



System Manager로 데이터 보호

ONTAP 9

NetApp
April 24, 2024

목차

System Manager로 데이터 보호	1
System Manager의 데이터 보호 개요	1
사용자 지정 데이터 보호 정책을 생성합니다	1
스냅샷 복사본을 구성합니다	2
스냅샷 복사본을 삭제하기 전에 반환 가능 공간을 계산하십시오	2
스냅샷 복사본 디렉토리에 대한 클라이언트 액세스를 사용하거나 사용하지 않도록 설정합니다	2
미러링 및 보관 준비	3
미러와 볼트를 구성합니다	4
보호 관계를 다시 동기화합니다	5
이전 스냅샷 복사본에서 볼륨을 복원합니다	5
Snapshot 복사본에서 복구	6
새 볼륨으로 복원합니다	6
보호 관계를 역재동기화합니다	6
SnapMirror 대상에 데이터를 제공합니다	7
스토리지 VM 재해 복구 구성	7
SVM DR 대상에서 데이터 제공	8
소스 스토리지 VM을 다시 활성화합니다	8
대상 스토리지 VM을 다시 동기화합니다	9
SnapMirror를 사용하여 데이터를 클라우드에 백업합니다	9
Cloud Backup을 사용하여 데이터를 백업합니다	11

System Manager로 데이터 보호

System Manager의 데이터 보호 개요

이 섹션에서는 ONTAP 9.7 이상 릴리즈의 System Manager에서 데이터 보호를 구성하고 관리하는 방법을 알아봅니다.

ONTAP 9.7 이하에서 System Manager를 사용하고 있는 경우 를 참조하십시오 ["ONTAP System Manager 클래식 설명서"](#)

스냅샷 복사본, 미러링, 볼트, 미러 및 소산 관계를 작성하고 관리하여 데이터를 보호합니다.

`_SnapMirror_` 는 지리적으로 원격 사이트의 운영 스토리지에서 보조 스토리지로 페일오버하도록 설계된 재해 복구 기술입니다. 그 이름이 시사하는 것처럼 SnapMirror는 운영 사이트에서 재해가 발생한 경우에도 데이터를 계속 제공할 수 있는 보조 스토리지에 작업 데이터의 복제본 또는 미러를 생성합니다.

`a_vault_` 는 표준 준수 및 기타 거버넌스 관련 용도로 D2D 스냅샷 복사 복제를 위해 설계되었습니다. 일반적으로 타겟에 현재 소스 볼륨에 있는 스냅샷 복사본만 포함되어 있는 SnapMirror 관계와는 대조적으로, 소산 대상에서는 훨씬 더 오랜 기간 동안 생성된 시점 Snapshot 복사본을 유지합니다.

ONTAP 9.10.1.1부터 S3 SnapMirror를 사용하여 S3 버킷 간에 데이터 보호 관계를 생성할 수 있습니다. 타겟 버킷은 로컬 또는 원격 ONTAP 시스템 또는 StorageGRID 및 AWS와 같은 비 ONTAP 시스템에 있을 수 있습니다. 자세한 내용은 을 참조하십시오 ["S3 SnapMirror 개요"](#).

사용자 지정 데이터 보호 정책을 생성합니다

기본 보호 정책이 요구사항에 적합하지 않은 경우 System Manager를 사용하여 사용자 지정 데이터 보호 정책을 생성할 수 있습니다. ONTAP 9.11.1부터 시스템 관리자를 사용하여 사용자 정의 미러 및 볼트 정책을 생성하고 레거시 정책을 표시하고 선택할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.

소스 클러스터와 대상 클러스터 모두에 사용자 지정 보호 정책을 생성합니다.

단계

1. 보호 > 로컬 정책 설정 * 을 클릭합니다.
2. 보호 정책 * 에서 을 클릭합니다 →.
3. Protection Policies * 창에서 를 클릭합니다 + Add .
4. 새 정책 이름을 입력하고 정책 범위를 선택합니다.
5. 정책 유형을 선택합니다. 볼트 전용 또는 미러 전용 정책을 추가하려면 * Asynchronous * 를 선택하고 * 기존 정책 유형 사용 * 을 클릭합니다.
6. 필수 필드에 내용을 입력합니다.
7. 저장 * 을 클릭합니다.
8. 다른 클러스터에서 이 단계를 반복합니다.

스냅샷 복사본을 구성합니다

스냅샷 복사본 정책을 생성하여 자동으로 생성되는 스냅샷 복사본의 최대 수와 생성 빈도를 지정할 수 있습니다. 이 정책은 스냅샷 복사본을 생성할 시기, 유지할 복사본 수 및 이름을 지정하는 방법을 지정합니다.

이 절차를 수행하면 로컬 클러스터에만 스냅샷 복사본 정책이 생성됩니다.

단계

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭합니다.
2. Snapshot Policies * 에서 를 클릭합니다 → 을 클릭한 다음 을 클릭합니다 + Add .
3. 정책 이름을 입력하고 정책 범위를 선택한 다음 * Schedules * 에서 를 클릭합니다 + Add 일정 세부 정보를 입력합니다.

스냅샷 복사본을 삭제하기 전에 반환 가능 공간을 계산하십시오

ONTAP 9.10.1부터 시스템 관리자를 사용하여 삭제할 스냅샷 복사본을 선택하고 반환 청구를 할 수 있는 공간을 먼저 계산할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 스냅샷 복사본을 삭제할 볼륨을 선택합니다.
3. Snapshot 복사본 * 을 클릭합니다.
4. 하나 이상의 스냅샷 복사본을 선택합니다.
5. 회수 가능 공간 계산 * 을 클릭합니다.

스냅샷 복사본 디렉토리에 대한 클라이언트 액세스를 사용하거나 사용하지 않도록 설정합니다


ONTAP 9.10.1부터 System Manager를 사용하여 클라이언트 시스템이 볼륨의 스냅샷 복사본 디렉토리에 액세스하도록 하거나 사용하지 않도록 설정할 수 있습니다. 액세스를 설정하면 스냅샷 복사본 디렉토리가 클라이언트에 표시되고 Windows 클라이언트가 드라이브를 스냅샷 복사본 디렉토리에 매핑하여 콘텐츠를 보고 액세스할 수 있습니다.

볼륨 설정을 편집하거나 볼륨의 공유 설정을 편집하여 볼륨의 스냅샷 복사본 디렉토리에 대한 액세스를 사용하거나 사용하지 않도록 설정할 수 있습니다.

볼륨을 편집하여 스냅샷 복사본 디렉토리에 대한 클라이언트 액세스를 사용하거나 사용하지 않도록 설정합니다

볼륨의 스냅샷 복사본 디렉토리는 기본적으로 클라이언트에서 액세스할 수 있습니다.


단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 표시하거나 숨길 스냅샷 복사본 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 클릭합니다  를 클릭하고 * 편집 * 을 선택합니다.
4. Snapshot 복사본(로컬) 설정 * 섹션에서 클라이언트에 스냅샷 복사본 디렉토리 표시 * 를 선택하거나 선택 취소합니다.
5. 저장 * 을 클릭합니다.

공유를 편집하여 스냅샷 복사본 디렉토리에 대한 클라이언트 액세스를 설정하거나 해제합니다

볼륨의 스냅샷 복사본 디렉토리는 기본적으로 클라이언트에서 액세스할 수 있습니다.

단계

1. 스토리지 > 공유 * 를 클릭합니다.
2. 표시하거나 숨길 스냅샷 복사본 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 클릭합니다  를 클릭하고 * 편집 * 을 선택합니다.
4. 공유 속성 * 섹션에서 * 클라이언트가 스냅샷 복사본 디렉토리에 액세스할 수 있도록 허용 * 을 선택하거나 선택 취소합니다.
5. 저장 * 을 클릭합니다.

미러링 및 보관 준비


데이터 백업 및 재해 복구를 위해 데이터를 원격 클러스터로 복제하여 보호할 수 있습니다.


몇 가지 기본 보호 정책을 사용할 수 있습니다. 사용자 지정 정책을 사용하려면 보호 정책을 만들어야 합니다.



단계

1. 로컬 클러스터에서 * 보호 > 개요 * 를 클릭합니다.
2. 클러스터 간 설정 * 을 확장합니다. 네트워크 인터페이스 추가 * 를 클릭하고 클러스터에 대한 인터클러스터 네트워크 인터페이스를 추가합니다.

원격 클러스터에서 이 단계를 반복합니다.
3. 원격 클러스터에서 * 보호 > 개요 * 를 클릭합니다. 을 클릭합니다  Cluster 피어 섹션에서 * Generate Passphrase * 를 클릭합니다.
4. 생성된 암호를 복사하여 로컬 클러스터에 붙여넣습니다.
5. 로컬 클러스터의 클러스터 피어에서 * 피어 클러스터 * 를 클릭하고 로컬 및 원격 클러스터를 피어로 지정합니다.

- 필요에 따라 스토리지 VM 피어에서 를 클릭합니다 : 그리고 스토리지 VM을 피어로 하기 위해 * 피어 스토리지 VM * 을 선택합니다.
 - 볼륨 보호 * 를 클릭하여 볼륨을 보호합니다. LUN을 보호하려면 * 스토리지 > LUN * 을 클릭하고 보호할 LUN을 선택한 다음 을 클릭합니다  Protect.
- 필요한 데이터 보호 유형에 따라 보호 정책을 선택합니다.
- 볼륨 및 LUN이 로컬 클러스터에서 제대로 보호되었는지 확인하려면 * 스토리지 > 볼륨 * 또는 * 스토리지 > LUN * 을 클릭하고 볼륨/LUN 보기를 확장합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 준비 개요"
ONTAP 명령줄 인터페이스입니다	"클러스터 피어 관계를 생성합니다"

미러와 볼트를 구성합니다

재해 발생 시 데이터를 보호하고 롤백할 수 있는 여러 개의 보관된 데이터 버전을 가질 수 있도록 볼륨의 미러 및 볼트를 작성합니다. ONTAP 9.11.1부터 시스템 관리자를 사용하여 미리 작성된 사용자 정의 미러 및 볼트 정책을 선택하고, 레거시 정책을 표시 및 선택하고, 볼륨 및 스토리지 VM을 보호할 때 보호 정책에 정의된 전송 일정을 재정의할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.




ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 사용하고 시스템 관리자를 사용하여 SnapMirror를 구성한 경우, ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리즈로 업그레이드할 계획이면 ONTAP 9.9.1.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용해야 합니다.

이 절차를 수행하면 원격 클러스터에 데이터 보호 정책이 생성됩니다. 소스 클러스터와 대상 클러스터는 데이터 교환을 위해 인터클러스터 네트워크 인터페이스를 사용합니다. 이 절차에서는 를 가정합니다 ["인터클러스터 네트워크 인터페이스가 만들어지고 볼륨이 포함된 클러스터가 피어링됩니다"](#) (페어링됨) 또한 피어 스토리지 VM을 사용하여 데이터를 보호할 수도 있지만, 스토리지 VM을 피어링되지 않고 사용 권한을 설정하면 보호 관계가 생성될 때 스토리지 VM이 자동으로 피어링됩니다.



단계

- 보호할 볼륨 또는 LUN을 선택합니다. * 스토리지 > 볼륨 * 또는 * 스토리지 > LUN * 을 클릭한 다음 원하는 볼륨 또는 LUN 이름을 클릭합니다.
- 을 클릭합니다  Protect.
- 대상 클러스터와 스토리지 VM을 선택합니다.
- 비동기식 정책이 기본적으로 선택됩니다. 동기식 정책을 선택하려면 * 추가 옵션 * 을 클릭합니다.

5. 보호 * 를 클릭합니다.
6. 선택한 볼륨 또는 LUN의 * SnapMirror(로컬 또는 원격) * 탭을 클릭하여 보호가 올바르게 설정되었는지 확인합니다.

관련 정보

- ["SnapMirror 파일오버 테스트 볼륨을 생성하고 삭제합니다"](#).

ONTAP에서 이 작업을 수행하는 다른 방법


에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SnapVault를 사용한 볼륨 백업 개요"
ONTAP 명령줄 인터페이스입니다	"복제 관계를 생성합니다"

보호 관계를 다시 동기화합니다

재해 발생 후 원래 소스 볼륨을 다시 사용할 수 있으면 대상 볼륨에서 데이터를 재동기화하고 보호 관계를 다시 설정할 수 있습니다.

이 절차는 원래 소스 볼륨의 데이터를 다시 제공하고 원래 보호 관계를 다시 시작할 수 있도록 비동기 관계에서 원래 소스 볼륨의 데이터를 대체합니다.

단계


1. 보호 > 관계 * 를 클릭한 다음 재동기화하려는 끊어진 관계를 클릭합니다.
2. 을 클릭합니다  그런 다음 * 재동기화 * 를 선택합니다.
3. 관계 * 에서 관계 상태를 확인하여 재동기화 진행률을 모니터링합니다. 재동기화가 완료되면 상태가 "미러링"으로 변경됩니다.

이전 스냅샷 복사본에서 볼륨을 복원합니다

볼륨의 데이터가 손실되거나 손상된 경우 이전 스냅샷 복사본에서 복원하여 데이터를 롤백할 수 있습니다.

이 절차는 소스 볼륨의 현재 데이터를 이전 스냅샷 복사본 버전의 데이터로 대체합니다. 대상 클러스터에서 이 작업을 수행해야 합니다.

단계

1. 보호 > 관계 * 를 클릭한 다음 소스 볼륨 이름을 클릭합니다.
2. 을 클릭합니다  그런 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 소스 볼륨은 기본적으로 선택됩니다. 소스 이외의 볼륨을 선택하려면 * 기타 볼륨 * 을 클릭합니다.
4. 대상 * 에서 복원하려는 스냅샷 복사본을 선택합니다.
5. 소스와 대상이 서로 다른 클러스터에 있는 경우 원격 클러스터에서 * 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	" SnapVault를 사용한 볼륨 복원 개요 "
ONTAP 명령줄 인터페이스입니다	" SnapMirror 대상에서 볼륨 내용을 복원합니다 "

Snapshot 복사본에서 복구

스냅샷 복사본에서 복원하여 볼륨을 이전 시점으로 복구할 수 있습니다.

이 절차는 스냅샷 복사본에서 볼륨을 복원합니다.

단계

1. Storage * 를 클릭하고 볼륨을 선택합니다.
2. Snapshot 복사본 * 에서 을 클릭합니다 : 복원하려는 스냅샷 복사본 옆에 있는 * 복원 * 을 선택합니다.

새 볼륨으로 복원합니다

ONTAP 9.8부터 시스템 관리자를 사용하여 대상 볼륨의 백업된 데이터를 원래 소스 이외의 볼륨으로 복원할 수 있습니다.

다른 볼륨으로 복원할 때 기존 볼륨을 선택하거나 새 볼륨을 만들 수 있습니다.

단계

1. 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 을 클릭합니다 : 를 클릭하고 * 복원 * 을 클릭합니다.
3. 소스 * 섹션에서 * 기타 볼륨 * 을 선택하고 클러스터 및 스토리지 VM을 선택합니다.
4. 기존 볼륨 * 또는 * 새 볼륨 생성 * 을 선택합니다.
5. 새 볼륨을 생성하는 경우 볼륨 이름을 입력합니다.
6. Destination * 섹션에서 복구할 스냅샷 복사본을 선택합니다.
7. 저장 * 을 클릭합니다.
8. 관계 * 에서 관계에 대한 * 전송 상태 * 를 보고 복원 진행률을 모니터링합니다.

보호 관계를 역재동기화합니다

ONTAP 9.8부터 System Manager를 사용하여 역방향 재동기화 작업을 수행하여 기존 보호 관계를 삭제하고 소스 볼륨과 대상 볼륨의 기능을 반대로 되돌릴 수 있습니다. 그런 다음, 소스를 복구 또는 교체하고 소스를 업데이트하고 시스템의 원래 구성을 다시 설정하는 동안 대상 볼륨을 사용하여 데이터를 제공합니다.



System Manager는 클러스터 내 관계와의 역방향 재동기화를 지원하지 않습니다. ONTAP CLI를 사용하여 클러스터 내 관계와 역방향 재동기화 작업을 수행할 수 있습니다.

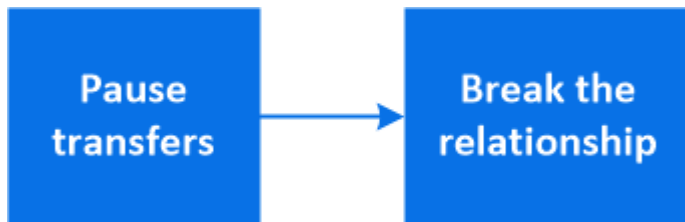
역방향 재동기화 작업을 수행할 때 공통 스냅샷 복사본의 데이터보다 최신 소스 볼륨의 데이터가 삭제됩니다.

단계

1. 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 을 클릭합니다 그리고 * 역방향 재동기화 * 를 클릭합니다.
3. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 역방향 재동기화 진행률을 모니터링합니다.

SnapMirror 대상에 데이터를 제공합니다

소스를 사용할 수 없게 될 때 미러 대상에서 데이터를 제공하려면 대상에 대한 예약된 전송을 중지한 다음 SnapMirror 관계를 끊어 대상을 쓰기 가능으로 만듭니다.



단계

1. 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭한 다음 원하는 볼륨 이름을 클릭합니다.
2. 을 클릭합니다 .
3. 예약된 전송 중지: * 일시 중지 * 를 클릭합니다.
4. 대상을 쓰기 가능 상태로 만듭니다. * Break * (중단 *)를 클릭합니다.
5. 기본 * 관계 * 페이지로 이동하여 관계 상태가 "연결 해제"로 표시되는지 확인합니다.

다음 단계:

비활성화된 소스 볼륨을 다시 사용할 수 있는 경우 관계를 다시 동기화하여 현재 데이터를 원래 소스 볼륨으로 복사해야 합니다. 이 프로세스는 원본 소스 볼륨의 데이터를 대체합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 개요"
ONTAP 명령줄 인터페이스입니다	"대상 볼륨을 활성화합니다"

스토리지 VM 재해 복구 구성

System Manager를 사용하면 스토리지 VM 재해 복구(스토리지 VM DR) 관계를 생성하여 한

스토리지 VM 구성을 다른 스토리지 VM 구성으로 복제할 수 있습니다. 운영 사이트에서 재해가 발생할 경우 대상 스토리지 VM을 빠르게 활성화할 수 있습니다.

대상에서 이 절차를 완료합니다. 예를 들어, 소스 스토리지 VM에 SMB가 구성되어 있는 경우 새 보호 정책을 생성해야 하는 경우 System Manager를 사용하여 정책을 생성하고 * 보호 정책 추가 * 창에서 * ID 보존 * 옵션을 선택해야 합니다.

자세한 내용은 을 참조하십시오 ["사용자 지정 데이터 보호 정책을 생성합니다"](#).



단계

1. 대상 클러스터에서 * 보호 > 관계 * 를 클릭합니다.
2. 관계 * 에서 보호 를 클릭하고 * 스토리지 VM(DR) * 를 선택합니다.
3. 보호 정책을 선택합니다. 맞춤형 보호 정책을 생성한 경우 해당 정책을 선택한 다음 복제할 소스 클러스터와 스토리지 VM을 선택합니다. 새 스토리지 VM 이름을 입력하여 새 대상 스토리지 VM을 생성할 수도 있습니다.
4. 저장 * 을 클릭합니다.

SVM DR 대상에서 데이터 제공

ONTAP 9.8부터 System Manager를 사용하여 재해 발생 후 대상 스토리지 VM을 활성화할 수 있습니다. 대상 스토리지 VM을 활성화하면 SVM 대상 볼륨을 쓸 수 있고 데이터를 클라이언트에 제공할 수 있습니다.

단계

1. 소스 클러스터에 액세스할 수 있는 경우 SVM이 중지되었는지 확인합니다. * 스토리지 > 스토리지 VM * 으로 이동하고 SVM을 위한 * 상태 * 열을 확인합니다.
2. 소스 SVM 상태가 "실행 중"인 경우 중지하고 선택하십시오  를 선택하고 * Stop * 을 선택합니다.
3. 대상 클러스터에서 원하는 보호 관계를 찾습니다. * 보호 > 관계 * 로 이동합니다.
4. 을 클릭합니다  및 * Activate Destination Storage VM * 을 선택합니다.

소스 스토리지 VM을 다시 활성화합니다

ONTAP 9.8부터는 시스템 관리자를 사용하여 재해 발생 후 소스 스토리지 VM을 다시 활성화할 수 있습니다. 소스 스토리지 VM을 다시 활성화하면 대상 스토리지 VM이 중지되고 소스에서 대상으로 복제가 다시 설정됩니다.


이 작업에 대해

소스 스토리지 VM을 다시 활성화하면 System Manager가 백그라운드에서 다음 작업을 수행합니다.

- SnapMirror 재동기화를 사용하여 원래 대상에서 원래 소스로 역방향 SVM DR 관계를 생성합니다
- 대상 SVM을 중지합니다
- SnapMirror 관계를 업데이트합니다
- SnapMirror 관계를 설정합니다
- 원래 SVM을 다시 시작합니다

- 원본 소스의 SnapMirror 재동기화를 원래 타겟으로 다시 실행합니다
- SnapMirror 관계를 정리합니다

단계

1. 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 을 클릭합니다  를 클릭하고 * 소스 스토리지 VM 다시 활성화 * 를 클릭합니다.
3. Relationships * 에서 보호 관계에 대한 * Transfer Status * 를 보고 소스 재활성화 진행률을 모니터링합니다.


대상 스토리지 VM을 다시 동기화합니다

ONTAP 9.8부터는 System Manager를 사용하여 소스 스토리지 VM의 데이터 및 구성 세부 정보를 손상된 보호 관계에 있는 대상 스토리지 VM으로 재동기화하고 관계를 다시 설정할 수 있습니다.

ONTAP 9.11.1에는 재해 복구 연습을 수행할 때 전체 데이터 웨어하우스 재구축을 우회하는 옵션이 도입되어 생산 단계로 빠르게 돌아갈 수 있습니다.

원래 관계의 대상에서만 재동기화 작업을 수행합니다. 재동기화를 수행하면 소스 스토리지 VM의 데이터보다 최신 대상 스토리지 VM의 데이터가 삭제됩니다.

단계

1. 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 선택적으로 * 빠른 재동기화 수행 * 을 선택하여 재해 복구 리허설 중에 전체 데이터 웨어하우스 재구축을 우회합니다.
3. 을 클릭합니다  다시 동기화 * 를 클릭합니다.
4. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 재동기화 진행률을 모니터링합니다.

SnapMirror를 사용하여 데이터를 클라우드에 백업합니다

ONTAP 9.9.1부터 System Manager를 사용하여 데이터를 클라우드로 백업하고 클라우드 스토리지에서 다른 볼륨으로 데이터를 복원할 수 있습니다. StorageGRID 또는 ONTAP S3를 클라우드 오브젝트 저장소로 사용할 수 있습니다.

SnapMirror 클라우드 기능을 사용하기 전에 NetApp Support 사이트에서 SnapMirror 클라우드 API 라이선스 키를 요청해야 합니다. "[SnapMirror Cloud API 라이선스 키 요청](#)". 지침에 따라 비즈니스 기회에 대한 간단한 설명을 제공하고 제공된 이메일 주소로 이메일을 보내 API 키를 요청해야 합니다. API 키를 얻는 방법에 대한 추가 지침이 포함된 이메일 응답을 24시간 이내에 받아야 합니다.

클라우드 오브젝트 저장소를 추가합니다

SnapMirror 클라우드 백업을 구성하기 전에 StorageGRID 또는 ONTAP S3 클라우드 오브젝트 저장소를 추가해야 합니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.

2. 을 클릭합니다 **+** Add.

기본 정책을 사용하여 백업합니다

기본 클라우드 보호 정책인 DailyBackup을 사용하여 기존 볼륨에 대한 SnapMirror Cloud 백업을 빠르게 구성할 수 있습니다.

단계

1. 보호 > 개요 * 를 클릭하고 * Cloud에 볼륨 백업 * 을 선택합니다.
2. 클라우드로 처음 백업하는 경우 표시된 라이선스 필드에 SnapMirror Cloud API 라이선스 키를 입력합니다.
3. 인증 및 계속 * 을 클릭합니다.
4. 소스 볼륨을 선택합니다.
5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

사용자 지정 클라우드 백업 정책을 생성합니다

SnapMirror 클라우드 백업에 기본 DailyBackup 클라우드 정책을 사용하지 않으려면 고유한 정책을 생성할 수 있습니다.

단계

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭하고 * 보호 정책 * 을 선택합니다.
2. 추가 * 를 클릭하고 새 정책 세부 정보를 입력합니다.
3. Policy Type * 섹션에서 * Back to Cloud * 를 선택하여 클라우드 정책을 생성하고 있음을 나타냅니다.
4. 저장 * 을 클릭합니다.

볼륨 * 페이지에서 백업을 생성합니다

System Manager * Volumes * 페이지에서 여러 볼륨에 대한 클라우드 백업을 한 번에 선택 및 생성하려는 경우 또는 사용자 지정 보호 정책을 사용하려는 경우에 사용할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 클라우드에 백업할 볼륨을 선택하고 * 보호 * 를 클릭합니다.
3. 볼륨 보호 * 창에서 * 추가 옵션 * 을 클릭합니다.
4. 정책을 선택합니다.


기본 정책, DailyBackup 또는 직접 생성한 사용자 지정 클라우드 정책을 선택할 수 있습니다.

5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

클라우드에서 복원

System Manager를 사용하여 클라우드 스토리지에서 소스 클러스터의 다른 볼륨으로 백업된 데이터를 복원할 수 있습니다.


단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. Back Up to Cloud * 탭을 선택합니다.
3. 을 클릭합니다  복원할 소스 볼륨 옆의 * 복원 * 을 선택합니다.
4. 소스 * 에서 스토리지 VM을 선택한 다음 데이터를 복원할 볼륨의 이름을 입력합니다.
5. 대상 * 에서 복원하려는 스냅샷 복사본을 선택합니다.
6. 저장 * 을 클릭합니다.

SnapMirror 클라우드 관계를 삭제합니다

System Manager를 사용하여 클라우드 관계를 삭제할 수 있습니다.


단계

1. 스토리지 > 볼륨 * 을 클릭하고 삭제할 볼륨을 선택합니다.
2. 을 클릭합니다  소스 볼륨 옆에 있는 * Delete * 를 선택합니다.
3. 클라우드 오브젝트 저장소 끝점을 삭제하려면 * 클라우드 오브젝트 저장소 끝점 삭제(선택 사항) * 를 선택합니다.
4. 삭제 * 를 클릭합니다.

클라우드 오브젝트 저장소를 제거합니다

클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부가 아닌 경우 System Manager를 사용하여 클라우드 오브젝트 저장소를 제거할 수 있습니다. 클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부인 경우 삭제할 수 없습니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.
2. 삭제할 오브젝트 저장소를 선택하고 을 클릭합니다  를 선택하고 * 삭제 * 를 선택합니다.

Cloud Backup을 사용하여 데이터를 백업합니다

ONTAP 9.9.1부터 Cloud Backup을 사용하여 System Manager를 사용하여 클라우드의 데이터를 백업할 수 있습니다.



Cloud Backup은 FlexVol 읽기-쓰기 볼륨 및 데이터 보호(DP) 볼륨을 지원합니다. FlexGroup 볼륨 및 SnapLock 볼륨은 지원되지 않습니다.

시작하기 전에

BlueXP에서 계정을 설정하려면 다음 절차를 수행해야 합니다. 서비스 계정의 경우 "계정 관리자" 역할을 생성해야 합니다. (다른 서비스 계정 역할에는 System Manager와의 연결을 설정하는 데 필요한 권한이 없습니다.)

1. "BlueXP에서 계정을 만듭니다".
2. "BlueXP에서 커넥터를 만듭니다" 공급한 클라우드 공급업체는 다음과 같습니다.
 - Microsoft Azure를 참조하십시오
 - AWS(Amazon Web Services)
 - Google Cloud Platform(GCP)
 - StorageGRID(ONTAP 9.10.1)



ONTAP 9.10.1부터 StorageGRID를 클라우드 백업 공급자로 선택할 수 있지만 BlueXP가 사내에 구축된 경우에만 가능합니다. BlueXP 커넥터는 사내에 설치해야 하며 BlueXP SaaS(Software-as-a-Service) 애플리케이션을 통해 사용할 수 있습니다.

3. "BlueXP에서 Cloud Backup Service를 구독합니다" (적절한 라이선스 필요).
4. "BlueXP를 사용하여 액세스 키와 비밀 키를 생성합니다".

클러스터를 BlueXP에 등록합니다

BlueXP 또는 System Manager를 사용하여 클러스터를 BlueXP에 등록할 수 있습니다.

단계

1. System Manager에서 * 보호 개요 * 로 이동합니다.
2. Cloud Backup Service * 에서 다음 세부 정보를 제공합니다.
 - 클라이언트 ID입니다
 - 클라이언트 암호 키입니다
3. Register and Continue * 를 선택합니다.

클라우드 백업 활성화

클러스터를 BlueXP에 등록한 후에는 클라우드 백업을 활성화하고 클라우드에 대한 첫 번째 백업을 시작해야 합니다.

단계

1. 시스템 관리자에서 * 보호 > 개요 * 를 클릭한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 클라이언트 ID * 및 * 클라이언트 암호 * 를 입력합니다.



ONTAP 9.10.1부터 * 클라우드 사용 비용에 대해 자세히 알아보기 * 를 클릭하여 클라우드 사용 비용에 대해 알아볼 수 있습니다.

3. 연결 및 Cloud Backup Service 사용 * 을 클릭합니다.
4. 선택한 공급자에 따라 * Cloud Backup Service * 활성화 페이지에서 다음 세부 정보를 제공합니다.

이 클라우드 공급자의 경우...

다음 데이터를 입력하십시오...

Azure를 지원합니다	<ul style="list-style-type: none"> • Azure 구독 ID입니다 • 지역 • 리소스 그룹 이름(기존 또는 신규)
설치하고	<ul style="list-style-type: none"> • AWS 계정 ID입니다 • 액세스 키 • 비밀 키 • 지역
Google Cloud Project(GCP)	<ul style="list-style-type: none"> • Google Cloud 프로젝트 이름 • Google Cloud Access 키 • Google Cloud 비밀 키 • 지역
StorageGRID(ONTAP 9.10.1 이상, BlueXP 사내 배포 전용)	<ul style="list-style-type: none"> • 서버 • SG 액세스 키 • SG 비밀 키

5. 보호 정책 * 선택:

- * 기존 정책 *: 기존 정책을 선택합니다.
- * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.



ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.



Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

- 볼륨이 아카이빙된 후 경과한 일 수입니다.
- 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정합니다.
- AWS의 경우 아카이브 스토리지 클래스를 선택합니다.

6. 백업할 볼륨을 선택합니다.

7. 저장 * 을 선택합니다.

Cloud Backup에 사용되는 보호 정책을 편집합니다

Cloud Backup에 사용되는 보호 정책을 변경할 수 있습니다.

단계

1. 시스템 관리자에서 * 보호 > 개요 * 를 클릭한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 을 클릭합니다 ;, * 편집 * 을 차례로 클릭합니다.
3. 보호 정책 * 선택:
 - * 기존 정책 *: 기존 정책을 선택합니다.
 - * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.



ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.



Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

- 볼륨이 아카이빙된 후 경과한 일 수입니다.
- 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정합니다.
- AWS의 경우 아카이브 스토리지 클래스를 선택합니다.

4. 저장 * 을 선택합니다.

클라우드에서 새 볼륨 또는 LUN 보호

새 볼륨 또는 LUN을 생성할 때 볼륨 또는 LUN에 대해 클라우드에 백업할 수 있도록 SnapMirror 보호 관계를 설정할 수 있습니다.

시작하기 전에

- SnapMirror 라이선스가 있어야 합니다.
- 인터클러스터 LIF를 구성해야 합니다.
- NTP를 구성해야 합니다.
- 클러스터가 ONTAP 9.9.1을 실행 중이어야 합니다.

이 작업에 대해

다음과 같은 클러스터 구성에서는 클라우드에서 새 볼륨 또는 LUN을 보호할 수 없습니다.

- 클러스터가 MetroCluster 환경에 있을 수 없습니다.
- SVM-DR은 지원되지 않습니다.
- FlexGroups는 Cloud Backup을 사용하여 백업할 수 없습니다.

단계

1. 볼륨 또는 LUN을 프로비저닝할 때 System Manager의 * 보호 * 페이지에서 * SnapMirror 사용(로컬 또는 원격) * 확인란을 선택합니다.
2. Cloud Backup 정책 유형을 선택합니다.
3. 클라우드 백업이 활성화되지 않은 경우 * Cloud Backup Service * 활성화 를 선택합니다.

클라우드의 기존 볼륨 또는 LUN 보호

기존 볼륨 및 LUN에 대해 SnapMirror 보호 관계를 설정할 수 있습니다.

단계

1. 기존 볼륨 또는 LUN을 선택하고 * 보호 * 를 클릭합니다.
2. 볼륨 보호 * 페이지에서 보호 정책에 대해 * Cloud Backup Service * 를 사용하여 백업 * 을 지정합니다.
3. 보호 * 를 클릭합니다.
4. 보호 * 페이지에서 * SnapMirror 활성화(로컬 또는 원격) * 확인란을 선택합니다.
5. Cloud Backup Service 사용 * 을 선택합니다.

백업 파일에서 데이터를 복원합니다

BlueXP 인터페이스를 사용하는 경우에만 데이터 복원, 관계 업데이트, 관계 삭제 등의 백업 관리 작업을 수행할 수 있습니다. 을 참조하십시오 ["백업 파일에서 데이터를 복원합니다"](#) 를 참조하십시오.

저작권 정보

Copyright © 2024 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.