



한 **SVM**에서 다른 **SVM**으로 볼륨을 다시 호스팅 ONTAP 9

NetApp
February 12, 2026

목차

한 SVM에서 다른 SVM으로 볼륨을 다시 호스팅	1
SVM 간에 볼륨을 재호스팅할 준비가 필요합니다.....	1
SMB 볼륨을 재호스팅합니다	1
NFS 볼륨을 재호스팅합니다.....	3
SAN 볼륨을 재호스팅합니다.....	4
SnapMirror 관계에서 볼륨 재호스팅	6
ONTAP에서 볼륨 재호스트에서는 기능이 지원되지 않습니다.....	8

한 SVM에서 다른 SVM으로 볼륨을 다시 호스팅

SVM 간에 볼륨을 재호스팅할 준비가 필요합니다

볼륨 재호스트 작업을 통해 SnapMirror 복사본 없이 NAS 또는 SAN 볼륨을 한 SVM에서 다른 SVM으로 재할당할 수 있습니다. 정확한 재호스트 절차는 사용되는 클라이언트 액세스 프로토콜과 볼륨 유형에 따라 다릅니다. 볼륨 재호스팅은 데이터 액세스 및 볼륨 관리를 위한 운영 중단 작업입니다.

SVM 간에 볼륨을 재호스팅할 수 있으려면 먼저 다음 조건이 충족되어야 합니다.

- 볼륨이 온라인 상태여야 합니다
- 볼륨 프로토콜은 SAN 또는 NAS여야 합니다
 - NAS 프로토콜 볼륨의 경우 볼륨은 접합 경로의 일부가 아니어야 하며 마운트 해제해야 합니다
- 볼륨이 SnapMirror 관계에 있는 경우 관계를 삭제한 후 관계 정보만 해제하거나 볼륨 재호스트를 시작하기 전에 관계를 해제해야 합니다
 - 볼륨 재호스트 작업 후에 SnapMirror 관계를 다시 동기화할 수 있습니다
- SVM 하위 유형은 소스 및 대상 SVM에서 모두 같아야 합니다
 - 동일한 하위 유형의 SVM 간에만 볼륨을 재호스팅할 수 있습니다
- 볼륨은 FlexClone 또는 FlexClone 상위 볼륨일 수 없습니다
 - FlexClone은 상위 볼륨 또는 클론 볼륨을 재호스팅하기 전에 분할해야 합니다

SMB 볼륨을 재호스팅합니다

SMB 프로토콜을 사용하여 데이터를 제공하는 볼륨을 재호스팅할 수 있습니다. 재호스팅 작업 후 클라이언트가 계속 데이터에 액세스할 수 있도록 하려면 정책 및 관련 규칙을 수동으로 구성해야 합니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- 소스 SVM 및 대상 SVM Active Directory 도메인이 서로 다르면 볼륨의 개체에 액세스하지 못할 수 있습니다.
- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

ONTAP 9.8 이상을 사용하는 경우 재호스트 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 소스 SVM에 로컬 사용자 및 그룹이 있을 경우 설정된 파일 및 디렉토리(ACL)에 대한 사용 권한은 볼륨 재호스트 작업 후에 더 이상 유효하지 않습니다.

감사 ACL(SACL)에도 마찬가지입니다.

- 재호스팅 작업 후에는 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
 - 볼륨 및 qtree 익스포트 정책
 - 안티바이러스 정책
 - 볼륨 효율성 정책
 - QoS(서비스 품질) 정책
 - 스냅샷 정책
 - 할당량 규칙
 - NS-SWITCH 및 NAME SERVICES 구성 익스포트 정책 및 규칙
 - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동 같은 볼륨 관리 작업이 실행되고 있지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.
- 소스 SVM 및 타겟 SVM에는 동일한 Active Directory 및 realmDNS 도메인이 있어야 합니다.
- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.



로컬 사용자 및 그룹이 구성되어 있고 해당 사용자 또는 그룹에 대해 설정된 권한이 있는 해당 볼륨에 파일 및 디렉토리가 있는 경우 이러한 권한은 더 이상 유효하지 않습니다.

단계

1. 볼륨 재호스트 작업이 실패할 경우 CIFS 공유에 대한 정보가 손실되지 않도록 CIFS 공유에 대한 정보를 기록합니다.
2. 상위 볼륨에서 볼륨을 마운트 해제합니다.

'볼륨 마운트 해제'

3. 고급 권한 레벨로 전환합니다.

세트 프리빌리지 고급

4. 대상 SVM에서 볼륨 재호스팅:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm
```

5. 대상 SVM의 적절한 접합 경로 아래에 볼륨을 마운트합니다.

'볼륨 마운트'입니다

6. 재호스트된 볼륨에 대한 CIFS 공유 생성:

'vserver cifs share create

7. 소스 SVM과 타겟 SVM 간에 DNS 도메인이 서로 다른 경우 새로운 사용자와 그룹을 생성합니다.
8. 새로 대상 SVM LIF와 재호스팅 볼륨의 접합 경로로 CIFS 클라이언트를 업데이트합니다.

작업을 마친 후

재호스트된 볼륨에서 정책 및 관련 규칙을 수동으로 재구성해야 합니다.

"SMB 구성"

"SMB 및 NFS 멀티 프로토콜 구성"

NFS 볼륨을 재호스팅합니다

NFS 프로토콜을 사용하여 데이터를 제공하는 볼륨을 재호스팅할 수 있습니다. 재호스팅 작업 후에도 클라이언트가 계속 데이터에 액세스할 수 있도록 하려면 볼륨을 SVM의 익스포트 정책과 연결하고 정책 및 관련 규칙을 수동으로 구성해야 합니다.

이 작업에 대해

- 재호스팅은 종단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

ONTAP 9.8 이상을 사용하는 경우 재호스트 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 재호스팅 작업 후에는 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
 - 볼륨 및 qtree 익스포트 정책
 - 안티바이러스 정책
 - 볼륨 효율성 정책
 - QoS(서비스 품질) 정책
 - 스냅샷 정책
 - 할당량 규칙
 - NS-SWITCH 및 NAME SERVICES 구성 익스포트 정책 및 규칙
 - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.

- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.

단계

1. 볼륨 재호스트 작업이 실패할 경우 NFS 정책에 대한 정보가 손실되지 않도록 NFS 익스포트 정책에 대한 정보를 기록합니다.

2. 상위 볼륨에서 볼륨을 마운트 해제합니다.

'볼륨 마운트 해제'

3. 고급 권한 레벨로 전환합니다.

세트 프리빌리지 고급

4. 대상 SVM에서 볼륨 재호스팅:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

대상 SVM의 기본 익스포트 정책이 재호스팅 볼륨에 적용됩니다.

5. 익스포트 정책 생성:

'vserver export-policy create'

6. 재호스트된 볼륨의 내보내기 정책을 사용자 정의 익스포트 정책으로 업데이트합니다.

볼륨 수정

7. 대상 SVM의 적절한 접합 경로 아래에 볼륨을 마운트합니다.

'볼륨 마운트'입니다

8. NFS 서비스가 대상 SVM에서 실행되고 있는지 확인합니다.

9. 재호스트된 볼륨에 대한 NFS 액세스를 재개합니다.

10. 대상 SVM LIF를 반영하도록 NFS 클라이언트 자격 증명 및 LIF 구성을 업데이트합니다.

볼륨 액세스 경로(LIF 및 접합 경로)가 변경되었기 때문입니다.

작업을 마친 후

재호스트된 볼륨에서 정책 및 관련 규칙을 수동으로 재구성해야 합니다. 자세한 내용은 ["NFS 구성"](#) 참조하십시오.

SAN 볼륨을 재호스팅합니다

매핑된 LUN을 통해 데이터를 제공하는 SAN 볼륨을 재호스팅할 수 있습니다. 대상 SVM에서 이니시에이터 그룹(igroup)을 다시 생성한 후 볼륨 재호스트 작업에서 동일한 SVM에서 볼륨을 자동으로 재매핑할 수 있습니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

ONTAP 9.8 이상을 사용하는 경우 재호스팅 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 재호스팅 작업 후 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스팅된 볼륨에서 수동으로 재구성해야 합니다.
 - 안티바이러스 정책
 - 볼륨 효율성 정책
 - QoS(서비스 품질) 정책
 - 스냅샷 정책
 - NS-SWITCH 및 NAME SERVICES 구성 익스포트 정책 및 규칙
 - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 볼륨 또는 LUN에 활성 I/O가 없어야 합니다.
- 대상 SVM에 동일한 이름의 igroup이 없지만 다른 이니시에이터가 있는지 확인해야 합니다.

igroup의 이름이 동일한 경우 SVM(소스 또는 타겟) 중 하나에서 igroup의 이름을 변경해야 합니다.

- 'force-unmap-LUNs' 옵션을 설정해야 합니다.
 - 'force-unmap-LUNs' 옵션의 기본값은 'false'입니다.
 - "force-unmap-LUNs" 옵션을 "true"로 설정하면 경고 또는 확인 메시지가 표시되지 않습니다.

단계

1. 타겟 볼륨에 LUN 매핑 정보 기록:

```
lun mapping show volume volume vserver source_svm
```

이 단계는 볼륨 재호스팅에 장애가 발생할 경우 LUN 매핑에 대한 정보가 손실되지 않도록 하는 사전 예방 단계입니다.

에 대한 자세한 내용은 `lun mapping show volume` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 타겟 볼륨과 연결된 igroup을 삭제합니다.
3. 타겟 볼륨을 대상 SVM으로 다시 호스팅:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

4. 타겟 볼륨의 LUN을 적절한 igroup에 매핑:

- 볼륨 재호스트는 타겟 볼륨에서 LUN을 보존하지만 LUN은 매핑 해제된 상태로 유지됩니다.
- LUN을 매핑할 때 대상 SVM 포트 세트를 사용합니다.
- 자동 재매핑-LUN 옵션이 true로 설정되어 있으면 재호스팅 후 LUN이 자동으로 매핑됩니다.

SnapMirror 관계에서 볼륨 재호스팅

SnapMirror 관계의 일부로 정의된 볼륨을 재호스팅할 수 있습니다. 관계를 다시 호스팅하기 전에 고려해야 할 몇 가지 문제가 있습니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- 재호스팅 작업 후 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
 - 볼륨 및 qtree 익스포트 정책
 - 안티바이러스 정책
 - 볼륨 효율성 정책
 - QoS(서비스 품질) 정책
 - 스냅샷 정책
 - 할당량 규칙
 - NS-SWITCH 및 NAME SERVICES 구성 익스포트 정책 및 규칙
 - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.
- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.

단계

1. SnapMirror 관계 유형을 기록합니다.

스냅미러 쇼

이 단계는 볼륨 재호스트에 장애가 발생할 경우 SnapMirror 관계 유형에 대한 정보가 손실되지 않도록 하는 사전 예방 단계입니다.

2. 대상 클러스터에서 SnapMirror 관계를 삭제합니다.

스냅미러 삭제

SnapMirror 관계를 해제하지 마십시오. 그렇지 않으면 타겟 볼륨의 데이터 보호 기능이 손실되고 재호스팅 작업 후에는 관계를 다시 설정할 수 없습니다.

3. 소스 클러스터에서 SnapMirror 관계 정보를 제거합니다.

```
snapmirror release -relationship-info-only true
```

`-relationship-info-only` 스냅샷을 삭제하지 않고 소스 관계 정보를 제거하도록 매개 변수를 `true` 설정합니다.

4. 볼륨이 마운트된 경우 마운트 해제합니다.

```
volume unmount -vserver <source_svm> -volume <vol_name>
```

5. 고급 권한 레벨로 전환합니다.

세트 프리빌리지 고급

6. 대상 SVM에서 볼륨 재호스팅:

```
volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver <destination_svm>
```

7. SVM 피어링 관계가 없을 경우, 소스 SVM과 타겟 SVM 간에 SVM 피어 관계를 생성합니다.

```
'vserver peer create
```

8. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 생성합니다.

스냅미러 생성

DP 볼륨을 호스팅하는 SVM에서 'napmirror create' 명령을 실행해야 합니다. 재호스트된 볼륨은 SnapMirror 관계의 소스 또는 대상이 될 수 있습니다.

9. SnapMirror 관계를 다시 동기화합니다.

관련 정보

- ["설정"](#)
- ["SnapMirror를 참조하십시오"](#)
- ["볼륨 재호스팅"](#)
- ["볼륨 마운트 해제"](#)
- ["SVM 피어 생성"](#)

ONTAP에서 볼륨 재호스트에서는 기능이 지원되지 않습니다

볼륨 재호스트를 지원하지 않는 ONTAP 기능에는 몇 가지가 있습니다. 재호스트 작업을 시도하기 전에 이러한 기능을 숙지해야 합니다.

다음 기능은 볼륨 재호스트에서는 지원되지 않습니다.

- SVM DR
- MetroCluster 구성



다른 SVM에서 볼륨을 FlexClone 볼륨으로 클론 복제하는 것은 MetroCluster 구성에서도 지원되지 않습니다.

- SnapLock 볼륨
- NetApp 볼륨 암호화(NVE) 볼륨(ONTAP 9.8 이전 버전)

9.8 이전의 ONTAP 릴리스에서는 볼륨을 다시 호스팅하기 전에 볼륨의 암호화를 해제해야 합니다. 볼륨 암호화 키는 SVM 키에 따라 다릅니다. 볼륨이 다른 SVM으로 이동하고 소스 또는 타겟 SVM에서 멀티테넌트 키 구성이 활성화된 경우 볼륨 및 SVM 키가 일치하지 않습니다.

ONTAP 9.8부터 NVE로 볼륨을 재호스팅할 수 있습니다.

- FlexGroup 볼륨
- 클론 볼륨

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.