHOST-NAME.prbac'을 사용하여 액세스 권한을 확인합니다.

DHOST-NAME.prbac과 Sdgeneric.prbac 파일이 모두 없는 경우, 'sapdrive.conf' 파일에 정의된 설정 변수 "*all-access-if-RBAC-unspecified*"를 확인하십시오.

지정된 호스트에서 지정된 vFiler 장치로 액세스 제어를 설정하는 것은 수동 작업입니다. 해당 호스트의 액세스는 영향을 받는 vFiler 유닛의 루트 볼륨에 있는 파일에 의해 제어됩니다. 이 파일에는 '/vol/<vFiler root volume>/sdprbac/sdhost-name.prbac'이 포함되어 있습니다. 여기서 '*host-name*'은 gethostname(3)이 반환한 영향을 받는 호스트의 이름입니다. 이 파일을 액세스할 수 있는 호스트에서 이 파일을 읽을 수 있지만 쓸 수 없도록 해야 합니다.

> 호스트 이름을 확인하려면 호스트 이름 명령을 실행합니다.

파일이 비어 있거나 읽을 수 없거나 형식이 잘못된 경우 UNIX용 SnapDrive는 호스트 액세스 권한을 해당 작업에 부여하지 않습니다.

파일이 없으면 SnapDrive for UNIX는 'sapdrive.conf' 파일에서 구성 변수 '*all-access-if-RBAC-unspecified*'를 확인합니다. 이 변수가 "On"(기본값)으로 설정되어 있으면 호스트가 해당 스토리지 시스템에서 이러한 모든 작업을 완벽하게 액세스할 수 있습니다. 변수가 "off"로 설정되어 있으면 SnapDrive for UNIX는 해당 스토리지 시스템에서 액세스 제어가 적용되는 작업을 수행할 수 있는 호스트 권한을 거부합니다.

사용 가능한 액세스 제어 수준

SnapDrive for UNIX는 사용자에게 다양한 액세스 제어 수준을 제공합니다. 이러한 액세스 수준은 스냅샷 복사본 및 스토리지 시스템 작업과 관련이 있습니다.

다음과 같은 액세스 수준을 설정할 수 있습니다.

- 없음 — 호스트에 스토리지 시스템에 대한 액세스 권한이 없습니다.
- 스냅 생성 — 호스트에서 스냅샷 복사본을 생성할 수 있습니다.
- 스냅 사용 — 호스트에서 스냅샷 복사본을 삭제하고 이름을 바꿀 수 있습니다.
- 모두 스냅 — 호스트에서 스냅샷 복사본을 생성, 복구, 삭제 및 이름 변경할 수 있습니다.
- 스토리지 생성 삭제 — 호스트는 스토리지를 생성, 크기 조정 및 삭제할 수 있습니다.
- 스토리지 사용 — 호스트는 스토리지를 연결 및 연결 해제할 수 있으며 스토리지에서 클론 분할 추정치 및 클론 분할 시작을 수행할 수도 있습니다.
- 스토리지 모두 — 호스트는 스토리지를 생성, 삭제, 연결 및 연결 해제할 수 있으며 스토리지에서 클론 분할 추정치 및 클론 분할 시작을 수행할 수도 있습니다.
- 모든 액세스 — 호스트는 UNIX용 이전의 모든 SnapDrive 작업에 액세스할 수 있습니다.

각 수준은 다릅니다. 특정 작업에 대해서만 권한을 지정하는 경우 UNIX용 SnapDrive는 이러한 작업만 실행할 수 있습니다. 예를 들어, 스토리지 사용을 지정하는 경우 호스트는 SnapDrive for UNIX를 사용하여 스토리지를 연결 및

연결 해제할 수 있지만 액세스 제어 권한에 따라 관리되는 다른 작업은 수행할 수 없습니다.

액세스 제어 권한을 설정합니다

스토리지 시스템의 루트 볼륨에 특수 디렉토리와 파일을 생성하여 SnapDrive for UNIX에서 액세스 제어 권한을 설정할 수 있습니다.

루트 사용자로 로그인했는지 확인합니다.

단계

1. 대상 스토리지 시스템의 루트 볼륨에 'dsprbac' 디렉토리를 생성합니다.

   루트 볼륨을 액세스 가능하게 만드는 한 가지 방법은 NFS를 사용하여 볼륨을 마운트하는 것입니다.

2. 'dsprbac' 디렉토리에 권한 파일을 작성합니다. 다음 내용이 참인지 확인하십시오.
   - 파일 이름은 DHOST-NAME.prbac이어야 합니다. 여기서 host-name은 액세스 권한을 지정하는 호스트의 이름입니다.
   - UNIX용 SnapDrive에서 읽을 수는 있지만 수정할 수는 없도록 파일을 읽기 전용으로 설정해야 합니다.

     dev-sun1 액세스 권한을 호스트에게 부여하려면 스토리지 시스템에 '/vol/vol1/sdprbac/sddev-sun1.prbac' 파일을 생성합니다

3. 해당 호스트에 대한 파일의 권한을 설정합니다.

   파일에 다음 형식을 사용해야 합니다.

   - 하나의 권한 수준만 지정할 수 있습니다. 호스트에 모든 작업에 대한 전체 액세스 권한을 부여하려면 ALL ACCESS 문자열을 입력합니다.
   - 권한 문자열은 파일에서 첫 번째 문자열이어야 합니다. 권한 문자열이 첫 번째 줄에 없으면 파일 형식이 유효하지 않습니다.
   - 권한 문자열은 대/소문자를 구분하지 않습니다.
   - 사용 권한 문자열 앞에 공백이 없어야 합니다.
   - 설명은 허용되지 않습니다.

     이러한 유효한 권한 문자열은 다음과 같은 액세스 수준을 허용합니다.

   - 없음 — 호스트에 스토리지 시스템에 대한 액세스 권한이 없습니다.
   - 스냅 생성 — 호스트에서 스냅샷 복사본을 생성할 수 있습니다.
   - 스냅 사용 — 호스트에서 스냅샷 복사본을 삭제하고 이름을 바꿀 수 있습니다.
   - 모두 스냅 — 호스트에서 스냅샷 복사본을 생성, 복구, 삭제 및 이름 변경할 수 있습니다.
   - 스토리지 생성 삭제 — 호스트는 스토리지를 생성, 크기 조정 및 삭제할 수 있습니다.
   - 스토리지 사용 — 호스트는 스토리지를 연결 및 연결 해제할 수 있으며 스토리지에서 클론 분할 추정치 및 클론 분할 시작을 수행할 수도 있습니다.
   - 스토리지 모두 — 호스트는 스토리지를 생성, 삭제, 연결 및 연결 해제할 수 있으며 스토리지에서 클론 분할 추정치 및 클론 분할 시작을 수행할 수도 있습니다.

- 모든 액세스 — 호스트는 UNIX용 이전의 모든 SnapDrive 작업에 액세스할 수 있습니다. 이러한 각 사용 권한 문자열은 서로 다릅니다. 스냅 사용을 지정하는 경우 호스트는 스냅샷 복사본을 삭제하거나 이름을 바꿀 수 있지만 스냅샷 복사본을 생성하거나 스토리지 프로비저닝 작업을 수행하거나 복구할 수는 없습니다.

설정한 권한에 관계없이 호스트는 표시 및 목록 작업을 수행할 수 있습니다.

4. 다음 명령을 입력하여 액세스 권한을 확인합니다.

   '* SnapDrive config access show_filer_name_*'

액세스 제어 권한 보기

SnapDrive config access show 명령을 실행하여 액세스 제어 권한을 볼 수 있습니다.

단계

1. 'SnapDrive config access show' 명령어를 실행한다.

   이 명령의 형식은 'SnapDrive config access{show|list}filename'입니다

   명령의 'show' 또는 'list' 버전을 입력하든 상관없이 동일한 파라미터를 사용할 수 있습니다.

   이 명령줄은 스토리지 시스템 토스터를 검사하여 호스트에 있는 권한을 확인합니다. 출력에 따라 이 스토리지 시스템의 호스트에 대한 사용 권한은 모두 스냅됩니다.

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

   이 예에서는 사용 권한 파일이 스토리지 시스템에 없기 때문에 SnapDrive for UNIX는 'sapdrive.conf' 파일에서 변수 '*all-access-if-RBAC-unspecified*'를 확인하여 호스트에 있는 사용 권한을 결정합니다. 이 변수는 모든 액세스 수준으로 설정된 권한 파일을 생성하는 것과 동일한 설정 으로 설정됩니다.

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

이 예에서는 스토리지 시스템 토스터에 사용 권한 파일이 없는 경우 수신하는 메시지 종류와 'sapdrive.conf' 파일의 변수 '*all-access-if-RBAC-unspecified*'가 'off'로 설정되어 있음을 보여 줍니다.

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

스토리지 시스템의 로그인 정보

사용자 이름 또는 암호를 사용하면 UNIX용 SnapDrive에서 각 스토리지 시스템을 액세스할 수 있습니다. 또한 루트로 로그인하는 것 외에도 SnapDrive for UNIX를 실행하는 사람이 메시지가 표시될 때 올바른 사용자 이름 또는 암호를 제공해야 하기 때문에 보안이 제공됩니다. 로그인이 손상된 경우 이를 삭제하고 새 사용자 로그인을 설정할 수 있습니다.

설정할 때 각 스토리지 시스템에 대한 사용자 로그인을 생성했습니다. UNIX용 SnapDrive가 스토리지 시스템과 함께 작동하려면 이 로그인 정보를 제공해야 합니다. 스토리지 시스템을 설정할 때 지정한 내용에 따라 각 스토리지 시스템에서 동일한 로그인 또는 고유 로그인을 사용할 수 있습니다.

UNIX용 SnapDrive는 이러한 로그인 및 암호를 각 호스트에 암호화된 형식으로 저장합니다. SnapDrive for UNIX는 스토리지 시스템과 통신할 때 '*SnapDrive.conf*' 구성 변수 '*use-https-to-filer=on*'을 설정하여 이 정보를 암호화하도록 지정할 수 있습니다.

로그인 정보 지정

스토리지 시스템의 사용자 로그인 정보를 지정해야 합니다. 스토리지 시스템을 설정할 때 지정한 내용에 따라 각 스토리지 시스템은 동일한 사용자 이름이나 암호 또는 고유한 사용자 이름이나 암호를 사용할 수 있습니다. 모든 스토리지 시스템에서 동일한 사용자 이름 또는 암호 정보를 사용하는 경우 다음 단계를 한 번 수행해야 합니다. 스토리지 시스템에서 고유한 사용자 이름 또는 암호를 사용하는 경우 각 스토리지 시스템에 대해 다음 단계를 반복해야 합니다.

루트 사용자로 로그인했는지 확인합니다.

단계

1. 다음 명령을 입력합니다.

   '* SnapDrive config set_user_name filename_[*filename…*] * '

   '*user_name*'은(는) 처음 설정할 때 해당 스토리지 시스템에 대해 지정된 사용자 이름입니다.

   '*filename*'은(는) 스토리지 시스템의 이름입니다.

   '*[filename…]*'은(는) 모두 동일한 사용자 로그인 또는 암호를 가지고 있는 경우 한 명령줄에 여러 스토리지 시스템 이름을 입력할 수 있음을 정의합니다. 하나 이상의 스토리지 시스템의 이름을 입력해야 합니다.

2. 암호가 있는 경우 프롬프트에 암호를 입력합니다.

   > 암호를 설정하지 않은 경우 암호를 묻는 메시지가 나타나면 Enter 키(null 값)를 누릅니다.

   다음 예에서는 토스터라는 스토리지 시스템에 대해 '루트'라는 사용자를 설정합니다.

   ```
   # snapdrive config set `root` toaster
   Password for root:
   Retype Password:
   ```

   이 예에서는 세 개의 스토리지 시스템에 대해 "root"라는 사용자를 설정합니다.

   ```
   # snapdrive config set root toaster oven broiler
   Password for root:
   Retype Password:
   ```

3. 다른 사용자 이름 또는 암호를 사용하는 다른 스토리지 시스템이 있는 경우 이 단계를 반복합니다.

UNIX용 SnapDrive에 연결된 스토리지 시스템 사용자 이름을 확인하는 중입니다

"SnapDrive 구성 목록" 명령을 실행하여 SnapDrive for UNIX가 스토리지 시스템에 연결한 사용자 이름을 확인할 수 있습니다.

루트 사용자로 로그인해야 합니다.

단계

1. 다음 명령을 입력합니다.

   '* SnapDrive 구성 목록 * '

   이 명령은 SnapDrive for UNIX에서 사용자가 지정된 모든 시스템의 사용자 이름 또는 스토리지 시스템 쌍을 표시합니다. 스토리지 시스템의 암호는 표시되지 않습니다.

   이 예에서는 Rapunzel 및 중형 스토리지 시스템이라는 스토리지 시스템과 연결된 사용자를 표시합니다.

   ```
   # snapdrive config list
   user name           storage system name
   ----------------------------
   rumplestiltskins    rapunzel
   longuser            mediumstoragesystem
   ```

스토리지 시스템에 대한 사용자 로그인을 삭제하는 중입니다

"SnapDrive config delete" 명령을 실행하여 하나 이상의 스토리지 시스템에 대한 사용자 로그인을 삭제할 수 있습니다.

루트 사용자로 로그인했는지 확인합니다.

단계

1. 다음 명령을 입력합니다.

   (* SnapDrive config delete_appliance_name [appliance_name]_ *

   '*appliance_name*'은(는) 사용자 로그인 정보를 삭제할 스토리지 시스템의 이름입니다.

   UNIX용 SnapDrive는 지정한 스토리지 시스템의 사용자 이름 또는 암호 로그인 정보를 제거합니다.

   > UNIX용 SnapDrive가 스토리지 시스템을 액세스하도록 설정하려면 새 사용자 로그인을 지정해야 합니다.

HTTP 설정

호스트 플랫폼에 HTTP를 사용하도록 UNIX용 SnapDrive를 구성할 수 있습니다.

루트 사용자로 로그인했는지 확인합니다.

단계

1. 'napdrive.conf' 파일을 백업합니다.
2. 텍스트 편집기에서 'napdrive.conf' 파일을 엽니다.
3. '*use-https-to-filer*' 변수의 값을 'off'로 변경합니다.

'napdrive.conf' 파일을 수정할 때는 다음 단계를 수행하는 것이 좋습니다.

a. 수정할 행에 주석을 표시합니다.
b. 주석 처리된 줄을 복사합니다.
c. 파운드(#) 기호를 제거하여 복사한 텍스트의 주석을 제거합니다.
d. 값을 수정합니다.

4. 변경한 후 파일을 저장합니다.

   SnapDrive for UNIX는 시작할 때마다 이 파일을 자동으로 검사합니다. 변경 사항을 적용하려면 SnapDrive for UNIX 데몬을 다시 시작해야 합니다.