



# Unified Manager에서 보호 관계 설정

## OnCommand Unified Manager 9.5

NetApp  
December 20, 2023

# 목차

Unified Manager에서 보호 관계 설정 .....	1
시작하기 전에 .....	1
단계 .....	1
Workflow Automation과 Unified Manager 간 연결 구성 .....	1
Workflow Automation에서 Unified Manager 데이터 소스 캐싱 검증 .....	2
상태/볼륨 세부 정보 페이지에서 SnapMirror 보호 관계 생성 .....	3
상태/볼륨 세부 정보 페이지에서 SnapVault 보호 관계 생성 .....	4
전송 효율성을 극대화하기 위한 SnapVault 정책 생성 .....	5
전송 효율성을 최대화할 수 있도록 SnapMirror 정책 생성 .....	5
SnapMirror 및 SnapVault 일정 생성 .....	6

# 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

- OnCommand 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 Automation](#)를 설정합니다
  - [Workflow Automation](#)에서 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 4.2 이상이어야 합니다.
- WFA 서버에 "'Clustered Data ONTAP을 관리하기 위한 WFA 팩'" 버전 9.5.0 이상이 설치되어 있어야 합니다. 필요한 팩은 NetAppStorage Automation Store에서 다운로드할 수 있습니다.

#### "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.
- OnCommand 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

## 단계

1. 도구 모음에서 \* 를 클릭합니다  \* 를 선택한 다음 왼쪽 설정 메뉴에서 \* Workflow Automation \* 을 클릭합니다.
2. 설정/워크플로우 자동화 \* 페이지의 \* OnCommand Unified Manager 데이터베이스 사용자 \* 영역에서 이름을 선택하고 Unified Manager 및 Workflow Automation 연결을 지원하기 위해 생성한 데이터베이스 사용자의 암호를 입력합니다.
3. 설정/워크플로우 자동화 \* 페이지의 \* OnCommand Workflow Automation 자격 증명 \* 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.

설정/워크플로우 자동화 페이지가 표시됩니다.

6. 웹 UI를 다시 로드하고 Workflow Automation 기능을 추가하려면 \* 예 \* 를 클릭합니다.

## 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.

# 상태/볼륨 세부 정보 페이지에서 SnapMirror 보호 관계 생성

상태/볼륨 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

- OnCommand 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)
- 볼륨이 FlexGroup 볼륨인 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. 상태/볼륨 \* 세부 정보 페이지의 \* 보호 \* 탭에서 보호할 볼륨의 이름을 마우스 오른쪽 버튼으로 토폴로지 뷰에서 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.

상태/볼륨 세부 정보 페이지로 돌아갑니다.

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

작업의 작업과 세부 정보가 보호/작업 세부 정보 페이지에 표시됩니다.

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

새 관계가 상태/볼륨 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.

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

볼륨에서 데이터 백업을 보호하기 위해 사용할 수 있도록 상태/볼륨 세부 정보 페이지를 사용하여 SnapVault 관계를 생성할 수 있습니다.

### 시작하기 전에

- OnCommand 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. 상태/볼륨 \* 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.

상태/볼륨 세부 정보 페이지로 돌아갑니다.

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

보호/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 상태/볼륨 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

- OnCommand 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

- OnCommand 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

- OnCommand 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.

## 저작권 정보

Copyright © 2023 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.