NetApp Disaster Recovery 설명서

NetApp Disaster Recovery

NetApp
February 04, 2026

목차

NetApp Disaster Recovery 설명서

릴리스 노트

NetApp Disaster Recovery 의 새로운 기능

NetApp Disaster Recovery 의 새로운 기능을 알아보세요.

2026년 1월 12일

버전 4.2.9

온프레미스 환경에서 여러 콘솔 에이전트 지원

온프레미스 재해 복구를 사용하는 경우 이제 각 vCenter 인스턴스에 콘솔 에이전트를 배포하여 복원력을 향상시킬 수 있습니다.

예를 들어, 두 개의 사이트(사이트 A와 B)가 있는 경우 사이트 A에는 콘솔 에이전트 A를 vCenter 1, ONTAP 배포 1 및 ONTAP 배포 2에 연결할 수 있습니다. 사이트 B는 콘솔 에이전트 B를 vCenter 2 및 ONTAP 배포 3 및 4에 연결할 수 있습니다.

재해 복구 환경에서 콘솔 에이전트에 대한 자세한 내용은 다음을 참조하십시오. "콘솔 에이전트 만들기".

데이터스토어 기반 보호를 사용하는 복제 계획에 대해 장애 조치 후 **VM**을 추가합니다**.**

장애 조치가 발생하면 데이터스토어 기반 보호를 사용하는 모든 복제 계획에는 데이터스토어에 추가된 VM이 포함됩니다. 단, 해당 VM이 검색된 경우에 한합니다. 장애 조치가 완료되기 전에 추가된 VM에 대한 매핑 세부 정보를 제공해야 합니다.

자세한 내용은 다음을 참조하세요. "장애 조치 애플리케이션".

새 이메일 알림

재해 복구 시스템은 이제 다음과 같은 이벤트에 대한 이메일 알림을 제공합니다.

- 용량 사용 한계에 근접하고 있습니다
- 보고서 생성 완료
- 직업 실패
- 면허 만료 또는 위반 사항

스웨거 개선 사항

이제 재해 복구 환경에서 Swagger 문서를 확인할 수 있습니다. 재해 복구에서 설정을 선택한 다음 **API** 문서를 선택하여 Swagger에 연결하거나 브라우저의 시크릿/개인 모드에서 다음 URL을 방문하세요. "https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas".

개선된 사용자 인터페이스

재해 복구 기능이 향상된 경고 및 오류 해결 기능을 제공합니다. 이번 릴리스에서는 취소된 작업이 사용자 인터페이스에 표시되지 않던 오류가 수정되었습니다. 취소된 작업이 이제 표시됩니다. 또한 동일한 대상 네트워크가 여러 개의 서로

다른 소스 네트워크에 매핑될 경우 새로운 경고 메시지가 표시됩니다.

복제 계획에 기본값으로 추가된 **VM** 폴더 구조를 유지합니다**.**

복제본을 생성할 때, 새로운 기본 설정은 VM 폴더 구조를 유지하는 것입니다. 복구 대상에 원래 폴더 계층 구조가 없는 경우 재해 복구 기능이 이를 생성합니다. 원래 폴더 계층 구조를 무시하려면 이 옵션을 선택 해제하면 됩니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기".

2025년 12월 9일

버전 4.2.8P1

폴더 계층 구조 유지

기본적으로 재해 복구는 장애 조치 시 VM 인벤토리 계층 구조(폴더 구조)를 유지합니다. 복구 대상에 필요한 폴더가 없으면 재해 복구가 해당 폴더를 만듭니다.

이제 새로운 부모 VM 폴더를 지정하거나 원래 폴더 계층 구조 유지 옵션의 선택을 취소하여 이 설정을 재정의할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기".

간소화된 콘솔 에이전트 업데이트

재해 복구는 이제 작업 환경에서 여러 콘솔 에이전트를 사용하기 위한 간소화된 프로세스를 지원합니다. 콘솔 에이전트 간에 전환하려면 vCenter 구성을 편집하고, 자격 증명을 다시 검색하고, 복제 계획을 새로 고쳐서 새 콘솔 에이전트를 사용해야 합니다.

자세한 내용은 다음을 참조하세요. "스위치 콘솔 에이전트".

2025년 12월 1일

버전 4.2.8

Google Cloud NetApp Volumes 사용하여 **Google Cloud VMware Engine** 지원

NetApp Disaster Recovery 이제 마이그레이션, 장애 조치, 장애 복구 및 테스트 작업을 위해 Google Cloud NetApp Volumes 사용하여 Google Cloud VMware Engine을 지원합니다. 이러한 통합을 통해 온프레미스 환경과 Google Cloud 간의 원활한 재해 복구 워크플로가 가능해집니다.

검토하세요"전제 조건" 그리고"제한 사항" Google Cloud를 위해.

2025년 11월 10일

버전 4.2.7

계단식 장애 조치 지원

이제 ONTAP 에서 계단식 관계를 구성하고 해당 복제 관계의 모든 단계를 재해 복구에 사용할 수 있습니다.

등록 중 **VMware** 하드웨어 지원 다운그레이드

재해 복구는 이제 등록 중에 VMware 하드웨어를 이전 버전의 vSphere로 다운그레이드하는 것을 지원합니다. 이 기능은 소스 ESX 호스트가 재해 복구 사이트보다 최신 버전을 실행하는 경우에 유용합니다.

자세한 내용은 다음을 참조하세요. "NetApp Disaster Recovery 에서 복제 계획 만들기".

우아한 종료

재해 복구 기능은 이제 VM의 전원을 끄는 대신 정상적으로 종료합니다. VM의 전원을 끄는 데 10분 이상 걸리는 경우 재해 복구 기능이 해당 VM의 전원을 끕니다.

사전 백업 스크립팅 지원

이제 백업을 생성하기 전에 실행할 사용자 정의 스크립팅을 장애 조치 워크플로에 삽입할 수 있습니다. 사전 백업 스크립팅을 사용하면 스냅샷이 복제되기 전에 VM 상태를 제어하고 전환을 위해 VM을 준비할 수 있습니다. 예를 들어, 장애 조치 후 다른 스크립트를 사용하여 다시 마운트될 NFS 마운트를 마운트 해제하는 스크립트를 삽입할 수 있습니다.

자세한 내용은 다음을 참조하세요. "NetApp Disaster Recovery 에서 복제 계획 만들기".

2025년 10월 6일

버전 4.2.6

BlueXP disaster recovery 이제 **NetApp Disaster Recovery** 입니다**.**

BlueXP disaster recovery NetApp Disaster Recovery 로 이름이 변경되었습니다.

BlueXP 는 이제 **NetApp Console** 입니다**.**

강화되고 재구성된 BlueXP 기반을 기반으로 구축된 NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경에서 NetApp 스토리지와 NetApp Data Services 중앙에서 관리하여 실시간 통찰력, 더 빠른 워크플로, 간소화된 관리를 제공하며, 높은 보안성과 규정 준수를 보장합니다.

변경된 사항에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 릴리스 노트".

기타 업데이트

- Amazon FSx for NetApp ONTAP 통한 Amazon Elastic VMware Service(EVS) 지원은 공개 미리 보기 단계에 있었습니다. 이번 릴리스를 통해 이제 일반적으로 사용할 수 있게 되었습니다. 자세한 내용은 다음을 참조하세요 ."Amazon Elastic VMware Service 및 Amazon FSx for NetApp ONTAP 사용한 NetApp Disaster Recovery 소개" .
- 온프레미스 배포에 대한 검색 시간 단축을 포함한 스토리지 검색 개선
- 역할 기반 액세스 제어(RBAC) 및 향상된 사용자 권한을 포함한 IAM(Identity and Access Management) 지원
- Azure VMware 솔루션 및 Cloud Volumes ONTAP 에 대한 Private Preview 지원. 이 지원을 통해 이제 Cloud Volumes ONTAP 스토리지를 사용하여 온프레미스에서 Azure VMware 솔루션으로 재해 복구 보호를 구성할 수 있습니다.

2025년 8월 4일

버전 4.2.5P2

NetApp Disaster Recovery 업데이트

이 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

- 여러 스토리지 가상 머신에서 제공되는 동일한 LUN을 처리하기 위해 VMFS 지원이 개선되었습니다.
- 이미 마운트 해제되거나 삭제된 데이터 저장소를 처리하기 위해 테스트 해체 정리를 개선했습니다.
- 제공된 네트워크 내에 입력된 게이트웨이가 포함되어 있는지 확인할 수 있도록 서브넷 매핑이 개선되었습니다.
- VM 이름에 ".com"이 포함되어 있는 경우 복제 계획이 실패할 수 있는 문제를 수정했습니다.
- 복제 계획 생성의 일부로 볼륨을 생성할 때 대상 볼륨이 소스 볼륨과 동일하지 않도록 하는 제한이 제거되었습니다.
- Azure Marketplace에서 NetApp Intelligent Services에 대한 PAYGO(종량제) 구독 지원을 추가하고 무료 평가판 대화 상자에 Azure Marketplace에 대한 링크를 추가했습니다.

  자세한 내용은 다음을 참조하세요. "NetApp Disaster Recovery 라이선싱" 그리고 "NetApp Disaster Recovery 에 대한 라이선싱 설정" .

2025년 7월 14일

버전 4.2.5

NetApp Disaster Recovery 의 사용자 역할

NetApp Disaster Recovery 이제 각 사용자가 특정 기능과 작업에 대해 갖는 액세스를 관리하는 역할을 사용합니다.

이 서비스는 NetApp Disaster Recovery 에 특정한 다음 역할을 사용합니다.

- 재해 복구 관리자: NetApp Disaster Recovery 에서 모든 작업을 수행합니다.
- 재해 복구 장애 조치 관리자: NetApp Disaster Recovery 에서 장애 조치 및 마이그레이션 작업을 수행합니다.
- 재해 복구 애플리케이션 관리자: 복제 계획을 만들고 수정하고 테스트 장애 조치를 시작합니다.
- 재해 복구 뷰어: NetApp Disaster Recovery 에서 정보를 볼 수 있지만, 어떤 작업도 수행할 수 없습니다.

NetApp Disaster Recovery 서비스를 클릭하고 처음으로 구성하는 경우 **SnapCenterAdmin** 권한이나 조직 관리자 역할이 있어야 합니다.

자세한 내용은 다음을 참조하세요."NetApp Disaster Recovery 의 사용자 역할 및 권한" .

"모든 서비스에 대한 액세스 역할에 대해 알아보세요".

NetApp Disaster Recovery 의 기타 업데이트

- 향상된 네트워크 검색
- 확장성 개선:
  - 모든 세부 정보 대신 필요한 메타데이터만 필터링

    - VM 리소스를 더 빠르게 검색하고 업데이트하기 위한 검색 개선
    - 데이터 검색 및 데이터 업데이트를 위한 메모리 최적화 및 성능 최적화
    - vCenter SDK 클라이언트 생성 및 풀 관리 개선
- 다음 예약 또는 수동 검색 시 오래된 데이터 관리:
    - vCenter에서 VM이 삭제되면 이제 NetApp Disaster Recovery 복제 계획에서 자동으로 해당 VM을 제거합니다.
    - vCenter에서 데이터 저장소나 네트워크가 삭제되면 이제 NetApp Disaster Recovery 복제 계획 및 리소스 그룹에서도 해당 데이터 저장소나 네트워크를 삭제합니다.
    - vCenter에서 클러스터, 호스트 또는 데이터 센터가 삭제되면 이제 NetApp Disaster Recovery 복제 계획 및 리소스 그룹에서 해당 항목을 삭제합니다.
- 이제 브라우저의 시크릿 모드에서도 Swagger 문서에 액세스할 수 있습니다. NetApp Disaster Recovery 에서 설정 옵션 > API 설명서를 통해 액세스할 수 있으며, 브라우저의 시크릿 모드에서 다음 URL을 통해 직접 액세스할 수도 있습니다. "Swagger 문서" .
- 어떤 상황에서는 장애 복구 작업 후 작업이 완료된 후에도 iGroup이 남겨지는 경우가 있었습니다. 이 업데이트는 오래된 iGroup을 제거합니다.
- 복제 계획에 NFS FQDN이 사용된 경우 NetApp Disaster Recovery 이제 이를 IP 주소로 확인합니다. 이 업데이트는 재해 복구 사이트에서 FQDN을 확인할 수 없는 경우에 유용합니다.
- UI 정렬 개선
- 성공적인 검색 후 vCenter 크기 조정 세부 정보를 캡처하기 위한 로그 개선

2025년 6월 30일

버전 4.2.4P2

발견 개선

이 업데이트는 검색 프로세스를 개선하여 검색에 필요한 시간을 줄여줍니다.

2025년 6월 23일

버전 4.2.4P1

서브넷 매핑 개선

이 업데이트에서는 새로운 검색 기능을 통해 서브넷 매핑 추가 및 편집 대화 상자가 개선되었습니다. 이제 검색어를 입력하여 특정 서브넷을 빠르게 찾을 수 있어 서브넷 매핑을 더 쉽게 관리할 수 있습니다.

2025년 6월 9일

버전 4.2.4

Windows 로컬 관리자 암호 솔루션**(LAPS)** 지원

Windows 로컬 관리자 암호 솔루션(Windows LAPS)은 Active Directory에서 로컬 관리자 계정의 암호를 자동으로 관리하고 백업하는 Windows 기능입니다.

이제 도메인 컨트롤러 세부 정보를 제공하여 서브넷 매핑 옵션을 선택하고 LAPS 옵션을 확인할 수 있습니다. 이 옵션을 사용하면 각 가상 머신에 대한 비밀번호를 제공할 필요가 없습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

2025년 5월 13일

버전 4.2.3

서브넷 매핑

이 릴리스에서는 서브넷 매핑을 사용하여 새로운 방식으로 장애 조치 시 IP 주소를 관리할 수 있으며, 이를 통해 각 vCenter에 대한 서브넷을 추가할 수 있습니다. 이렇게 하면 각 가상 네트워크에 대한 IPv4 CIDR, 기본 게이트웨이, DNS가 정의됩니다.

장애 조치 시 NetApp Disaster Recovery 매핑된 가상 네트워크에 제공된 CIDR을 보고 각 vNIC의 적절한 IP 주소를 결정하고 이를 사용하여 새 IP 주소를 파생합니다.

예를 들어:

- 네트워크A = 10.1.1.0/24
- 네트워크B = 192.168.1.0/24

VM1에는 NetworkA에 연결된 vNIC(10.1.1.50)가 있습니다. NetworkA는 복제 계획 설정에서 NetworkB에 매핑됩니다.

장애 조치 시 NetApp Disaster Recovery 원래 IP 주소(10.1.1)의 네트워크 부분을 대체하고 원래 IP 주소(10.1.1.50)의 호스트 주소(.50)를 유지합니다. VM1의 경우 NetApp Disaster Recovery NetworkB의 CIDR 설정을 살펴보고 NetworkB의 네트워크 부분인 192.168.1을 사용하고 호스트 부분(.50)은 그대로 유지하여 VM1의 새 IP 주소를 생성합니다. 새로운 IP는 192.168.1.50이 됩니다.

요약하자면, 호스트 주소는 동일하게 유지되지만 네트워크 주소는 사이트 서브넷 매핑에 구성된 주소로 대체됩니다. 이를 통해 장애 조치 시 IP 주소 재할당을 보다 쉽게 관리할 수 있으며, 특히 관리해야 할 네트워크가 수백 개이고 VM이 수천 개일 경우 더욱 그렇습니다.

사이트에 서브넷 매핑을 포함하는 방법에 대한 자세한 내용은 다음을 참조하세요. "vCenter 서버 사이트 추가" .

스킵 보호

이제 복제 계획 장애 조치 후 서비스가 자동으로 역방향 보호 관계를 생성하지 않도록 보호를 건너뛸 수 있습니다. NetApp Disaster Recovery 에서 다시 온라인으로 전환하기 전에 복원된 사이트에서 추가 작업을 수행하려는 경우 이 기능이 유용합니다.

장애 조치를 시작하면 기본적으로 서비스는 복제 계획의 각 볼륨에 대해 역방향 보호 관계를 자동으로 생성합니다(원본 소스 사이트가 온라인 상태인 경우). 즉, 서비스는 대상 사이트에서 소스 사이트로 SnapMirror 관계를 생성합니다. 또한 이 서비스는 장애 복구를 시작하면 SnapMirror 관계를 자동으로 되돌립니다.

장애 조치를 시작할 때 이제 보호 건너뛰기 옵션을 선택할 수 있습니다. 이를 통해 서비스는 SnapMirror 관계를 자동으로 반전시키지 않습니다. 대신 복제 계획의 양쪽에 쓰기 가능한 볼륨이 남습니다.

원래 소스 사이트가 다시 온라인 상태가 되면 복제 계획 작업 메뉴에서 *리소스 보호*를 선택하여 역방향 보호를 설정할 수 있습니다. 이는 계획의 각 볼륨에 대해 역방향 복제 관계를 생성하려고 시도합니다. 보호가 복구될 때까지 이 작업을

반복해서 실행할 수 있습니다. 보호가 복구되면 평소와 같은 방식으로 장애 복구를 시작할 수 있습니다.

자세한 내용은 건너뛰기 보호에 대한 내용을 참조하세요. "원격 사이트로 애플리케이션 장애 조치" .

SnapMirror 복제 계획에서 업데이트를 일정에 추가합니다**.**

NetApp Disaster Recovery 이제 기본 ONTAP SnapMirror 정책 스케줄러나 ONTAP 과의 타사 통합과 같은 외부 스냅샷 관리 솔루션을 사용할 수 있도록 지원합니다. 복제 계획의 모든 데이터 저장소(볼륨)에 이미 다른 곳에서 관리되는 SnapMirror 관계가 있는 경우 NetApp Disaster Recovery 에서 해당 스냅샷을 복구 지점으로 사용할 수 있습니다.

구성하려면 복제 계획 > 리소스 매핑 섹션에서 데이터 저장소 매핑을 구성할 때 플랫폼 관리 백업 및 보존 일정 사용 확인란을 선택합니다.

해당 옵션을 선택하면 NetApp Disaster Recovery 백업 일정을 구성하지 않습니다. 그러나 테스트, 장애 조치, 장애 복구 작업을 위해 스냅샷이 계속 생성될 수 있으므로 보존 일정을 구성해야 합니다.

이것이 구성된 후에는 서비스가 정기적으로 예약된 스냅샷을 찍지 않고 대신 외부 엔터티를 사용하여 해당 스냅샷을 찍고 업데이트합니다.

복제 계획에서 외부 스냅샷 솔루션을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

2025년 4월 16일

버전 4.2.2

VM에 대한 예약된 검색

NetApp Disaster Recovery 24시간마다 검색을 수행합니다. 이번 릴리스를 통해 이제 필요에 맞게 검색 일정을 사용자 지정하고 필요할 때 성능에 미치는 영향을 줄일 수 있습니다. 예를 들어, VM 수가 많은 경우 검색 일정을 48시간마다 실행되도록 설정할 수 있습니다. VM 수가 적은 경우 검색 일정을 12시간마다 실행되도록 설정할 수 있습니다.

검색 일정을 예약하고 싶지 않으면 예약된 검색 옵션을 비활성화하고 언제든지 수동으로 검색을 새로 고칠 수 있습니다.

자세한 내용은 다음을 참조하세요. "vCenter 서버 사이트 추가" .

리소스 그룹 데이터 저장소 지원

이전에는 VM별로만 리소스 그룹을 만들 수 있었습니다. 이 릴리스에서는 데이터 저장소별로 리소스 그룹을 만들 수 있습니다. 복제 계획을 만들고 해당 계획에 대한 리소스 그룹을 만들면 데이터 저장소의 모든 VM이 나열됩니다. 이 기능은 다수의 VM이 있고 이를 데이터 저장소별로 그룹화하려는 경우에 유용합니다.

다음과 같은 방법으로 데이터 저장소를 사용하여 리소스 그룹을 만들 수 있습니다.

- 데이터 저장소를 사용하여 리소스 그룹을 추가하는 경우 데이터 저장소 목록을 볼 수 있습니다. 하나 이상의 데이터 저장소를 선택하여 리소스 그룹을 만들 수 있습니다.
- 복제 계획을 만들고 계획 내에서 리소스 그룹을 만들면 데이터 저장소에서 VM을 볼 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

무료 체험판 또는 라이센스 만료 알림

이 릴리스에서는 무료 평가판이 60일 후에 만료된다는 알림을 제공하여 라이선스를 받을 시간을 확보할 수 있도록 합니다. 이 릴리스에서는 라이센스가 만료되는 날에 대한 알림도 제공합니다.

서비스 업데이트 알림

이번 릴리스에서는 서비스가 업그레이드되고 서비스가 유지 관리 모드로 전환되었음을 나타내는 배너가 상단에 나타납니다. 배너는 서비스가 업그레이드될 때 나타나고 업그레이드가 완료되면 사라집니다. 업그레이드가 진행되는 동안 UI에서 작업을 계속할 수 있지만 새로운 작업을 제출할 수는 없습니다. 업데이트가 완료되고 서비스가 프로덕션 모드로 돌아온 후에 예약된 작업이 실행됩니다.

2025년 3월 10일

버전 4.2.1

지능형 프록시 지원

NetApp Console 에이전트는 지능형 프록시를 지원합니다. 지능형 프록시는 온프레미스 시스템을 NetApp Disaster Recovery 에 연결하는 가볍고 안전하며 효율적인 방법입니다. VPN이나 직접 인터넷 접속이 필요 없이 시스템과 NetApp Disaster Recovery 간의 안전한 연결을 제공합니다. 이 최적화된 프록시 구현은 로컬 네트워크 내의 API 트래픽을 오프로드합니다.

프록시가 구성되면 NetApp Disaster Recovery VMware 또는 ONTAP 과 직접 통신을 시도하고 직접 통신이 실패하면 구성된 프록시를 사용합니다.

NetApp Disaster Recovery 프록시 구현에는 HTTPS 프로토콜을 사용하여 콘솔 에이전트와 모든 vCenter 서버 및 ONTAP 어레이 간에 포트 443 통신이 필요합니다. 콘솔 에이전트 내의 NetApp Disaster Recovery 에이전트는 모든 작업을 수행할 때 VMware vSphere, VC 또는 ONTAP 과 직접 통신합니다.

NetApp Disaster Recovery 용 지능형 프록시에 대한 자세한 내용은 다음을 참조하세요. "NetApp Disaster Recovery 위한 인프라 설정" .

NetApp Console 에서 일반 프록시 설정에 대한 자세한 내용은 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

언제든지 무료 체험을 종료하세요

언제든지 무료 체험을 중단할 수 있으며, 체험 기간이 만료될 때까지 기다릴 수도 있습니다.

보다 "무료 체험 종료" .

2025년 2월 19일

버전 4.2

VMFS 스토리지의 **VM** 및 데이터 저장소에 대한 **ASA r2** 지원

NetApp Disaster Recovery 의 이 릴리스에서는 VMFS 스토리지의 VM 및 데이터 저장소에 대한 ASA r2에 대한 지원을 제공합니다. ASA r2 시스템에서 ONTAP 소프트웨어는 SAN 환경에서 지원되지 않는 기능을 제거하는 동시에 필수적인 SAN 기능을 지원합니다.

이 릴리스는 ASA r2에 대해 다음 기능을 지원합니다.

- 기본 스토리지에 대한 일관성 그룹 프로비저닝(계층 구조 없이 단일 레벨만 있는 플랫 일관성 그룹만 해당)
- SnapMirror 자동화를 포함한 백업(일관성 그룹) 작업

NetApp Disaster Recovery 에서 ASA r2를 지원하려면 ONTAP 9.16.1이 필요합니다.

데이터 저장소는 ONTAP 볼륨이나 ASA r2 스토리지 유닛에 마운트할 수 있지만 NetApp Disaster Recovery 의 리소스 그룹에는 ONTAP 의 데이터 저장소와 ASA r2의 데이터 저장소를 모두 포함할 수 없습니다. 리소스 그룹에서 ONTAP 의 데이터 저장소나 ASA r2의 데이터 저장소를 선택할 수 있습니다.

2024년 10월 30일

보고

이제 풍경을 분석하는 데 도움이 되는 보고서를 생성하고 다운로드할 수 있습니다. 사전 설계된 보고서는 장애 조치(failover)와 장애 복구(failback)를 요약하고, 모든 사이트의 복제 세부 정보를 표시하며, 지난 7일간의 작업 세부 정보를 표시합니다.

참조하다 "재해 복구 보고서 만들기" .

30일 무료 체험

이제 NetApp Disaster Recovery 의 30일 무료 평가판에 등록할 수 있습니다. 이전에는 무료 체험 기간이 90일이었습니다.

참조하다 "라이센스 설정" .

복제 계획 비활성화 및 활성화

이전 릴리스에는 일일 및 주간 일정을 지원하는 데 필요한 장애 조치 테스트 일정 구조에 대한 업데이트가 포함되었습니다. 이 업데이트를 적용하려면 새로운 일일 및 주간 장애 조치 테스트 일정을 사용할 수 있도록 모든 기존 복제 계획을 비활성화했다가 다시 활성화해야 합니다. 이는 일회성 요구 사항입니다.

방법은 다음과 같습니다.

1. 메뉴에서 *복제 계획*을 선택합니다.
2. 계획을 선택하고 작업 아이콘을 선택하여 드롭다운 메뉴를 표시합니다.
3. *비활성화*를 선택하세요.
4. 몇 분 후에 *활성화*를 선택하세요.

폴더 매핑

복제 계획을 생성하고 컴퓨팅 리소스를 매핑할 때 이제 폴더를 매핑하여 데이터 센터, 클러스터 및 호스트에 대해 지정한 폴더에 VM을 복구할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

장애 조치, 장애 복구 및 테스트 장애 조치에 사용할 수 있는 **VM** 세부 정보

장애가 발생하고 장애 조치를 시작하거나, 장애 복구를 수행하거나, 장애 조치를 테스트하는 경우 이제 VM의 세부 정보를 확인하고 다시 시작되지 않은 VM을 식별할 수 있습니다.

참조하다 "원격 사이트로 애플리케이션 장애 조치" .

순서가 지정된 부팅 시퀀스를 사용한 **VM** 부팅 지연

복제 계획을 만들 때 이제 계획에 있는 각 VM에 대한 부팅 지연을 설정할 수 있습니다. 이를 통해 VM이 시작될 순서를 설정하여 후속 우선순위 VM이 시작되기 전에 모든 우선순위 1 VM이 실행되도록 할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

VM 운영 체제 정보

복제 계획을 만들면 이제 계획에 있는 각 VM의 운영 체제를 볼 수 있습니다. 이는 리소스 그룹에서 VM을 어떻게 그룹화할지 결정하는 데 유용합니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

VM 이름 별칭

복제 계획을 만들 때 이제 재해 복구 사이트의 VM 이름에 접두사와 접미사를 추가할 수 있습니다. 이를 통해 계획에 있는 VM에 대해 보다 설명적인 이름을 사용할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

오래된 스냅샷 정리

지정한 보존 기간을 넘어서 더 이상 필요하지 않은 스냅샷은 삭제할 수 있습니다. 스냅샷 보존 횟수를 줄이면 시간이 지남에 따라 스냅샷이 누적될 수 있으며, 이제 스냅샷을 제거하여 공간을 확보할 수 있습니다. 이 작업은 언제든지 필요할 때 수행할 수 있으며, 복제 계획을 삭제할 때도 수행할 수 있습니다.

자세한 내용은 다음을 참조하세요. "사이트, 리소스 그룹, 복제 계획, 데이터 저장소 및 가상 머신 정보를 관리합니다." .

스냅샷 조정

이제 소스와 대상 간에 동기화되지 않은 스냅샷을 조정할 수 있습니다. 이는 NetApp Disaster Recovery 외부의 대상에서 스냅샷이 삭제된 경우 발생할 수 있습니다. 이 서비스는 24시간마다 소스의 스냅샷을 자동으로 삭제합니다. 하지만 필요에 따라 이를 수행할 수도 있습니다. 이 기능을 사용하면 모든 사이트에서 스냅샷이 일관성을 유지하도록 할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 관리" .

2024년 9월 20일

온프레미스 간 **VMware VMFS** 데이터 저장소 지원

이 릴리스에는 온프레미스 스토리지로 보호되는 iSCSI 및 FC를 위한 VMware vSphere 가상 머신 파일 시스템(VMFS) 데이터 저장소에 마운트된 VM에 대한 지원이 포함됩니다. 이전에는 이 서비스에서 iSCSI 및 FC에 대한 VMFS 데이터 저장소를 지원하는 _기술 미리보기_가 제공되었습니다.

iSCSI 및 FC 프로토콜과 관련된 추가 고려 사항은 다음과 같습니다.

- FC 지원은 복제가 아닌 클라이언트 프런트엔드 프로토콜을 위한 것입니다.
- NetApp Disaster Recovery ONTAP 볼륨당 하나의 LUN만 지원합니다. 볼륨에는 여러 개의 LUN이 있어서는 안 됩니다.
- 모든 복제 계획의 경우 대상 ONTAP 볼륨은 보호된 VM을 호스팅하는 소스 ONTAP 볼륨과 동일한 프로토콜을 사용해야 합니다. 예를 들어, 소스가 FC 프로토콜을 사용하는 경우 대상도 FC를 사용해야 합니다.

2024년 8월 2일

FC용 온프레미스 간 **VMware VMFS** 데이터 저장소 지원

이 릴리스에는 FC로 보호되는 온프레미스 스토리지를 위한 VMware vSphere 가상 머신 파일 시스템(VMFS) 데이터 저장소에 마운트된 VM에 대한 지원에 대한 _기술 미리보기_가 포함되어 있습니다. 이전에는 이 서비스에서 iSCSI용 VMFS 데이터 저장소를 지원하는 기술 미리보기가 제공되었습니다.

NetApp 미리 본 워크로드 용량에 대해 요금을 청구하지 않습니다.

작업 취소

이 릴리스에서는 이제 Job Monitor UI에서 작업을 취소할 수 있습니다.

참조하다 "작업 모니터링" .

2024년 7월 17일

장애 조치 테스트 일정

이 릴리스에는 일일 및 주간 일정을 지원하는 데 필요한 장애 조치 테스트 일정 구조에 대한 업데이트가 포함되어 있습니다. 이 업데이트를 적용하려면 새로운 일일 및 주간 장애 조치 테스트 일정을 사용할 수 있도록 모든 기존 복제 계획을 비활성화했다가 다시 활성화해야 합니다. 이는 일회성 요구 사항입니다.

방법은 다음과 같습니다.

1. 메뉴에서 *복제 계획*을 선택합니다.
2. 계획을 선택하고 작업 아이콘을 선택하여 드롭다운 메뉴를 표시합니다.
3. *비활성화*를 선택하세요.
4. 몇 분 후에 *활성화*를 선택하세요.

복제 계획 업데이트

이 릴리스에는 복제 계획 데이터에 대한 업데이트가 포함되어 있어 "스냅샷을 찾을 수 없음" 문제가 해결되었습니다. 이렇게 하려면 모든 복제 계획에서 보존 횟수를 1로 변경하고 주문형 스냅샷을 시작해야 합니다. 이 프로세스는 새로운 백업을 만들고 이전 백업을 모두 제거합니다.

방법은 다음과 같습니다.

1. 메뉴에서 *복제 계획*을 선택합니다.

2. 복제 계획을 선택하고, 장애 조치 매핑 탭을 선택한 다음, 편집 연필 아이콘을 선택합니다.
3. 데이터 저장소 화살표를 선택하여 확장합니다.
4. 복제 계획에서 보존 횟수 값을 확인하세요. 이러한 단계를 완료한 후에는 원래 값을 다시 설정해야 합니다.
5. 카운트를 1로 줄이세요.
6. 주문형 스냅샷을 시작합니다. 이렇게 하려면 복제 계획 페이지에서 계획을 선택하고 작업 아이콘을 선택한 다음 *지금 스냅샷 찍기*를 선택합니다.
7. 스냅샷 작업이 성공적으로 완료되면 복제 계획의 개수를 첫 번째 단계에서 기록한 원래 값으로 다시 늘립니다.
8. 기존의 모든 복제 계획에 대해 이 단계를 반복합니다.

2024년 7월 5일

이 NetApp Disaster Recovery 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

AFF A 시리즈 지원

이 릴리스는 NetApp AFF A 시리즈 하드웨어 플랫폼을 지원합니다.

온프레미스 간 VMware VMFS 데이터 저장소 지원

이 릴리스에는 온프레미스 스토리지로 보호되는 VMware vSphere 가상 머신 파일 시스템(VMFS) 데이터 저장소에 마운트된 VM에 대한 지원에 대한 _기술 미리보기_가 포함되어 있습니다. 이 릴리스에서는 온프레미스 VMware 워크로드에서 VMFS 데이터 저장소가 있는 온프레미스 VMware 환경으로의 재해 복구가 기술 미리 보기에서 지원됩니다.

NetApp 미리 본 워크로드 용량에 대해 요금을 청구하지 않습니다.

복제 계획 업데이트

애플리케이션 페이지에서 데이터 저장소별로 VM을 필터링하고 리소스 매핑 페이지에서 추가 대상 세부 정보를 선택하면 복제 계획을 더 쉽게 추가할 수 있습니다. 참조하다 "복제 계획 만들기" .

복제 계획 편집

이번 릴리스에서는 장애 조치 매핑 페이지가 개선되어 명확성이 향상되었습니다.

참조하다 "계획 관리" .

VM 편집

이번 릴리스에서는 계획에서 VM을 편집하는 프로세스에 몇 가지 사소한 UI 개선 사항이 포함되었습니다.

참조하다 "VM 관리" .

업데이트 장애 조치

장애 조치를 시작하기 전에 이제 VM의 상태와 전원이 켜져 있는지 꺼져 있는지 확인할 수 있습니다. 이제 장애 조치 프로세스를 통해 지금 스냅샷을 찍거나 스냅샷을 선택할 수 있습니다.

참조하다 "원격 사이트로 애플리케이션 장애 조치" .

장애 조치 테스트 일정

이제 장애 조치 테스트를 편집하고 장애 조치 테스트에 대한 일일, 주간, 월간 일정을 설정할 수 있습니다.

참조하다 "계획 관리" .

필수 정보 업데이트

NetApp Disaster Recovery 필수 구성 요소 정보가 업데이트되었습니다.

참조하다 "NetApp Disaster Recovery 필수 구성 요소" .

2024년 5월 15일

이 NetApp Disaster Recovery 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

온프레미스에서 온프레미스로 **VMware** 워크로드 복제

이 기능은 이제 일반 공급 기능으로 출시되었습니다. 이전에는 기능이 제한된 기술 미리보기였습니다.

라이센스 업데이트

NetApp Disaster Recovery 사용하면 90일 무료 평가판에 가입하거나 Amazon Marketplace에서 사용량에 따라 지불하는(PAYGO) 구독을 구매하거나 NetApp 영업 담당자나 NetApp 지원 사이트(NSS)에서 얻을 수 있는 NetApp 라이선스 파일(NLF)인 Bring Your Own License(BYOL)를 사용할 수 있습니다.

NetApp Disaster Recovery 에 대한 라이선싱 설정에 대한 자세한 내용은 다음을 참조하세요."라이센스 설정" .

"NetApp Disaster Recovery 에 대해 자세히 알아보세요".

2024년 3월 5일

이는 NetApp Disaster Recovery 의 일반 공급 릴리스로, 다음 업데이트가 포함되어 있습니다.

라이센스 업데이트

NetApp Disaster Recovery 사용하면 90일 무료 평가판에 가입하거나 NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)인 BYOL(Bring Your Own License)을 사용할 수 있습니다. NetApp Console 구독에서 BYOL을 활성화하려면 라이선스 일련 번호를 사용할 수 있습니다. NetApp Disaster Recovery 요금은 데이터 저장소의 프로비저닝된 용량을 기준으로 합니다.

NetApp Disaster Recovery 에 대한 라이선싱 설정에 대한 자세한 내용은 다음을 참조하세요. "라이센스 설정" .

모든 NetApp Console 데이터 서비스에 대한 라이선스 관리에 대한 자세한 내용은 다음을 참조하세요. "모든 NetApp Console 데이터 서비스에 대한 라이선스 관리" .

일정 편집

이 릴리스를 사용하면 규정 준수 및 장애 조치 테스트를 위한 일정을 설정하여 필요할 경우 해당 테스트가 올바르게

작동하는지 확인할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

2024년 2월 1일

이 NetApp Disaster Recovery 미리 보기 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

네트워크 강화

이 릴리스에서는 이제 VM CPU 및 RAM 값의 크기를 조정할 수 있습니다. 이제 VM에 대한 네트워크 DHCP 또는 정적 IP 주소를 선택할 수도 있습니다.

- DHCP: 이 옵션을 선택하면 VM에 대한 자격 증명을 제공합니다.
- 고정 IP: 소스 VM에서 동일하거나 다른 정보를 선택할 수 있습니다. 출처와 동일한 것을 선택하면 자격 증명을 입력할 필요가 없습니다. 반면, 소스의 다른 정보를 사용하기로 선택한 경우 자격 증명, IP 주소, 서브넷 마스크, DNS 및 게이트웨이 정보를 제공할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

사용자 정의 스크립트

이제 장애 조치 후 프로세스에 포함될 수 있습니다. 사용자 정의 스크립트를 사용하면 장애 조치 프로세스 후에 NetApp Disaster Recovery 스크립트를 실행하도록 할 수 있습니다. 예를 들어, 장애 조치가 완료된 후 사용자 정의 스크립트를 사용하여 모든 데이터베이스 트랜잭션을 재개할 수 있습니다.

자세한 내용은 다음을 참조하세요. "원격 사이트로 장애 조치" .

SnapMirror 관계

이제 복제 계획을 개발하는 동안 SnapMirror 관계를 만들 수 있습니다. 이전에는 NetApp Disaster Recovery 외부에서 관계를 만들어야 했습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

일관성 그룹

복제 계획을 만들 때 서로 다른 볼륨과 서로 다른 SVM에 속한 VM을 포함할 수 있습니다. NetApp Disaster Recovery 모든 볼륨을 포함하여 일관성 그룹 스냅샷을 만들고 모든 보조 위치를 업데이트합니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

VM 전원 켜짐 지연 옵션

복제 계획을 만들 때 리소스 그룹에 VM을 추가할 수 있습니다. 리소스 그룹을 사용하면 각 VM에 지연 시간을 설정하여 지연된 순서로 전원이 켜지도록 할 수 있습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

애플리케이션 일관성 스냅샷 복사본

애플리케이션과 일관된 스냅샷 복사본을 생성하도록 지정할 수 있습니다. 이 서비스는 애플리케이션을 정지시킨 다음 스냅샷을 찍어 애플리케이션의 일관된 상태를 얻습니다.

자세한 내용은 다음을 참조하세요. "복제 계획 만들기" .

2024년 1월 11일

NetApp Disaster Recovery 의 이 미리 보기 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

대시보드를 더 빠르게

이번 릴리스를 통해 대시보드의 다른 페이지에 있는 정보에 더 빠르게 액세스할 수 있습니다.

"NetApp Disaster Recovery 에 대해 알아보세요".

2023년 10월 20일

NetApp Disaster Recovery 의 이 미리 보기 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

온프레미스 **NFS** 기반 **VMware** 워크로드 보호

이제 NetApp Disaster Recovery 사용하면 퍼블릭 클라우드뿐만 아니라 온프레미스 NFS 기반 VMware 환경의 재해로부터 온프레미스 NFS 기반 VMware 워크로드를 보호할 수 있습니다. NetApp Disaster Recovery 재해 복구 계획의 완료를 조율합니다.

> 이 미리보기 제공을 통해 NetApp 일반 공급 전에 제공 세부 정보, 내용 및 일정을 수정할 권리가 있습니다.

"NetApp Disaster Recovery 에 대해 자세히 알아보세요".

2023년 9월 27일

NetApp Disaster Recovery 의 이 미리 보기 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

대시보드 업데이트

이제 대시보드에서 옵션을 선택하여 정보를 더 빠르고 쉽게 검토할 수 있습니다. 또한 대시보드에는 이제 장애 조치 및 마이그레이션 상태가 표시됩니다.

참조하다 "대시보드에서 재해 복구 계획의 상태를 확인하세요." .

복제 계획 업데이트

- **RPO**: 이제 복제 계획의 데이터 저장소 섹션에 복구 지점 목표(RPO)와 보존 횟수를 입력할 수 있습니다. 이는 설정된 시간보다 오래되지 않은 데이터의 양을 나타냅니다. 예를 들어, 5분으로 설정하면 비즈니스에 중요한 요구 사항에 영향을 미치지 않고도 재해가 발생해도 시스템은 최대 5분 동안의 데이터를 잃을 수 있습니다.

  참조하다 "복제 계획 만들기" .

- 네트워킹 향상: 복제 계획의 가상 머신 섹션에서 소스와 대상 위치 간의 네트워킹을 매핑할 때 NetApp Disaster Recovery 이제 DHCP 또는 정적 IP의 두 가지 옵션을 제공합니다. 이전에는 DHCP만 지원되었습니다. 고정 IP의 경우 서브넷, 게이트웨이, DNS 서버를 구성합니다. 또한 이제 가상 머신에 대한 자격 증명을 입력할 수 있습니다.

  참조하다 "복제 계획 만들기" .

- 일정 편집: 이제 복제 계획 일정을 업데이트할 수 있습니다.

  참조하다 "리소스 관리" .

- * SnapMirror 자동화*: 이 릴리스에서 복제 계획을 생성하는 동안 다음 구성 중 하나로 소스 볼륨과 대상 볼륨 간의 SnapMirror 관계를 정의할 수 있습니다.
  - 1에서 1까지
  - 팬아웃 아키텍처의 1대다
  - 일관성 그룹으로서 다수 대 1
  - 다대다

    참조하다 "복제 계획 만들기" .

2023년 8월 1일

NetApp Disaster Recovery 미리보기

NetApp Disaster Recovery 미리보기는 재해 복구 워크플로를 자동화하는 클라우드 기반 재해 복구 서비스입니다. NetApp Disaster Recovery 미리 보기를 사용하면 Amazon FSx for ONTAP 을 사용하여 AWS의 VMware Cloud(VMC)에서 NetApp 스토리지를 실행하는 온프레미스 NFS 기반 VMware 워크로드를 보호할 수 있습니다.

> ⓘ 이 미리보기 제공을 통해 NetApp 일반 공급 전에 제공 세부 정보, 내용 및 일정을 수정할 권리가 있습니다.

"NetApp Disaster Recovery 에 대해 자세히 알아보세요".

이 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

부팅 순서에 대한 리소스 그룹 업데이트

재해 복구 또는 복제 계획을 만들 때 가상 머신을 기능적 리소스 그룹에 추가할 수 있습니다. 리소스 그룹을 사용하면 요구 사항을 충족하는 논리적 그룹에 종속된 가상 머신 세트를 넣을 수 있습니다. 예를 들어, 그룹에는 복구 시 실행할 수 있는 부팅 순서가 포함될 수 있습니다. 이 릴리스에서는 각 리소스 그룹에 하나 이상의 가상 머신을 포함할 수 있습니다. 가상 머신은 계획에 포함한 순서에 따라 전원이 켜집니다. 참조하다 "복제할 애플리케이션을 선택하고 리소스 그룹을 할당합니다." .

복제 검증

재해 복구 또는 복제 계획을 만들고 마법사에서 재발을 식별하고 재해 복구 사이트로 복제를 시작하면 30분마다 NetApp Disaster Recovery 복제가 실제로 계획에 따라 발생하는지 확인합니다. 작업 모니터 페이지에서 진행 상황을 모니터링할 수 있습니다. 참조하다 "다른 사이트에 애플리케이션 복제" .

복제 계획은 **RPO(**복구 지점 목표**)** 전송 일정을 보여줍니다**.**

재해 복구 또는 복제 계획을 만들 때 VM을 선택합니다. 이 릴리스에서는 이제 데이터 저장소 또는 VM에 연결된 각 볼륨과 연관된 SnapMirror 볼 수 있습니다. SnapMirror 일정과 연결된 RPO 전송 일정도 볼 수 있습니다. RPO는 재해 발생 후 복구에 백업 일정이 충분한지 여부를 판단하는 데 도움이 됩니다. 참조하다 "복제 계획 만들기" .

작업 모니터 업데이트

이제 작업 모니터 페이지에 새로 고침 옵션이 포함되어 작업의 최신 상태를 확인할 수 있습니다. 참조하다 "재해 복구 작업 모니터링" .

2023년 5월 18일

이는 NetApp Disaster Recovery 의 최초 릴리스입니다.

클라우드 기반 재해 복구 서비스

NetApp Disaster Recovery 재해 복구 워크플로를 자동화하는 클라우드 기반 재해 복구 서비스입니다. NetApp Disaster Recovery 미리 보기를 사용하면 Amazon FSx for ONTAP 을 사용하여 AWS의 VMware Cloud(VMC)에서 NetApp 스토리지를 실행하는 온프레미스 NFS 기반 VMware 워크로드를 보호할 수 있습니다.

"NetApp Disaster Recovery 에 대해 자세히 알아보세요".

NetApp Disaster Recovery 의 제한 사항

알려진 제한 사항은 이 서비스 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 나타냅니다.

검색을 실행하기 전에 장애 복구가 완료될 때까지 기다리십시오**.**

장애 조치가 완료된 후에는 소스 vCenter에서 수동으로 검색을 시작하지 마세요. 장애 복구가 완료될 때까지 기다린 다음 소스 vCenter에서 검색을 시작합니다.

NetApp Console Amazon FSx for NetApp ONTAP 검색하지 못할 수 있습니다**.**

때로는 NetApp Console Amazon FSx for NetApp ONTAP 클러스터를 검색하지 못하는 경우가 있습니다. FSx 자격 증명이 올바르지 않기 때문일 수 있습니다.

해결 방법: NetApp Console 에 Amazon FSx for NetApp ONTAP 클러스터를 추가하고 주기적으로 클러스터를 새로 고쳐 변경 사항을 표시합니다.

NetApp Disaster Recovery 에서 ONTAP FSx 클러스터를 제거해야 하는 경우 다음 단계를 완료하세요.

1. NetApp Console 에이전트에서 클라우드 공급자의 연결 옵션을 사용하고 콘솔 에이전트가 실행되는 Linux VM에 연결하고 다음을 사용하여 "occm" 서비스를 다시 시작합니다. `docker restart occm` 명령.

참조하다 "기존 콘솔 에이전트 관리" .

1. NetApp Console 시스템 페이지에서 Amazon FSx for ONTAP 시스템을 다시 추가하고 FSx 자격 증명을 제공합니다.

참조하다 "Amazon FSx for NetApp ONTAP 만들기" .

2. NetApp Disaster Recovery 에서 사이트*를 선택하고 **vCenter** 행에서 *작업 옵션을 선택합니다.  , 작업 메뉴에서 *새로 고침*을 선택하여 NetApp Disaster Recovery 에서 FSx 검색을 새로 고칩니다.

   이를 통해 데이터 저장소, 가상 머신 및 대상 관계가 다시 검색됩니다.

Google Cloud NetApp Volumes 의 제한 사항

- 장애 조치 테스트를 실행한 후에는 최소 52시간을 기다려야 복제 볼륨이 삭제됩니다. 볼륨을 수동으로 삭제해야 합니다. 52시간 후에 장애 조치를 다시 테스트할 수 있습니다.
- 마운트 작업의 어떤 부분이 실패하면 장애 조치가 성공하지 못하고 작업 시간이 초과됩니다. Google에서 문제를 조사하는 데 최대 3일이 소요되며, 이 기간 동안 vCenter의 모든 데이터 저장소 관련 작업이 차단됩니다.

시작하기

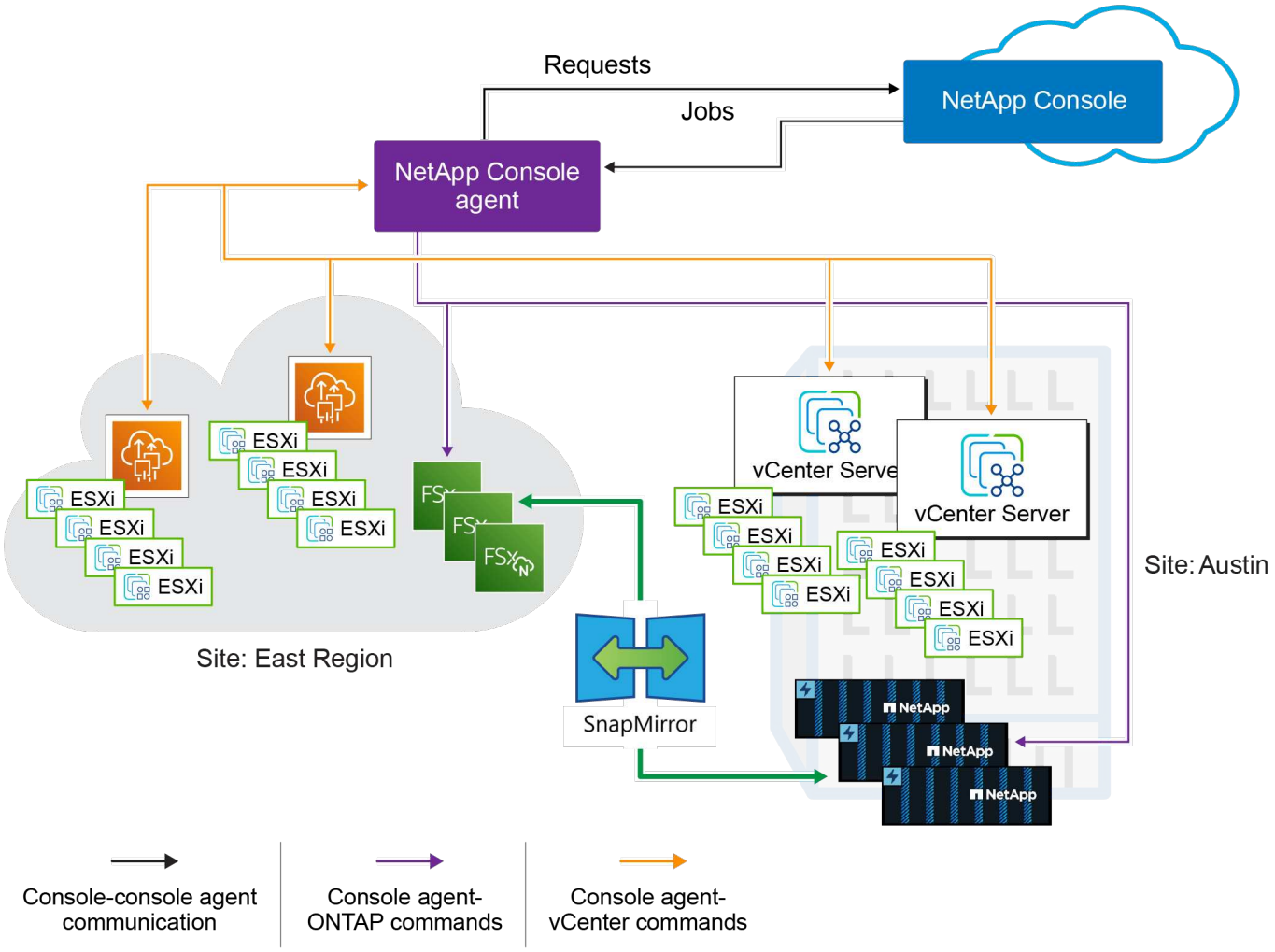
VMware용 NetApp Disaster Recovery 에 대해 알아보세요

클라우드로의 재해 복구는 사이트 중단 및 데이터 손상 사고로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. VMware용 NetApp Disaster Recovery 사용하면 ONTAP 스토리지를 실행하는 온프레미스 VMware VM 또는 데이터스토어 워크로드를 NetApp 클라우드 스토리지를 사용하여 퍼블릭 클라우드의 VMware 소프트웨어 정의 데이터 센터로 복제하거나 ONTAP 스토리지를 사용하는 다른 온프레미스 VMware 환경으로 재해 복구 사이트로 복제할 수 있습니다. 재해 복구를 사용하여 VM 작업 부하를 한 사이트에서 다른 사이트로 마이그레이션할 수도 있습니다.

NetApp Disaster Recovery 재해 복구 워크플로를 자동화하는 클라우드 기반 재해 복구 서비스입니다. NetApp Disaster Recovery 사용하면 온프레미스 NFS 기반 워크로드와 VMware vSphere 가상 머신 파일 시스템(VMFS) 데이터 저장소를 iSCSI 및 FC에서 실행되는 NetApp 스토리지를 다음 중 하나로 보호할 수 있습니다.

- Amazon FSx for NetApp ONTAP 사용한 Amazon Elastic VMware Service(EVS) 자세한 내용은 다음을 참조하세요."Amazon Elastic VMware Service 및 Amazon FSx for NetApp ONTAP 사용한 NetApp Disaster Recovery 소개" .
- Amazon FSx for NetApp ONTAP 사용한 AWS의 VMware Cloud(VMC)
- NetApp Cloud Volumes ONTAP (iSCSI)를 사용한 Azure VMware 솔루션(AVS)(비공개 미리보기)
- Google Cloud NetApp Volumes 사용한 Google Cloud VMware Engine(GCVE)
- ONTAP 스토리지를 갖춘 또 다른 온프레미스 NFS 및/또는 VMFS 기반(iSCSI/FC) VMware 환경

NetApp Disaster Recovery ONTAP SnapMirror 기술과 통합된 기본 VMware 오케스트레이션을 사용하여 VMware VM과 관련 디스크 OS 이미지를 보호하는 동시에 ONTAP 의 모든 스토리지 효율성 이점을 유지합니다. 재해 복구는 이러한 기술을 재해 복구 사이트로의 복제 전송에 사용합니다. 이를 통해 기본 및 보조 사이트에서 업계 최고의 스토리지 효율성(압축 및 중복 제거)이 가능해집니다.



NetApp Console

NetApp Disaster Recovery NetApp Console 통해 액세스할 수 있습니다.

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지 및 데이터 서비스를 중앙에서 관리할 수 있는 기능을 제공합니다. NetApp 데이터 서비스에 액세스하고 사용하려면 콘솔이 필요합니다. 관리 인터페이스로서, 하나의 인터페이스에서 여러 스토리지 리소스를 관리할 수 있습니다. 콘솔 관리자는 기업 내 모든 시스템의 저장소와 서비스에 대한 액세스를 제어할 수 있습니다.

NetApp Console 사용하려면 라이선스나 구독이 필요하지 않으며, 스토리지 시스템이나 NetApp 데이터 서비스에 대한 연결을 보장하기 위해 클라우드에 Console 에이전트를 배포해야 할 때만 요금이 부과됩니다. 그러나 콘솔에서 액세스할 수 있는 일부 NetApp 데이터 서비스는 라이선스 기반이거나 구독 기반입니다.

자세히 알아보세요 "NetApp Console" .

VMware용 NetApp Disaster Recovery 사용의 이점

NetApp Disaster Recovery 다음과 같은 이점을 제공합니다.

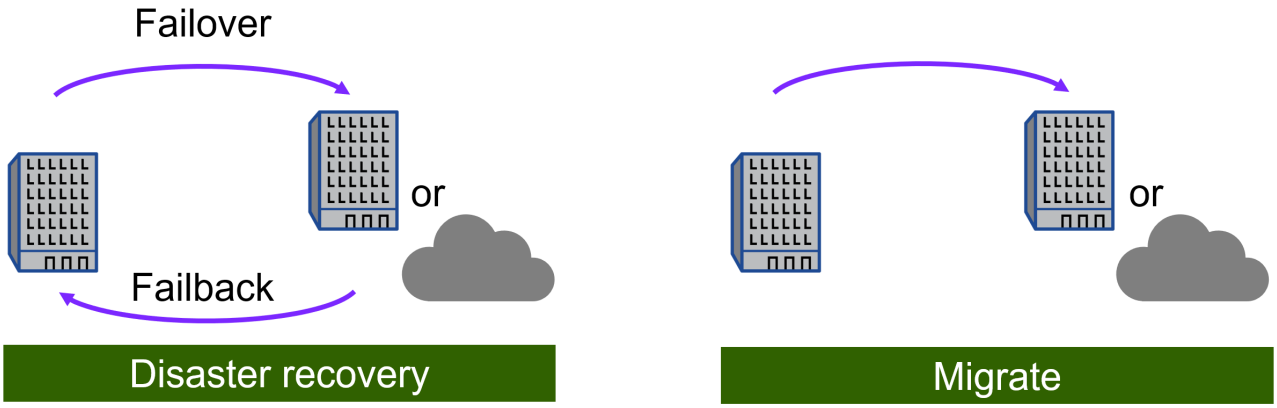
- 여러 시점 복구 작업을 통해 vCenter에서 애플리케이션을 검색하고 복구하는 데 필요한 사용자 환경이 간소화되었습니다.

- 운영 비용이 절감되고 최소한의 리소스로 재해 복구 계획을 수립하고 조정할 수 있어 총 소유 비용이 낮아집니다.
- 운영을 중단시키지 않고 가상 장애 조치 테스트를 통해 지속적인 재해 복구 준비를 갖춥니다. 운영 작업 부하에 영향을 주지 않고 정기적으로 DR 장애 조치 계획을 테스트할 수 있습니다.
- IT 환경의 역동적인 변화에 대응하고 재해 복구 계획에서 이를 해결할 수 있는 능력을 갖춰 가치 실현 시간을 단축하세요.
- 가상 서버 어플라이언스(VSA)를 배포하고 유지 관리할 필요 없이 ONTAP 과 VMware의 백엔드 오케스트레이션을 통해 스토리지와 가상 계층을 동시에 관리할 수 있는 기능입니다.
- VMware용 DR 솔루션은 리소스를 많이 소모할 수 있습니다. 많은 DR 솔루션은 VSA를 사용하여 VMware 가상 계층에서 VM을 복제하는데, 이는 더 많은 컴퓨팅 리소스를 소모하고 ONTAP 의 귀중한 스토리지 효율성을 잃을 수 있습니다. 재해 복구는 ONTAP SnapMirror 기술을 사용하므로 ONTAP 의 모든 기본 데이터 압축 및 중복 제거 효율성을 갖춘 증분형 영구 복제 모델을 사용하여 프로덕션 데이터 저장소에서 재해 복구 사이트로 데이터를 복제할 수 있습니다.

VMware용 NetApp Disaster Recovery 로 할 수 있는 일

NetApp Disaster Recovery 사용하면 다음과 같은 목표를 달성하기 위해 여러 NetApp 기술을 최대한 활용할 수 있습니다.

- SnapMirror 복제를 사용하여 온프레미스 프로덕션 사이트의 VMware 앱을 클라우드 또는 온프레미스의 재해 복구 원격 사이트로 복제합니다.
- VMware 워크로드를 원래 사이트에서 다른 사이트로 마이그레이션합니다.
- 장애 조치 테스트를 수행합니다. 이렇게 하면 서비스가 임시 가상 머신을 생성합니다. 재해 복구는 선택된 스냅샷에서 새로운 FlexClone 볼륨을 만들고, FlexClone 볼륨에 의해 백업되는 임시 데이터 저장소를 ESXi 호스트에 매핑합니다. 이 프로세스는 온프레미스 ONTAP 스토리지나 AWS의 FSx for NetApp ONTAP 스토리지에서 추가적인 물리적 용량을 소모하지 않습니다. 원본 소스 볼륨은 수정되지 않으며 재해 복구 중에도 복제 작업을 계속할 수 있습니다.
- 재해 발생 시 필요에 따라 기본 사이트를 재해 복구 사이트로 장애 조치할 수 있습니다. 재해 복구 사이트는 Amazon FSx for NetApp ONTAP 이 포함된 AWS의 VMware Cloud 또는 ONTAP 포함된 온프레미스 VMware 환경입니다.
- 재해가 해결된 후 재해 복구 사이트에서 기본 사이트로 필요에 따라 장애 복구합니다.
- 효율적인 관리를 위해 VM이나 데이터 저장소를 논리적 리소스 그룹으로 그룹화합니다.



vSphere 서버 구성은 vSphere Server의 NetApp Disaster Recovery 외부에서 수행됩니다.

비용

NetApp NetApp Disaster Recovery 평가판 사용에 대해 요금을 청구하지 않습니다.

NetApp Disaster Recovery NetApp 라이선스 또는 Amazon Web Services를 통한 연간 구독 기반 플랜을 통해 사용할 수 있습니다.

일부 릴리스에는 기술 미리보기가 포함되어 있습니다. NetApp 미리 본 워크로드 용량에 대해서는 요금을 청구하지 않습니다. 보다"NetApp Disaster Recovery 의 새로운 기능" 최신 기술 미리보기에 대한 정보를 확인하세요.

라이센스

다음 라이선스 유형을 사용할 수 있습니다.

- 30일 무료 체험판에 등록하세요.
- Amazon Web Services(AWS) Marketplace 또는 Microsoft Azure Marketplace에서 사용량에 따라 지불하는(PAYGO) 구독을 구매하세요. 이 라이선스를 사용하면 장기 약정 없이 고정 보호 용량 라이선스를 구매할 수 있습니다.
- BYOL(Bring Your Own License)은 NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)입니다. NetApp Console 에서 라이선스 일련 번호를 사용하여 BYOL을 활성화할 수 있습니다.

모든 NetApp 데이터 서비스에 대한 라이선스는 NetApp Console 의 구독을 통해 관리됩니다. BYOL을 설정한 후 콘솔에서 해당 서비스에 대한 활성 라이선스를 볼 수 있습니다.

이 서비스는 보호된 ONTAP 볼륨에 호스팅된 데이터 양을 기준으로 라이센스가 부여됩니다. 이 서비스는 보호된 VM을 해당 vCenter 데이터 저장소에 매핑하여 어떤 볼륨을 라이선싱 목적으로 고려해야 하는지 결정합니다. 각 데이터스토어는 ONTAP 볼륨이나 LUN에 호스팅됩니다. ONTAP 에서 해당 볼륨이나 LUN에 대해 보고한 사용 용량은 라이선스 결정에 사용됩니다.

보호된 볼륨은 여러 개의 VM을 호스팅할 수 있습니다. 일부는 NetApp Disaster Recovery 리소스 그룹에 속하지 않을 수도 있습니다. 그럼에도 불구하고 해당 볼륨이나 LUN의 모든 VM이 사용하는 저장 용량은 라이선스 최대 용량에 포함됩니다.

NetApp Disaster Recovery 요금은 복제 계획이 있는 VM이 하나 이상 있는 경우 소스 사이트의 데이터 저장소 사용 용량을 기준으로 부과됩니다. 장애 조치된 데이터 저장소의 용량은 용량 허용량에 포함되지 않습니다. BYOL의 경우, 데이터가 허용된 용량을 초과하면 NetApp Console 에서 추가 용량 라이선스를 얻거나 라이선스를 업그레이드할 때까지 서비스 작업이 제한됩니다.

NetApp Disaster Recovery 에 대한 라이선싱 설정에 대한 자세한 내용은 다음을 참조하세요."NetApp Disaster Recovery 라이선스 설정" .

30일 무료 체험

30일 무료 평가판을 통해 NetApp Disaster Recovery 체험해 보세요.

30일 평가판 사용 기간이 끝난 후 계속 사용하려면 클라우드 공급업체에서 PAYGO(Pay-as-you-go) 구독을 받거나

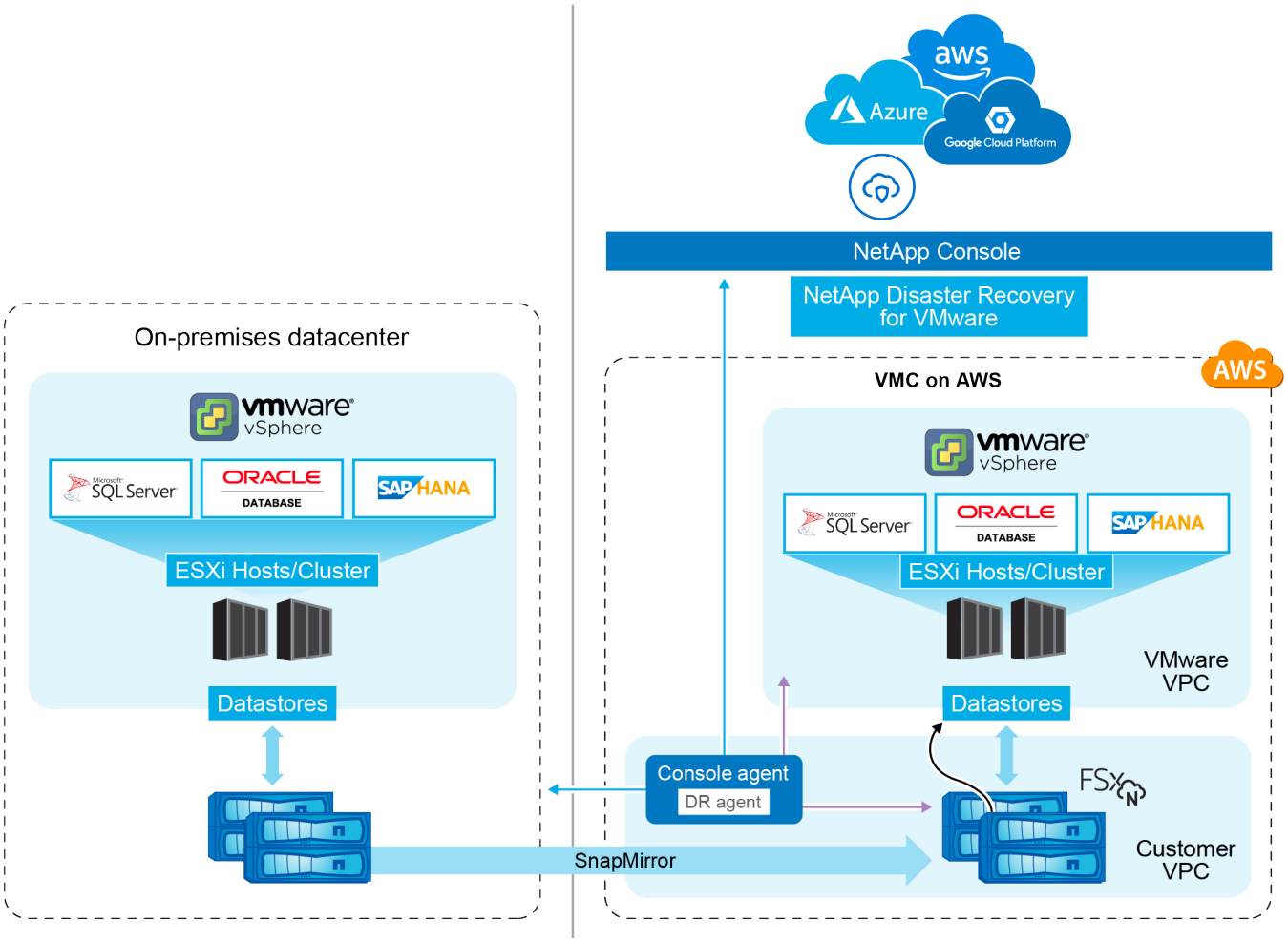
NetApp 에서 BYOL 라이선스를 구매해야 합니다.

언제든지 라이선스를 구매할 수 있으며, 30일 평가판이 종료될 때까지 요금이 청구되지 않습니다.

NetApp Disaster Recovery 작동 방식

NetApp Disaster Recovery NetApp Console 소프트웨어 서비스(SaaS) 환경 내에서 호스팅되는 서비스입니다. 재해 복구는 온프레미스 사이트에서 Amazon FSx for ONTAP 또는 다른 온프레미스 사이트로 복제된 워크로드를 복구할 수 있습니다. 이 서비스는 SnapMirror 수준에서 VMware Cloud on AWS에 가상 머신을 등록하고, VMware 네트워크 가상화 및 보안 플랫폼인 NSX-T에서 직접 네트워크 매핑을 통해 복구를 자동화합니다. 이 기능은 모든 Virtual Machine Cloud 환경에 포함되어 있습니다.

NetApp Disaster Recovery ONTAP SnapMirror 기술을 사용하여 매우 효율적인 복제를 제공하고 ONTAP 증분형 영구 스냅샷 효율성을 보존합니다. SnapMirror 복제는 애플리케이션과 일관된 스냅샷 복사본이 항상 동기화되고 장애 조치 직후에 데이터를 즉시 사용할 수 있도록 보장합니다.



재해가 발생하면 이 서비스는 SnapMirror 관계를 끊고 대상 사이트를 활성화하여 다른 온프레미스 VMware 환경이나 VMC에 있는 가상 머신을 복구하는 데 도움을 줍니다.

- 이 서비스를 사용하면 가상 머신을 원래 소스 위치로 복구할 수도 있습니다.
- 원래 가상 머신을 방해하지 않고 재해 복구 장애 조치 프로세스를 테스트할 수 있습니다. 이 테스트는 볼륨의 FlexClone 생성하여 가상 머신을 격리된 네트워크로 복구합니다.

- 장애 조치 또는 테스트 장애 조치 프로세스의 경우 가상 머신을 복구할 최신(기본값) 스냅샷이나 선택한 스냅샷을 선택할 수 있습니다.

재해 복구의 구성 요소

재해 복구는 다음 구성 요소를 사용하여 VMware 워크로드에 대한 재해 복구를 제공합니다.

- * NetApp Console*: 재해 복구 계획을 관리하기 위한 사용자 인터페이스입니다. NetApp Console 사용하면 온프레미스 및 클라우드 환경 전반에서 복제 계획, 리소스 그룹 및 장애 조치 작업을 만들고 관리할 수 있습니다.
- 콘솔 에이전트: 클라우드 호스팅 네트워크나 온프레미스 VMware 환경에서 실행되는 가벼운 소프트웨어 구성 요소입니다. NetApp Console 과 통신하고 온프레미스 환경과 재해 복구 사이트 간의 데이터 복제를 관리합니다. 콘솔 에이전트는 VMware 환경의 가상 머신에 설치됩니다.
- * ONTAP 스토리지 클러스터*: ONTAP 스토리지 클러스터는 VMware 워크로드를 호스팅하는 기본 스토리지 시스템입니다. ONTAP 스토리지 클러스터는 재해 복구 계획을 위한 기본 스토리지 인프라를 제공합니다. 재해 복구는 ONTAP 스토리지 API를 사용하여 온프레미스 어레이와 Amazon FSx for NetApp ONTAP 과 같은 클라우드 기반 솔루션과 ONTAP 스토리지 클러스터를 관리합니다.
- **vCenter** 서버: VMware vCenter는 VMware 환경을 위한 관리 서버입니다. ESXi 호스트와 관련 데이터 저장소를 관리합니다. 콘솔 에이전트는 VMware vCenter와 통신하여 온프레미스 환경과 재해 복구 사이트 간의 데이터 복제를 관리합니다. 여기에는 ONTAP LUN 및 볼륨을 데이터 저장소로 등록하고, VM을 재구성하고, VM을 시작 및 중지하는 작업이 포함됩니다.

재해 복구 보호 워크플로

복제 계획이 리소스 그룹에 할당되면 재해 복구는 리소스 그룹과 계획의 모든 구성 요소에 대한 검색 검사를 수행하여 계획을 활성화할 수 있는지 확인합니다.

이 검사가 성공하면 재해 복구는 다음 초기화 단계를 수행합니다.

1. 대상 리소스 그룹의 각 VM에 대해 호스팅 VMware 데이터 저장소를 식별합니다.
2. 발견된 각 VMware 데이터스토어에 대해 호스팅 ONTAP FlexVol volume 이나 LUN을 식별합니다.
3. 발견된 각 ONTAP 볼륨과 LUN에 대해 소스 볼륨과 대상 사이트의 대상 볼륨 사이에 기존 SnapMirror 관계가 있는지 확인합니다.
    a. 기존 SnapMirror 관계가 없는 경우 새 대상 볼륨을 만들고 보호되지 않은 각 소스 볼륨 간에 새 SnapMirror 관계를 만듭니다.
    b. 기존 SnapMirror 관계가 있는 경우 해당 관계를 사용하여 모든 복제 작업을 수행합니다.

재해 복구가 모든 관계를 생성하고 초기화한 후, 서비스는 예약된 각 백업에서 다음과 같은 데이터 보호 단계를 수행합니다.

1. "애플리케이션 일관성"으로 표시된 각 VM에 대해 VMtools를 사용하여 지원되는 애플리케이션을 백업 상태로 전환합니다.
2. 보호된 VMware 데이터스토어를 호스팅하는 모든 ONTAP 볼륨의 새 스냅샷을 만듭니다.
3. SnapMirror 업데이트 작업을 수행하여 해당 스냅샷을 대상 ONTAP 클러스터에 복제합니다.
4. 보존된 스냅샷 수가 복제 계획에 정의된 최대 스냅샷 보존 기간을 초과했는지 확인하고 소스 및 대상 볼륨에서 불필요한 스냅샷을 삭제합니다.

지원되는 보호 대상 및 데이터 저장소 유형

지원되는 데이터 저장소 유형 NetApp Disaster Recovery 다음 데이터 저장소 유형을 지원합니다.

- ONTAP 클러스터에 있는 ONTAP FlexVol 볼륨에 호스팅된 NFS 데이터 저장소입니다.
- iSCSI 또는 FC 프로토콜을 사용하는 VMware vSphere 가상 머신 파일 시스템(VMFS) 데이터 저장소

지원되는 보호 대상

- Amazon FSx for NetApp ONTAP 사용한 AWS의 VMware Cloud(VMC)
- ONTAP 스토리지 또는 온프레미스 FC/iSCSI VMSF를 갖춘 또 다른 온프레미스 NFS 기반 VMware 환경
- Amazon Elastic VMware 서비스
- NetApp Cloud Volumes ONTAP (iSCSI)를 사용한 Azure VMware 솔루션(AVS)(비공개 미리보기)
- Google Cloud NetApp Volumes 사용한 Google Cloud VMware Engine(GCVE)

NetApp Disaster Recovery 에 도움이 될 수 있는 용어

재해 복구와 관련된 용어를 이해하면 도움이 될 수 있습니다.

- 데이터 저장소: VMDK 파일을 보관하기 위해 파일 시스템을 사용하는 VMware vCenter 데이터 컨테이너입니다. 일반적인 데이터 저장소 유형은 NFS, VMFS, vSAN 또는 vVol입니다. 재해 복구는 NFS 및 VMFS 데이터 저장소를 지원합니다. 각 VMware 데이터스토어는 단일 ONTAP 볼륨 또는 LUN에 호스팅됩니다. 재해 복구는 ONTAP 클러스터에 있는 FlexVol 볼륨에 호스팅된 NFS 및 VMFS 데이터 저장소를 지원합니다.
- 복제 계획: 백업이 발생하는 빈도와 장애 조치 이벤트를 처리하는 방법에 대한 일련의 규칙입니다. 계획은 하나 이상의 리소스 그룹에 할당됩니다.
- 복구 지점 목표**(RPO)**: 재해 발생 시 허용되는 최대 데이터 손실량입니다. RPO는 복제 계획의 데이터 복제 빈도 또는 복제 일정에 정의됩니다.
- 복구 시간 목표**(RTO)**: 재해로부터 복구하는 데 허용되는 최대 시간입니다. RTO는 복제 계획에 정의되어 있으며, DR 사이트로 장애 조치하고 모든 VM을 다시 시작하는 데 걸리는 시간입니다.
- 리소스 그룹: 여러 VM을 단일 단위로 관리할 수 있는 논리적 컨테이너입니다. VM은 한 번에 하나의 리소스 그룹에만 속할 수 있습니다. 보호하려는 각 애플리케이션이나 작업 부하에 대해 리소스 그룹을 만들 수 있습니다.
- 사이트: 일반적으로 하나 이상의 vCenter 클러스터와 ONTAP 스토리지를 호스팅하는 물리적 데이터 센터 또는 클라우드 위치와 연결된 논리적 컨테이너입니다.

NetApp Disaster Recovery 필수 구성 요소

NetApp Disaster Recovery 사용하기 전에 해당 환경이 ONTAP 스토리지, VMware vCenter 클러스터 및 NetApp Console 요구 사항을 충족하는지 확인하세요.

소프트웨어 버전

요소	최소 버전
Amazon FSx for NetApp ONTAP	사용 가능한 최신 버전

요소	최소 버전
Google Google Cloud NetApp Volumes 사용하는 Google Cloud VMware Engine	사용 가능한 최신 버전
ONTAP 소프트웨어	ONTAP 9.10.0 이상
AWS용 VMware 클라우드	사용 가능한 최신 버전
VMware 온프레미스 vCenter	7.0u3 이상

Google Cloud 필수 구성 요소 및 고려 사항

Google Cloud NetApp Volumes 사용하여 Google Cloud VMware Engine에서 재해 복구를 수행하는 경우 올바른 권한을 구성하고 언급된 고려 사항을 준수해야 합니다.

- Google SRE 팀에 문의하여 다음을 허용 목록에 추가하세요.
  - 온프레미스 스토리지에서 Google Cloud NetApp Volumes 로 스냅샷을 전송하는 동기화 API입니다.
  - 데이터 저장소를 만들고, 마운트하고, 마운트 해제하기 위한 VMware 엔진을 갖춘 Google 프로젝트입니다.
- 당신은해야합니다"볼륨 하이브리드 복제 허용 목록에 대한 요청을 제출하세요." .
- 주의하세요"Google Cloud NetApp Volumes 할당량 및 제한" .
- 복제 계획에는 볼륨이나 데이터 저장소를 하나만 추가할 수 있습니다.
- 검토하다"제한 사항" .

장애 조치 고려 사항

- 장애 조치는 최신 스냅샷을 사용해서만 지원됩니다. 필요한 경우 장애 조치 중에 새 스냅샷을 생성할 수 있습니다(즉, 선택적 스냅샷 옵션을 비활성화해야 합니다).
- 장애 조치 후에는 새로운 스냅샷을 만들 수 없습니다.
- 장애 조치 후에는 스냅샷을 보관하고 조정할 수 없습니다.

장애 복구 고려 사항

- 장애 복구는 선택적 스냅샷 옵션을 통해서만 가능합니다. 새로운 스냅샷을 찍어서 장애 복구를 수행할 수 없습니다.
- 온프레미스 스토리지와 Google Cloud NetApp Volumes 스토리지 클러스터 간의 클러스터 피어링을 제거하는 경우 온프레미스 클러스터에서 클러스터 및 스토리지 VM 피어링 항목을 수동으로 지워야 합니다. 자세한 내용은 다음을 참조하세요. "vserver 피어 관계 삭제".

Google Cloud 권한

Google Cloud의 서비스 주체에는 다음 역할이나 동등한 권한이 할당되어야 합니다.

- "컴퓨팅 관리자 역할"
- "NetApp Console 에 대한 Google Cloud 권한"
- "Google Cloud NetApp Volumes 관리자"

- "VMware Engine 서비스 관리자"

NetApp Console 권한

NetApp Console 사용자는 다음과 같은 역할을 가져야 합니다.

- "Google Cloud NetApp Volumes 관리자"
- "SnapCenter 관리자"
- "재해 복구 장애 조치 관리자"

ONTAP 스토리지 전제 조건

이러한 필수 구성 요소는 NetApp ONTAP 인스턴스의 ONTAP 또는 Amazon FSX에 적용됩니다.

- 소스 클러스터와 대상 클러스터는 피어 관계가 있어야 합니다.
- 재해 복구 볼륨을 호스팅하는 SVM은 대상 클러스터에 있어야 합니다.
- 소스 SVM과 대상 SVM은 피어 관계가 있어야 합니다.
- Amazon FSx for NetApp ONTAP 사용하여 배포하는 경우 다음 필수 조건이 적용됩니다.
  - VMware DR 데이터 저장소를 호스팅하려면 Amazon FSx for NetApp ONTAP 인스턴스가 VPC에 있어야 합니다. 시작하려면 다음을 참조하세요."Amazon FSx for ONTAP 설명서" .

VMware vCenter 클러스터 필수 구성 요소

이러한 필수 구성 요소는 온프레미스 vCenter 클러스터와 VMware Cloud for AWS 소프트웨어 정의 데이터 센터(SDDC)에 모두 적용됩니다.

- 검토"vCenter 권한" NetApp Disaster Recovery 에 필요합니다.
- NetApp Disaster Recovery 관리하려는 모든 VMware 클러스터는 ONTAP 볼륨을 사용하여 보호하려는 모든 VM을 호스팅합니다.
- NetApp Disaster Recovery 에서 관리하는 모든 VMware 데이터 저장소는 다음 프로토콜 중 하나를 사용해야 합니다.
  - NFS
  - iSCSI 또는 FC 프로토콜을 사용하는 VMFS
- VMware vSphere 버전 7.0 업데이트 3(7.0v3) 이상
- VMware Cloud SDDC를 사용하는 경우 다음 필수 구성 요소가 적용됩니다.
  - VMware Cloud Console에서 관리자 및 NSX Cloud 관리자 서비스 역할을 사용하세요. 조직 역할에는 조직 소유자도 사용합니다. 참조하다 "AWS FSx for NetApp ONTAP 설명서와 함께 VMware Cloud Foundations 사용" .
  - VMware Cloud SDDC를 Amazon FSx for NetApp ONTAP 인스턴스와 연결합니다. 참조하다 "Amazon FSx for NetApp ONTAP 배포 정보와 AWS의 VMware Cloud 통합" .

NetApp Console 필수 구성 요소

NetApp Console 시작하기

아직 하지 않았다면, "NetApp Console 에 가입하고 조직을 만드세요" .

ONTAP 및 VMware에 대한 자격 증명 수집

- Amazon FSx for ONTAP 및 AWS 자격 증명은 NetApp Disaster Recovery 관리하는 NetApp Console 프로젝트 내의 시스템에 추가되어야 합니다.
- NetApp Disaster Recovery vCenter 자격 증명이 필요합니다. NetApp Disaster Recovery 에 사이트를 추가할 때 vCenter 자격 증명을 입력합니다.

  필요한 vCenter 권한 목록은 다음을 참조하세요."NetApp Disaster Recovery 에 필요한 vCenter 권한" . 사이트를 추가하는 방법에 대한 지침은 다음을 참조하세요."사이트 추가" .

NetApp Console 에이전트 만들기

콘솔 에이전트는 콘솔이 ONTAP 스토리지 및 VMware vCenter 클러스터와 통신할 수 있도록 하는 소프트웨어 구성 요소입니다. 재해 복구가 제대로 작동하려면 이것이 필요합니다. 에이전트는 개인 네트워크(온프레미스 데이터 센터 또는 클라우드 VPC)에 상주하며 ONTAP 스토리지 인스턴스와 추가 서버 및 애플리케이션 구성 요소와 통신합니다. 재해 복구의 경우 이는 관리되는 vCenter 클러스터에 대한 액세스입니다.

NetApp Console 에 콘솔 에이전트를 설정해야 합니다. 에이전트를 사용하면 재해 복구 서비스에 적합한 기능이 포함됩니다.

- NetApp Disaster Recovery 표준 모드 에이전트 배포에서만 작동합니다. 보다 "표준 모드에서 NetApp Console 시작하기" .
- 원본 및 대상 vCenter 클러스터 모두 동일한 Console 에이전트를 사용하도록 하십시오.
- 필요한 콘솔 에이전트 유형:
  - 온프레미스 간 재해 복구: 재해 복구 사이트에 온프레미스 Console 에이전트를 설치합니다. 이 방법을 사용하면 기본 사이트에 장애가 발생하더라도 DR 사이트에서 가상 리소스를 다시 시작하는 서비스가 중단되지 않습니다. 을 참조하십시오 "온프레미스에 콘솔 에이전트 설치 및 설정".

    재해 복구는 온프레미스 구성을 사용하는 여러 콘솔 에이전트도 지원합니다. 이 시나리오에서 콘솔 에이전트는 vCenter 및 ONTAP 어레이 클러스터에 대한 작업을 지시하며, 소스와 대상 각각에 자체 콘솔 에이전트가 있습니다. 콘솔 에이전트 또는 사이트 장애 발생 시 지연 시간을 줄이고 복구 시간을 단축하려면 여러 콘솔 에이전트를 사용하는 것이 좋습니다.

  - 온프레미스에서 **AWS**로: AWS VPC에 AWS용 콘솔 에이전트를 설치합니다. 참조하다 "AWS의 콘솔 에이전트 설치 옵션" .

    온프레미스 간 연결의 경우 온프레미스 콘솔 에이전트를 사용하세요. 온프레미스에서 AWS로 이동하는 경우 소스 온프레미스 vCenter와 대상 온프레미스 vCenter에 액세스할 수 있는 AWS 콘솔 에이전트를 사용합니다.

  - 설치된 콘솔 에이전트는 재해 복구에서 관리할 vCenter 클러스터에서 관리하는 모든 VMware vCenter 클러스터 인스턴스와 ESXi 호스트에 액세스할 수 있어야 합니다.
- NetApp Disaster Recovery 에서 관리할 모든 ONTAP 어레이는 NetApp Disaster Recovery 관리하는 데 사용될 NetApp Console 프로젝트 내의 모든 시스템에 추가되어야 합니다.

보다 "온프레미스 ONTAP 클러스터를 찾아보세요" .

- NetApp Disaster Recovery 위한 지능형 프록시 설정에 대한 자세한 내용은 다음을 참조하세요."NetApp Disaster Recovery 위한 인프라 설정" .

작업량 전제 조건

애플리케이션 일관성 프로세스가 성공적으로 수행되도록 하려면 다음 전제 조건을 적용하세요.

- 보호할 VM에서 VMware 도구(또는 Open VM 도구)가 실행 중인지 확인하세요.
- Microsoft SQL Server, Oracle Database 또는 둘 다를 실행하는 Windows VM의 경우, 데이터베이스에서 VSS 작성기를 활성화해야 합니다.
- Linux 운영 체제에서 실행되는 Oracle 데이터베이스의 경우 Oracle 데이터베이스 SYSDBA 역할에 대해 운영 체제 사용자 인증이 활성화되어 있어야 합니다.

더 많은 정보

- 필요한 vCenter 권한
- NetApp Disaster Recovery 지원하는 Amazon EVS의 필수 구성 요소

NetApp Disaster Recovery 위한 빠른 시작

NetApp Disaster Recovery 시작하는 데 필요한 단계에 대한 개요는 다음과 같습니다. 각 단계 내의 링크를 클릭하면 자세한 내용을 제공하는 페이지로 이동합니다.


필수 조건 검토

"시스템이 이러한 요구 사항을 충족하는지 확인하세요." .


NetApp Disaster Recovery 설정

- "서비스를 위한 인프라를 구축하세요" .
- "라이센스 설정" .


다음은 무엇인가요**?**

서비스를 설정한 후에는 다음 작업을 수행하세요.

- "NetApp Disaster Recovery 에 vCenter 사이트 추가" .
- "첫 번째 리소스 그룹을 만드세요" .
- "첫 번째 복제 계획을 만드세요" .
- "다른 사이트에 애플리케이션 복제" .
- "원격 사이트로 애플리케이션 장애 조치" .

- "원래 소스 사이트로 애플리케이션을 다시 장애 조치합니다." .
- "사이트, 리소스 그룹 및 복제 계획 관리" .
- "재해 복구 작업 모니터링" .

NetApp Disaster Recovery 위한 인프라 설정

NetApp Disaster Recovery 사용하려면 Amazon Web Services(AWS)와 NetApp Console에서 몇 가지 단계를 수행하여 설정해야 합니다.

검토"전제 조건" 시스템이 준비되었는지 확인하세요.

다음 인프라에서 NetApp Disaster Recovery 사용할 수 있습니다.

- 온프레미스 VMware 플러스 ONTAP 데이터 센터를 VMware Cloud on AWS 및 Amazon FSx for NetApp ONTAP 기반 AWS DR 인프라로 복제하는 하이브리드 클라우드 DR입니다.
- 온프레미스 VMware와 ONTAP vCenter를 다른 온프레미스 VMware와 ONTAP vCenter로 복제하는 프라이빗 클라우드 DR입니다.

Amazon FSx for NetApp ONTAP 활용한 하이브리드 클라우드

이 방법은 NFS 프로토콜을 사용하여 ONTAP FlexVol 볼륨에 호스팅된 데이터 저장소를 사용하는 온프레미스 프로덕션 vCenter 인프라로 구성됩니다. DR 사이트는 NFS 프로토콜을 사용하는 하나 이상의 FSx for ONTAP 인스턴스에서 제공하는 FlexVol 볼륨에 호스팅된 데이터 저장소를 사용하는 하나 이상의 VMware Cloud SDDC 인스턴스로 구성됩니다.

프로덕션 사이트와 DR 사이트는 AWS 호환 보안 연결을 통해 연결됩니다. 일반적인 연결 유형은 보안 VPN(개인 또는 AWS 제공), AWS Direct Connect 또는 기타 승인된 상호 연결 방법입니다.

AWS 클라우드 인프라와 관련된 재해 복구의 경우 AWS용 콘솔 에이전트를 사용해야 합니다. 에이전트는 FSx for ONTAP 인스턴스와 동일한 VPC에 설치해야 합니다. 다른 VPC에 추가 FSx for ONTAP 인스턴스가 배포된 경우, 에이전트를 호스팅하는 VPC는 다른 VPC에 액세스할 수 있어야 합니다.

AWS 가용성 영역

AWS는 특정 지역 내의 하나 이상의 가용성 영역(AZ)에 솔루션을 배포하는 것을 지원합니다. 재해 복구는 AWS에서 호스팅하는 두 가지 서비스인 VMware Cloud for AWS와 AWS FSx for NetApp ONTAP 사용합니다.

- **AWS용 VMware Cloud**: 단일 AZ 또는 이중 AZ 스트레치 클러스터 SDDC 환경에서의 배포를 지원합니다. 재해 복구는 Amazon VMware Cloud for AWS에 대해서만 단일 AZ SDDC 배포를 지원합니다.
- * NetApp ONTAP 용 AWS FSx*: 듀얼 AZ 구성으로 배포하는 경우 각 볼륨은 단일 FSx 시스템이 소유합니다. 각 볼륨은 단일 FSx 시스템이 소유합니다. 볼륨의 데이터는 두 번째 FSx 시스템에 미러링됩니다. FSx for ONTAP 시스템은 단일 또는 이중 AZ 배포로 구축할 수 있습니다. 재해 복구는 FSx for ONTAP 배포를 위한 단일 및 다중 AZ FSx를 모두 지원합니다.

모범 사례: AWS DR 사이트 구성의 경우 NetApp VMware Cloud와 AWS FSx for ONTAP 인스턴스 모두에 단일 AZ 배포를 사용할 것을 권장합니다. AWS를 DR에 사용하기 때문에 여러 AZ를 도입하는 데 이점이 없습니다. 다중 AZ는 비용과 복잡성을 증가시킬 수 있습니다.

온프레미스에서 **AWS**로

AWS는 프라이빗 데이터 센터를 AWS 클라우드에 연결하기 위해 다음과 같은 방법을 제공합니다. 각 솔루션에는 이점과 비용 고려사항이 있습니다.

- **AWS Direct Connect**: 이는 AWS 파트너가 제공하는, 귀하의 개인 데이터 센터와 동일한 지리적 영역에 위치한 AWS 클라우드 상호 연결입니다. 이 솔루션은 공용 인터넷 연결이 필요 없이 로컬 데이터 센터와 AWS 클라우드 간에 안전하고 개인적인 연결을 제공합니다. 이는 AWS가 제공하는 가장 직접적이고 효율적인 연결 방법입니다.
- **AWS** 인터넷 게이트웨이: AWS 클라우드 리소스와 외부 컴퓨팅 리소스 간의 공용 연결을 제공합니다. 이러한 유형의 연결은 일반적으로 보안이 필요하지 않은 HTTP/HTTPS 서비스와 같이 외부 고객에게 서비스를 제공하는 데 사용됩니다. 서비스 품질 제어, 보안, 연결 보장이 없습니다. 이러한 이유로 이 연결 방법은 프로덕션 데이터 센터를 클라우드에 연결하는 데 권장되지 않습니다.
- **AWS** 사이트 간 **VPN**: 이 가상 사설망 연결은 공용 인터넷 서비스 제공자와 함께 안전한 액세스 연결을 제공하는 데 사용할 수 있습니다. VPN은 AWS 클라우드에서 송수신되는 모든 데이터를 암호화하고 복호화합니다. VPN은 소프트웨어 기반이거나 하드웨어 기반일 수 있습니다. 기업용 애플리케이션의 경우, 공용 인터넷 서비스 제공자(ISP)는 DR 복제에 적절한 대역폭과 지연 시간이 제공되도록 서비스 품질을 보장해야 합니다.

모범 사례: AWS DR 사이트 구성의 경우 NetApp AWS Direct Connect를 사용할 것을 권장합니다. 이 솔루션은 엔터프라이즈 애플리케이션에 최고의 성능과 보안을 제공합니다. 사용할 수 없는 경우 VPN과 함께 고성능 공용 ISP 연결을 사용해야 합니다. ISP가 적절한 네트워크 성능을 보장하기 위해 상용 QoS 서비스 수준을 제공하는지 확인하세요.

VPC 간 상호 연결

AWS는 다음과 같은 유형의 VPC-VPC 상호연결을 제공합니다. 각 솔루션에는 이점과 비용 고려사항이 있습니다.

- **VPC** 피어링: 두 VPC 간의 개인 연결입니다. 이는 AWS가 제공하는 가장 직접적이고 효율적인 연결 방법입니다. VPC 피어링은 동일하거나 다른 AWS 지역에 있는 VPC를 연결하는 데 사용할 수 있습니다.
- **AWS** 인터넷 게이트웨이: 일반적으로 AWS VPC 리소스와 비 AWS 리소스 및 엔드포인트 간의 연결을 제공하는 데 사용됩니다. 모든 트래픽은 "헤어핀" 경로를 따릅니다. 즉, 다른 VPC로 향하는 VPC 트래픽은 인터넷 게이트웨이를 통해 AWS 인프라를 빠져나와 동일하거나 다른 게이트웨이를 통해 AWS 인프라로 돌아갑니다. 이는 엔터프라이즈 VMware 솔루션에 적합한 VPC 연결 유형이 아닙니다.
- **AWS Transit Gateway**: 이는 각 VPC가 단일 중앙 게이트웨이에 연결될 수 있도록 하는 중앙 집중식 라우터 기반 연결 유형으로, 이 게이트웨이는 모든 VPC 간 트래픽에 대한 중앙 허브 역할을 합니다. 이를 VPN 솔루션에 연결하여 온프레미스 데이터 센터 리소스가 AWS VPC 호스팅 리소스에 액세스할 수 있도록 할 수도 있습니다. 이러한 유형의 연결을 구현하려면 일반적으로 추가 비용이 필요합니다.

모범 사례: VMware Cloud와 단일 FSx for ONTAP VPC를 포함하는 DR 솔루션의 경우 NetApp VPC 피어 연결을 사용할 것을 권장합니다. 여러 FSx for ONTAP VPC가 배포된 경우 여러 VPC 피어 연결의 관리 오버헤드를 줄이기 위해 AWS Transit Gateway를 사용하는 것이 좋습니다.

AWS를 사용하여 온프레미스에서 클라우드로의 보호를 준비하세요

AWS를 사용하여 온프레미스에서 클라우드로의 보호를 위한 NetApp Disaster Recovery 설정하려면 다음을 설정해야 합니다.

- NetApp ONTAP 용 AWS FSx 설정
- AWS SDDC에 VMware Cloud 설정

NetApp ONTAP 용 AWS FSx 설정

- Amazon FSx for NetApp ONTAP 파일 시스템을 만듭니다.
  - ONTAP 에 대한 FSx를 프로비저닝하고 구성합니다. Amazon FSx for NetApp ONTAP NetApp ONTAP 파일 시스템을 기반으로 높은 안정성, 확장성, 고성능, 다양한 기능을 갖춘 파일 스토리지를 제공하는 완전 관리형 서비스입니다.
  - 다음 단계를 따르세요 "기술 보고서 4938: VMware Cloud on AWS를 사용하여 Amazon FSx ONTAP NFS 데이터 저장소로 마운트" 그리고 "Amazon FSx for NetApp ONTAP 빠른 시작" FSx for ONTAP 프로비저닝하고 구성합니다.
- 시스템에 Amazon FSx for ONTAP 을 추가하고 FSx for ONTAP 에 대한 AWS 자격 증명을 추가합니다.
- AWS FSx for ONTAP 인스턴스에서 대상 ONTAP SVM을 생성하거나 확인합니다.
- NetApp Console 에서 소스 온프레미스 ONTAP 클러스터와 FSx for ONTAP 인스턴스 간의 복제를 구성합니다.

참조하다 "ONTAP 시스템용 FSx를 설정하는 방법" 자세한 단계는 다음을 참조하세요.

AWS SDDC에 VMware Cloud 설정

"AWS의 VMware 클라우드"AWS 생태계에서 VMware 기반 워크로드에 대한 클라우드 네이티브 환경을 제공합니다. 각 VMware 소프트웨어 정의 데이터 센터(SDDC)는 Amazon Virtual Private Cloud(VPC)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지, 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다.

AWS에서 VMware Cloud 환경을 구성하려면 다음 단계를 따르세요. "AWS에서 가상화 환경 배포 및 구성" 파일럿 라이트 클러스터는 재해 복구 목적으로도 사용될 수 있습니다.

프라이빗 클라우드

NetApp Disaster Recovery 사용하면 하나 이상의 vCenter 클러스터에 호스팅된 VMware VM을 보호할 수 있습니다. 즉, VM 데이터 저장소를 동일한 개인 데이터 센터에 있는 다른 vCenter 클러스터나 원격 개인 또는 공동 배치된 데이터 센터에 복제할 수 있습니다.

온프레미스 간 상황의 경우, 물리적 사이트 중 하나에 콘솔 에이전트를 설치합니다.

재해 복구는 이더넷과 TCP/IP를 사용하여 사이트 간 복제를 지원합니다. 모든 변경 사항을 복구 지점 목표(RPO) 시간 프레임 내에 DR 사이트에 복제할 수 있도록 프로덕션 사이트 VM에서 데이터 변경률을 지원할 수 있는 적절한 대역폭이 있는지 확인하세요.

온프레미스 간 보호를 준비하세요

온프레미스 간 보호를 위해 NetApp Disaster Recovery 설정하기 전에 다음 요구 사항이 충족되는지 확인하세요.

- ONTAP 저장
  - ONTAP 자격 증명이 있는지 확인하세요.
  - 재해 복구 사이트를 만들거나 확인하세요.
  - 대상 ONTAP SVM을 생성하거나 확인하세요.
  - 소스 및 대상 ONTAP SVM이 피어링되었는지 확인하세요.
- vCenter 클러스터

- 보호하려는 VM이 NFS 데이터 저장소(ONTAP NFS 볼륨 사용) 또는 VMFS 데이터 저장소(NetApp iSCSI LUN 사용)에 호스팅되어 있는지 확인하세요.
- 검토"vCenter 권한" NetApp Disaster Recovery 에 필요합니다.
- 재해 복구 사용자 계정(기본 vCenter 관리자 계정 아님)을 만들고 해당 계정에 vCenter 권한을 할당합니다.

지능형 프록시 지원

NetApp Console 에이전트는 지능형 프록시를 지원합니다. 지능형 프록시는 온프레미스 환경을 NetApp Console 에 연결하는 가볍고 안전하며 효율적인 방법입니다. VPN이나 직접 인터넷 접속이 필요 없이 시스템과 콘솔 서비스 간의 안전한 연결을 제공합니다. 이 최적화된 프록시 구현은 로컬 네트워크 내의 API 트래픽을 오프로드합니다.

프록시가 구성되면 NetApp Disaster Recovery VMware 또는 ONTAP 과 직접 통신을 시도하고 직접 통신이 실패하면 구성된 프록시를 사용합니다.

NetApp Disaster Recovery 프록시 구현에는 HTTPS 프로토콜을 사용하여 콘솔 에이전트와 모든 vCenter 서버 및 ONTAP 어레이 간에 포트 443 통신이 필요합니다. 콘솔 에이전트 내의 NetApp Disaster Recovery 에이전트는 모든 작업을 수행할 때 VMware vSphere, VC 또는 ONTAP 과 직접 통신합니다.

NetApp Console 에서 일반 프록시 설정에 대한 자세한 내용은 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

NetApp Disaster Recovery 에 액세스

NetApp Console 사용하여 NetApp Disaster Recovery 서비스에 로그인합니다.

로그인하려면 NetApp 지원 사이트 자격 증명을 사용하거나 이메일과 비밀번호를 사용하여 NetApp 클라우드 로그인에 가입할 수 있습니다. "로그인에 대해 자세히 알아보세요" .

특정 작업에는 특정 사용자 역할이 필요합니다. "NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

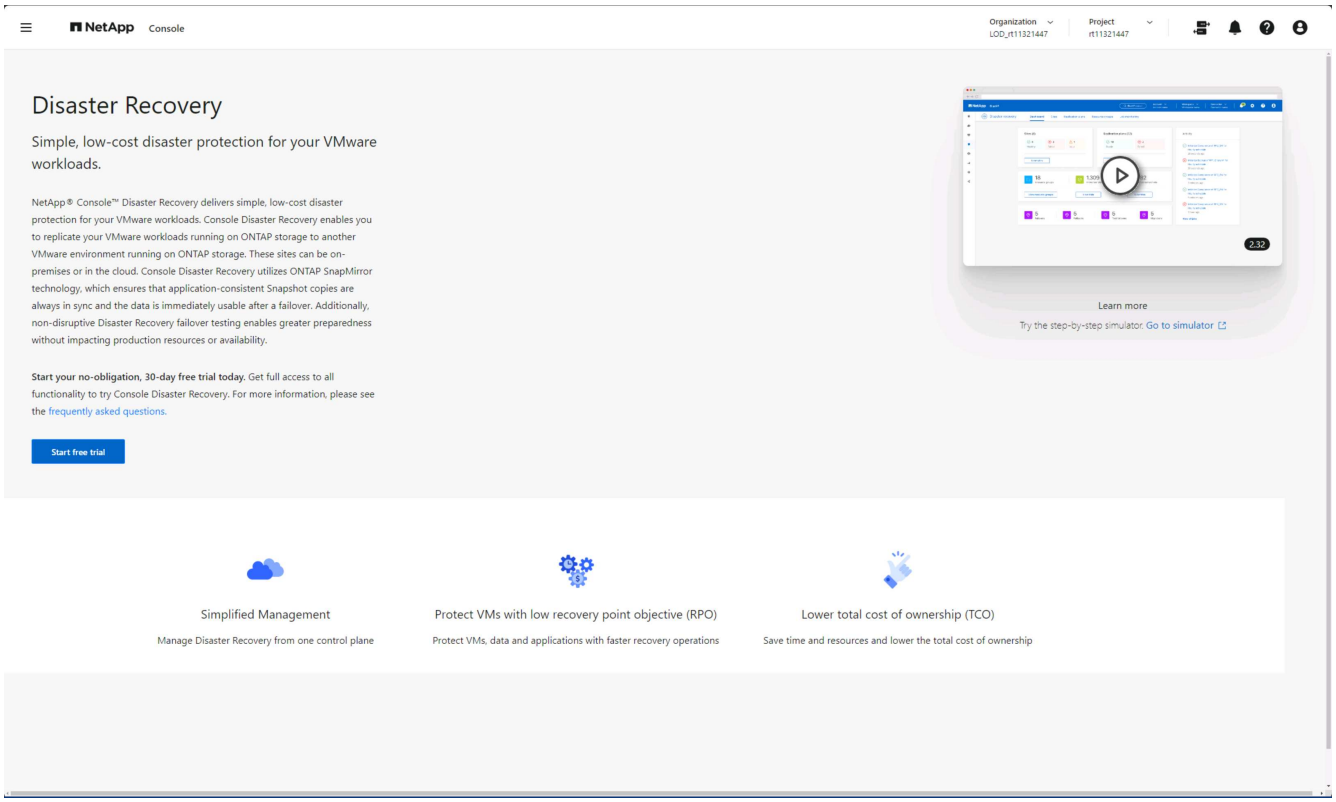
단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console" .

   NetApp Console 로그인 페이지가 나타납니다.

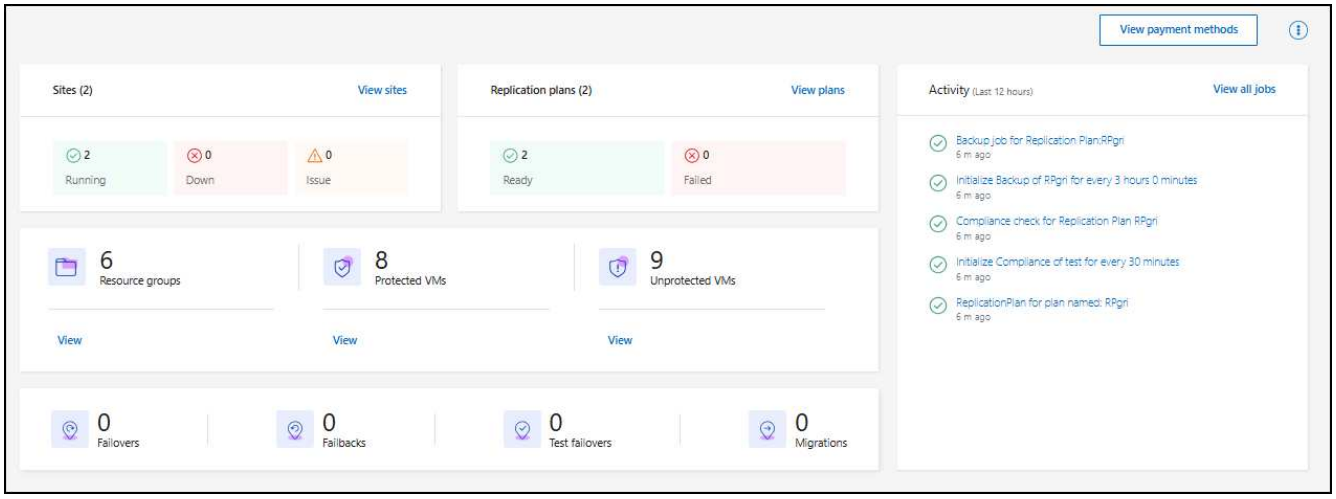
2. NetApp Console 에 로그인합니다.
3. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타나고 무료 체험판에 가입할 수 있습니다.



그렇지 않으면 NetApp Disaster Recovery 보드가 나타납니다.

- 아직 NetApp Console 에이전트를 추가하지 않은 경우 에이전트를 추가해야 합니다. 에이전트를 추가하려면 다음을 참조하세요. "콘솔 에이전트에 대해 알아보세요" .
- 기존 에이전트가 있는 NetApp Console 사용자인 경우 "재해 복구"를 선택하면 등록에 대한 메시지가 나타납니다.
- 이미 해당 서비스를 사용하고 있는 경우, "재해 복구"를 선택하면 대시보드가 나타납니다.



NetApp Disaster Recovery 에 대한 라이선싱 설정

NetApp Disaster Recovery 사용하면 무료 평가판, 사용량에 따른 지불 구독 또는 자체 라이선스 사용 등 다양한 라이선스 플랜을 사용할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 애플리케이션 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 액세스 역할에 대해 알아보세요".

라이선스 옵션 다음 라이선싱 옵션을 사용할 수 있습니다.

- 30일 무료 체험판에 등록하세요.
- Amazon Web Services(AWS) Marketplace 또는 Microsoft Azure Marketplace에서 사용량에 따라 지불하는(PAYGO) 구독을 구매하세요.
- BYOL(Bring Your Own License)은 NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)입니다. NetApp Console 에서 라이선스 일련 번호를 사용하여 BYOL을 활성화할 수 있습니다.

> NetApp Disaster Recovery 요금은 복제 계획이 있는 VM이 하나 이상 있는 경우 소스 사이트의 데이터 저장소 사용 용량을 기준으로 부과됩니다. 장애 조치된 데이터 저장소의 용량은 용량 허용량에 포함되지 않습니다. BYOL의 경우, 데이터가 허용된 용량을 초과하면 NetApp Console 에서 추가 용량 라이선스를 얻거나 라이선스를 업그레이드할 때까지 서비스 작업이 제한됩니다.

"구독에 대해 자세히 알아보세요".

무료 체험 기간이 종료되거나 라이선스가 만료된 후에도 서비스에서 다음 작업을 수행할 수 있습니다.

- 작업 부하나 복제 계획 등의 리소스를 확인합니다.
- 작업 부하나 복제 계획 등의 리소스를 삭제합니다.
- 평가판 기간이나 라이선스에 따라 생성된 모든 예약된 작업을 실행합니다.

30일 무료 체험판을 이용해 보세요

30일 무료 평가판을 통해 NetApp Disaster Recovery 사용해 보세요.

> 시험 기간 동안에는 수용 인원 제한이 적용되지 않습니다.

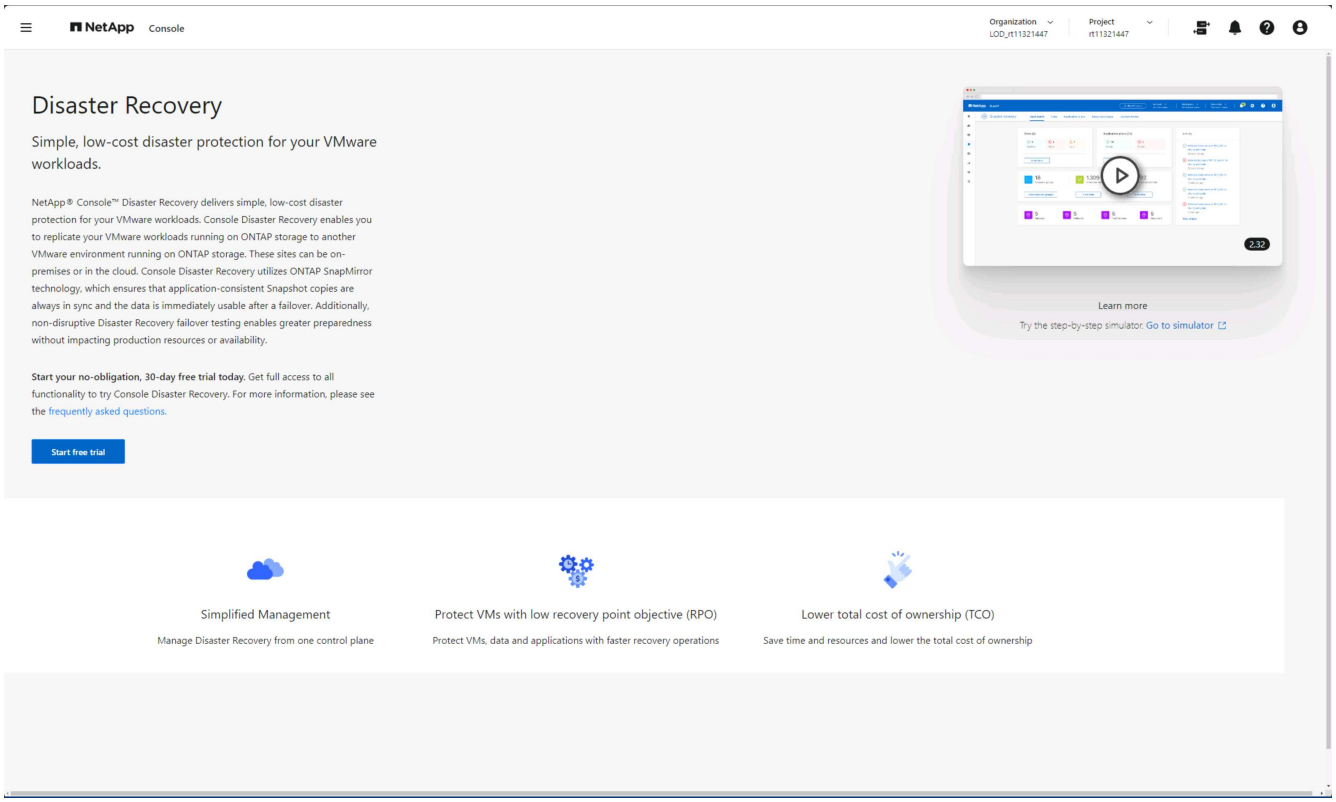
평가판 사용 후 계속 사용하려면 BYOL 라이선스 또는 PAYGO AWS 구독을 구매해야 합니다. 언제든지 라이선스를 받을 수 있으며, 체험 기간이 종료될 때까지 요금이 청구되지 않습니다.

체험판 기간 동안에는 모든 기능을 사용할 수 있습니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.



3. 다른 서비스에 대한 콘솔 에이전트를 아직 추가하지 않았다면 하나 추가하세요.

   콘솔 에이전트를 추가하려면 다음을 참조하세요. "콘솔 에이전트에 대해 알아보세요" .

4. 에이전트를 설정한 후 NetApp Disaster Recovery 랜딩 페이지에서 에이전트를 추가하는 버튼이 무료 평가판을 시작하는 버튼으로 변경됩니다. *무료 체험 시작*을 선택하세요.
5. vCenter를 추가하여 시작하세요.

   자세한 내용은 다음을 참조하십시오. "vCenter 사이트 추가" .

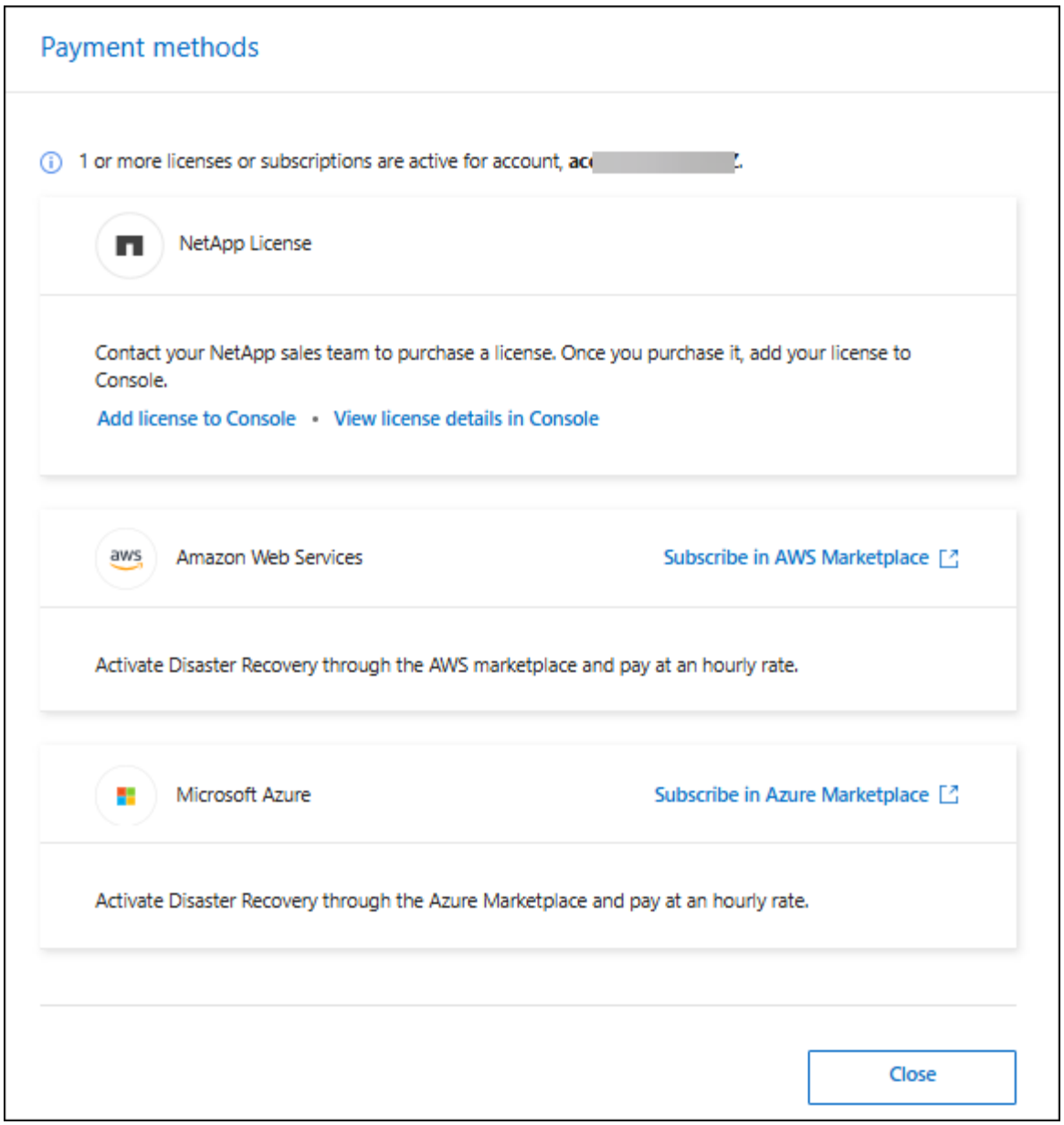
체험 기간이 종료된 후 마켓플레이스 중 하나를 통해 구독하세요.

무료 평가판이 종료된 후에는 NetApp 에서 라이선스를 구매하거나 AWS Marketplace 또는 Microsoft Azure Marketplace를 통해 구독할 수 있습니다. 이 절차는 마켓플레이스 중 하나에서 직접 구독하는 방법에 대한 간략한 개요를 제공합니다.

단계

1. NetApp Disaster Recovery 에서 무료 평가판이 만료된다는 메시지가 표시됩니다. 메시지에서 *구독 또는 라이선스 구매*를 선택하세요.

   또는, 에서 *결제 방법 보기*를 선택하세요.



2. **AWS Marketplace**에서 구독 또는 *Azure Marketplace에서 구독*을 선택하세요.
3. AWS Marketplace 또는 Microsoft Azure Marketplace를 사용하여 * NetApp Disaster Recovery*를 구독하세요.
4. NetApp Disaster Recovery 로 돌아오면 구독이 완료되었다는 메시지가 표시됩니다.

   NetApp Console 구독 페이지에서 구독 세부 정보를 볼 수 있습니다. "NetApp Console 사용하여 구독 관리에 대해 자세히 알아보세요.".

평가판이 종료된 후 **NetApp** 통해 **BYOL** 라이선스를 구매하세요.

평가판이 종료된 후에는 NetApp 영업 담당자를 통해 라이선스를 구매할 수 있습니다.

자체 라이선스를 가져오는 경우(BYOL) 설정에는 라이선스 구매, NetApp 라이선스 파일(NLF) 가져오기, NetApp Console 에 라이선스 추가가 포함됩니다.

- NetApp Console 에 라이선스 추가 ** NetApp 영업 담당자로부터 NetApp Disaster Recovery 라이선스를 구매한

후 콘솔에서 라이선스를 관리할 수 있습니다.

"NetApp Console 사용하여 라이선스를 추가하는 방법에 대해 알아보세요.".

라이센스가 만료되면 업데이트하세요

라이선스 기간이 만료일에 가까워지거나 라이선스 용량이 한도에 도달하면 NetApp Disaster Recovery UI에서 알림을 받게 됩니다. 스캔한 데이터에 액세스하는 데 방해가 되지 않도록 NetApp Disaster Recovery 라이선스가 만료되기 전에 업데이트할 수 있습니다.

이 메시지는 NetApp Console 과 다음에도 나타납니다. "알림" .

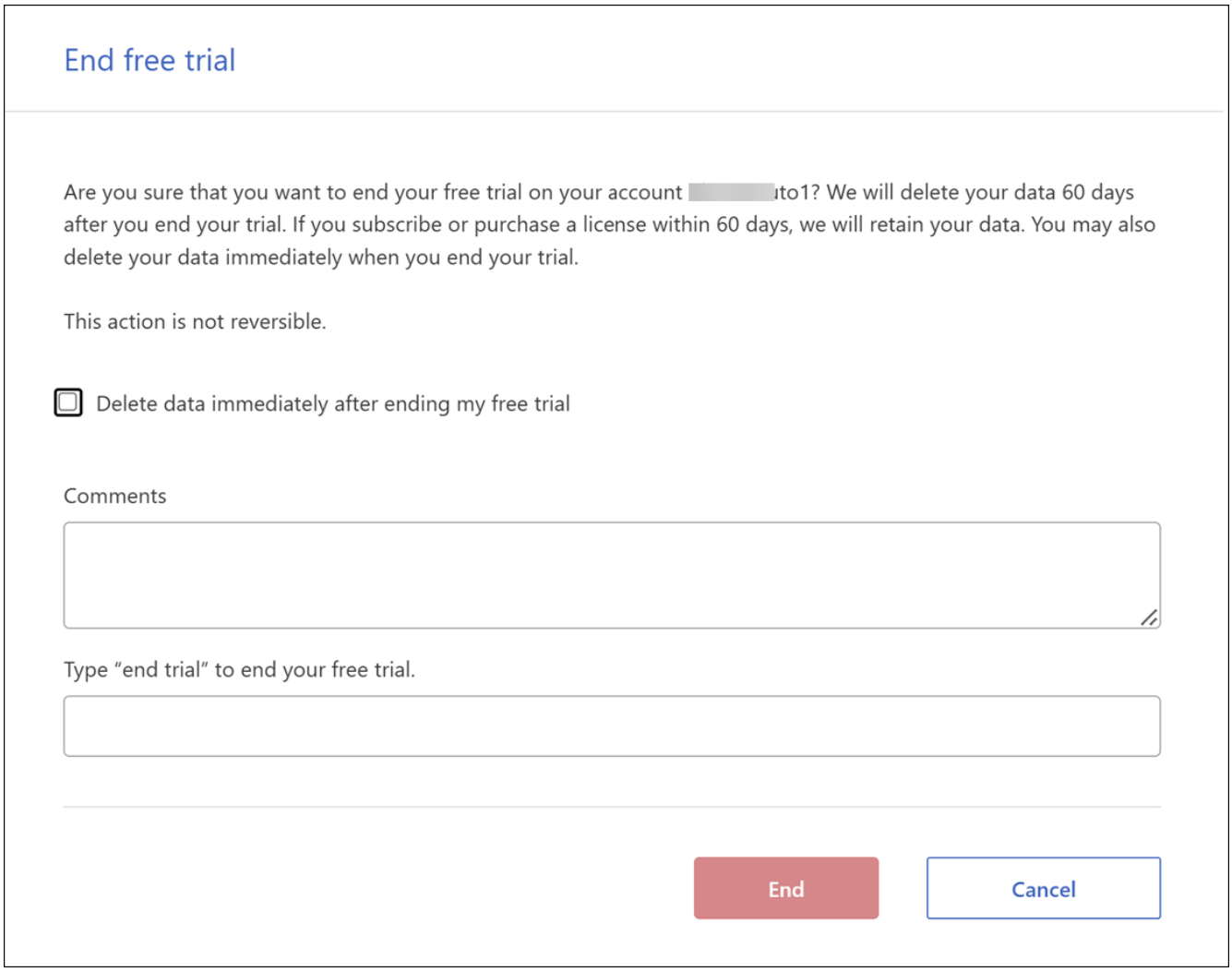
"NetApp Console 사용하여 라이선스 업데이트에 대해 알아보세요".

무료 체험 종료

언제든지 무료 체험을 중단할 수 있으며, 체험 기간이 만료될 때까지 기다릴 수도 있습니다.

단계

1. NetApp Disaster Recovery 에서 *무료 평가판 - 세부 정보 보기*를 선택합니다.
2. 드롭다운 세부정보에서 *무료 체험 종료*를 선택하세요.



3. 모든 데이터를 삭제하려면 *무료 체험 종료 후 즉시 데이터 삭제*를 선택하세요.

   이렇게 하면 모든 일정, 복제 계획, 리소스 그룹, vCenter 및 사이트가 삭제됩니다. 감사 데이터, 운영 로그, 작업 내역은 제품 수명이 끝날 때까지 보관됩니다.

   무료 평가판을 종료하고, 데이터 삭제를 요청하지 않았으며, 라이선스나 구독을 구매하지 않은 경우, NetApp Disaster Recovery 는 무료 평가판 종료 후 60일 후에 모든 데이터를 삭제합니다.

4. 텍스트 상자에 "체험판 종료"를 입력합니다.
5. *끝*을 선택하세요.

NetApp Disaster Recovery 사용

NetApp Disaster Recovery 개요 사용

NetApp Disaster Recovery 사용하면 다음과 같은 목표를 달성할 수 있습니다.

- "재해 복구 계획의 상태를 확인하세요" .
- "vCenter 사이트 추가" .
- "VM을 함께 구성하기 위해 리소스 그룹을 만듭니다."
- "재해 복구 계획 만들기" .
- "VMware 앱 복제"SnapMirror 복제를 사용하여 기본 사이트에서 클라우드의 재해 복구 원격 사이트로 데이터를 전송합니다.
- "VMware 앱 마이그레이션"기본 사이트에서 다른 사이트로.
- "장애 조치 테스트"원래 가상 머신을 방해하지 않고.
- 재난 발생 시,"기본 사이트를 장애 조치합니다" FSx for NetApp ONTAP 사용하여 AWS에서 VMware Cloud로 전환합니다.
- 재난이 해결된 후,"실패로 돌아가다" 재해 복구 사이트에서 기본 사이트로.
- "재해 복구 작업 모니터링"작업 모니터링 페이지에서.

대시보드에서 NetApp Disaster Recovery 계획의 상태를 확인하세요.

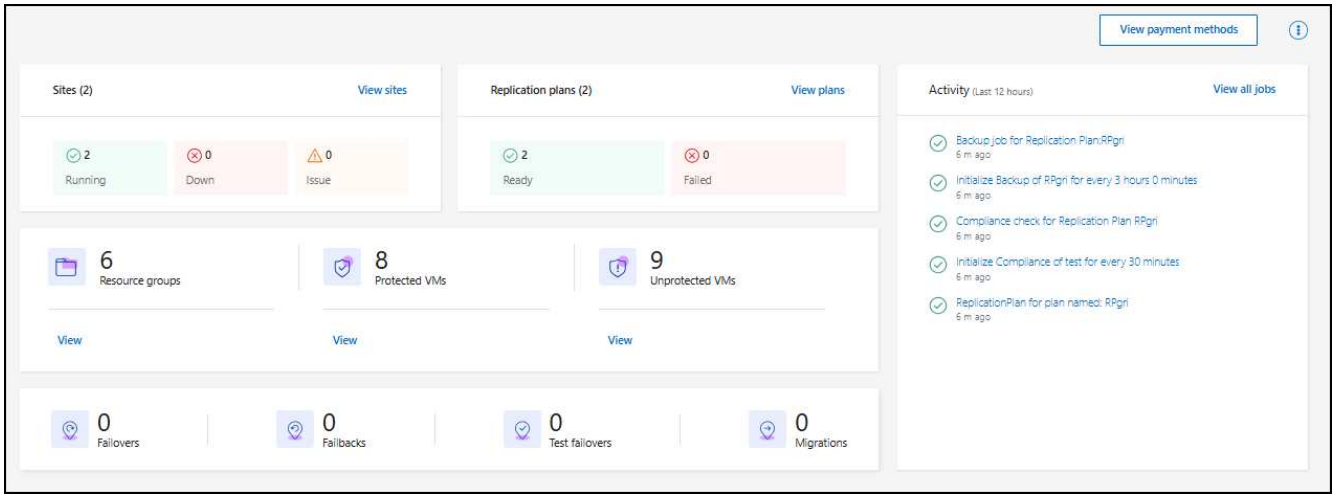
NetApp Disaster Recovery 대시보드를 사용하면 재해 복구 사이트와 복제 계획의 상태를 확인할 수 있습니다. 어떤 사이트와 계획이 정상인지, 연결이 끊겼는지, 성능이 저하되었는지 빠르게 확인할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 애플리케이션 관리자 또는 재해 복구 뷰어 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. NetApp Disaster Recovery 메뉴에서 *대시보드*를 선택합니다.



4. 대시보드에서 다음 정보를 검토하세요.
   - 사이트: 사이트의 상태를 확인하세요. 사이트는 다음 상태 중 하나를 가질 수 있습니다.
     - 실행 중: vCenter가 연결되고 정상 작동하며 실행 중입니다.
     - 다운: vCenter에 접근할 수 없거나 연결 문제가 있습니다.
     - 문제: vCenter에 접근할 수 없거나 연결 문제가 있습니다.

       사이트 세부 정보를 보려면 상태에 대해 *모두 보기*를 선택하거나 모든 사이트를 보려면 *사이트 보기*를 선택하세요.
   - 복제 계획: 계획의 상태를 확인합니다. 계획은 다음 상태 중 하나를 가질 수 있습니다.
     - 준비가 된
     - 실패한

       복제 계획 세부 정보를 검토하려면 상태에 대해 *모두 보기*를 선택하거나, 모두 보려면 *복제 계획 보기*를 선택하세요.
   - 리소스 그룹: 리소스 그룹의 상태를 확인합니다. 리소스 그룹은 다음 상태 중 하나를 가질 수 있습니다.
   - 보호된 **VM**: VM은 리소스 그룹의 일부입니다.
   - 보호되지 않은 **VM**: VM이 리소스 그룹의 일부가 아닙니다.

     자세한 내용을 보려면 각 항목 아래의 보기 링크를 선택하세요.
   - 장애 조치, 테스트 장애 조치 및 마이그레이션의 수. 예를 들어, 두 개의 계획을 만들고 해당 목적지로 마이그레이션한 경우 마이그레이션 수는 "2"로 표시됩니다.
5. 활동 창에서 모든 작업을 검토합니다. 작업 모니터에서 모든 작업을 보려면 *모든 작업 보기*를 선택하세요.

NetApp Disaster Recovery 에서 사이트에 vCenter 추가

재해 복구 계획을 만들려면 먼저 NetApp Console 에서 기본 vCenter 서버를 사이트에 추가하고 대상 vCenter 재해 복구 사이트를 추가해야 합니다.

소스 및 대상 vCenter가 모두 동일한 NetApp Console 에이전트를 사용하는지 확인하세요.

vCenter가 추가되면 NetApp Disaster Recovery vCenter 클러스터, ESXi 호스트, 데이터 저장소, 스토리지 공간, 가상 머신 세부 정보, SnapMirror 복제본, 가상 머신 네트워크를 포함하여 vCenter 환경에 대한 심층 검색을 수행합니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

이 작업에 관하여

이전 릴리스에서 vCenter를 추가하고 검색 일정을 사용자 지정하려면 vCenter 서버 사이트를 편집하고 일정을 설정해야 합니다.

NetApp Disaster Recovery 24시간마다 검색을 수행합니다. 사이트를 설정한 후에는 vCenter를 편집하여 필요에 맞게 검색 일정을 사용자 지정할 수 있습니다. 예를 들어, VM 수가 많은 경우 검색 일정을 23시간 59분마다 실행되도록 설정할 수 있습니다. VM 수가 적은 경우 검색 일정을 12시간마다 실행되도록 설정할 수 있습니다. 최소 간격은 30분이고, 최대 간격은 24시간입니다.

환경에 대한 최신 정보를 얻으려면 먼저 몇 가지 수동 검색을 수행해야 합니다. 그 후에는 일정을 자동으로 실행되도록 설정할 수 있습니다.

이전 버전의 vCenter가 있고 검색이 실행되는 시점을 변경하려면 vCenter 서버 사이트를 편집하고 일정을 설정하세요.

새로 추가되거나 삭제된 VM은 다음에 예약된 검색이나 즉각적인 수동 검색 중에 인식됩니다.

VM은 복제 계획이 다음 상태 중 하나인 경우에만 보호될 수 있습니다.

- 준비가 된
- 장애 복구가 커밋되었습니다.
- 테스트 장애 조치가 커밋되었습니다.

사이트의 **vCenter** 클러스터 각 사이트에는 하나 이상의 vCenter가 포함되어 있습니다. 이러한 vCenter는 하나 이상의 ONTAP 스토리지 클러스터를 사용하여 NFS 또는 VMFS 데이터 저장소를 호스팅합니다.

vCenter 클러스터는 하나의 사이트에만 존재할 수 있습니다. 사이트에 vCenter 클러스터를 추가하려면 다음 정보가 필요합니다.

- vCenter 관리 IP 주소 또는 FQDN
- 작업을 수행하는 데 필요한 권한이 있는 vCenter 계정의 자격 증명입니다. 보다"필수 vCenter 권한" 자세한 내용은.
- 클라우드 호스팅 VMware 사이트의 경우 필요한 클라우드 액세스 키
- vCenter에 액세스하기 위한 보안 인증서입니다.

이 서비스는 자체 서명된 보안 인증서 또는 중앙 인증 기관(CA)의 인증서를 지원합니다.

단계

1. 에 로그인하세요 "NetApp Console" .

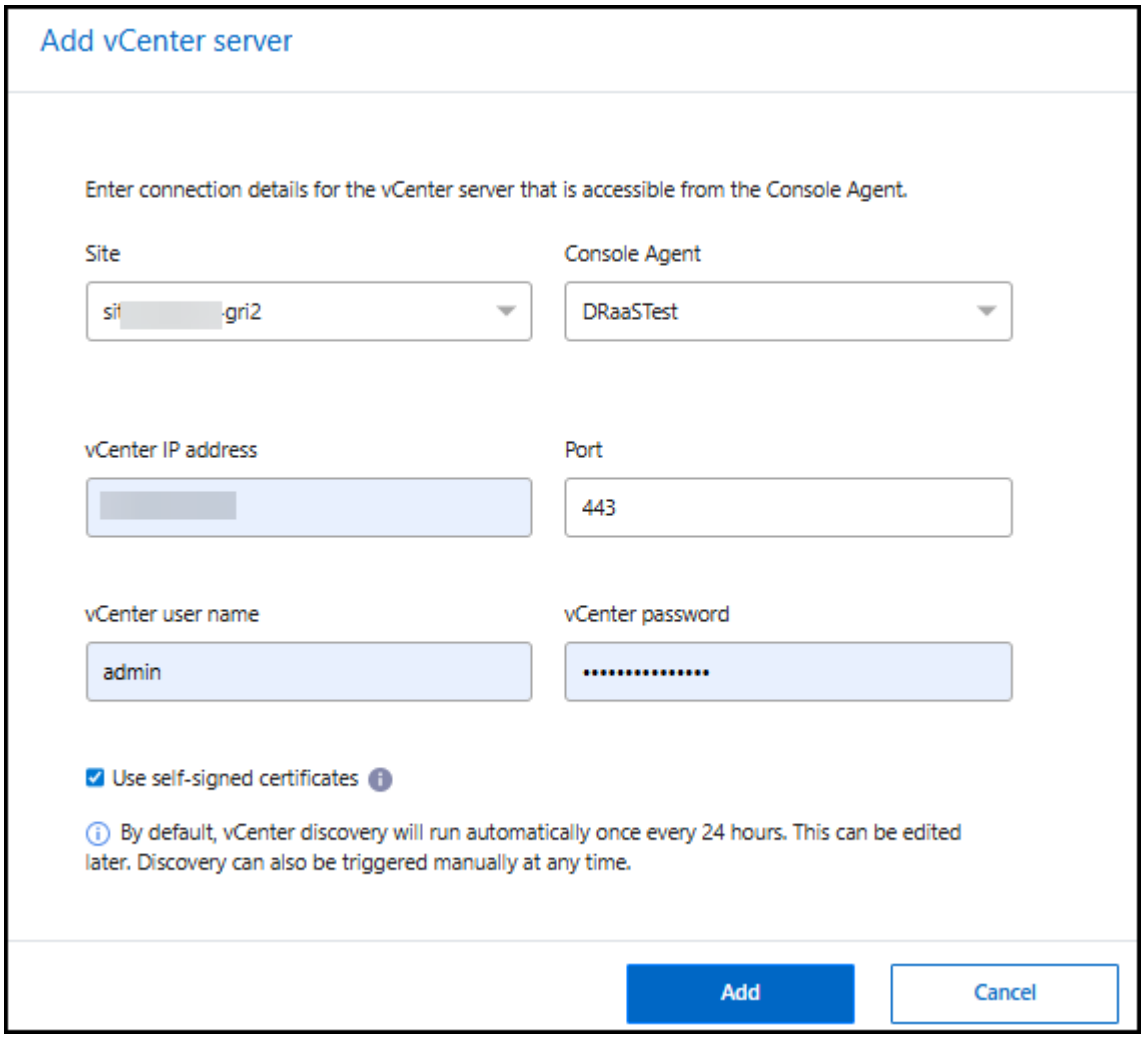
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.

   NetApp 재해 복구를 처음 사용하는 경우 vCenter 정보를 추가해야 합니다. 이미 vCenter 정보를 추가한 경우 대시보드가 표시됩니다.

   추가하는 사이트 유형에 따라 다른 필드가 나타납니다.

3. 이미 vCenter 사이트가 있고 더 추가하려는 경우 메뉴에서 *사이트*를 선택한 다음 *추가*를 선택합니다.
4. 사이트 페이지에서 사이트를 선택하고 *vCenter 추가*를 선택합니다.
5. 소스: 소스 vCenter 사이트에 대한 정보를 입력하려면 *vCenter 서버 검색*을 선택합니다.

   vCenter 사이트를 더 추가하려면 *사이트*를 선택한 다음 *추가*를 선택합니다.



   - 사이트를 선택한 다음 NetApp Console 에이전트를 선택하고 vCenter 자격 증명을 제공합니다.
   - 온프레미스 사이트에만 해당: 소스 vCenter에 대한 자체 서명 인증서를 수락하려면 상자를 선택하세요.

     자체 서명 인증서는 다른 인증서만큼 안전하지 않습니다. vCenter가 인증 기관(CA) 인증서로 구성되지 않은 경우 이 상자를 선택해야 합니다. 그렇지 않으면 vCenter에 대한 연결이 작동하지 않습니다.

6. *추가*를 선택하세요.

   다음으로 대상 vCenter를 추가합니다.

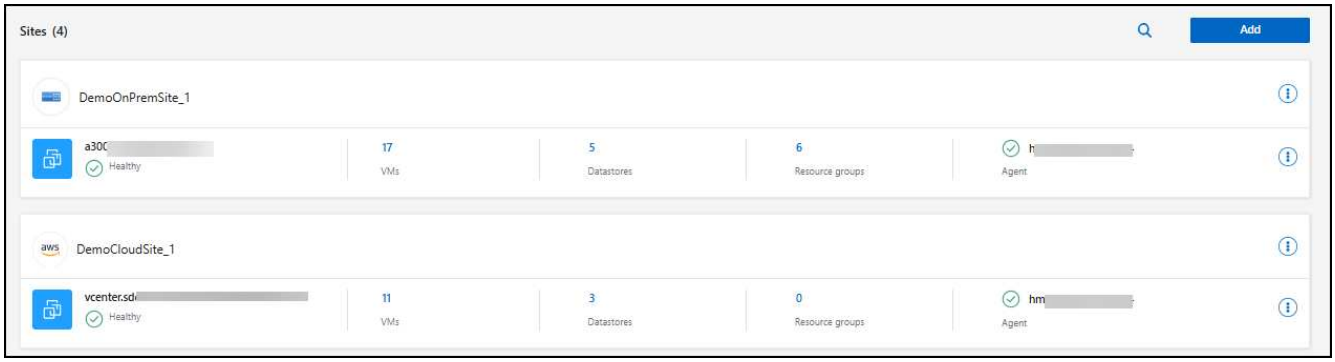
7. 대상 vCenter에 대한 사이트를 다시 추가합니다.
8. 다시 *vCenter 추가*를 선택하고 대상 vCenter 정보를 추가합니다.
9. 목표:

   a. 대상 사이트와 위치를 선택하세요. 대상이 클라우드인 경우 *AWS*를 선택하세요.

      - (클라우드 사이트에만 적용) **API** 토큰: 조직의 서비스 액세스를 승인하려면 API 토큰을 입력하세요. 특정 조직 및 서비스 역할을 제공하여 API 토큰을 생성합니다.
      - (클라우드 사이트에만 적용) 긴 조직 **ID**: 조직의 고유 ID를 입력하세요. NetApp Console 의 계정 섹션에서 사용자 이름을 클릭하면 이 ID를 식별할 수 있습니다.

   b. *추가*를 선택하세요.

      소스 및 대상 vCenter가 사이트 목록에 나타납니다.



10. 작업 진행 상황을 보려면 메뉴에서 *작업 모니터링*을 선택하세요.

vCenter 사이트에 대한 서브넷 매핑 추가

서브넷 매핑을 사용하면 장애 조치 작업 시 IP 주소를 관리할 수 있으며, 이를 통해 각 vCenter에 대한 서브넷을 추가할 수 있습니다. 이렇게 하면 각 가상 네트워크에 대한 IPv4 CIDR, 기본 게이트웨이, DNS가 정의됩니다.

장애 조치 시 NetApp Disaster Recovery 매핑된 네트워크의 CIDR을 사용하여 각 vNIC에 새 IP 주소를 할당합니다.

예를 들어:

- 네트워크A = 10.1.1.0/24
- 네트워크B = 192.168.1.0/24

VM1에는 NetworkA에 연결된 vNIC(10.1.1.50)가 있습니다. NetworkA는 복제 계획 설정에서 NetworkB에 매핑됩니다.

장애 조치 시 NetApp Disaster Recovery 원래 IP 주소(10.1.1)의 네트워크 부분을 대체하고 원래 IP 주소(10.1.1.50)의 호스트 주소(.50)를 유지합니다. VM1의 경우 NetApp Disaster Recovery NetworkB의 CIDR 설정을 살펴보고 NetworkB의 네트워크 부분인 192.168.1을 사용하고 호스트 부분(.50)은 그대로 유지하여 VM1의 새 IP 주소를 생성합니다. 새로운 IP는 192.168.1.50이 됩니다.

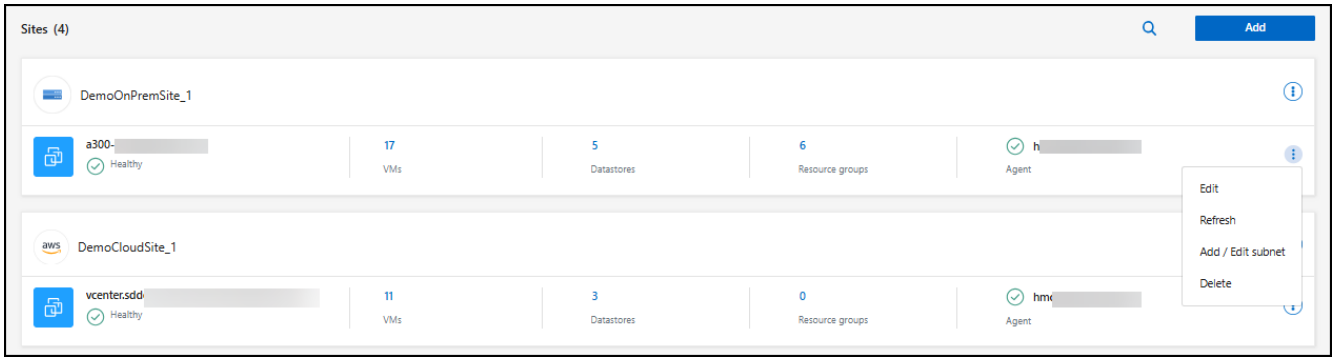
요약하자면, 호스트 주소는 동일하게 유지되지만 네트워크 주소는 사이트 서브넷 매핑에 구성된 주소로 대체됩니다. 이를 통해 장애 조치 시 IP 주소 재할당을 보다 쉽게 관리할 수 있으며, 특히 관리해야 할 네트워크가 수백 개이고 VM이 수천 개일 경우 더욱 그렇습니다.

서브넷 매핑을 사용하는 것은 선택적인 2단계 프로세스입니다.

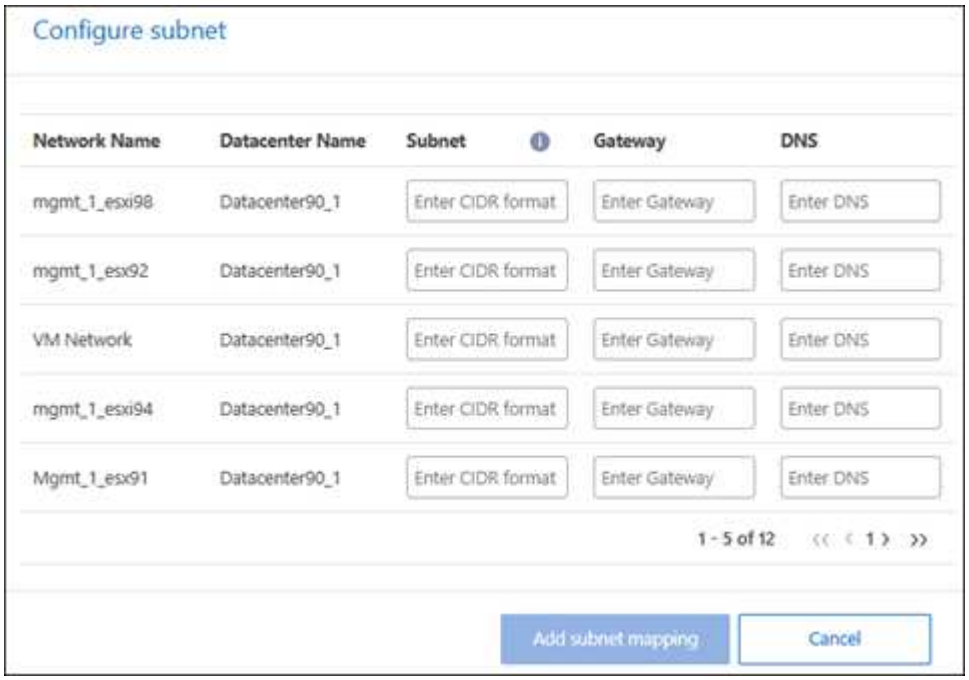
- 먼저, 각 vCenter 사이트에 대한 서브넷 매핑을 추가합니다.
- 둘째, 복제 계획에서 가상 머신 탭과 대상 IP 필드에서 서브넷 매핑을 사용할 것임을 표시합니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *사이트*를 선택합니다.
2. 행동으로부터 오른쪽에 있는 아이콘을 클릭하고 *서브넷 추가*를 선택하세요.



서브넷 구성 페이지가 나타납니다.



3. 서브넷 구성 페이지에서 다음 정보를 입력합니다.
   a. 서브넷: 서브넷의 IPv4 CIDR을 /32까지 입력하세요.

CIDR 표기법은 IP 주소와 네트워크 마스크를 지정하는 방법입니다. /24는 넷마스크를 나타냅니다. 숫자는 IP 주소로 구성되며, "/" 뒤에 있는 숫자는 IP 주소의 비트 수가 네트워크를 나타내는 것을 나타냅니다. 예를 들어, 192.168.0.50/24의 경우 IP 주소는 192.168.0.50이고 네트워크 주소의 총 비트 수는 24입니다. 192.168.0.50 255.255.255.0은 192.168.0.0/24가 됩니다.

b. 게이트웨이: 서브넷의 기본 게이트웨이를 입력하세요.

c. DNS: 서브넷의 DNS를 입력하세요.

4. *서브넷 매핑 추가*를 선택합니다.

복제 계획에 대한 서브넷 매핑 선택

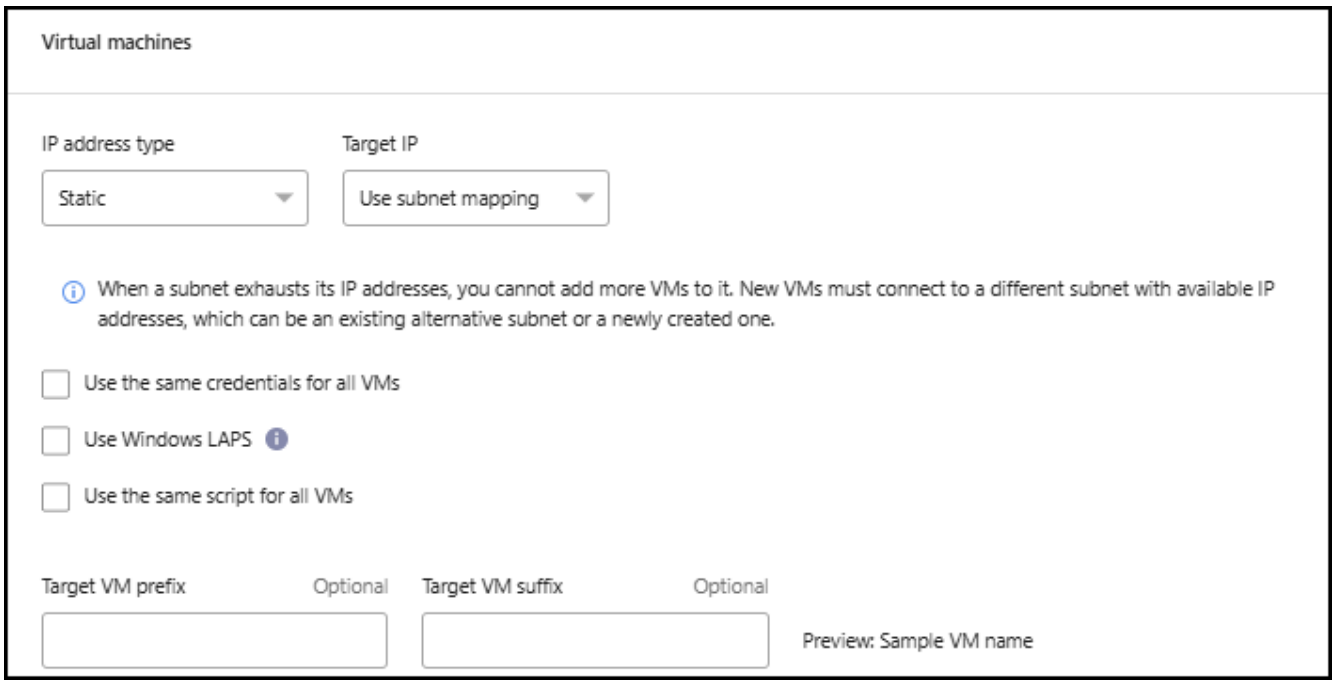
복제 계획을 생성할 때 복제 계획에 대한 서브넷 매핑을 선택할 수 있습니다.

서브넷 매핑을 사용하는 것은 선택적인 2단계 프로세스입니다.

- 먼저, 각 vCenter 사이트에 대한 서브넷 매핑을 추가합니다.
- 둘째, 복제 계획에서 서브넷 매핑을 사용할 것임을 표시합니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.
2. 복제 계획을 추가하려면 *추가*를 선택하세요.
3. vCenter 서버를 추가하고, 리소스 그룹이나 애플리케이션을 선택하고, 매핑을 완료하여 평소와 같은 방식으로 필드를 완성합니다.
4. 복제 계획 > 리소스 매핑 페이지에서 가상 머신 섹션을 선택합니다.



5. 대상 **IP** 필드의 드롭다운 목록에서 *서브넷 매핑 사용*을 선택합니다.

VM이 두 개 있는 경우(예: 하나는 Linux이고 다른 하나는 Windows인 경우) Windows에 대한 자격 증명만 필요합니다.

6. 복제 계획 생성을 계속합니다.

vCenter 서버 사이트를 편집하고 검색 일정을 사용자 정의합니다.

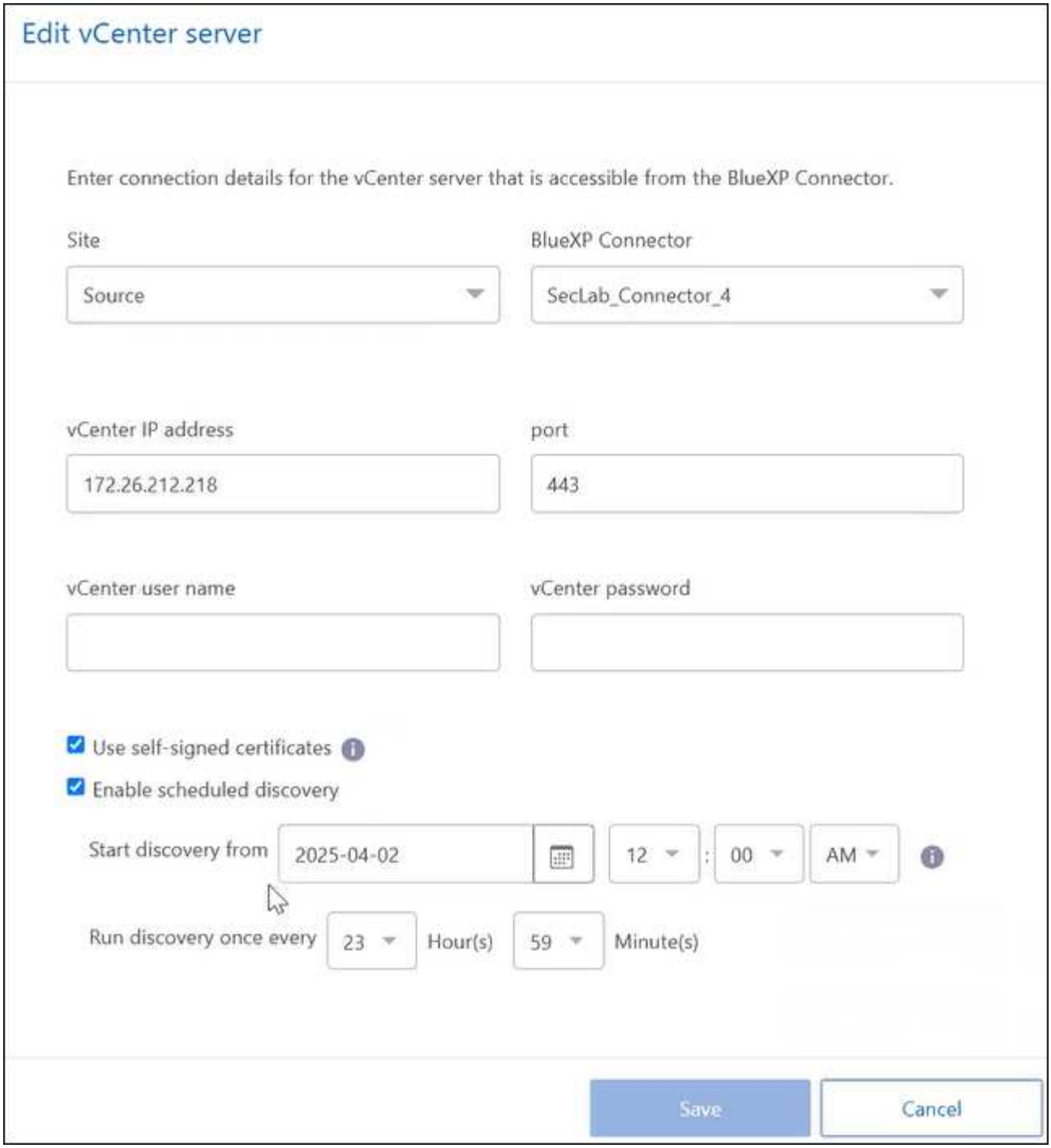
vCenter 서버 사이트를 편집하여 검색 일정을 사용자 지정할 수 있습니다. 예를 들어, VM 수가 많은 경우 검색 일정을 23시간 59분마다 실행되도록 설정할 수 있습니다. VM 수가 적은 경우 검색 일정을 12시간마다 실행되도록 설정할 수 있습니다.

이전 버전의 vCenter가 있고 검색이 실행되는 시점을 변경하려면 vCenter 서버 사이트를 편집하고 일정을 설정하세요.

검색 일정을 예약하지 않으려면 예약된 검색 옵션을 비활성화하고 언제든지 수동으로 검색을 새로 고칠 수 있습니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *사이트*를 선택합니다.
2. 편집하려는 사이트를 선택하세요.
3. 작업을 선택하세요 오른쪽에 있는 아이콘을 클릭하고 *편집*을 선택하세요.
4. vCenter 서버 편집 페이지에서 필요에 따라 필드를 편집합니다.
5. 검색 일정을 사용자 지정하려면 예약된 검색 활성화 상자를 선택하고 원하는 날짜와 시간 간격을 선택하세요.



6. *저장*을 선택하세요.

검색을 수동으로 새로 고침

언제든지 수동으로 검색 내용을 새로 고칠 수 있습니다. 이 기능은 VM을 추가하거나 제거한 후 NetApp Disaster Recovery 에서 정보를 업데이트하려는 경우에 유용합니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *사이트*를 선택합니다.
2. 새로 고침할 사이트를 선택하세요.

3. 작업을 선택하세요  오른쪽에 있는 아이콘을 클릭하고 *새로 고침*을 선택하세요.

NetApp Disaster Recovery 에서 VM을 함께 구성하기 위한 리소스 그룹 생성

vCenter 사이트를 추가한 후에는 리소스 그룹을 만들어 VM 또는 데이터 저장소별로 VM을 단일 단위로 보호할 수 있습니다. 리소스 그룹을 사용하면 요구 사항을 충족하는 논리적 그룹으로 종속 VM 세트를 구성할 수 있습니다. 예를 들어, 하나의 애플리케이션과 연관된 VM을 그룹화하거나 유사한 계층을 갖는 애플리케이션을 그룹화할 수 있습니다. 또 다른 예로, 그룹에는 복구 시 실행할 수 있는 지연된 부팅 순서가 포함될 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 애플리케이션 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

이 작업에 관하여

VM 자체를 그룹화하거나 데이터 저장소의 VM을 그룹화할 수 있습니다.

다음 방법을 사용하여 리소스 그룹을 만들 수 있습니다.

- 리소스 그룹 옵션에서
- 재해 복구 또는 복제 계획을 만드는 동안. 소스 vCenter 클러스터에서 호스팅되는 VM이 많은 경우 복제 계획을 만드는 동안 리소스 그룹을 만드는 것이 더 쉬울 수 있습니다. 복제 계획을 생성하는 동안 리소스 그룹을 생성하는 방법에 대한 지침은 다음을 참조하세요."복제 계획 만들기" .

각 리소스 그룹에는 하나 이상의 VM이나 데이터 저장소가 포함될 수 있습니다. VM은 복제 계획에 포함된 순서에 따라 전원이 켜집니다. 리소스 그룹 목록에서 VM이나 데이터 저장소를 위아래로 끌어서 순서를 변경할 수 있습니다.

리소스 그룹에 관하여

리소스 그룹을 사용하면 여러 VM이나 데이터 저장소를 단일 단위로 결합할 수 있습니다.

예를 들어, 판매 시점 관리 애플리케이션은 데이터베이스, 비즈니스 로직, 매장을 위해 여러 개의 VM을 사용할 수 있습니다. 이러한 모든 VM을 하나의 리소스 그룹으로 관리할 수 있습니다. 애플리케이션에 필요한 모든 VM의 VM 시작 순서, 네트워크 연결 및 복구에 대한 복제 계획 규칙을 적용하기 위해 리소스 그룹을 설정합니다.

어떻게 작동하나요**?**

NetApp Disaster Recovery 리소스 그룹에서 VM을 호스팅하는 기본 ONTAP 볼륨과 LUN을 복제하여 VM을 보호합니다. 이를 위해 시스템은 리소스 그룹에서 VM을 호스팅하는 각 데이터 저장소의 이름을 vCenter에 쿼리합니다. 그런 다음 NetApp Disaster Recovery 해당 데이터 저장소를 호스팅하는 소스 ONTAP 볼륨이나 LUN을 식별합니다. 모든 보호는 SnapMirror 복제를 사용하여 ONTAP 볼륨 수준에서 수행됩니다.

리소스 그룹의 VM이 서로 다른 데이터 저장소에 호스팅되는 경우 NetApp Disaster Recovery 다음 방법 중 하나를 사용하여 ONTAP 볼륨 또는 LUN의 데이터 일관성 스냅샷을 만듭니다.

FlexVol 볼륨의 상대적 위치	스냅샷 복제 프로세스
여러 데이터 저장소 - *동일한 SVM*의 FlexVol 볼륨	• ONTAP 일관성 그룹이 생성되었습니다. • 일관성 그룹의 스냅샷이 촬영되었습니다. • 볼륨 범위 SnapMirror 복제가 수행되었습니다.
여러 데이터 저장소 - *여러 SVM*의 FlexVol 볼륨	• ONTAP API: `cg_start` . 모든 볼륨을 정지하여 스냅샷을 찍을 수 있도록 하고 모든 리소스 그룹 볼륨의 볼륨 범위 스냅샷을 시작합니다. • ONTAP API: `cg_end` . 모든 볼륨에서 I/O를 재개하고 스냅샷이 촬영된 후 볼륨 범위 SnapMirror 복제를 활성화합니다.

리소스 그룹을 만들 때 다음 사항을 고려하세요.

- 리소스 그룹에 데이터 저장소를 추가하기 전에 먼저 VM의 수동 검색이나 예약된 검색을 시작하세요. 이렇게 하면 VM이 검색되어 리소스 그룹에 나열됩니다. 수동 검색을 시작하지 않으면 VM이 리소스 그룹에 나열되지 않을 수 있습니다.
- 데이터 저장소에 최소한 하나의 VM이 있는지 확인하세요. 데이터 저장소에 VM이 없으면 재해 복구는 데이터 저장소를 검색하지 않습니다.
- 단일 데이터 저장소는 두 개 이상의 복제 계획으로 보호되는 VM을 호스팅해서는 안 됩니다.
- 동일한 데이터 저장소에 보호된 VM과 보호되지 않은 VM을 호스팅하지 마세요. 보호된 VM과 보호되지 않은 VM이 동일한 데이터 저장소에 호스팅되는 경우 다음과 같은 문제가 발생할 수 있습니다.
  - NetApp Disaster Recovery SnapMirror 사용하고 시스템이 ONTAP 볼륨 전체를 복제하므로 해당 볼륨의 사용된 용량은 라이선싱 고려 사항에 사용됩니다. 이 경우 보호된 VM과 보호되지 않은 VM이 모두 사용하는 볼륨 공간이 이 계산에 포함됩니다.
  - 리소스 그룹과 연관된 데이터 저장소를 재해 복구 사이트로 장애 조치해야 하는 경우, 장애 조치 프로세스를 통해 보호되지 않은 VM(리소스 그룹에 속하지 않지만 ONTAP 볼륨에 호스팅된 VM)이 소스 사이트에 더 이상 존재하지 않게 되므로 소스 사이트의 보호되지 않은 VM이 실패하게 됩니다. 또한 NetApp Disaster Recovery 장애 조치 vCenter 사이트에서 보호되지 않은 VM을 시작하지 않습니다.
- VM을 보호하려면 리소스 그룹에 포함되어야 합니다.

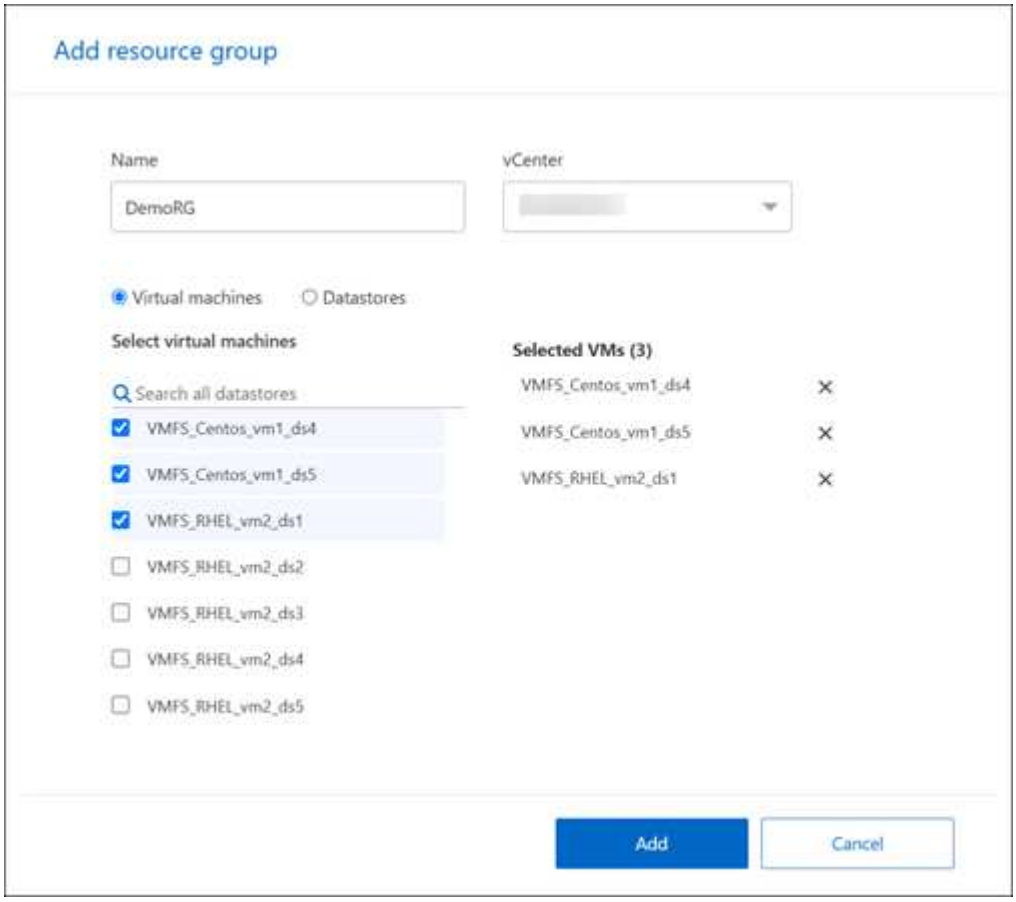
모범 사례: NetApp Disaster Recovery 배포하기 전에 VM을 구성하여 "데이터 저장소 확산"을 최소화하세요. 보호가 필요한 VM을 데이터 저장소 하위 집합에 배치하고, 보호하지 않을 VM을 다른 데이터 저장소 하위 집합에 배치합니다. 주어진 데이터 저장소의 VM이 서로 다른 복제 계획으로 보호되지 않도록 합니다.

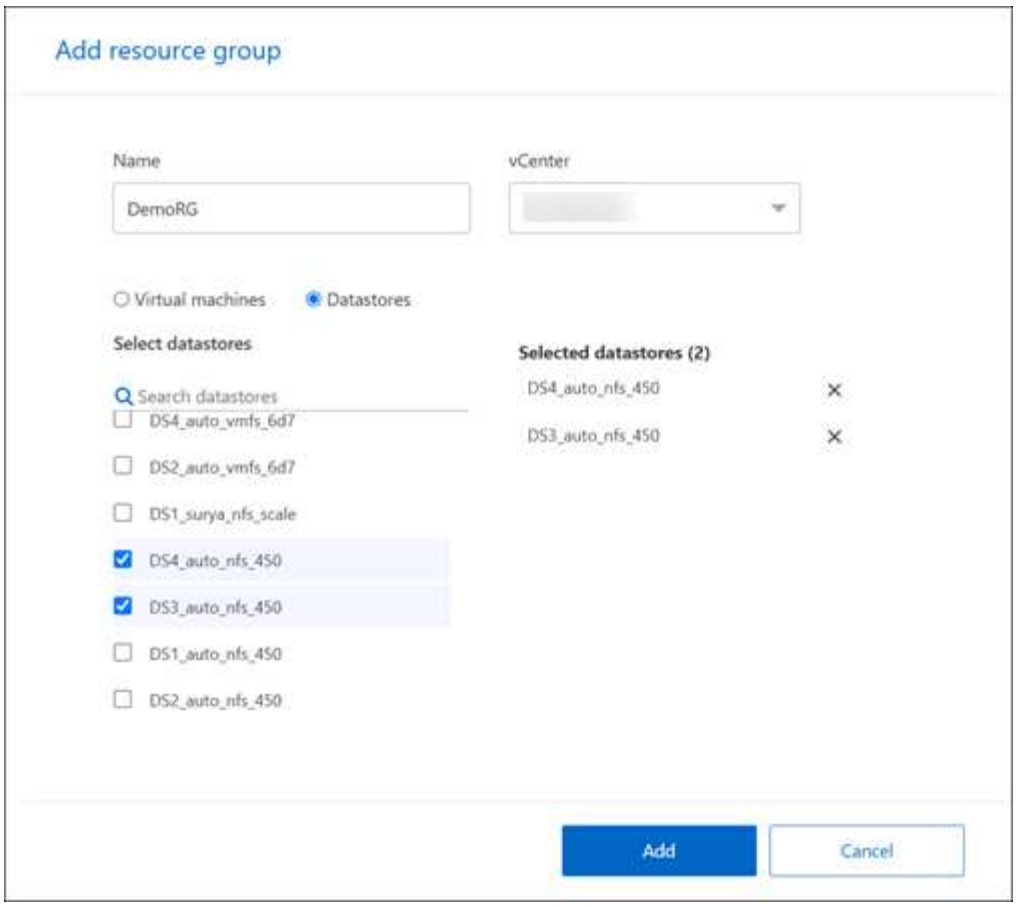
단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. NetApp Disaster Recovery 메뉴에서 *리소스 그룹*을 선택합니다.
4. *추가*를 선택하세요.
5. 리소스 그룹의 이름을 입력하세요.
6. VM이 있는 소스 vCenter 클러스터를 선택합니다.
7. 검색 방법에 따라 가상 머신 또는 *데이터 저장소*를 선택하세요.
8. 리소스 그룹 추가 탭을 선택합니다. 시스템은 선택된 vCenter 클러스터에 있는 모든 데이터 저장소 또는 VM을

나열합니다. *데이터 저장소*를 선택한 경우 시스템은 선택한 vCenter 클러스터의 모든 데이터 저장소를 나열합니다. *가상 머신*을 선택한 경우 시스템은 선택한 vCenter 클러스터에 있는 모든 VM을 나열합니다.

9. 리소스 그룹 추가 페이지의 왼쪽에서 보호하려는 VM을 선택합니다.





10. 원하는 경우 목록에서 각 VM을 위나 아래로 끌어서 오른쪽에 있는 VM의 순서를 변경합니다. VM은 포함된 순서에 따라 전원이 켜집니다.
11. *추가*를 선택하세요.

NetApp Disaster Recovery 에서 복제 계획 만들기

vCenter 사이트를 추가한 후에는 재해 복구 또는 복제 계획을 만들 준비가 된 것입니다. 복제 계획은 VMware 인프라의 데이터 보호를 관리합니다. 소스 및 대상 vCenter를 선택하고, 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법을 그룹화합니다. 예를 들어, 하나의 애플리케이션과 연관된 가상 머신(VM)을 그룹화하거나 유사한 계층을 갖는 애플리케이션을 그룹화할 수 있습니다. 이러한 계획을 때로 _청사진_이라고 부르기도 합니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

이 작업에 관하여

복제 계획을 만들고 규정 준수 및 테스트 일정을 편집할 수도 있습니다. 프로덕션 작업 부하에 영향을 주지 않고 VM의 테스트 장애 조치를 실행합니다.

여러 데이터 저장소에서 여러 VM을 보호할 수 있습니다. NetApp Disaster Recovery 보호된 VM 데이터 저장소를

호스팅하는 모든 ONTAP 볼륨에 대한 ONTAP 일관성 그룹을 생성합니다.

VM은 복제 계획이 다음 상태 중 하나인 경우에만 보호될 수 있습니다.

- 준비가 된
- 장애 복구가 커밋되었습니다.
- 테스트 장애 조치가 커밋되었습니다.

복제 계획 스냅샷

재해 복구는 소스 및 대상 클러스터에서 동일한 수의 스냅샷을 유지합니다. 기본적으로 이 서비스는 24시간마다 스냅샷 조정 프로세스를 수행하여 소스 및 대상 클러스터의 스냅샷 수가 동일한지 확인합니다.

다음과 같은 상황에서는 소스 클러스터와 대상 클러스터 간의 스냅샷 수가 달라질 수 있습니다.

- 일부 상황에서는 재해 복구 외부의 ONTAP 작업이 볼륨에서 스냅샷을 추가하거나 제거할 수 있습니다.
  - 소스 사이트에 누락된 스냅샷이 있는 경우, 관계에 대한 기본 SnapMirror 정책에 따라 대상 사이트의 해당 스냅샷이 삭제될 수 있습니다.
  - 대상 사이트에 누락된 스냅샷이 있는 경우, 서비스는 관계에 대한 기본 SnapMirror 정책에 따라 다음에 예약된 스냅샷 조정 프로세스 중에 소스 사이트에서 해당 스냅샷을 삭제할 수 있습니다.
- 복제 계획의 스냅샷 보존 횟수가 감소하면 서비스는 새로 줄어든 보존 횟수를 충족하기 위해 소스 사이트와 대상 사이트에서 가장 오래된 스냅샷을 삭제하게 됩니다.

이러한 경우 재해 복구는 다음 일관성 검사 시 소스 및 대상 클러스터에서 이전 스냅샷을 제거합니다. 또는 관리자는 *작업*을 선택하여 즉시 스냅샷 정리를 수행할 수 있습니다. ••• 복제 계획에서 아이콘을 선택하고 *스냅샷 정리*를 선택합니다.

이 서비스는 24시간마다 스냅샷 대칭 검사를 수행합니다.

시작하기 전에

- SnapMirror 관계를 생성하기 전에 재해 복구 외부에서 클러스터와 SVM 피어링을 설정합니다.
- Google Cloud를 사용하면 복제 계획에 볼륨이나 데이터 저장소를 하나만 추가할 수 있습니다.

> NetApp Disaster Recovery 배포하기 전에 VM을 구성하여 "데이터 저장소 확산"을 최소화하세요. 보호가 필요한 VM을 데이터 저장소 하위 집합에 배치하고, 보호하지 않을 VM을 다른 데이터 저장소 하위 집합에 배치합니다. 데이터 저장소 기반 보호를 사용하여 모든 데이터 저장소의 VM이 보호되도록 합니다.

계획을 세우세요

마법사가 다음 단계를 안내합니다.

- vCenter 서버를 선택하세요.
- 복제하려는 VM이나 데이터 저장소를 선택하고 리소스 그룹을 할당합니다.
- 소스 환경의 리소스가 대상 환경에 어떻게 매핑되는지 매핑합니다.
- 계획이 실행되는 빈도를 설정하고, 게스트 호스팅 스크립트를 실행하고, 부팅 순서를 설정하고, 복구 지점 목표를

선택합니다.

- 계획을 검토하세요.

계획을 세울 때는 다음 지침을 따라야 합니다.

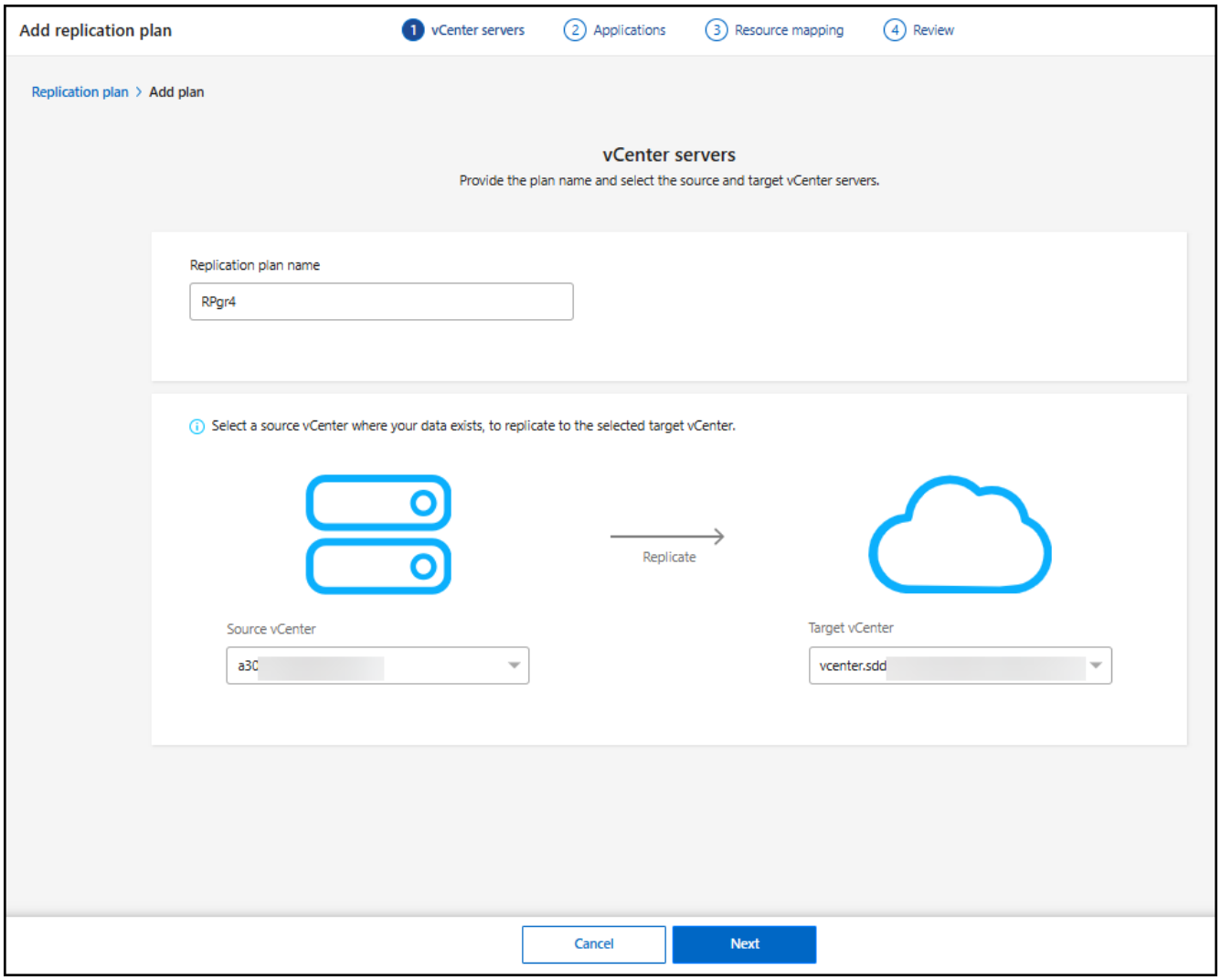
- 계획의 모든 VM에 대해 동일한 자격 증명을 사용합니다.
- 계획에 있는 모든 VM에 동일한 스크립트를 사용합니다.
- 계획에 있는 모든 VM에 대해 동일한 서브넷, DNS 및 게이트웨이를 사용합니다.

vCenter 서버 선택

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택하고 *추가*를 선택합니다. 또는 서비스를 처음 사용하는 경우 대시보드에서 *복제 계획 추가*를 선택하세요.



4. 복제 계획의 이름을 만듭니다.
5. 소스 및 대상 vCenter 목록에서 소스 및 대상 vCenter를 선택합니다.
6. *다음*을 선택하세요.

복제할 애플리케이션을 선택하고 리소스 그룹을 할당합니다.

다음 단계는 필요한 VM이나 데이터 저장소를 기능적 리소스 그룹으로 그룹화하는 것입니다. 리소스 그룹을 사용하면 공통 스냅샷으로 일련의 VM이나 데이터 저장소를 보호할 수 있습니다.

복제 계획에서 애플리케이션을 선택하면 계획에 있는 각 VM 또는 데이터 저장소의 운영 체제를 볼 수 있습니다. 이는 리소스 그룹에서 VM이나 데이터 저장소를 어떻게 그룹화할지 결정하는 데 유용합니다.

각 리소스 그룹에는 하나 이상의 VM이나 데이터 저장소가 포함될 수 있습니다.

리소스 그룹을 만들 때 다음 사항을 고려하세요.

- 리소스 그룹에 데이터 저장소를 추가하기 전에 먼저 VM의 수동 검색이나 예약된 검색을 시작하세요. 이렇게 하면 VM이 검색되어 리소스 그룹에 나열됩니다. 수동 검색을 트리거하지 않으면 VM이 리소스 그룹에 나열되지 않을 수 있습니다.
- 데이터 저장소에 최소한 하나의 VM이 있는지 확인하세요. 데이터 저장소에 VM이 없으면 데이터 저장소가 검색되지 않습니다.
- 단일 데이터 저장소는 두 개 이상의 복제 계획으로 보호되는 VM을 호스팅해서는 안 됩니다.
- 동일한 데이터 저장소에 보호된 VM과 보호되지 않은 VM을 호스팅하지 마세요. 보호된 VM과 보호되지 않은 VM이 동일한 데이터 저장소에 호스팅되는 경우 다음과 같은 문제가 발생할 수 있습니다.
  - NetApp Disaster Recovery SnapMirror 사용하고 시스템이 ONTAP 볼륨 전체를 복제하므로 해당 볼륨의 사용된 용량은 라이선싱 고려 사항에 사용됩니다. 이 경우 보호된 VM과 보호되지 않은 VM이 모두 사용하는 볼륨 공간이 이 계산에 포함됩니다.
  - 리소스 그룹과 연관된 데이터 저장소를 재해 복구 사이트로 장애 조치해야 하는 경우, 장애 조치 프로세스를 통해 보호되지 않은 VM(리소스 그룹에 속하지 않지만 ONTAP 볼륨에 호스팅된 VM)이 소스 사이트에 더 이상 존재하지 않게 되므로 소스 사이트의 보호되지 않은 VM이 실패하게 됩니다. 또한 NetApp Disaster Recovery 장애 조치 vCenter 사이트에서 보호되지 않은 VM을 시작하지 않습니다.
- VM을 보호하려면 리소스 그룹에 포함되어야 합니다.

VMS가 동일한 IP 주소를 사용하여 프로덕션 네트워크에 연결되는 것을 방지하기 위해 장애 조치 테스트를 위한 별도의 전용 매핑 세트를 만듭니다.

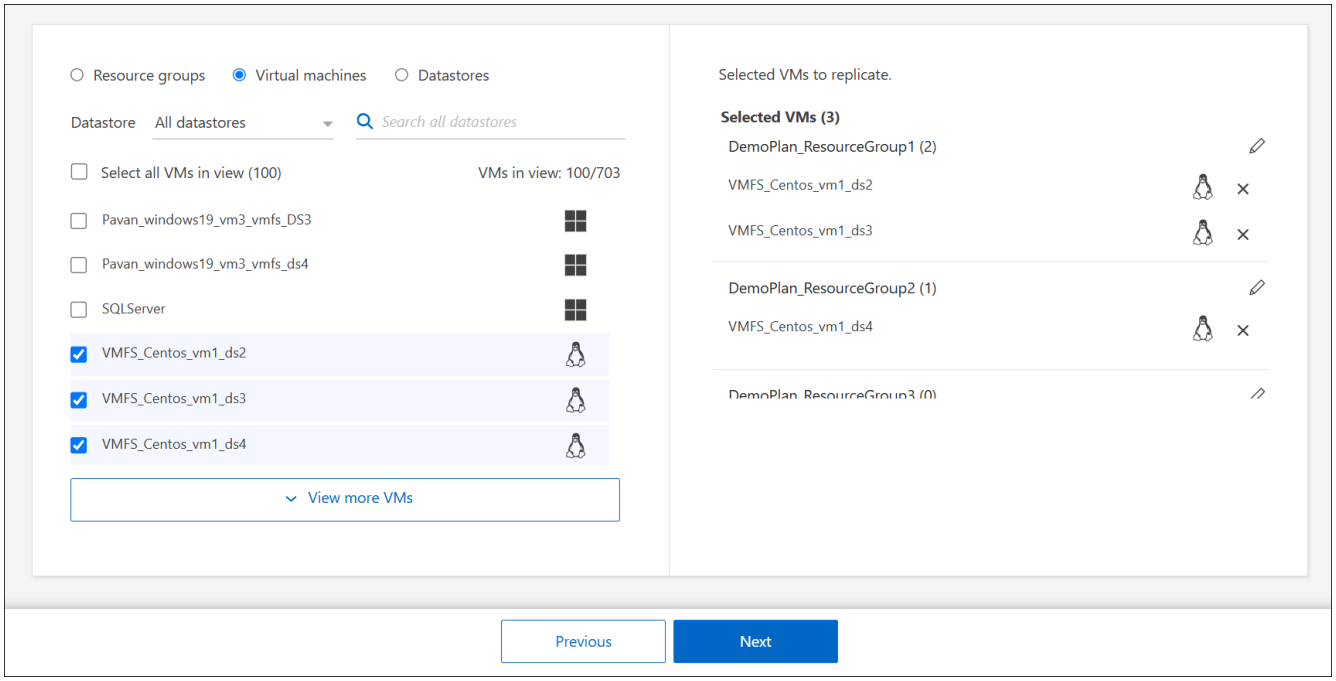
단계

1. 가상 머신 또는 *데이터 저장소*를 선택하세요.
2. 선택적으로 특정 VM이나 데이터 저장소를 이름으로 검색할 수 있습니다.
3. 애플리케이션 페이지의 왼쪽에서 보호하려는 VM이나 데이터 저장소를 선택하고 선택한 그룹에 할당합니다.

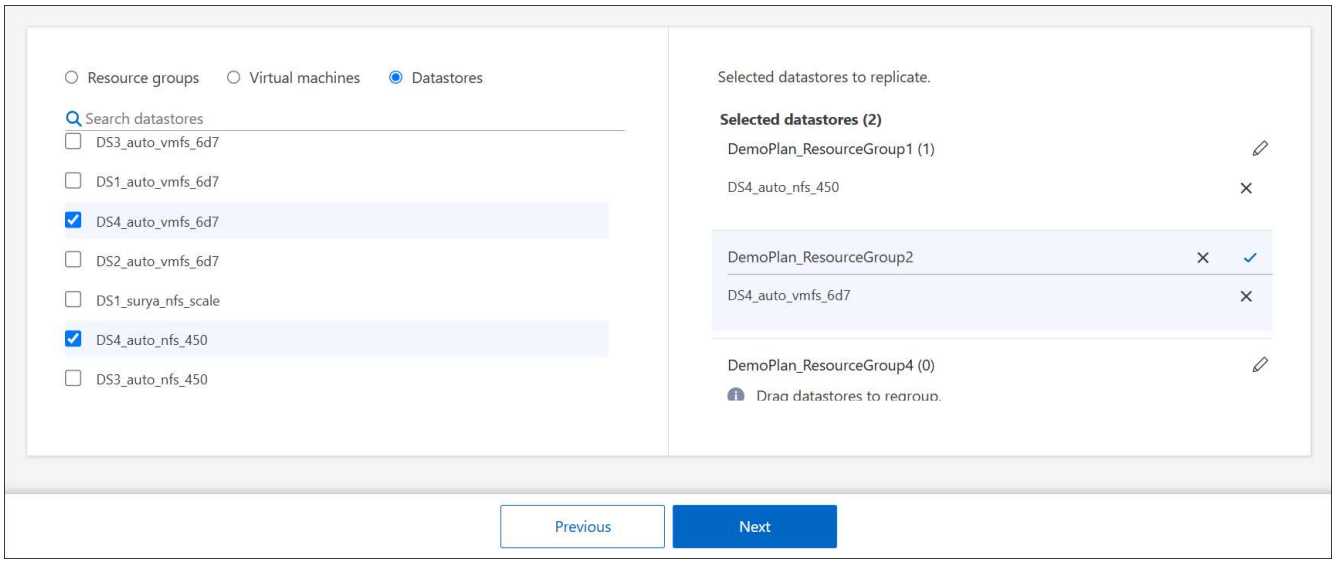
   소스 vCenter는 온프레미스 vCenter에 있어야 합니다. 대상 vCenter는 동일 사이트 또는 원격 사이트에 있는 두 번째 온프레미스 vCenter이거나, VMware Cloud on AWS와 같은 클라우드 기반 소프트웨어 정의 데이터 센터(SDDC)일 수 있습니다. 두 vCenter 모두 재해 복구 작업 환경에 이미 추가되어 있어야 합니다.

   선택한 리소스는 자동으로 그룹 1에 추가되고 새로운 그룹 2가 시작됩니다. 마지막 그룹에 리소스를 추가할 때마다

다른 그룹이 추가됩니다.



또는 데이터 저장소의 경우:



4. 선택적으로 다음 중 하나를 수행하세요.
   - 그룹 이름을 변경하려면 그룹 *편집*을 클릭하세요. 상.
   - 그룹에서 리소스를 제거하려면 리소스 옆에 있는 *X*를 선택하세요.
   - 리소스를 다른 그룹으로 이동하려면 해당 리소스를 새 그룹으로 끌어다 놓으세요.

> 데이터 저장소를 다른 리소스 그룹으로 이동하려면 원치 않는 데이터 저장소의 선택을 취소하고 복제 계획을 제출합니다. 그런 다음 다른 복제 계획을 만들거나 편집하고 데이터 저장소를 다시 선택합니다.

5. *다음*을 선택하세요.

소스 리소스를 대상에 매핑합니다.

리소스 매핑 단계에서는 소스 환경의 리소스를 대상에 매핑하는 방법을 지정합니다. 복제 계획을 만들 때 계획에 있는 각 VM에 대한 부팅 지연과 순서를 설정할 수 있습니다. 이를 통해 VM이 시작되는 순서를 설정할 수 있습니다.

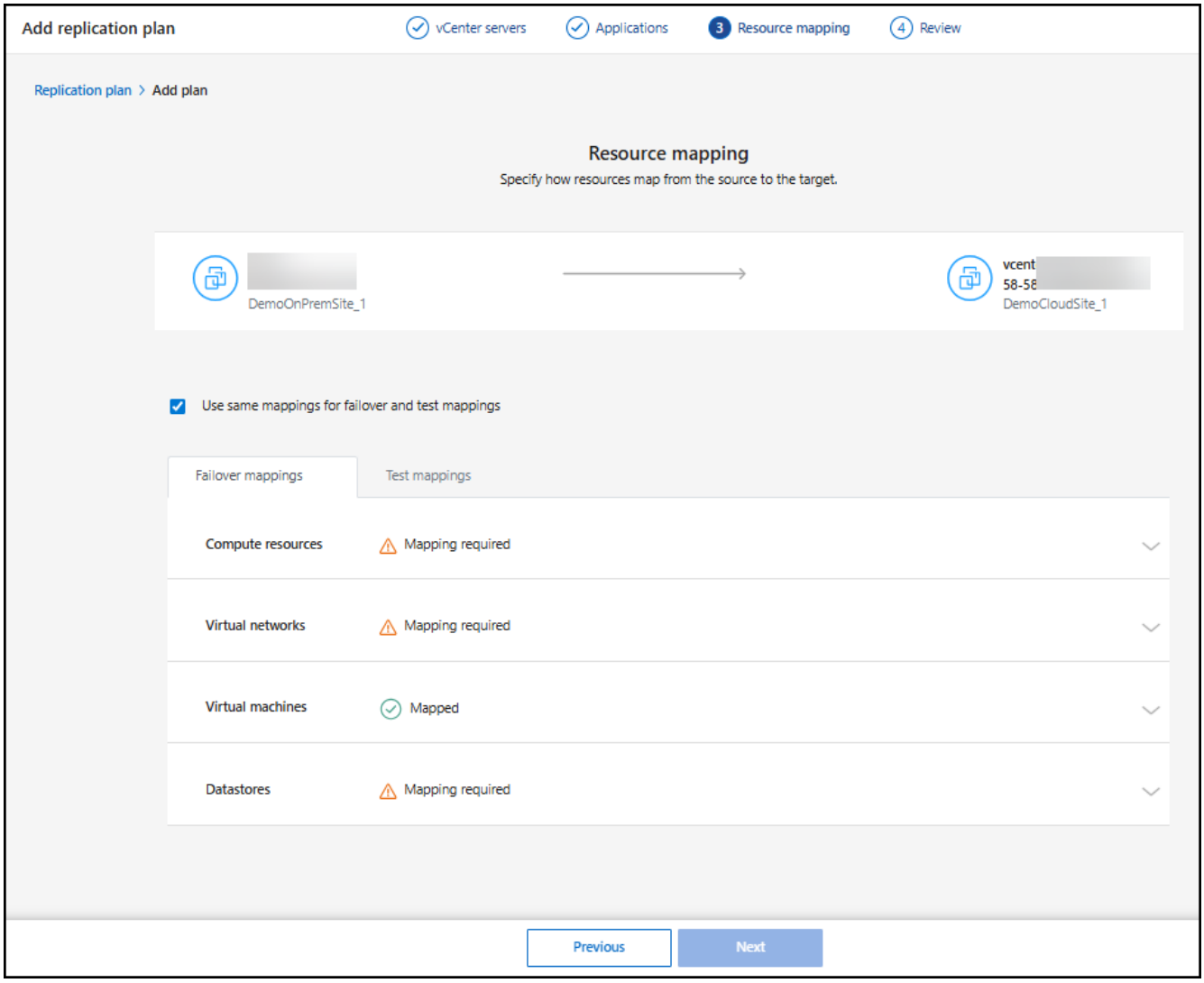
DR 계획의 일부로 테스트 장애 조치를 수행하려는 경우 장애 조치 테스트 중에 시작된 VM이 프로덕션 VM을 방해하지 않도록 테스트 장애 조치 매핑 세트를 제공해야 합니다. 테스트 VM에 다른 IP 주소를 제공하거나 테스트 VM의 가상 NIC를 프로덕션과 분리되어 있지만 IP 구성은 동일한 다른 네트워크(버블 또는 테스트 네트워크라고 함)에 매핑하여 이를 달성할 수 있습니다.

시작하기 전에

이 서비스에서 SnapMirror 관계를 생성하려면 클러스터와 해당 SVM 피어링이 NetApp Disaster Recovery 외부에서 이미 설정되어 있어야 합니다.

단계

1. 리소스 매핑 페이지에서 장애 조치 및 테스트 작업 모두에 동일한 매핑을 사용하려면 확인란을 선택하십시오.



2. 장애 조치 매핑 탭에서 각 리소스 오른쪽에 있는 아래쪽 화살표를 선택하고 각 섹션의 리소스를 매핑합니다.

- 컴퓨팅 리소스
- 가상 네트워크
- 가상 머신
- 데이터 저장소

맵 리소스 **>** 컴퓨팅 리소스 섹션

컴퓨팅 리소스 섹션은 장애 조치 후 VM이 복원될 위치를 정의합니다. 소스 vCenter 데이터 센터와 클러스터를 대상 데이터 센터와 클러스터에 매핑합니다.

선택적으로 VM을 특정 vCenter ESXi 호스트에서 다시 시작할 수 있습니다. VMWare DRS가 활성화된 경우, DR 구성 정책을 충족하기 위해 필요한 경우 VM을 자동으로 대체 호스트로 이동할 수 있습니다.

선택적으로, 이 복제 계획에 있는 모든 VM을 vCenter의 고유한 폴더에 넣을 수 있습니다. 이를 통해 vCenter 내에서 장애 조치된 VM을 빠르게 구성할 수 있는 쉬운 방법이 제공됩니다.

컴퓨팅 리소스 옆에 있는 아래쪽 화살표를 선택합니다.

- 소스 및 대상 데이터 센터
- 대상 클러스터
- 대상 호스트 (선택 사항): 클러스터를 선택한 후 이 정보를 설정할 수 있습니다.

vCenter에 클러스터의 여러 호스트를 관리하도록 구성된 DRS(분산 리소스 스케줄러)가 있는 경우 호스트를 선택할 필요가 없습니다. 호스트를 선택하면 NetApp Disaster Recovery 모든 VM을 선택한 호스트에 배치합니다. * 대상 **VM** 폴더 (선택 사항): 선택한 VM을 저장할 새 루트 폴더를 만듭니다.

맵 리소스 **>** 가상 네트워크 섹션

VM은 가상 네트워크에 연결된 가상 NIC를 사용합니다. 장애 조치 프로세스에서 서비스는 이러한 가상 NIC를 대상 VMware 환경에 정의된 가상 네트워크에 연결합니다. 리소스 그룹의 VM에서 사용하는 각 소스 가상 네트워크에 대해 서비스에는 대상 가상 네트워크 할당이 필요합니다.

동일한 대상 가상 네트워크에 여러 개의 소스 가상 네트워크를 할당할 수 있습니다. 하지만 이로 인해 IP 네트워크 구성 충돌이 발생할 수 있습니다. 여러 개의 소스 네트워크를 단일 대상 네트워크에 매핑하여 모든 소스 네트워크가 동일한 구성을 갖도록 할 수 있습니다.

장애 조치 매핑 탭에서 가상 네트워크 옆에 있는 아래쪽 화살표를 선택합니다. 소스 가상 LAN과 대상 가상 LAN을 선택합니다.

적절한 가상 LAN에 대한 네트워크 매핑을 선택합니다. 가상 LAN은 이미 프로비저닝되어 있으므로 VM을 매핑할 적절한 가상 LAN을 선택하세요.

맵 리소스 **>** 가상 머신 섹션

다음 옵션 중 하나를 설정하여 복제 계획으로 보호되는 리소스 그룹의 각 VM을 대상 vCenter 가상 환경에 맞게 구성할 수 있습니다.

- 가상 CPU의 수

- 가상 DRAM의 양
- IP 주소 구성
- 장애 조치 프로세스의 일부로 게스트 OS 셸 스크립트를 실행하는 기능
- 고유한 접두사와 접미사를 사용하여 장애 조치된 VM 이름을 변경하는 기능
- VM 장애 조치 중 재시작 순서를 설정하는 기능

장애 조치 매핑 탭에서 가상 머신 옆에 있는 아래쪽 화살표를 선택합니다.

VM의 기본값은 매핑됩니다. 기본 매핑은 VM이 프로덕션 환경에서 사용하는 것과 동일한 설정(동일한 IP 주소, 서브넷 마스크, 게이트웨이)을 사용합니다.

기본 설정을 변경하는 경우 대상 IP 필드를 "소스와 다름"으로 변경해야 합니다.

설정을 "소스와 다름"으로 변경하는 경우 VM 게스트 OS 자격 증명을 제공해야 합니다.

이 섹션에는 선택 사항에 따라 다양한 필드가 표시될 수 있습니다.

장애 조치된 각 VM에 할당된 가상 CPU 수를 늘리거나 줄일 수 있습니다. 하지만 각 VM에는 최소한 하나의 가상 CPU가 필요합니다. 각 VM에 할당된 가상 CPU와 가상 DRAM의 수를 변경할 수 있습니다. 기본 가상 CPU 및 가상 DRAM 설정을 변경하려는 가장 일반적인 이유는 대상 vCenter 클러스터 노드에 소스 vCenter 클러스터만큼 사용 가능한 리소스가 많지 않은 경우입니다.

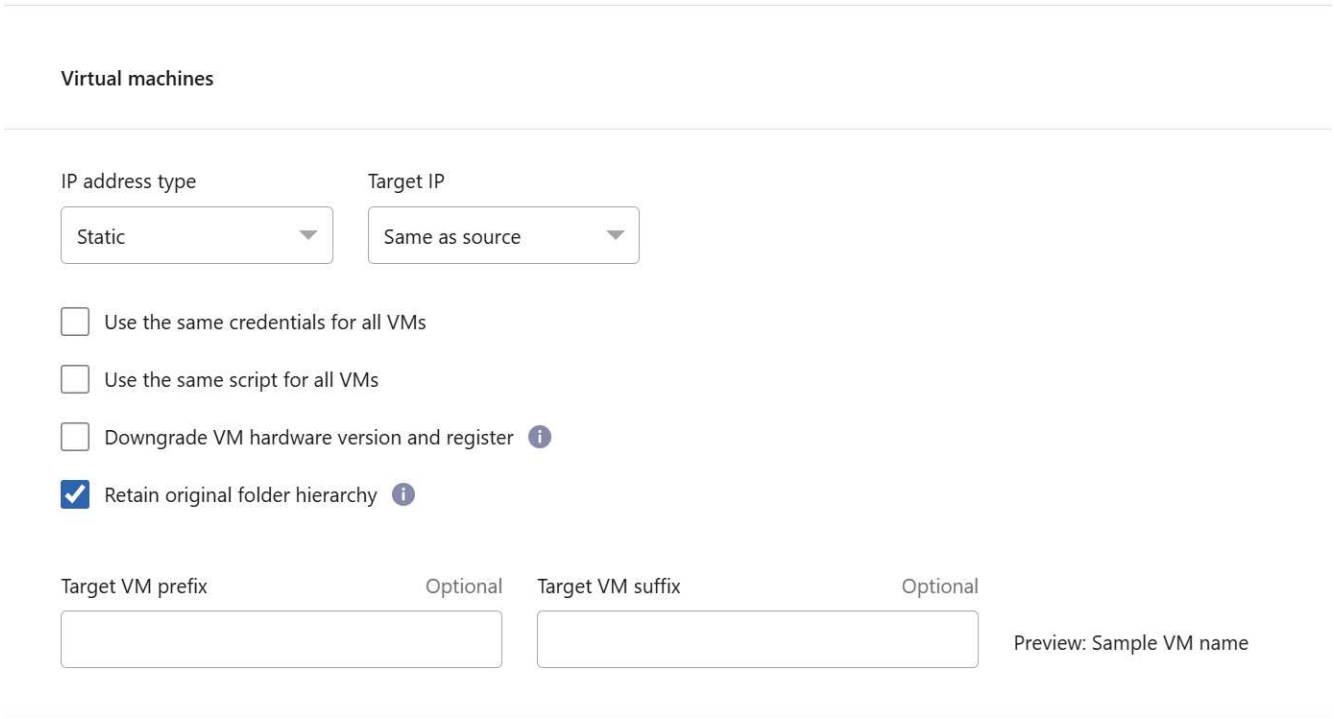
네트워크 설정 재해 복구는 VM 네트워크에 대한 광범위한 구성 옵션을 지원합니다. 대상 사이트에 소스 사이트의 프로덕션 가상 네트워크와 다른 TCP/IP 설정을 사용하는 가상 네트워크가 있는 경우 이를 변경해야 할 수도 있습니다.

가장 기본적인(기본) 수준에서 설정은 대상 사이트의 각 VM에 대해 소스 사이트에서 사용되는 것과 동일한 TCP/IP 네트워크 설정을 사용합니다. 이렇게 하려면 소스 및 대상 가상 네트워크에서 동일한 TCP/IP 설정을 구성해야 합니다.

이 서비스는 VM에 대한 정적 또는 동적 호스트 구성 프로토콜(DHCP) IP 구성의 네트워크 설정을 지원합니다. DHCP는 호스트 네트워크 포트의 TCP/IP 설정을 동적으로 구성하는 표준 기반 방법을 제공합니다. DHCP는 최소한 TCP/IP 주소를 제공해야 하며, 기본 게이트웨이 주소(외부 인터넷 연결로 라우팅하기 위한), 서브넷 마스크, DNS 서버 주소도 제공할 수 있습니다. DHCP는 일반적으로 직원의 데스크톱, 노트북, 휴대폰 연결과 같은 최종 사용자 컴퓨팅 장치에 사용되지만 서버와 같은 모든 네트워킹 컴퓨팅 장치에도 사용될 수 있습니다.

- 동일한 서브넷 마스크**, DNS** 및 게이트웨이 설정 사용 옵션: 이러한 설정은 일반적으로 동일한 가상 네트워크에 연결된 모든 VM에서 동일하므로 한 번만 구성하고 재해 복구에서 복제 계획으로 보호되는 리소스 그룹의 모든 VM에 대한 설정을 사용하는 것이 더 쉬울 수 있습니다. 일부 VM이 다른 설정을 사용하는 경우 이 상자의 선택을 취소하고 각 VM에 대해 해당 설정을 제공해야 합니다.
- **IP** 주소 유형: 대상 가상 네트워크 요구 사항에 맞게 VM 구성을 재구성합니다. NetApp Disaster Recovery DHCP 또는 정적 IP의 두 가지 옵션을 제공합니다. 고정 IP의 경우 서브넷 마스크, 게이트웨이, DNS 서버를 구성합니다. 또한 VM에 대한 자격 증명을 입력하세요.
  - **DHCP**: VM이 DHCP 서버에서 네트워크 구성 정보를 가져오도록 하려면 이 설정을 선택합니다. 이 옵션을 선택하면 VM에 대한 자격 증명만 제공됩니다.
  - 고정 **IP**: IP 구성 정보를 수동으로 지정하려면 이 설정을 선택하세요. 다음 중 하나를 선택할 수 있습니다: 소스와 동일, 소스와 다름, 서브넷 매핑. 출처와 동일한 것을 선택하면 자격 증명을 입력할 필요가 없습니다. 반면, 소스의 다른 정보를 사용하기로 선택한 경우 자격 증명, VM의 IP 주소, 서브넷 마스크, DNS 및 게이트웨이 정보를 제공할 수 있습니다. VM 게스트 OS 자격 증명은 글로벌 수준이나 각 VM 수준에서 제공되어야 합니다.

이 기능은 대규모 환경을 더 작은 대상 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고도 재해 복구 테스트를 수행할 때 매우 유용할 수 있습니다.



- 스크립트: 사용자 지정 게스트 OS 호스팅 스크립트를 .sh, .bat 또는 .ps1 형식으로 후처리로 포함할 수 있습니다. 사용자 지정 스크립트를 사용하면 재해 복구 시스템에서 장애 조치, 장애 복구 및 마이그레이션 프로세스 후에 해당 스크립트를 실행할 수 있습니다. 예를 들어, 사용자 지정 스크립트를 사용하여 장애 조치가 완료된 후 모든 데이터베이스 트랜잭션을 재개할 수 있습니다. 이 서비스는 명령줄 매개변수를 지원하는 Microsoft Windows 또는 지원되는 모든 Linux 변형 운영 체제를 실행하는 가상 머신 내에서 스크립트를 실행할 수 있습니다. 스크립트를 개별 VM에 할당하거나 복제 계획에 있는 모든 VM에 할당할 수 있습니다.

  VM 게스트 OS에서 스크립트 실행을 활성화하려면 다음 조건을 충족해야 합니다.

  - VM에 VMware Tools를 설치해야 합니다.
  - 스크립트를 실행하려면 적절한 사용자 자격 증명과 적절한 게스트 OS 권한이 제공되어야 합니다.
  - 선택적으로 스크립트에 대한 시간 초과 값을 초 단위로 포함합니다.

    Microsoft Windows를 실행하는 **VM**: Windows 배치(.bat) 또는 PowerShell(ps1) 스크립트를 실행할 수 있습니다. Windows 스크립트는 명령줄 인수를 사용할 수 있습니다. 각 인수의 형식을 지정하세요. `arg_name$value` 형식, 여기서 `arg_name` 는 인수의 이름입니다. `$value` 인수의 값이며 세미콜론으로 각각을 구분합니다. `argument$value` 쌍.

  Linux를 실행하는 **VM**: VM에서 사용하는 Linux 버전에서 지원하는 모든 셸 스크립트(.sh)를 실행할 수 있습니다. Linux 스크립트는 명령줄 인수를 사용할 수 있습니다. 세미콜론으로 구분된 값 목록으로 인수를 제공합니다. 명명된 인수는 지원되지 않습니다. 각 인수를 다음에 추가합니다. `Arg[x]` 인수 목록과 포인터를 사용하여 각 값을 참조합니다. `Arg[x]` 예를 들어 배열, `value1;value2;value3` .

- **VM** 하드웨어 버전 다운그레이드 및 등록: 대상 ESX 호스트 버전이 소스 버전보다 이전인 경우 등록 중에 일치하도록 이 옵션을 선택합니다.
- 원본 폴더 계층 구조 유지: 기본적으로 재해 복구는 장애 조치 시 VM 인벤토리 계층 구조(폴더 구조)를 유지합니다. 복구 대상에 원래 폴더 계층 구조가 없는 경우 재해 복구는 해당 계층 구조를 생성합니다.

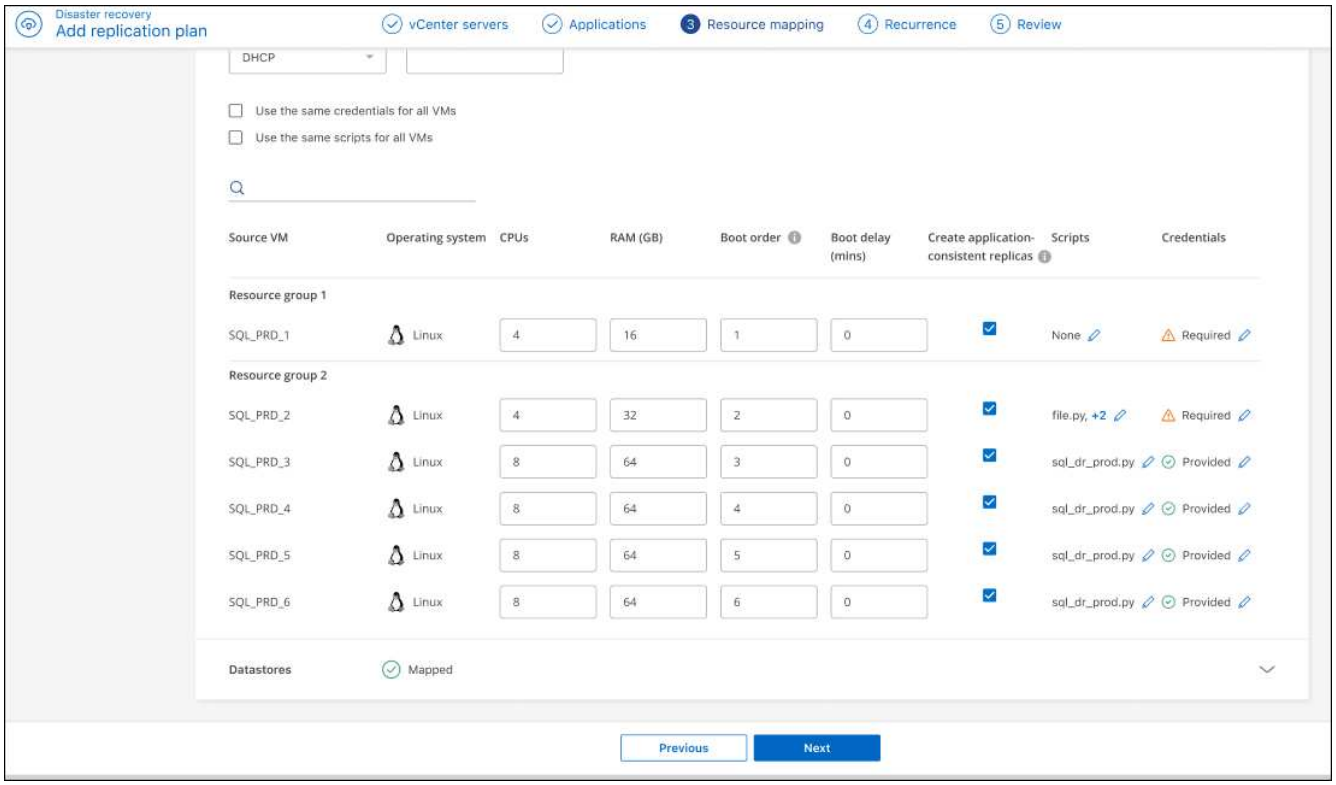
원래 폴더 계층 구조를 무시하려면 이 상자의 선택을 취소하세요.

- 대상 **VM** 접두사 및 접미사: 가상 머신 세부 정보에서 선택적으로 장애 조치된 각 VM 이름에 접두사와 접미사를 추가할 수 있습니다. 이는 동일한 vCenter 클러스터에서 실행되는 프로덕션 VM과 장애 조치된 VM을 구별하는 데 도움이 될 수 있습니다. 예를 들어, VM 이름에 "DR-" 접두사와 "-failover" 접미사를 추가할 수 있습니다. 일부 사람들은 재해 발생 시 다른 사이트에서 일시적으로 VM을 호스팅하기 위해 두 번째 프로덕션 vCenter를 추가합니다. 접두사나 접미사를 추가하면 장애 조치된 VM을 빠르게 식별하는 데 도움이 될 수 있습니다. 사용자 정의 스크립트에서도 접두사나 접미사를 사용할 수 있습니다.

  컴퓨팅 리소스 섹션에서 대상 VM 폴더를 설정하는 대체 방법을 사용할 수 있습니다.

- 소스 **VM CPU** 및 **RAM**: 가상 머신 세부 정보에서 선택적으로 VM CPU 및 RAM 매개변수의 크기를 조정할 수 있습니다.

  DRAM은 기가바이트(GiB) 또는 메가바이트(MiB) 단위로 구성할 수 있습니다. 각 VM에는 최소 1MiB의 RAM이 필요하지만, 실제 용량은 VM 게스트 OS와 실행 중인 모든 애플리케이션이 효율적으로 작동할 수 있을 만큼 커야 합니다.



- 부팅 순서: 리소스 그룹 전체에서 선택한 모든 가상 머신에 대한 장애 조치 후 부팅 순서를 수정할 수 있습니다. 기본적으로 모든 VM은 병렬로 부팅됩니다. 하지만 이 단계에서 변경할 수 있습니다. 이는 후속 우선순위 VM이 시작되기 전에 모든 우선순위 1 VM이 실행 중인지 확인하는 데 유용합니다.

  재해 복구는 부팅 순서 번호가 같은 모든 가상 머신을 병렬로 부팅합니다.

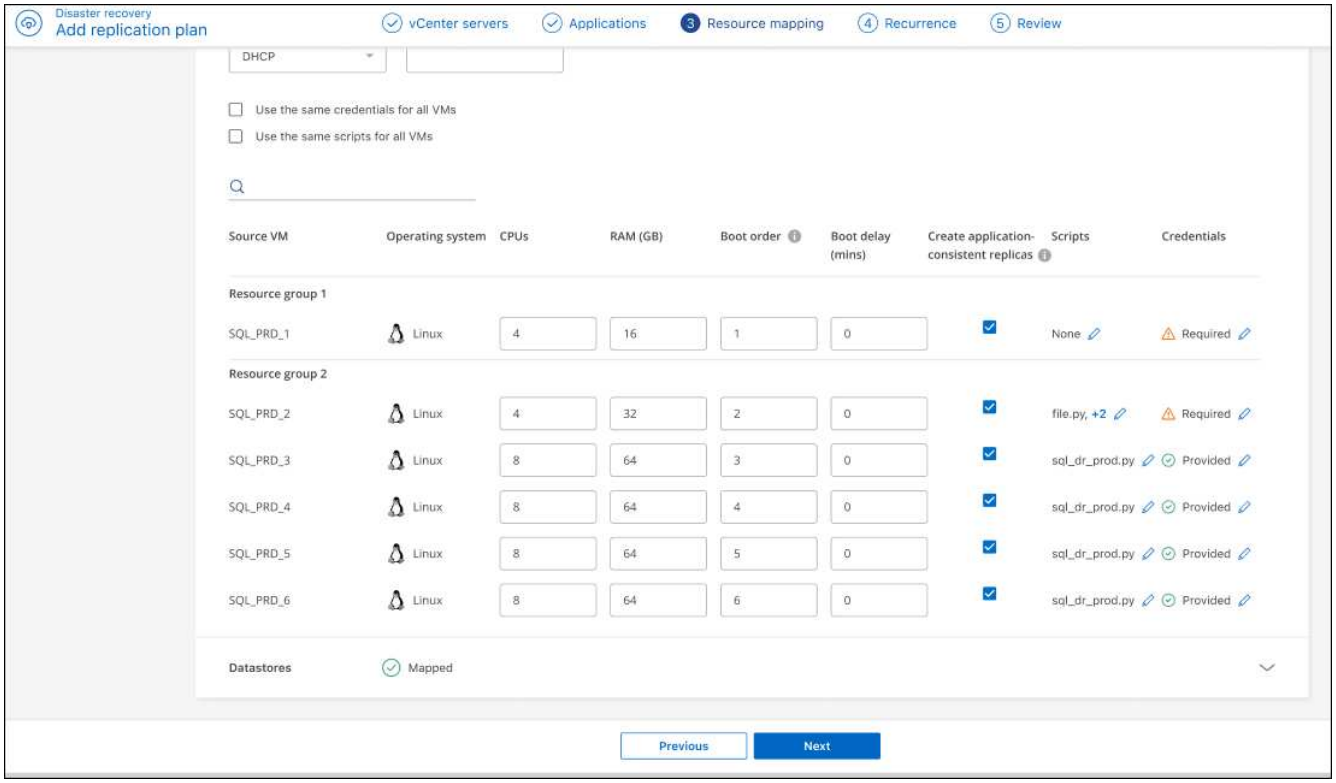
  - 순차 부팅: 각 VM에 고유한 번호를 지정하여 지정된 순서대로 부팅합니다(예: 1, 2, 3, 4, 5).
  - 동시 부팅: 모든 VM에 동일한 번호를 할당하여 동시에 부팅합니다(예: 1,1,1,1,2,2,3,4,4).

- 부팅 지연: 부팅 작업의 지연 시간을 분 단위로 조정합니다. 이는 VM이 전원 켜기 프로세스를 시작하기 전에 기다리는 시간을 나타냅니다. 0~10분 사이의 값을 입력하세요.

부팅 순서를 기본값으로 재설정하려면 *VM 설정을 기본값으로 재설정*을 선택한 다음 기본값으로 다시 변경할 설정을 선택합니다.

- 애플리케이션 일관성 복제본 생성: 애플리케이션 일관성 스냅샷 복사본을 생성할지 여부를 나타냅니다. 이 서비스는 애플리케이션을 정지시킨 다음 스냅샷을 찍어 애플리케이션의 일관된 상태를 얻습니다. 이 기능은 Windows 및 Linux에서 실행되는 Oracle과 Windows에서 실행되는 SQL Server에서 지원됩니다. 자세한 내용은 다음을 참조하세요.
- **Windows LAPS** 사용: Windows 로컬 관리자 암호 솔루션(Windows LAPS)을 사용하는 경우 이 상자를 선택하세요. 이 옵션은 고정 **IP** 옵션을 선택한 경우에만 사용할 수 있습니다. 이 상자를 선택하면 각 가상 머신에 대한 비밀번호를 제공할 필요가 없습니다. 대신 도메인 컨트롤러 세부 정보를 제공하세요.

  Windows LAPS를 사용하지 않는 경우 VM은 Windows VM이고 VM 행의 자격 증명 옵션이 활성화됩니다. VM에 대한 자격 증명을 제공할 수 있습니다.



애플리케이션과 일관된 복제본 생성

많은 VM은 Oracle이나 Microsoft SQL Server와 같은 데이터베이스 서버를 호스팅합니다. 이러한 데이터베이스 서버에는 스냅샷이 생성될 때 데이터베이스가 일관된 상태를 유지하도록 애플리케이션과 일관된 스냅샷이 필요합니다.

애플리케이션 일관성 스냅샷은 스냅샷이 생성될 때 데이터베이스가 일관된 상태임을 보장합니다. 이는 장애 조치 또는 장애 복구 작업 후에 데이터베이스를 일관된 상태로 복원할 수 있도록 보장하기 때문에 중요합니다.

데이터베이스 서버에서 관리하는 데이터는 데이터베이스 서버를 호스팅하는 VM과 동일한 데이터 저장소에 호스팅될 수도 있고, 다른 데이터 저장소에 호스팅될 수도 있습니다. 다음 표는 재해 복구에서 애플리케이션 일관성 스냅샷에 지원되는 구성을 보여줍니다.

데이터 위치	지원됨	노트
VM과 동일한 vCenter 데이터 저장소 내	예	데이터베이스 서버와 데이터베이스가 모두 동일한 데이터 저장소에 있으므로 장애 조치 시 서버와 데이터가 모두 동기화됩니다.
VM의 다른 vCenter 데이터 저장소 내에서	아니요	재해 복구는 데이터베이스 서버의 데이터가 다른 vCenter 데이터 저장소에 있는 경우를 식별할 수 없습니다. 서비스는 데이터를 복제할 수 없지만 데이터베이스 서버 VM은 복제할 수 있습니다. 데이터베이스 데이터를 복제할 수는 없지만, 이 서비스는 데이터베이스 서버가 VM 백업 시점에 데이터베이스가 정지되도록 모든 필수 단계를 수행하도록 보장합니다.
외부 데이터 소스 내에서	아니요	데이터가 게스트 마운트된 LUN이나 NFS 공유에 있는 경우 재해 복구는 데이터를 복제할 수 없지만 데이터베이스 서버 VM은 복제할 수 있습니다. 데이터베이스 데이터를 복제할 수는 없지만, 이 서비스는 데이터베이스 서버가 VM 백업 시점에 데이터베이스가 정지되도록 모든 필수 단계를 수행하도록 보장합니다.

예약된 백업 중에 재해 복구는 데이터베이스 서버를 중지한 다음 데이터베이스 서버를 호스팅하는 VM의 스냅샷을 만듭니다. 이렇게 하면 스냅샷을 찍을 때 데이터베이스가 일관된 상태를 유지하게 됩니다.

- Windows VM의 경우, 서비스는 Microsoft 볼륨 섀도 복사본 서비스(VSS)를 사용하여 두 데이터베이스 서버와 조정합니다.
- Linux VM의 경우, 이 서비스는 일련의 스크립트를 사용하여 Oracle 서버를 백업 모드로 전환합니다.

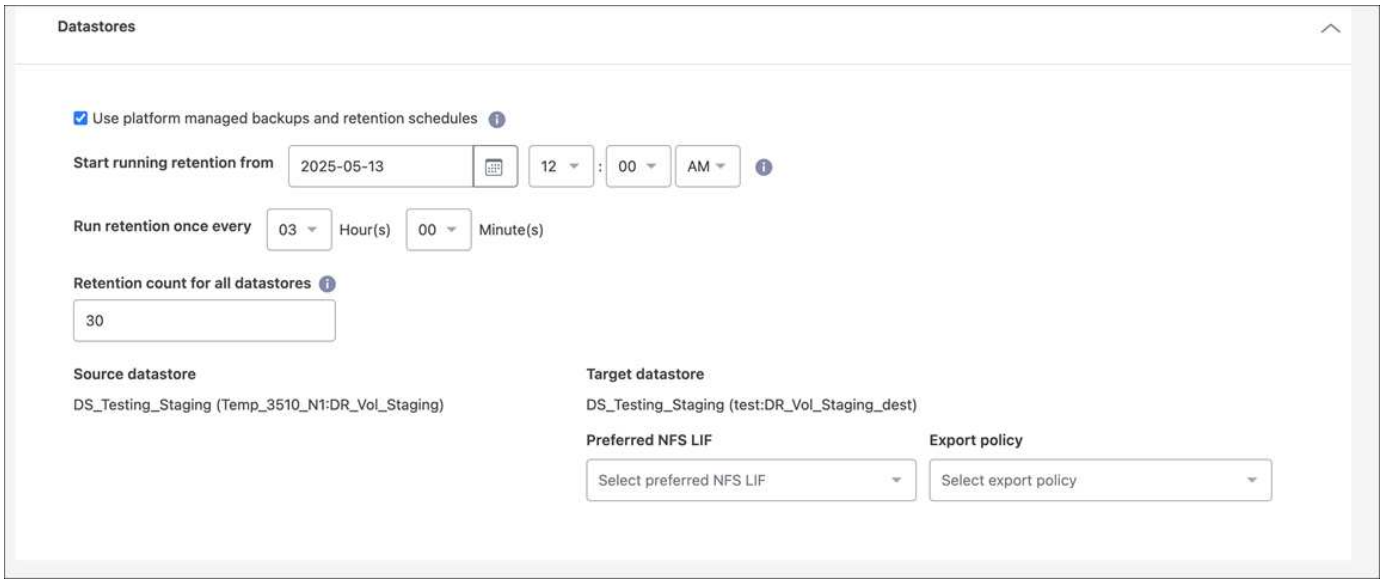
VM과 호스팅 데이터 저장소의 애플리케이션 일관성 복제본을 활성화하려면 각 VM에 대해 애플리케이션 일관성 복제본 만들기 옆의 상자를 선택하고 적절한 권한이 있는 게스트 로그인 자격 증명을 제공합니다.

맵 리소스 **>** 데이터 저장소 섹션

VMware 데이터스토어는 ONTAP FlexVol 볼륨이나 VMware VMFS를 사용하는 ONTAP iSCSI 또는 FC LUN에 호스팅됩니다. 데이터 저장소 섹션을 사용하여 대상 ONTAP 클러스터, 스토리지 가상 머신(SVM), 볼륨 또는 LUN을 정의하여 디스크 데이터를 대상에 복제합니다.

데이터 저장소 옆에 있는 아래쪽 화살표를 선택하세요. VM 선택에 따라 데이터 저장소 매핑이 자동으로 선택됩니다.

이 섹션은 선택에 따라 활성화되거나 비활성화될 수 있습니다.



- 플랫폼 관리 백업 및 보존 일정 사용: 외부 스냅샷 관리 솔루션을 사용하는 경우 이 상자를 선택하세요. NetApp Disaster Recovery 기본 ONTAP SnapMirror 정책 스케줄러나 타사 통합과 같은 외부 스냅샷 관리 솔루션의 사용을 지원합니다. 복제 계획의 모든 데이터 저장소(볼륨)에 이미 다른 곳에서 관리되는 SnapMirror 관계가 있는 경우 NetApp Disaster Recovery 에서 해당 스냅샷을 복구 지점으로 사용할 수 있습니다.

  이 옵션을 선택하면 NetApp Disaster Recovery 백업 일정을 구성하지 않습니다. 그러나 테스트, 장애 조치 및 장애 복구 작업을 위해 스냅샷이 계속 생성될 수 있으므로 보존 일정을 구성해야 합니다.

  이것이 구성된 후에는 서비스가 정기적으로 예약된 스냅샷을 찍지 않고 대신 외부 엔터티를 사용하여 해당 스냅샷을 찍고 업데이트합니다.

- 시작 시간: 백업 및 보존을 시작할 날짜와 시간을 입력합니다.
- 실행 간격: 시간 간격을 시간과 분으로 입력하세요. 예를 들어, 1시간을 입력하면 서비스는 매 시간 스냅샷을 찍습니다.
- 보존 횟수: 보존하려는 스냅샷 수를 입력하세요.

  각 스냅샷 간의 데이터 변경률과 함께 보관되는 스냅샷 수는 소스와 대상 모두에서 사용되는 저장 공간의 양을 결정합니다. 더 많은 스냅샷을 보관할수록 더 많은 저장 공간이 사용됩니다.

- 소스 및 대상 데이터 저장소: 여러 개의 (팬아웃) SnapMirror 관계가 있는 경우 사용할 대상을 선택할 수 있습니다. 볼륨에 이미 SnapMirror 관계가 설정된 경우 해당 소스 및 대상 데이터 저장소가 나타납니다. SnapMirror 관계가 없는 볼륨의 경우 대상 클러스터를 선택하고, 대상 SVM을 선택하고, 볼륨 이름을 제공하여 지금 SnapMirror 관계를 만들 수 있습니다. 이 서비스는 볼륨과 SnapMirror 관계를 생성합니다.

  이 서비스에서 SnapMirror 관계를 생성하려면 클러스터와 해당 SVM 피어링이 NetApp Disaster Recovery 외부에서 이미 설정되어 있어야 합니다.

  - VM이 동일한 볼륨과 동일한 SVM에 속하는 경우 서비스는 표준 ONTAP 스냅샷을 수행하고 보조 대상을 업데이트합니다.
  - VM이 서로 다른 볼륨에 있고 동일한 SVM에 있는 경우 서비스는 모든 볼륨을 포함하여 일관성 그룹 스냅샷을 만들고 보조 대상을 업데이트합니다.
  - VM이 서로 다른 볼륨과 SVM에 속하는 경우 서비스는 동일하거나 다른 클러스터에 있는 모든 볼륨을 포함하여 일관성 그룹 시작 단계와 커밋 단계 스냅샷을 수행하고 보조 대상을 업데이트합니다.

◦ 장애 조치 중에 원하는 스냅샷을 선택할 수 있습니다. 최신 스냅샷을 선택하면 서비스는 주문형 백업을 생성하고, 대상을 업데이트하고, 해당 스냅샷을 장애 조치에 사용합니다.

- 선호하는 **NFS LIF** 및 내보내기 정책: 일반적으로 서비스에서 선호하는 NFS LIF 및 내보내기 정책을 선택하게 합니다. 특정 NFS LIF 또는 내보내기 정책을 사용하려면 각 필드 옆에 있는 아래쪽 화살표를 선택하고 적절한 옵션을 선택하세요.

  장애 조치 이벤트 후에 볼륨에 대해 특정 데이터 인터페이스(LIF)를 선택적으로 사용할 수 있습니다. 대상 SVM에 여러 개의 LIF가 있는 경우 데이터 트래픽을 분산하는 데 유용합니다.

  NAS 데이터 액세스 보안에 대한 추가 제어를 위해 서비스는 다양한 데이터 저장소 볼륨에 특정 NAS 내보내기 정책을 할당할 수 있습니다. 내보내기 정책은 데이터 저장소 볼륨에 액세스하는 NFS 클라이언트에 대한 액세스 제어 규칙을 정의합니다. 내보내기 정책을 지정하지 않으면 서비스는 SVM에 대한 기본 내보내기 정책을 사용합니다.

보호된 VM을 호스팅할 소스 및 대상 vCenter ESXi 호스트에만 볼륨 액세스를 제한하는 전용 내보내기 정책을 만드는 것이 좋습니다. 이렇게 하면 외부 엔터티가 NFS 내보내기에 액세스할 수 없습니다.

테스트 장애 조치 매핑 추가

단계

1. 테스트 환경에 대해 다른 매핑을 설정하려면 상자의 선택을 취소하고 테스트 매핑 탭을 선택합니다.
2. 이전과 마찬가지로 각 탭을 살펴보겠습니다. 하지만 이번에는 테스트 환경입니다.

   테스트 매핑 탭에서 가상 머신 및 데이터 저장소 매핑이 비활성화됩니다.

나중에 전체 계획을 테스트할 수 있습니다. 지금은 테스트 환경에 대한 매핑을 설정하고 있습니다.

복제 계획을 검토하세요

마지막으로 복제 계획을 검토하는 데 잠시 시간을 내세요.

나중에 복제 계획을 비활성화하거나 삭제할 수 있습니다.

단계

1. 각 탭의 정보를 검토하세요: 계획 세부 정보, 장애 조치 매핑 및 VM.
2. *플랜 추가*를 선택하세요.

   해당 계획이 계획 목록에 추가되었습니다.

규정 준수를 테스트하고 장애 조치 테스트가 작동하는지 확인하기 위해 일정을 편집합니다.

필요할 때 올바르게 작동하는지 확인하기 위해 규정 준수 및 장애 조치 테스트를 위한 일정을 설정하는 것이 좋습니다.

- 규정 준수 시간 영향: 복제 계획이 생성되면 서비스는 기본적으로 규정 준수 일정을 생성합니다. 기본 준수 시간은 30분입니다. 이 시간을 변경하려면 복제 계획에서 일정을 편집하면 됩니다.
- 테스트 장애 조치 영향: 요청 시 또는 일정에 따라 장애 조치 프로세스를 테스트할 수 있습니다. 이를 통해 복제

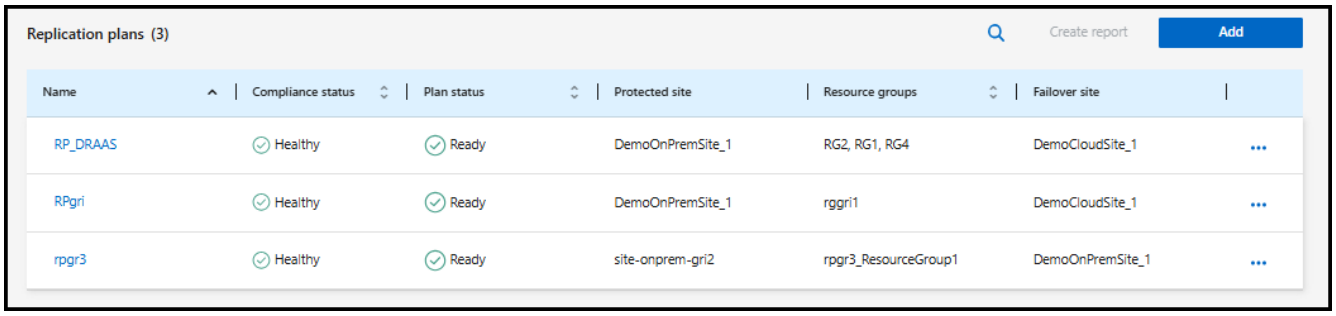
계획에 지정된 대상으로 가상 머신의 장애 조치를 테스트할 수 있습니다.

테스트 장애 조치는 FlexClone 볼륨을 생성하고, 데이터 저장소를 마운트하고, 해당 데이터 저장소로 작업 부하를 이동합니다. 테스트 장애 조치 작업은 프로덕션 워크로드, 테스트 사이트에서 사용되는 SnapMirror 관계, 그리고 정상적으로 작동을 계속해야 하는 보호 워크로드에는 영향을 미치지 않습니다.

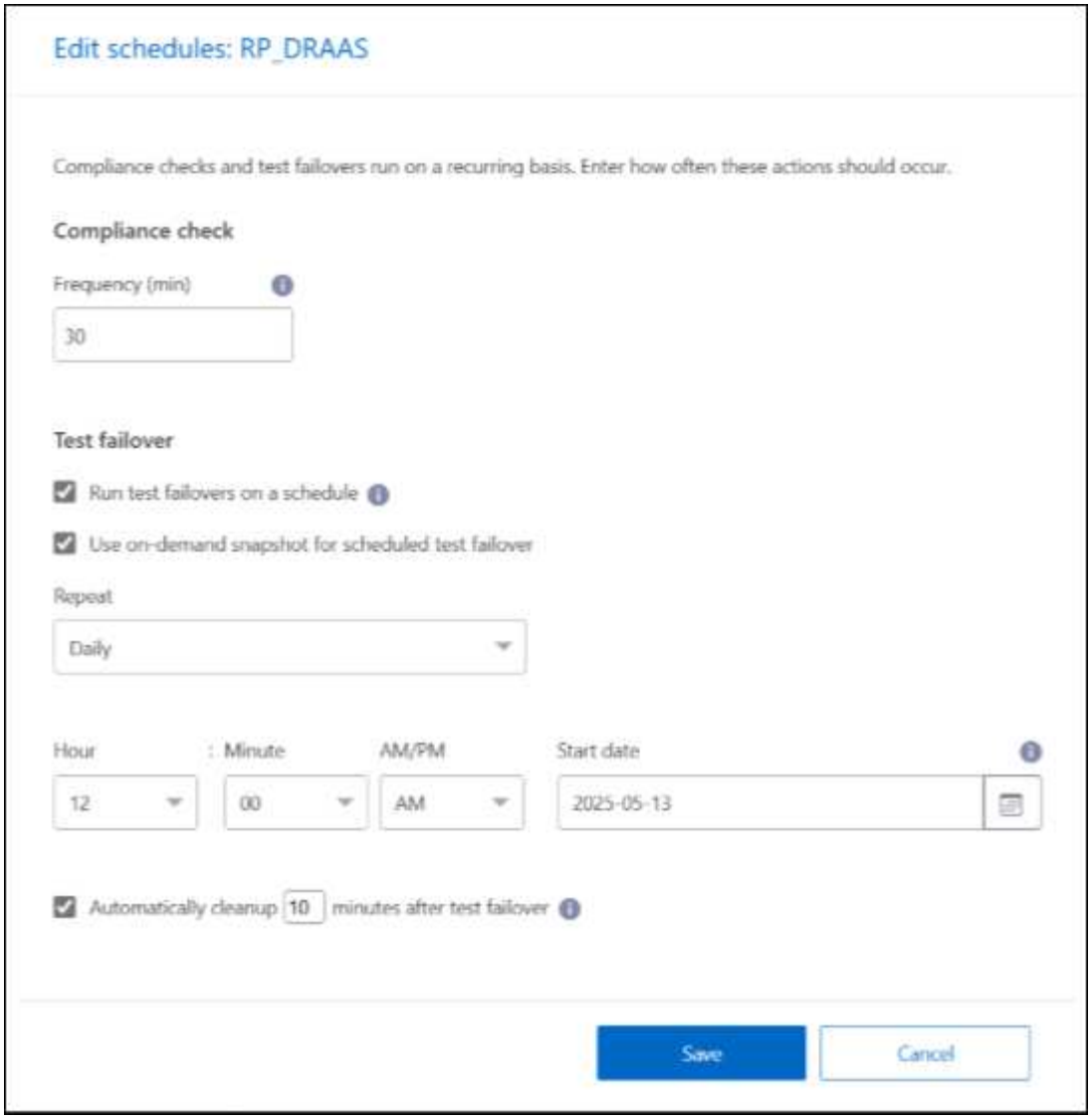
일정에 따라 장애 조치 테스트가 실행되고 워크로드가 복제 계획에 지정된 대상으로 이동하는지 확인합니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.



2. *작업*을 선택하세요 ••• 아이콘을 클릭하고 *일정 편집*을 선택하세요.
3. NetApp Disaster Recovery 테스트 규정 준수 여부를 확인하는 빈도를 분 단위로 입력합니다.
4. 장애 조치 테스트가 정상적으로 진행되는지 확인하려면 *매월 일정에 따라 장애 조치 실행*을 선택하세요.
   a. 테스트를 실행할 날짜와 시간을 선택하세요.
   b. 테스트를 시작할 날짜를 yyyy-mm-dd 형식으로 입력하세요.



5. 예약된 테스트 장애 조치에 주문형 스냅샷 사용: 자동 테스트 장애 조치를 시작하기 전에 새 스냅샷을 찍으려면 이 상자를 선택하세요.
6. 장애 조치 테스트가 완료된 후 테스트 환경을 정리하려면 *테스트 장애 조치 후 자동으로 정리*를 선택하고 정리가 시작되기 전까지 기다릴 시간(분)을 입력합니다.

> 이 프로세스는 테스트 위치에서 임시 VM의 등록을 해제하고, 생성된 FlexClone 볼륨을 삭제하고, 임시 데이터 저장소의 마운트를 해제합니다.

7. *저장*을 선택하세요.

NetApp Disaster Recovery 사용하여 다른 사이트에 애플리케이션 복제

NetApp Disaster Recovery 사용하면 SnapMirror 복제를 사용하여 소스 사이트의 VMware 앱을 클라우드의 재해 복구 원격 사이트로 복제할 수 있습니다.

재해 복구 계획을 만들고 마법사에서 재발을 식별하고 재해 복구 사이트로 복제를 시작하면 NetApp Disaster Recovery 30분마다 복제가 실제로 계획에 따라 발생하는지 확인합니다. 작업 모니터 페이지에서 진행 상황을 모니터링할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 장애 조치 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

시작하기 전에

복제를 시작하기 전에 복제 계획을 만들고 앱을 복제하도록 선택해야 합니다. 그러면 작업 메뉴에 복제 옵션이 나타납니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. 메뉴에서 *복제 계획*을 선택합니다.
4. 복제 계획을 선택하세요.
5. 오른쪽에서 작업 옵션을 선택하세요 ••• 그리고 *복제*를 선택하세요.

NetApp Disaster Recovery 사용하여 애플리케이션을 다른 사이트로 마이그레이션

NetApp Disaster Recovery 사용하면 소스 사이트의 VMware 앱을 다른 사이트로 마이그레이션할 수 있습니다.

복제 계획을 만들고 마법사에서 반복을 식별하고 마이그레이션을 시작하면 30분마다 NetApp Disaster Recovery 마이그레이션이 실제로 계획에 따라 발생하는지 확인합니다. 작업 모니터 페이지에서 진행 상황을 모니터링할 수 있습니다.

시작하기 전에

마이그레이션을 시작하기 전에 복제 계획을 만들고 앱을 마이그레이션하도록 선택해야 합니다. 그러면 작업 메뉴에 마이그레이션 옵션이 나타납니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. 메뉴에서 *복제 계획*을 선택합니다.
4. 복제 계획을 선택하세요.
5. 오른쪽에서 작업 옵션을 선택하세요 ••• *마이그레이션*을 선택하세요.

NetApp Disaster Recovery 사용하여 원격 사이트로 애플리케이션 장애 조치

재해 발생 시 온프레미스 VMware 사이트를 다른 온프레미스 VMware 사이트나 AWS의 VMware Cloud로 장애 조치합니다. 필요할 때 성공하는지 확인하기 위해 장애 조치 프로세스를 테스트할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 장애 조치 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

이 작업에 관하여

장애 조치 시 재해 복구는 기본적으로 가장 최근의 SnapMirror 스냅샷 복사본을 사용하지만, SnapMirror 의 보존 정책에 따라 특정 시점의 스냅샷을 선택할 수도 있습니다. 랜섬웨어 공격과 같이 가장 최근의 복제본이 손상된 경우 특정 시점 옵션을 사용하십시오.

이 프로세스는 프로덕션 사이트가 정상인지 여부와 중요 인프라 장애 외의 다른 이유로 재해 복구 사이트로 장애 조치를 수행하는지에 따라 다릅니다.

- 소스 vCenter 또는 ONTAP 클러스터에 액세스할 수 없는 중요한 프로덕션 사이트 장애: NetApp Disaster Recovery 하면 복원할 사용 가능한 스냅샷을 선택할 수 있습니다.
- 프로덕션 환경이 정상입니다. "지금 스냅샷을 찍으세요" 또는 이전에 만든 스냅샷을 선택할 수 있습니다.

이 절차는 복제 관계를 끊고, vCenter 소스 VM을 오프라인으로 전환하고, 재해 복구 vCenter에 볼륨을 데이터 저장소로 등록하고, 계획의 장애 조치 규칙을 사용하여 보호된 VM을 다시 시작하고, 대상 사이트에서 읽기/쓰기를 활성화합니다.

장애 조치 프로세스 테스트

장애 조치를 시작하기 전에 프로세스를 테스트할 수 있습니다. 이 테스트는 가상 머신을 오프라인으로 만들지 않습니다.

장애 조치 테스트 중에 재해 복구는 임시로 가상 머신을 생성합니다. Risaster Recovery는 FlexClone 볼륨을 지원하는 임시 데이터 저장소를 ESXi 호스트에 매핑합니다.

이 프로세스는 온프레미스 ONTAP 스토리지 또는 AWS의 NetApp ONTAP 스토리지용 FSx에 추가적인 물리적 용량을 소모하지 않습니다. 원본 소스 볼륨은 수정되지 않으며, 복제 작업은 재해 복구 중에도 계속될 수 있습니다.

테스트가 끝나면 정리 테스트 옵션을 사용하여 가상 머신을 재설정해야 합니다. 권장사항이지만 필수사항은 아닙니다.

테스트 장애 조치 작업은 프로덕션 워크로드, 테스트 사이트에서 사용되는 SnapMirror 관계, 그리고 정상적으로 작동을 계속해야 하는 보호 워크로드에는 영향을 미치지 않습니다.

테스트 장애 조치의 경우 재해 복구는 다음 작업을 수행합니다.

- 대상 클러스터와 SnapMirror 관계에 대한 사전 검사를 수행합니다.
- 대상 사이트 ONTAP 클러스터의 각 보호된 ONTAP 볼륨에 대해 선택한 스냅샷에서 새 FlexClone 볼륨을 만듭니다.

- 데이터 저장소가 VMFS인 경우 각 LUN에 iGroup을 생성하여 매핑합니다.
- vCenter 내에서 대상 가상 머신을 새로운 데이터 저장소로 등록합니다.
- 리소스 그룹 페이지에서 캡처한 부팅 순서에 따라 대상 가상 머신의 전원을 켭니다.
- "애플리케이션 일관성"으로 표시된 VM에서 지원되는 모든 데이터베이스 애플리케이션을 취소합니다.
- 소스 vCenter 및 ONTAP 클러스터가 여전히 활성 상태인 경우, 장애 조치 상태에서 모든 변경 사항을 원래 소스 사이트로 복제하기 위해 역방향 SnapMirror 관계를 만듭니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.
4. 복제 계획을 선택하세요.
5. 오른쪽에서 작업 옵션을 선택하세요 ••• *테스트 장애 조치*를 선택합니다.
6. 테스트 장애 조치 페이지에서 "테스트 장애 조치"를 입력하고 *테스트 장애 조치*를 선택합니다.
7. 테스트가 완료되면 테스트 환경을 정리합니다.

장애 조치 테스트 후 테스트 환경 정리

장애 조치 테스트가 완료되면 테스트 환경을 정리해야 합니다. 이 프로세스에서는 테스트 위치에서 임시 VM, FlexClone 및 임시 데이터 저장소를 제거합니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.
2. 복제 계획을 선택하세요.
3. 오른쪽에서 작업 옵션을 선택하세요. ••• 그런 다음 *장애 조치 테스트 정리*를 수행합니다.
4. 테스트 페일오버 페이지에서 "페일오버 정리"를 입력한 다음 "페일오버 테스트 정리"를 선택합니다.

소스 사이트를 재해 복구 사이트로 장애 조치합니다.

재해 발생 시 FSx for NetApp ONTAP 사용하여 온프레미스 VMware 사이트를 다른 온프레미스 VMware 사이트나 AWS의 VMware Cloud로 필요에 따라 장애 조치합니다.

장애 조치 프로세스에는 다음 작업이 포함됩니다.

- 재해 복구는 대상 클러스터와 SnapMirror 관계에 대한 사전 검사를 수행합니다.
- 최신 스냅샷을 선택한 경우 SnapMirror 업데이트가 수행되어 최신 변경 사항이 복제됩니다.
- 소스 가상 머신의 전원이 꺼졌습니다.
- SnapMirror 관계가 끊어지고 대상 볼륨이 읽기/쓰기가 가능해졌습니다.
- 스냅샷 선택에 따라 활성 파일 시스템은 지정된 스냅샷(최신 또는 선택)으로 복원됩니다.
- 데이터스토어는 복제 계획에서 수집된 정보를 기반으로 VMware 또는 VMC 클러스터나 호스트에 생성되어 마운트됩니다. 데이터 저장소가 VMFS인 경우 각 LUN에 iGroup을 생성하여 매핑합니다.

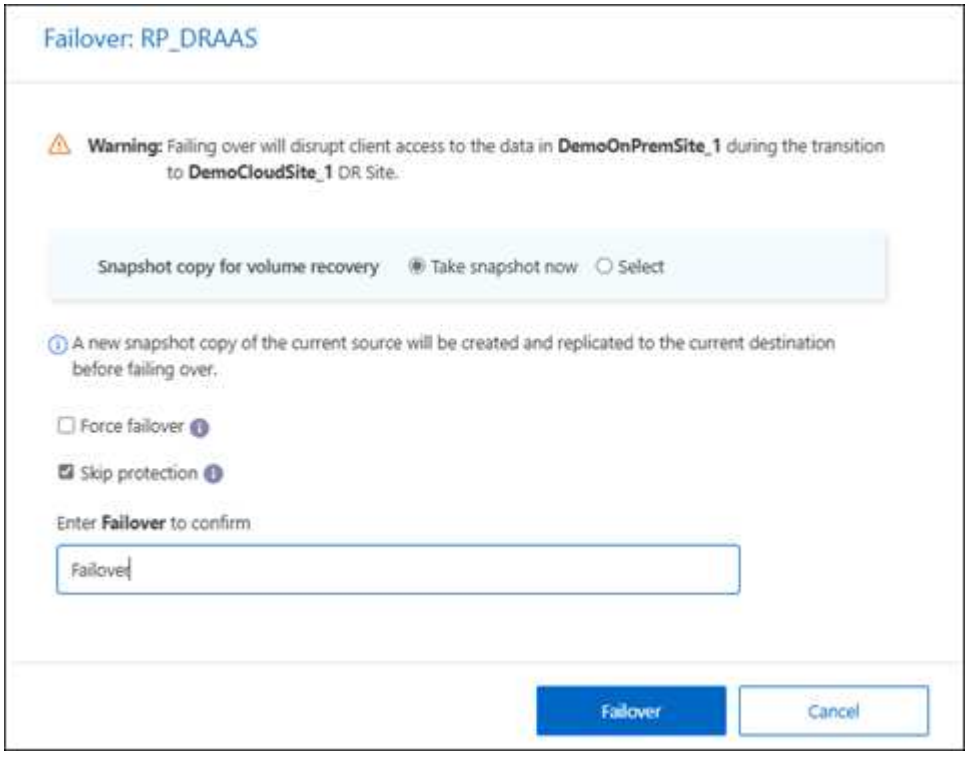
- 대상 가상 머신은 vCenter에 새로운 데이터 저장소로 등록됩니다.
- 대상 가상 머신은 리소스 그룹 페이지에서 캡처한 부팅 순서에 따라 전원이 켜집니다.
- 소스 vCenter가 여전히 활성 상태인 경우 장애 조치 중인 모든 소스 측 VM의 전원을 끕니다.
- "애플리케이션 일관성"으로 표시된 VM에서 지원되는 모든 데이터베이스 애플리케이션을 취소합니다.
- 소스 vCenter 및 ONTAP 클러스터가 여전히 활성 상태인 경우, 장애 조치 상태에서 모든 변경 사항을 원래 소스 사이트로 복제하기 위해 역방향 SnapMirror 관계를 생성합니다. SnapMirror 관계는 대상 가상 머신에서 소스 가상 머신으로 반전됩니다.

데이터스토어 기반 복제 계획의 경우, VM을 추가하고 검색했지만 매핑 세부 정보를 제공하지 않은 경우 해당 VM이 장애 조치에 포함됩니다. 장애 조치가 실패하면 작업에 알림이 표시됩니다. 장애 조치를 성공적으로 완료하려면 매핑 세부 정보를 제공해야 합니다.

장애 조치가 시작된 후 재해 복구 사이트의 vCenter에서 복구된 VM(가상 머신, 네트워크, 데이터 저장소)을 볼 수 있습니다. 기본적으로 가상 머신은 워크로드 폴더로 복구됩니다.

단계

1. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.
2. 복제 계획을 선택하세요.
3. 오른쪽에서 작업 옵션을 선택하세요 ••• 그리고 *장애 조치*를 선택합니다.



4. 장애 조치 페이지에서 지금 새 스냅샷을 생성하거나 데이터 저장소의 기존 스냅샷을 선택하여 복구 기반으로 사용할 수 있습니다. 기본 설정은 최신 버전입니다.

   장애 조치가 발생하기 전에 현재 소스의 스냅샷이 촬영되어 현재 대상에 복제됩니다.

5. 선택적으로, 일반적으로 장애 조치가 발생하지 않도록 하는 오류가 감지된 경우에도 장애 조치가 발생하도록 하려면

*강제 장애 조치*를 선택합니다.

6. 선택적으로, 복제 계획 장애 조치 후 서비스가 자동으로 역방향 SnapMirror 보호 관계를 생성하지 않도록 하려면 *보호 건너뛰기*를 선택합니다. NetApp Disaster Recovery 에서 다시 온라인으로 전환하기 전에 복원된 사이트에서 추가 작업을 수행하려는 경우 이 기능이 유용합니다.

> 복제 계획 작업 메뉴에서 *리소스 보호*를 선택하여 역방향 보호를 설정할 수 있습니다. 이는 계획의 각 볼륨에 대해 역방향 복제 관계를 생성하려고 시도합니다. 보호가 복구될 때까지 이 작업을 반복해서 실행할 수 있습니다. 보호가 복구되면 평소와 같은 방식으로 장애 복구를 시작할 수 있습니다.

7. 상자에 "장애 조치"를 입력합니다.
8. *장애 조치*를 선택합니다.
9. 진행 상황을 확인하려면 메뉴에서 *작업 모니터링*을 선택하세요.

NetApp Disaster Recovery 사용하여 애플리케이션을 원래 소스로 다시 장애 복구합니다.

재해가 해결된 후 재해 복구 사이트에서 소스 사이트로 장애 복구하여 정상적인 운영으로 돌아갑니다. 복구할 스냅샷을 선택할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 장애 조치 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

페일백에 관하여

페일백 시 NetApp Disaster Recovery 복제 방향을 반전하기 전에 모든 변경 사항을 원래 소스 가상 머신으로 복제(재동기화)합니다. 이 과정은 대상과의 관계 전환이 완료된 상태에서 시작되며 다음과 같은 단계를 포함합니다.

- 복구된 사이트에 대한 규정 준수 검사를 수행합니다.
- 복구된 사이트에 있는 것으로 식별된 각 vCenter 클러스터에 대한 vCenter 정보를 새로 고칩니다.
- 대상 사이트에서 가상 머신의 전원을 끄고 등록을 해제하고 볼륨을 마운트 해제합니다.
- 원본 소스에서 SnapMirror 관계를 끊어서 읽기/쓰기가 가능하도록 합니다.
- 복제를 되돌리려면 SnapMirror 관계를 다시 동기화합니다.
- 소스 가상 머신의 전원을 켜고 등록한 후 소스에 볼륨을 마운트합니다.

시작하기 전에

데이터스토어 기반 보호를 사용하는 경우, 데이터스토어에 추가된 VM은 장애 조치 프로세스 중에 데이터스토어에 추가될 수 있습니다. 이러한 상황이 발생한 경우, 장애 복구를 시작하기 전에 해당 VM에 대한 추가 매핑 정보를 제공해야 합니다. 리소스 매핑을 편집하려면 다음을 참조하세요. "복제 계획 관리".

단계

1. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
2. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.
3. 복제 계획을 선택하세요.
4. 오른쪽에서 작업 옵션을 선택하세요 ••• 그리고 *장애 복구*를 선택하세요.
5. 장애 복구를 시작하려면 복제 계획의 이름을 입력하십시오.
6. 복구할 데이터 저장소의 스냅샷을 선택합니다. 기본값은 최신입니다.
7. 작업 진행 상황을 모니터링하려면 재해 복구 메뉴에서 *작업 모니터링*을 선택하십시오.

NetApp Disaster Recovery 사용하여 사이트, 리소스 그룹, 복제 계획, 데이터 저장소 및 가상 머신 정보를 관리합니다.

NetApp Disaster Recovery 모든 리소스에 대한 개요와 보다 자세한 관점을 제공합니다.

- 사이트
- 리소스 그룹
- 복제 계획
- 데이터 저장소
- 가상 머신

작업에는 다양한 NetApp Console 역할이 필요합니다. 자세한 내용은 각 작업의 필수 **NetApp Console** 역할 섹션을 참조하세요.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

vCenter 사이트 관리

vCenter 사이트 이름과 사이트 유형(온프레미스 또는 AWS)을 편집할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 역할.

단계

1. 메뉴에서 *사이트*를 선택합니다.
2. 작업 옵션을 선택하세요  vCenter 이름 오른쪽에서 *편집*을 선택합니다.
3. vCenter 사이트 이름과 위치를 편집합니다.

리소스 그룹 관리

VM 또는 데이터 저장소별로 리소스 그룹을 만들 수 있습니다. 복제 계획을 생성할 때나 생성한 후에 추가할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자 또는 재해 복구 애플리케이션

관리자 역할.

다음과 같은 방법으로 데이터 저장소별로 리소스 그룹을 만들 수 있습니다.

- 데이터 저장소를 사용하여 리소스 그룹을 추가하는 경우 데이터 저장소 목록을 볼 수 있습니다. 하나 이상의 데이터 저장소를 선택하여 리소스 그룹을 만들 수 있습니다.
- 복제 계획을 만들고 계획 내에서 리소스 그룹을 만들면 데이터 저장소에서 VM을 볼 수 있습니다.

리소스 그룹을 사용하여 다음 작업을 수행할 수 있습니다.

- 리소스 그룹 이름을 변경합니다.
- 리소스 그룹에 VM을 추가합니다.
- 리소스 그룹에서 VM을 제거합니다.
- 리소스 그룹을 삭제합니다.

리소스 그룹 생성에 대한 자세한 내용은 다음을 참조하세요."VM을 함께 구성하기 위한 리소스 그룹 생성" .

단계

1. 메뉴에서 *리소스 그룹*을 선택합니다.
2. 리소스 그룹을 추가하려면 *그룹 추가*를 선택하세요.
3. 작업 옵션을 선택하여 리소스 그룹을 수정하거나 삭제할 수 있습니다. ••• .

복제 계획 관리

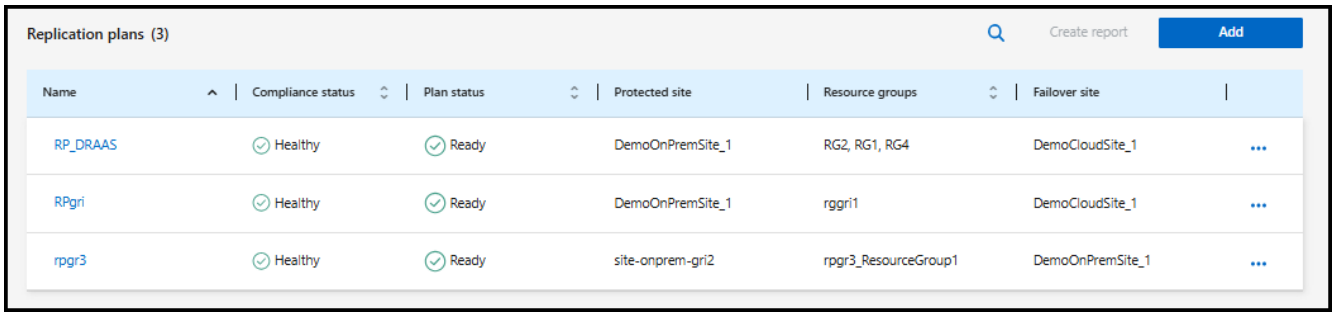
복제 계획을 비활성화, 활성화 및 삭제할 수 있습니다. 일정을 변경할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

- 복제 계획을 일시적으로 일시 중지하려면 해당 계획을 비활성화한 다음 나중에 다시 활성화할 수 있습니다.
- 더 이상 해당 계획이 필요하지 않으면 삭제할 수 있습니다.

단계

1. 메뉴에서 *복제 계획*을 선택합니다.



2. 계획 세부 정보를 보려면 작업 옵션을 선택하세요. ••• *플랜 세부정보 보기*를 선택하세요.
3. 다음 중 하나를 수행하세요.

- 플랜 세부 정보를 편집하려면(반복 일정을 변경하려면) 플랜 세부 정보 탭을 선택하고 오른쪽에 있는 편집 아이콘을 선택하세요.
- 리소스 매핑을 편집하려면 장애 조치 매핑 탭을 선택하고 편집 아이콘을 선택합니다.
- 가상 머신을 추가하거나 편집하려면 가상 머신 탭을 선택하고 **VM** 추가 옵션이나 편집 아이콘을 선택하세요.

4. 왼쪽의 탐색 경로에서 "복제 계획"을 선택하여 계획 목록으로 돌아갑니다.
5. 계획에 대한 작업을 수행하려면 복제 계획 목록에서 작업 옵션을 선택하세요. ••• 계획의 오른쪽에서 일정 편집, 테스트 장애 조치, 장애 조치, 장애 복구, 마이그레이션, 지금 스냅샷 찍기, 이전 스냅샷 정리, 비활성화, 활성화 또는 *삭제*와 같은 옵션을 선택합니다.
6. 테스트 장애 조치 일정을 설정하거나 변경하거나 규정 준수 빈도 검사를 설정하려면 작업 옵션을 선택하세요. ••• 계획 오른쪽에서 *일정 편집*을 선택하세요.
   a. 일정 편집 페이지에서 장애 조치 규정 준수 검사를 수행할 빈도를 분 단위로 입력합니다.
   b. *일정에 따라 테스트 장애 조치 실행*을 선택합니다.
   c. 반복 옵션에서 일일, 주간 또는 월간 일정을 선택합니다.
   d. *저장*을 선택하세요.

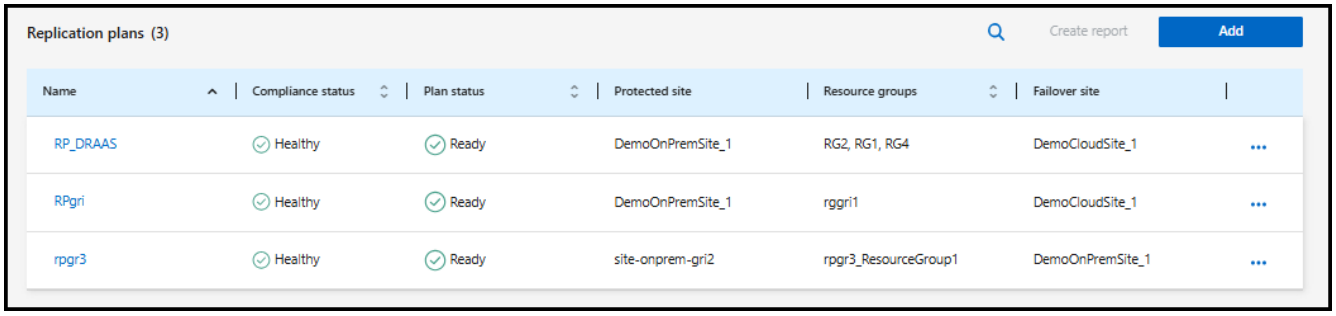
필요에 따라 스냅샷 조정

재해 복구는 24시간마다 소스의 스냅샷을 자동으로 삭제합니다. 소스와 대상 간의 스냅샷이 동기화되지 않은 것을 발견하면 사이트 간 일관성을 유지하기 위해 스냅샷 간의 불일치를 해결해야 합니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

단계

1. 메뉴에서 *복제 계획*을 선택합니다.



2. 복제 계획 목록에서 작업 옵션을 선택하세요. ••• 그런 다음 스냅샷을 조정합니다.
3. 조정 정보를 검토하세요.
4. *조정*을 선택하세요.

복제 계획 삭제

복제 계획을 삭제하면 해당 계획에서 생성된 기본 및 보조 스냅샷도 삭제할 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

단계

1. 메뉴에서 *복제 계획*을 선택합니다.
2. 작업 옵션을 선택하세요 ••• 계획 오른쪽에서 *삭제*를 선택하세요.
3. 기본 스냅샷, 보조 스냅샷 또는 계획에서 생성된 메타데이터만 삭제할지 여부를 선택합니다.
4. 삭제를 확인하려면 "delete"를 입력하세요.
5. *삭제*를 선택하세요.

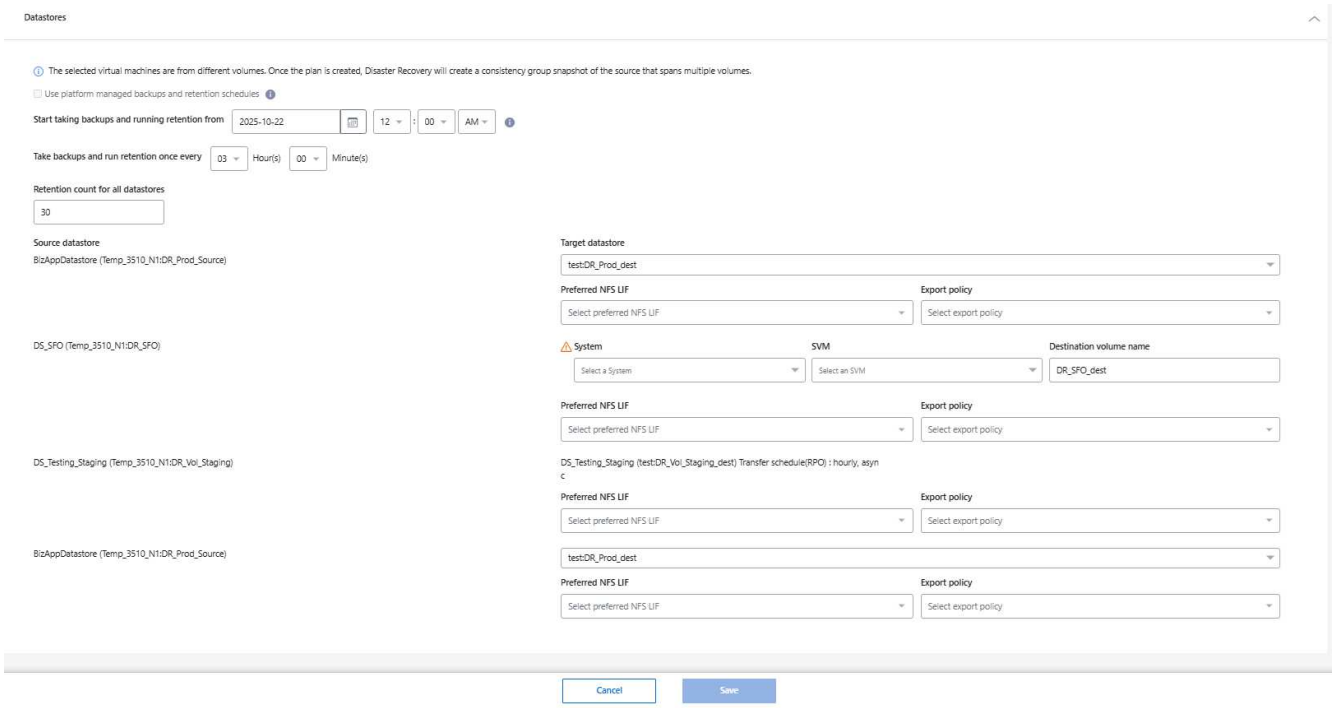
장애 조치 일정에 대한 보존 횟수 변경

보존 횟수를 변경하면 저장된 데이터 저장소의 수를 늘리거나 줄일 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

단계

1. 메뉴에서 *복제 계획*을 선택합니다.
2. 복제 계획을 선택한 다음 장애 조치 매핑 탭을 선택합니다. 편집 연필 아이콘을 선택합니다.
3. 데이터 저장소 행에서 아래쪽 화살표를 선택하여 확장합니다.



4. 모든 데이터 저장소의 보존 횟수 값을 변경합니다.
5. 복제 계획을 선택한 후 작업 메뉴를 선택한 다음 *오래된 스냅샷 정리*를 선택하여 대상에서 오래된 스냅샷을 제거하여 새 보존 횟수와 일치시킵니다.

데이터 저장소 정보 보기

소스와 대상에 얼마나 많은 데이터 저장소가 있는지에 대한 정보를 볼 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자, 재해 복구 애플리케이션 관리자 또는 재해 복구 뷰어 역할.

단계

1. 메뉴에서 *대시보드*를 선택합니다.
2. 사이트 행에서 vCenter를 선택합니다.
3. *데이터 저장소*를 선택하세요.
4. 데이터 저장소 정보를 확인하세요.

가상 머신 정보 보기

소스와 대상에 존재하는 가상 머신의 수와 CPU, 메모리, 사용 가능한 용량에 대한 정보를 볼 수 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자, 재해 복구 애플리케이션 관리자 또는 재해 복구 뷰어 역할.

단계

1. 메뉴에서 *대시보드*를 선택합니다.
2. 사이트 행에서 vCenter를 선택합니다.
3. *가상 머신*을 선택하세요.
4. 가상 머신 정보를 확인합니다.

NetApp Disaster Recovery 작업 모니터링

모든 NetApp Disaster Recovery 작업을 모니터링하고 진행 상황을 확인할 수 있습니다.

채용공고 보기

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 애플리케이션 관리자 또는 재해 복구 뷰어 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. 메뉴에서 *작업 모니터링*을 선택합니다.
4. 운영과 관련된 모든 직무를 탐색하고 타임스탬프와 상태를 검토합니다.
5. 특정 직업의 세부 정보를 보려면 해당 행을 선택하세요.
6. 정보를 새로 고치려면 *새로 고침*을 선택하세요.

작업 취소

작업이 진행 중이거나 대기 중인 경우 계속 진행하고 싶지 않으면 해당 작업을 취소할 수 있습니다. 동일한 상태에 갇힌 작업을 취소하고 대기열에서 다음 작업을 비우고 싶을 수 있습니다. 시간이 초과되기 전에 작업을 취소하고 싶을 수도 있습니다.

필수 **NetApp Console** 역할 조직 관리자, 폴더 또는 프로젝트 관리자, 재해 복구 관리자, 재해 복구 장애 조치 관리자 또는 재해 복구 애플리케이션 관리자 역할.

"NetApp Disaster Recovery 의 사용자 역할 및 권한에 대해 알아보세요.". "모든 서비스에 대한 NetApp Console 액세스 역할에 대해 알아보세요.".

단계

1. NetApp Console 왼쪽 탐색 모음에서 보호 > *재해 복구*를 선택합니다.
2. 메뉴에서 *작업 모니터링*을 선택합니다.
3. 작업 모니터 페이지에서 취소하려는 작업의 ID를 기록해 둡니다.

   작업은 "진행 중" 또는 "대기 중" 상태여야 합니다.

4. 작업 열에서 *작업 취소*를 선택합니다.

NetApp Disaster Recovery 보고서 만들기

NetApp Disaster Recovery 보고서를 검토하면 재해 복구 준비 상태를 분석하는 데 도움이 될 수 있습니다. 사전 설계된 보고서에는 지난 7일 동안 계정 내 모든 사이트에 대한 테스트 장애 조치 요약, 복제 계획 세부 정보, 작업 세부 정보가 포함됩니다.

PDF, HTML 또는 JSON 형식으로 보고서를 다운로드할 수 있습니다.

다운로드 링크는 6시간 동안 유효합니다.

단계

1. 에 로그인하세요 "NetApp Console" .
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.
3. NetApp Console 왼쪽 탐색 모음에서 *복제 계획*을 선택합니다.
4. *보고서 만들기*를 선택하세요.
5. 파일 형식 유형과 지난 7일 이내의 기간을 선택하세요.
6. *만들기*를 선택하세요.

   보고서가 표시되려면 몇 분 정도 걸릴 수 있습니다.

7. 보고서를 다운로드하려면 *보고서 다운로드*를 선택하고 관리자의 다운로드 폴더에서 보고서를 선택하세요.

참조

NetApp Disaster Recovery를 위한 필수 vCenter 권한

NetApp Disaster Recovery가 서비스를 수행하려면 vCenter 계정에 최소한의 vCenter 권한 세트가 있어야 합니다. 이러한 권한에는 데이터 저장소 등록 및 등록 해제, 가상 머신(VM) 시작 및 중지, VM 재구성 등이 포함됩니다.

다음 표는 Disaster Recovery가 vCenter 클러스터와 인터페이스하는 데 필요한 모든 권한을 나열합니다.

유형	권한 이름**(vSphere** 클라이언트**)**	권한 이름**(API)**	설명
데이터 저장소	Datastore.Config	데이터 저장소 구성	데이터 저장소 구성을 허용합니다.
	Datastore.Delete	데이터 저장소 제거	데이터 저장소를 제거할 수 있습니다.
	데이터스토어.Rename	데이터 저장소 이름 바꾸기	데이터 저장소의 이름을 변경할 수 있습니다.
폴더	폴더.생성	폴더 생성	새 폴더 생성을 허용합니다.
	폴더.삭제	폴더 삭제	폴더를 삭제할 수 있습니다. 해당 개체와 상위 개체 모두에 대한 권한이 필요합니다.
	폴더.이름 바꾸기	폴더 이름 변경	폴더 이름을 수정할 수 있습니다.
네트워크	네트워크 할당	네트워크 할당	VM에 네트워크를 할당할 수 있도록 합니다.
	Network.Config	구성	네트워크 구성을 허용합니다.
가상 머신 구성	VirtualMachine.구성.AdvancedConfig	고급 구성	VM의 구성 파일에서 고급 매개 변수를 추가하거나 수정할 수 있습니다.
	VirtualMachine.구성.설정	설정 변경	일반 VM 설정을 변경할 수 있습니다.
	VirtualMachine.Config.CPUCount	CPU 수 변경	가상 CPU 수를 변경할 수 있습니다.
	VirtualMachine.Config.Memory	메모리 변경	VM에 할당된 메모리 양을 변경할 수 있습니다.
	VirtualMachine.구성.리소스	리소스 변경	리소스 풀에서 VM 노드의 리소스 구성을 변경할 수 있습니다.
	VirtualMachine.Config.이름 바꾸기	이름 바꾸기	VM의 이름을 바꾸거나 메모를 수정할 수 있습니다.
	VirtualMachine.구성.EditDevice	장치 설정 수정	기존 디바이스의 속성을 변경할 수 있습니다.
	VirtualMachine.구성.ReloadFromPath	경로에서 다시 로드	ID를 유지하면서 VM 구성 경로를 변경할 수 있습니다.
	VirtualMachine.구성.ResetGuestInfo	게스트 정보 재설정	VM의 게스트 운영 체제 정보를 편집할 수 있습니다.

유형	권한 이름(vSphere 클라이언트)	권한 이름(API)	설명
가상 머신 게스트	VirtualMachine.GuestOperations.ModifyAliases	게스트 작업 별칭 수정	VM의 별칭을 수정할 수 있습니다.
	VirtualMachine.GuestOperations.QueryAliases	게스트 작업 별칭 쿼리	VM의 별칭을 쿼리할 수 있습니다.
	VirtualMachine.GuestOperations.Modify	게스트 작업 수정	파일을 VM으로 전송하는 것을 포함한 수정 작업을 허용합니다.
	VirtualMachine.GuestOperations.Execute	게스트 작업 프로그램 실행	VM 내부에서 애플리케이션을 실행할 수 있도록 허용합니다.
	VirtualMachine.GuestOperations.Query	게스트 작업 쿼리	게스트 운영 체제에 대한 쿼리를 허용합니다. 작업에는 파일 목록 보기가 포함됩니다.
가상 머신 상호 작용	VirtualMachine.Interact.AnswerQuestion	질문에 답하세요	VM 상태 전환 또는 런타임 오류 중에 발생하는 문제를 해결할 수 있습니다.
	VirtualMachine.Interact.PowerOff	전원 끄기	전원이 켜진 VM의 전원을 끌 수 있습니다.
	VirtualMachine.Interact.PowerOn	전원 켜기	VM의 전원을 켜거나 재개할 수 있습니다.
	VirtualMachine.상호작용.ToolsInstall	VMware Tools 설치	VMware Tools 설치 프로그램의 마운트/마운트 해제를 허용합니다.
	VirtualMachine.인벤토리.CreateFromExisting	기존 항목에서 생성	템플릿에서 VM을 복제하거나 배포할 수 있습니다.
	VirtualMachine.Inventory.Create	새로 만들기	VM을 생성하고 리소스를 할당할 수 있습니다.
	VirtualMachine.인벤토리.등록	등록	기존 VM을 인벤토리에 추가할 수 있습니다.
	VirtualMachine.Inventory.Delete	제거	VM과 해당 파일을 삭제할 수 있습니다. 개체와 상위 개체 모두에 대한 권한이 필요합니다.
	VirtualMachine.Inventory.Unregister	등록 취소	VM 등록 취소를 허용합니다. 이 권한에는 개체와 상위 개체 모두에 대한 권한이 필요합니다.
가상 머신 프로비저닝	VirtualMachine.Provisioning.Clone	가상 머신 복제	VM을 복제하고 리소스를 할당할 수 있습니다.
	VirtualMachine.Provisioning.Customize	게스트 맞춤 설정	VM의 게스트 운영 체제를 사용자 지정할 수 있습니다.
	VirtualMachine.Provisioning.ModifyCustSpecs	사용자 지정 사양 수정	사용자 지정 사양을 생성, 수정 또는 삭제할 수 있습니다.
	VirtualMachine.프로비저닝.ReadCustSpecs	사용자 지정 사양 읽기	VM의 사용자 지정 사양을 읽을 수 있도록 합니다.

유형	권한 이름(vSphere 클라이언트)	권한 이름(API)	설명
가상 머신 서비스 구성	VirtualMachine.Namespace.Query	쿼리 서비스 구성	VM 서비스 목록을 검색할 수 있습니다.
	VirtualMachine.Namespace.ReadContent	서비스 구성 읽기	기존 VM 서비스 구성을 검색할 수 있습니다.
가상 머신 스냅샷	VirtualMachine.상태.CreateSnapshot	스냅샷 생성	VM의 현재 상태에서 스냅샷을 생성할 수 있습니다.
	VirtualMachine.상태.RemoveSnapshot	스냅샷 제거	스냅샷을 제거할 수 있습니다.
	VirtualMachine.상태.RenameSnapshot	스냅샷 이름 바꾸기	스냅샷의 이름을 바꾸거나 설명을 업데이트할 수 있습니다.
	VirtualMachine.State.RevertToSnapshot	스냅샷으로 되돌리기	VM을 특정 스냅샷의 상태로 되돌릴 수 있습니다.

NetApp Disaster Recovery 사용할 때 콘솔 에이전트 전환

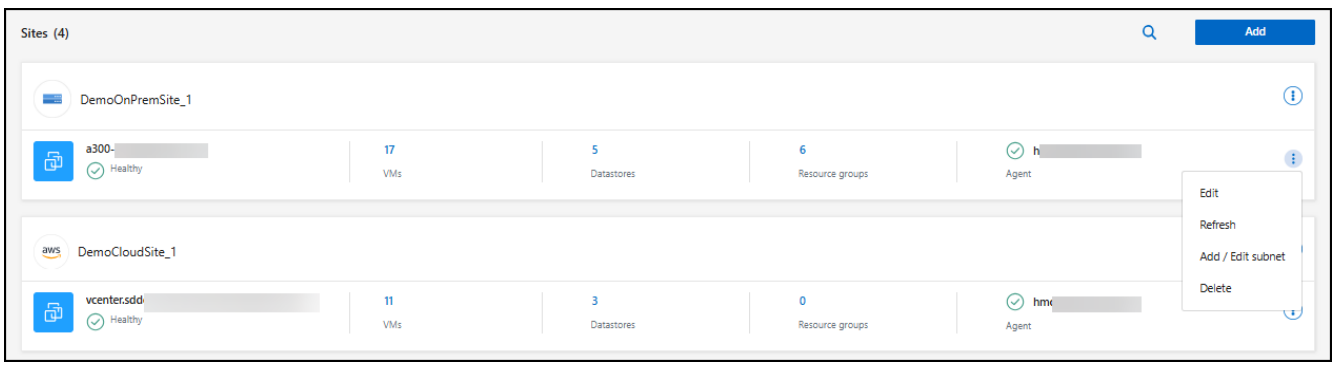
NetApp Console 단일 작업 환경에서 여러 콘솔 에이전트를 사용하는 것을 지원합니다. 여러 콘솔 에이전트를 사용하면 다른 콘솔 에이전트에서 유지 관리를 수행하는 동안 또는 콘솔 에이전트에 오류가 발생하는 경우 리소스에 대한 액세스를 유지하는 데 도움이 될 수 있습니다. 각 콘솔 에이전트에는 고유한 식별자가 있으므로 콘솔 에이전트를 부적절하게 전환하면 작업 환경에서 리소스 가용성이 손상될 수 있습니다.

시작하기 전에

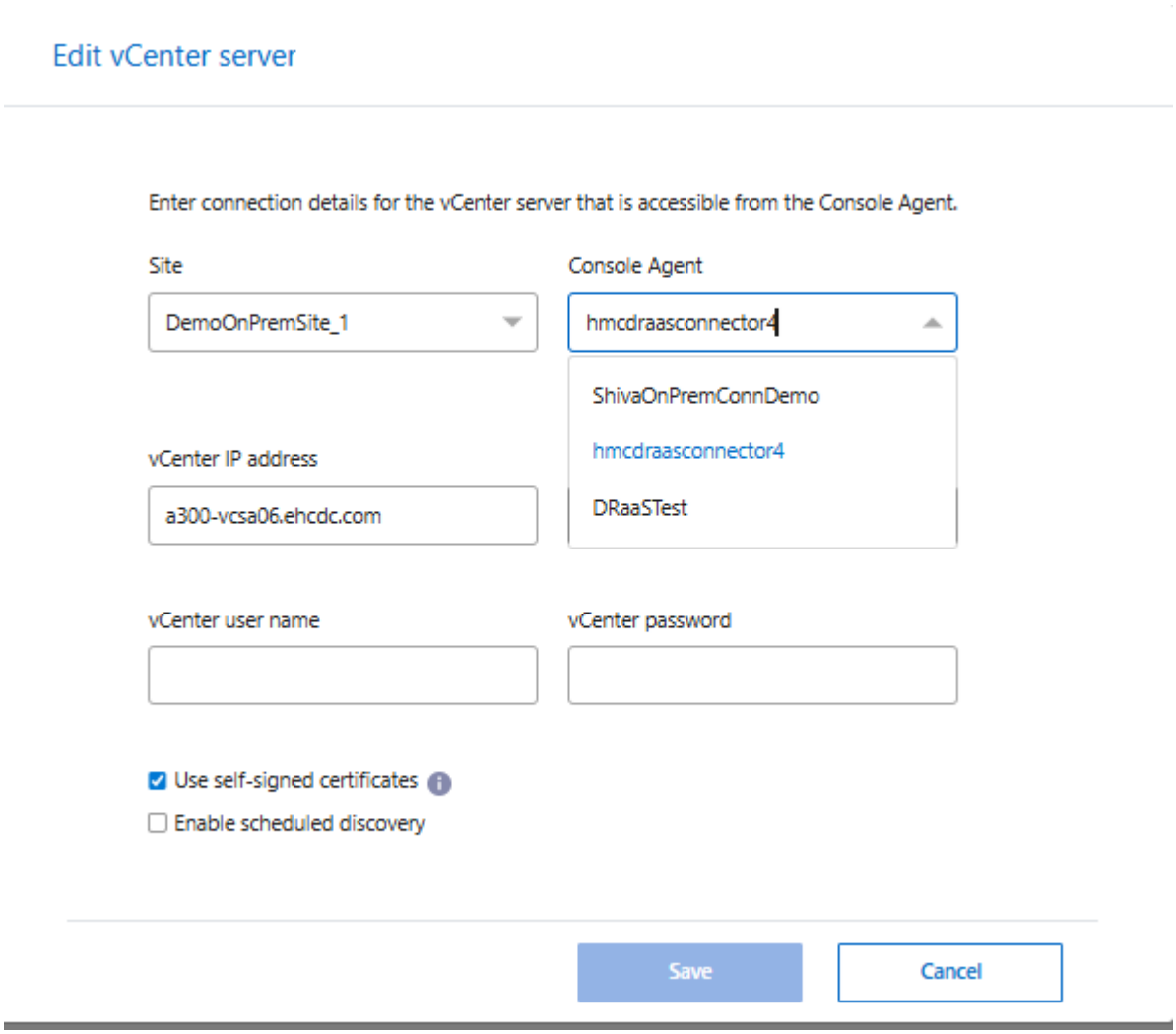
- 당신은 가지고 있어야 합니다작업 환경에 대해 최소 두 개의 콘솔 에이전트를 추가했습니다. .
- 두 콘솔 에이전트 모두 동일한 ONTAP 클러스터를 포함해야 합니다.

단계

1. 재해 복구에서 사이트를 선택합니다.
2. 소스 및 대상 vCenter 모두에 대한 콘솔 에이전트를 변경해야 합니다. 수정하려는 vCenter를 식별합니다. vCenter에 대한 작업 메뉴를 선택한 다음 편집을 선택합니다.



3. 드롭다운 메뉴에서 사용할 콘솔 에이전트를 선택하고 vCenter 사용자 이름과 비밀번호를 다시 입력합니다. 저장을 선택하세요.



4. 수정하려는 각 추가 vCenter에 대해 2단계와 3단계를 반복합니다.
5. 수정한 vCenter에서 vCenter를 새로 고쳐서 새로운 콘솔 에이전트를 검색합니다. 수정한 모든 vCenter에 대해 이 단계를 반복합니다.
6. 재해 복구에서 복제 계획으로 이동합니다.
7. 워크플로를 재개하는 데 사용할 복제 계획을 식별합니다. 동작 메뉴를 선택하세요 ... 그런 다음 리소스 새로 고침을 클릭합니다. 작업 모니터링에서 작업 상태를 모니터링할 수 있습니다.

더 많은 정보

- "콘솔 에이전트에 대해 알아보세요"

Amazon EVS와 함께 NetApp Disaster Recovery 사용

Amazon Elastic VMware Service 및 Amazon FSx for NetApp ONTAP 사용한 NetApp Disaster Recovery 소개

점점 더 많은 고객이 VMware vSphere 기반과 같은 프로덕션 컴퓨팅 워크로드를 위해 가상화된 인프라에 더 의존하게 되었습니다. 가상 머신(VM)이 비즈니스에 더욱 중요해짐에 따라 고객은 물리적 컴퓨팅 리소스와 동일한 유형의 재해로부터 이러한 VM을 보호해야 합니다. 현재 제공되는 재해 복구(DR) 솔루션은 복잡하고 비용이 많이 들며 리소스가 많이 필요합니다. 가상화된 인프라에 사용되는 최대 규모의 스토리지 공급업체 NetApp 모든 유형의 ONTAP 스토리지 호스팅 데이터를 보호하는 것과 동일한 방식으로 고객의 VM을 보호하는 데 큰 관심을 가지고 있습니다. 이러한 목표를 달성하기 위해 NetApp NetApp Disaster Recovery 서비스를 만들었습니다.

모든 DR 솔루션의 주요 과제 중 하나는 DR 복제 및 복구 인프라를 제공하기 위해 추가적인 컴퓨팅, 네트워크 및 스토리지 리소스를 구매, 구성 및 유지 관리하는 데 드는 증가 비용을 관리하는 것입니다. 중요한 온프레미스 가상 리소스를 보호하는 데 널리 사용되는 옵션 중 하나는 클라우드 호스팅 가상 리소스를 DR 복제 및 복구 인프라로 사용하는 것입니다. Amazon은 NetApp ONTAP 호스팅 VM 인프라와 호환되는 비용 효율적인 리소스를 제공할 수 있는 솔루션의 한 예입니다.

Amazon은 가상 사설 클라우드(VPC) 내에서 VMware Cloud Foundation을 지원하는 Amazon Elastic VMware Service(Amazon EVS)를 출시했습니다. Amazon EVS는 AWS의 복원력과 성능과 함께 익숙한 VMware 소프트웨어 및 도구를 제공하여 Amazon EVS vCenter를 온프레미스 가상화 인프라의 확장 기능으로 통합할 수 있도록 합니다.

Amazon EVS에는 스토리지 리소스가 포함되어 있지만, 스토리지 사용량이 많은 작업 부하가 있는 조직의 경우 기본 스토리지를 사용하면 효율성이 떨어질 수 있습니다. 이러한 경우 Amazon EVS를 Amazon FSx for NetApp ONTAP 스토리지(Amazon FSxN)와 함께 사용하면 더욱 유연한 스토리지 솔루션을 제공할 수 있습니다. 또한 온프레미스에서 NetApp ONTAP 스토리지 솔루션을 사용하여 VMware 인프라를 호스팅하는 경우 FSx for ONTAP 이 포함된 Amazon EVS를 사용하면 온프레미스와 클라우드 호스팅 인프라 간에 동급 최고의 데이터 상호 운용성과 보호 기능을 얻을 수 있습니다.

Amazon FSx for NetApp ONTAP 에 대한 정보는 다음을 참조하세요. "Amazon FSx for NetApp ONTAP 시작하기" .

Amazon EVS 및 Amazon FS를 사용한 NetApp ONTAP 용 NetApp Disaster Recovery 솔루션 개요

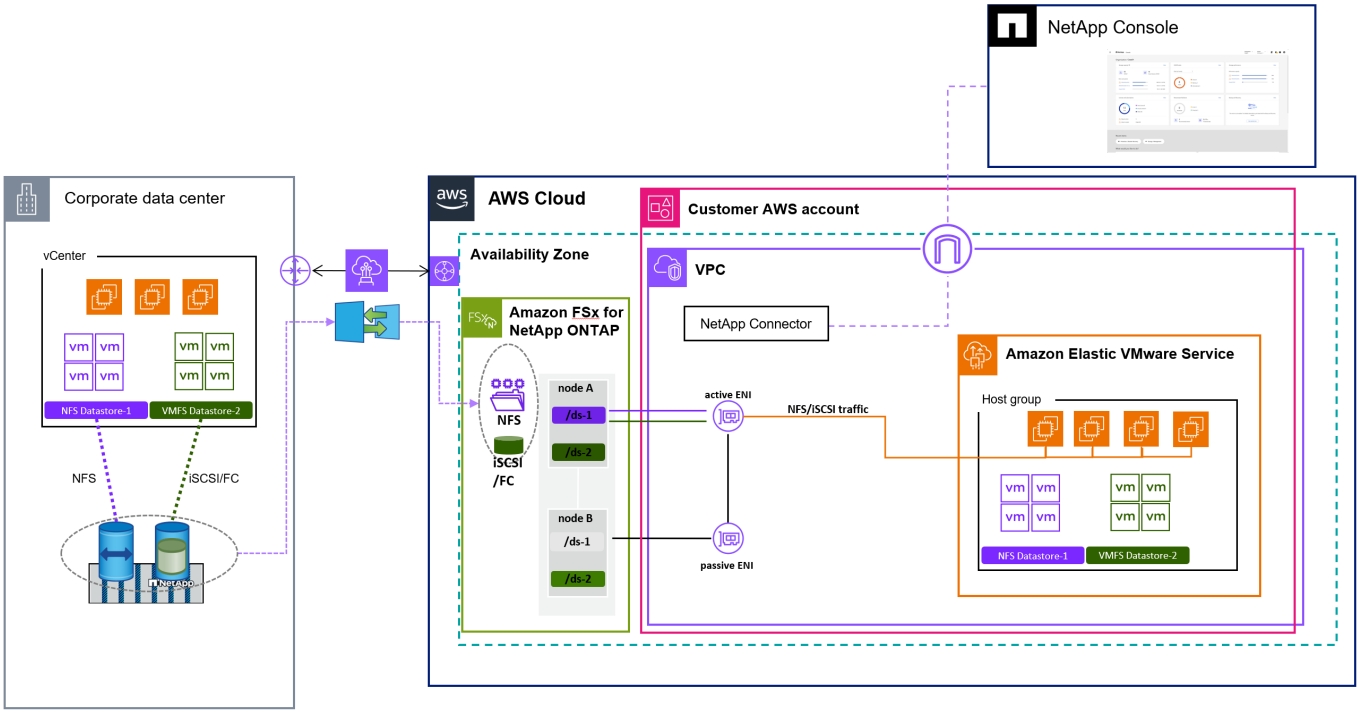
NetApp Disaster Recovery NetApp Console 소프트웨어 즉 서비스 환경 내에서 호스팅되는 부가가치 서비스로, 핵심 NetApp Console 아키텍처에 따라 달라집니다. 콘솔 내 VMware 보호를 위한 DR 서비스는 여러 가지 주요 구성 요소로 구성됩니다.

NetApp Disaster Recovery 솔루션에 대한 전체 개요는 다음을 참조하세요."VMware용 NetApp Disaster Recovery에 대해 알아보세요" .

온프레미스 VMware 호스팅 가상 머신을 Amazon AWS로 보호하려면 해당 서비스를 사용하여 Amazon FSx for NetApp ONTAP 스토리지 호스팅 데이터스토어를 통해 Amazon EVS로 백업하세요.

다음 그림은 Amazon EVS를 사용하여 VM을 보호하는 서비스의 작동 방식을 보여줍니다.

Amazon EVS 및 FSx for ONTAP 사용한 NetApp Disaster Recovery 개요



1. Amazon EVS는 귀하의 계정에서 단일 가용성 영역(AZ) 구성과 가상 사설 클라우드(VPC) 내에 배포됩니다.
2. FSx for ONTAP 파일 시스템은 Amazon EVS 배포와 동일한 AZ에 배포됩니다. 파일 시스템은 ENI(Elastic Network Interface), VPC 피어 연결 또는 AmazonTransit Gateway를 통해 Amazon EVS에 직접 연결됩니다.
3. NetApp Console 에이전트가 VPC에 설치되었습니다. NetApp Console 에이전트는 로컬 물리적 데이터 센터와 Amazon AWS에서 호스팅되는 리소스 모두에서 VMware 인프라의 재해 복구를 관리하는 NetApp Disaster Recovery 에이전트를 포함하여 여러 데이터 관리 서비스(에이전트라고 함)를 호스팅합니다.
4. NetApp Disaster Recovery 에이전트는 NetApp Console 클라우드 호스팅 서비스와 안전하게 통신하여 작업을 수신하고 해당 작업을 적절한 온프레미스 및 AWS 호스팅 vCenter와 ONTAP 스토리지 인스턴스에 배포합니다.
5. NetApp Console 클라우드 호스팅 UI 콘솔을 사용하여 복제 계획을 생성하면 보호해야 할 VM, 해당 VM을 보호해야 하는 빈도, 온프레미스 사이트에서 장애 조치가 발생할 경우 해당 VM을 다시 시작하기 위해 수행해야 하는 절차 등을 지정할 수 있습니다.
6. 복제 계획은 보호된 VM을 호스팅하는 vCenter 데이터 저장소와 해당 데이터 저장소를 호스팅하는 ONTAP 볼륨을 결정합니다. FSx for ONTAP 클러스터에 볼륨이 아직 없으면 NetApp Disaster Recovery 자동으로 볼륨을 생성합니다.
7. 식별된 각 소스 ONTAP 볼륨에 대해 각 대상 FSx for ONTAP 호스팅 ONTAP 볼륨에 대한 SnapMirror 관계가 생성되고 복제 계획에서 사용자가 제공한 RPO를 기반으로 복제 일정이 생성됩니다.
8. 기본 사이트에 장애가 발생하는 경우 관리자는 NetApp Console 에서 수동 장애 조치 프로세스를 시작하고 복원 지점으로 사용할 백업을 선택합니다.
9. NetApp Disaster Recovery 에이전트는 FSx for ONTAP 호스팅 데이터 보호 볼륨을 활성화합니다.
10. 에이전트는 활성화된 각 FSx for ONTAP 볼륨을 Amazon EVS vCenter에 등록하고, 보호된 각 VM을 Amazon EVS vCenter에 등록한 후 복제 계획에 포함된 사전 정의된 규칙에 따라 각각을 시작합니다.

NetApp Disaster Recovery 위한 NetApp Console 에이전트 설치

NetApp Console 에이전트를 사용하면 NetApp Console 배포를 인프라에 연결하여 AWS, Azure, Google Cloud 또는 온프레미스 환경 전반에서 솔루션을 안전하게 오케스트레이션할 수

있습니다. Console 에이전트는 NetApp Console이 데이터 인프라를 관리하는 데 필요한 작업을 실행합니다. Console 에이전트는 NetApp Disaster Recovery 서비스형 소프트웨어 계층에서 수행해야 하는 작업이 있는지 지속적으로 폴링합니다.

NetApp Disaster Recovery의 경우, 수행되는 작업은 각 서비스의 네이티브 API를 사용하여 VMware vCenter 클러스터와 ONTAP 스토리지 인스턴스를 오케스트레이션하여 온프레미스 환경에서 실행되는 프로덕션 VM을 보호합니다. Console 에이전트는 네트워크의 어느 위치에든 설치할 수 있지만, NetApp Disaster Recovery의 경우 재해 복구 사이트에 Console 에이전트를 설치하는 것이 좋습니다. DR 사이트에 설치하면 기본 사이트에 장애가 발생하더라도 NetApp Console UI가 Console 에이전트와의 연결을 유지하고 해당 DR 사이트 내에서 복구 프로세스를 오케스트레이션할 수 있습니다.

설치

- Disaster Recovery를 사용하려면 Console 에이전트를 표준 모드로 설치하십시오. Console 에이전트 설치 유형에 대한 자세한 내용은 "NetApp Console 배포 모드에 대해 알아보세요"를 참조하십시오.

Console 에이전트의 구체적인 설치 단계는 배포 유형에 따라 다릅니다. "콘솔 에이전트에 대해 알아보세요"자세한 내용은 해당 문서를 참조하십시오.

Amazon AWS에 Console 에이전트를 설치하는 가장 간단한 방법은 AWS Marketplace를 이용하는 것입니다. AWS Marketplace를 사용한 Console 에이전트 설치에 대한 자세한 내용은 "AWS 마켓플레이스에서 Console 에이전트를 생성하세요."를 참조하십시오.

Amazon EVS에 대한 NetApp Disaster Recovery 구성

Amazon EVS에 대한 NetApp Disaster Recovery 구성 개요

NetApp Console 에이전트를 설치한 후에는 재해 복구 프로세스에 참여할 모든 ONTAP 스토리지와 VMware vCenter 리소스를 NetApp Disaster Recovery 와 통합해야 합니다.

- "NetApp Disaster Recovery 지원하는 Amazon EVS의 필수 구성 요소"
- "NetApp Disaster Recovery 에 ONTAP 스토리지 어레이 추가"
- "Amazon EVS에 대한 NetApp Disaster Recovery 활성화"
- "NetApp Disaster Recovery 에 vCenter 사이트 추가"
- "NetApp Disaster Recovery 에 vCenter 클러스터 추가"

NetApp Disaster Recovery 지원하는 Amazon EVS의 필수 구성 요소

Amazon EVS를 NetApp Disaster Recovery와 연동하여 구성하기 위한 요구 사항을 검토하고 충족했는지 확인하십시오.

필수 조건

- "Disaster Recovery를 위한 일반적인 전제 조건"를 검토해 보세요.
- NetApp Disaster Recovery 에 필요한 작업을 수행하는 데 필요한 특정 VMware 권한이 있는 vCenter 사용자 계정을 만듭니다.

기본 "administrator@vsphere.com" 관리자 계정을 사용하지 않는 것을 권장합니다. 대신, 재해 복구 프로세스에 참여할 모든 vCenter 클러스터에 NetApp Disaster Recovery 전용 사용자 계정을 생성해야 합니다. 필요한 특정 권한 목록은 "NetApp Disaster Recovery 에 필요한 vCenter 권한 "를 참조하십시오.

- 재해 복구로 보호되는 VM을 호스팅할 모든 vCenter 데이터스토어가 NetApp ONTAP 스토리지 리소스에 있는지 확인하십시오.

  재해 복구는 Amazon FSx for NetApp ONTAP을 사용할 때 iSCSI의 NFS 및 VMFS를 지원합니다(FC는 지원하지 않음). 재해 복구는 FC를 지원하지만 Amazon FSx for NetApp ONTAP은 지원하지 않습니다.

- Amazon EVS vCenter가 Amazon FSx for NetApp ONTAP 스토리지 클러스터에 연결되어 있는지 확인하십시오.
- 보호 대상 가상 머신에 VMware Tools가 설치되어 있는지 확인하십시오.
- 온프레미스 네트워크가 Amazon에서 승인한 연결 방식을 사용하여 AWS VPC 네트워크에 연결되어 있는지 확인하십시오. AWS Direct Connect, AWS Private Link 또는 AWS Site-to-Site VPN을 사용하는 것이 좋습니다.
- Disaster Recovery를 사용하는 EVS의 연결 및 포트 요구 사항을 검토하고 준수하는지 확인하십시오.

소스	목적지	포트	세부 정보
Amazon FSxN	사내 ONTAP	TCP 11104, 11105, ICMP	SnapMirror
사내 ONTAP	Amazon FSxN	TCP 11104, 11105, ICMP	SnapMirror
NetApp Console 에이전트	사내 ONTAP	TCP 443, ICMP만 해당	API 호출
NetApp Console 에이전트	Amazon FSxN	TCP 441, ICMP 전용	API 호출
NetApp Console 에이전트	vCenter(온프레미스, EVS), ESXi 호스트(온프레미스, EVS)	443	API 호출, 스크립트 실행

NetApp Disaster Recovery 사용하여 **Amazon EVS**용 **NetApp Console** 시스템에 온프레미스 어레이 추가

NetApp Disaster Recovery 사용하기 전에 온프레미스 및 클라우드 호스팅 스토리지 인스턴스를 NetApp Console 시스템에 추가해야 합니다.

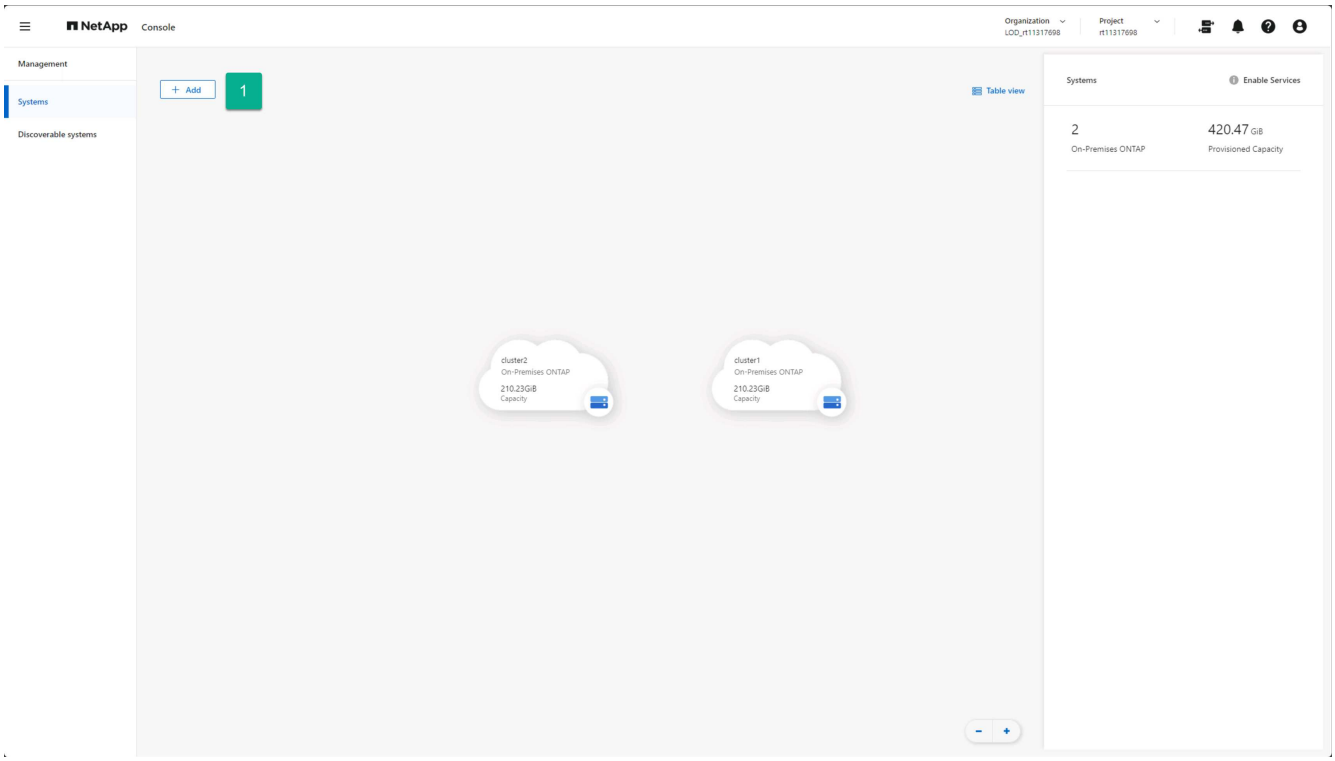
다음을 수행해야 합니다.

- NetApp Console 시스템에 온프레미스 어레이를 추가합니다.
- NetApp Console 시스템에 Amazon FSx for NetApp ONTAP (FSx for ONTAP) 인스턴스를 추가합니다.

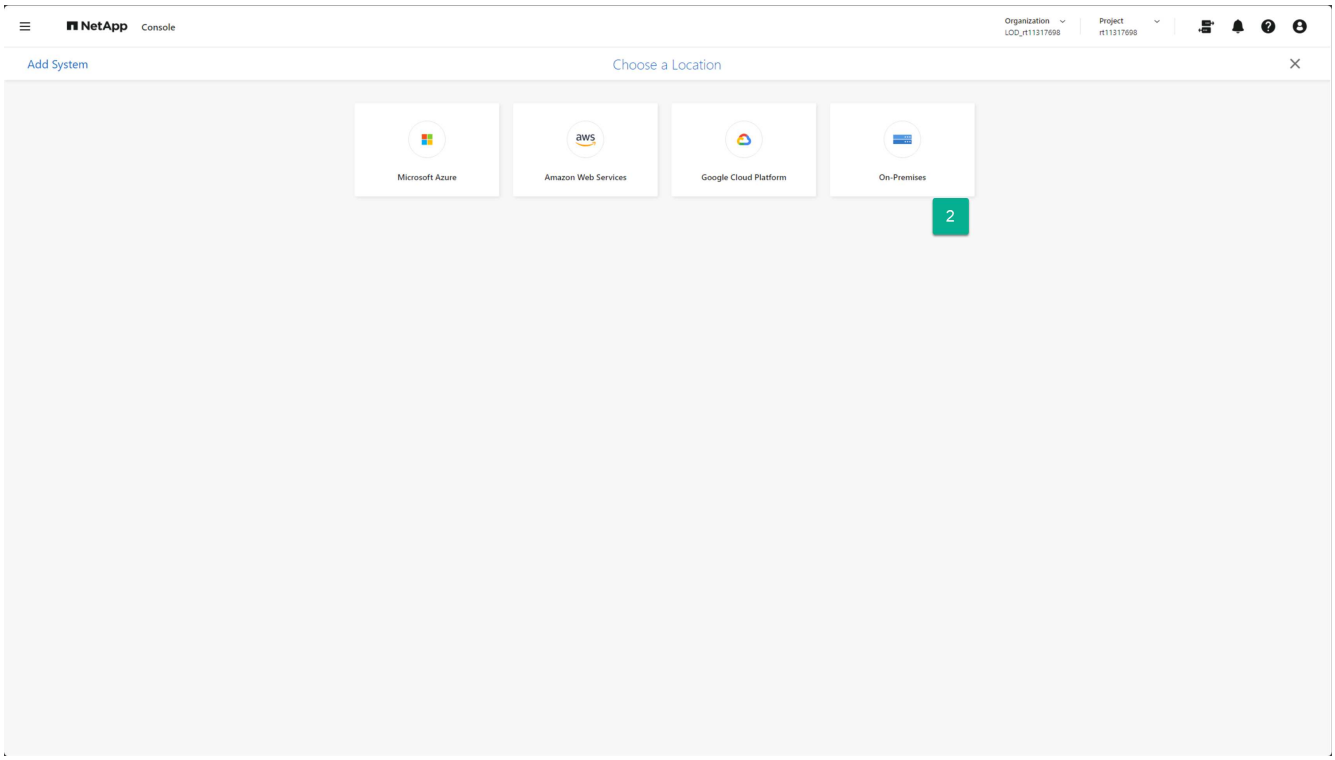
NetApp Console 시스템에 온프레미스 스토리지 어레이 추가

NetApp Console 시스템에 온프레미스 ONTAP 스토리지 리소스를 추가합니다.

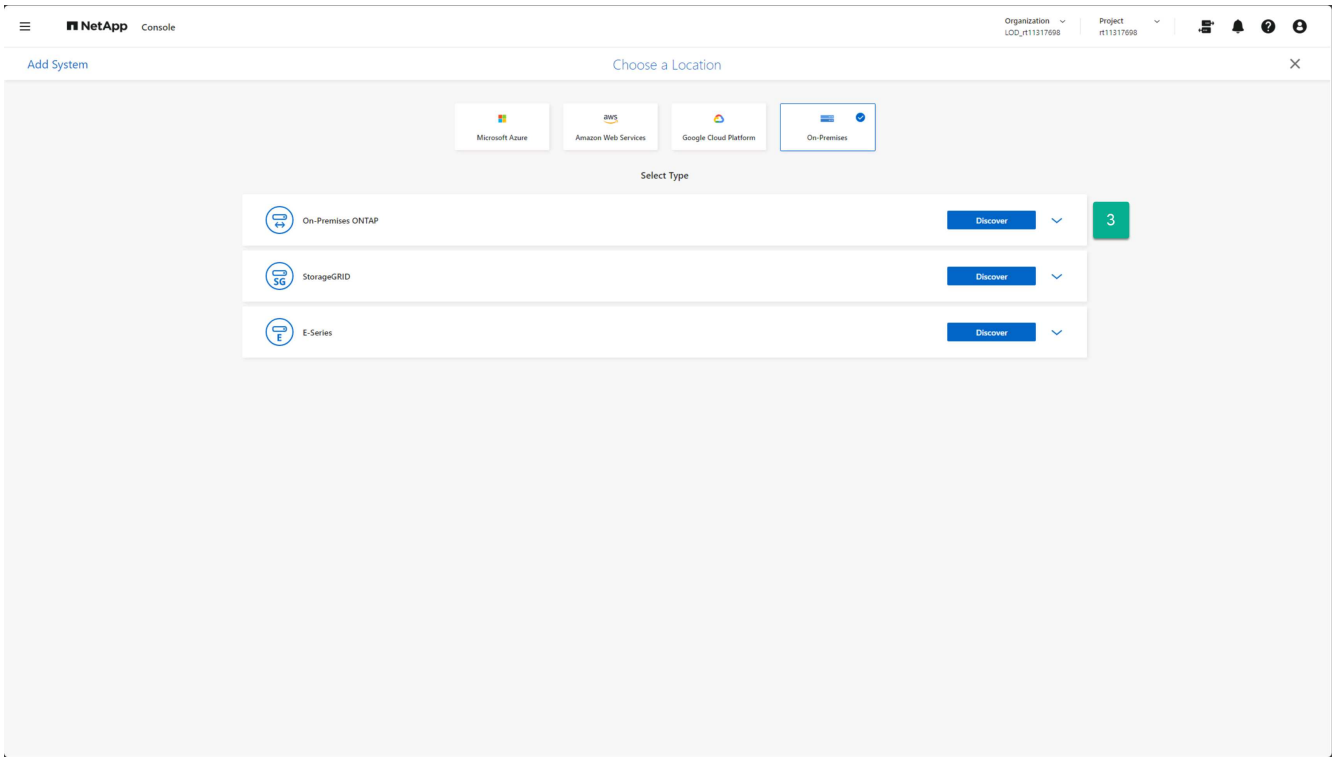
1. NetApp Console 시스템 페이지에서 *시스템 추가*를 선택합니다.



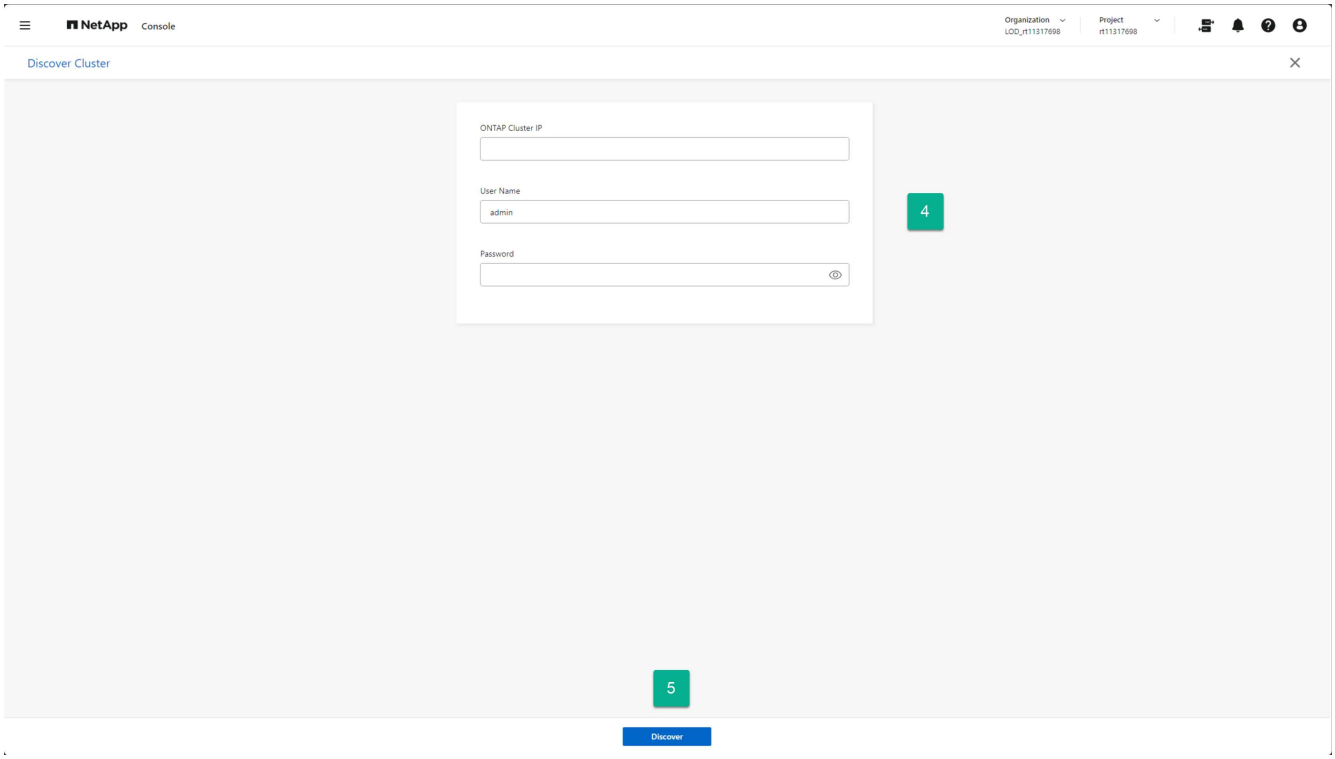
2. 시스템 추가 페이지에서 온프레미스 카드를 선택합니다.



3. On-Premises ONTAP 카드에서 *Discover*를 선택하세요.



4. 클러스터 검색 페이지에서 다음 정보를 입력합니다.
   a. ONTAP 어레이 클러스터 관리 포트의 IP 주소
   b. 관리자 사용자 이름
   c. 관리자 비밀번호
5. 페이지 하단의 *발견*을 선택하세요.

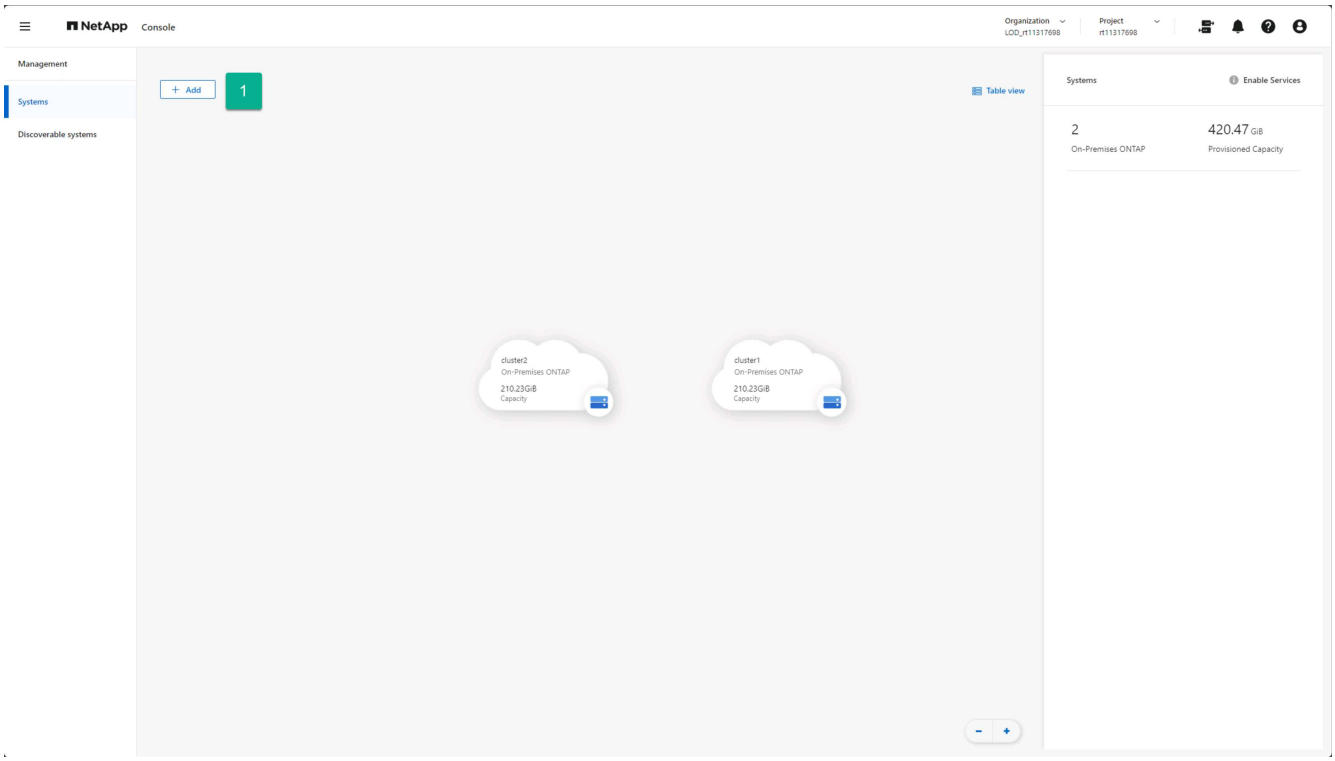


6. vCenter 데이터스토어를 호스팅할 각 ONTAP 어레이에 대해 1~5단계를 반복합니다.

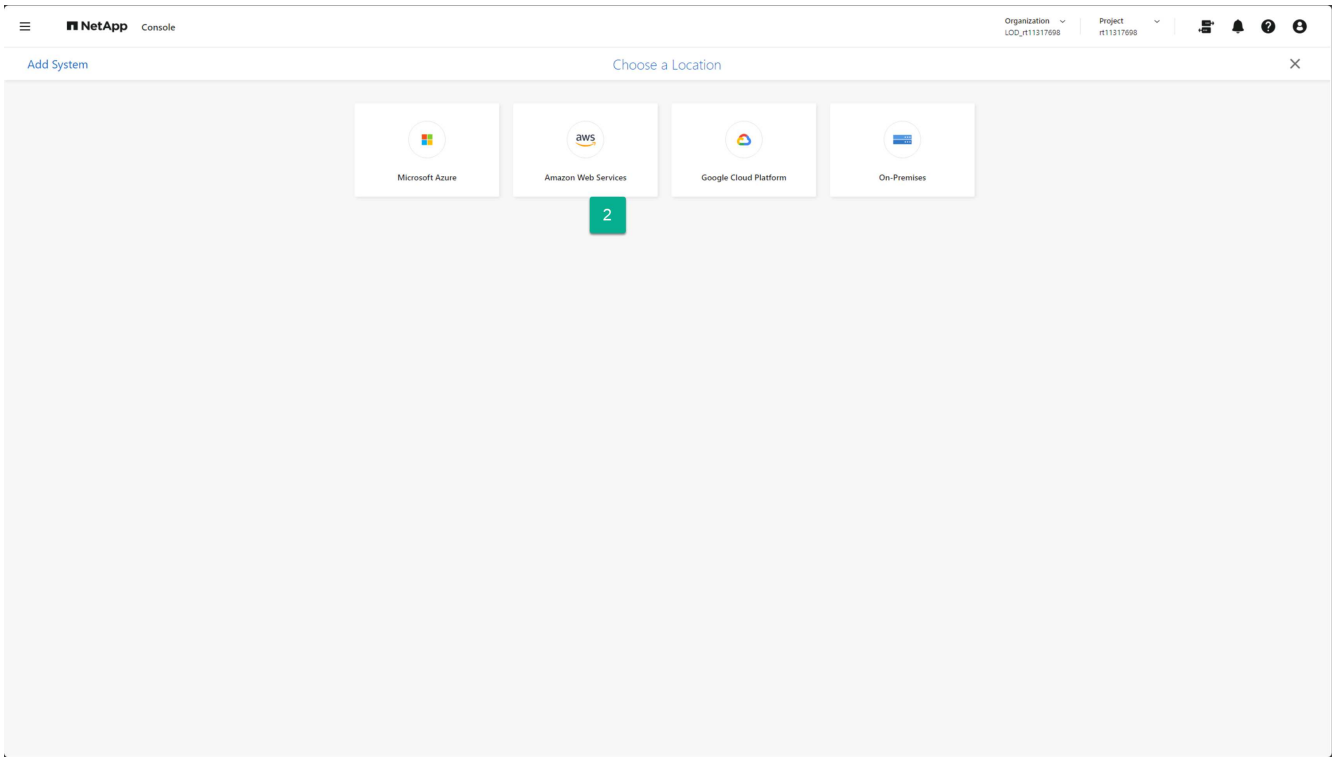
NetApp Console 시스템에 **Amazon FSx for NetApp ONTAP** 스토리지 인스턴스 추가

다음으로, NetApp Console 시스템에 Amazon FSx for NetApp ONTAP 스토리지 리소스를 추가합니다.

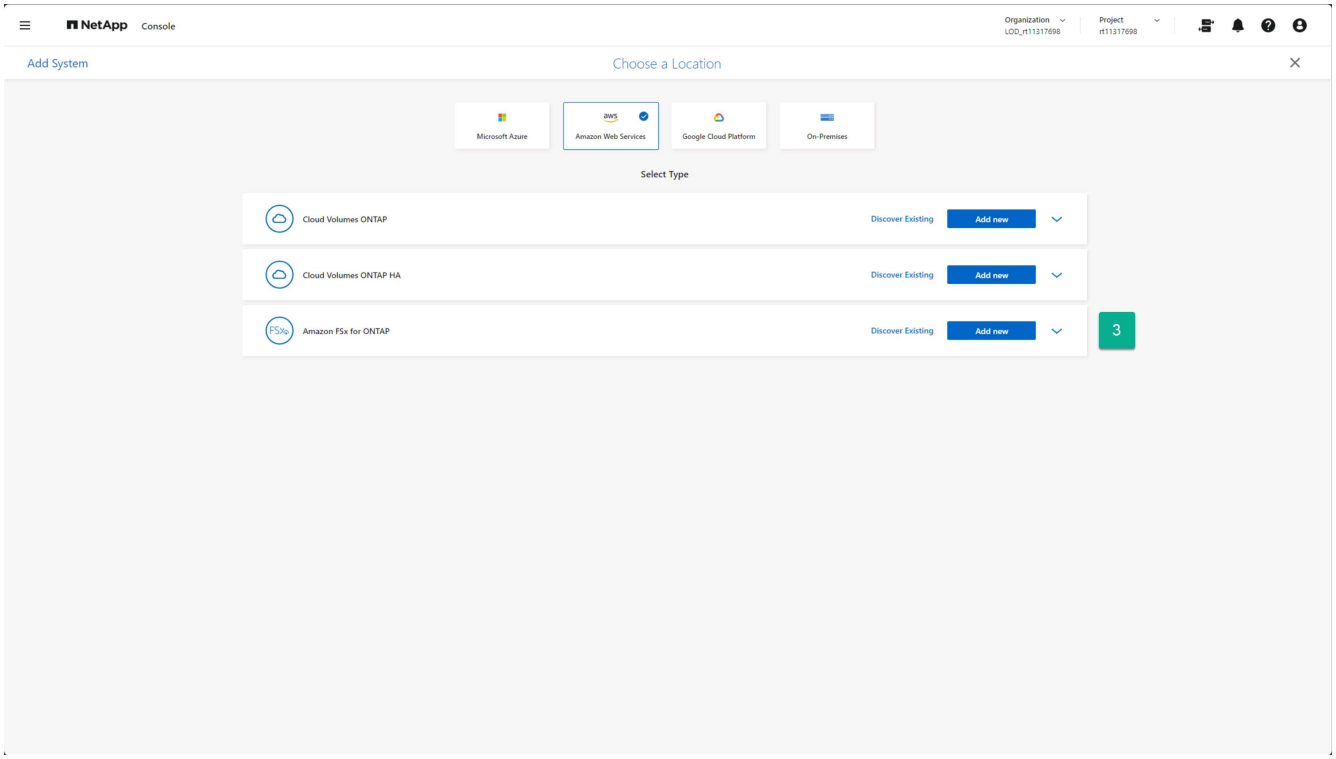
1. NetApp Console 시스템 페이지에서 *시스템 추가*를 선택합니다.



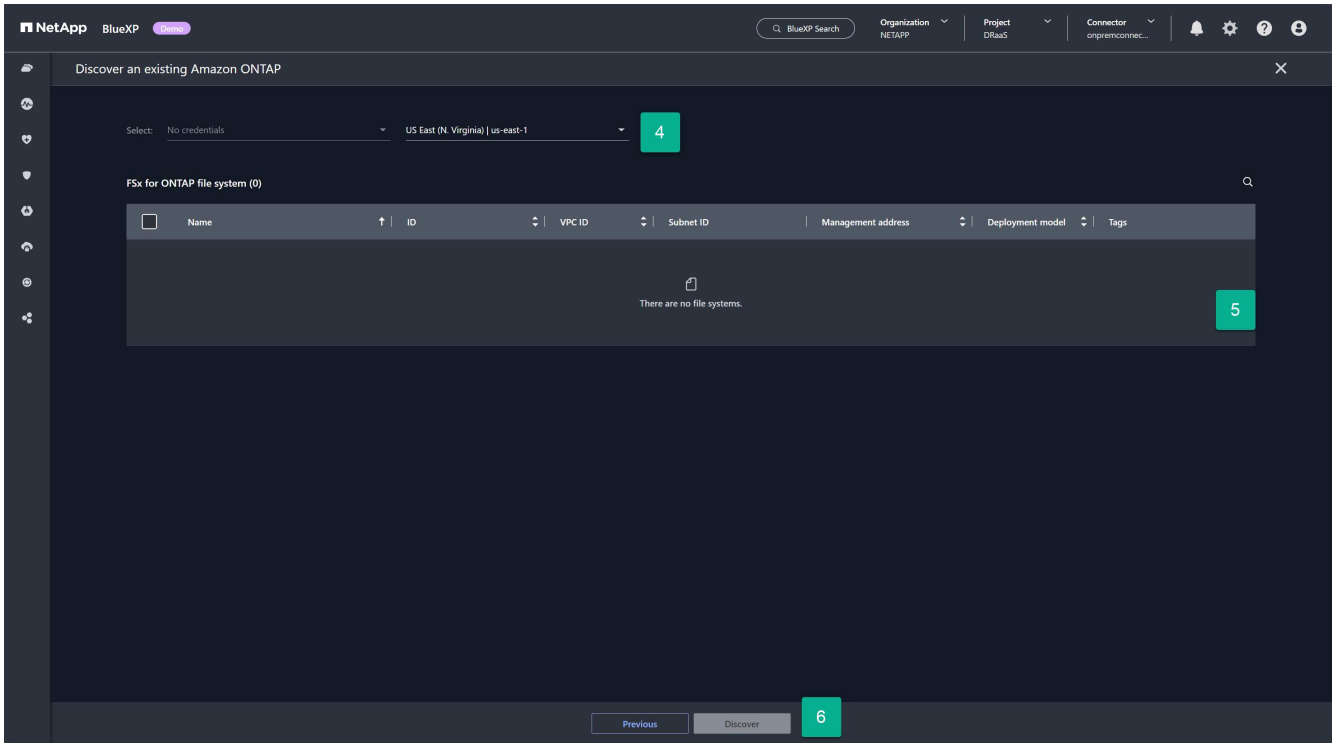
2. 시스템 추가 페이지에서 **Amazon Web Services** 카드를 선택합니다.



3. Amazon FSx for ONTAP 카드에서 기존 검색 링크를 선택합니다.



4. FSx for ONTAP 인스턴스를 호스팅하는 자격 증명과 AWS 지역을 선택합니다.
5. 추가할 FSx for ONTAP 파일 시스템을 하나 이상 선택하세요.
6. 페이지 하단의 *발견*을 선택하세요.



7. vCenter 데이터스토어를 호스팅할 각 FSx for ONTAP 인스턴스에 대해 1~6단계를 반복합니다.

Amazon EVS용 **NetApp Console** 계정에 **NetApp Disaster Recovery** 서비스 추가

NetApp Disaster Recovery 사용하기 전에 구매해야 하는 라이선스 제품입니다. 라이센스에는 여러 유형이 있으며 라이센스를 구매하는 방법도 여러 가지입니다. 라이선스는 특정 기간 동안 특정 양의 데이터를 보호할 수 있는 권한을 부여합니다.

NetApp Disaster Recovery 라이선스에 대한 자세한 내용은 다음을 참조하세요."NetApp Disaster Recovery 에 대한 라이선싱 설정" .

라이센스 유형

주요 라이센스 유형은 두 가지입니다.

- NetApp 다음을 제공합니다."30일 체험판 라이선스" ONTAP 및 VMware 리소스를 사용하여 NetApp Disaster Recovery 평가하는 데 사용할 수 있습니다. 이 라이선스는 보호된 용량을 무제한으로 30일 동안 사용할 수 있도록 제공합니다.
- 30일 평가판 기간 이후에도 DR 보호를 원하시면 프로덕션 라이선스를 구매하세요. 이 라이선스는 NetApp의 클라우드 파트너 마켓플레이스를 통해 구매할 수 있지만, 이 가이드에서는 Amazon AWS Marketplace를 사용하여 NetApp Disaster Recovery 용 마켓플레이스 라이선스를 구매하는 것이 좋습니다. Amazon Marketplace를 통해 라이선스를 구매하는 방법에 대해 자세히 알아보려면 다음을 참조하세요."AWS Marketplace를 통해 구독하세요" .

재해 복구 용량 요구 사항 크기 조정

라이선스를 구매하기 전에 보호해야 할 ONTAP 스토리지 용량이 얼마인지 파악해야 합니다. NetApp ONTAP 스토리지를 사용하는 이점 중 하나는 NetApp 데이터를 저장하는 방식이 매우 효율적이라는 것입니다. ONTAP 볼륨에 저장된 모든 데이터(VMware 데이터스토어 호스팅 등)는 매우 효율적인 방식으로 저장됩니다. ONTAP 물리적 저장소에 데이터를 쓸 때 압축, 중복 제거, 압축의 세 가지 유형의 저장 효율성을 기본적으로 사용합니다. 결과적으로 저장 효율성은 저장되는 데이터 유형에 따라 1.5:1에서 4:1 사이가 됩니다. 실제로 NetApp 다음을 제공합니다. "저장 효율성

보장" 특정 작업 부하에 대해서.

NetApp Disaster Recovery 모든 ONTAP 스토리지 효율성이 적용된 후 라이선스 목적으로 용량을 계산하므로 이 방법이 유용할 수 있습니다. 예를 들어, 서비스를 사용하여 보호하려는 100개의 VM을 호스팅하기 위해 vCenter 내에 100테라바이트(TiB) NFS 데이터 저장소를 프로비저닝했다고 가정해 보겠습니다. 또한, 데이터가 ONTAP 볼륨에 기록될 때 자동으로 적용되는 스토리지 효율성 기술로 인해 해당 VM이 33TiB(3:1 스토리지 효율성)만 사용한다고 가정해 보겠습니다. NetApp Disaster Recovery 100TiB가 아닌 33TiB에 대해서만 라이선스가 필요합니다. 이는 다른 DR 솔루션과 비교했을 때 DR 솔루션의 총 소유 비용에 매우 큰 이점이 될 수 있습니다.

단계

1. 보호할 VMware 데이터스토어를 호스팅하는 각 볼륨에서 얼마나 많은 데이터가 소모되는지 확인하려면 각 볼륨에 대해 ONTAP CLI 명령을 실행하여 디스크 용량 소모량을 확인하세요. `volume show-space -volume < volume name > -vserver < SVM name >`.

   예를 들어:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
------------------------------      --------     ------
User Data                             163.4MB         3%
Filesystem Metadata                     172KB         0%
Inodes                                 2.93MB         0%
Snapshot Reserve                       292.9MB         5%
Total Metadata                          185KB         0%
Total Used                             459.4MB         8%
Total Physical Used                    166.4MB         3%
```

2. 각 볼륨의 총 물리적 사용량 값을 확인하세요. 이는 NetApp Disaster Recovery 보호해야 하는 데이터 양이며, 라이선스가 필요한 용량을 결정하는 데 사용되는 값입니다.

Amazon EVS용 NetApp Disaster Recovery 에 사이트 추가

VM 인프라를 보호하기 전에 보호할 VM을 호스팅하는 VMware vCenter 클러스터와 해당 vCenter가 있는 위치를 파악해야 합니다. 첫 번째 단계는 소스 및 대상 데이터 센터를 나타내는 사이트를 만드는 것입니다. 사이트는 장애 도메인 또는 복구 도메인입니다.

다음을 만들어야 합니다.

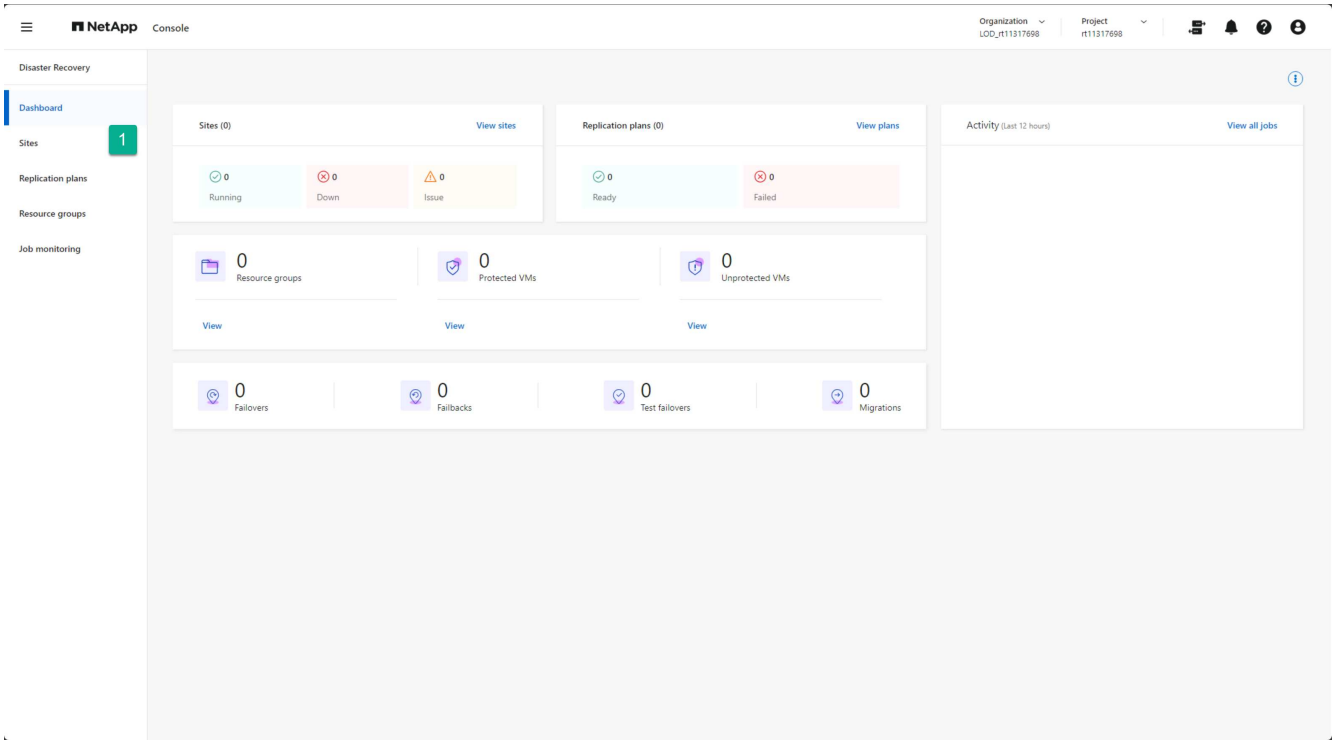
- 프로덕션 vCenter 클러스터가 있는 각 프로덕션 데이터 센터를 나타내는 사이트
- Amazon EVS/ Amazon FSx for NetApp ONTAP 클라우드 데이터 센터를 위한 사이트

온프레미스 사이트 만들기

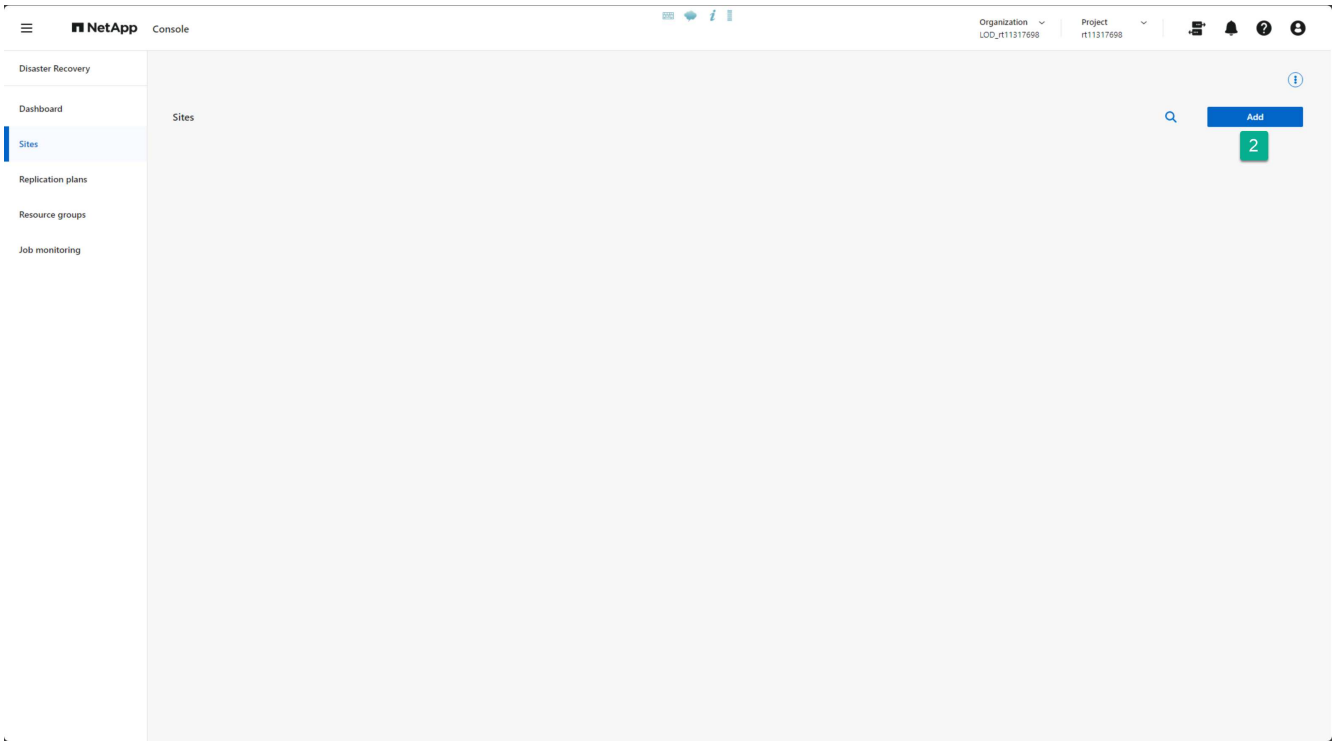
프로덕션 vCenter 사이트를 만듭니다.

단계

1. NetApp Console 왼쪽 탐색 모음에서 보호 > *재해 복구*를 선택합니다.
2. NetApp Disaster Recovery 의 모든 페이지에서 사이트 옵션을 선택합니다.

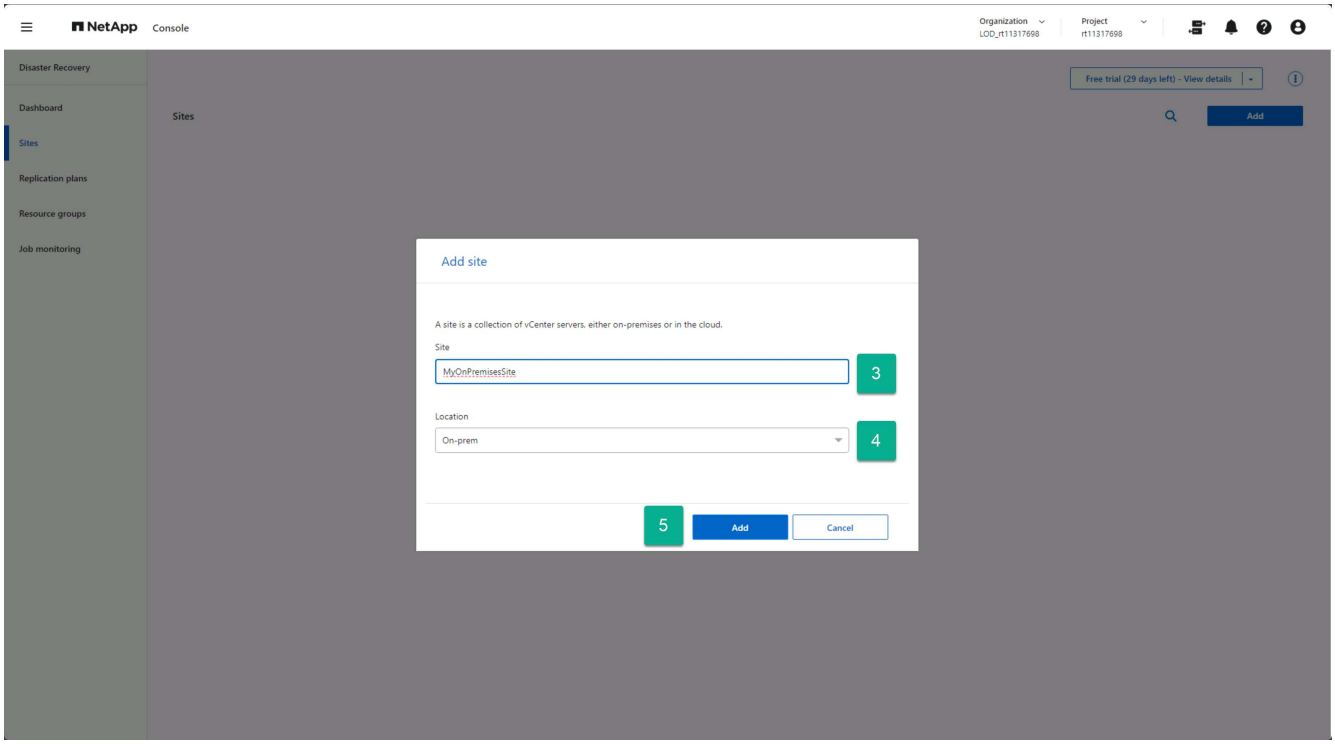


3. 사이트 옵션에서 *추가*를 선택합니다.



4. 사이트 추가 대화 상자에서 사이트 이름을 입력합니다.
5. 위치로 "온프레미스"를 선택합니다.

6. *추가*를 선택하세요.

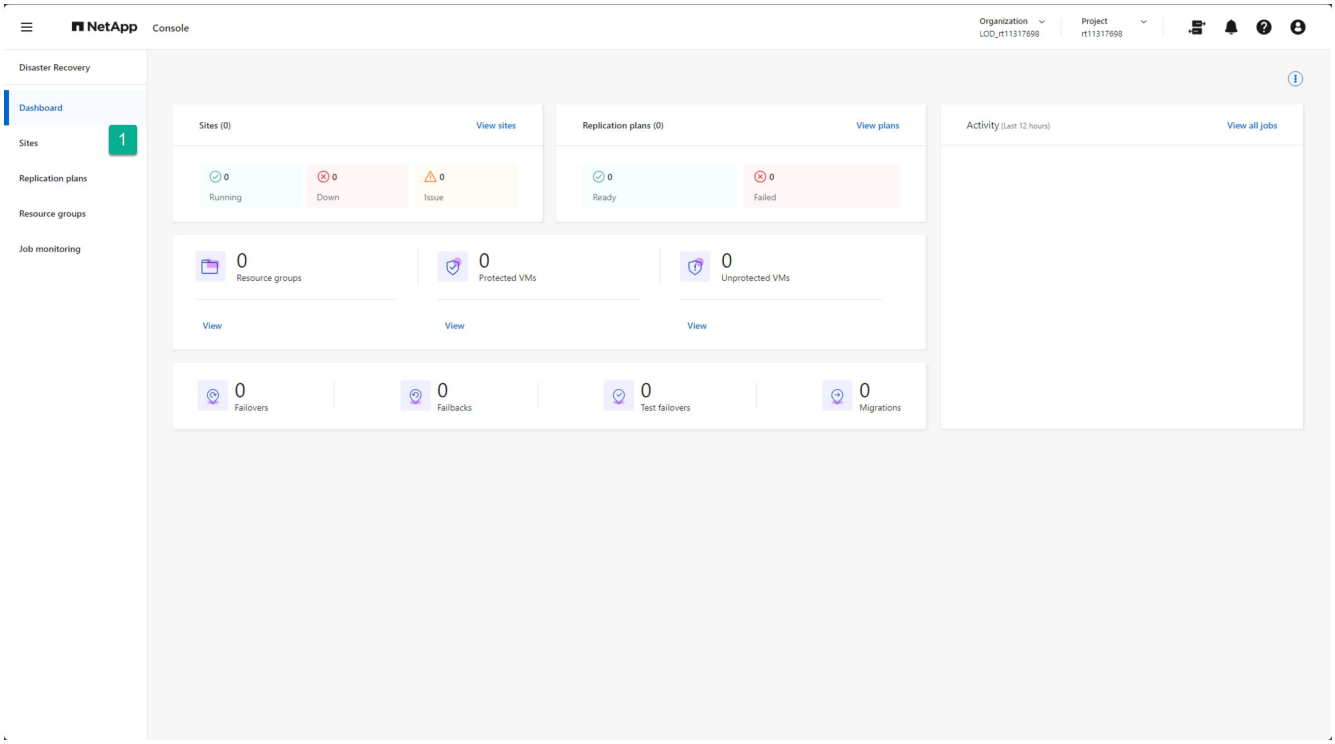


다른 프로덕션 vCenter 사이트가 있는 경우 동일한 단계를 사용하여 추가할 수 있습니다.

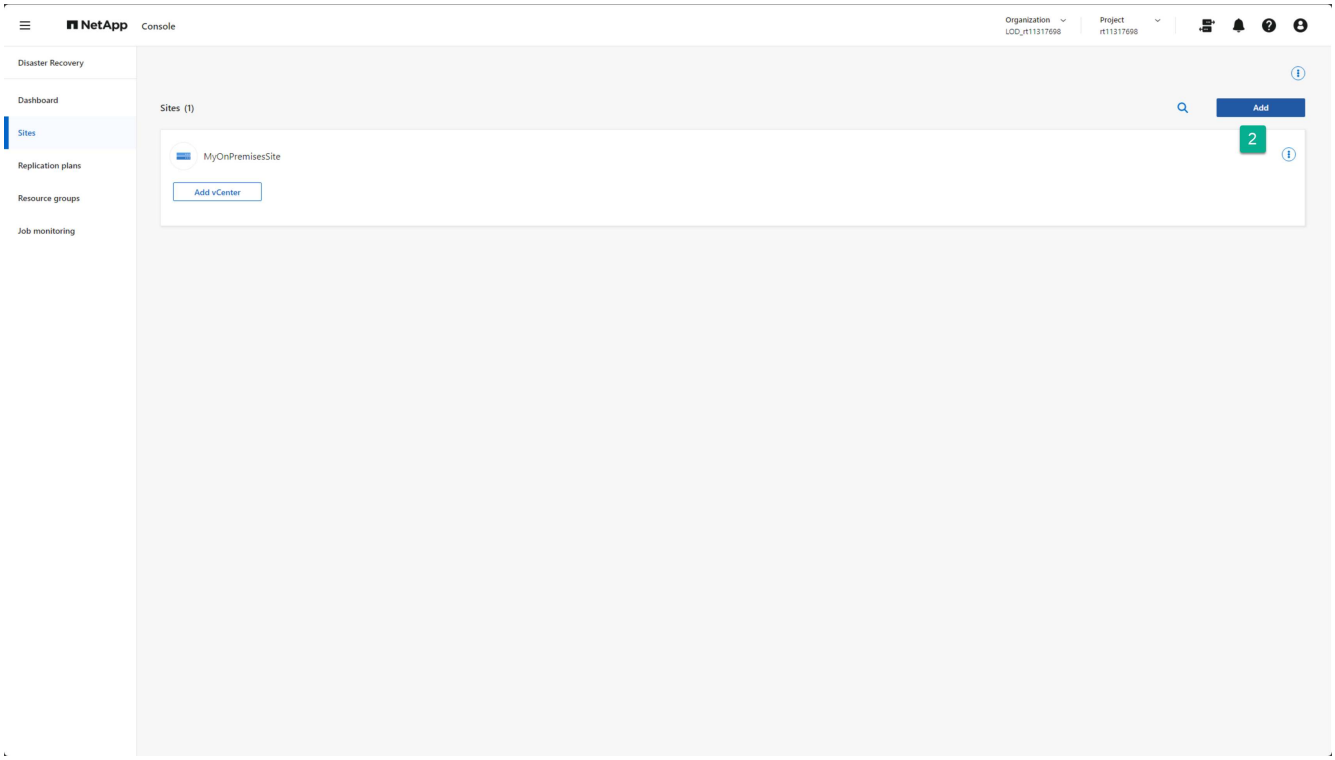
Amazon 클라우드 사이트 만들기

Amazon FSx for NetApp ONTAP 스토리지를 사용하여 Amazon EVS에 대한 DR 사이트를 만듭니다.

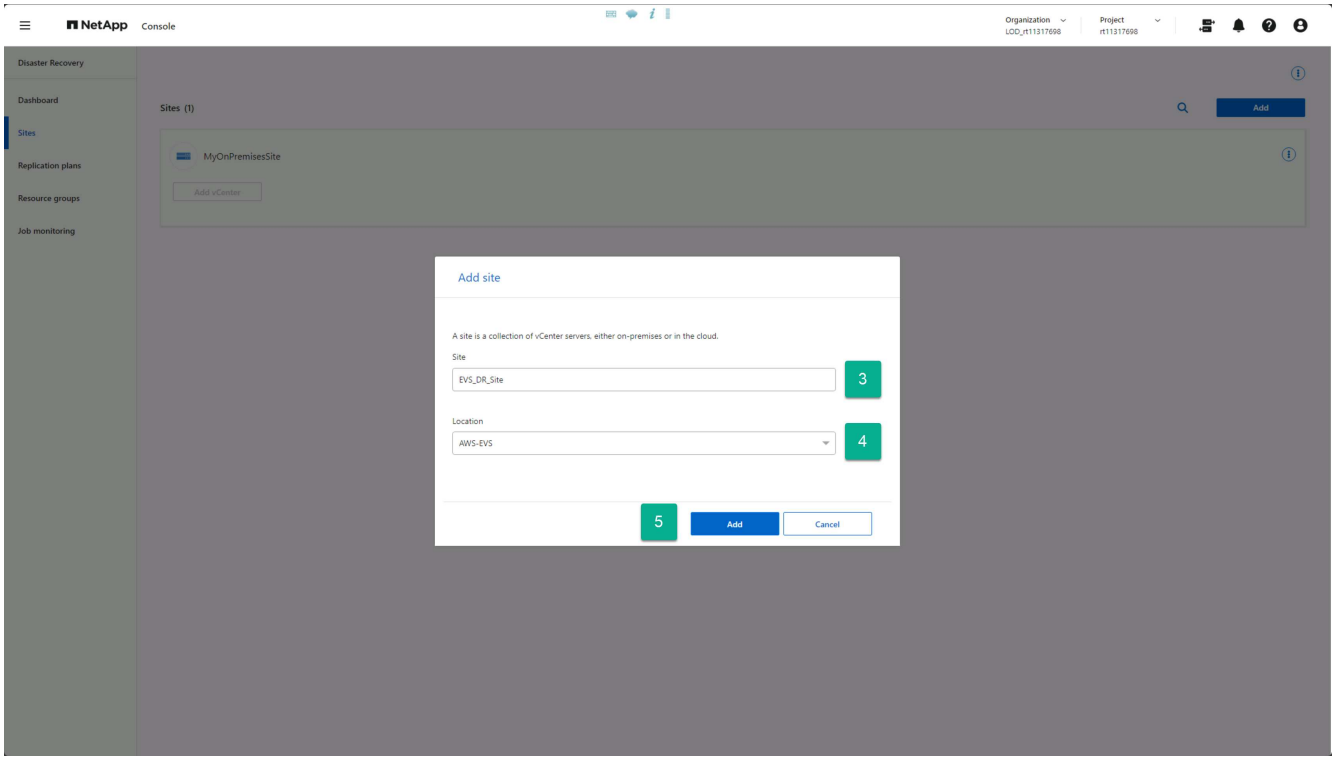
1. NetApp Disaster Recovery 의 모든 페이지에서 사이트 옵션을 선택합니다.



2. 사이트 옵션에서 *추가*를 선택합니다.



3. 사이트 추가 대화 상자에서 사이트 이름을 입력합니다.
4. 위치로 "AWS-EVS"를 선택합니다.
5. *추가*를 선택하세요.



결과

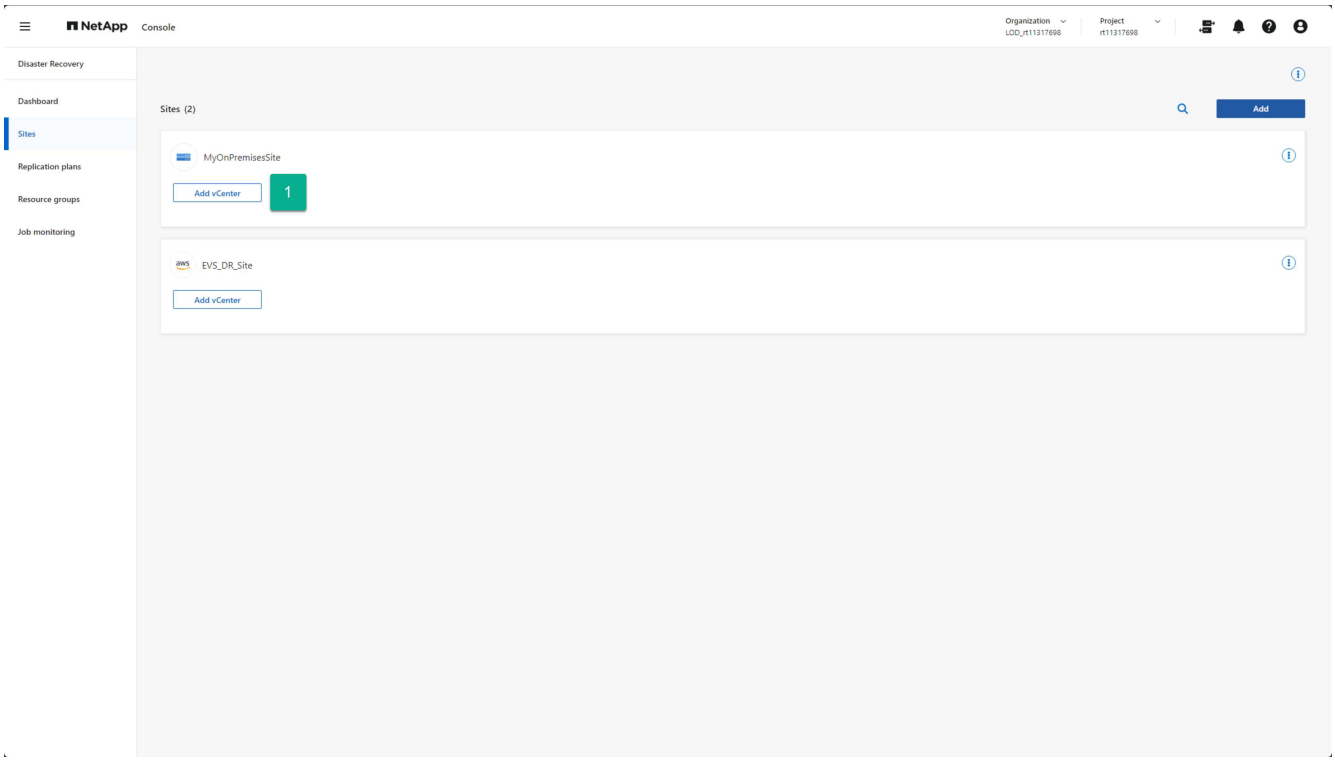
이제 프로덕션(소스) 사이트와 DR(대상) 사이트가 생성되었습니다.

NetApp Disaster Recovery 에 온프레미스 및 **Amazon EVS vCenter** 클러스터 추가

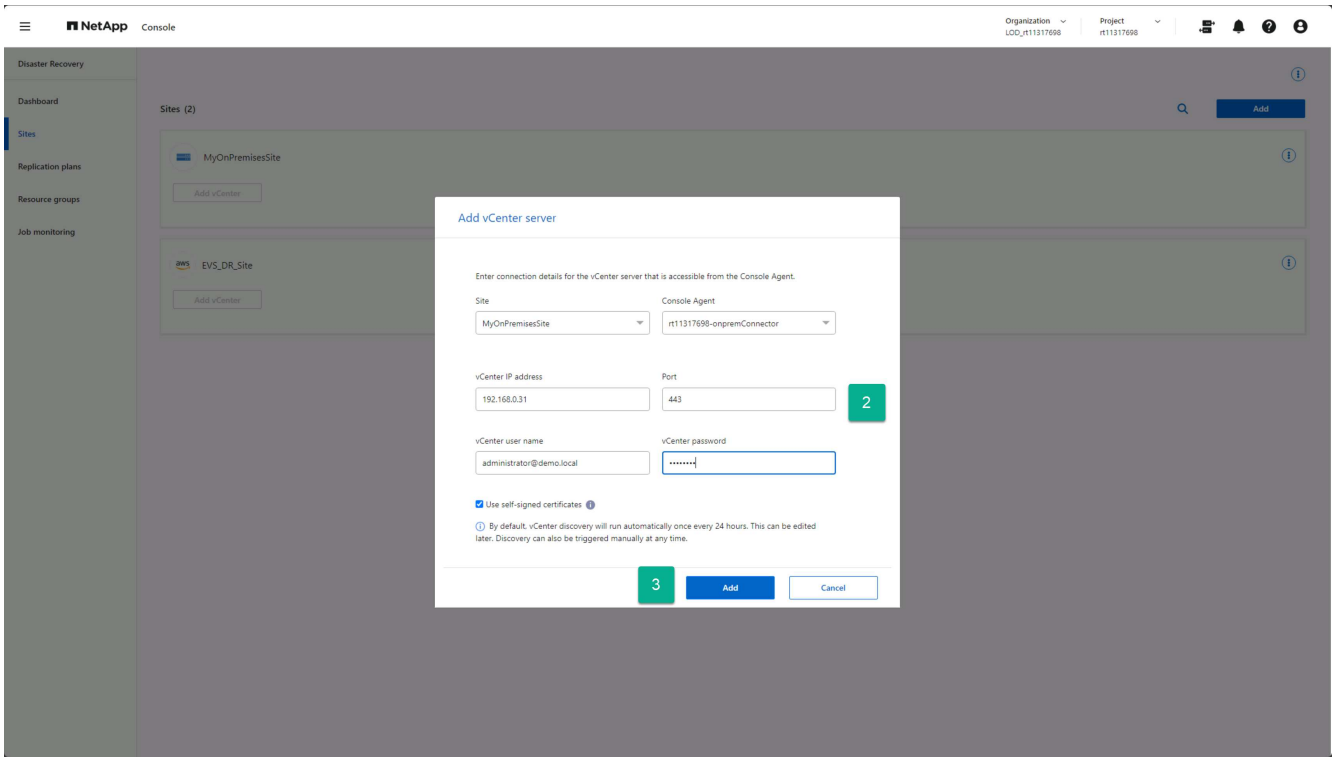
사이트가 생성되었으므로 이제 NetApp Disaster Recovery 의 각 사이트에 vCenter 클러스터를 추가합니다. 각 사이트를 만들 때 우리는 각 사이트 유형을 지정했습니다. 이를 통해 NetApp Disaster Recovery 각 사이트 유형에 호스팅된 vCenter에 필요한 액세스 유형을 알 수 있습니다. Amazon EVS의 장점 중 하나는 Amazon EVS vCenter와 온프레미스 vCenter 사이에 실질적인 차이가 없다는 것입니다. 둘 다 동일한 연결 및 인증 정보가 필요합니다.

각 사이트에 **vCenter**를 추가하는 단계

1. 사이트 옵션에서 원하는 사이트에 대해 *vCenter 추가*를 선택합니다.



2. vCenter 서버 추가 대화 상자에서 다음 정보를 선택하거나 제공합니다.
   a. AWS VPC 내에 호스팅된 NetApp Console 에이전트입니다.
   b. 추가할 vCenter의 IP 주소 또는 FQDN입니다.
   c. 다르다면 포트 값을 vCenter 클러스터 관리자가 사용하는 TCP 포트로 변경하세요.
   d. NetApp Disaster Recovery 에서 vCenter를 관리하는 데 사용할 이전에 만든 계정의 vCenter 사용자 이름입니다.
   e. 제공된 사용자 이름에 대한 vCenter 비밀번호입니다.
   f. 회사에서 외부 인증 기관(CA)이나 vCenter Endpoint 인증서 저장소를 사용하여 vCenter에 액세스하는 경우 자체 서명 인증서 사용 확인란의 선택을 취소합니다. 그렇지 않으면 상자를 체크된 상태로 두세요.
3. *추가*를 선택하세요.



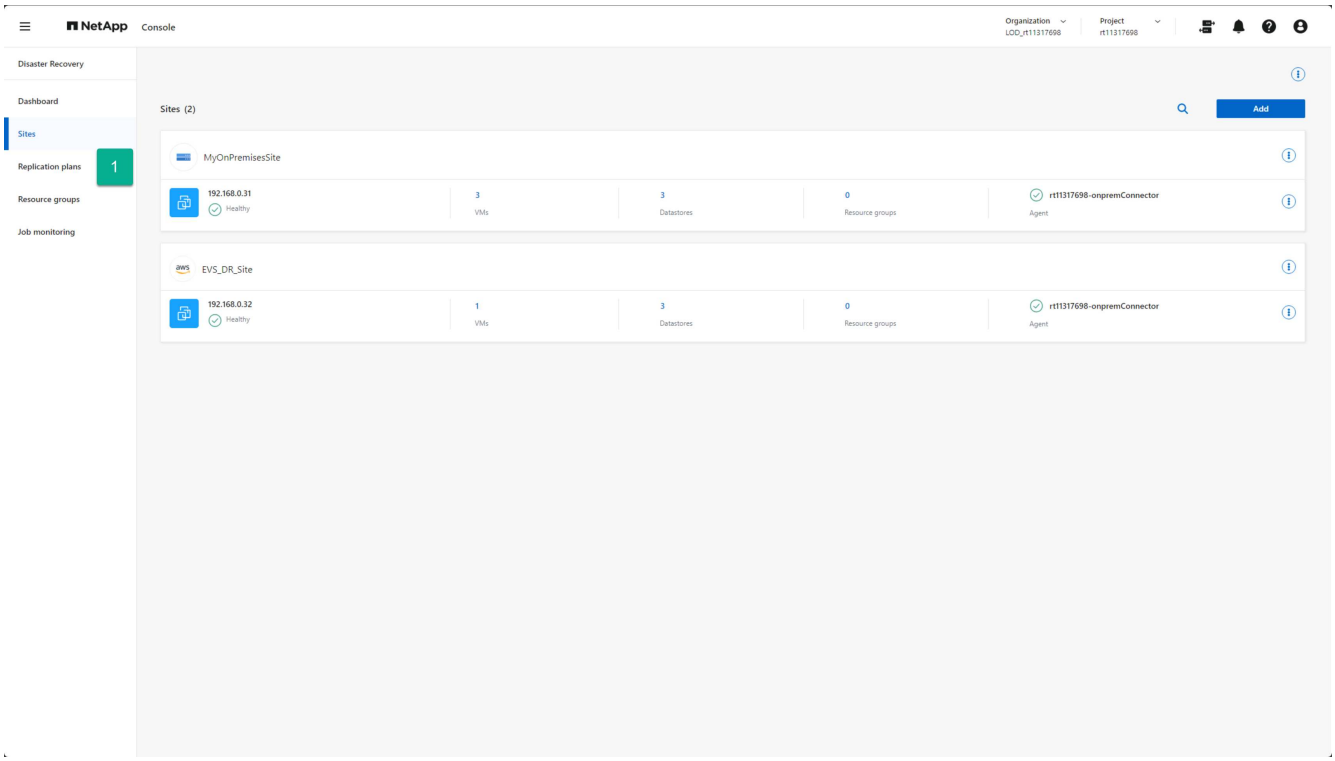
Amazon EVS에 대한 복제 계획 생성

NetApp Disaster Recovery 개요에서 복제 계획 만들기

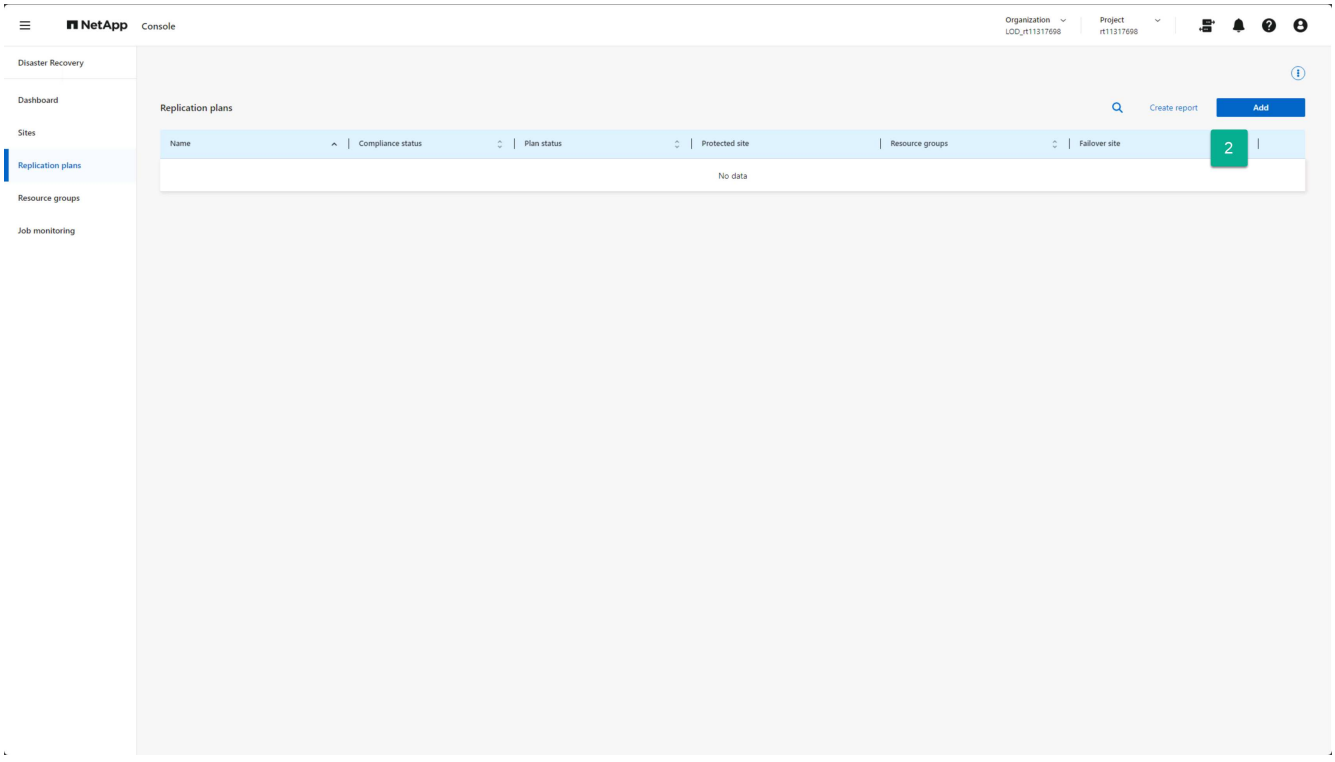
온프레미스 사이트에서 보호할 vCenter가 있고 Amazon FSx for NetApp ONTAP 사용하도록 구성된 Amazon EVS 사이트가 DR 대상으로 사용 가능해지면 온프레미스 사이트 내의 vCenter 클러스터에 호스팅된 모든 VM 세트를 보호하기 위한 복제 계획(RP)을 생성할 수 있습니다.

복제 계획 생성 프로세스를 시작하려면:

1. NetApp Disaster Recovery 화면에서 복제 계획 옵션을 선택합니다.



2. 복제 계획 페이지에서 *추가*를 선택합니다.



그러면 복제 계획 생성 마법사가 열립니다.

계속하기"복제 계획 마법사 생성 1단계" .

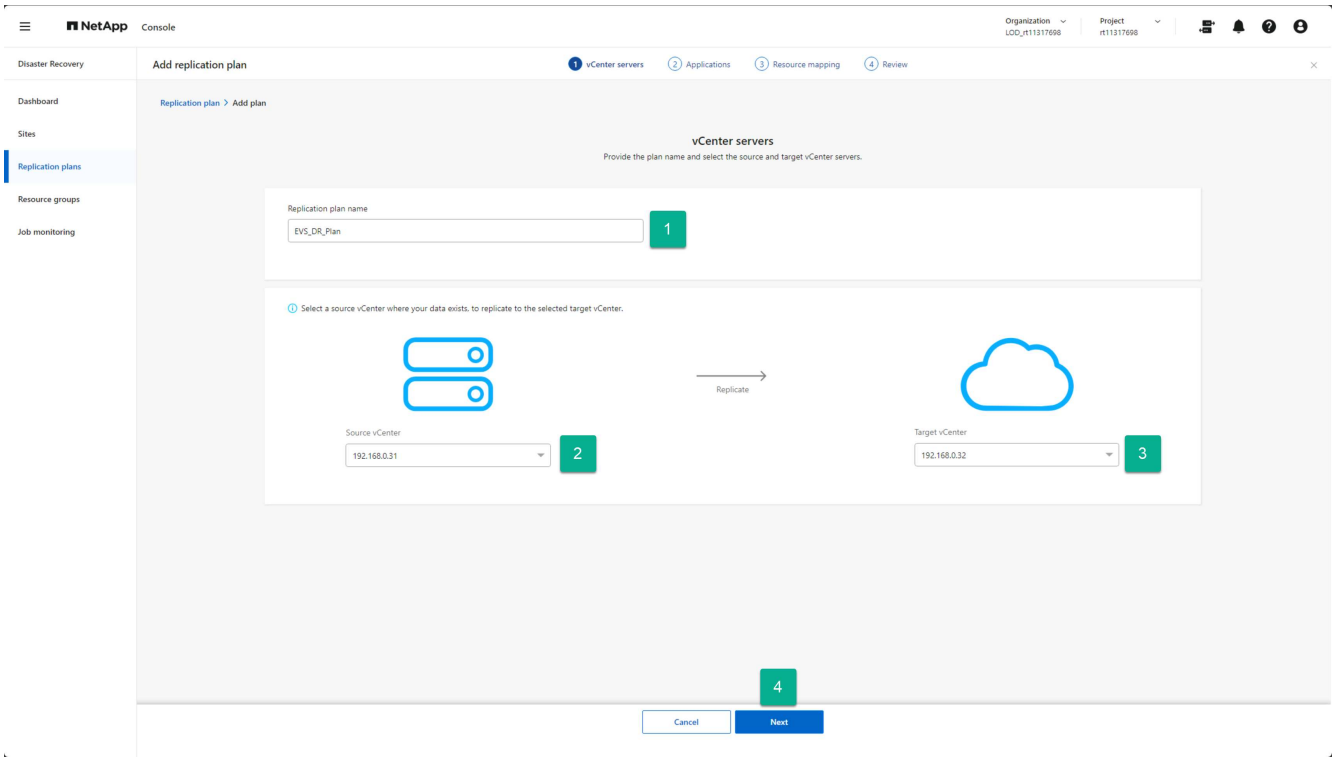
복제 계획 만들기: **1**단계 **- NetApp Disaster Recovery** 에서 **vCenter** 선택

먼저 NetApp Disaster Recovery 사용하여 복제 계획 이름을 제공하고 복제를 위한 소스 및 대상 vCenter를 선택합니다.

1. 복제 계획에 대한 고유한 이름을 입력하세요.

   복제 계획 이름에는 영숫자 문자와 밑줄(_)만 허용됩니다.

2. 소스 vCenter 클러스터를 선택하세요.
3. 대상 vCenter 클러스터를 선택하세요.
4. *다음*을 선택하세요.



계속하기"복제 계획 마법사 2단계 생성" .

복제 계획 만들기: **2**단계 **- NetApp Disaster Recovery** 에서 **VM** 리소스 선택

NetApp Disaster Recovery 사용하여 보호할 가상 머신을 선택합니다.

보호를 위해 VM을 선택하는 방법에는 여러 가지가 있습니다.

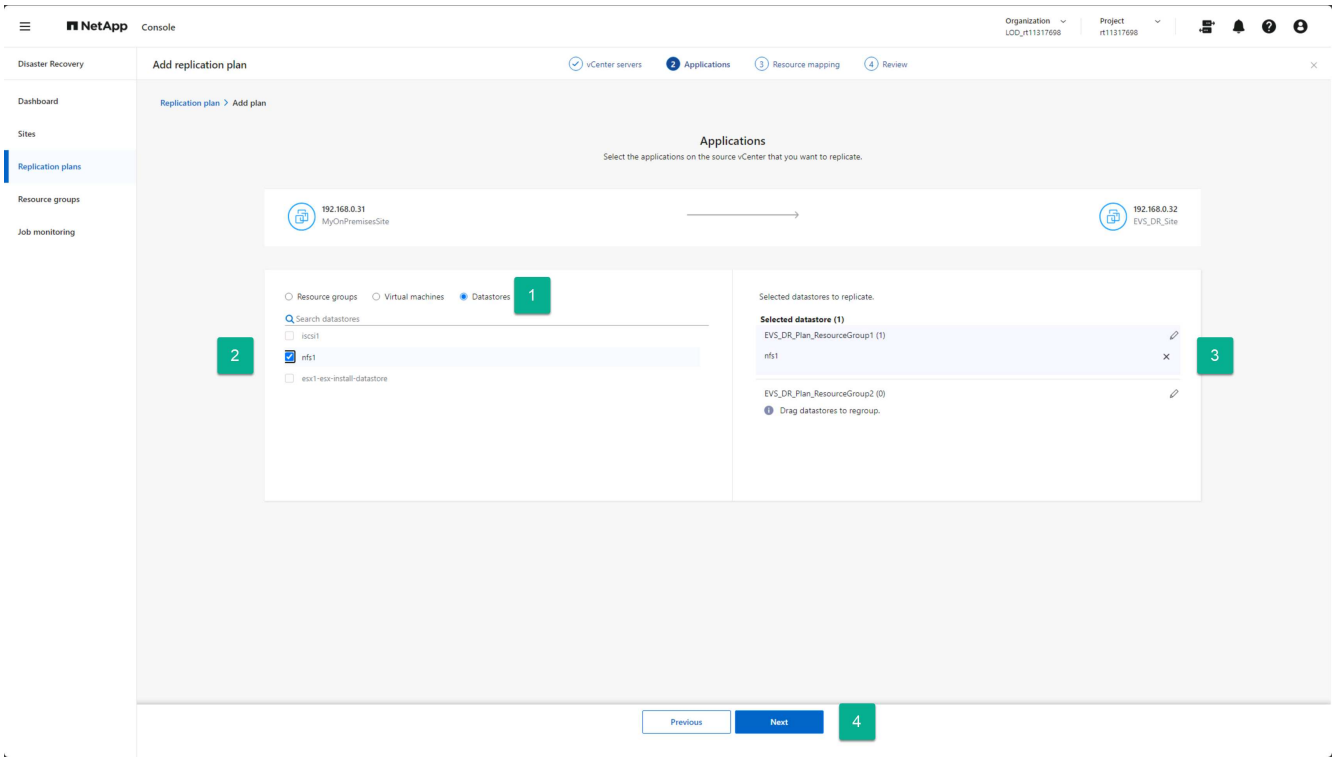
- 개별 **VM** 선택: 가상 머신 버튼을 클릭하면 보호할 개별 VM을 선택할 수 있습니다. 각 VM을 선택하면 서비스는 화면 오른쪽에 있는 기본 리소스 그룹에 해당 VM을 추가합니다.
- 이전에 생성한 리소스 그룹 선택: NetApp Disaster Recovery 메뉴의 리소스 그룹 옵션을 사용하여 미리 사용자 지정 리소스 그룹을 만들 수 있습니다. 이는 필수 사항이 아니며, 복제 계획 프로세스의 일부로 다른 두 가지 방법을 사용하여 리소스 그룹을 만들 수 있습니다. 자세한 내용은 다음을 참조하십시오. "복제 계획 만들기" .
- 전체 **vCenter** 데이터스토어 선택: 이 복제 계획으로 보호해야 할 VM이 많은 경우 개별 VM을 선택하는 것이

효율적이지 않을 수 있습니다. NetApp Disaster Recovery 볼륨 기반 SnapMirror 복제를 사용하여 VM을 보호하므로 데이터 저장소에 있는 모든 VM은 볼륨의 일부로 복제됩니다. 대부분의 경우 NetApp Disaster Recovery 사용하여 데이터 저장소에 있는 모든 VM을 보호하고 다시 시작해야 합니다. 이 옵션을 사용하면 선택한 데이터 저장소에 호스팅된 모든 VM을 보호된 VM 목록에 추가하도록 서비스에 지시할 수 있습니다.

이 가이드에서는 전체 vCenter 데이터스토어를 선택합니다.

이 페이지에 접근하는 단계

1. 복제 계획 페이지에서 응용 프로그램 섹션으로 이동합니다.
2. 열리는 신청 페이지에서 정보를 검토하세요.



데이터 저장소를 선택하는 단계:

1. *데이터 저장소*를 선택하세요.
2. 보호하려는 각 데이터 저장소 옆에 있는 확인란을 선택하세요.
3. (선택 사항) 리소스 그룹 이름 옆에 있는 연필 아이콘을 선택하여 리소스 그룹의 이름을 적절한 이름으로 바꿉니다.
4. *다음*을 선택하세요.

계속하기"복제 계획 마법사 3단계 생성" .

복제 계획 만들기: **3**단계 **- NetApp Disaster Recovery** 에서 리소스 매핑

NetApp Disaster Recovery 사용하여 보호하려는 VM 목록을 만든 후 장애 조치 중에 사용할 장애 조치 매핑 및 VM 구성 정보를 제공합니다.

네 가지 주요 유형의 정보를 매핑해야 합니다.

- 컴퓨팅 리소스

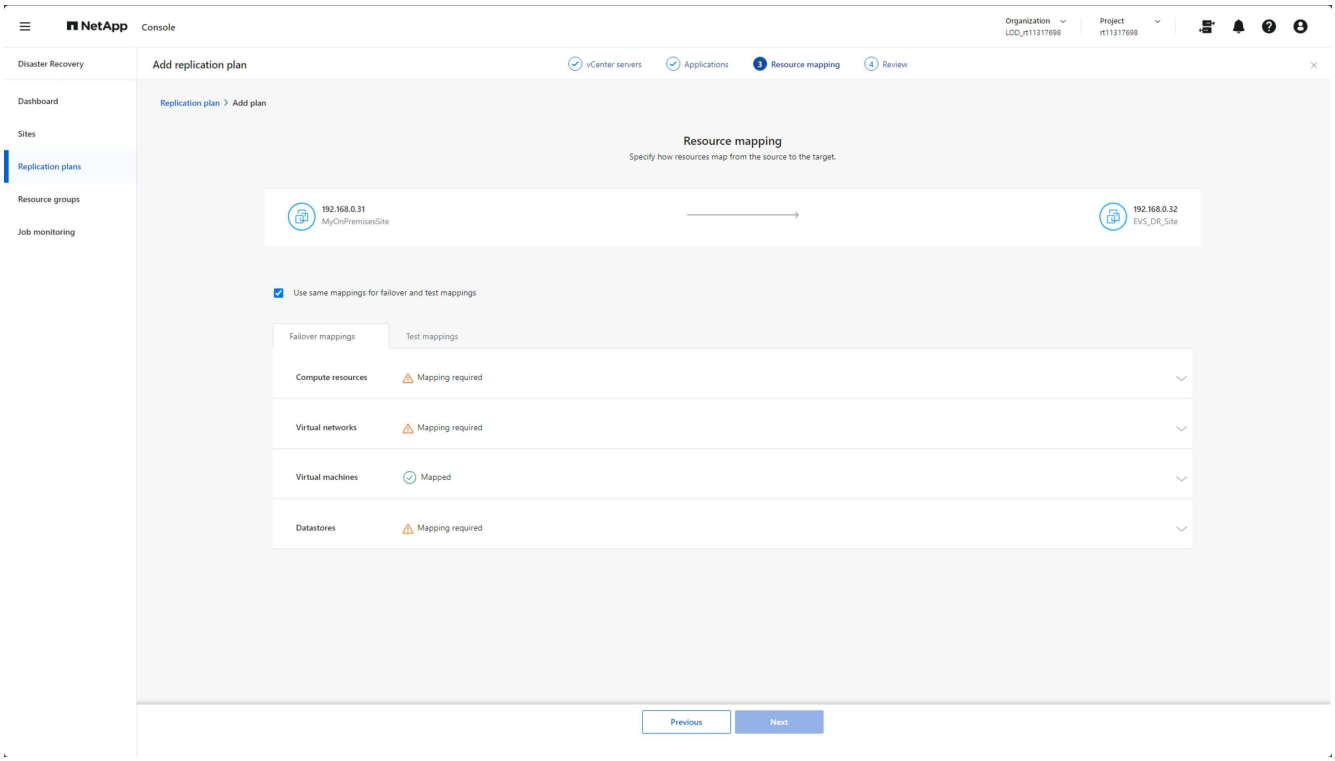
- 가상 네트워크
- VM 재구성
- 데이터 저장소 매핑

각 VM에는 처음 세 가지 유형의 정보가 필요합니다. 보호할 VM을 호스팅하는 각 데이터스토어에 대해 데이터스토어 매핑이 필요합니다.

- 주의 아이콘이 있는 섹션( ) 매핑 정보를 제공해야 합니다.
- 체크 아이콘( )이 표시된 섹션)이 매핑되었거나 기본 매핑이 있습니다. 현재 구성이 요구 사항을 충족하는지 검토하세요.

이 페이지에 접근하는 단계

1. 복제 계획 페이지에서 리소스 매핑 섹션으로 이동합니다.
2. 열리는 리소스 매핑 페이지에서 정보를 검토하세요.



3. 필요한 각 매핑 카테고리를 열려면 섹션 옆에 있는 아래쪽 화살표(**v**)를 선택하세요.

컴퓨팅 리소스 매핑

사이트는 여러 개의 가상 데이터 센터와 여러 개의 vCenter 클러스터를 호스팅할 수 있으므로 장애 조치(failover) 발생 시 VM을 복구할 vCenter 클러스터를 식별해야 합니다.

컴퓨팅 리소스를 매핑하는 단계

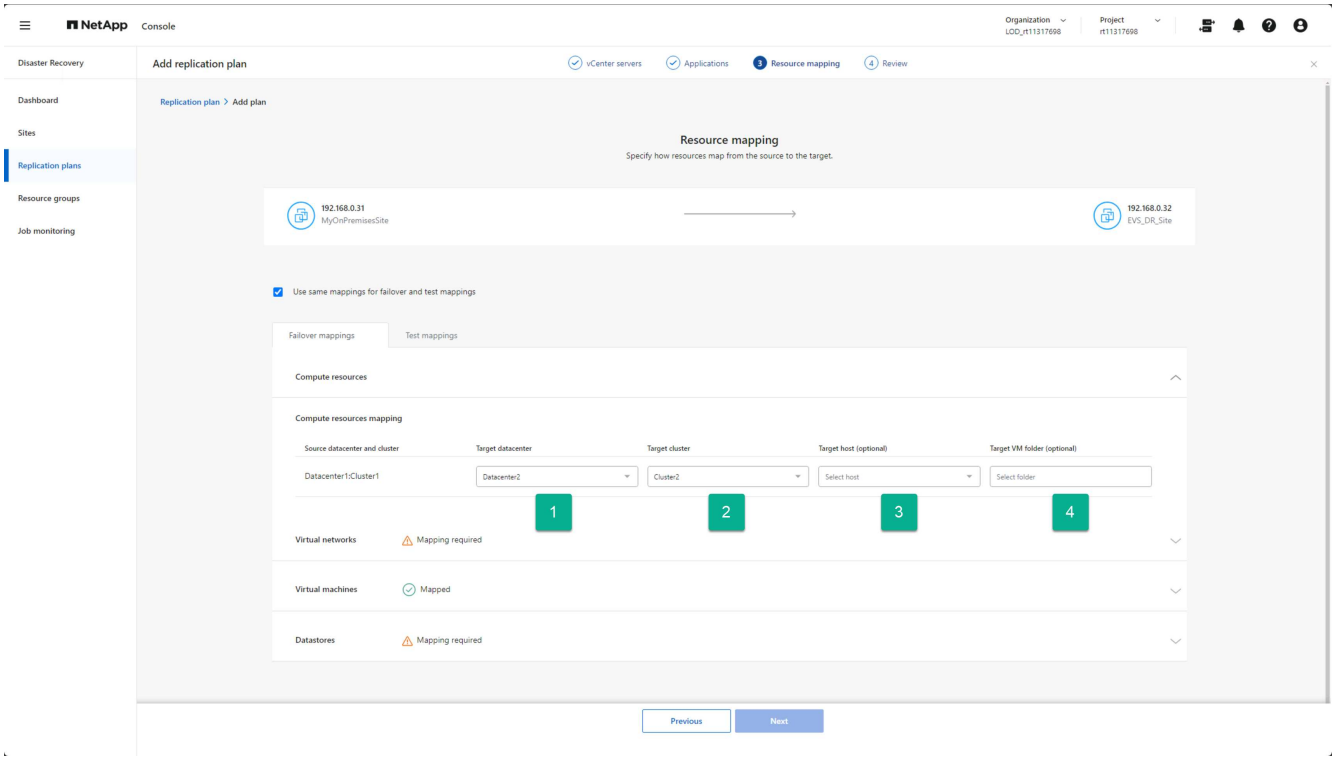
1. DR 사이트에 있는 데이터 센터 목록에서 가상 데이터 센터를 선택합니다.

2. 선택한 가상 데이터 센터 내의 클러스터 목록에서 데이터스토어와 VM을 호스팅할 클러스터를 선택합니다.
3. (선택 사항) 대상 클러스터에서 대상 호스트를 선택합니다.

   NetApp Disaster Recovery vCenter에서 클러스터에 추가된 첫 번째 호스트를 선택하므로 이 단계는 필요하지 않습니다. 그 시점에서 VM은 해당 ESXi 호스트에서 계속 실행되거나 VMware DRS는 구성된 DRS 규칙에 따라 필요에 따라 VM을 다른 ESXi 호스트로 이동합니다.

4. (선택 사항) VM 등록을 저장할 최상위 vCenter 폴더의 이름을 제공합니다.

   이는 귀하의 조직적 필요에 따른 것이며 필수 사항은 아닙니다.

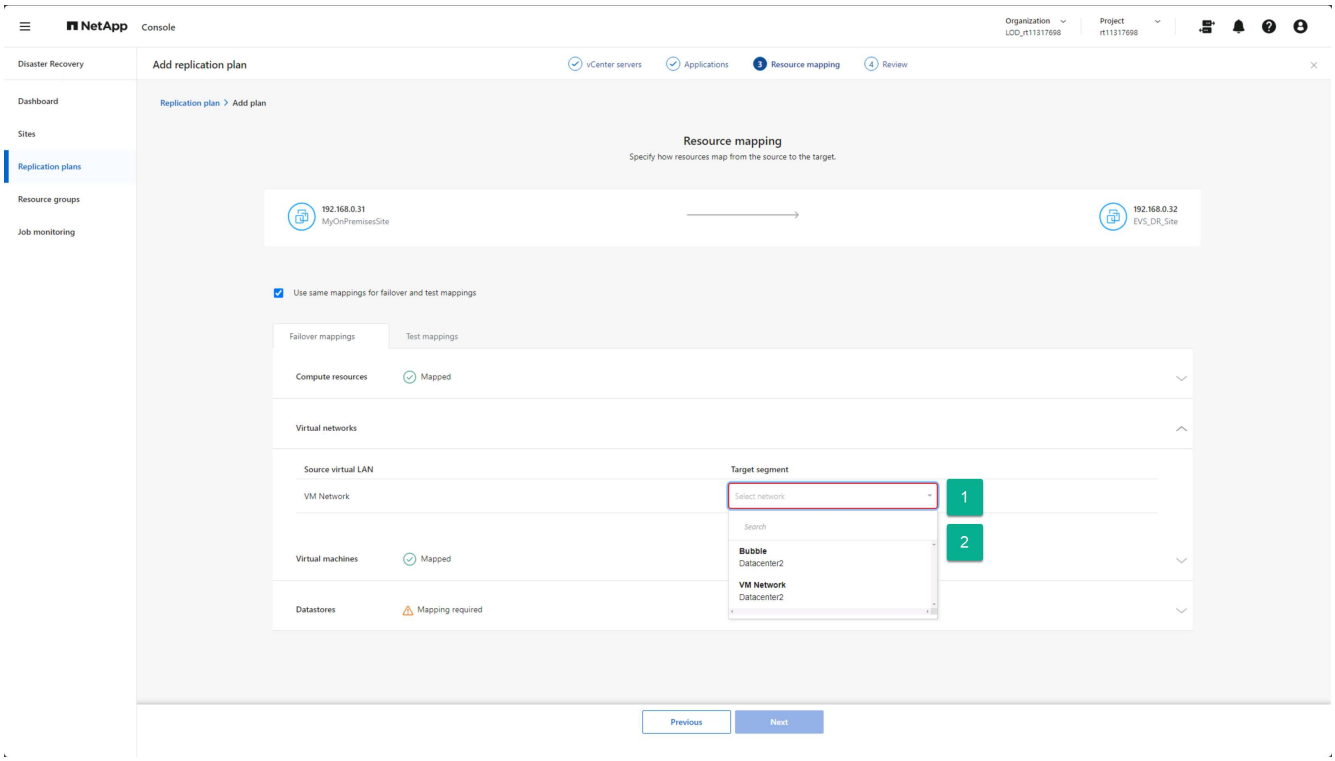


가상 네트워크 리소스 매핑

각 VM은 vCenter 네트워크 인프라 내의 가상 네트워크에 연결된 하나 이상의 가상 NIC를 가질 수 있습니다. DR 사이트에서 재시작 시 각 VM이 원하는 네트워크에 제대로 연결되었는지 확인하려면 이러한 VM을 연결할 DR 사이트 가상 네트워크를 식별합니다. 이를 위해 온프레미스 사이트의 각 가상 네트워크를 DR 사이트의 연결된 네트워크에 매핑합니다.

각 소스 가상 네트워크를 매핑할 대상 가상 네트워크를 선택하세요

1. 드롭다운 목록에서 대상 세그먼트를 선택합니다.
2. 나열된 각 소스 가상 네트워크에 대해 이전 단계를 반복합니다.



장애 조치 중 **VM** 재구성에 대한 옵션 정의

각 VM은 DR vCenter 사이트에서 올바르게 작동하려면 수정이 필요할 수 있습니다. 가상 머신 섹션에서는 필요한 변경 사항을 제공할 수 있습니다.

기본적으로 NetApp Disaster Recovery 온프레미스 소스 사이트에서 사용되는 것과 동일한 설정을 각 VM에 사용합니다. 이는 VM이 동일한 IP 주소, 가상 CPU, 가상 DRAM 구성을 사용한다고 가정합니다.

네트워크 재구성

지원되는 IP 주소 유형은 정적 및 DHCP입니다. 고정 IP 주소의 경우 다음과 같은 대상 IP 설정이 있습니다.

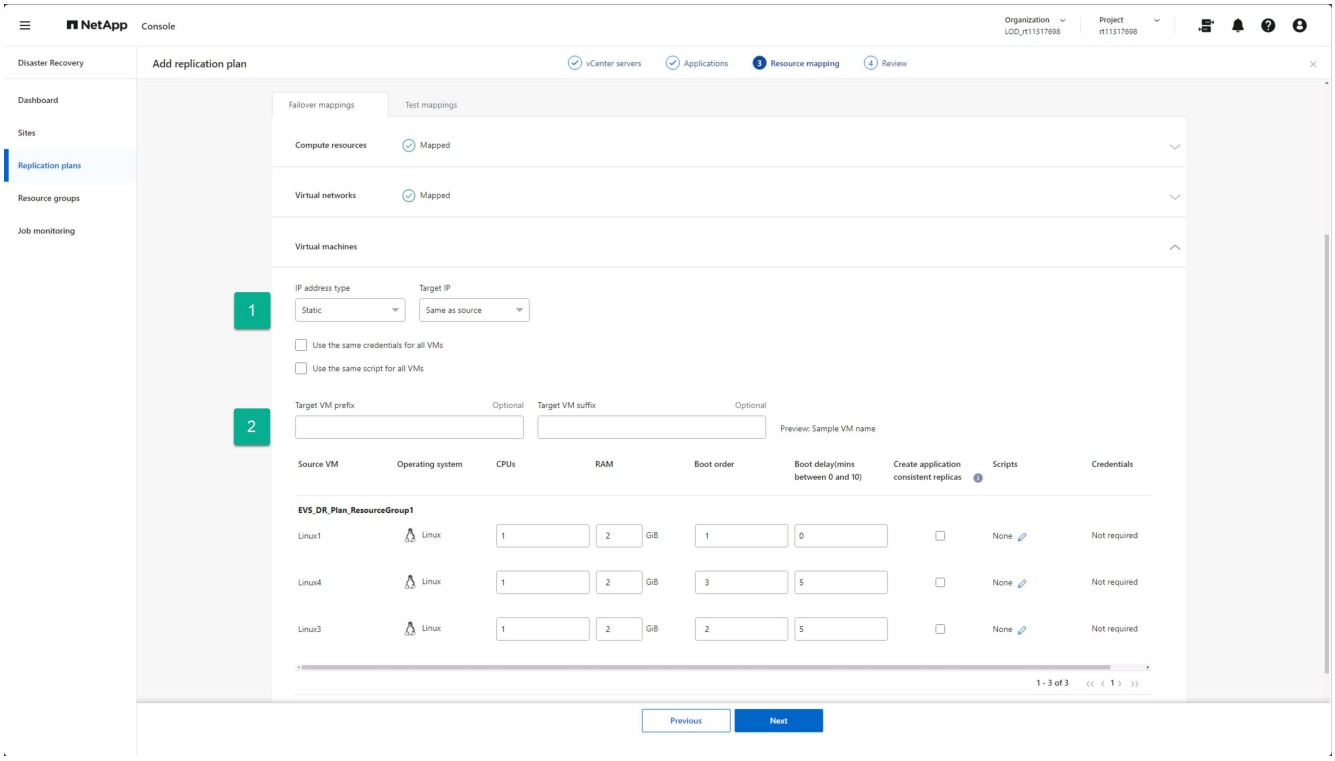
- 소스와 동일: 이름에서 알 수 있듯이, 이 서비스는 소스 사이트의 VM에서 사용된 것과 동일한 IP 주소를 대상 VM에서 사용합니다. 이렇게 하려면 이전 단계에서 매핑된 가상 네트워크를 동일한 서브넷 설정으로 구성해야 합니다.
- 소스와 다름: 서비스는 이전 섹션에서 매핑한 대상 가상 네트워크에서 사용되는 적절한 서브넷에 대해 구성해야 하는 각 VM에 대한 IP 주소 필드 세트를 제공합니다. 각 VM에 대해 IP 주소, 서브넷 마스크, DNS 및 기본 게이트웨이 값을 제공해야 합니다. 선택적으로 모든 VM에 대해 동일한 서브넷 마스크, DNS 및 게이트웨이 설정을 사용하면 모든 VM이 동일한 서브넷에 연결되는 경우 프로세스가 간소화됩니다.
- 서브넷 매핑: 이 옵션은 대상 가상 네트워크의 CIDR 구성에 따라 각 VM의 IP 주소를 재구성합니다. 이 기능을 사용하려면 사이트 페이지의 vCenter 정보에서 변경한 대로 각 vCenter의 가상 네트워크에 서비스 내에서 정의된 CIDR 설정이 있는지 확인하세요.

서브넷을 구성한 후 서브넷 매핑은 소스 및 대상 VM 구성 모두에 대해 동일한 IP 주소 단위 구성 요소를 사용하지만 제공된 CIDR 정보를 기반으로 IP 주소의 서브넷 구성 요소를 대체합니다. 이 기능을 사용하려면 소스 및 대상 가상 네트워크가 모두 동일한 IP 주소 클래스를 가져야 합니다. `/xx` CIDR의 구성 요소). 이를 통해 대상 사이트에서 모든 보호된 VM을 호스팅할 수 있는 충분한 IP 주소를 확보할 수 있습니다.

이 EVS 설정의 경우 소스 및 대상 IP 구성이 동일하며 추가 재구성이 필요하지 않다고 가정합니다.

네트워크 설정 재구성을 변경합니다.

1. 장애 조치된 VM에 사용할 IP 주소 유형을 선택합니다.
2. (선택 사항) 선택적 접두사 및 접미사 값을 제공하여 재시작된 VM에 대한 VM 이름 변경 체계를 제공합니다.

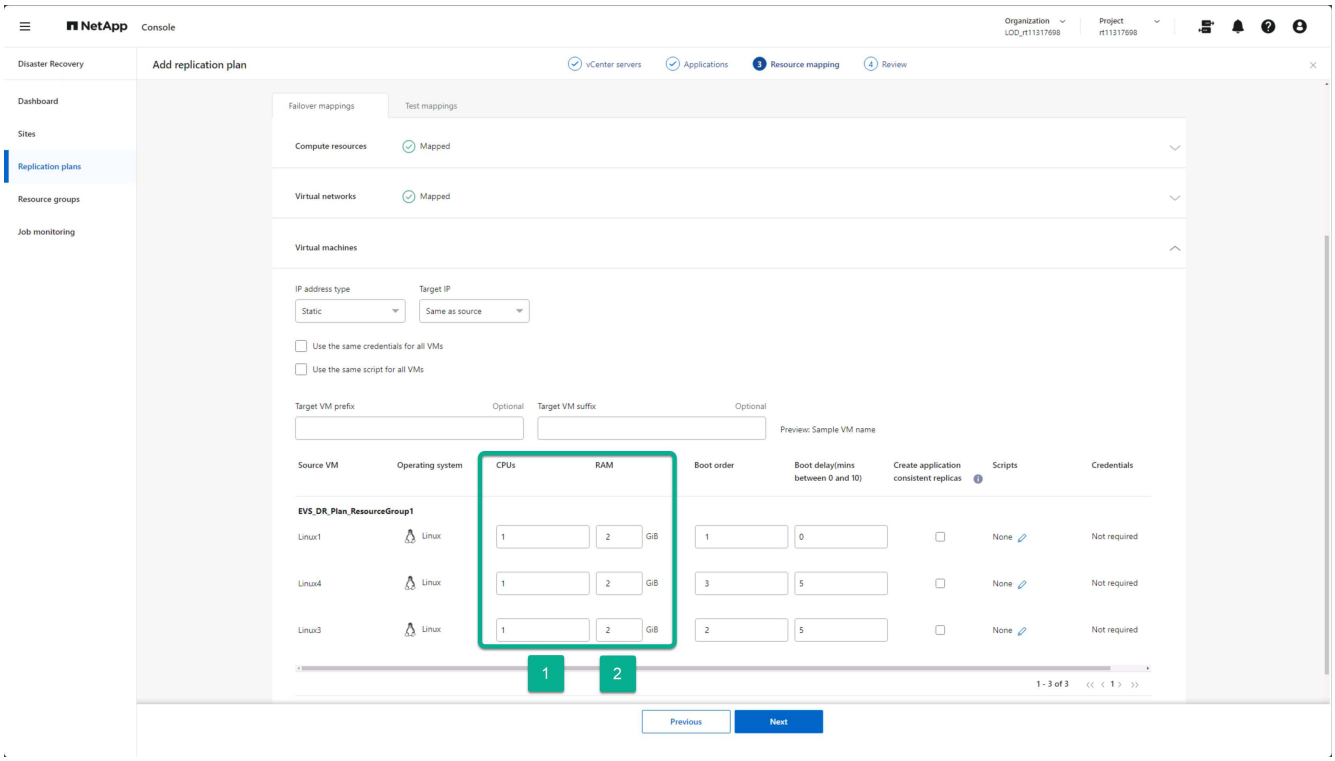


VM 컴퓨팅 리소스 재구성

VM 컴퓨팅 리소스를 재구성하는 데에는 여러 가지 옵션이 있습니다. NetApp Disaster Recovery 가상 CPU 수, 가상 DRAM 양, VM 이름 변경을 지원합니다.

VM 구성 변경 사항을 지정합니다.

1. (선택 사항) 각 VM이 사용해야 하는 가상 CPU 수를 수정합니다. DR vCenter 클러스터 호스트에 소스 vCenter 클러스터만큼 CPU 코어가 많지 않은 경우 이 작업이 필요할 수 있습니다.
2. (선택 사항) 각 VM이 사용해야 하는 가상 DRAM의 양을 수정합니다. DR vCenter 클러스터 호스트에 소스 vCenter 클러스터 호스트만큼 많은 물리적 DRAM이 없는 경우 이 작업이 필요할 수 있습니다.

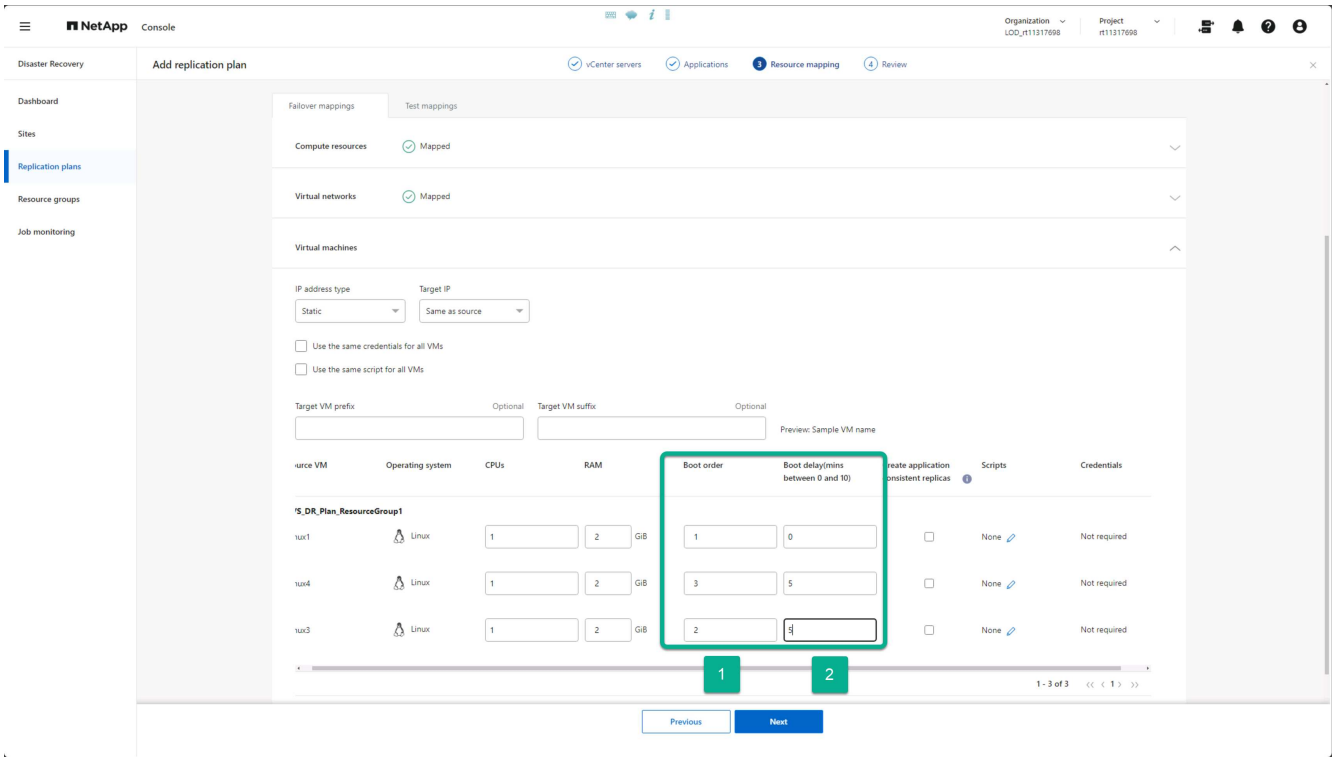


부팅 순서

NetApp Disaster Recovery 부팅 순서 필드를 기반으로 VM의 순서화된 재시작을 지원합니다. 부팅 순서 필드는 각 리소스 그룹의 VM이 시작되는 방식을 나타냅니다. 부팅 순서 필드에 동일한 값이 있는 VM은 병렬로 부팅됩니다.

부팅 순서 설정 수정

1. (선택 사항) VM을 다시 시작할 순서를 수정합니다. 이 필드는 숫자 값을 사용합니다. NetApp Disaster Recovery 동일한 숫자 값을 갖는 VM을 병렬로 다시 시작하려고 시도합니다.
2. (선택 사항) VM을 다시 시작할 때마다 사용할 지연 시간을 제공합니다. 이 VM의 재시작이 완료된 후, 다음으로 높은 부팅 순서 번호를 가진 VM이 시작되기 전에 시간이 주입됩니다. 이 숫자는 분 단위입니다.



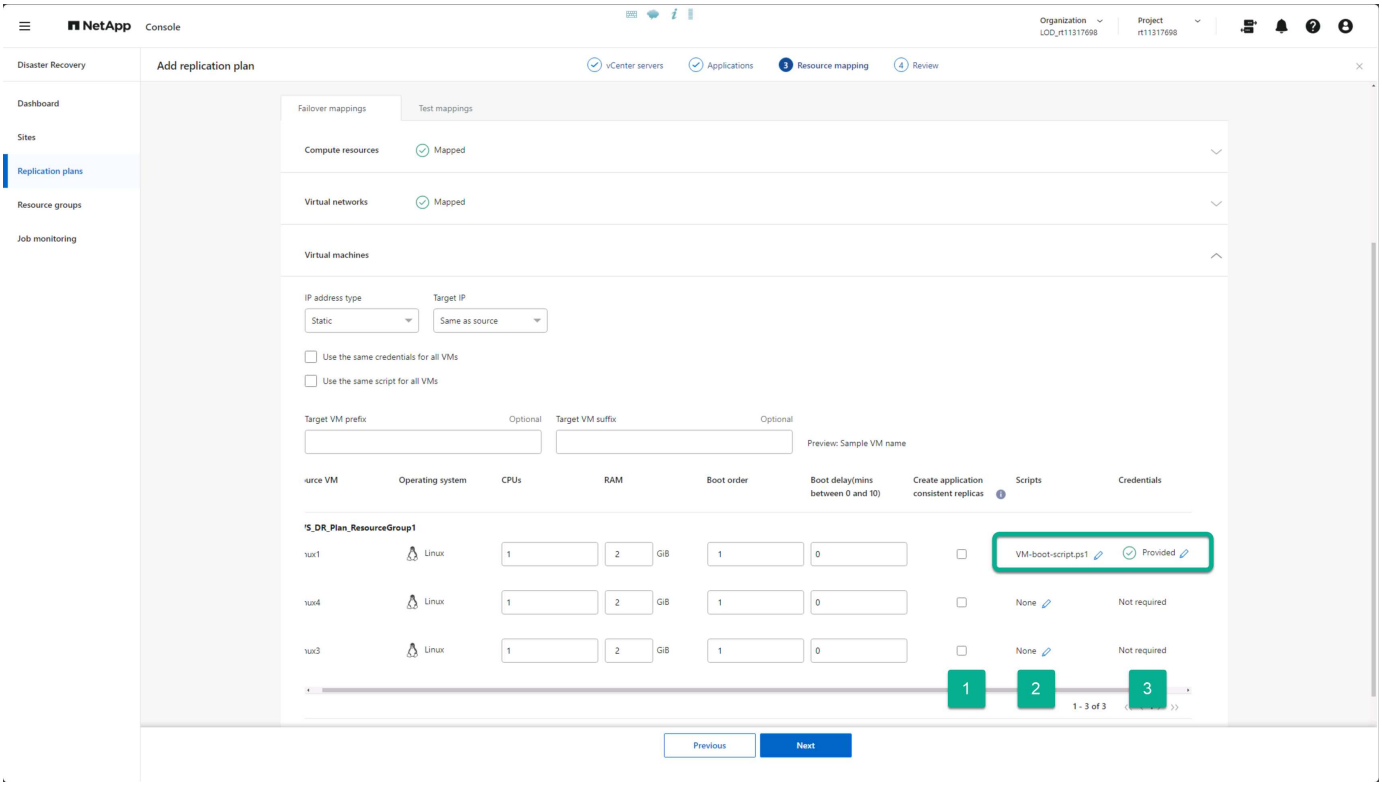
사용자 정의 게스트 **OS** 작업

NetApp Disaster Recovery 각 VM에 대해 일부 게스트 OS 작업을 수행하는 것을 지원합니다.

- NetApp Disaster Recovery Oracle 데이터베이스와 Microsoft SQL Server 데이터베이스를 실행하는 VM의 애플리케이션 일관성 백업을 수행할 수 있습니다.
- NetApp Disaster Recovery 각 VM의 게스트 OS에 적합한 사용자 정의 스크립트를 실행할 수 있습니다. 이러한 스크립트를 실행하려면 스크립트에 나열된 작업을 실행할 수 있는 충분한 권한을 가진 게스트 OS에서 허용하는 사용자 자격 증명이 필요합니다.

각 **VM**의 사용자 정의 게스트 **OS** 작업 수정

1. (선택 사항) VM이 Oracle 또는 SQL Server 데이터베이스를 호스팅하는 경우 애플리케이션 일관성 복제본 만들기 확인란을 선택합니다.
2. (선택 사항) 시작 프로세스의 일부로 게스트 OS 내에서 사용자 지정 작업을 수행하려면 모든 VM에 대한 스크립트를 업로드합니다. 모든 VM에서 단일 스크립트를 실행하려면 강조 표시된 확인란을 사용하고 필드를 완성하세요.
3. 특정 구성을 변경하려면 작업을 수행할 수 있는 적절한 권한이 있는 사용자 자격 증명이 필요합니다. 다음의 경우 자격 증명을 제공하세요.
    - 스크립트는 게스트 OS에 의해 VM 내에서 실행됩니다.
    - 애플리케이션과 일관된 스냅샷을 수행해야 합니다.



지도 데이터 저장소

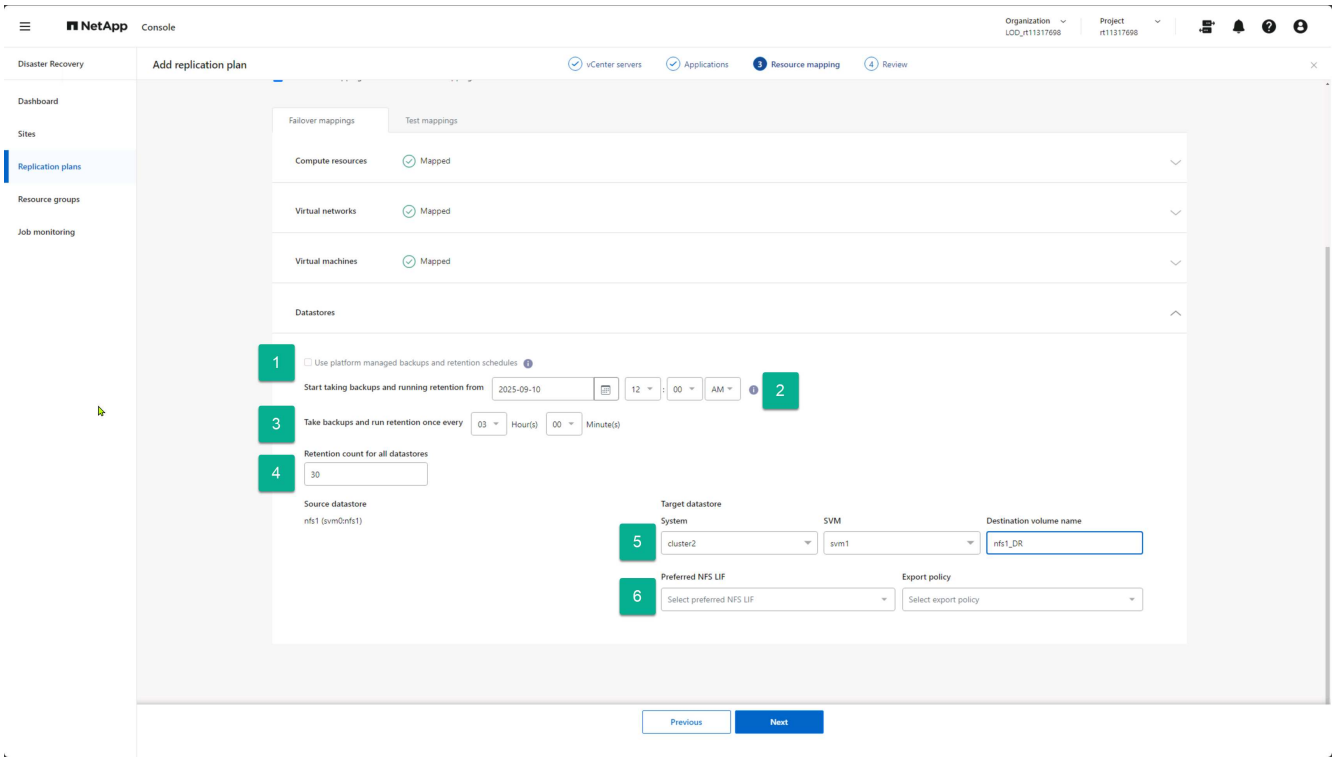
복제 계획을 만드는 마지막 단계는 ONTAP 데이터 저장소를 어떻게 보호해야 하는지 식별하는 것입니다. 이러한 설정은 복제 계획 복구 지점 목표(RPO), 유지해야 하는 백업 수, 각 vCenter 데이터스토어의 호스팅 ONTAP 볼륨을 복제할 위치를 정의합니다.

기본적으로 NetApp Disaster Recovery 자체 스냅샷 복제 일정을 관리합니다. 그러나 선택적으로 데이터 저장소 보호를 위해 기존 SnapMirror 복제 정책 일정을 사용하도록 지정할 수 있습니다.

또한, 어떤 데이터 LIF(논리적 인터페이스)와 내보내기 정책을 사용할지 선택적으로 사용자 지정할 수 있습니다. 이러한 설정을 제공하지 않으면 NetApp Disaster Recovery 해당 프로토콜(NFS, iSCSI 또는 FC)과 연결된 모든 데이터 LIF를 사용하고 NFS 볼륨에 대한 기본 내보내기 정책을 사용합니다.

데이터 저장소(볼륨) 매핑을 구성하려면

1. (선택 사항) 기존 ONTAP SnapMirror 복제 일정을 사용할지 아니면 NetApp Disaster Recovery VM 보호를 관리할지(기본값) 결정합니다.
2. 서비스가 백업을 시작해야 하는 시작점을 제공합니다.
3. 서비스가 백업을 수행하고 이를 DR 대상 Amazon FSx for NetApp ONTAP 클러스터에 복제해야 하는 빈도를 지정합니다.
4. 얼마나 많은 과거 백업을 보관해야 하는지 지정합니다. 이 서비스는 소스 및 대상 스토리지 클러스터에서 동일한 수의 백업을 유지 관리합니다.
5. (선택 사항) 각 볼륨에 대한 기본 논리 인터페이스(데이터 LIF)를 선택합니다. 아무것도 선택하지 않으면 볼륨 액세스 프로토콜을 지원하는 대상 SVM의 모든 데이터 LIF가 구성됩니다.
6. (선택 사항) NFS 볼륨에 대한 내보내기 정책을 선택합니다. 선택하지 않으면 기본 내보내기 정책이 사용됩니다.



계속하기"복제 계획 마법사 생성 4단계" .

복제 계획 만들기: **4**단계 **- NetApp Disaster Recovery** 설정 확인

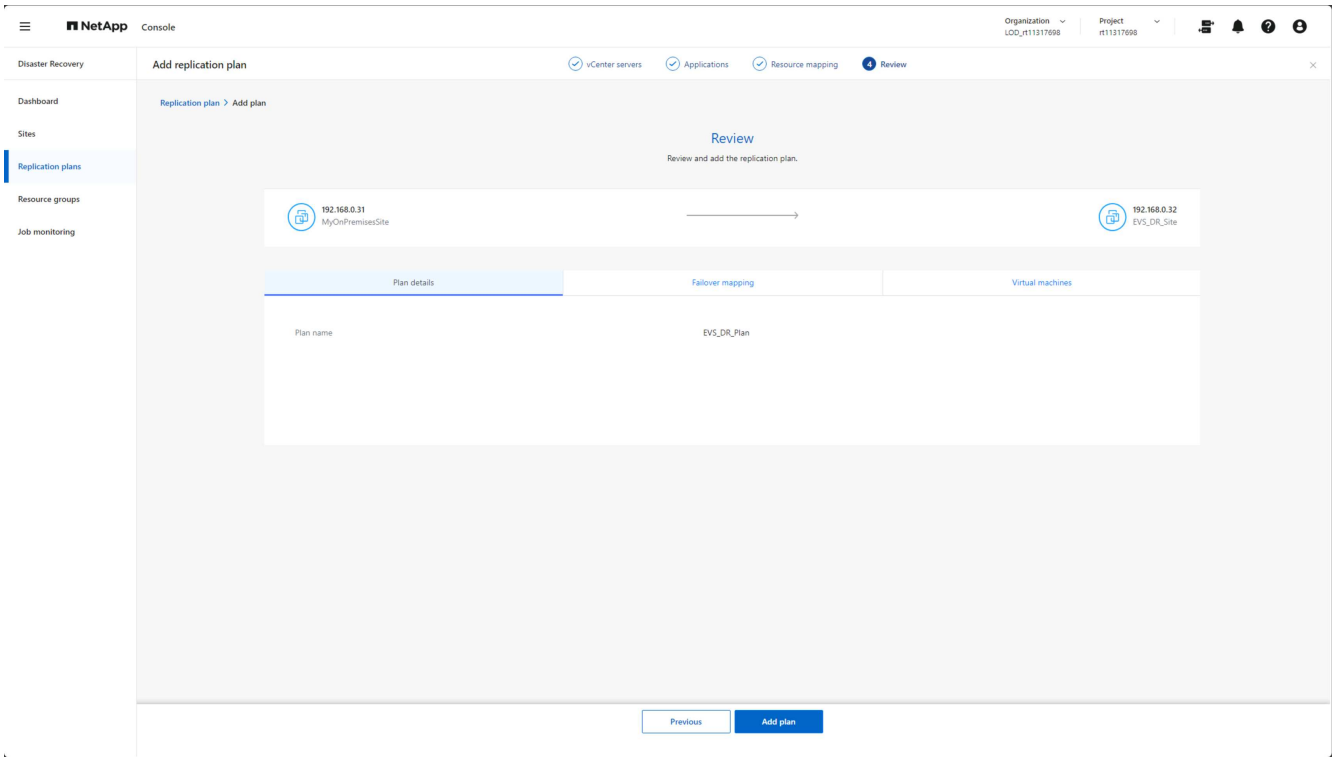
NetApp Disaster Recovery 에 복제 계획 정보를 추가한 후 입력한 정보가 올바른지 확인하세요.

단계

1. 복제 계획을 활성화하기 전에 설정을 검토하려면 *저장*을 선택하세요.

   각 탭을 선택하여 설정을 검토하고 연필 아이콘을 선택하여 모든 탭에서 변경 사항을 적용할 수 있습니다.

   복제 계획 설정
   검토



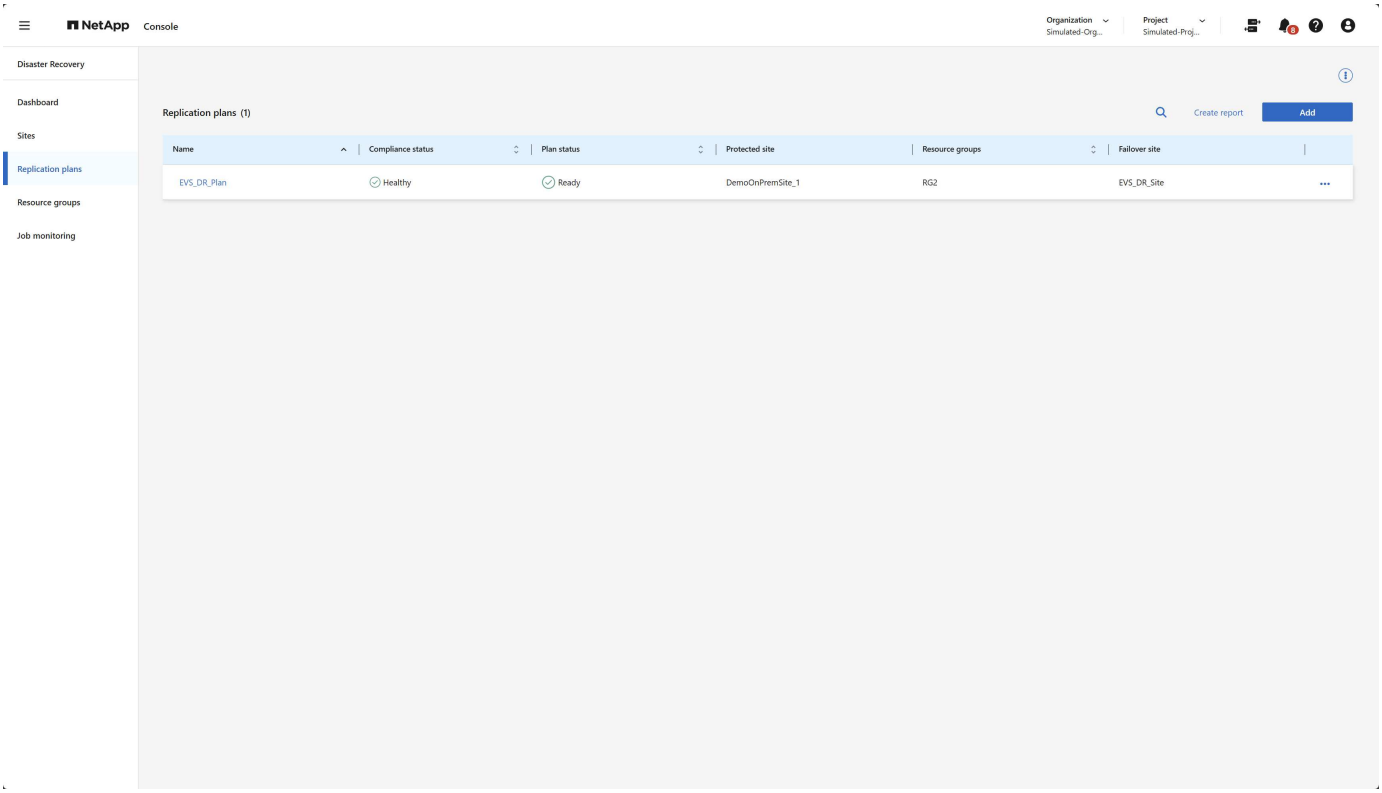
2. 모든 설정이 올바른지 확인한 후 화면 하단에서 *플랜 추가*를 선택하세요.

계속하기"복제 계획 확인" .

NetApp Disaster Recovery 에서 모든 것이 제대로 작동하는지 확인하세요**.**

NetApp Disaster Recovery 에 복제 계획을 추가한 후에는 복제 계획 페이지로 돌아가서 복제 계획과 해당 상태를 볼 수 있습니다. 복제 계획이 정상 상태인지 확인해야 합니다. 그렇지 않은 경우 복제 계획의 상태를 확인하고 계속 진행하기 전에 문제를 해결해야 합니다.

그림: 복제 계획
페이지



NetApp Disaster Recovery 모든 구성 요소(ONTAP 클러스터, vCenter 클러스터 및 VM)에 액세스할 수 있고 서비스가 VM을 보호할 수 있는 적절한 상태인지 확인하기 위해 일련의 테스트를 수행합니다. 이를 규정 준수 점검이라고 하며, 정기적으로 실행됩니다.

복제 계획 페이지에서 다음 정보를 볼 수 있습니다.

- 마지막 준수 검사 상태
- 복제 계획의 복제 상태
- 보호된 (소스) 사이트의 이름
- 복제 계획으로 보호되는 리소스 그룹 목록
- 장애 조치(대상) 사이트의 이름

NetApp Disaster Recovery 사용하여 복제 계획 작업 수행

Amazon EVS 및 Amazon FSx for NetApp ONTAP 과 함께 NetApp Disaster Recovery 사용하면 장애 조치, 테스트 장애 조치, 리소스 새로 고침, 마이그레이션, 지금 스냅샷 만들기, 복제 계획 비활성화/활성화, 이전 스냅샷 정리, 스냅샷 조정, 복제 계획 삭제 및 일정 편집 등의 작업을 수행할 수 있습니다.

장애 조치

가장 먼저 수행해야 할 작업은 절대로 일어나지 않기를 바라는 작업입니다. 즉, 온프레미스 운영 사이트에서 심각한 장애가 발생할 경우 DR(대상) 데이터 센터로 장애 조치를 취하는 것입니다.

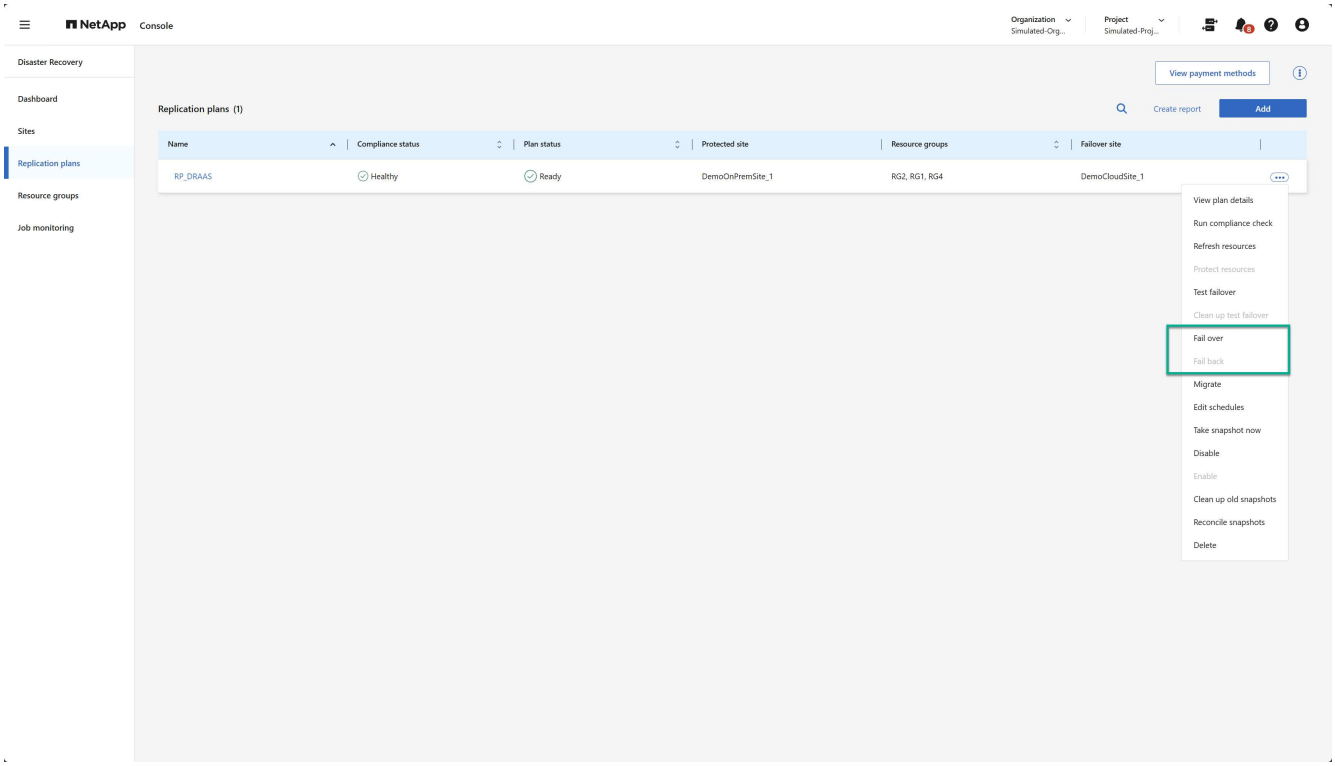
장애 조치는 수동으로 시작되는 프로세스입니다.

장애 조치 작업에 액세스하는 단계

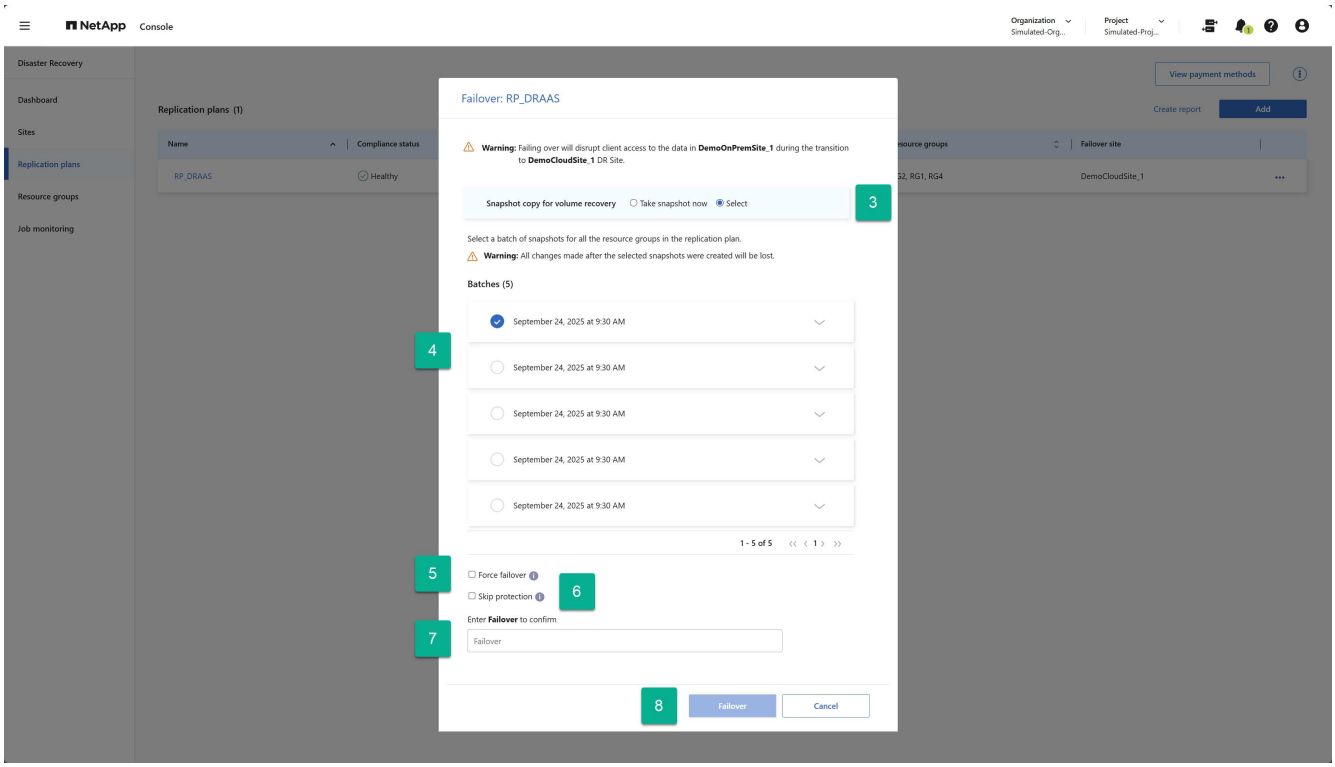
1. NetApp Console 왼쪽 탐색 모음에서 보호 > *재해 복구*를 선택합니다.
2. NetApp Disaster Recovery 메뉴에서 *복제 계획*을 선택합니다.

장애 조치를 수행하는 단계

1. 복제 계획 페이지에서 복제 계획의 작업 옵션을 선택하세요. ••• .
2. *장애 조치*를 선택합니다.



3. 프로덕션(보호) 사이트에 접근할 수 없는 경우 이전에 만든 스냅샷을 복구 이미지로 선택하세요. 이렇게 하려면 *선택*을 선택하세요.
4. 복구에 사용할 백업을 선택하세요.
5. (선택 사항) 복제 계획의 상태에 관계없이 NetApp Disaster Recovery 장애 조치 프로세스를 강제로 실행할지 여부를 선택합니다. 이것은 최후의 수단으로만 사용해야 합니다.
6. (선택 사항) 프로덕션 사이트가 복구된 후 NetApp Disaster Recovery 자동으로 역방향 보호 관계를 생성할지 여부를 선택합니다.
7. 계속 진행하려면 "Failover"라는 단어를 입력하세요.
8. *장애 조치*를 선택합니다.



테스트 장애 조치

테스트 장애 조치는 두 가지 차이점을 제외하면 장애 조치와 비슷합니다.

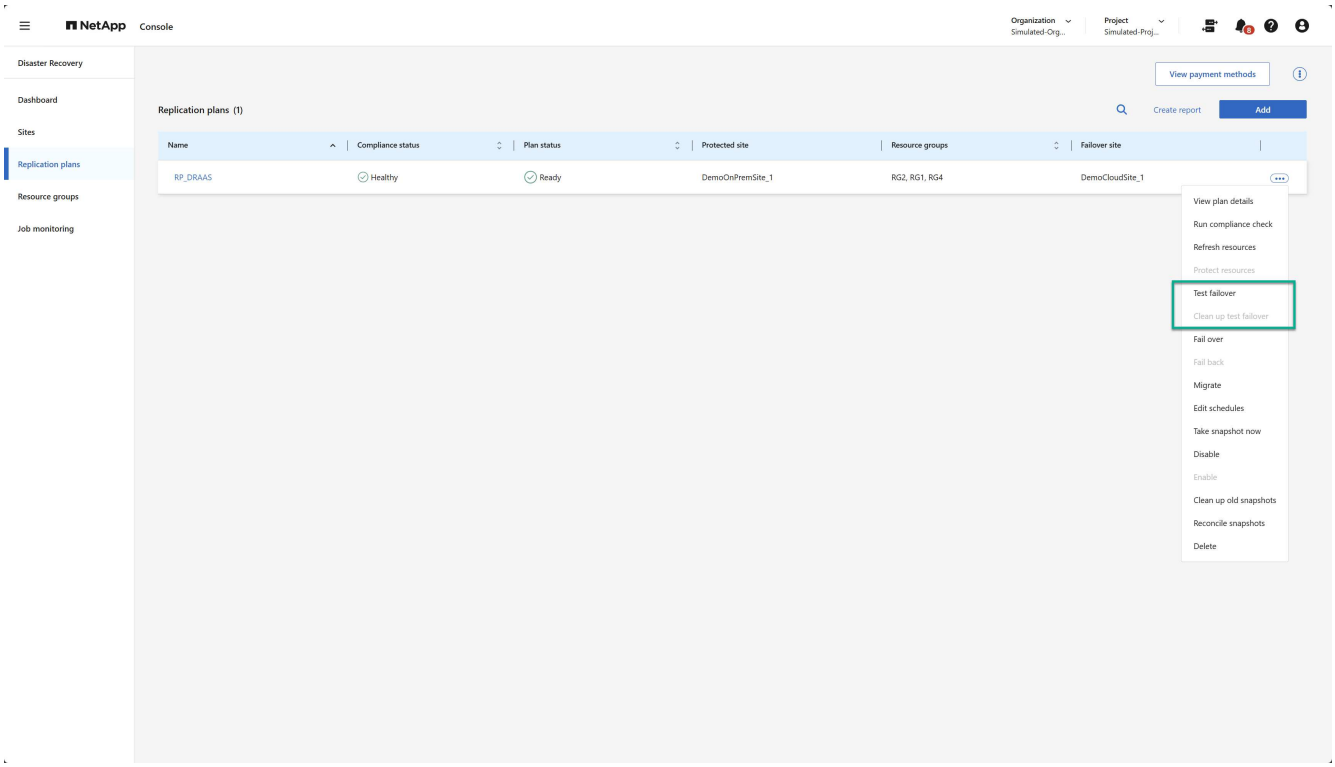
- 프로덕션 사이트는 여전히 활성화되어 있으며 모든 VM은 예상대로 작동하고 있습니다.
- 프로덕션 VM에 대한 NetApp Disaster Recovery 보호가 계속됩니다.

이는 대상 사이트에서 기본 ONTAP FlexClone 볼륨을 사용하여 수행됩니다. 테스트 장애 조치에 대해 자세히 알아보려면 다음을 참조하세요."원격 사이트로 애플리케이션 장애 조치 | NetApp 문서" .

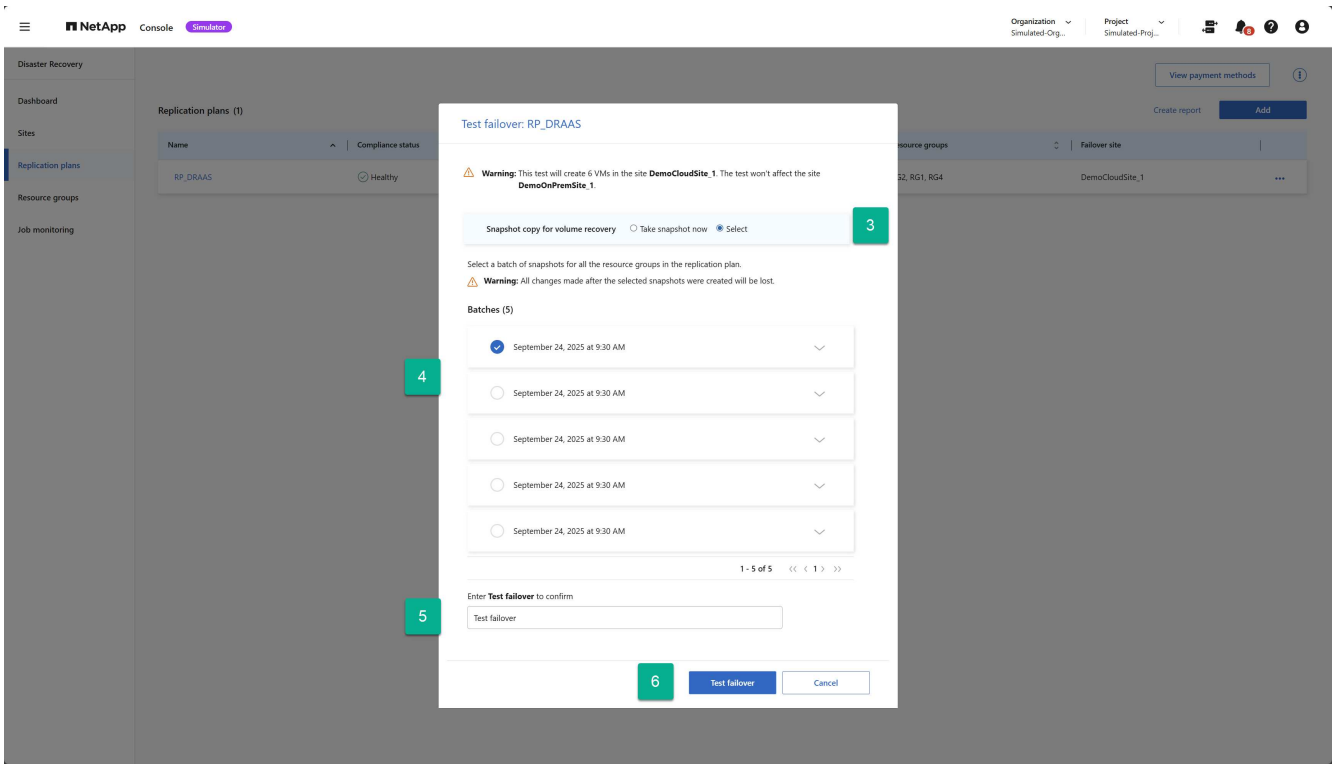
테스트 장애 조치를 실행하는 단계는 실제 장애 조치를 실행하는 데 사용되는 단계와 동일하지만 복제 계획의 상황에 맞는 메뉴에서 테스트 장애 조치 작업을 사용한다는 점이 다릅니다.

단계

1. 복제 계획의 작업 옵션을 선택하세요 ••• .
2. 메뉴에서 *테스트 장애 조치*를 선택합니다.



3. 프로덕션 환경의 최신 상태를 가져올지(지금 스냅샷 찍기) 아니면 이전에 만든 복제 계획 백업을 사용할지(선택) 결정
4. 이전에 생성한 백업을 선택한 경우 복구에 사용할 백업을 선택하세요.
5. 계속 진행하려면 "테스트 장애 조치"라는 단어를 입력하세요.
6. *테스트 장애 조치*를 선택합니다.

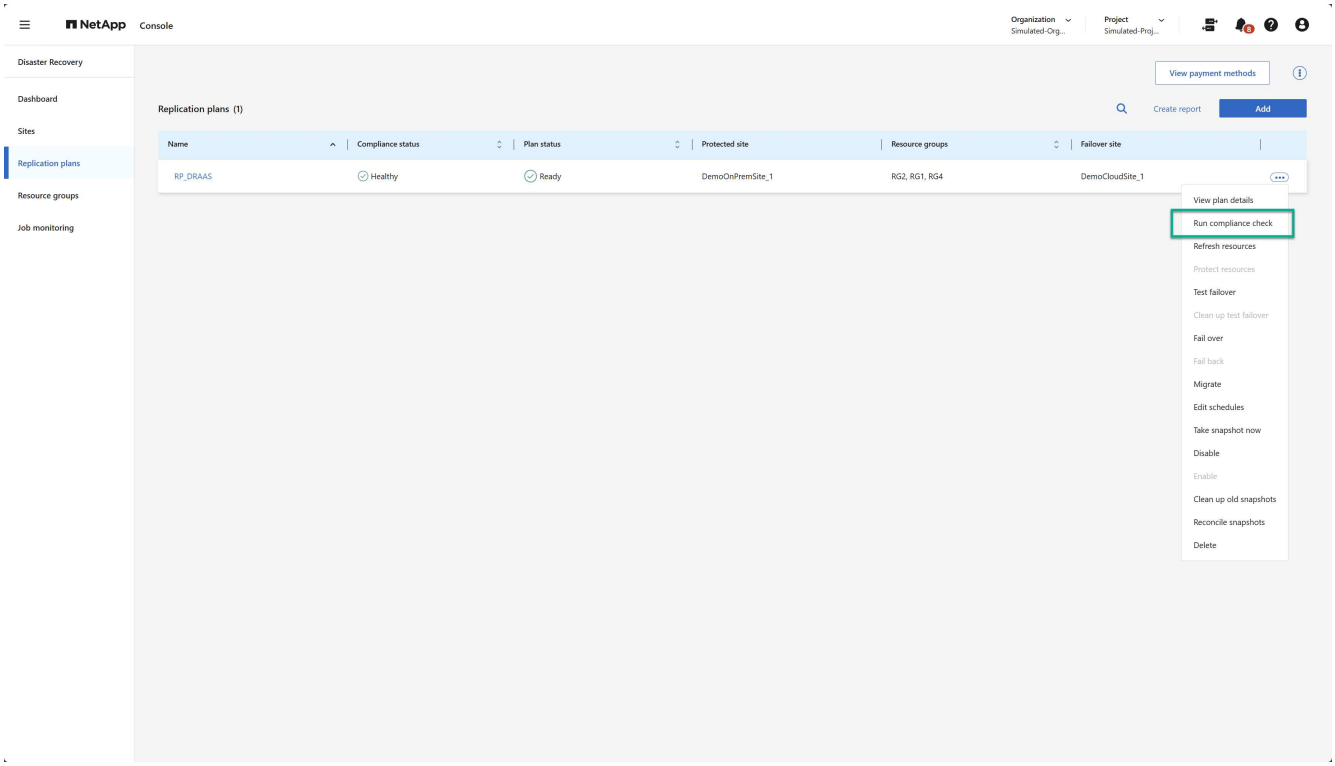


규정 준수 확인 실행

기본적으로 규정 준수 검사는 3시간마다 실행됩니다. 언제든지 수동으로 규정 준수 검사를 실행하고 싶을 수도 있습니다.

단계

1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 복제 계획의 작업 메뉴에서 규정 준수 검사 실행 옵션을 선택하세요.



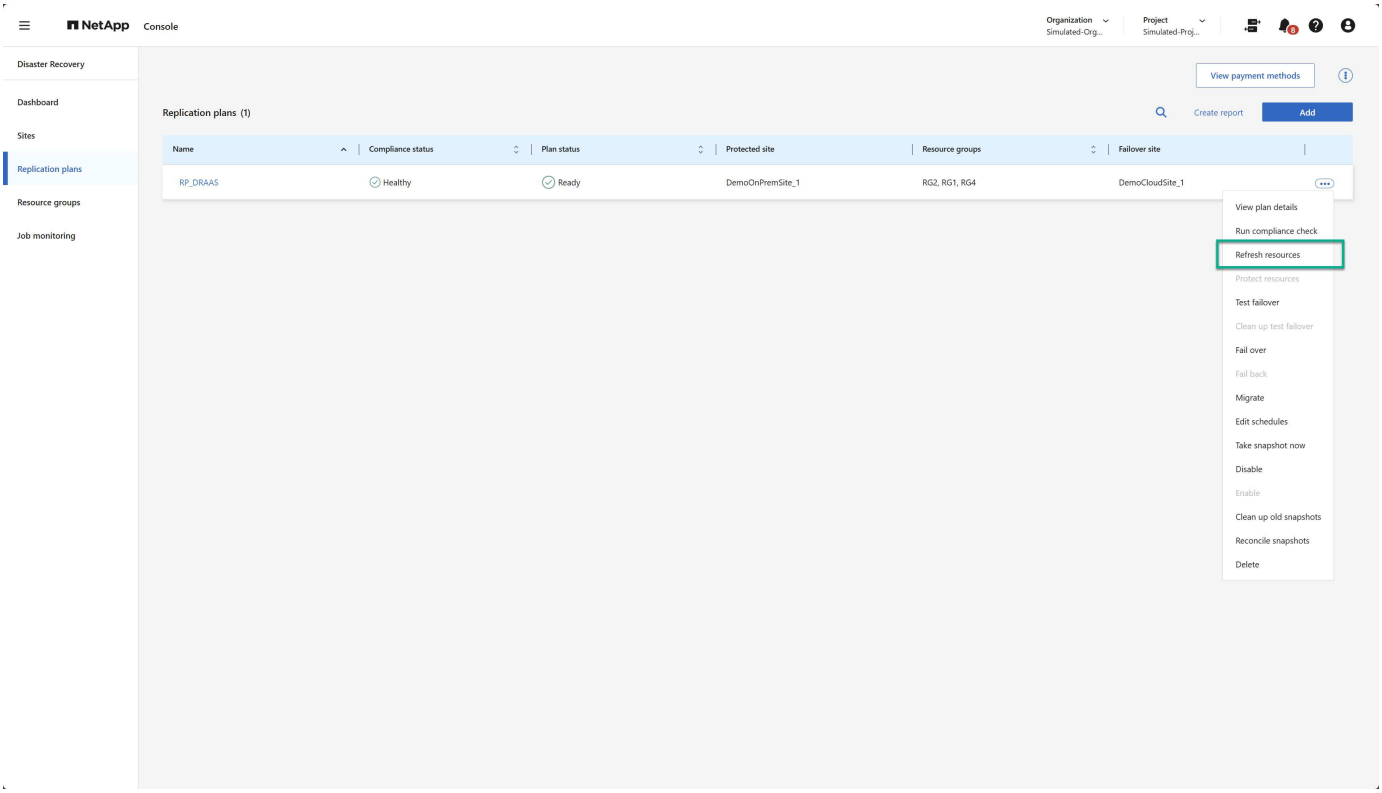
3. NetApp Disaster Recovery 규정 준수 검사를 자동으로 실행하는 빈도를 변경하려면 복제 계획의 작업 메뉴에서 일정 편집 옵션을 선택하세요.

리소스 새로 고침

VM 추가 또는 삭제, 데이터 저장소 추가 또는 삭제, 데이터 저장소 간 VM 이동 등 가상 인프라를 변경할 때마다 NetApp Disaster Recovery 서비스에서 영향을 받는 vCenter 클러스터를 새로 고쳐야 합니다. 이 서비스는 기본적으로 24시간마다 자동으로 이 작업을 수행하지만, 수동으로 새로 고침하면 최신 가상 인프라 정보를 사용할 수 있고 DR 보호에 반영됩니다.

새로 고침이 필요한 경우는 두 가지가 있습니다.

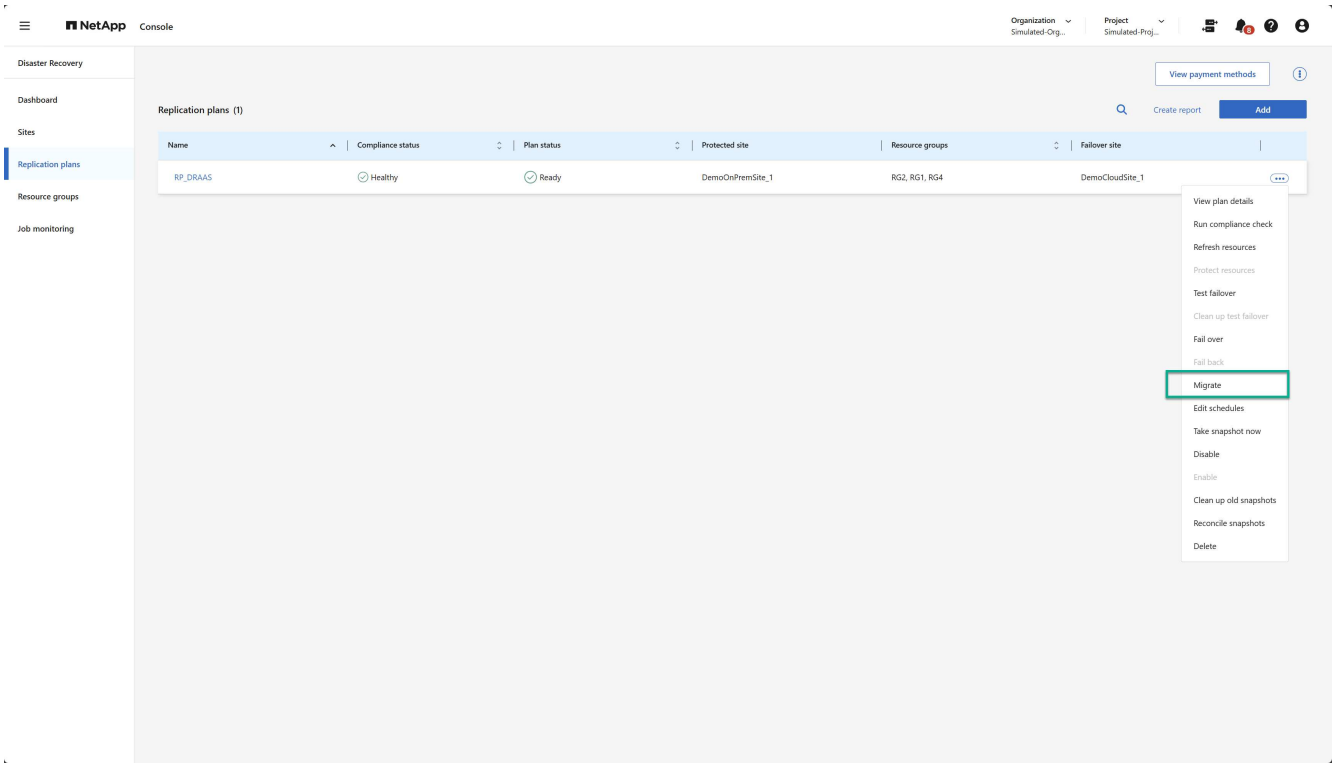
- vCenter 새로 고침: vCenter 클러스터에서 VM이 추가되거나 삭제되거나 이동될 때마다 vCenter 새로 고침을 수행합니다.
- 복제 계획 새로 고침: 동일한 소스 vCenter 클러스터의 데이터 저장소 간에 VM이 이동될 때마다 복제 계획 새로 고침을 수행합니다.



이주하다

NetApp Disaster Recovery 주로 재해 복구 사용 사례에 사용되지만, 소스 사이트에서 대상 사이트로 VM 세트를 한 번만 이동할 수도 있습니다. 이는 클라우드 프로젝트로의 조직적인 마이그레이션을 위한 것일 수도 있고, 악천후, 정치적 갈등 또는 기타 잠재적인 일시적 재앙과 같은 재해를 피하기 위해 사용될 수도 있습니다.

1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 복제 계획의 VM을 대상 Amazon EVS 클러스터로 이동하려면 복제 계획의 작업 메뉴에서 *마이그레이션*을 선택합니다.

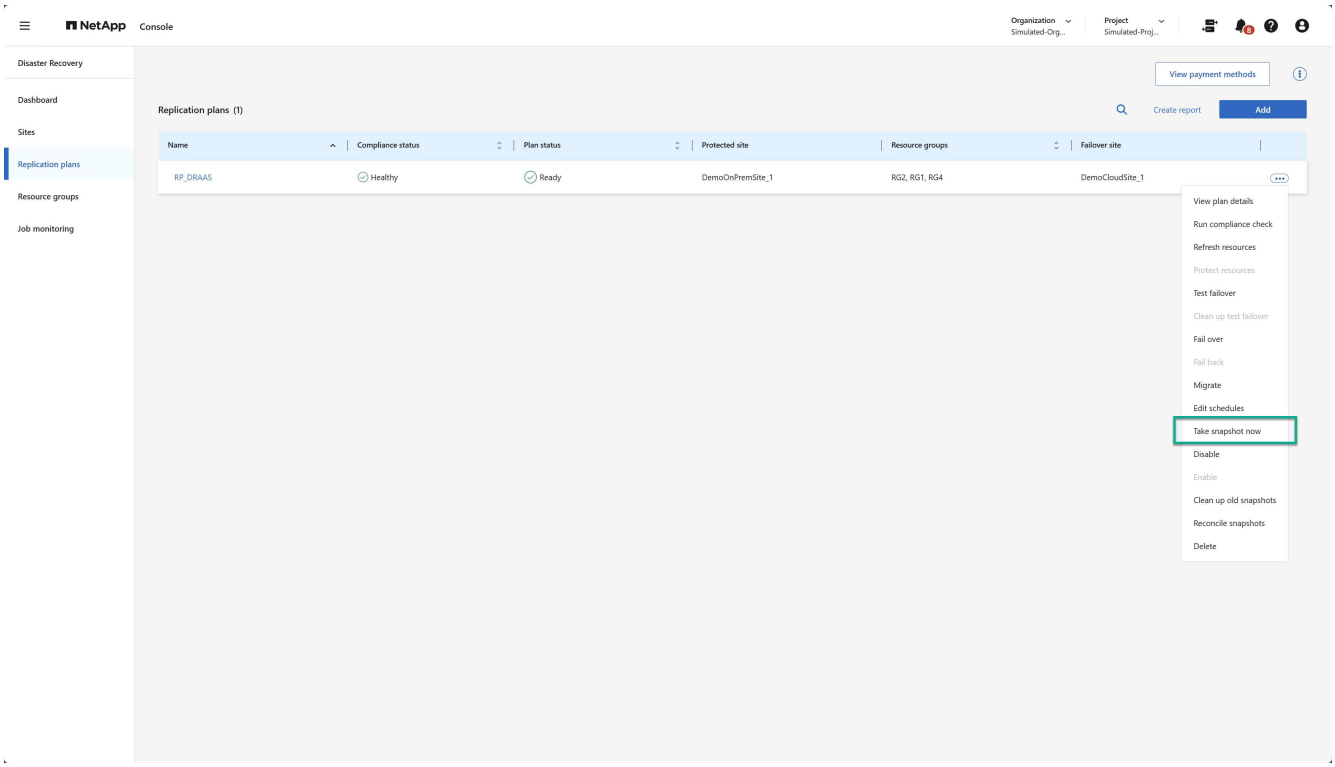


3. 마이그레이션 대화 상자에 정보를 입력합니다.

지금 스냅샷을 찍어보세요

언제든지 복제 계획의 즉각적인 스냅샷을 찍을 수 있습니다. 이 스냅샷은 복제 계획의 스냅샷 보존 횟수에 의해 설정된 NetApp Disaster Recovery 고려 사항에 포함됩니다.

1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 복제 계획 리소스의 즉각적인 스냅샷을 찍으려면 복제 계획의 작업 메뉴에서 *지금 스냅샷 찍기*를 선택하세요.

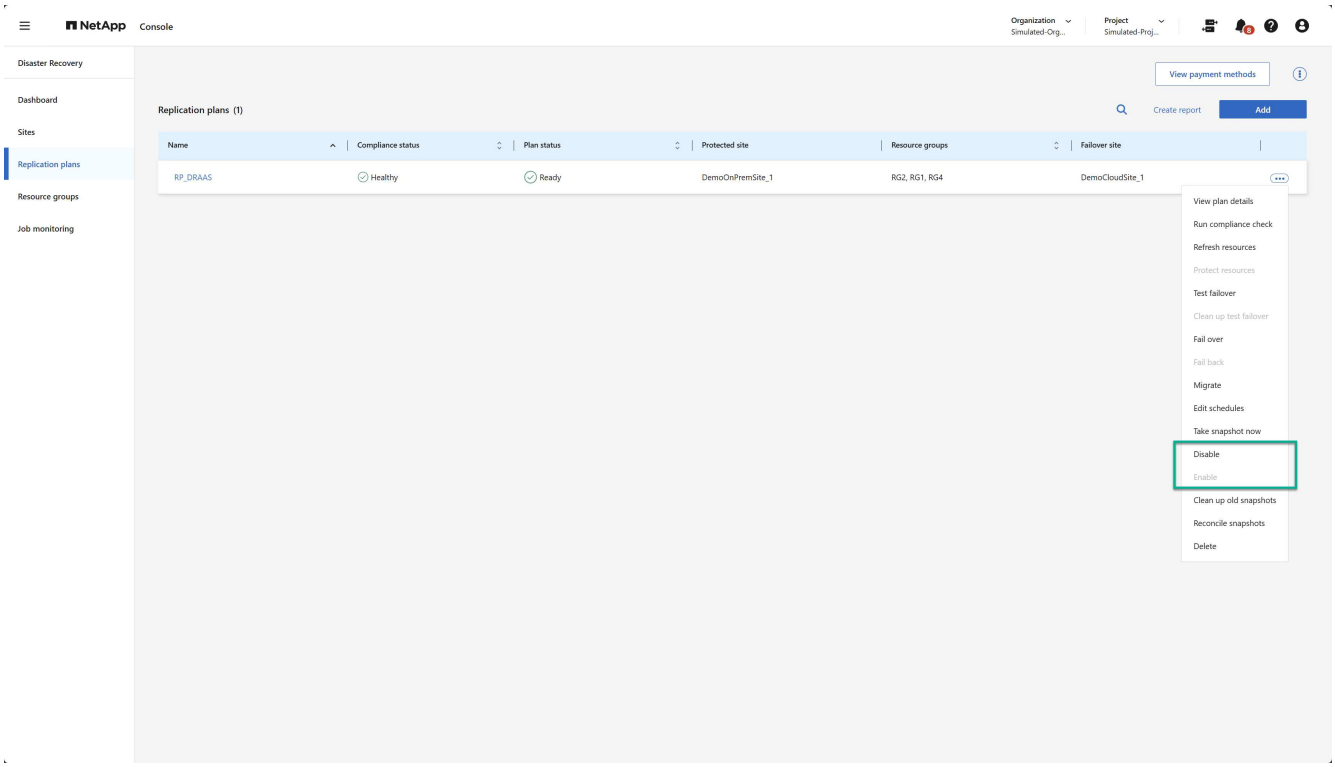


복제 계획 비활성화 또는 활성화

복제 프로세스에 영향을 줄 수 있는 작업이나 유지 관리를 수행하기 위해 복제 계획을 일시적으로 중지해야 할 수도 있습니다. 이 서비스는 복제를 중지하고 시작하는 방법을 제공합니다.

1. 복제를 일시적으로 중지하려면 복제 계획의 작업 메뉴에서 *비활성화*를 선택합니다.
2. 복제를 다시 시작하려면 복제 계획의 작업 메뉴에서 *활성화*를 선택합니다.

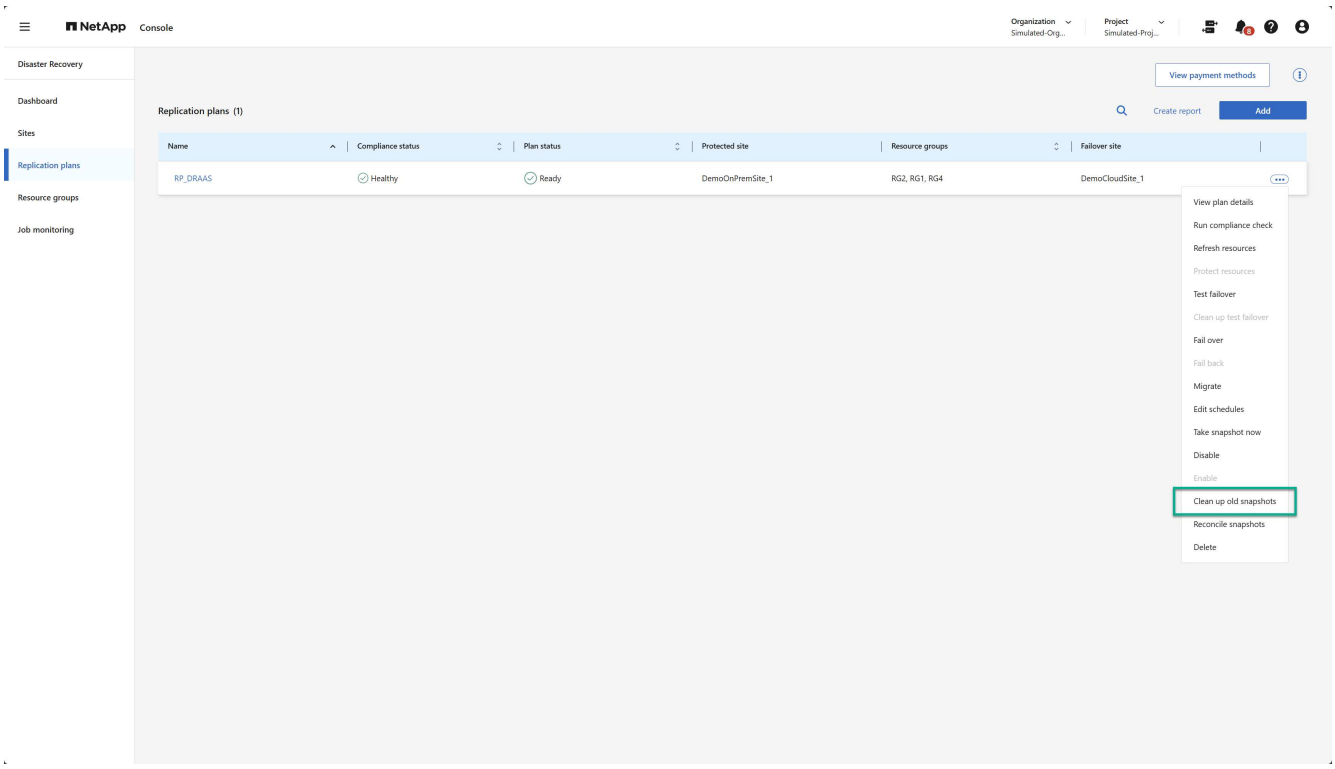
   복제 계획이 활성화되면 활성화 명령이 회색으로 표시됩니다. 복제 계획이 비활성화되면 비활성화 명령은 회색으로 표시됩니다.



오래된 스냅샷 정리

소스 및 대상 사이트에 보관된 이전 스냅샷을 정리하는 것이 좋습니다. 복제 계획의 스냅샷 보존 횟수가 변경되면 이런 일이 발생할 수 있습니다.

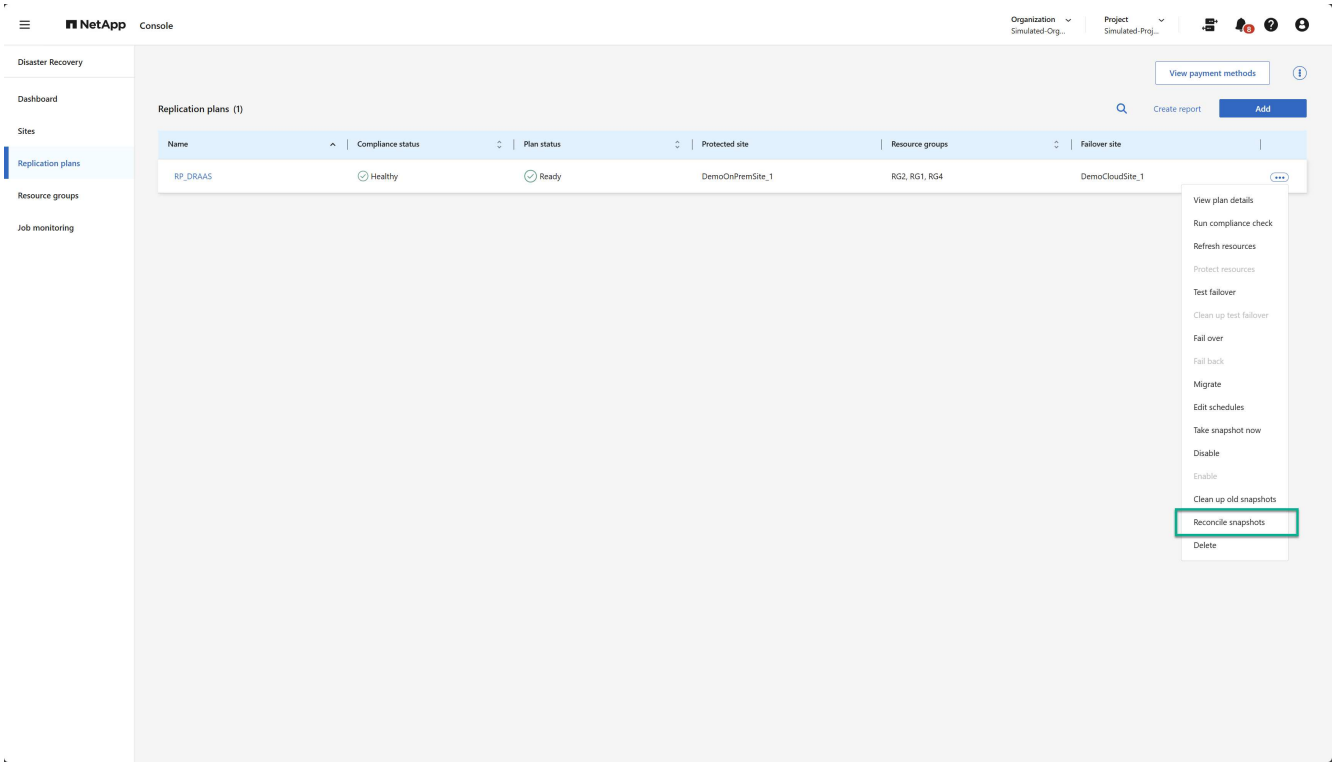
1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 이러한 이전 스냅샷을 수동으로 제거하려면 복제 계획의 작업 메뉴에서 *이전 스냅샷 정리*를 선택합니다.



스냅샷 조정

이 서비스는 ONTAP 볼륨 스냅샷을 조정하므로 ONTAP 스토리지 관리자가 서비스의 지식 없이 ONTAP System Manager, ONTAP CLI 또는 ONTAP REST API를 사용하여 스냅샷을 직접 삭제할 수 있습니다. 이 서비스는 대상 클러스터에 없는 소스의 스냅샷을 24시간마다 자동으로 삭제합니다. 하지만 필요에 따라 이를 수행할 수도 있습니다. 이 기능을 사용하면 모든 사이트에서 스냅샷이 일관성을 유지하도록 할 수 있습니다.

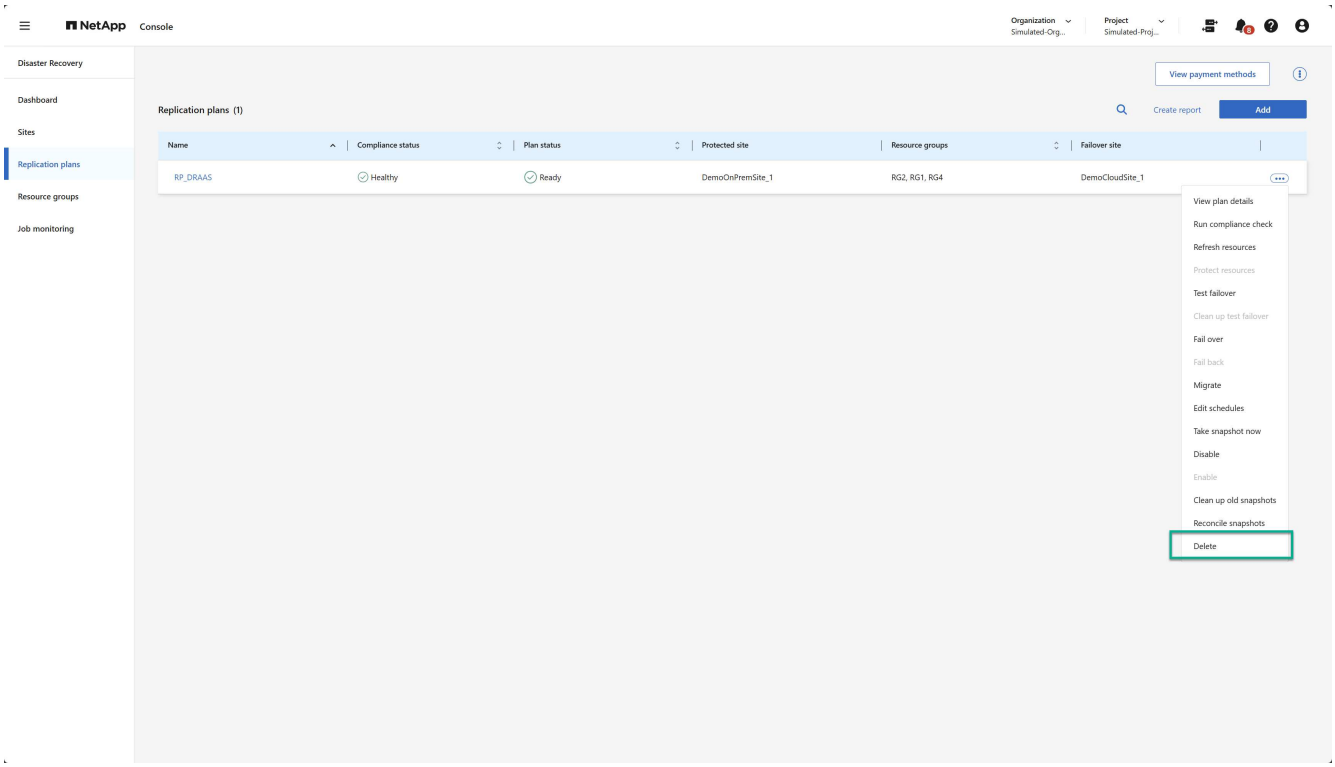
1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 대상 클러스터에 없는 스냅샷을 소스 클러스터에서 삭제하려면 복제 계획의 작업 메뉴에서 *스냅샷 조정*을 선택합니다.



복제 계획 삭제

복제 계획이 더 이상 필요하지 않으면 삭제할 수 있습니다.

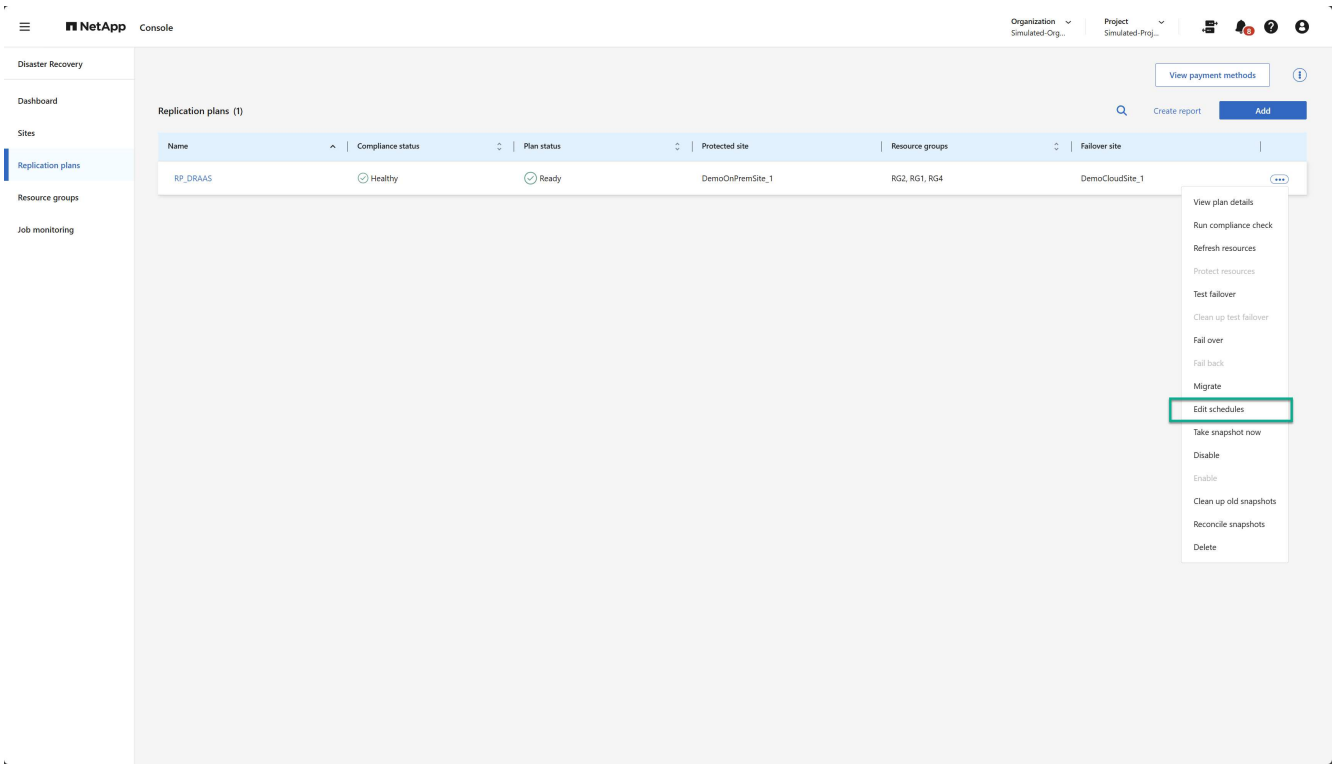
1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 복제 계획을 삭제하려면 복제 계획의 상황에 맞는 메뉴에서 *삭제*를 선택합니다.



일정 편집

테스트 장애 조치와 규정 준수 검사라는 두 가지 작업이 정기적으로 자동으로 수행됩니다.

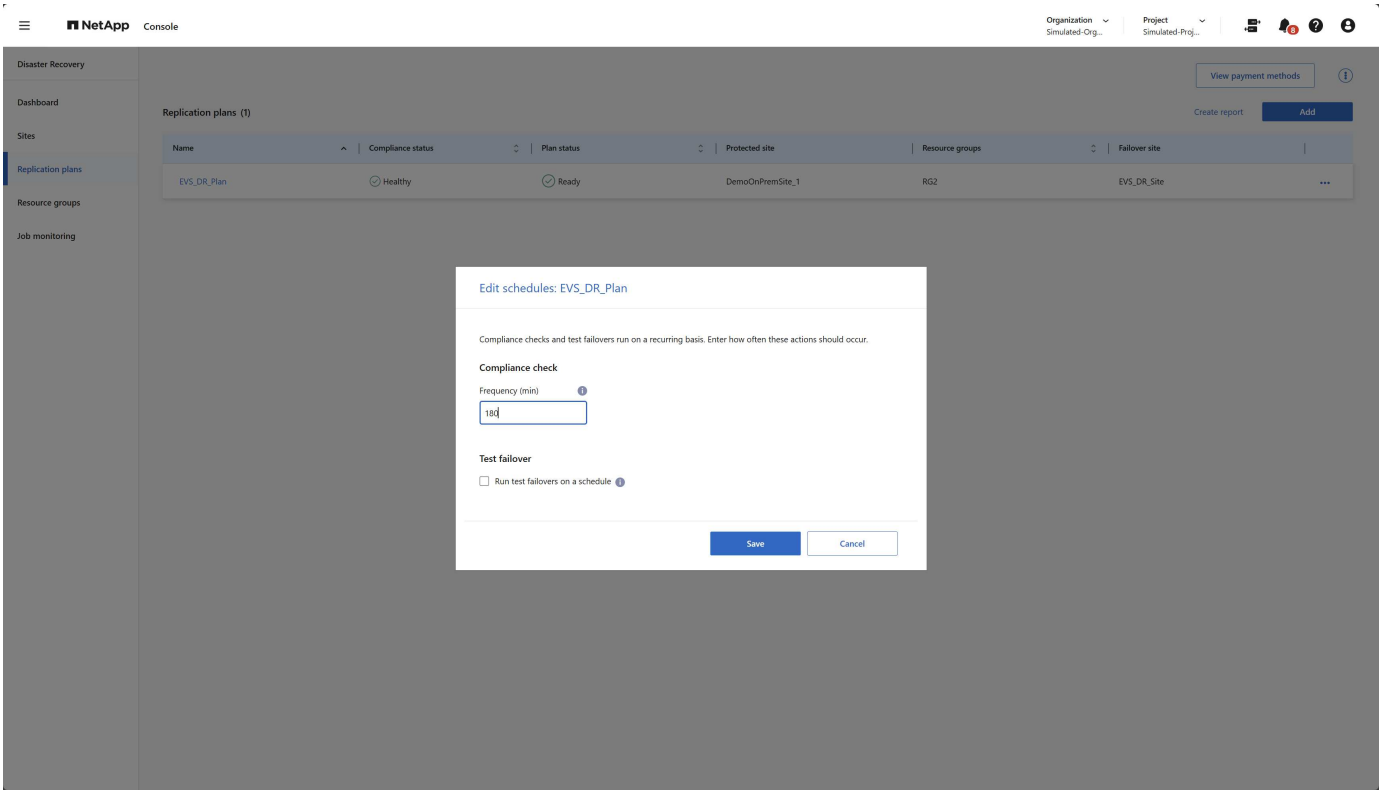
1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. 이 두 작업 중 하나에 대한 일정을 변경하려면 복제 계획에 대해 *일정 편집*을 선택합니다.



규정 준수 확인 간격 변경

기본적으로 규정 준수 검사는 3시간마다 수행됩니다. 30분에서 24시간 사이의 간격으로 변경할 수 있습니다.

이 간격을 변경하려면 일정 편집 대화 상자에서 빈도 필드를 변경하세요.



자동 테스트 장애 조치 일정 예약

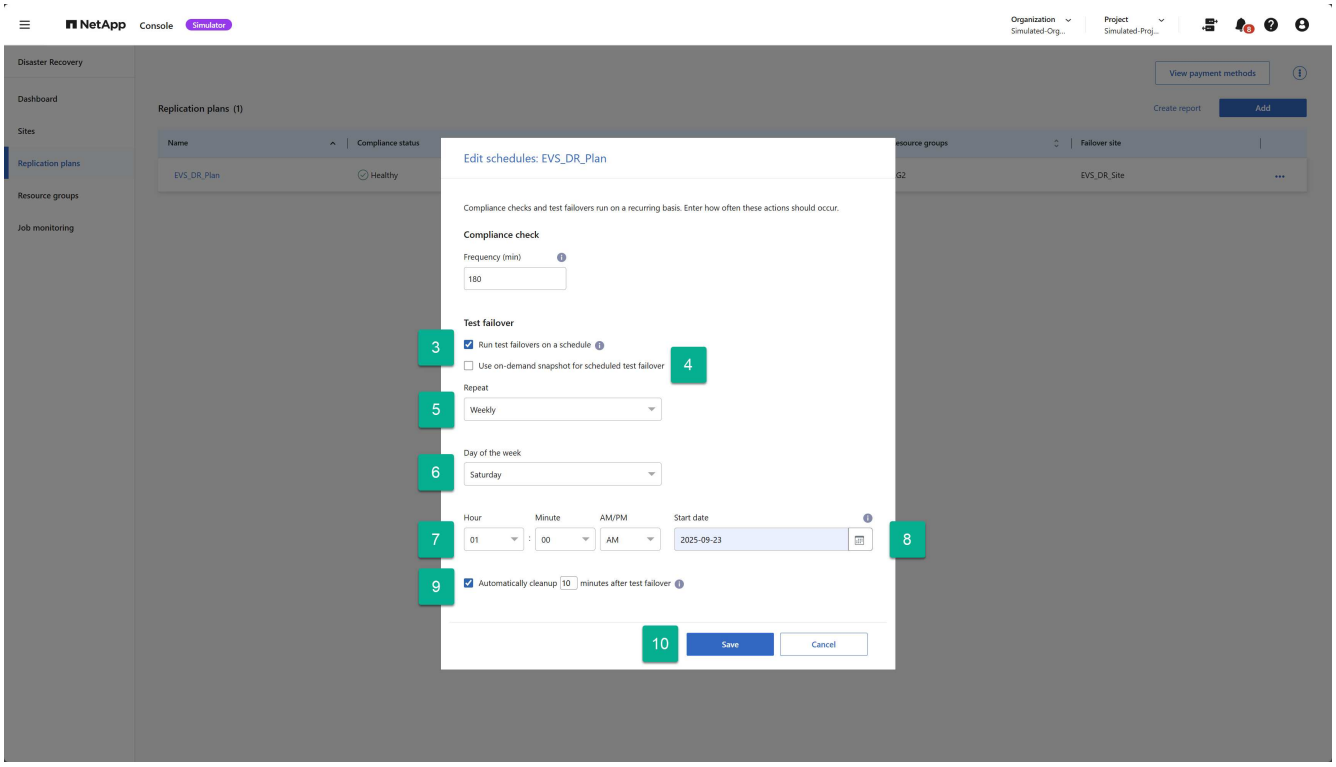
테스트 장애 조치는 기본적으로 수동으로 실행됩니다. 자동 테스트 장애 조치를 예약하면 복제 계획이 예상대로 수행되는지 확인하는 데 도움이 됩니다. 테스트 장애 조치 프로세스에 대해 자세히 알아보려면 다음을 참조하세요."장애 조치 프로세스 테스트" .

테스트 장애 조치를 예약하는 단계

1. 작업 옵션을 선택하세요 ••• 복제 계획 옆에 있습니다.
2. *장애 조치 실행*을 선택합니다.
3. 일정에 따라 테스트 장애 조치 실행 확인란을 선택합니다.
4. (선택 사항) *예약된 테스트 장애 조치에 주문형 스냅샷 사용*을 선택합니다.
5. 반복 드롭다운에서 간격 유형을 선택합니다.
6. 테스트 장애 조치를 수행할 시기를 선택하세요
   a. 주간: 요일을 선택하세요
   b. 월별: 해당 월의 날짜를 선택하세요
7. 테스트 장애 조치를 실행할 시간을 선택하세요
8. 시작 날짜를 선택하세요.
9. 서비스가 테스트 환경을 자동으로 정리할지 여부와 정리 프로세스가 시작되기 전에 테스트 환경을 얼마나 오랫동안

실행할지 결정합니다.

10. *저장*을 선택하세요.



NetApp Disaster Recovery 에 대한 자주 묻는 질문

이 FAQ는 질문에 대한 빠른 답변을 찾는 데 도움이 될 수 있습니다.

- NetApp Disaster Recovery URL은 무엇입니까?* 브라우저에서 URL을 입력하세요. "https://console.netapp.com/" NetApp 콘솔에 액세스합니다.
- NetApp Disaster Recovery 사용하려면 라이선스가 필요합니까?* 전체 액세스를 위해서는 NetApp Disaster Recovery 라이선스가 필요합니다. 하지만 무료 체험판을 통해 직접 체험해 볼 수는 있습니다.

NetApp Disaster Recovery 에 대한 라이선싱 설정에 대한 자세한 내용은 다음을 참조하세요."NetApp Disaster Recovery 라이선스 설정" .

- NetApp Disaster Recovery 어떻게 액세스합니까?* NetApp Disaster Recovery 어떠한 활성화도 필요하지 않습니다. 재해 복구 옵션은 NetApp Console 왼쪽 탐색 창에 자동으로 나타납니다.

지식과 지원

지원 등록

NetApp Console 과 해당 스토리지 솔루션, 데이터 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로를 활성화하려면 지원 등록도 필요합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품 설명서의 "도움말 받기 "를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

지원 등록 개요

지원 자격을 활성화하기 위한 등록 방법은 두 가지가 있습니다.

- NetApp Console 계정 일련 번호를 등록합니다(콘솔의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호).

  이는 콘솔 내의 모든 서비스에 대한 단일 지원 구독 ID 역할을 합니다. 각 콘솔 계정을 등록해야 합니다.

- 클라우드 공급업체의 마켓플레이스에서 구독과 관련된 Cloud Volumes ONTAP 일련 번호를 등록합니다(20자리 909201xxxxxxxx 일련 번호).

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 NetApp Console 에서 생성됩니다.

두 가지 유형의 일련 번호를 모두 등록하면 지원 티켓 개설 및 자동 사례 생성과 같은 기능을 사용할 수 있습니다. 아래 설명된 대로 콘솔에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 **NetApp Console** 등록

지원을 등록하고 지원 자격을 활성화하려면 NetApp Console 계정의 한 사용자가 NetApp 지원 사이트 계정을 콘솔 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

NSS 계정이 있는 NetApp 고객이라면 콘솔을 통해 지원을 등록하기만 하면 됩니다.

단계

1. 관리 > *자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.

3. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 과정이 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 *지원*을 선택하세요.

   리소스 페이지에는 귀하의 콘솔 계정이 지원을 위해 등록되어 있다는 내용이 표시됩니다.

   다른 콘솔 사용자는 NetApp 지원 사이트 계정을 로그인과 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 귀하의 계정이 지원을 위해 등록되지 않았다는 의미는 아닙니다. 조직 내 한 명의 사용자가 이러한 단계를 따랐다면 귀하의 계정은 등록되었습니다.

기존 고객이지만 **NSS** 계정이 없습니다.

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 콘솔 로그인과 연결해야 합니다.

단계

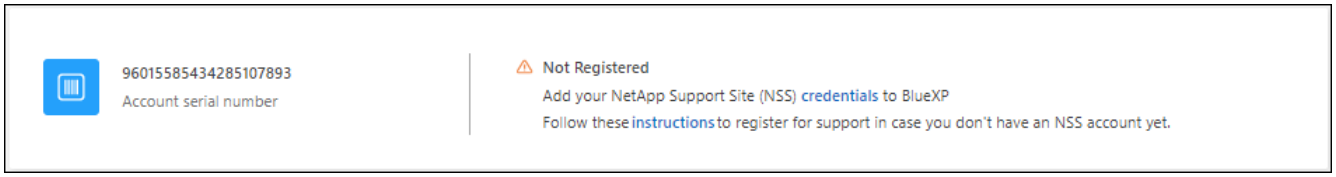
1. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 콘솔 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp 의 새로운 기능

NetApp 처음 사용하시고 NSS 계정이 없으신 경우 아래의 각 단계를 따르세요.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.
2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾으세요.



3. 로 이동 "NetApp 지원 등록 사이트" *저는 등록된 NetApp 고객이 아닙니다*를 선택하세요.
4. 필수 입력란(빨간색 별표가 있는 항목)을 작성해 주세요.
5. 제품군 필드에서 *클라우드 관리자*를 선택한 다음 해당 청구 제공자를 선택하세요.
6. 위의 2단계에서 계정 일련번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호정책을 읽었는지 확인하세요.

   이 안전한 거래를 마무리하기 위해 제공된 사서함으로 이메일이 즉시 전송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인하세요.

7. 이메일 내에서 작업을 확인하세요.

   확인을 클릭하면 귀하의 요청이 NetApp 에 제출되고 NetApp 지원 사이트 계정을 만드는 것이 좋습니다.

8. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
    a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
    b. 위에 사용된 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 처리 속도가 빨라집니다.

당신이 완료한 후

이 과정에서 NetApp 귀하에게 연락을 드릴 것입니다. 이는 신규 사용자를 대상으로 한 일회성 온보딩 과정입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

Cloud Volumes ONTAP 지원을 위한 NSS 자격 증명 연결

Cloud Volumes ONTAP 에 대한 다음 주요 워크플로를 활성화하려면 NetApp 지원 사이트 자격 증명을 콘솔 계정과 연결해야 합니다.

- 지원을 위해 Pay-as-you-go Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  콘솔에서 라이선스 키를 업로드하고 구매한 기간 동안 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

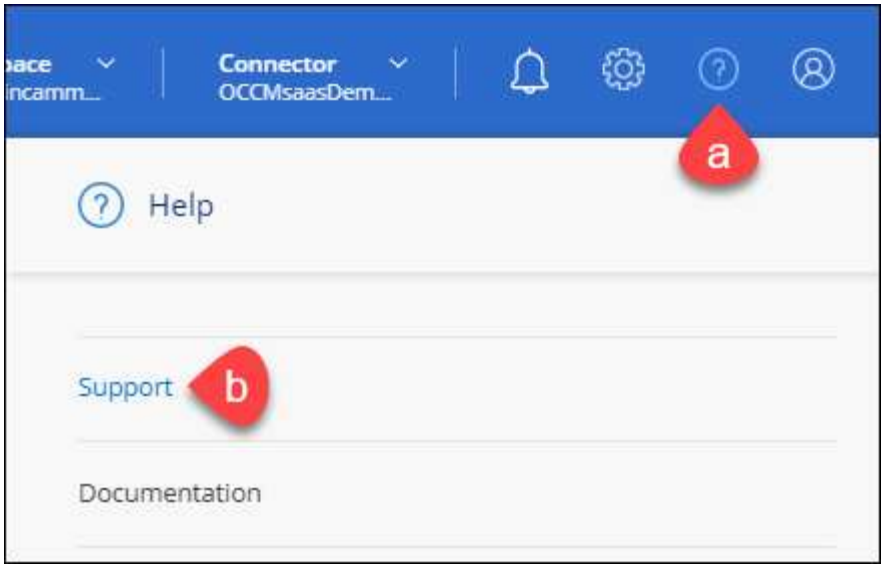
NSS 자격 증명을 NetApp Console 계정과 연결하는 것은 콘솔 사용자 로그인과 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 콘솔 계정 ID와 연결됩니다. 콘솔 조직에 속한 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. *NSS 관리 > NSS 계정 추가*를 선택하세요.
3. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 이동합니다.

   NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하여 인증 과정을 진행합니다.

   이러한 작업을 통해 콘솔은 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록과 같은 작업에 NSS 계정을 사용할 수 있습니다.

   다음 사항에 유의하세요.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트나 임시 계정이어서는 안 됩니다). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - 해당 계정이 파트너 수준 계정인 경우 NSS 계정은 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하는데 파트너 수준 계정이 이미 있는 경우 다음과 같은 오류 메시지가 표시됩니다.

     "이 계정에는 다른 유형의 NSS 사용자가 이미 있으므로 NSS 고객 유형이 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있고 파트너 수준 계정을 추가하려는 경우에도 마찬가지입니다.

   - 로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

     이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. ••• 메뉴.

   - 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

     이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

도움을 받으세요

NetApp 다양한 방법으로 NetApp Console 과 클라우드 서비스에 대한 지원을 제공합니다. 지식 기반(KB) 문서와 커뮤니티 포럼 등 광범위한 무료 셀프 지원 옵션을 24시간 연중무휴로 이용할 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

클라우드 공급자 파일 서비스에 대한 지원을 받으세요

클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 설명서를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

NetApp 과 해당 스토리지 솔루션, 데이터 서비스에 대한 특정 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하세요.

셀프 지원 옵션 사용

다음 옵션은 주 7일, 하루 24시간 무료로 이용 가능합니다.

- 설명서

  현재 보고 있는 NetApp Console 문서입니다.

- "지식 기반"

  NetApp 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  NetApp Console 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새로운 토론을 만들어 보세요.

NetApp 지원을 통해 사례 만들기

위에 나열된 셀프 지원 옵션 외에도, 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

- 사례 만들기 기능을 사용하려면 먼저 NetApp 지원 사이트 자격 증명을 콘솔 로그인과 연결해야 합니다. "콘솔 로그인과 관련된 자격 증명을 관리하는 방법을 알아보세요." .
- 일련 번호가 있는 ONTAP 시스템에 대한 사례를 개설하는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어야 합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. 리소스 페이지에서 기술 지원 아래에 있는 사용 가능한 옵션 중 하나를 선택하세요.

a. 전화로 상담원과 통화하고 싶으시면 *전화하기*를 선택하세요. netapp.com에서 전화할 수 있는 전화번호가 나열된 페이지로 이동하게 됩니다.

b. NetApp 지원 전문가에게 티켓을 열려면 *사례 만들기*를 선택하세요.

   - 서비스: 문제와 관련된 서비스를 선택하세요. 예를 들어, * NetApp Console*은 콘솔 내 워크플로 또는 기능과 관련된 기술 지원 문제에 대한 구체적인 내용입니다.
   - 시스템: 스토리지에 해당되는 경우 * Cloud Volumes ONTAP* 또는 *온프레미스*를 선택한 다음 연관된 작업 환경을 선택합니다.

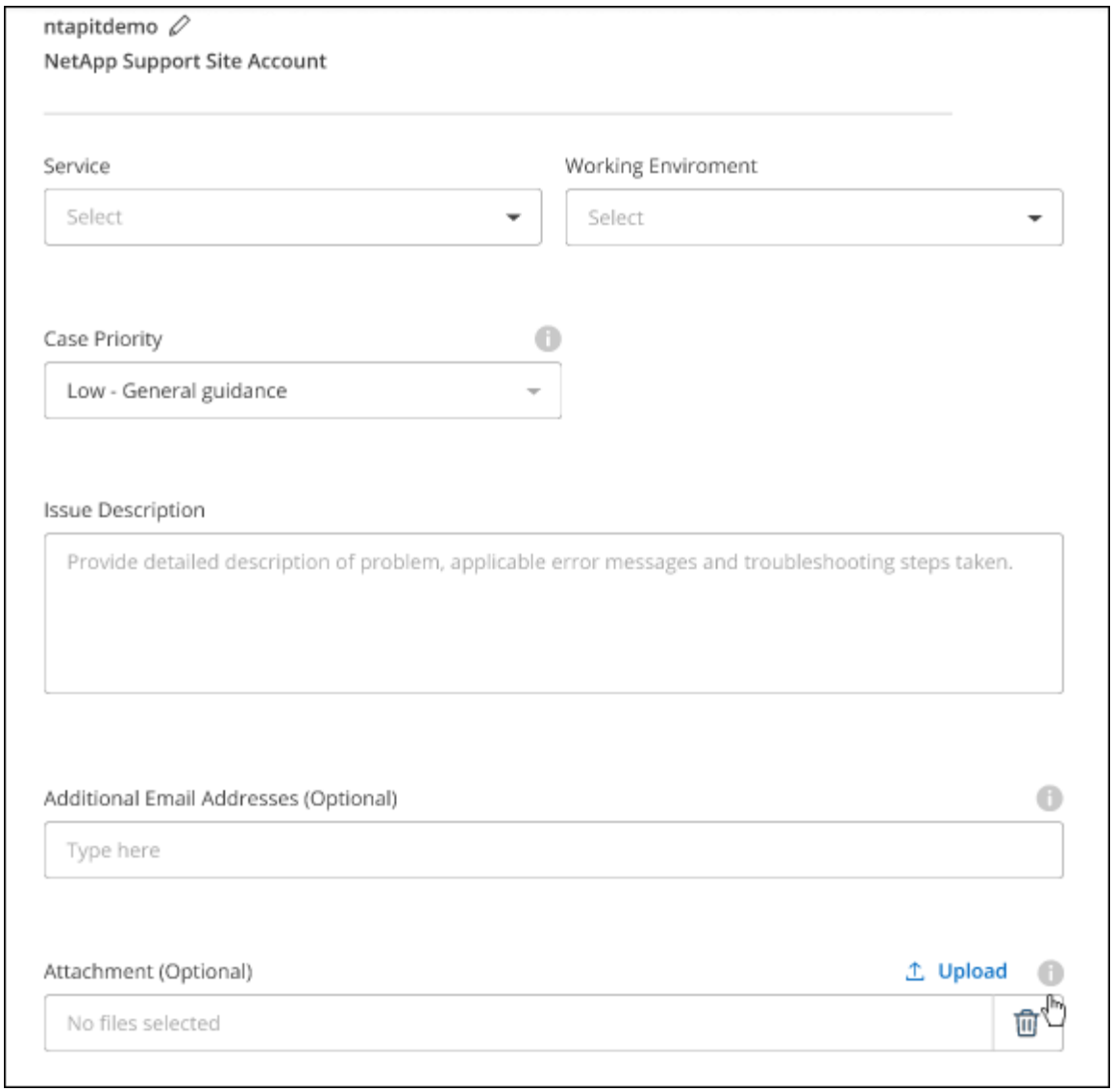
     시스템 목록은 콘솔 조직 범위 내에 있으며, 상단 배너에서 선택한 콘솔 에이전트입니다.

   - 사례 우선순위: 낮음, 보통, 높음 또는 중요로 사례의 우선순위를 선택합니다.

     이러한 우선순위에 대한 자세한 내용을 알아보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으세요.

   - 문제 설명: 해당 오류 메시지나 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공하세요.
   - 추가 이메일 주소: 이 문제를 다른 사람에게 알리려면 추가 이메일 주소를 입력하세요.
   - 첨부파일(선택사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.



당신이 완료한 후

지원 사례 번호가 포함된 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 연락드릴 것입니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 만들기"라는 이름의 작업을 찾으세요. 가장 오른쪽에 있는 버튼을 누르면 동작을 확장하여 자세한 내용을 볼 수 있습니다.

사례를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 사례를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 NetApp Console 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 작업 환경 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 비기술적 사례를 제출하세요 https://mysupport.netapp.com/site/help

지원 사례 관리

콘솔에서 직접 활성화된 지원 사례와 해결된 지원 사례를 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된

사례를 관리할 수 있습니다.

다음 사항에 유의하세요.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기를 제공합니다.
  - 왼쪽 보기는 귀하가 제공한 NSS 계정 사용자에 의해 지난 3개월 동안 열린 총 사례를 보여줍니다.
  - 오른쪽 보기는 사용자 NSS 계정을 기준으로 지난 3개월 동안 회사 수준에서 열린 총 사례를 보여줍니다.

  표의 결과는 귀하가 선택한 보기와 관련된 사례를 반영합니다.
- 관심 있는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하세요.
- 사례별로 사례 메모를 업데이트하거나 아직 닫힘 또는 닫힘 보류 상태가 아닌 사례를 닫는 기능을 제공합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. *사례 관리*를 선택하고 메시지가 표시되면 콘솔에 NSS 계정을 추가합니다.

   사례 관리 페이지는 콘솔 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 표시합니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요에 따라 표에 표시되는 정보를 수정합니다.
   - *조직 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하세요.
   - 열의 내용을 필터링합니다.
   - 표에 나타나는 열을 변경하려면 다음을 선택하세요. 그런 다음 표시하려는 열을 선택합니다.
4. 기존 사례를 관리하려면 다음을 선택하세요. 그리고 사용 가능한 옵션 중 하나를 선택하세요:
   - 사례 보기: 특정 사례에 대한 전체 세부 정보를 확인하세요.
   - 사례 메모 업데이트: 문제에 대한 추가 세부 정보를 제공하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.
   - 사건 종결: 사건을 종결하는 이유를 자세히 입력하고 *사건 종결*을 선택하세요.

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

"NetApp Disaster Recovery 에 대한 알림"