



보호 관계 생성, 모니터링 및 문제 해결 Active IQ Unified Manager 9.7

NetApp
April 17, 2024

목차

보호 관계 생성, 모니터링 및 문제 해결	1
SnapMirror 보호 유형입니다	1
Unified Manager에서 보호 관계 설정	2
보호 관계 페일오버 및 페일백 수행	8
보호 작업 실패 해결	12
지연 문제 해결	16

보호 관계 생성, 모니터링 및 문제 해결

Unified Manager를 사용하면 보호 관계를 생성하고, 관리 대상 클러스터에 저장된 데이터의 미리 보호 및 백업 소산 보호를 모니터링 및 해결하고, 데이터를 덮어쓰거나 손실된 경우 데이터를 복원할 수 있습니다.

SnapMirror 보호 유형입니다

데이터 스토리지 토폴로지 구축에 따라 Unified Manager를 사용하여 다양한 유형의 SnapMirror 보호 관계를 구성할 수 있습니다. SnapMirror 보호의 모든 변형 기능은 페일오버 재해 복구 보호를 제공하지만 성능, 버전 유연성 및 다중 백업 복사본 보호에 있어 다른 기능을 제공합니다.

기존의 SnapMirror 비동기식 보호 관계

기존의 SnapMirror 비동기식 보호 기능은 소스 볼륨과 타겟 볼륨 간의 블록 복제 미리 보호 기능을 제공합니다.

기존 SnapMirror 관계에서는 미리 작업이 블록 복제를 기반으로 하므로 미리 작업이 대체 SnapMirror 관계보다 더 빠르게 실행됩니다. 그러나 기존 SnapMirror 보호에서는 동일한 주요 릴리즈(예: 버전 8.x에서 8.x 또는 9.x에서 9.x)내의 소스 볼륨과 동일한 부 버전 이상의 ONTAP 소프트웨어에서 타겟 볼륨을 실행해야 합니다.

버전에 상관없이 유연하게 복제할 수 있는 SnapMirror 비동기식 보호

버전에 상관없이 유연하게 복제할 수 있는 SnapMirror 비동기식 보호 기능은 소스 볼륨과 타겟 볼륨 간에 논리적 복제 미리 보호 기능을 제공합니다. 이는 서로 다른 버전의 ONTAP 8.3.1, 8.3.1에서 9.1, 9.2.2 에서 9.2 등)로 실행 중인 볼륨에서도 마찬가지입니다.

버전에 상관없이 유연하게 복제 가능한 SnapMirror 관계에서는 미러링 작업이 기존 SnapMirror 관계에서와 같이 빠르게 실행되지 않습니다.

느린 실행 속도 때문에 버전에 상관없이 유연하게 복제 보호를 지원하는 SnapMirror는 다음 중 하나를 구현하는 데 적합하지 않습니다.

- 소스 객체에는 보호할 파일이 1,000만 개 이상 있습니다.
- 보호 데이터에 대한 복구 지점 목표는 2시간 이하입니다. 즉, 대상에는 항상 소스의 데이터보다 2시간 이상 오래된 미러링된 복구 가능한 데이터가 포함되어 있어야 합니다.

나열된 상황 중 하나에서 기본 SnapMirror 보호의 신속한 블록 복제 기반 실행이 필요합니다.

버전에 상관없이 유연하게 복제 및 백업 옵션을 사용하는 SnapMirror 비동기 보호

버전에 상관없이 유연하게 복제 및 백업 옵션을 사용하는 SnapMirror 비동기 보호 기능은 소스 볼륨과 타겟 볼륨 간의 미러링 보호 기능과 미러링된 데이터의 여러 복사본을 대상에 저장하는 기능을 제공합니다.

스토리지 관리자는 소스에서 타겟으로 미러링되는 스냅샷 복사본을 지정할 수 있으며, 복사본이 소스에서 삭제되더라도 해당 복사본을 대상에서 보존할 기간을 지정할 수도 있습니다.

버전에 상관없이 유연한 복제 및 백업 옵션과 SnapMirror 관계를 사용하면 기존 SnapMirror 관계에서와 같이 미러링 작업이 신속하게 실행되지 않습니다.

SnapMirror 유니파이드 복제(미러링 및 소산)

SnapMirror 통합 복제를 사용하면 동일한 대상 볼륨에 재해 복구 및 아카이빙을 구성할 수 있습니다. SnapMirror와 마찬가지로 통합 데이터 보호는 처음 호출할 때 기본 전송을 수행합니다. 기본 통합 데이터 보호 정책 ""MirrorAndVault""에 따른 기본 전송은 소스 볼륨의 스냅샷 복사본을 만든 다음, 해당 복사본과 데이터 블록이 대상 볼륨에 참조되도록 전송합니다. SnapVault와 마찬가지로, 통합 데이터 보호에도 이전 Snapshot 복사본이 기본 안에 포함되지 않습니다.

SnapMirror Synchronous 보호 및 엄격한 동기화

"사전" 동기화로 SnapMirror Synchronous를 활용하면 1차 볼륨과 2차 볼륨이 항상 서로 진정한 복제본으로 유지됩니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 실패가 발생하면 운영 볼륨에 대한 클라이언트 입출력이 중단됩니다.

SnapMirror Synchronous 보호 - 정기적인 동기화

"리플러" 동기화를 통한 SnapMirror Synchronous 보호에서는 1차 볼륨과 2차 볼륨이 항상 서로 진정한 복사본일 필요가 없으며, 따라서 1차 볼륨의 가용성이 보장됩니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 실패가 발생하면 운영 볼륨과 보조 볼륨이 동기화되지 않고 클라이언트 입출력이 운영 볼륨으로 계속됩니다.



상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 동기 보호 관계를 모니터링할 때는 복원 단추와 관계 작업 단추를 사용할 수 없습니다.

Unified Manager에서 보호 관계 설정

Unified Manager 및 OnCommand Workflow Automation를 사용하여 데이터를 보호하기 위해 SnapMirror 및 SnapVault 관계를 설정하기 위해 수행해야 하는 몇 가지 단계가 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 2개의 클러스터 또는 2개의 SVM(스토리지 가상 머신) 간에 피어 관계를 설정해야 합니다.
- OnCommand Workflow Automation을 Unified Manager와 통합해야 함:
 - ["OnCommand Workflow Automation를 설정합니다"](#)
 - [Workflow Automation에서 Unified Manager 데이터 소스 캐싱 검증](#)

단계

1. 만들려는 보호 관계 유형에 따라 다음 중 하나를 수행합니다.
 - [SnapMirror 보호 관계를 생성합니다.](#)
 - ["SnapVault 보호 관계를 생성합니다."](#)
2. 관계에 대한 정책을 만들려면 만드는 관계 유형에 따라 다음 중 하나를 실행합니다.
 - [SnapVault 정책을 생성합니다.](#)
 - [SnapMirror 정책을 생성합니다.](#)

3. SnapMirror 또는 SnapVault 일정을 생성합니다.

Workflow Automation과 Unified Manager 간 연결 구성

WFA(OnCommand Workflow Automation)와 Unified Manager 간에 보안 연결을 구성할 수 있습니다. Workflow Automation에 연결하면 SnapMirror 및 SnapVault 구성 워크플로우와 같은 보호 기능을 사용할 수 있으며 SnapMirror 관계를 관리하는 데 필요한 명령을 사용할 수 있습니다.

시작하기 전에

- Workflow Automation의 설치 버전은 5.1 이상이어야 합니다.



WFA 5.1에는 "'Clustered Data ONTAP를 관리하기 위한 WFA 팩'이 포함되어 있으므로 NetApp Storage Automation Store에서 이 팩을 다운로드하여 이전에 필요한 WFA 서버에 별도로 설치할 필요가 없습니다. ["ONTAP 관리를 위한 WFA 팩"](#)

- WFA 및 Unified Manager 연결을 지원하려면 Unified Manager에서 생성한 데이터베이스 사용자의 이름이 있어야 합니다.

이 데이터베이스 사용자에게 통합 스키마 사용자 역할이 할당되어야 합니다.

- Workflow Automation에서 관리자 역할 또는 설계자 역할을 할당해야 합니다.
- Workflow Automation 설정을 사용하려면 호스트 주소, 포트 번호 443, 사용자 이름 및 암호가 있어야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * Workflow Automation * 을 클릭합니다.
2. Workflow Automation * 페이지의 * 데이터베이스 사용자 * 영역에서 이름을 선택하고 Unified Manager 및 Workflow Automation 연결을 지원하기 위해 생성한 데이터베이스 사용자의 암호를 입력합니다.
3. 페이지의 * Workflow Automation Credentials * 영역에서 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 Workflow Automation 설정의 사용자 이름 및 암호를 입력합니다.

Unified Manager 서버 포트(포트 443)를 사용해야 합니다.

4. 저장 * 을 클릭합니다.
5. 자체 서명된 인증서를 사용하는 경우 * 예 * 를 클릭하여 보안 인증서를 승인합니다.

Workflow Automation 페이지가 표시됩니다.

6. 웹 UI를 다시 로드하고 Workflow Automation 기능을 추가하려면 * 예 * 를 클릭합니다.
 - 관련 정보 *

["NetApp 설명서: OnCommand Workflow Automation\(최신 릴리즈\)"](#)

Workflow Automation에서 Unified Manager 데이터 소스 캐싱 검증

Workflow Automation에서 데이터 소스 획득이 성공적인지 확인하여 Unified Manager 데이터 소스 캐싱이 제대로 작동하는지 확인할 수 있습니다. Workflow Automation을 Unified Manager와 통합하면 통합 후 Workflow Automation 기능을 사용할 수 있는지 확인할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 Workflow Automation에서 관리자 역할 또는 설계자 역할이 할당되어야 합니다.

단계

1. Workflow Automation UI에서 * Execution * > * Data Sources * 를 선택합니다.
2. Unified Manager 데이터 소스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 * Acquire Now * 를 선택합니다.
3. 취득이 오류 없이 성공하는지 확인합니다.

Workflow Automation을 Unified Manager와 성공적으로 통합하려면 구입 오류를 해결해야 합니다.

OnCommand Workflow Automation를 재설치하거나 업그레이드하면 어떻게 됩니까

OnCommand Workflow Automation를 재설치하거나 업그레이드하기 전에 OnCommand Workflow Automation과 Unified Manager 간의 연결을 먼저 제거하고 현재 실행 중이거나 예약된 모든 OnCommand Workflow Automation 작업이 중지되었는지 확인해야 합니다.

또한 OnCommand Workflow Automation에서 Unified Manager를 수동으로 삭제해야 합니다.

OnCommand Workflow Automation를 재설치하거나 업그레이드한 후에는 Unified Manager와의 연결을 다시 설정해야 합니다.

Unified Manager에서 OnCommand Workflow Automation 설정을 제거하는 중입니다

Workflow Automation을 더 이상 사용하지 않으려는 경우 Unified Manager에서 OnCommand Workflow Automation 설정을 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창의 왼쪽 설정 메뉴에서 * 일반 * > * Workflow Automation * 을 클릭합니다.
2. Workflow Automation * 페이지에서 * 설정 제거 * 를 클릭합니다.

볼륨/상태 세부 정보 페이지에서 SnapMirror 보호 관계 생성

볼륨/상태 세부 정보 페이지를 사용하여 보호 목적으로 데이터 복제를 사용하도록 SnapMirror

관계를 만들 수 있습니다. SnapMirror 복제를 사용하면 소스의 데이터 손실 발생 시 대상 볼륨에서 데이터를 복원할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

이 작업에 대해

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우)

성능에 영향을 주지 않고 최대 10개의 보호 작업을 동시에 수행할 수 있습니다. 11 ~ 30개의 작업을 동시에 실행할 경우 성능에 약간의 영향을 줄 수 있습니다. 30개 이상의 작업을 동시에 실행하는 것은 권장되지 않습니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 보호할 볼륨의 이름을 토폴로지 뷰에서 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다.

보호 구성 대화 상자가 표시됩니다.

3. SnapMirror * 탭을 보고 대상 정보를 구성하려면 * SnapMirror * 를 클릭합니다.
4. 필요에 따라 * 고급 * 을 클릭하여 공간 보장을 설정한 다음 * 적용 * 을 클릭합니다.
5. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
6. 적용 * 을 클릭합니다.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

작업의 작업 및 세부 정보가 작업 세부 정보 페이지에 표시됩니다.

8. Job * details 페이지에서 * Refresh * 를 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업 완료 시기를 결정합니다.
9. 작업 작업이 완료되면 브라우저에서 * Back * 을 클릭하여 * Volume/Health * 세부 정보 페이지로 돌아갑니다.

새 관계가 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

결과

구성 중에 지정한 대상 SVM에 따라, 고급 설정에서 지정한 옵션에 따라 SnapMirror 관계가 달라질 수 있습니다.

- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP에서 실행되는 타겟 SVM을 지정한 경우 블록 복제 기반

SnapMirror 관계가 기본 결과입니다.

- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP(버전 8.3 이상)에서 실행되는 타겟 SVM을 지정했지만 고급 설정에서 버전에 상관없이 유연한 복제를 사용하도록 설정한 경우, 버전에 상관없이 유연한 복제를 사용하는 SnapMirror 관계가 됩니다.
- 이전 버전의 ONTAP 8.3에서 실행되는 대상 SVM이나 이전 버전의 소스 볼륨보다 더 높은 버전을 사용하여 유연한 복제를 지원하는 경우에는 버전에 상관없이 유연한 복제를 사용하는 SnapMirror 관계가 자동으로 이루어집니다.

볼륨/상태 세부 정보 페이지에서 **SnapVault** 보호 관계 생성

볼륨/상태 세부 정보 페이지를 사용하여 SnapVault 관계를 생성하면 볼륨에서 데이터 백업을 보호할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 Workflow Automation을 설정해야 합니다.

이 작업에 대해

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우)

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 보호할 토폴로지 뷰의 볼륨을 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * Protect * > * SnapVault * 를 선택합니다.

보호 구성 대화 상자가 시작됩니다.

3. SnapVault * 를 클릭하여 * SnapVault * 탭을 보고 보조 리소스 정보를 구성합니다.
4. 고급 * 을 클릭하여 필요에 따라 중복제거, 압축, 자동 확장, 공간 보장을 설정하고 * 적용 * 을 클릭합니다.
5. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
6. 적용 * 을 클릭합니다.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

작업 세부 정보 페이지가 표시됩니다.

8. 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인하려면 * 새로 고침 * 을 클릭합니다.

작업 작업이 완료되면 볼륨/상태 세부 정보 페이지 토폴로지 뷰에 새 관계가 표시됩니다.

전송 효율성을 극대화하기 위한 **SnapVault** 정책 생성

새 SnapVault 정책을 생성하여 SnapVault 전송의 우선 순위를 설정할 수 있습니다. 보호 관계에서 정책을 사용하여 운영 스토리지에서 2차 스토리지로 전송 효율성을 극대화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료해야 합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapVault * 탭에서 * 관계 설정 * 영역의 * 정책 * 만들기 * 링크를 클릭합니다.

SnapVault(측정) 탭이 표시됩니다.

2. Policy Name * 필드에 정책을 지정할 이름을 입력합니다.
3. 전송 우선순위 * 필드에서 정책에 할당할 전송 우선순위를 선택합니다.
4. Comment * (주석 *) 필드에 정책에 대한 설명을 입력합니다.
5. Replication Label * 영역에서 필요에 따라 복제 레이블을 추가하거나 편집합니다.
6. Create * 를 클릭합니다.

새 정책이 정책 생성 드롭다운 목록에 표시됩니다.

전송 효율성을 최대화할 수 있도록 **SnapMirror** 정책 생성

SnapMirror 정책을 생성하여 보호 관계에 대한 SnapMirror 전송 우선순위를 지정할 수 있습니다. SnapMirror 정책을 사용하면 우선 순위를 지정하여 소스에서 대상으로 전송 효율성을 극대화할 수 있으므로 우선순위가 낮은 전송이 일반 우선 순위 전송 후에 실행되도록 예약할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 이 작업에서는 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료한 것으로 가정합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapMirror * 탭에서 * 관계 설정 * 영역의 * 정책 생성 * 링크를 클릭합니다.

SnapMirror 정책 생성 대화 상자가 표시됩니다.

2. Policy Name * 필드에 정책을 지정할 이름을 입력합니다.
3. Transfer Priority * 필드에서 정책에 할당할 전송 우선 순위를 선택합니다.
4. Comment * (주석 *) 필드에 정책에 대한 선택적 설명을 입력합니다.
5. Create * 를 클릭합니다.

새 정책이 SnapMirror 정책 드롭다운 목록에 표시됩니다.

SnapMirror 및 SnapVault 일정 생성

기본 또는 고급 SnapMirror 및 SnapVault 일정을 생성하여 데이터 변경 빈도에 따라 소스 또는 기본 볼륨에서 자동 데이터 보호 전송을 가능하게 할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료해야 합니다.
- 이 작업을 수행하려면 Workflow Automation을 설정해야 합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapMirror * 탭 또는 * SnapVault * 탭에서 * 관계 설정 * 영역에서 * 일정 생성 * 링크를 클릭합니다.

Create Schedule 대화상자가 표시됩니다.

2. [일정 이름] * 필드에 일정에 부여할 이름을 입력합니다.
3. 다음 중 하나를 선택합니다.

◦ * 기본 *

기본 간격 스타일 일정을 만들려면 선택합니다.

◦ * 고급 *

cron 스타일 일정을 만들려면 선택합니다.

4. Create * 를 클릭합니다.

새 일정이 SnapMirror 일정 또는 SnapVault 일정 드롭다운 목록에 표시됩니다.

보호 관계 페일오버 및 페일백 수행

하드웨어 장애 또는 재해로 인해 보호 관계의 소스 볼륨이 비활성화되어 있는 경우, Unified Manager의 보호 관계 기능을 사용하여 보호 대상을 읽기/쓰기로 액세스하고 소스가 다시 온라인 상태가 될 때까지 해당 볼륨으로 페일오버할 수 있습니다. 그런 다음 데이터를 제공하는 데 사용할 수 있는 경우 원래 소스로 페일백할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 OnCommand Workflow Automation을 설정해야 합니다.

단계

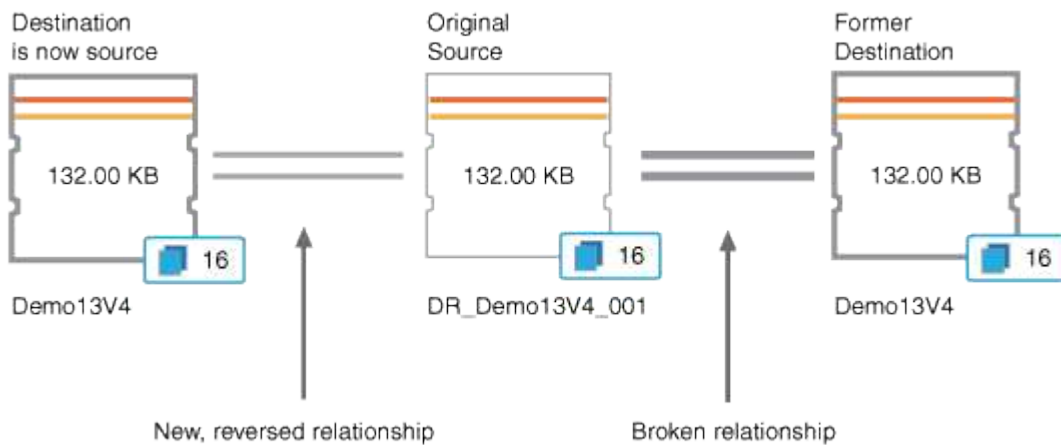
1. SnapMirror 관계를 발전시킬 수 있습니다.

대상을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환하려면 먼저 관계를 끊어야 하며, 그 후에 관계를 반대로 전환해야 합니다.

2. 보호 관계를 반대로 설정합니다.

원래 소스 볼륨을 다시 사용할 수 있는 경우 소스 볼륨을 복원하여 원래 보호 관계를 다시 설정할 수 있습니다. 소스를 복구하려면 먼저 소스를 이전 대상에 기록된 데이터와 동기화해야 합니다. 역방향 재동기화 작업을 사용하면 원래 관계의 역할을 바꾸고 소스 볼륨을 이전 대상과 동기화하여 새로운 보호 관계를 만들 수 있습니다. 새 관계에 대한 새 기본 스냅샷 복사본이 생성됩니다.

역관계는 다중 구간 관계와 비슷합니다.



3. 역방향 SnapMirror 관계를 나눕니다.

원본 소스 볼륨이 재동기화되어 데이터를 다시 제공할 수 있으면 중단 작업을 사용하여 역방향 관계를 끊어 보십시오.

4. 관계를 제거합니다.

역방향 관계가 더 이상 필요하지 않으면 원래 관계를 다시 설정하기 전에 해당 관계를 제거해야 합니다.

5. 관계를 다시 동기화합니다.

재동기화 작업을 사용하여 소스에서 대상으로 데이터를 동기화하고 원래 관계를 재설정합니다.

볼륨/상태 세부 정보 페이지에서 SnapMirror 관계 분리

볼륨/상태 세부 정보 페이지에서 보호 관계를 유지하고 SnapMirror 관계의 소스 볼륨과 타겟

볼륨 간의 데이터 전송을 중지할 수 있습니다. 데이터를 마이그레이션하거나, 재해 복구 또는 애플리케이션 테스트를 위해 관계를 끊을 수 있습니다. 대상 볼륨이 읽기-쓰기 볼륨으로 변경됩니다. SnapVault 관계를 끊을 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 분리할 SnapMirror 관계를 선택합니다.
2. 대상을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 * Break * (휴식 *)를 선택합니다.

[관계 분리] 대화상자가 표시됩니다.

3. 관계를 해제하려면 * 계속 * 을 클릭합니다.
4. 토폴로지에서 관계가 끊어졌는지 확인합니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 반대로 설정합니다

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 소스를 복구하거나 교체하는 동안 대상 볼륨을 사용하여 데이터를 읽기/쓰기로 변환하여 제공할 수 있습니다. 소스를 다시 사용하여 데이터를 수신할 수 있으면 역재동기화 작업을 사용하여 역방향의 관계를 설정하여 소스의 데이터를 읽기/쓰기 대상의 데이터와 동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 관계가 SnapVault 관계여야 합니다.
- 보호 관계가 이미 있어야 합니다.
- 보호 관계가 끊어야 합니다.
- 소스와 대상이 모두 온라인 상태여야 합니다.
- 소스가 다른 데이터 보호 볼륨의 대상이 아니어야 합니다.

이 작업에 대해

- 이 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신 소스의 데이터가 삭제됩니다.
- 역재동기화 관계에 생성된 정책 및 스케줄은 원래 보호 관계에 있는 정책과 동일합니다.

정책과 스케줄이 없으면 생성됩니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 소스와 대상을 반대로 이동할 SnapMirror 관계를 찾아 마우스 오른쪽 단추로 클릭합니다.
2. 메뉴에서 * Reverse Resync * 를 선택합니다.

역방향 재동기화 대화 상자가 표시됩니다.

3. 역방향 재동기화* 대화 상자에 표시된 관계가 역방향 재동기화 작업을 수행할 관계인지 확인한 다음 * 제출 * 을 클릭합니다.

역방향 재동기화 대화 상자가 닫히고 작업 링크가 볼륨/상태 세부 정보 페이지 맨 위에 표시됩니다.

4. 볼륨/상태 * 세부 정보 페이지에서 * 작업 보기 * 를 클릭하여 각 역방향 재동기화 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

5. 브라우저의 뒤로 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

모든 작업 작업이 성공적으로 완료되면 역방향 재동기화 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 제거합니다

보호 관계를 제거하여 선택한 소스와 대상 간의 기존 관계를 영구적으로 삭제할 수 있습니다. 예를 들어 다른 대상을 사용하여 관계를 만들려는 경우 이 작업은 모든 메타데이터를 제거하므로 실행 취소할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 제거할 SnapMirror 관계를 토폴로지 중에서 선택합니다.
2. 대상 이름을 마우스 오른쪽 단추로 클릭하고 메뉴에서 * 제거 * 를 선택합니다.

관계 제거 대화 상자가 표시됩니다.

3. 관계를 제거하려면 * 계속 * 을 클릭합니다.

볼륨/상태 세부 정보 페이지에서 관계가 제거됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 재동기화합니다

중단된 SnapMirror 또는 SnapVault 관계의 데이터를 다시 동기화한 다음 소스의 데이터가 대상의 데이터와 일치하도록 대상을 읽기/쓰기로 만들 수 있습니다. 소스 볼륨에서 필요한 공통 스냅샷 복사본이 삭제되어 SnapMirror 또는 SnapVault 업데이트가 실패하는 경우에도

재동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation를 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 재동기화하려는 보호 관계를 토폴로지에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * 재동기화 * 를 선택합니다.

또는 * Actions * 메뉴에서 * Relationship * > * ResSynchronize * 를 선택하여 현재 세부 정보를 보고 있는 관계를 다시 동기화합니다.

재동기화 대화 상자가 표시됩니다.

3. 재동기화 옵션 * 탭에서 전송 우선 순위 및 최대 전송 속도를 선택합니다.
4. 소스 스냅샷 복사본 * 을 클릭한 다음 * 스냅샷 복사본 * 열에서 * 기본값 * 을 클릭합니다.

소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

5. 기본 스냅샷 복사본을 전송하지 않고 기존 스냅샷 복사본을 지정하려면 * 기존 스냅샷 복사본 * 을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
6. 제출 * 을 클릭합니다.

재동기화 대화 상자로 돌아갑니다.

7. 재동기화할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정할 다음 소스에 대해 * 기본값 * 을 클릭합니다.
8. Submit * 을 클릭하여 재동기화 작업을 시작합니다.

재동기화 작업이 시작되고 볼륨/상태 세부 정보 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

9. 볼륨/상태 * 세부 정보 페이지에서 * 작업 보기 * 를 클릭하여 각 재동기화 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

10. 브라우저의 뒤로 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

모든 작업 작업이 성공적으로 완료되면 재동기화 작업이 완료됩니다.

보호 작업 실패 해결

이 워크플로우에서는 Unified Manager 대시보드에서 보호 작업 장애를 식별하고 해결하는 방법의 예를 제공합니다.

시작하기 전에

이 워크플로의 일부 작업에서는 관리자 역할을 사용하여 로그인해야 하므로 다양한 기능을 사용하는 데 필요한 역할에 익숙해야 합니다.

이 작업에 대해

이 시나리오에서는 대시보드 페이지에 액세스하여 보호 작업에 문제가 있는지 확인합니다. 보호 인시던트 영역에서 볼륨에 보호 작업 실패 오류가 표시된 작업이 종료된 인시던트가 있음을 알 수 있습니다. 이 오류를 조사하여 가능한 원인과 가능한 해결 방법을 결정합니다.

단계

1. Dashboard * Unresolved Incidents and Risks * 영역의 * Protection Incidents * 패널에서 * Protection job failed * 이벤트를 클릭합니다.



이벤트에 연결된 텍스트가 양식에 기록됩니다 object_name:/object_name - Error Name`예를 들면, 입니다 `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed.

실패한 보호 작업에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 요약 * 영역의 원인 필드에 있는 오류 메시지를 검토하여 문제를 확인하고 가능한 수정 조치를 평가합니다.

을 참조하십시오 [문제 식별 및 실패한 보호 작업에 대한 수정 조치 수행](#).

문제 식별 및 실패한 보호 작업에 대한 수정 조치 수행

이벤트 세부 정보 페이지의 원인 필드에서 작업 실패 오류 메시지를 검토하고 스냅샷 복사본 오류로 인해 작업이 실패했는지 확인합니다. 그런 다음 볼륨/상태 세부 정보 페이지로 이동하여 추가 정보를 수집합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

이벤트 세부 정보 페이지의 원인 필드에 제공된 오류 메시지에는 실패한 작업에 대한 다음 텍스트가 포함되어 있습니다.

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure..))
*Job Details*
```

이 메시지는 다음 정보를 제공합니다.

- 백업 또는 미러 작업이 성공적으로 완료되지 않았습니다.

이 작업에는 소스 볼륨 간의 보호 관계가 포함되었습니다 `cluster2_src_vol2` 가상 서버에서 `cluster2_src_svm` 및 타겟 볼륨입니다 `managed_svc2_vol3` 가상 서버에서 `클(를)` 선택합니다 `cluster3_dst_svm`.

- `에` 대한 스냅샷 복사본 작업이 실패했습니다 `0426cluster2_src_vol2snap` 소스 볼륨에서 `cluster2_src_svm:/cluster2_src_vol2`.

이 시나리오에서는 작업 실패의 원인 및 잠재적 시정 조치를 식별할 수 있습니다. 그러나 장애를 해결하려면 System Manager 웹 UI 또는 ONTAP CLI 명령에 액세스해야 합니다.

단계

1. 오류 메시지를 검토하고 소스 볼륨에서 스냅샷 복사본 작업이 실패했는지 확인하여 소스 볼륨에 문제가 있을 수 있음을 나타냅니다.

선택적으로 오류 메시지 끝에 있는 * 작업 세부 정보 * 링크를 클릭할 수 있지만 이 시나리오의 목적상 그렇게 하지 않도록 선택할 수 있습니다.

2. 이벤트 해결을 시도하기로 결정했으므로 다음을 수행합니다.

- a. 할당 대상 * 버튼을 클릭하고 메뉴에서 * Me * 를 선택합니다.
- b. 이벤트에 대한 경고가 설정된 경우 반복 알림 알림을 계속 수신하지 않도록 * 확인 * 버튼을 클릭합니다.
- c. 필요에 따라 이벤트에 대한 메모를 추가할 수도 있습니다.

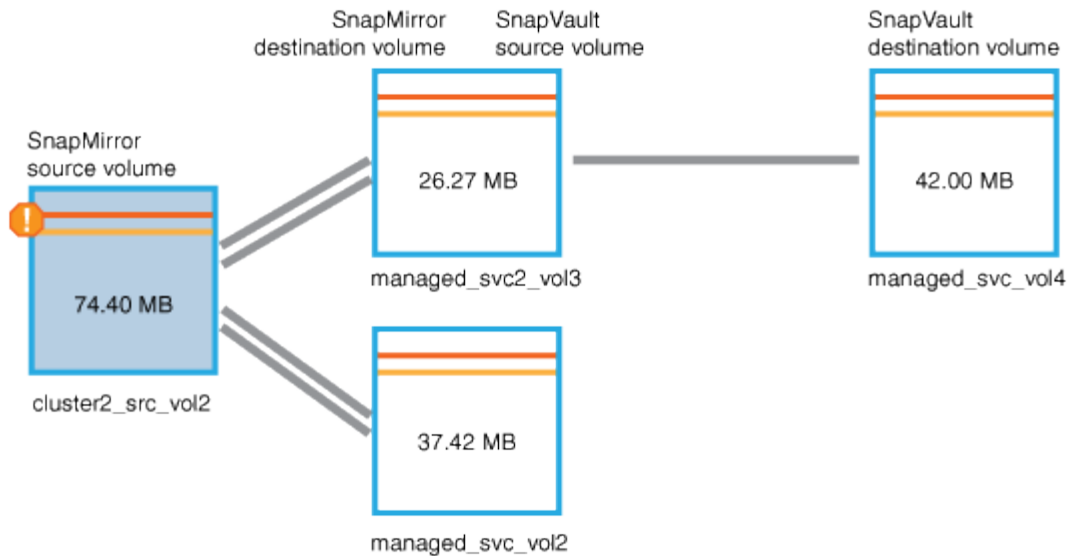
3. 소스 볼륨에 대한 세부 정보를 보려면 * 요약 * 창에서 * 소스 * 필드를 클릭합니다.

소스 * 필드에는 소스 객체의 이름이 들어 있습니다. 이 경우 스냅샷 복사본 작업이 예약된 볼륨입니다.

볼륨/상태 세부 정보 페이지가 `에` 표시됩니다 ``cluster2_src_vol2`` 보호 탭의 내용을 표시합니다.

4. 보호 토폴로지 그래프를 보면 토폴로지의 첫 번째 볼륨과 연관된 오류 아이콘이 표시됩니다. 이 아이콘은 SnapMirror 관계의 소스 볼륨입니다.

소스 볼륨 아이콘에는 해당 볼륨에 대해 설정된 경고 및 오류 임계값을 나타내는 가로 막바도 있습니다.



5. 오류 아이콘 위에 커서를 놓으면 임계값 설정이 표시되고 볼륨이 용량 문제를 나타내는 오류 임계값을 초과했음을 확인하는 팝업 대화 상자가 표시됩니다.
6. 용량 * 탭을 클릭합니다.

볼륨에 대한 용량 정보입니다 cluster2_src_vol2 표시됩니다.

7. 용량 * 패널에서 막대 그래프에 오류 아이콘이 표시됩니다. 이는 볼륨 용량이 볼륨에 설정된 임계값 수준을 초과했음을 나타냅니다.
8. 용량 그래프 아래에 볼륨 자동 확장 기능이 비활성화되어 있고 볼륨 공간 보장이 설정되어 있는 것을 볼 수 있습니다.

자동 증가를 사용하도록 설정할 수 있지만 이 시나리오의 목적상 용량 문제를 해결하는 방법을 결정하기 전에 추가 조사를하기로 결정합니다.

9. 아래로 스크롤하여 * 이벤트 * 목록으로 이동하여 보호 작업 실패, 전체 시점까지의 볼륨 일수 및 볼륨 공간 전체 이벤트가 생성되었는지 확인합니다.
10. Events* 목록에서 * Volume Space Full* 이벤트를 클릭하여 자세한 정보를 확인하고 이 이벤트가 용량 문제와 가장 관련이 있는 것으로 판단했습니다.

이벤트 세부 정보 페이지에는 소스 볼륨의 볼륨 공간 가득 참 이벤트가 표시됩니다.

11. 요약 * 영역에서 이벤트의 원인 필드를 읽습니다. The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
12. 요약 * 영역 아래에 권장 교정 조치가 표시됩니다.



제안된 시정 조치는 일부 이벤트에 대해서만 표시되므로 모든 유형의 이벤트에 대해 이 영역이 표시되지 않습니다.

볼륨 공간 가득 참 이벤트를 해결하기 위해 수행할 수 있는 권장 조치 목록을 클릭합니다.

- 이 볼륨에 대해 자동 확장 기능을 활성화합니다.
- 볼륨 크기를 조정합니다.
- 이 볼륨에서 중복 제거를 설정하고 실행합니다.

◦ 이 볼륨에 대해 압축을 활성화하고 실행합니다.

13. 볼륨에 대해 자동 확장을 활성화하기로 결정했지만, 그렇게 하려면 상위 애그리게이트에 사용 가능한 공간과 현재 볼륨 증가율을 확인해야 합니다.

a. 상위 집계, `cluster2_src_aggr1`를 클릭합니다.



Aggregate의 이름을 클릭하면 Aggregate에 대한 자세한 정보를 볼 수 있습니다.

Aggregate에 볼륨 자동 증가를 활성화할 수 있는 충분한 공간이 있는지 확인합니다.

b. 페이지 상단에서 중요 인시던트를 나타내는 아이콘을 확인하고 아이콘 아래에 있는 텍스트를 검토합니다.

"Days to Full: less than a day | Daily Growth Rate: 5.4%"를 결정합니다.

14. System Manager로 이동하거나 ONTAP CLI에 액세스하여 `volume autogrow` 옵션을 선택합니다.



자동 확장 기능을 설정할 때 사용할 수 있도록 볼륨 및 애그리게이트 이름을 기록해 둡니다.

15. 용량 문제를 해결한 후 Unified Manager 이벤트 세부 정보 페이지로 돌아가서 이벤트를 Resolved 로 표시합니다.

지연 문제 해결

이 워크플로에서는 지연 문제를 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 Unified ManagerDashboard 페이지에 액세스하는 관리자 또는 운영자로, 보호 관계에 문제가 있는지, 그리고 문제가 있는 경우 솔루션을 찾아야 합니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 작업에 대해

대시보드 페이지에서는 해결되지 않은 인시던트 및 위험 영역을 살펴보고 보호 위험 아래의 보호 창에서 SnapMirror 지연 오류를 확인할 수 있습니다.

단계

1. 대시보드 * 페이지의 * 보호 * 창에서 SnapMirror 관계 지연 오류를 찾아 클릭합니다.

LAG ERROR 이벤트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 이벤트 * 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.

- Summary(요약) 영역의 Cause(원인) 필드에 있는 오류 메시지를 검토하여 제안된 수정 조치가 있는지 확인합니다.
- 볼륨에 대한 세부 정보를 보려면 Summary(요약) 영역의 Source(소스) 필드에서 객체 이름(이 경우 볼륨)을 클릭합니다.

- 이 이벤트에 대해 추가되었을 수 있는 참고 사항을 찾습니다.
- 이벤트에 메모를 추가합니다.
- 특정 사용자에게 이벤트를 할당합니다.
- 이벤트를 확인하거나 해결합니다.

- 이 시나리오에서는 * Summary * (요약 *) 영역의 Source (소스) 필드에서 객체 이름(이 경우 볼륨)을 클릭하여 볼륨에 대한 세부 정보를 확인할 수 있습니다.

볼륨/상태 세부 정보 페이지의 보호 탭이 표시됩니다.

- Protection * 탭에서 토폴로지 다이어그램을 살펴봅니다.

지연 오류가 있는 볼륨은 3볼륨 SnapMirror 계단식 볼륨의 마지막 볼륨입니다. 선택한 볼륨의 윤곽선이 진한 회색으로 표시되고 소스 볼륨의 이중 주황색 선은 SnapMirror 관계 오류를 나타냅니다.



- SnapMirror 캐스케이드의 각 볼륨을 클릭합니다.

각 볼륨을 선택할 때 요약, 토폴로지, 기록, 이벤트, 관련 장치의 보호 정보 및 관련 경고 영역이 변경되어 선택한 볼륨과 관련된 세부 정보가 표시됩니다.

- Summary * (요약 *) 영역을 보고 각 볼륨의 * Update Schedule * (업데이트 일정 *) 필드에 있는 정보 아이콘 위에 커서를 놓습니다.

이 시나리오에서는 SnapMirror 정책이 DPDefault로, SnapMirror 일정은 시간 5분 후에 매시간 업데이트됩니다. 관계의 모든 볼륨이 동시에 SnapMirror 전송을 완료하려고 한다는 것을 알고 있습니다.

- 지연 문제를 해결하기 위해 각 대상이 전송을 완료한 후 SnapMirror 전송을 시작할 수 있도록 다중 구간 볼륨 중 두 개에 대한 일정을 수정합니다.

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.