데이터 보호 및 재해 복구

System Manager Classic

NetApp
April 09, 2024

목차

데이터 보호 및 재해 복구

클러스터 및 **SVM** 피어링 구성

클러스터 및 **SVM** 피어링 개요

클러스터 관리자는 클러스터와 SVM 간에 인증된 피어 관계를 생성하여 클러스터가 서로 통신하도록 함으로써 서로 다른 클러스터의 볼륨 간에 데이터를 복제할 수 있습니다. ONTAP 9.7 및 이전 ONTAP 9 릴리즈에서 제공되는 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 절차를 수행할 수 있습니다.

다음과 같은 경우 ONTAP System Manager_classic_interface를 사용하여 클러스터 피어 관계 및 SVM 피어 관계를 생성합니다.

- ONTAP 9.7 이하 ONTAP 9 릴리즈를 실행 중인 클러스터를 사용하고 있습니다.
- 인증된 클러스터 피어링 관계를 원합니다.
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- ONTAP CLI(Command-Line Interface) 또는 자동화된 스크립팅 도구가 아니라 System Manager를 사용하려고 합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

ONTAP 9.3의 ONTAP System Manager는 클러스터 및 SVM 간에 피어 관계를 구성하는 방법을 단순화합니다. 클러스터 피어링 절차와 SVM 피어링 절차는 모든 ONTAP 9 버전에 사용할 수 있습니다. 해당 버전의 ONTAP에 적합한 절차를 사용해야 합니다.

에서 이러한 작업을 수행하려면…	자세한 내용은…
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	• "System Manager를 이용한 클러스터 관리"
ONTAP CLI(명령줄 인터페이스)	• "CLI를 통한 클러스터 및 SVM 피어링 개요" 명령줄 인터페이스를 사용하여 클러스터 피어링 관계와 SVM 피어링 관계를 설정합니다. • "네트워크 관리" 명령줄 인터페이스를 사용하여 서브넷, 인터클러스터 LIF, 라우트, 방화벽 정책 및 기타 네트워킹 구성 요소를 구성합니다

클러스터 피어링을 위한 사전 요구사항

ONTAP 9.7 이하와 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 클러스터 피어링을 설정하기 전에 연결, 포트, IP 주소, 서브넷, 방화벽, 클러스터 명명 요구사항이

충족됩니다.

연결 요구 사항

로컬 클러스터의 모든 인터클러스터 LIF는 원격 클러스터의 모든 인터클러스터 LIF와 통신할 수 있어야 합니다.

반드시 필요한 것은 아니지만 일반적으로 동일한 서브넷에 있는 인터클러스터 LIF에 사용되는 IP 주소를 구성하는 것이 더 간단합니다. IP 주소는 데이터 LIF와 동일한 서브넷 또는 다른 서브넷에 상주할 수 있습니다. 각 클러스터에 사용되는 서브넷은 다음 요구사항을 충족해야 합니다.

- 서브넷에는 노드당 하나의 인터클러스터 LIF에 할당할 수 있는 충분한 IP 주소가 있어야 합니다.

  예를 들어, 6노드 클러스터에서 인터클러스터 통신에 사용되는 서브넷에는 사용 가능한 IP 주소가 6개 있어야 합니다.

각 노드에는 인터클러스터 네트워크의 IP 주소를 사용하는 인터클러스터 LIF가 있어야 합니다.

인터클러스터 LIF는 IPv4 주소 또는 IPv6 주소를 가질 수 있습니다.

> ONTAP 9를 사용하면 두 프로토콜을 모두 인터클러스터 LIF에 동시에 표시할 수 있도록 선택적으로 허용함으로써 피어링 네트워크를 IPv4에서 IPv6로 마이그레이션할 수 있습니다. 이전 릴리즈에서는 전체 클러스터에 대한 모든 인터클러스터 관계가 IPv4 또는 IPv6였습니다. 이는 프로토콜 변경이 잠재적으로 운영 중단이 발생할 수 있음을 의미합니다.

포트 요구 사항

인터클러스터 통신에 전용 포트를 사용하거나 데이터 네트워크에서 사용하는 포트를 공유할 수 있습니다. 포트는 다음 요구 사항을 충족해야 합니다.

- 지정된 원격 클러스터와 통신하는 데 사용되는 모든 포트는 동일한 IPspace에 있어야 합니다.

  여러 클러스터를 사용하여 다른 IPspace를 사용할 수 있습니다. IPspace 내에서만 쌍방향 전체 메시 연결이 필요합니다.

- 인터클러스터 통신에 사용되는 브로드캐스트 도메인에는 한 포트에서 다른 포트로 인터클러스터 통신이 페일오버할 수 있도록 노드당 두 개 이상의 포트가 포함되어야 합니다.

  브로드캐스트 도메인에 추가된 포트는 물리적 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.

- 모든 포트는 케이블로 연결되어야 합니다.
- 모든 포트가 정상 상태여야 합니다.
- 포트의 MTU 설정이 일치해야 합니다.

방화벽 요구 사항

방화벽과 인터클러스터 방화벽 정책은 다음 프로토콜을 허용해야 합니다.

- ICMP 서비스
- TCP - 포트 10000, 11104 및 11105를 통해 모든 인터클러스터 LIF의 IP 주소에 연결

- 인터클러스터 LIF 간 양방향 HTTPS

  CLI를 사용하여 클러스터 피어링을 설정할 때는 HTTPS가 필요하지 않지만 나중에 ONTAP 시스템 관리자를 사용하여 데이터 보호를 구성하면 HTTPS가 필요합니다.

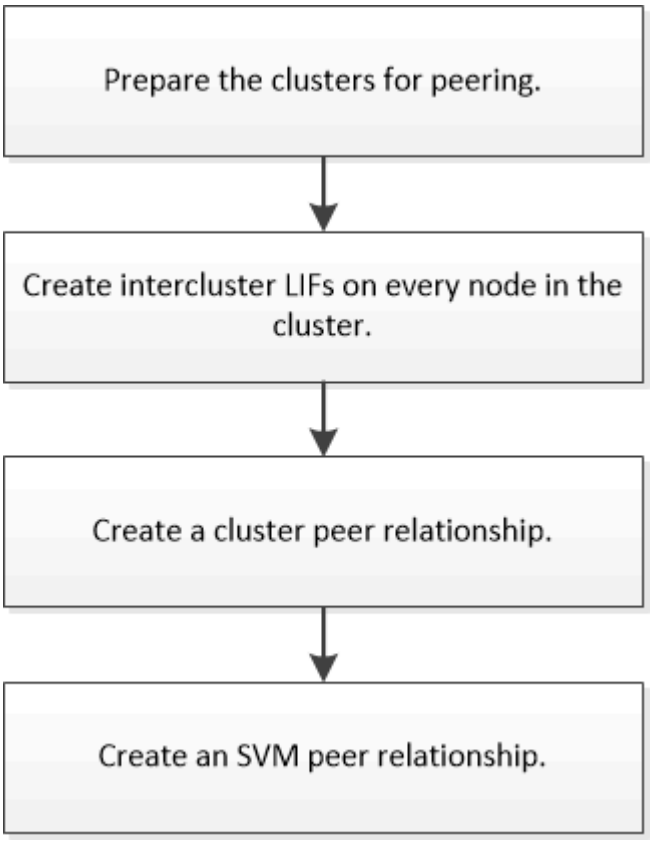
기본 '인터클러스터' 방화벽 정책은 HTTPS 프로토콜을 통해 모든 IP 주소(0.0.0.0/0)에서 액세스할 수 있도록 합니다. 필요한 경우 정책을 수정하거나 대체할 수 있습니다.

관련 정보

"데이터 보호"

클러스터 및 **SVM** 피어링 워크플로우

ONTAP 9.7 이하와 함께 ONTAP System Manager를 사용하여 피어링 관계를 설정할 수 있습니다. 피어링 관계를 구축하려면 각 클러스터를 피어링을 준비하고, 각 클러스터의 각 노드에 대한 인터클러스터 논리 인터페이스(LIF)를 생성하고, 클러스터 피어 관계를 설정한 다음 SVM 피어링 관계를 설정해야 합니다.



ONTAP 9.2 이하를 실행 중인 경우 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 생성하면서 SVM 피어링 관계를 생성합니다.

클러스터 피어링을 준비합니다

ONTAP 9.7 이하 버전의 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 클러스터 피어링 관계를 생성하기 전에, 각 클러스터의 시간이 외부 NTP(네트워크 시간 프로토콜) 서버와 동기화되는지 확인하고 사용하려는 서브넷, 포트 및 암호 문구를 결정해야

합니다.

단계

1. ONTAP 9.2 이하를 실행 중인 경우 각 클러스터 피어 관계에 사용할 암호를 결정합니다.

   암호는 8자 이상이어야 합니다.

다음 사이의 관계에 대해…	암호문은…
클러스터 A 및 클러스터 B	

   ONTAP 9.3부터 클러스터 피어 관계를 생성하는 동안 원격 클러스터에서 암호를 생성할 수 있습니다.

   "클러스터 피어 관계 생성(ONTAP 9.3부터 시작)"

2. 인터클러스터 LIF에 사용할 서브넷, IP 주소 및 포트를 식별합니다.

   기본적으로 IP 주소는 서브넷에서 자동으로 선택됩니다. IP 주소를 수동으로 지정하려면 IP 주소가 서브넷에서 이미 사용 가능한지 또는 나중에 서브넷에 추가될 수 있는지 확인해야 합니다. 서브넷에 대한 정보는 네트워크 탭에서 사용할 수 있습니다.

   다음 표와 유사한 테이블을 만들어 클러스터에 대한 정보를 기록합니다. 다음 표에서는 각 클러스터에 4개의 노드가 있다고 가정합니다. 클러스터에 노드가 4개 이상인 경우 추가 정보를 위해 행을 추가합니다.

	클러스터 A	클러스터 B
서브넷(ONTAP 9.2 이하)		
IP 주소(ONTAP 9.3부터 시작, ONTAP 9.2 이하의 경우 선택 사항)		
노드 1 포트		
노드 2 포트		
노드 3 포트		
노드 4 포트		

피어 관계 구성**(ONTAP 9.3**부터 시작**)**

피어 관계는 클러스터와 SVM이 데이터를 안전하게 교환할 수 있도록 네트워크 연결을 정의합니다. ONTAP 9.3부터 ONTAP 9.7까지 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 클러스터 및 SVM 간에 피어 관계를 구성하는 단순한 방법을 수행할 수 있습니다.

인터클러스터 **LIF** 만들기**(ONTAP 9.3**부터 시작**)**

ONTAP 9.3부터 ONTAP 9.7까지 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 클러스터 네트워크가 노드와 통신할 수 있도록 인터클러스터 논리 인터페이스(LIF)를 만들 수 있습니다. 피어 관계를 만들 각 클러스터의 각 노드에 피어링에 사용될 인터클러스터 LIF를 생성해야 합니다.

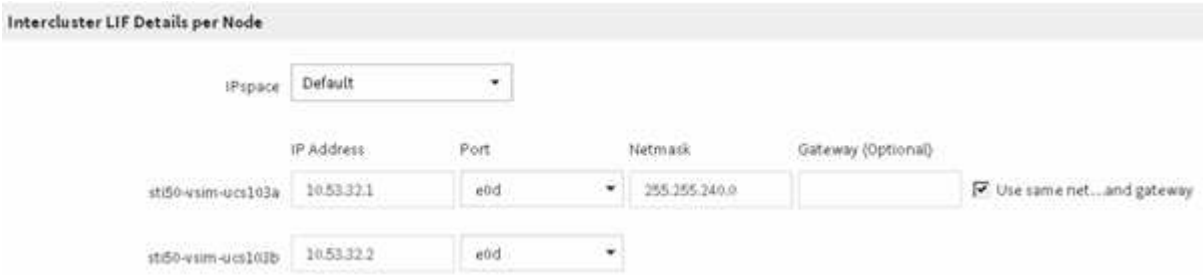
이 작업에 대해

예를 들어, IPspace A에서 클러스터 X를 사용하고 IPspace Y를 통해 클러스터 Y와 피어를 사용하려는 4노드 클러스터가 있는 경우 총 8개의 인터클러스터 LIF가 필요합니다. IPspace A에서 4개(노드당 1개) 및 Y에서 4개(노드당 1개)

피어 관계를 생성하려는 두 클러스터 모두에서 이 절차를 수행해야 합니다.

단계

1. 구성 * > * 고급 클러스터 설정 * 을 클릭합니다.
2. Setup Advanced Cluster Features * 창에서 * Cluster 피어링 * 옵션 옆의 * Proceed * 를 클릭합니다.
3. IPspace * 목록에서 IPspace를 선택합니다.
4. 각 노드의 IP 주소, 포트, 네트워크 마스크 및 게이트웨이 세부 정보를 입력합니다.



5. 제출 및 계속 * 을 클릭합니다.

다음 단계

클러스터 피어링을 계속하려면 클러스터 피어링 창에 클러스터 세부 정보를 입력해야 합니다.

클러스터 피어 관계 생성**(ONTAP 9.3**부터 시작**)**

ONTAP 9.3부터 ONTAP 9.7까지 ONTAP System Manager_classic_interface를 사용하면 원격 클러스터의 인터클러스터 LIF의 IP 주소와 시스템 생성 암호를 제공하여 두 클러스터 간에 클러스터 피어 관계를 만들 수 있습니다.

이 작업에 대해

ONTAP 9.6부터 클러스터 피어링 암호화는 새로 생성한 모든 클러스터 피어링 관계에서 기본적으로 활성화됩니다. ONTAP 9.6으로 업그레이드하기 전에 생성된 피어링 관계에 대해 클러스터 피어링 암호화를 수동으로 활성화해야 합니다. ONTAP 9.5 이전 버전을 실행하는 클러스터에서는 클러스터 피어링 암호화를 사용할 수 없습니다. 따라서 클러스터 피어링 암호화를 활성화하려면 피어링 관계의 두 클러스터가 ONTAP 9.6을 실행해야 합니다.

클러스터 피어링 암호화는 TLS(전송 보안 계층)를 사용하여 SnapMirror, FlexCache와 같은 ONTAP 기능에 대한 클러스터 간 피어링 통신을 보호합니다.

단계

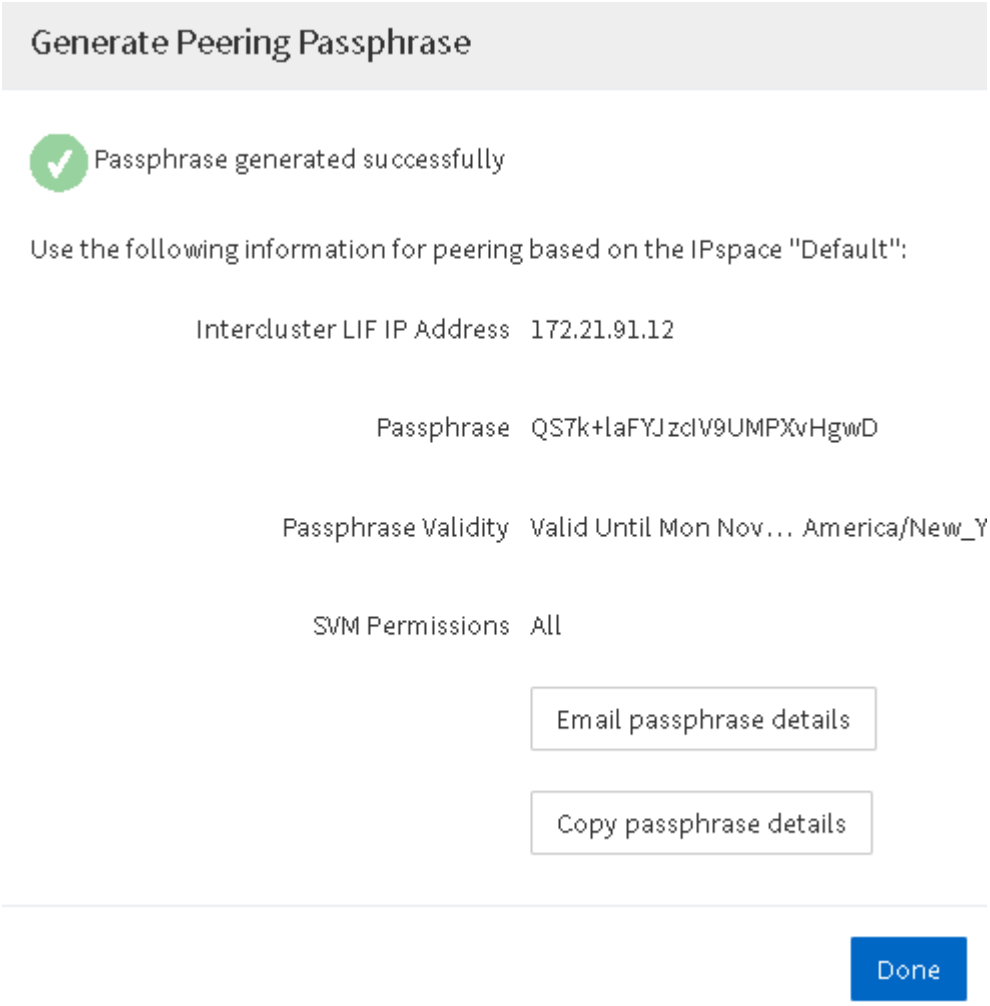
1. Target Cluster Intercluster LIF IP 주소 * 필드에 원격 클러스터의 LIF IP 주소를 입력합니다.
2. 원격 클러스터에서 암호를 생성합니다.

   a. 원격 클러스터의 관리 주소를 지정합니다.
   b. 관리 URL * 을 클릭하여 원격 클러스터에서 ONTAP 시스템 관리자를 시작합니다.
   c. 원격 클러스터에 로그인합니다.
   d. Cluster peer * 창에서 * Generate 피어링 Passphrase * 를 클릭합니다.
   e. IPspace, 암호문의 유효성 및 SVM 사용 권한을 선택합니다.

      모든 SVM이나 선택한 SVM을 피어링에 사용할 수 있습니다. SVM 피어 요청이 생성되면 원격 SVM에서 피어 관계를 승인하지 않고도 소스 SVM을 통해 허용되는 SVM을 자동으로 피어링됩니다.

   f. Generate * 를 클릭합니다.

      암호 정보가 표시됩니다.



   a. 암호 정보 복사 * 또는 * 이메일 암호 세부 정보 * 를 클릭합니다.
   b. 완료 * 를 클릭합니다.

3. 소스 클러스터에서 에서 생성한 암호를 입력합니다 2단계.
4. 클러스터 피어링 시작 * 을 클릭합니다.

   클러스터 피어 관계가 생성되었습니다.

5. 계속 * 을 클릭합니다.

다음 단계

피어링 프로세스를 계속 진행하려면 SVM 피어링 창에서 SVM 세부 정보를 지정해야 합니다.

SVM 피어 관계 생성

ONTAP 9.3부터 ONTAP 9.7까지 ONTAP System Manager_classic_interface를 사용하여 SVM 피어 관계를 생성할 수 있습니다. SVM(스토리지 가상 시스템) 피어링을 통해 두 SVM 간에 피어 관계를 설정하여 데이터 보호를 제공할 수 있습니다.

단계

1. 이니시에이터 SVM을 선택합니다.
2. 허용된 SVM 목록에서 타겟 SVM을 선택합니다.
3. SVM 피어링 시작 * 을 클릭합니다.
4. 계속 * 을 클릭합니다.

다음 단계

요약 창에서 인터클러스터 LIF, 클러스터 피어 관계 및 SVM 피어 관계를 볼 수 있습니다.

피어 관계 구성(ONTAP 9.2 이하)

ONTAP 9.2 또는 이전 ONTAP 9 릴리즈의 ONTAP System Manager_CLASSIC_INTERFACE를 사용하여 SVM 피어 관계를 생성할 수 있습니다.

피어 관계는 클러스터와 SVM이 데이터를 안전하게 교환할 수 있도록 네트워크 연결을 정의합니다. SVM 피어 관계를 생성하려면 먼저 클러스터 피어 관계를 생성해야 합니다.

모든 노드에 대한 인터클러스터 인터페이스 만들기(ONTAP 9.2 이하)

ONTAP 9.2 또는 이전 버전의 ONTAP 9 릴리스에 있는 ONTAP System Manager_classic_interface를 사용하면 피어링을 위해 사용될 인터클러스터 LIF를 만들 수 있습니다.

클러스터는 인터클러스터 통신 전용의 논리 인터페이스(LIF)를 통해 서로 통신합니다. 피어링에 사용될 각 IPspace 내에 인터클러스터 LIF를 생성해야 합니다. LIF는 피어 관계를 생성하려는 각 클러스터의 각 노드에 생성해야 합니다.

시작하기 전에

인터클러스터 LIF에 사용할 서브넷 및 포트와 선택적으로 IP 주소를 식별해야 합니다.

이 작업에 대해

피어 관계를 생성하려는 두 클러스터 모두에서 이 절차를 수행해야 합니다. 예를 들어, IPspace A에서 클러스터 X를 사용하고 IPspace Y를 통해 클러스터 Y와 피어를 사용하려는 4노드 클러스터가 있는 경우 총 8개의 인터클러스터 LIF가 필요합니다. IPspace A에서 4개(노드당 1개) 및 Y에서 4개(노드당 1개)

단계

1. [[step1-인터클러스터 LIF]] 소스 클러스터의 한 노드에 대한 인터클러스터 LIF를 만듭니다.
   a. 네트워크 인터페이스 * 창으로 이동합니다.
   b. Create * 를 클릭합니다.

      네트워크 인터페이스 생성 대화 상자가 표시됩니다.

   c. 인터클러스터 LIF의 이름을 입력합니다.

      첫 번째 노드의 인터클러스터 LIF에는 ""icl01""을 사용하고 두 번째 노드의 인터클러스터 LIF에는 ""icl02""를 사용할 수 있습니다.

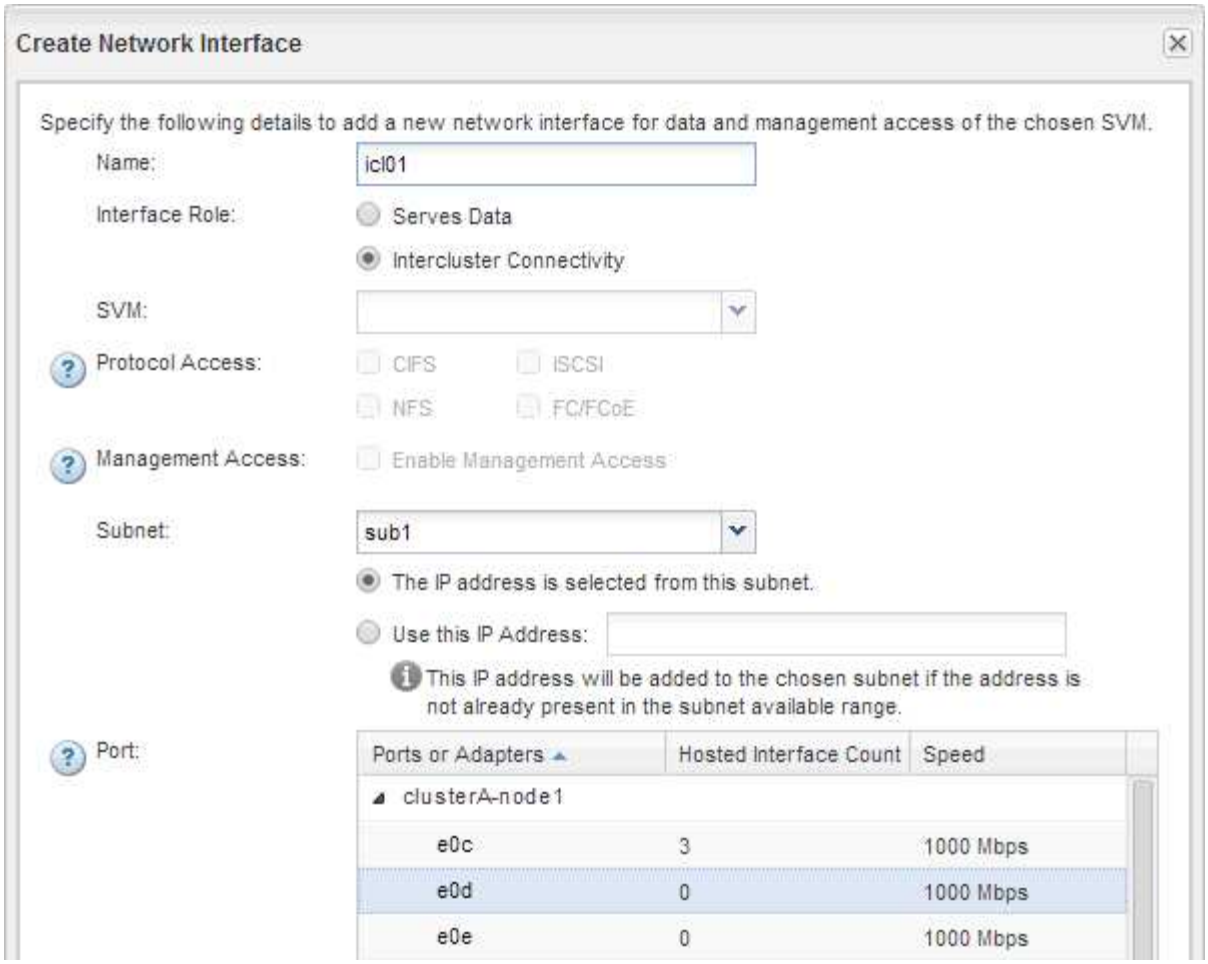
   d. 인터페이스 역할로 * Intercluster Connectivity * 를 선택합니다.
   e. IPspace를 선택합니다.
   f. 세부 정보 추가 * 대화 상자의 * IP 주소 할당 * 드롭다운 목록에서 * 서브넷 사용 * 을 선택한 다음 인터클러스터 통신에 사용할 서브넷을 선택합니다.

      기본적으로 IP 주소는 * Create * 를 클릭하면 서브넷에서 자동으로 선택됩니다. 자동으로 선택된 IP 주소를 사용하지 않으려면 노드가 인터클러스터 통신에 사용하는 IP 주소를 수동으로 지정해야 합니다.

   g. 노드가 인터클러스터 통신에 사용하는 IP 주소를 수동으로 지정하려면 * 이 IP 주소 사용 * 을 선택하고 IP 주소를 입력합니다.

      사용하려는 IP 주소가 서브넷에서 이미 사용 가능한지 또는 나중에 서브넷에 추가될 수 있는지 확인해야 합니다.

   h. Ports * 영역에서 구성할 노드를 클릭하고 이 노드에 사용할 포트를 선택합니다.
   i. 데이터 통신과의 인터클러스터 통신을 위해 포트를 공유하지 않기로 결정한 경우 선택한 포트가 * Hosted Interface Count * 열에 ""0""으로 표시되는지 확인합니다.



   j. Create * 를 클릭합니다.

2. 반복합니다 1단계 클러스터에 있는 각 노드에 대해

   클러스터의 각 노드에는 인터클러스터 LIF가 있습니다.

3. 다른 클러스터와의 피어 관계를 만들 때 나중에 사용할 수 있도록 인터클러스터 LIF의 IP 주소를 기록해 두십시오.

   a. 네트워크 인터페이스 * 창의 * 역할 * 열에서 을 클릭합니다 에서 * 모두 * 확인란의 선택을 취소한 다음 * 클러스터 간 * 을 선택합니다.

      네트워크 인터페이스 창에는 인터클러스터 LIF만 표시됩니다.

   b. IP 주소/WWPN * 열에 나열된 IP 주소를 적어 두거나 나중에 IP 주소를 검색할 수 있도록 * Network Interfaces * 창을 열어 두십시오.

      열 표시 아이콘( )를 클릭하여 표시하지 않을 열을 숨깁니다.

결과

각 클러스터의 모든 노드에는 서로 통신할 수 있는 인터클러스터 LIF가 있습니다.

클러스터 피어 관계 생성**(ONTAP 9.2** 이하**)**

ONTAP 9.2 이하 ONTAP 버전의 ONTAP System Manager_classic_interface를 사용하면 원격 클러스터의 인터클러스터 LIF의 IP 주소와 사전 지정된 암호를 입력하여 두 클러스터 간에

클러스터 피어 관계를 만들 수 있습니다. 그런 다음 관계가 성공적으로 생성되었는지 확인합니다.

시작하기 전에

- 피어로 사용하려는 클러스터의 모든 인터클러스터 LIF의 IP 주소를 알아야 합니다.
- 각 피어 관계에 사용할 암호를 알아야 합니다.

이 작업에 대해

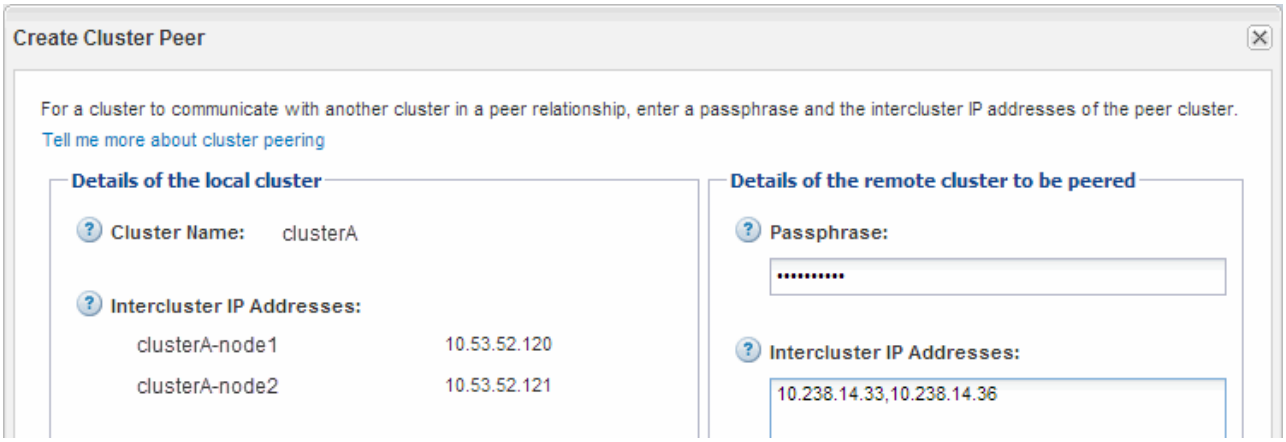
각 클러스터에서 이 절차를 수행해야 합니다.

단계

1. 소스 클러스터에서 대상 클러스터와 클러스터 피어 관계를 생성합니다.
   a. 구성 * 탭을 클릭합니다.
   b. 클러스터 설정 * 창에서 * 클러스터 피어 * 를 클릭합니다.
   c. Create * 를 클릭합니다.

      클러스터 피어 생성 * 대화 상자가 표시됩니다.

   d. 원격 클러스터 세부 정보 * 영역에서 두 피어가 인증된 클러스터 피어 관계를 보장하기 위해 사용할 암호를 지정합니다.
   e. 대상 클러스터의 모든 인터클러스터 LIF(노드당 1개)의 IP 주소를 쉼표로 구분하여 입력합니다.



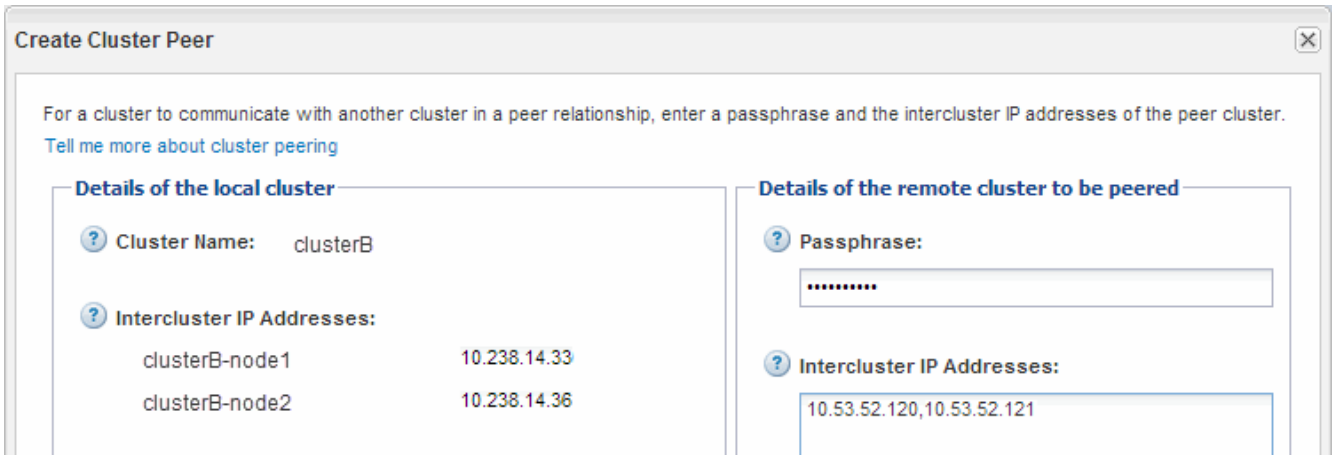
   f. Create * 를 클릭합니다.

      한 개의 클러스터만 구성되었기 때문에 인증 상태는 "보류 중"입니다.

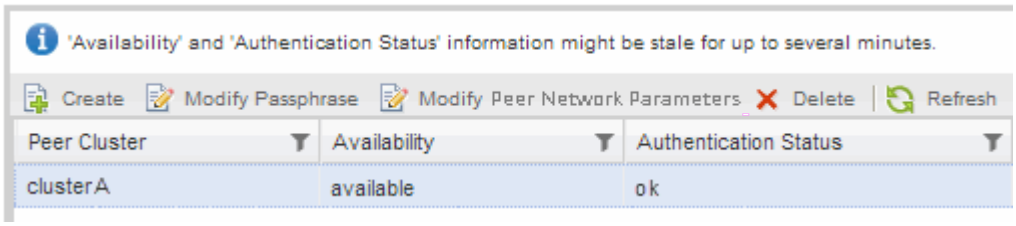
2. 대상 클러스터로 전환한 다음 소스 클러스터와 클러스터 피어 관계를 생성합니다.
   a. 구성 * 탭을 클릭합니다.
   b. 클러스터 설정 * 창에서 * 클러스터 피어 * 를 클릭합니다.
   c. Create * 를 클릭합니다.

      클러스터 피어 생성 대화 상자가 표시됩니다.

   d. 피어링할 원격 클러스터의 * 세부 정보 영역에서 에 지정한 것과 동일한 암호를 지정합니다 1d단계 및 소스 클러스터의 인터클러스터 LIF의 IP 주소를 클릭한 다음 * Create * 를 클릭합니다.



3. 대상 클러스터의 * Cluster 피어 * 창에서 소스 클러스터가 ""사용 가능""이고 인증 상태가 ""정상""인지 확인합니다.



업데이트된 정보를 보려면 * Refresh * (새로 고침 *)를 클릭해야 할 수도 있습니다.

두 클러스터는 피어 관계에 있습니다.

4. 소스 클러스터로 전환하고 대상 클러스터가 "사용 가능"이고 인증 상태가 "확인"인지 확인합니다.

업데이트된 정보를 보려면 * Refresh * (새로 고침 *)를 클릭해야 할 수도 있습니다.

다음 단계

소스 볼륨과 타겟 볼륨 사이에 데이터 보호 관계를 생성하면서 소스 및 타겟 SVM 간에 SVM 피어 관계를 생성합니다.

"SnapVault를 사용한 볼륨 백업"

"볼륨 재해 복구 준비"

볼륨 재해 복구

볼륨 재해 복구 개요

재해 발생 후 타겟 볼륨을 빠르게 활성화한 다음 ONTAP System Manager의 클래식 인터페이스(ONTAP 9.7 이하)를 사용하여 ONTAP에서 소스 볼륨을 다시 활성화할 수 있습니다.

다음과 같은 방법으로 볼륨 레벨 재해 복구를 수행하려면 이 절차를 사용하십시오.

- ONTAP 9를 실행하는 클러스터로 작업하고 있습니다.
- 클러스터 관리자입니다.

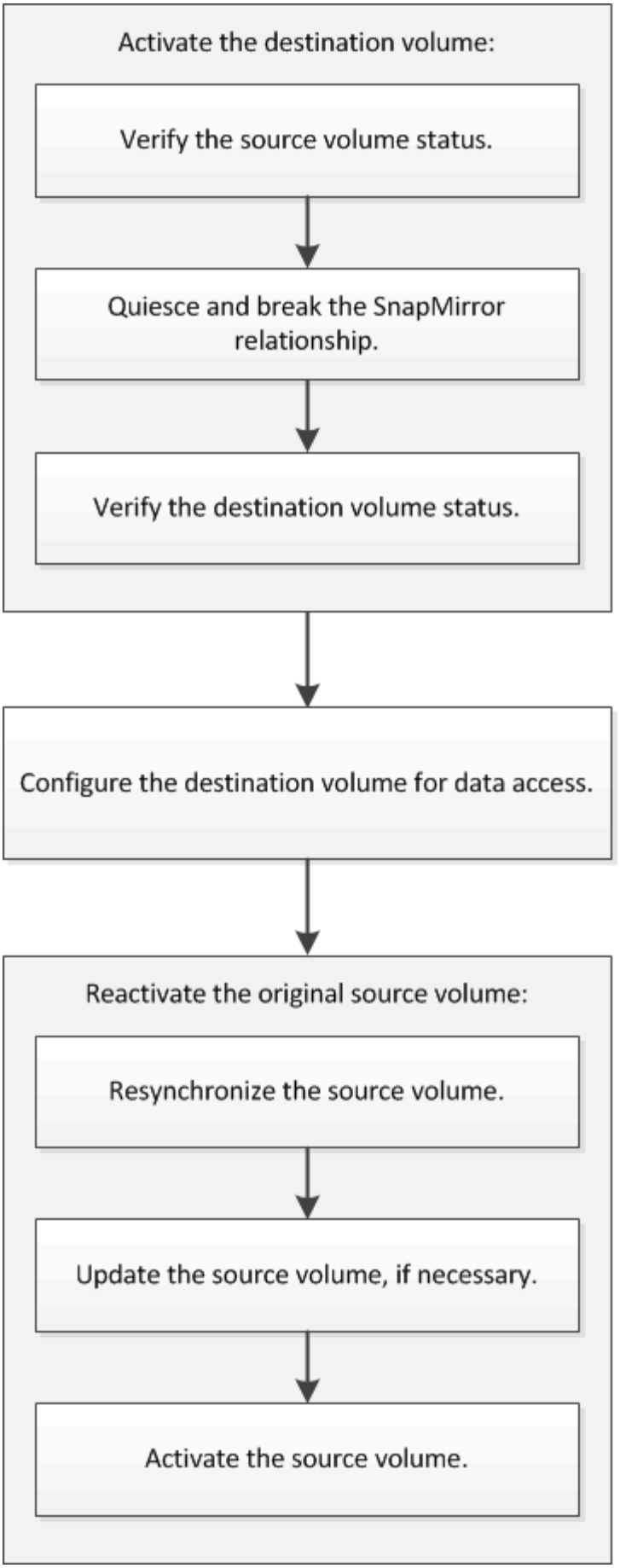
- 다음에 SnapMirror 관계를 구성했습니다 볼륨 재해 복구 준비
- 소스 클러스터의 클러스터 관리자는 데이터 손상 또는 실수로 데이터가 삭제되는 바이러스 감염과 같은 이벤트로 인해 소스 볼륨의 데이터를 사용할 수 없다고 선언했습니다.
- ONTAP 명령줄 인터페이스 또는 자동화된 스크립팅 도구가 아니라 System Manager를 사용하려고 합니다.
- ONTAP 9.7 이상을 위한 ONTAP 시스템 관리자 UI가 아니라 ONTAP 9.7 이전 릴리즈용 System Manager 클래식 인터페이스를 사용하려는 경우
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- 많은 개념적 배경을 읽고 싶지 않습니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"SnapMirror 대상에 데이터를 제공합니다"
ONTAP 명령줄 인터페이스입니다	"대상 볼륨을 활성화합니다"

볼륨 재해 복구 워크플로우

볼륨 재해 복구 워크플로우에는 대상 볼륨 활성화, 데이터 액세스를 위한 대상 볼륨 구성, 원래 소스 볼륨 재활성화가 포함됩니다.


Activate the destination volume:
Verify the source volume status.
Quiesce and break the SnapMirror relationship.
Verify the destination volume status.
Configure the destination volume for data access.
Reactivate the original source volume:
Resynchronize the source volume.
Update the source volume, if necessary.
Activate the source volume.

볼륨 레벨 재해 복구 관계를 관리하는 데 도움이 되는 추가 정보를 제공하고 데이터 리소스의 가용성을 보호하는 다른 재해 복구 방법을 제공합니다.

- SnapVault를 사용한 볼륨 백업

  서로 다른 ONTAP 클러스터에 있는 볼륨 간의 백업 볼트 관계를 빠르게 구성하는 방법에 대해 설명합니다.

- SnapVault를 사용한 볼륨 복원 관리

  ONTAP의 백업 볼트에서 볼륨을 빠르게 복원하는 방법에 대해 설명합니다.

대상 볼륨을 활성화합니다

데이터 손상, 실수로 인한 삭제 또는 오프라인 상태와 같은 이벤트로 인해 소스 볼륨에서 데이터를 처리할 수 없는 경우 소스 볼륨에서 데이터를 복구할 때까지 대상 볼륨을 활성화하여 데이터 액세스를 제공해야 합니다. 앞으로 SnapMirror 데이터 전송을 중지하고 SnapMirror 관계를 끊는 작업이 활성화 됩니다.

소스 볼륨의 상태를 확인합니다

소스 볼륨을 사용할 수 없는 경우 소스 볼륨이 오프라인 상태인지 확인한 다음 데이터 액세스를 제공하기 위해 활성화해야 하는 대상 볼륨을 식별해야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. Volumes * 창으로 이동합니다.
2. 소스 볼륨을 선택한 다음 소스 볼륨이 오프라인 상태인지 확인합니다.
3. SnapMirror 관계에서 대상 볼륨을 식별합니다.
   - ONTAP 9.3부터: 소스 볼륨을 두 번 클릭하여 세부 정보를 확인한 다음, * 보호 * 를 클릭하여 SnapMirror 관계에서 타겟 볼륨과 볼륨이 포함된 SVM 이름을 확인합니다.

   - ONTAP 9.2 이하: 볼륨 페이지 아래쪽에 있는 * 데이터 보호 * 탭을 클릭하여 SnapMirror 관계의 타겟 볼륨과 볼륨이 들어 있는 SVM 이름을 식별하십시오.

SnapMirror 관계를 발전시킬 수 있습니다

대상 볼륨을 활성화하려면 SnapMirror 관계를 중지 및 해제해야 합니다. 일시 중지 후에는 SnapMirror 데이터 전송이 비활성화됩니다.

시작하기 전에

타겟 볼륨은 대상 SVM 네임스페이스에 마운트되어야 합니다.

이 작업에 대해

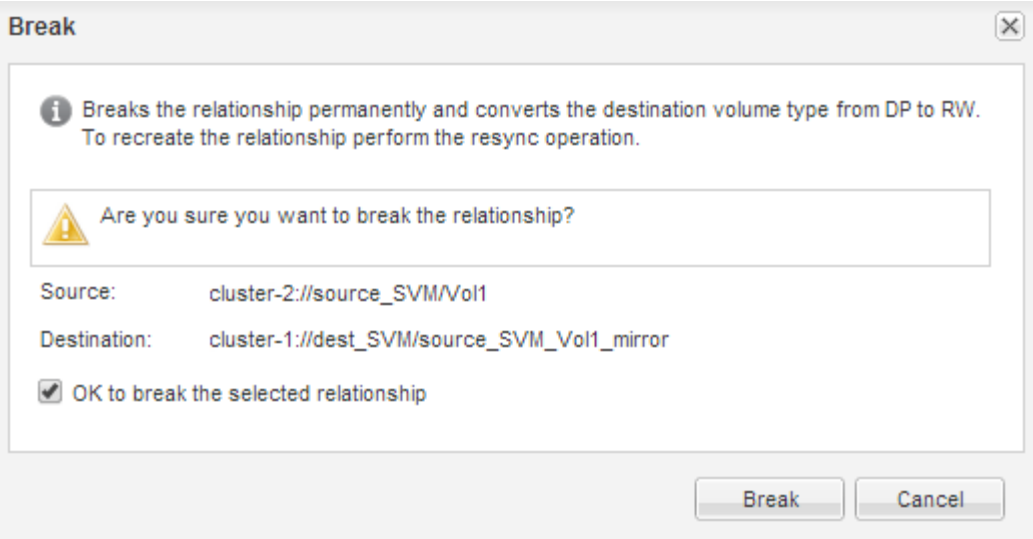
대상 * 클러스터에서 이 작업을 수행해야 합니다.

단계

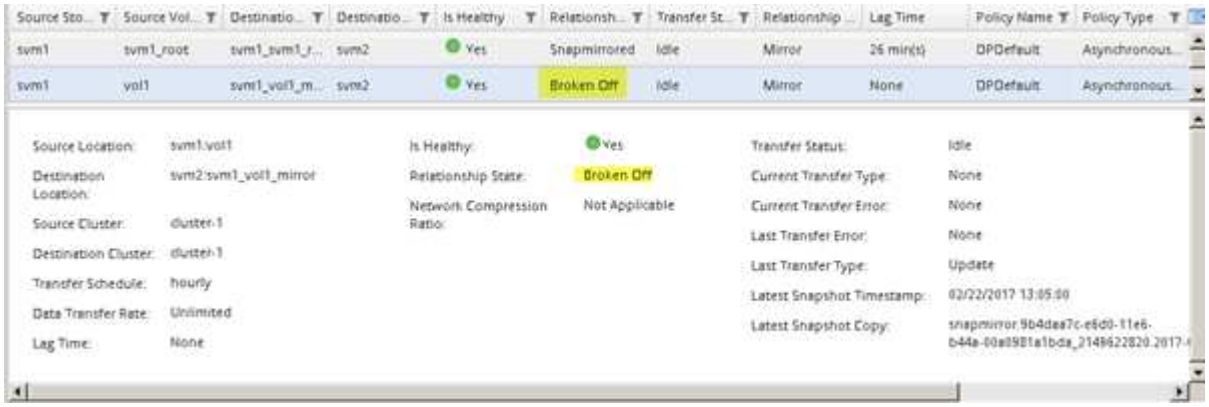
1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택합니다.
3. 운영 * > * 정지 * 를 클릭하여 향후 데이터 전송을 비활성화합니다.
4. 확인 확인란을 선택한 다음 * 정지 * 를 클릭합니다.

   일시 중지 작업에는 다소 시간이 걸릴 수 있습니다. 전송 상태가 "중지"로 표시될 때까지 SnapMirror 관계에 대해 다른 작업을 수행하지 않아야 합니다.

5. Operations * > * Break * 를 클릭합니다.
6. 확인 확인란을 선택한 다음 * Break * (휴식 *)를 클릭합니다.



SnapMirror 관계가 "부분 종료" 상태입니다.



대상 볼륨 상태를 확인합니다

SnapMirror 관계를 끊은 후에는 대상 볼륨에 읽기/쓰기 권한이 있고 대상 볼륨 설정이 소스 볼륨의 설정과 일치하는지 확인해야 합니다.

이 작업에 대해

대상 * 클러스터에서 이 작업을 수행해야 합니다.

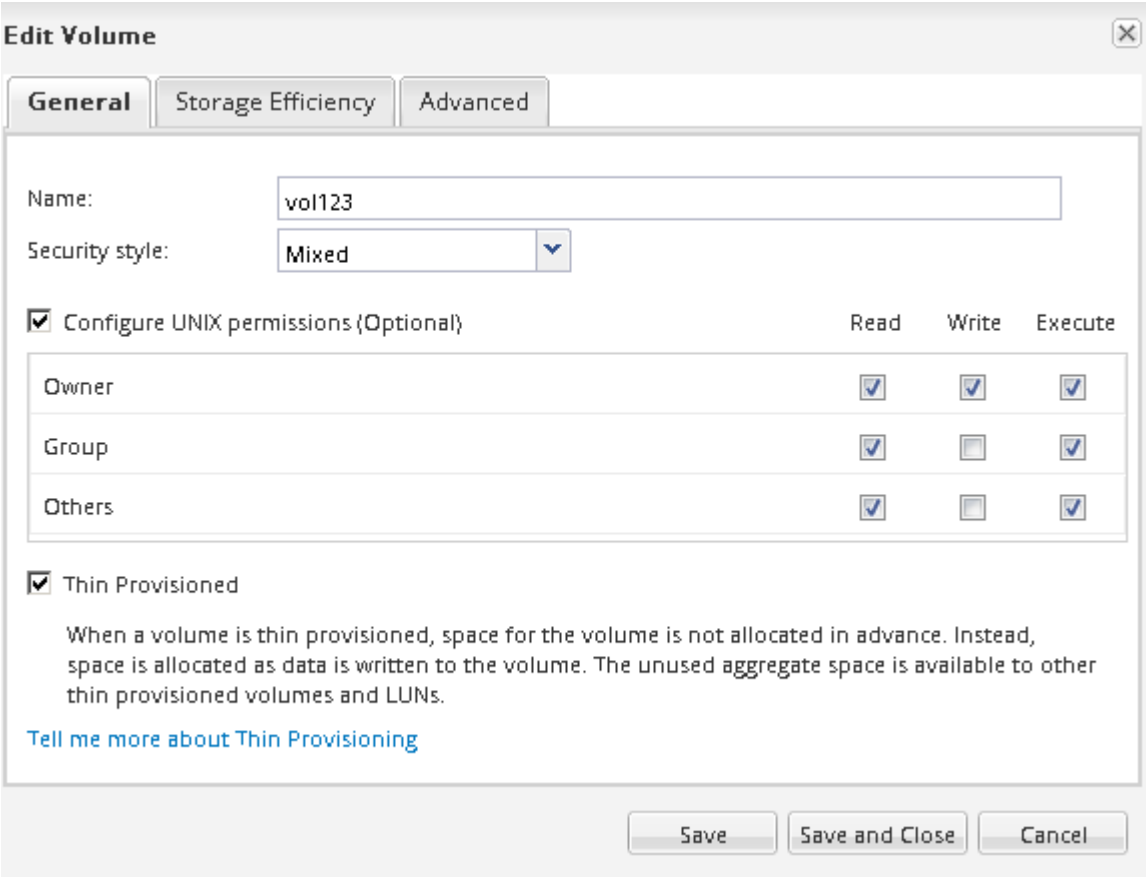
단계

1. Volumes * 창으로 이동합니다.
2. 볼륨 * 목록에서 대상 볼륨을 선택한 다음 대상 볼륨 유형이 읽기/쓰기 액세스를 나타내는 "RW"인지 확인합니다.
3. 타겟 볼륨의 씬 프로비저닝, 중복제거, 압축, 자동 확장 같은 볼륨 설정이 소스 볼륨의 설정과 일치하는지 확인합니다.

   SnapMirror 관계를 생성한 후 볼륨 설정 정보를 사용하여 대상 볼륨 설정을 확인할 수 있습니다.

4. 볼륨 설정이 일치하지 않으면 필요에 따라 대상 볼륨의 설정을 수정합니다.
   a. 편집 * 을 클릭합니다.
   b. 필요에 따라 환경에 대한 일반 설정, 스토리지 효율성 설정 및 고급 설정을 수정합니다.

c. 저장 후 닫기 * 를 클릭합니다.



d. 볼륨 * 목록의 열이 적절한 값으로 업데이트되었는지 확인합니다.

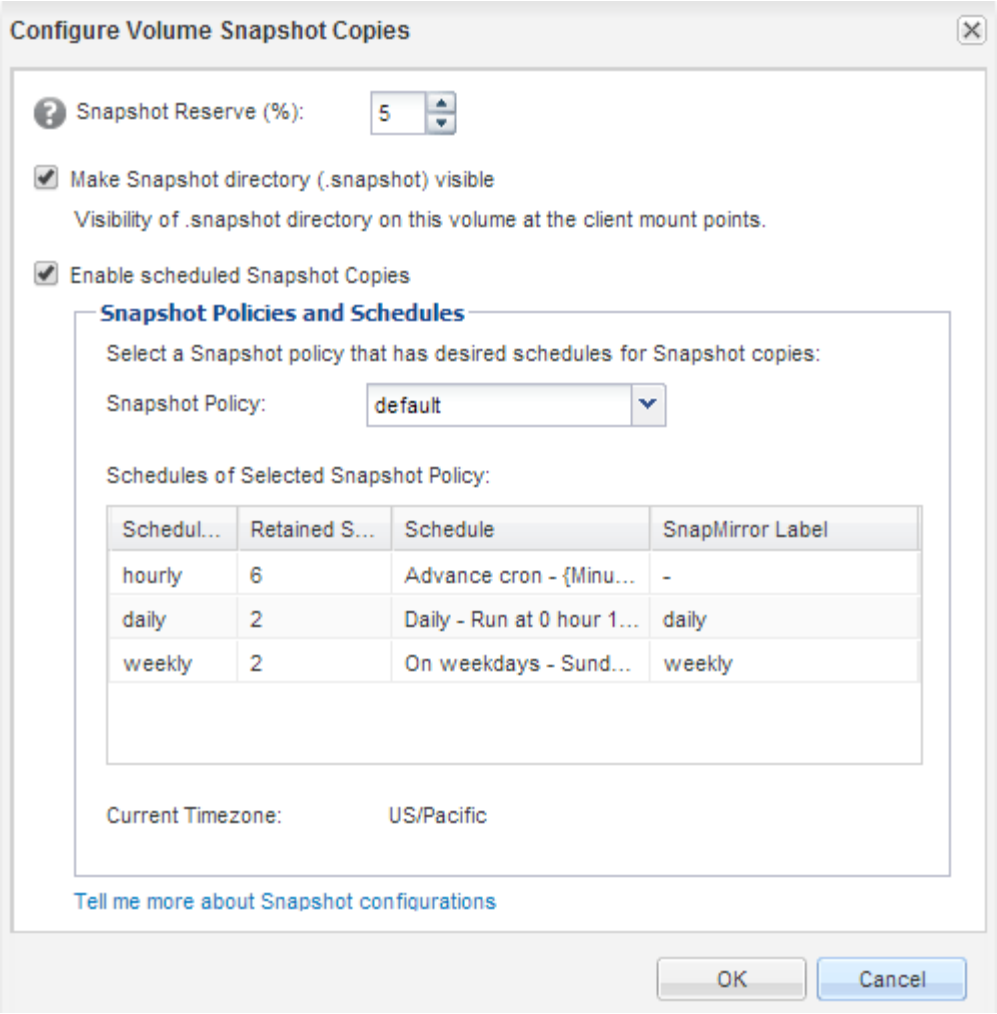
5. 타겟 볼륨에 대한 스냅샷 복사본 생성을 사용하도록 설정합니다.

a. ONTAP 버전에 따라 다음 방법 중 하나로 * 볼륨 스냅샷 복사본 구성 * 페이지로 이동합니다.

ONTAP 9.3부터 시작: 대상 볼륨을 선택한 다음 * 작업 * > * 스냅샷 관리 * > * 구성 * 을 클릭합니다.

ONTAP 9.2 이하: 대상 볼륨을 선택한 다음 * Snapshot 복사본 * > * 구성 * 을 클릭합니다.

b. 예약된 Snapshot 복사본 사용 * 확인란을 선택한 다음 * 확인 * 을 클릭합니다.



데이터 액세스를 위한 대상 볼륨을 구성합니다

대상 볼륨을 활성화한 후 데이터 액세스를 위해 볼륨을 구성해야 합니다. 소스 볼륨이 다시 활성화될 때까지 NAS 클라이언트와 SAN 호스트가 대상 볼륨의 데이터에 액세스할 수 있습니다.

이 작업에 대해

대상 * 클러스터에서 이 작업을 수행해야 합니다.

절차를 참조하십시오

- NAS 환경:
  a. 소스 볼륨이 소스 SVM에 마운트된 것과 동일한 접합 경로를 사용하여 NAS 볼륨을 네임스페이스에 마운트합니다.
  b. 대상 볼륨의 CIFS 공유에 적절한 ACL을 적용합니다.
  c. 대상 볼륨에 NFS 내보내기 정책을 할당합니다.
  d. 대상 볼륨에 할당량 규칙을 적용합니다.
  e. DNS 이름 확인 변경과 같은 필요한 단계를 수행하여 클라이언트를 대상 볼륨으로 리디렉션합니다.
  f. 클라이언트에서 NFS 및 CIFS 공유를 다시 마운트합니다.

- SAN 환경:
  a. LUN을 적절한 이니시에이터 그룹에 매핑하여 볼륨의 LUN을 SAN 클라이언트에서 사용할 수 있도록 합니다.
  b. iSCSI의 경우 SAN 호스트 이니시에이터에서 SAN LIF로 iSCSI 세션을 생성합니다.
  c. SAN 클라이언트에서 스토리지 재검색을 수행하여 연결된 LUN을 검색합니다.

다음 단계

소스 볼륨을 사용할 수 없게 된 문제를 해결해야 합니다. 가능하면 소스 볼륨을 다시 온라인으로 만든 다음 소스 볼륨을 재동기화하여 다시 활성화해야 합니다.

- 관련 정보 *

"ONTAP 9 문서 센터"

소스 볼륨을 다시 활성화합니다

소스 볼륨을 사용할 수 있게 되면 대상 볼륨에서 소스 볼륨으로 데이터를 재동기화하고 재동기화 작업 후 수정 사항을 업데이트한 다음 소스 볼륨을 활성화해야 합니다.

소스 볼륨을 재동기화합니다

소스 볼륨이 온라인 상태일 때 대상 볼륨과 소스 볼륨 간의 데이터를 재동기화하여 대상 볼륨의 최신 데이터를 복제해야 합니다.

시작하기 전에

소스 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

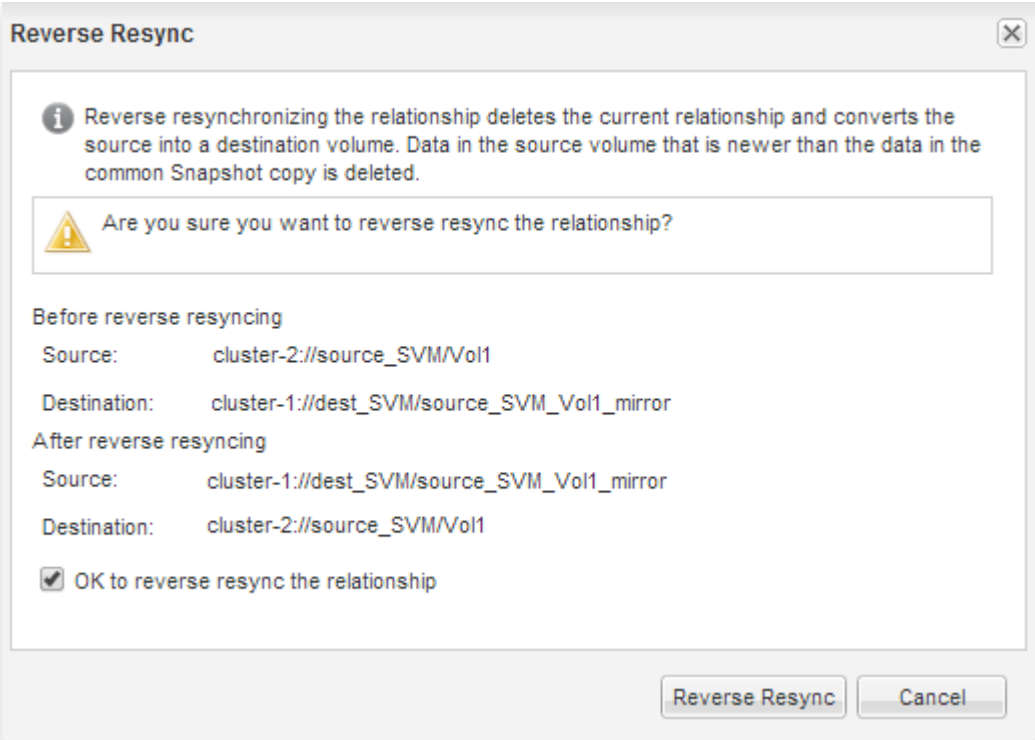
대상 * 클러스터에서 작업을 수행해야 합니다.

다음 이미지는 활성 대상 볼륨에서 읽기 전용 소스 볼륨으로 데이터가 복제되었음을 보여 줍니다.

단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택합니다.
3. SnapMirror 관계에 대해 구성된 전송 일정과 정책을 기록해 둡니다.
4. Operations * > * Reverse Resync * 를 클릭합니다.

5. 확인 확인란을 선택한 다음 * 역방향 재동기화 * 를 클릭합니다.



ONTAP 9.3부터 관계의 SnapMirror 정책이 "무러일스냅샷"으로 설정되고 미러 스케줄이 "없음"으로 설정됩니다.

ONTAP 9.2 이하를 실행 중인 경우 관계의 SnapMirror 정책이 DPDefault로 설정되고 미러 스케줄이 None으로 설정됩니다.

6. 소스 클러스터에서 원본 SnapMirror 관계의 보호 구성과 일치하는 SnapMirror 정책 및 일정을 지정합니다.
   a. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
      - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
      - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
   b. 재동기화된 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택한 다음 * 편집 * 을 클릭합니다.
   c. SnapMirror 정책 및 일정을 선택하고 * OK * 를 클릭합니다.

소스 볼륨을 업데이트합니다

소스 볼륨을 재동기화한 후 소스 볼륨을 활성화하기 전에 소스 볼륨에서 최신 변경 사항이 모두 업데이트되도록 할 수 있습니다.

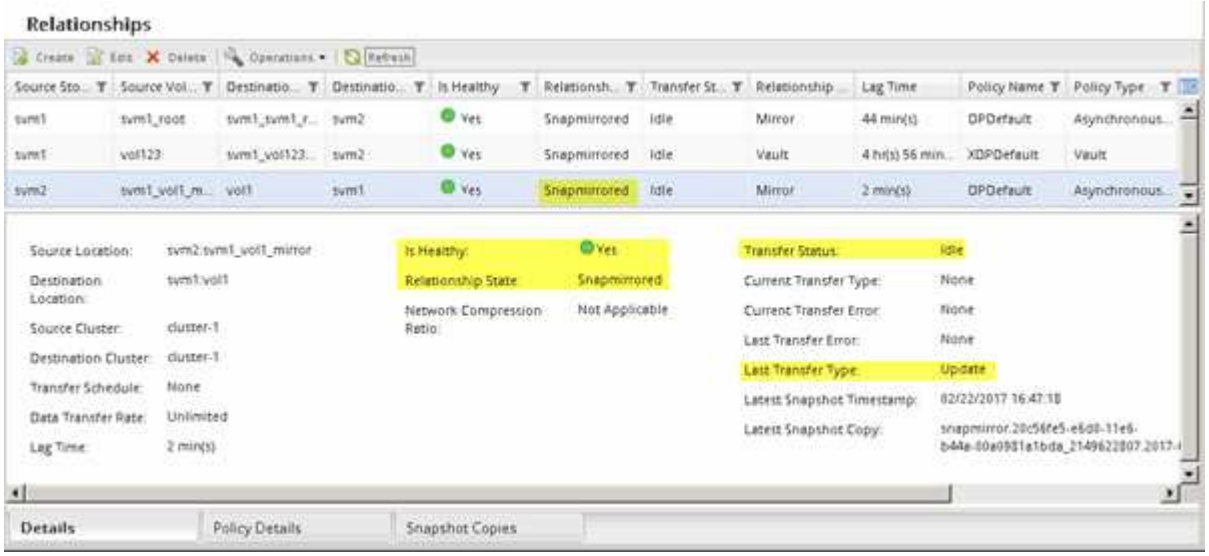
이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.

2. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택한 다음 * 운영 * > * 업데이트 * 를 클릭합니다.
3. 소스 볼륨과 타겟 볼륨 간의 최신 공통 스냅샷 복사본에서 증분 전송을 수행합니다.
   - ONTAP 9.3부터: * 정책에 따라 * 옵션을 선택합니다.
   - ONTAP 9.2 이하: * On demand * 옵션을 선택합니다.
4. * 선택 사항: * 전송에 사용되는 네트워크 대역폭을 제한하려면 * 전송 대역폭을 * 로 제한 을 선택한 다음 최대 전송 속도를 지정합니다.
5. Update * 를 클릭합니다.
6. 전송 상태가 Idle인지, 마지막 전송 유형이 * Details * 탭에서 Update인지 확인한다.



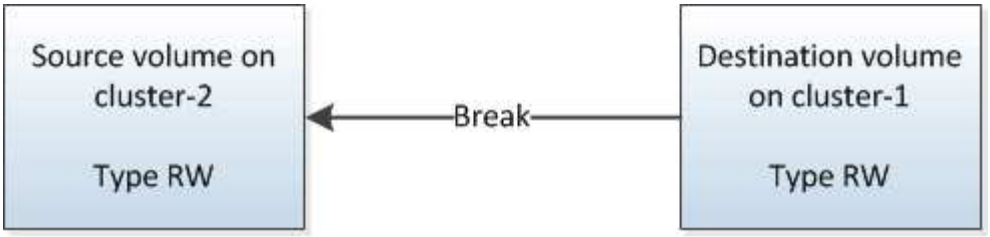
소스 볼륨을 다시 활성화합니다

대상 볼륨에서 소스 볼륨으로 데이터를 재동기화한 후 SnapMirror 관계를 끊어 소스 볼륨을 활성화해야 합니다. 다시 활성화된 소스 볼륨을 보호하기 위해 대상 볼륨을 재동기화해야 합니다.

이 작업에 대해

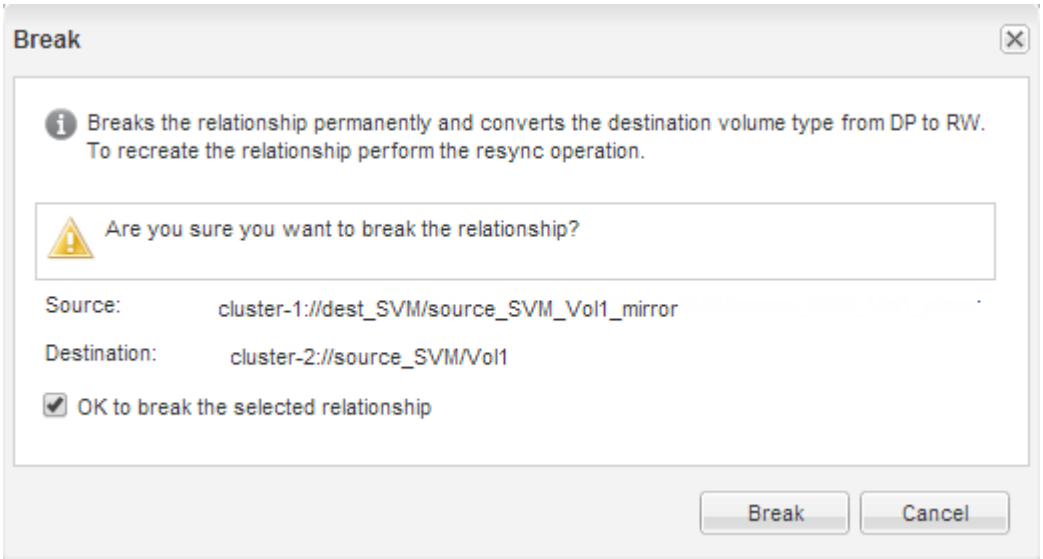
중단 및 역방향 재동기화 작업은 모두 * 소스 * 클러스터에서 수행됩니다.

다음 이미지는 SnapMirror 관계를 분리할 때 소스 볼륨과 타겟 볼륨이 읽기/쓰임을 보여 줍니다. 역방향 재동기화 작업 후 데이터는 활성 소스 볼륨에서 읽기 전용 타겟 볼륨으로 복제됩니다.

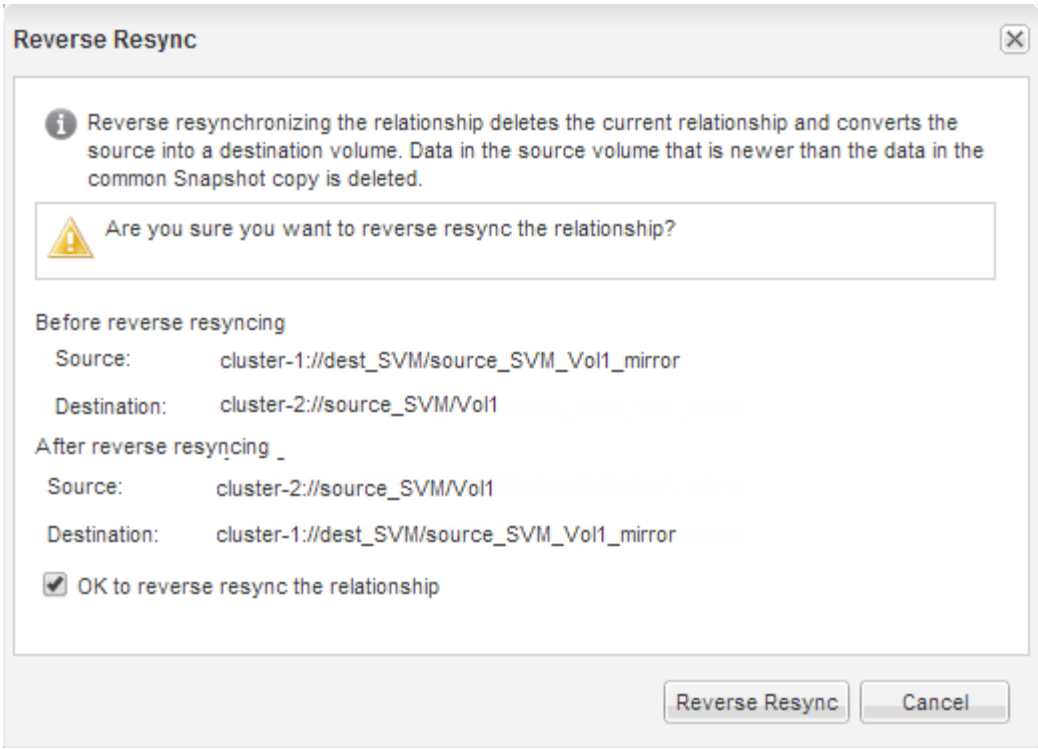


단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택합니다.
3. 작업 * > * 정지 * 를 클릭합니다.
4. 확인 확인란을 선택한 다음 * 정지 * 를 클릭합니다.
5. Operations * > * Break * 를 클릭합니다.
6. 확인 확인란을 선택한 다음 * Break * (휴식 *)를 클릭합니다.



7. Operations * > * Reverse Resync * 를 클릭합니다.
8. 확인 확인란을 선택한 다음 * 역방향 재동기화 * 를 클릭합니다.



ONTAP 9.3부터는 관계에 대한 SnapMirror 정책이 MirorAllSnapshots으로 설정되고 SnapMirror 일정이 None으로 설정됩니다.

ONTAP 9.2 이하를 실행 중인 경우 관계의 SnapMirror 정책이 DPDefault로 설정되고 SnapMirror 일정이 "None"으로 설정됩니다.

9. 볼륨 페이지에서 소스 볼륨으로 이동하여 생성한 SnapMirror 관계가 나열되고 관계 상태가 '스냅샷 미러링'인지 확인합니다.
10. 대상 클러스터에서 새 SnapMirror 관계에 대한 원래 SnapMirror 관계의 보호 구성과 일치하는 SnapMirror 정책 및 일정을 지정합니다.
    a. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
        - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
        - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
    b. 재활성화된 소스와 대상 볼륨 간의 SnapMirror 관계를 선택한 다음 * 편집 * 을 클릭합니다.
    c. SnapMirror 정책 및 일정을 선택하고 * OK * 를 클릭합니다.

결과

소스 볼륨은 읽기/쓰기 액세스 권한을 가지고 있으며 대상 볼륨에 의해 보호됩니다.

볼륨 재해 복구 준비

볼륨 재해 복구 준비 개요

재해 복구 준비를 위해 피어링된 ONTAP 클러스터에서 소스 볼륨을 빠르게 보호할 수 있습니다. 볼륨 재해 복구를 위해 피어링된 클러스터 간의 SnapMirror 관계를 구성하고 모니터링하려는

경우 이 절차를 사용해야 하며 작업에 대한 많은 개념적 배경이 필요하지 않습니다.

SnapMirror는 예약된 비동기식 블록 레벨 데이터 보호를 제공합니다. SnapMirror는 스냅샷 복사본을 복제하고 Qtree 및 LUN이 포함된 볼륨을 포함하여 중복제거, 데이터 압축 또는 둘 다 실행되는 NAS 또는 SAN 볼륨을 복제할 수 있습니다. SnapMirror 구성 정보는 ONTAP에서 클러스터의 모든 노드에 복제하는 데이터베이스에 저장됩니다.

다음 방법으로 볼륨 레벨 재해 복구를 위한 SnapMirror 관계를 생성하려는 경우 이 절차를 사용합니다.

- ONTAP 9를 실행하는 클러스터로 작업하고 있습니다.
- 클러스터 관리자입니다.
- 클러스터 피어 관계 및 SVM 피어 관계를 구성했습니다.

  "클러스터 및 SVM 피어링 구성"

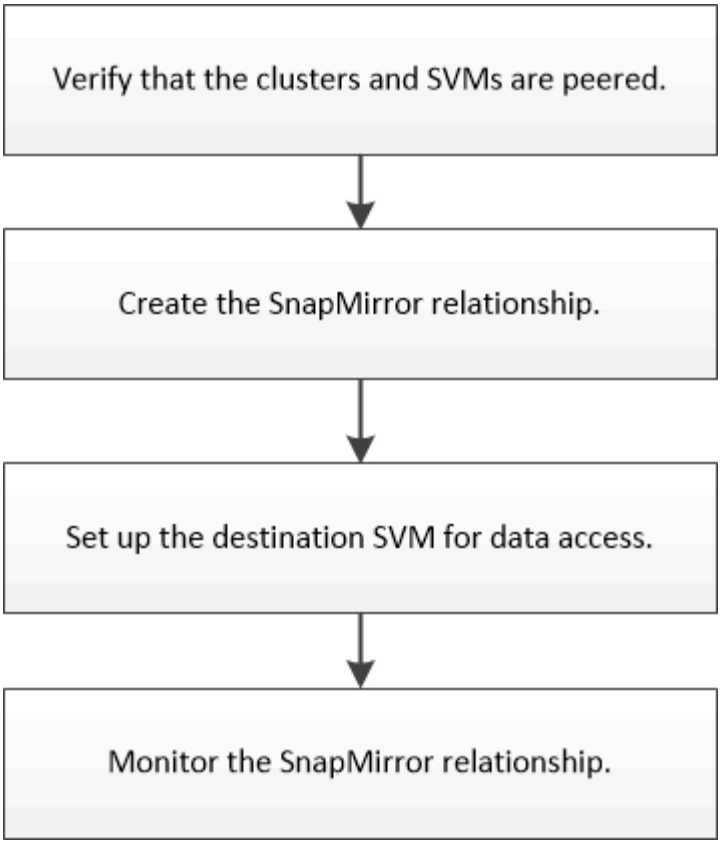
- 소스 및 대상 클러스터 모두에서 SnapMirror 라이센스를 활성화했습니다.
- 사용자 지정 정책을 만들지 않고 기본 정책 및 일정을 사용하려고 합니다.
- 사용 가능한 모든 옵션(ONTAP 9.7 이하)을 탐색하는 것이 아니라 모범 사례를 활용하고자 합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면…	자세한 내용은…
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"미러링 및 보관 준비"
ONTAP 명령줄 인터페이스입니다	"클러스터 피어 관계 생성(ONTAP 9.3 이상)"

볼륨 재해 복구 준비 워크플로우

재해 복구를 위한 볼륨을 준비하려면 클러스터 피어 관계를 확인하고, 피어링된 클러스터에 있는 볼륨 간에 SnapMirror 관계를 구축하고, 데이터 액세스를 위한 대상 SVM을 설정하고, SnapMirror 관계를 정기적으로 모니터링해야 합니다.



재해 복구 설정을 테스트하거나 재해가 발생할 때 대상 볼륨을 활성화하는 데 도움이 되는 추가 설명서가 제공됩니다. 재해 발생 후 소스 볼륨을 다시 활성화하는 방법에 대해서도 자세히 알아볼 수 있습니다.

볼륨 재해 복구

+ 재해 발생 후 대상 볼륨을 빠르게 활성화한 다음 ONTAP에서 소스 볼륨을 다시 활성화하는 방법에 대해 설명합니다.

클러스터 피어 관계 및 **SVM** 피어 관계를 확인합니다

재해 복구를 위한 볼륨을 설정하기 전에 소스 및 타겟 클러스터가 피어링되어 피어 관계를 통해 서로 통신하고 있는지 확인해야 합니다.

절차를 참조하십시오

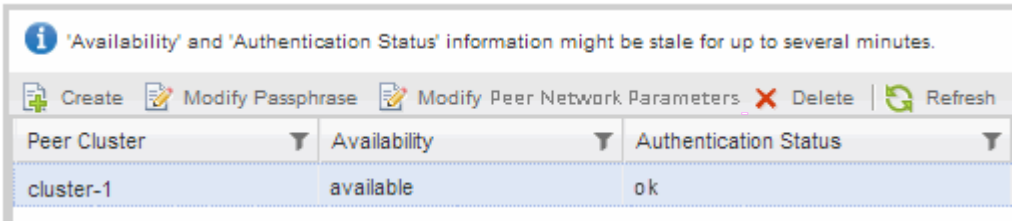
- ONTAP 9.3 이상을 실행 중인 경우 다음 단계를 수행하여 클러스터 피어 관계 및 SVM 피어 관계를 확인하십시오.
  a. 구성 * > * 클러스터 피어 * 를 클릭합니다.
  b. 피어링된 클러스터가 인증되었으며 사용 가능한지 확인합니다.

  c. 구성 * > * SVM 피어 * 를 클릭합니다.
  d. 대상 SVM이 소스 SVM으로 피어링되었는지 확인합니다.
- ONTAP 9.2 이하를 실행 중인 경우 다음 단계를 수행하여 클러스터 피어 관계 및 SVM 피어 관계를 확인하십시오.

a. 구성 * 탭을 클릭합니다.

b. 클러스터 세부 정보 * 창에서 * 클러스터 피어 * 를 클릭합니다.

c. 피어링된 클러스터가 인증되고 사용 가능한지 확인합니다.



d. SVM * 탭을 클릭하고 소스 SVM을 선택합니다.

e. 피어 스토리지 가상 시스템 * 영역에서 대상 SVM이 소스 SVM으로 피어링되었는지 확인합니다.

이 영역에서 피어링된 SVM이 없는 경우 SnapMirror 관계를 생성할 때 SVM 피어 관계를 생성할 수 있습니다.

SnapMirror 관계 만들기(ONTAP 9.2 이하)

SnapMirror 관계 생성**(ONTAP 9.3**부터**)**

한 클러스터의 소스 볼륨과 재해 복구를 위한 데이터 복제를 위한 피어링된 클러스터의 타겟 볼륨 간에 SnapMirror 관계를 생성해야 합니다.

시작하기 전에

- 대상 Aggregate에 사용 가능한 공간이 있어야 합니다.
- 사용자 액세스, 인증 및 클라이언트 액세스를 위한 환경 요구 사항을 충족하도록 두 클러스터를 적절히 구성 및 설정해야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 미러 관계를 생성할 볼륨을 선택한 다음 * 작업 * > * 보호 * 를 클릭합니다.
3. 관계 유형 * 섹션의 * 관계 유형 * 드롭다운 목록에서 * 미러 * 를 선택합니다.
4. Volumes:Protect Volumes * 페이지에서 다음 정보를 제공합니다.
   a. 관계 유형으로 * 미러 * 를 선택합니다.
   b. 타겟 클러스터, 타겟 SVM 및 타겟 볼륨 이름의 접미사를 선택합니다.

      피어링된 SVM과 허용된 SVM만 타겟 SVM 아래에 나열됩니다.

   c. 을 클릭합니다 .
   d. 고급 옵션 * 대화 상자에서 MirorAllSnapshots이 보호 정책으로 설정되어 있는지 확인합니다.

      SnapMirror 관계에 사용할 수 있는 또 다른 기본 보호 정책은 '기본값'과 'MirorLatest'입니다.

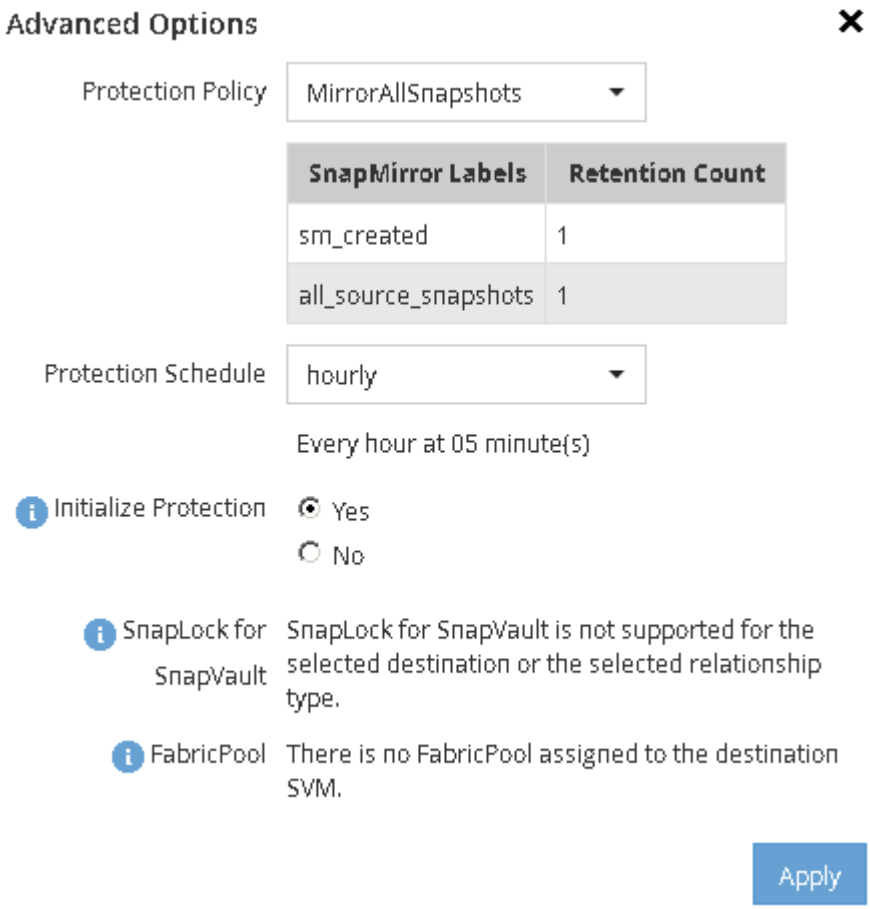
e. 보호 스케줄을 선택합니다.

   기본적으로 시간별 일정이 선택됩니다.

f. SnapVault 관계를 초기화하기 위해 * 예 * 가 선택되어 있는지 확인합니다.

   모든 데이터 보호 관계는 기본적으로 초기화됩니다. SnapMirror 관계를 초기화하면 타겟 볼륨에 소스 볼륨 보호를 시작할 기준이 있습니다.

g. 변경 사항을 저장하려면 * 적용 * 을 클릭합니다.



5. Save * 를 클릭하여 SnapMirror 관계를 생성합니다.
6. SnapMirror 관계의 관계 상태가 '미러됨' 상태인지 확인합니다.

   a. Volumes * 창으로 이동한 다음 SnapMirror 관계를 생성한 볼륨이 있는 볼륨을 선택합니다.

   b. 볼륨을 두 번 클릭하여 볼륨 세부 정보를 확인한 다음 * 보호 * 를 클릭하여 볼륨의 데이터 보호 상태를 확인합니다.

다음 단계

씬 프로비저닝, 중복제거, 압축, 자동 확장 등과 같은 소스 볼륨의 설정을 기록해야 합니다. 이 정보를 사용하여 SnapMirror 관계를 끊을 때 대상 볼륨 설정을 확인할 수 있습니다.

SnapMirror 관계 생성**(ONTAP 9.2** 이하**)**

한 클러스터의 소스 볼륨과 재해 복구를 위한 데이터 복제를 위한 피어링된 클러스터의 타겟 볼륨 간에 SnapMirror 관계를 생성해야 합니다.

시작하기 전에

- 대상 클러스터에 대한 클러스터 관리자 사용자 이름과 암호가 있어야 합니다.
- 대상 Aggregate에 사용 가능한 공간이 있어야 합니다.
- 사용자 액세스, 인증 및 클라이언트 액세스를 위한 환경 요구 사항을 충족하도록 두 클러스터를 적절히 구성 및 설정해야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 스토리지 * > * SVM * 을 클릭합니다.
2. SVM을 선택한 다음 * SVM 설정 * 을 클릭합니다.
3. 볼륨 * 탭을 클릭합니다.
4. 미러 관계를 생성할 볼륨을 선택한 다음 * 보호 * 를 클릭합니다.

   보호 관계 생성 창이 표시됩니다.

5. 관계 유형 * 섹션의 * 관계 유형 * 드롭다운 목록에서 * 미러 * 를 선택합니다.
6. 대상 볼륨 * 섹션에서 피어링된 클러스터를 선택합니다.
7. 타겟 볼륨에 SVM을 지정합니다.

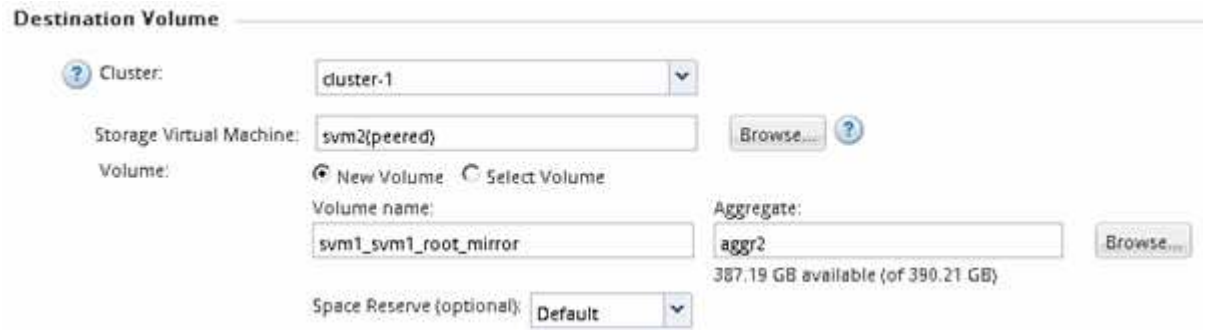
SVM이**...**	그러면**...**
자세히 들여다보았습니다	목록에서 피어링된 SVM을 선택합니다.
피어링되지 않았습니다	a. SVM을 선택합니다. b. 인증 * 을 클릭합니다. c. 피어링된 클러스터의 클러스터 관리자 자격 증명을 입력하고 * Create * 를 클릭합니다.

8. 새 대상 볼륨 생성:

   a. 새 볼륨 * 옵션을 선택합니다.

   b. 기본 볼륨 이름을 사용하거나 새 볼륨 이름을 지정합니다.

c. 대상 애그리게이트를 선택합니다.

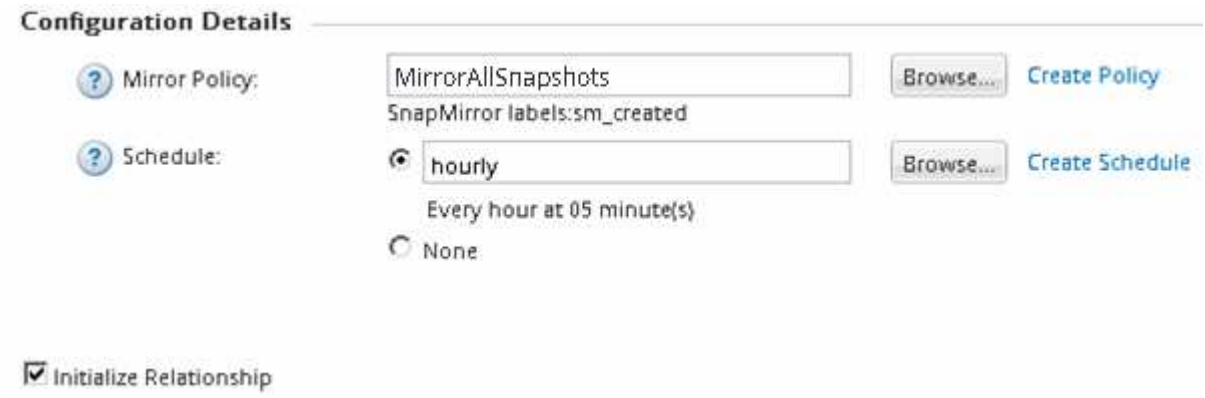


9. 구성 세부 정보 * 섹션에서 미러 정책으로 * MirrorAllSnapshots * 를 선택합니다.

   SnapMirror 관계에 사용할 수 있는 또 다른 기본 미러 정책은 '기본값'과 'MirorLatest'입니다.

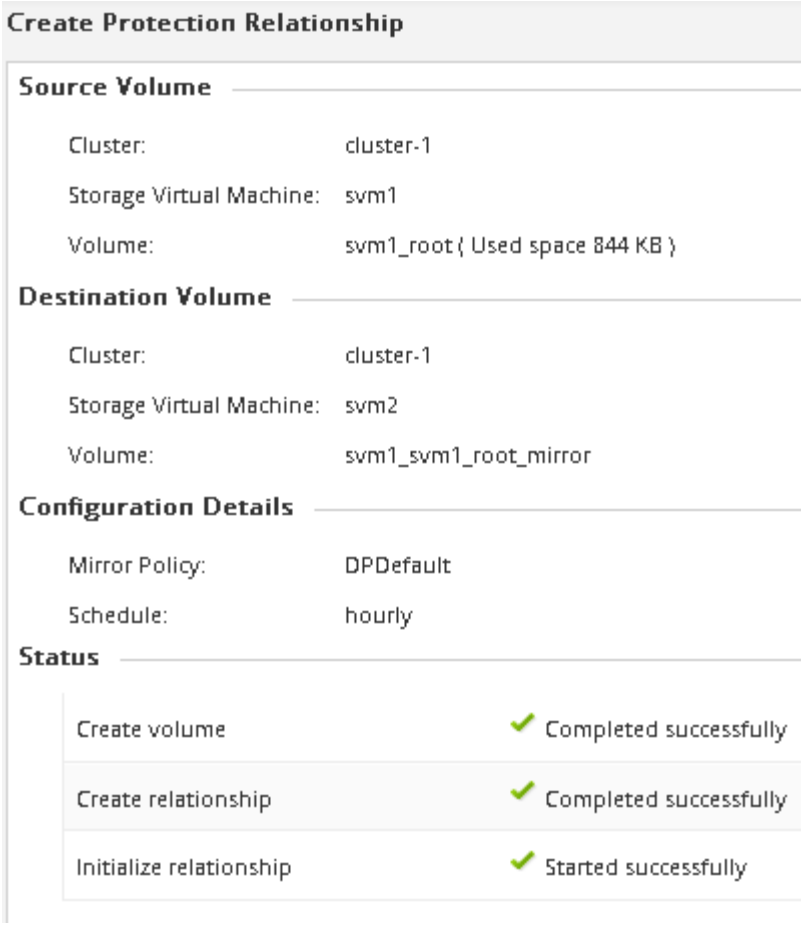
10. 스케줄 목록에서 보호 스케줄을 선택합니다.
11. 관계 초기화 * 확인란이 선택되어 있는지 확인한 다음 * 작성 * 을 클릭합니다.

    SnapMirror 관계를 초기화하면 타겟 볼륨에 소스 볼륨 보호를 시작할 기준이 있습니다.



소스 볼륨에서 타겟 볼륨으로 데이터의 기본 전송을 시작하여 관계가 초기화됩니다.

초기화 작업에는 약간의 시간이 걸릴 수 있습니다. 상태 섹션에는 각 작업의 상태가 표시됩니다.



12. SnapMirror 관계의 관계 상태를 확인합니다.
    a. 볼륨 * 목록에서 SnapMirror 관계를 생성한 볼륨을 선택한 다음 * 데이터 보호 * 를 클릭합니다.
    b. 데이터 보호 * 탭에서 생성한 SnapMirror 관계가 나열되고 관계 상태가 '스냅샷 복사'인지 확인합니다.

다음 단계

씬 프로비저닝, 중복제거, 압축, 자동 확장 등과 같은 소스 볼륨의 설정을 기록해야 합니다. 이 정보를 사용하여 SnapMirror 관계를 끊을 때 대상 볼륨 설정을 확인할 수 있습니다.

데이터 액세스를 위해 대상 **SVM**을 설정합니다

LIF, CIFS 공유, NAS 환경을 위한 엑스포트 정책, 타겟 볼륨을 포함하는 SVM의 SAN 환경을 위한 LIF 및 이니시에이터 그룹과 같은 필수 구성을 설정하여 타겟 볼륨을 활성화할 때 데이터 액세스 중단을 최소화할 수 있습니다.

이 작업에 대해

대상 볼륨이 포함된 SVM에 대해 * destination * 클러스터에서 이 작업을 수행해야 합니다.

절차를 참조하십시오

- NAS 환경:
  a. NAS LIF 생성:
  b. 소스에서 사용된 것과 동일한 공유 이름으로 CIFS 공유를 생성합니다.
  c. 적절한 NFS 엑스포트 정책을 생성합니다.
  d. 적절한 할당량 규칙을 생성합니다.
- SAN 환경:
  a. SAN LIF를 생성합니다.
  b. * 선택 사항: * 포트 세트 구성.
  c. 이니시에이터 그룹을 구성합니다.
  d. FC의 경우 FC 스위치를 조닝(Zoning)하여 SAN 클라이언트가 LIF에 액세스할 수 있도록 합니다.

다음 단계

소스 볼륨을 포함하는 SVM에서 변경이 있을 경우 타겟 볼륨이 포함된 SVM에서 수동으로 변경 사항을 복제해야 합니다.

- 관련 정보 *

"ONTAP 9 문서 센터"

SnapMirror 데이터 전송 상태를 모니터링합니다

SnapMirror 관계 상태를 주기적으로 모니터링하여 SnapMirror 데이터 전송이 지정된 일정에 따라 발생하는지 확인합니다.

이 작업에 대해

대상 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 선택한 다음 * Details * Bottom 탭에서 상태를 확인합니다.

   세부 정보 탭에는 SnapMirror 관계의 상태가 표시되고 전송 오류 및 지연 시간이 표시됩니다.

   - 건강은? 필드에 예 가 표시되어야 합니다.

     대부분의 SnapMirror 데이터 전송 장애 발생 시 이 필드에 "아니요"가 표시됩니다. 그러나 일부 실패 사례에서는 필드가 계속 Yes(예)로 표시됩니다. 데이터 전송 오류가 발생하지 않았는지 확인하려면 세부 정보 섹션에서 전송 오류를 확인해야 합니다.

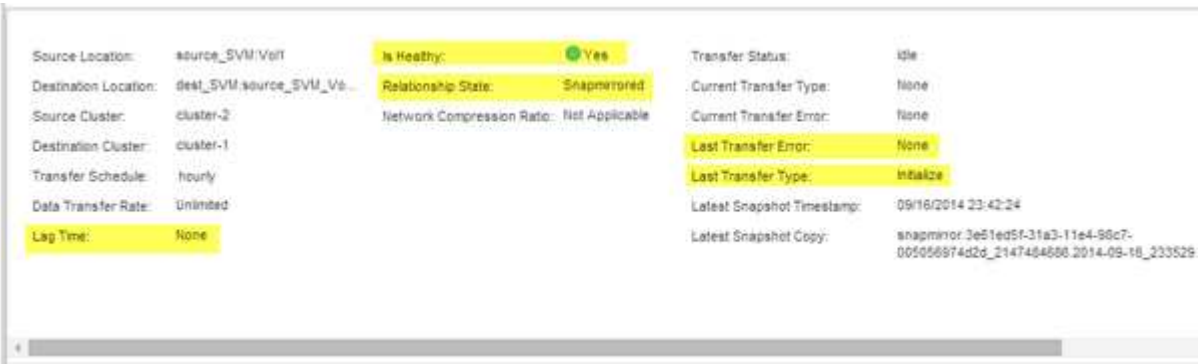
   - 관계 상태 필드에 '스냅샷 미러링'이 표시되어야 합니다.

- 지연 시간은 전송 일정 간격보다 길지 않아야 합니다.

  예를 들어, 전송 일정이 매시간 시간인 경우 지연 시간은 1시간 이상이어야 합니다.

  SnapMirror 관계의 모든 문제를 해결해야 합니다.

  "NetApp 기술 보고서 4015: ONTAP 9.1, 9.2에 대한 SnapMirror 구성 및 모범 사례"



SnapVault를 사용한 볼륨 백업

SnapVault를 사용한 볼륨 백업 개요

서로 다른 클러스터에 있는 볼륨 간에 SnapVault 백업 관계를 빠르게 구성할 수 있습니다. SnapVault 백업에는 데이터가 손상되거나 손실될 때 데이터를 복구하는 데 사용할 수 있는 대상 볼륨에 있는 읽기 전용 백업 복사본 세트가 포함되어 있습니다.

다음과 같은 방법으로 볼륨에 대한 SnapVault 백업 관계를 생성하려는 경우 이 절차를 사용합니다.

- ONTAP 9를 실행하는 클러스터로 작업하고 있습니다.
- 클러스터 관리자입니다.
- 클러스터 피어 관계 및 SVM 피어 관계를 구성했습니다.

  "클러스터 및 SVM 피어링 구성"

- 클러스터의 모든 노드가 동일한 버전의 ONTAP 9로 업그레이드된 후 SnapMirror 또는 SnapVault 라이센스를 활성화해야 합니다.
- 사용자 지정 정책을 생성하지 않고 기본 보호 정책 및 스케줄을 사용하려는 경우
- 단일 파일 또는 LUN 복원을 위한 데이터를 백업하지 않습니다.
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- 많은 개념적 배경을 읽고 싶지 않습니다.
- ONTAP 명령줄 인터페이스 또는 자동화된 스크립팅 도구가 아니라 System Manager를 사용하려고 합니다.
- ONTAP 9.7 이상을 위한 ONTAP 시스템 관리자 UI가 아니라 ONTAP 9.7 이전 릴리즈용 System Manager 클래식 인터페이스를 사용하려는 경우

이러한 가정이 현재 상황에 맞지 않거나 보다 개념적인 배경 정보를 원하는 경우 다음 리소스를 참조하십시오.

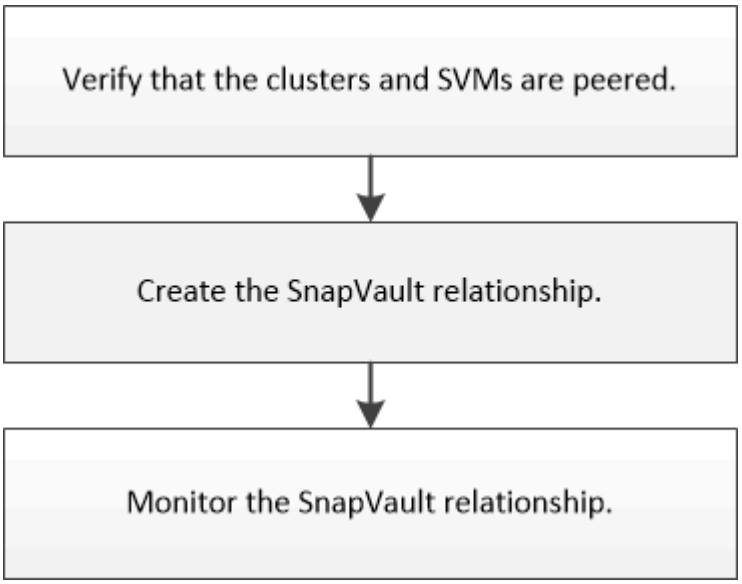
"NetApp 기술 보고서 4183: SnapVault 모범 사례"

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"미러와 볼트를 구성합니다"
ONTAP 명령줄 인터페이스입니다	"복제 관계를 생성합니다"

SnapVault 백업 구성 워크플로우

SnapVault 백업 관계 구성에는 클러스터 피어 관계 확인, 소스 볼륨과 타겟 볼륨 간의 SnapVault 관계 생성, SnapVault 관계 모니터링이 포함됩니다.



백업 데이터를 테스트하거나 소스 볼륨이 손실된 경우 대상 볼륨에서 데이터를 복원하는 데 도움이 되는 추가 설명서가 제공됩니다.

- SnapVault를 사용한 볼륨 복원 관리

  ONTAP의 SnapVault 백업에서 볼륨을 빠르게 복원하는 방법에 대해 설명합니다

클러스터 피어 관계 및 **SVM** 피어 관계를 확인합니다

SnapVault 기술을 사용하여 데이터 보호를 위한 볼륨을 설정하기 전에 소스 클러스터와 타겟 클러스터가 피어 관계를 통해 서로 피어링되어 상호 통신하고 있는지 확인해야 합니다. 또한 소스 SVM과 타겟 SVM이 피어링되어 피어 관계를 통해 서로 통신하고 있는지 확인해야 합니다.

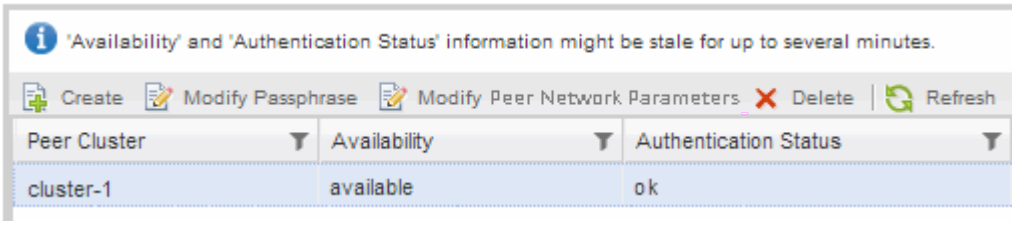
이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

절차를 참조하십시오

- ONTAP 9.3 이상을 실행 중인 경우 다음 단계를 수행하여 클러스터 피어 관계 및 SVM 피어 관계를 확인하십시오.
  a. 구성 * > * 클러스터 피어 * 를 클릭합니다.
  b. 피어링된 클러스터가 인증되었으며 사용 가능한지 확인합니다.

  c. 구성 * > * SVM 피어 * 를 클릭합니다.
  d. 대상 SVM이 소스 SVM으로 피어링되었는지 확인합니다.
- ONTAP 9.2 이하를 실행 중인 경우 다음 단계를 수행하여 클러스터 피어 관계 및 SVM 피어 관계를 확인하십시오.
  a. 구성 * 탭을 클릭합니다.
  b. 클러스터 세부 정보 * 창에서 * 클러스터 피어 * 를 클릭합니다.
  c. 피어링된 클러스터가 인증되고 사용 가능한지 확인합니다.



  d. SVM * 탭을 클릭하고 소스 SVM을 선택합니다.
  e. 피어 스토리지 가상 시스템 * 영역에서 대상 SVM이 소스 SVM으로 피어링되었는지 확인합니다.

     이 영역에서 피어링된 SVM이 없는 경우 SnapVault 관계를 생성할 때 SVM 피어 관계를 생성할 수 있습니다.

SnapVault 관계 만들기(ONTAP 9.2 이하)

SnapVault 관계 생성**(ONTAP 9.3**부터 시작**)**

피어링된 클러스터에서 소스 볼륨과 타겟 볼륨 간에 SnapVault 관계를 생성하여 SnapVault 백업을 생성해야 합니다.

시작하기 전에

- 대상 클러스터에 대한 클러스터 관리자 사용자 이름과 암호가 있어야 합니다.
- 대상 Aggregate에 사용 가능한 공간이 있어야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 스토리지 * > * 볼륨 * 을 클릭합니다.

2. 백업할 볼륨을 선택한 다음 * 작업 * > * 보호 * 를 클릭합니다.

   여러 소스 볼륨을 선택한 다음 단일 타겟 볼륨으로 SnapVault 관계를 생성할 수도 있습니다.

3. Volumes:Protect Volumes * 페이지에서 다음 정보를 제공합니다.

   a. 관계 유형 * 드롭다운 목록에서 * 볼트 * 를 선택합니다.
   b. 타겟 클러스터, 타겟 SVM 및 타겟 볼륨의 접미사를 선택합니다.

      피어링된 SVM과 허용된 SVM만 타겟 SVM 아래에 나열됩니다.

   대상 볼륨이 자동으로 생성됩니다. 대상 볼륨의 이름은 접미사가 추가된 소스 볼륨 이름입니다.

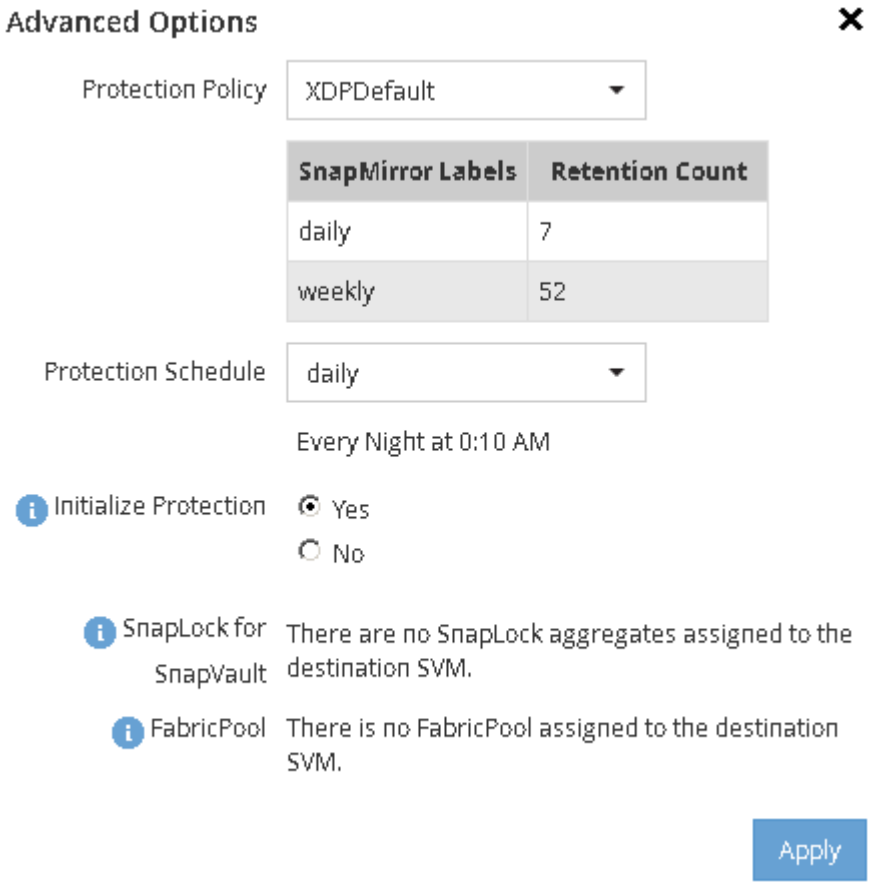
   a. 을 클릭합니다 .
   b. 고급 옵션 * 대화 상자에서 * 보호 정책 * 이 "XDPDefault"로 설정되어 있는지 확인합니다.
   c. 보호 일정 * 을 선택합니다.

      기본적으로 '일일' 일정이 선택됩니다.

   d. SnapVault 관계를 초기화하기 위해 * 예 * 가 선택되어 있는지 확인합니다.

      모든 데이터 보호 관계는 기본적으로 초기화됩니다.

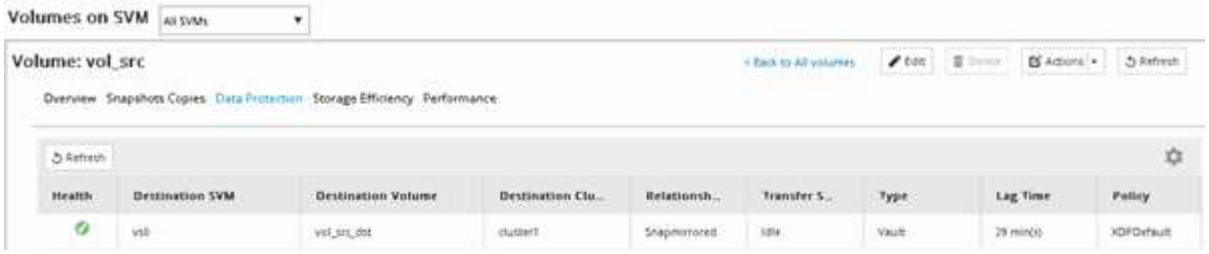
   e. 변경 사항을 저장하려면 * 적용 * 을 클릭합니다.



4. Volumes:Protect Volumes * 페이지에서 * Validate * 를 클릭하여 볼륨에 일치하는 SnapMirror 레이블이 있는지 확인합니다.
5. SnapVault 관계를 만들려면 * 저장 * 을 클릭합니다.
6. SnapVault 관계의 상태가 '스냅샷 미러링' 상태인지 확인합니다.

   a. Volumes * 창으로 이동한 다음 백업할 볼륨을 선택합니다.

   b. 볼륨을 확장하고 * 보호 * 를 클릭하여 볼륨의 데이터 보호 상태를 확인합니다.



SnapVault 관계 생성**(ONTAP 9.2** 이하**)**

피어링된 클러스터에서 소스 볼륨과 타겟 볼륨 간에 SnapVault 관계를 생성하여 SnapVault 백업을 생성해야 합니다.

시작하기 전에

- 대상 클러스터에 대한 클러스터 관리자 사용자 이름과 암호가 있어야 합니다.
- 대상 Aggregate에 사용 가능한 공간이 있어야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 스토리지 * > * SVM * 을 클릭합니다.
2. SVM을 선택한 다음 * SVM 설정 * 을 클릭합니다.
3. 볼륨 * 탭을 클릭합니다.
4. 백업할 볼륨을 선택한 다음 * 보호 * 를 클릭합니다.
5. [보호 관계 작성] * 대화 상자의 [관계 유형 *] 드롭다운 목록에서 * 볼트 * 를 선택합니다.
6. 대상 볼륨 * 섹션에서 피어링된 클러스터를 선택합니다.
7. 타겟 볼륨에 SVM을 지정합니다.

SVM이...	그러면...
자세히 들여다보았습니다	목록에서 피어링된 SVM을 선택합니다.

SVM이...	그러면...
피어링되지 않았습니다	a. SVM을 선택합니다. b. 인증 * 을 클릭합니다. c. 피어링된 클러스터의 클러스터 관리자 자격 증명을 입력하고 * Create * 를 클릭합니다.

8. 새 대상 볼륨 생성:

   a. 새 볼륨 * 옵션을 선택합니다.

   b. 기본 볼륨 이름을 사용하거나 새 볼륨 이름을 입력합니다.

   c. 대상 애그리게이트를 선택합니다.

   d. 중복 제거 사용 * 확인란이 선택되어 있는지 확인합니다.

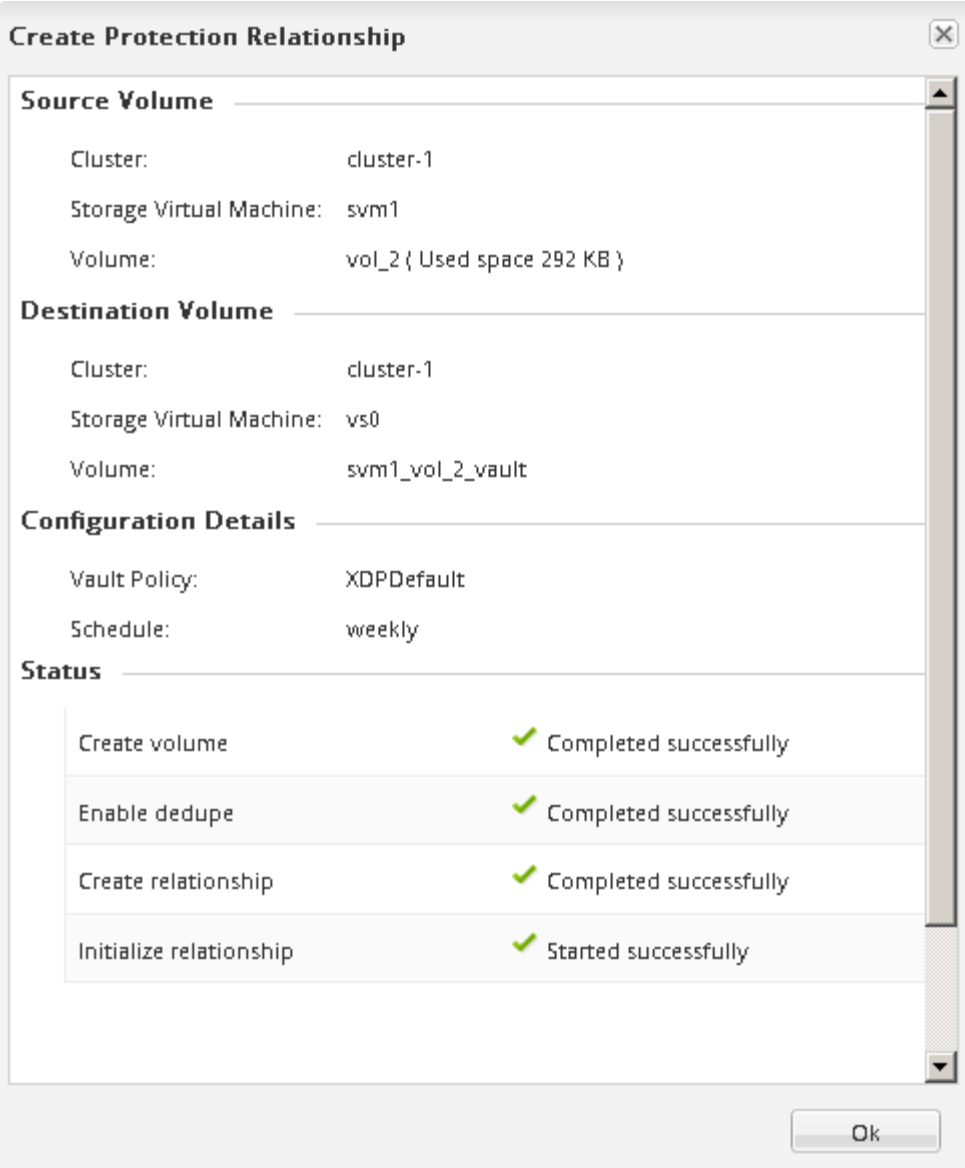
9. 구성 세부 정보 * 섹션에서 보호 정책으로 'XDPDefault'를 선택합니다.

10. 스케줄 목록에서 보호 스케줄을 선택합니다.

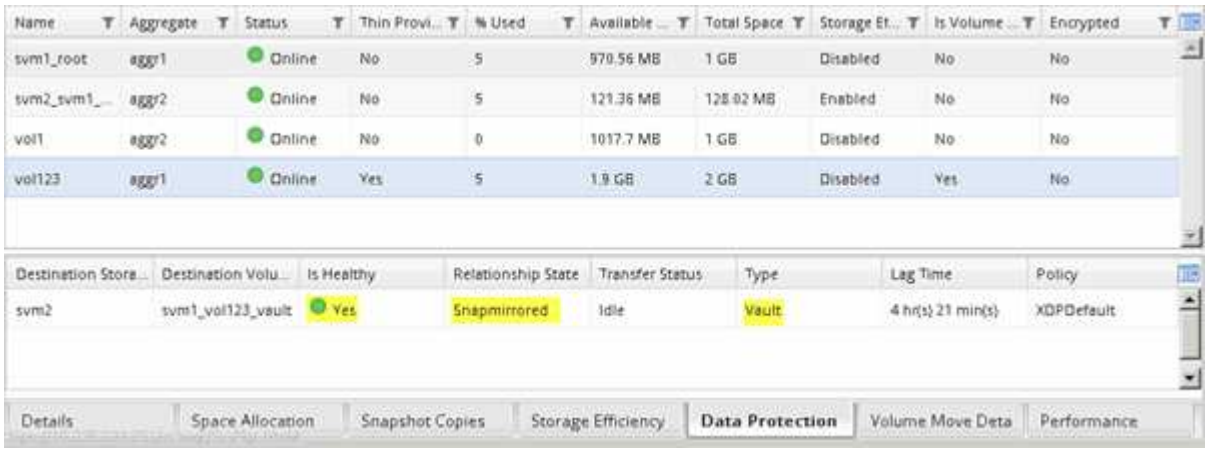
11. 기본 스냅샷 복사본을 전송하려면 * 관계 초기화 * 확인란이 선택되어 있는지 확인한 다음 * 생성 * 을 클릭합니다

마법사는 지정된 볼트 정책 및 스케줄과 관계를 작성합니다. 소스 볼륨에서 타겟 볼륨으로 데이터의 기본 전송을 시작하여 관계가 초기화됩니다.

상태 섹션에는 각 작업의 상태가 표시됩니다.



12. SnapVault 관계의 관계 상태가 '스냅샷 복사' 상태인지 확인합니다.
    a. 볼륨 목록에서 볼륨을 선택한 다음 * 데이터 보호 * 를 클릭합니다.
    b. Data Protection * Bottom 탭에서 생성한 SnapMirror 관계가 나열되고 관계 상태가 '스냅샷 미러링'이고 유형이 '볼트'인지 확인합니다.



SnapVault 관계를 모니터링합니다

SnapVault 관계의 상태를 주기적으로 모니터링하여 지정된 스케줄에 따라 데이터가 대상 볼륨에 백업되도록 해야 합니다.

이 작업에 대해

대상 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. 소스와 대상 볼륨 간의 SnapVault 관계를 선택한 다음 * Details * Bottom 탭에서 상태를 확인합니다.

   SnapVault 관계 상태, 전송 오류 및 지연 시간이 표시됩니다.

   - 건강은? 필드에 예 가 표시되어야 합니다.

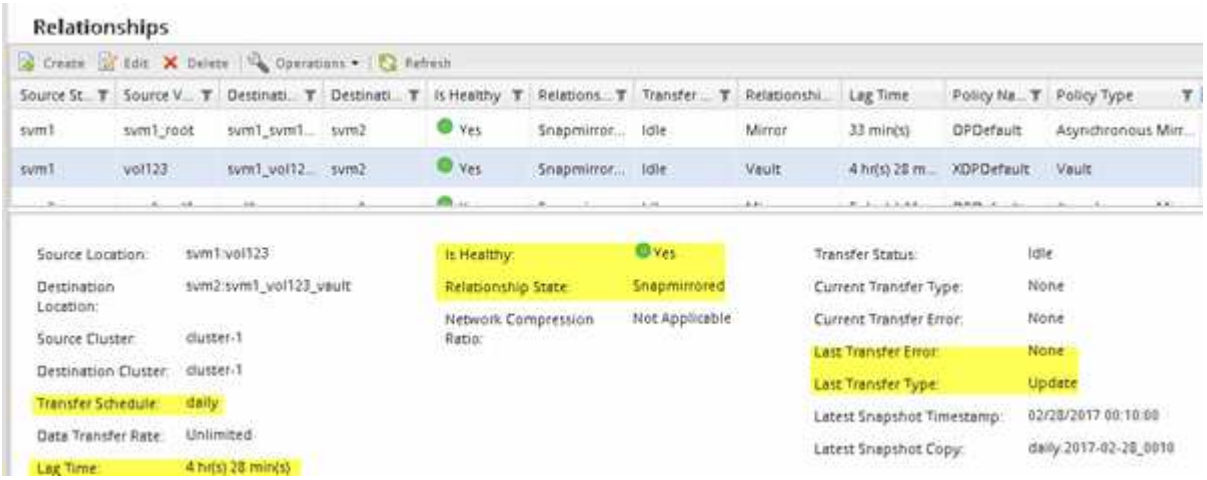
     대부분의 데이터 전송 실패 시 필드에 No가 표시됩니다. 그러나 일부 실패 사례에서는 필드가 계속 Yes(예)로 표시됩니다. 데이터 전송 오류가 발생하지 않았는지 확인하려면 세부 정보 섹션에서 전송 오류를 확인해야 합니다.

   - 관계 상태 필드에 '스냅샷 미러링'이 표시되어야 합니다.
   - 지연 시간은 전송 일정 간격보다 클 수 없습니다.

     예를 들어, 전송 스케줄이 매일 인 경우 지연 시간은 1일을 초과할 수 없습니다.

     SnapVault 관계의 모든 문제를 해결해야 합니다. SnapMirror 관계에 대한 문제 해결 절차도 SnapVault 관계에 적용됩니다.

     "NetApp 기술 보고서 4015: ONTAP 9.1, 9.2에 대한 SnapMirror 구성 및 모범 사례"



SnapVault를 사용한 볼륨 복원 관리

SnapVault를 사용한 볼륨 복원 개요

데이터 손실이 발생할 경우 ONTAP의 SnapVault 백업에서 볼륨을 빠르게 복원할 수 있습니다.

볼트 백업에서 다음과 같은 방법으로 복원하려는 경우 이 절차를 사용합니다.

- ONTAP 9를 실행하는 클러스터로 작업하고 있습니다.
- 클러스터 관리자입니다.
- 에 설명된 절차에 따라 볼트 관계를 구성했습니다 SnapVault를 사용한 볼륨 백업
- 단일 파일 또는 LUN 복원을 수행하지 않습니다.
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- 많은 개념적 배경을 읽고 싶지 않습니다.
- ONTAP 9.7 이상을 위한 ONTAP 시스템 관리자 UI가 아니라 ONTAP 9.7 이전 릴리즈용 System Manager 클래식 인터페이스를 사용하려는 경우

이러한 가정이 현재 상황에 맞지 않거나 보다 개념적인 배경 정보를 원하는 경우 다음 리소스를 참조하십시오.

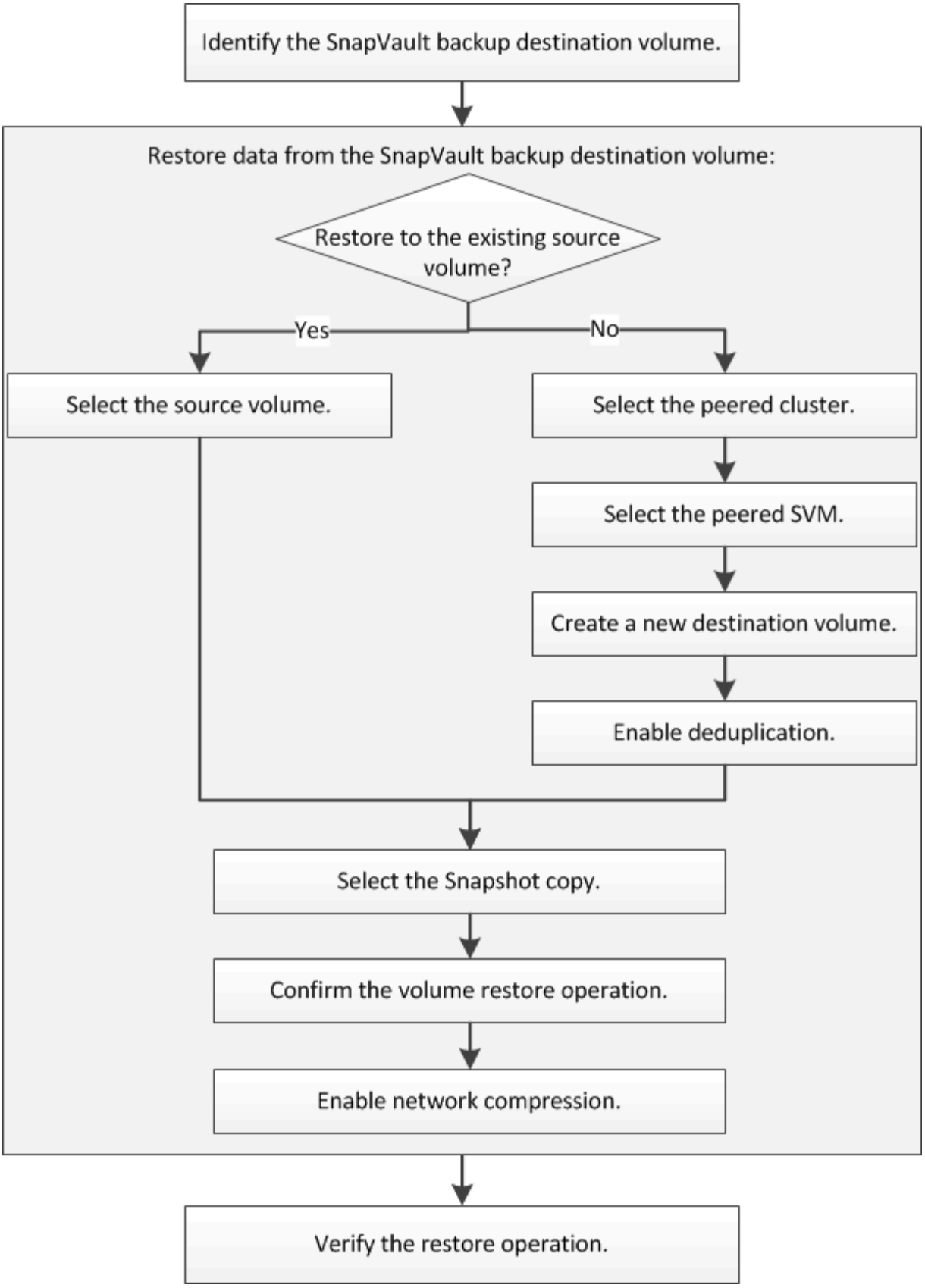
"NetApp 기술 보고서 4183: SnapVault 모범 사례"

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"이전 스냅샷 복사본에서 볼륨을 복원합니다"
ONTAP 명령줄 인터페이스입니다	"SnapMirror 대상에서 볼륨 내용을 복원합니다"

볼륨 복원 워크플로우

소스 볼륨을 사용할 수 없거나 데이터가 손상된 경우 SnapVault 백업에서 복원을 수행할 수 있습니다. SnapVault 백업에서 볼륨을 복원하려면 SnapVault 대상 볼륨을 선택하고 새 볼륨이나 기존 볼륨으로 복원하며 복원 작업을 확인해야 합니다.



SnapVault 백업 관계를 관리하고 다른 데이터 보호 방법을 사용하여 데이터 리소스의 가용성을 보호하는 데 도움이 되는 추가 정보가 제공됩니다.

- 볼륨 재해 복구 준비

재해 복구 준비 시 다른 ONTAP 클러스터에서 대상 볼륨을 빠르게 구성하는 방법에 대한 설명은 에 나와 있습니다.

- 볼륨 재해 복구

  재해 발생 후 다른 ONTAP 클러스터에서 대상 볼륨을 빠르게 활성화하는 방법과 복구 후 소스 볼륨을 다시 활성화하여 SnapMirror 관계를 원래 상태로 복원하는 방법에 대해 설명합니다.

SnapVault 백업 대상 볼륨을 식별합니다

소스 볼륨의 데이터가 손상되었거나 손실될 때 데이터를 복원할 SnapVault 백업 대상 볼륨을 식별해야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 웹 브라우저에 URL 'https://IP-address-of-cluster-management-LIF` 를 입력하고 클러스터 관리자 자격 증명을 사용하여 System Manager에 로그인합니다.
2. Volumes * 창으로 이동합니다.
3. SnapVault 관계에서 타겟 볼륨과 볼륨을 포함하는 SVM의 이름을 식별합니다.
   - ONTAP 9.3 이상: 볼륨을 두 번 클릭하여 세부 정보를 확인한 다음 * 보호 * 를 클릭합니다.
   - ONTAP 9.2 이하: 볼륨 창 아래쪽에 있는 * 데이터 보호 * 탭을 클릭합니다.

SnapVault 백업에서 데이터를 복원합니다

SnapVault 백업 대상 볼륨을 선택한 후에는 백업 데이터를 테스트하기 위해 새 볼륨에 복구 작업을 수행하거나 기존 볼륨에 복원 작업을 수행하여 손실되거나 손상된 데이터를 복원해야 합니다.

이 작업에 대해

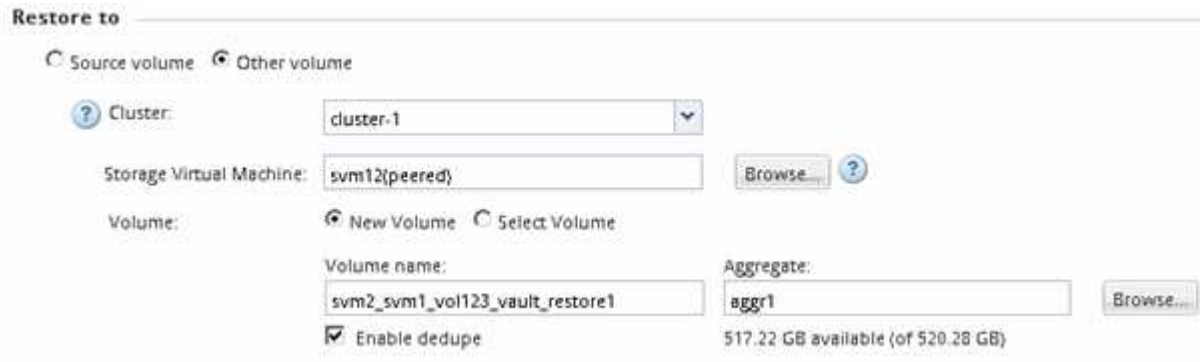
대상 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 실행 중인 System Manager 버전에 따라 다음 단계 중 하나를 수행하십시오.
   - ONTAP 9.4 이하: * 보호 * > * 관계 * 를 클릭합니다.
   - ONTAP 9.5부터 * 보호 * > * 볼륨 관계 * 를 클릭합니다.
2. SnapVault 백업 대상 볼륨이 포함된 SVM을 선택하고 * 운영 * > * 복원 * 을 클릭합니다.
3. Restore * 대화 상자에서 데이터를 원래 소스 볼륨 또는 새 볼륨으로 복원합니다.

복원하려는 대상...	그러면...
원래 소스 볼륨입니다	소스 볼륨 * 을 선택합니다.

복원하려는 대상...	그러면...
새 볼륨	a. 다른 볼륨 * 을 선택합니다. b. 피어링된 클러스터와 피어링된 SVM을 볼륨 선택 c. 목록에서 피어링된 SVM을 선택합니다. d. SVM을 피어링하지 않은 경우 SVM 피어 관계를 생성합니다. i. SVM을 선택합니다. ii. 인증 * 을 클릭합니다. iii. 피어링된 클러스터의 클러스터 관리자 자격 증명을 입력하고 * Create * 를 클릭합니다. e. 새 볼륨 * 을 선택합니다. f. 기본 이름을 'Destination_SVM_name_destination_volume_name_restore' 형식으로 표시하려면 새 이름을 지정하고 볼륨의 포함된 애그리게이트를 선택합니다. g. Enable dedupe * 확인란을 선택합니다.



4. 최신 스냅샷 복사본을 선택하거나 복원하려는 특정 스냅샷 복사본을 선택합니다.
5. OK를 선택하여 스냅샷 복사본에서 볼륨을 복원합니다 *.
6. 복원 작업 중에 전송되는 데이터를 압축하려면 * 네트워크 압축 사용 * 확인란을 선택합니다.
7. 복원 * 을 클릭합니다.

   복원 프로세스 중에 복원 중인 볼륨이 읽기 전용으로 변경됩니다. 복구 작업이 완료되면 임시 관계가 제거되고 복구된 볼륨이 읽기/쓰기로 변경됩니다.

8. 메시지 상자에서 * 확인 * 을 클릭합니다.

복구 작업을 확인합니다

SnapVault 백업 대상 볼륨에서 복구 작업을 수행한 후에는 소스 클러스터에서 복구 작업의 상태를 확인해야 합니다.

이 작업에 대해

소스 * 클러스터에서 이 작업을 수행해야 합니다.

단계

1. Volumes * 창으로 이동합니다.
2. 볼륨 목록에서 소스 볼륨을 선택하고 ONTAP 버전에 따라 다음 작업 중 하나를 수행합니다.
   - ONTAP 9.3부터: 소스 볼륨을 두 번 클릭하여 세부 정보를 확인한 다음, * 보호 * 를 클릭하여 SnapMirror 관계에서 타겟 볼륨과 볼륨이 포함된 SVM 이름을 확인합니다.
   - ONTAP 9.2 이하: * 데이터 보호 * 아래쪽 탭을 클릭하여 SnapMirror 관계의 타겟 볼륨과 볼륨이 들어 있는 SVM 이름을 식별하십시오. 유형 필드에 일시적으로 복원(Restore)이 표시됩니다. 복원 작업이 완료되면 이 필드에 Vault가 표시됩니다.

     SnapVault 관계의 모든 문제를 해결해야 합니다. SnapMirror 관계에 대한 문제 해결 절차도 SnapVault 관계에 적용됩니다.

"NetApp 기술 보고서 4015: ONTAP 9.1, 9.2에 대한 SnapMirror 구성 및 모범 사례"