NetApp Disaster Recovery 사용

NetApp Disaster Recovery

NetApp
January 12, 2026

목차

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.

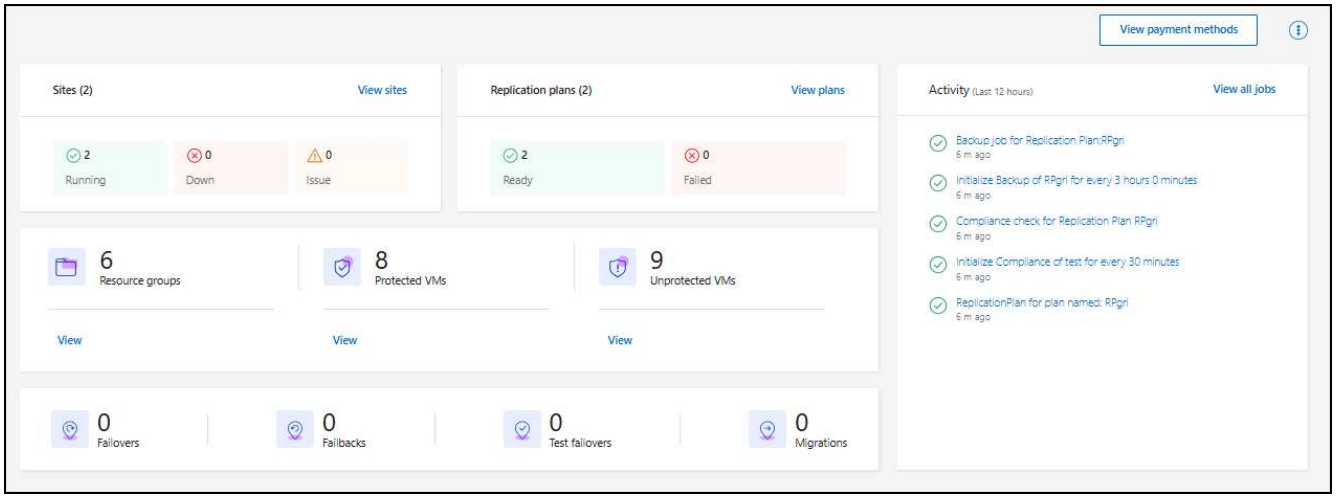
NetApp Disaster Recovery 대시보드를 사용하면 재해 복구 사이트와 복제 계획의 상태를 확인할 수 있습니다. 어떤 사이트와 계획이 정상인지, 연결이 끊겼는지, 성능이 저하되었는지 빠르게 확인할 수 있습니다.

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" .

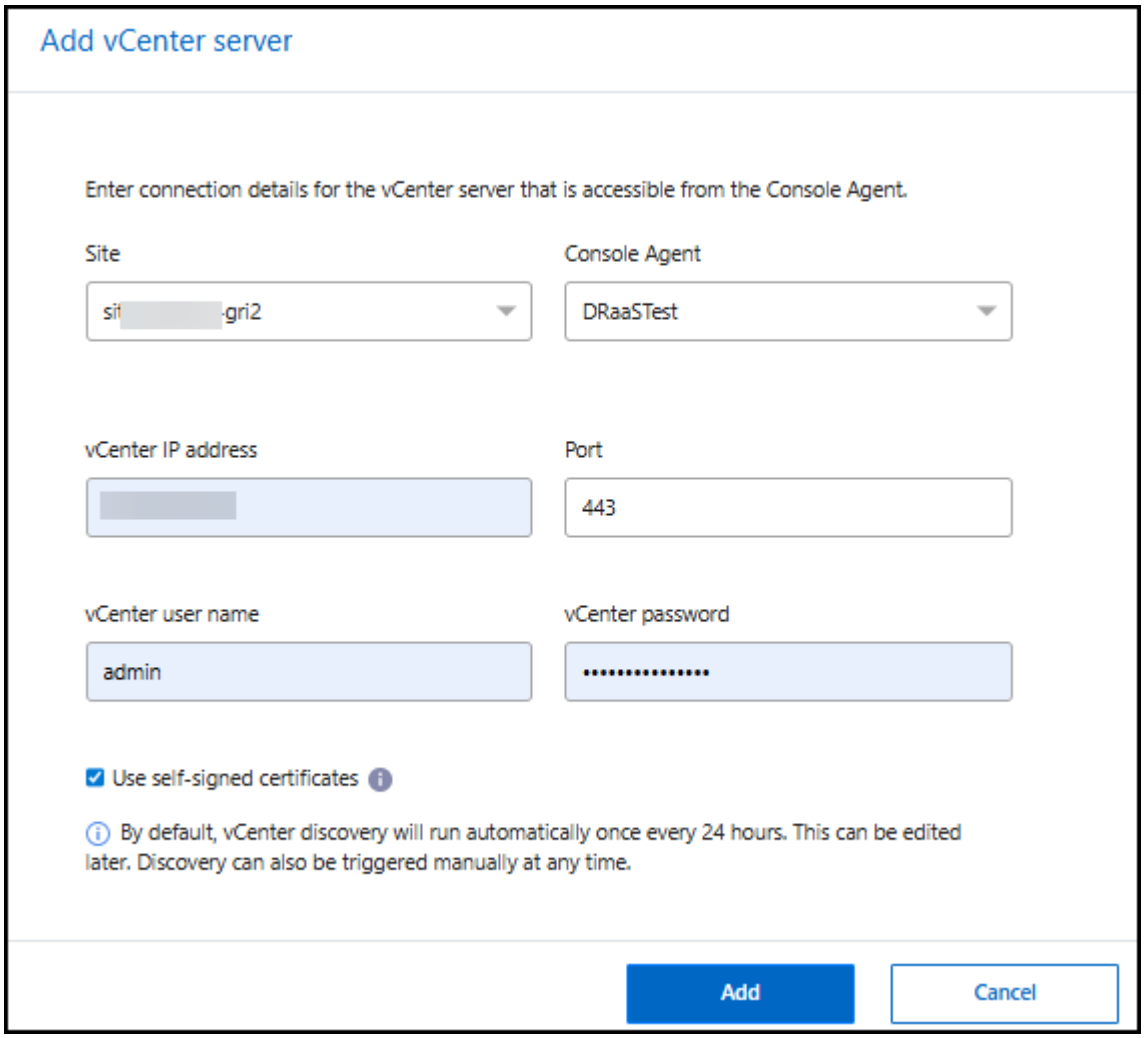
2. NetApp Console 왼쪽 탐색에서 보호 > *재해 복구*를 선택합니다.

   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.

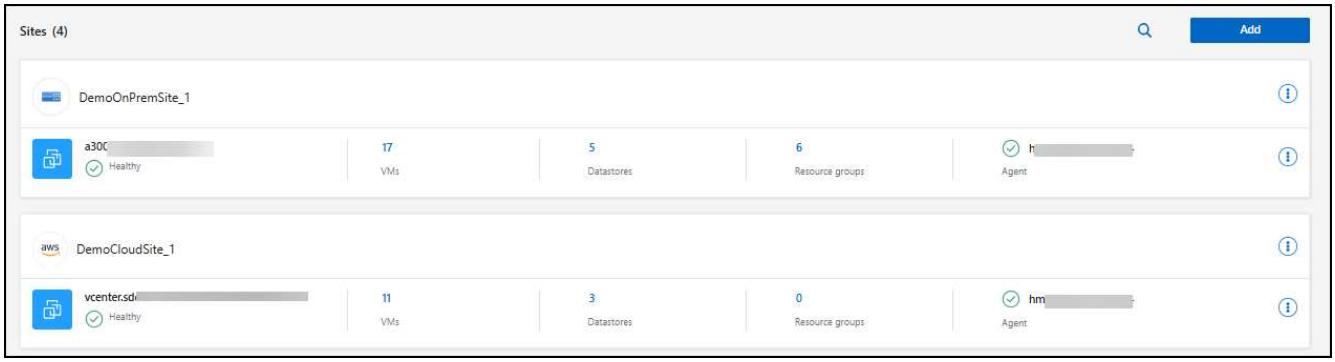
7. 대상 vCenter에 대한 사이트를 다시 추가합니다.
8. 다시 *vCenter 추가*를 선택하고 대상 vCenter 정보를 추가합니다.
9. 목표:

   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.

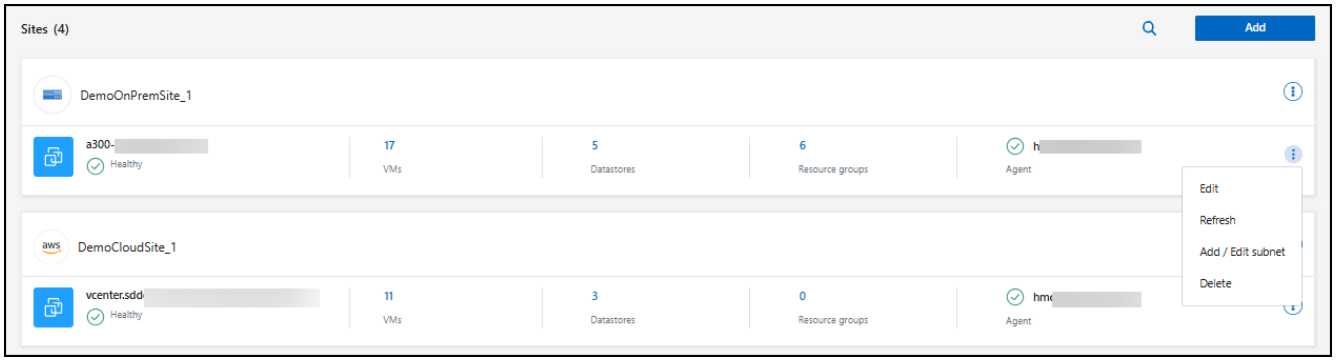
요약하자면, 호스트 주소는 동일하게 유지되지만 네트워크 주소는 사이트 서브넷 매핑에 구성된 주소로 대체됩니다. 이를 통해 장애 조치 시 IP 주소 재할당을 보다 쉽게 관리할 수 있으며, 특히 관리해야 할 네트워크가 수백 개이고 VM이 수천 개일 경우 더욱 그렇습니다.

서브넷 매핑을 사용하는 것은 선택적인 2단계 프로세스입니다.

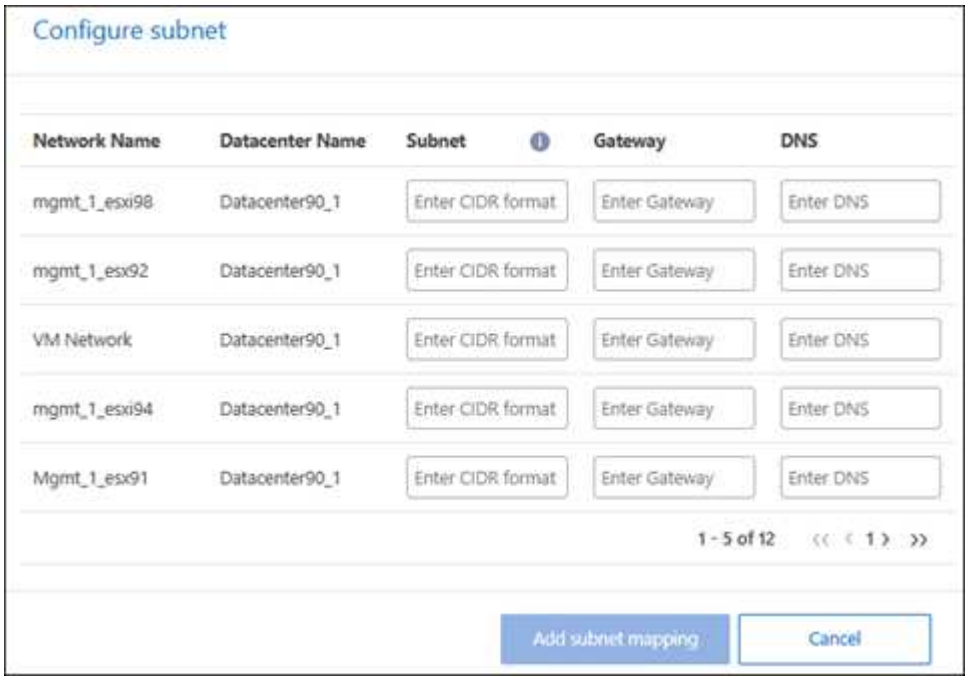
- 먼저, 각 vCenter 사이트에 대한 서브넷 매핑을 추가합니다.
- 둘째, 복제 계획에서 가상 머신 탭과 대상 IP 필드에서 서브넷 매핑을 사용할 것임을 표시합니다.

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

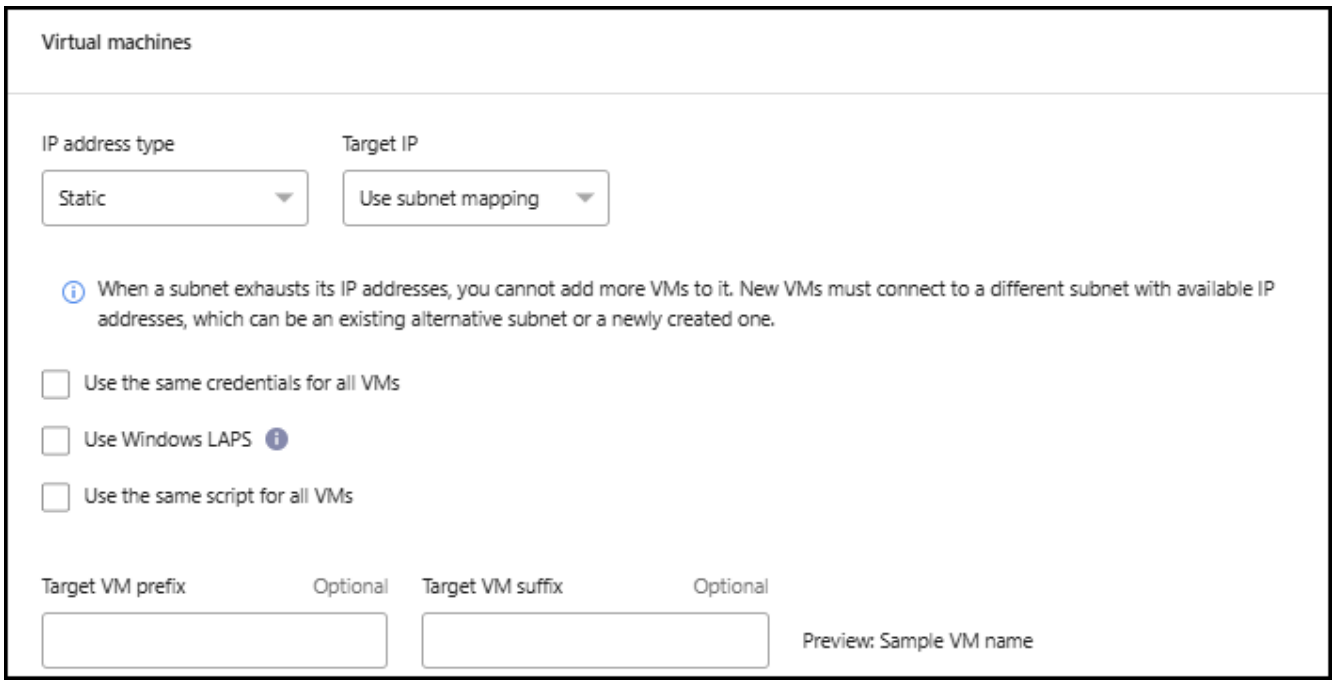
복제 계획을 생성할 때 복제 계획에 대한 서브넷 매핑을 선택할 수 있습니다.

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.

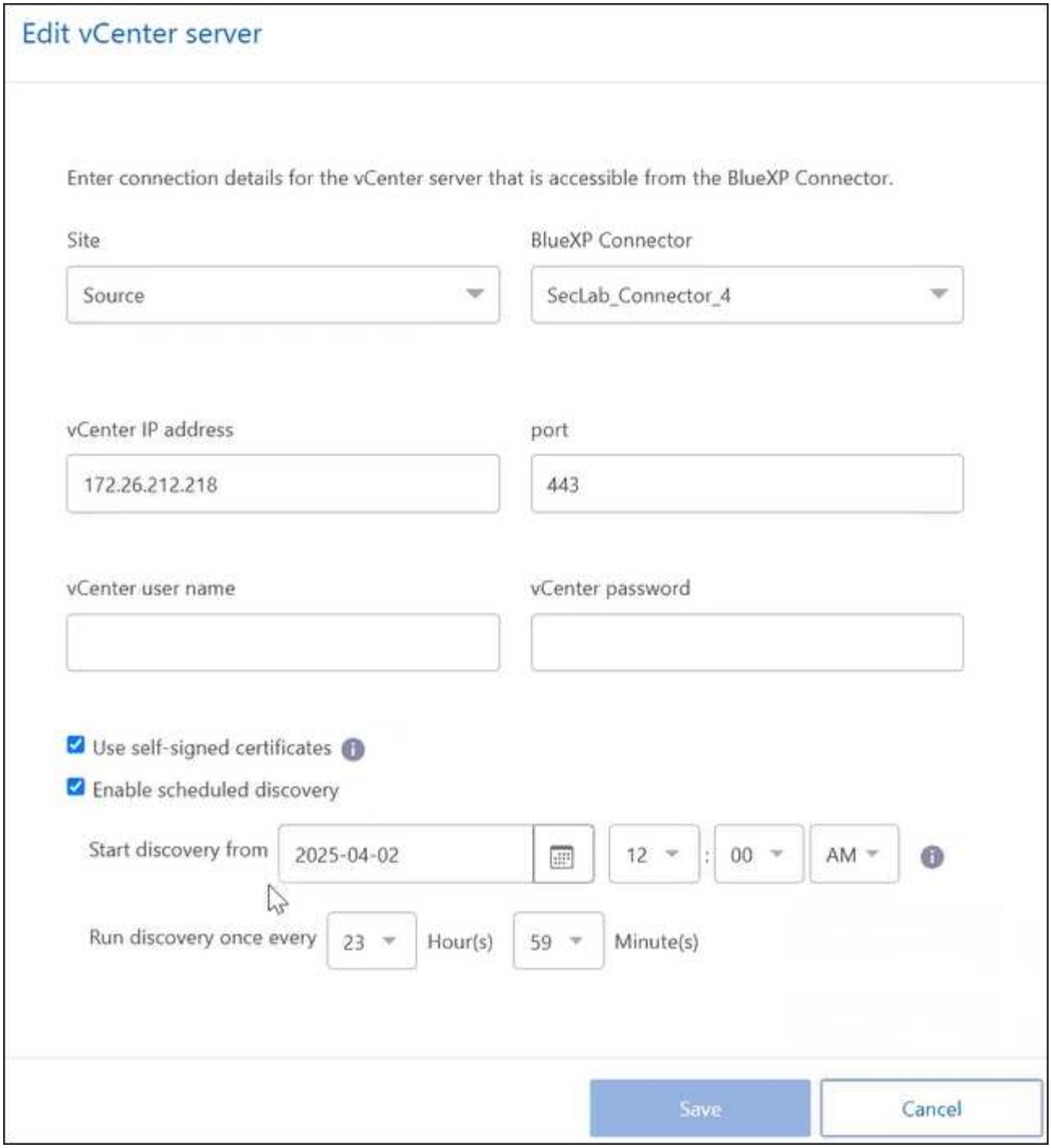
vCenter 서버 사이트를 편집하여 검색 일정을 사용자 지정할 수 있습니다. 예를 들어, VM 수가 많은 경우 검색 일정을 23시간 59분마다 실행되도록 설정할 수 있습니다. VM 수가 적은 경우 검색 일정을 12시간마다 실행되도록 설정할 수 있습니다.

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.

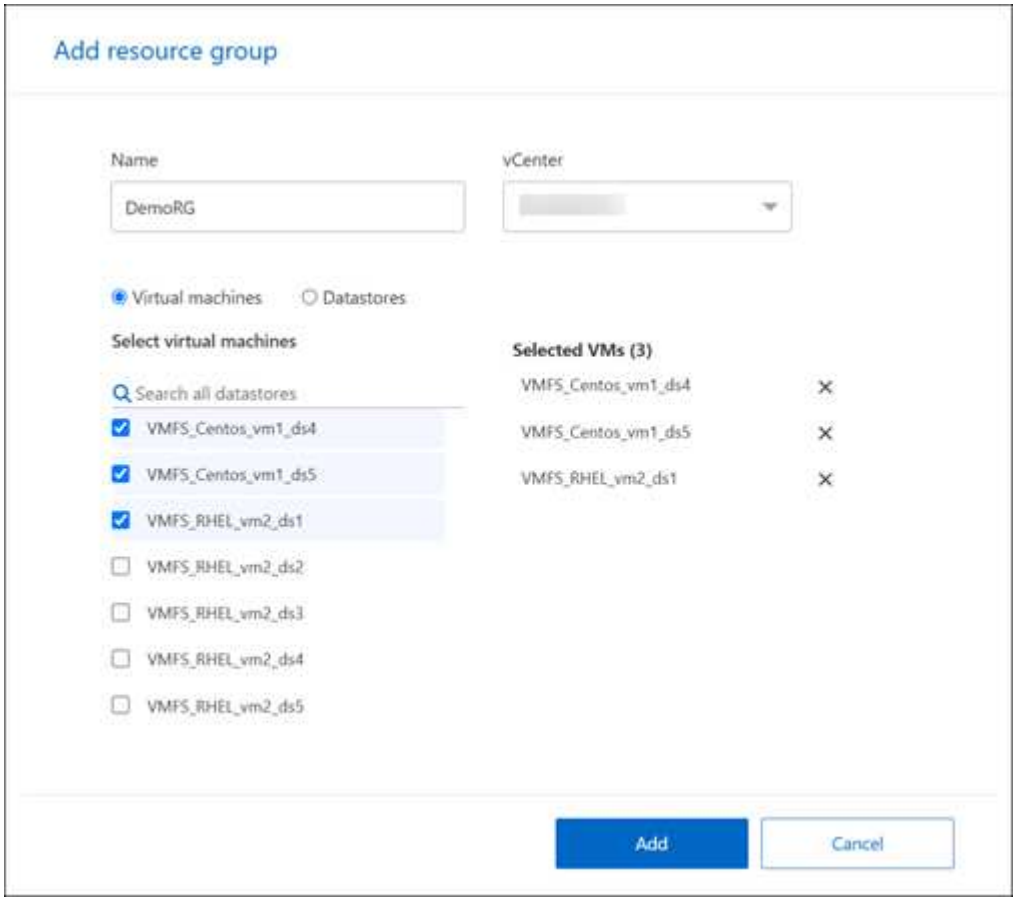
모범 사례: NetApp Disaster Recovery 배포하기 전에 VM을 구성하여 "데이터 저장소 확산"을 최소화하세요. 보호가 필요한 VM을 데이터 저장소 하위 집합에 배치하고, 보호하지 않을 VM을 다른 데이터 저장소 하위 집합에 배치합니다. 주어진 데이터 저장소의 VM이 서로 다른 복제 계획으로 보호되지 않도록 합니다.

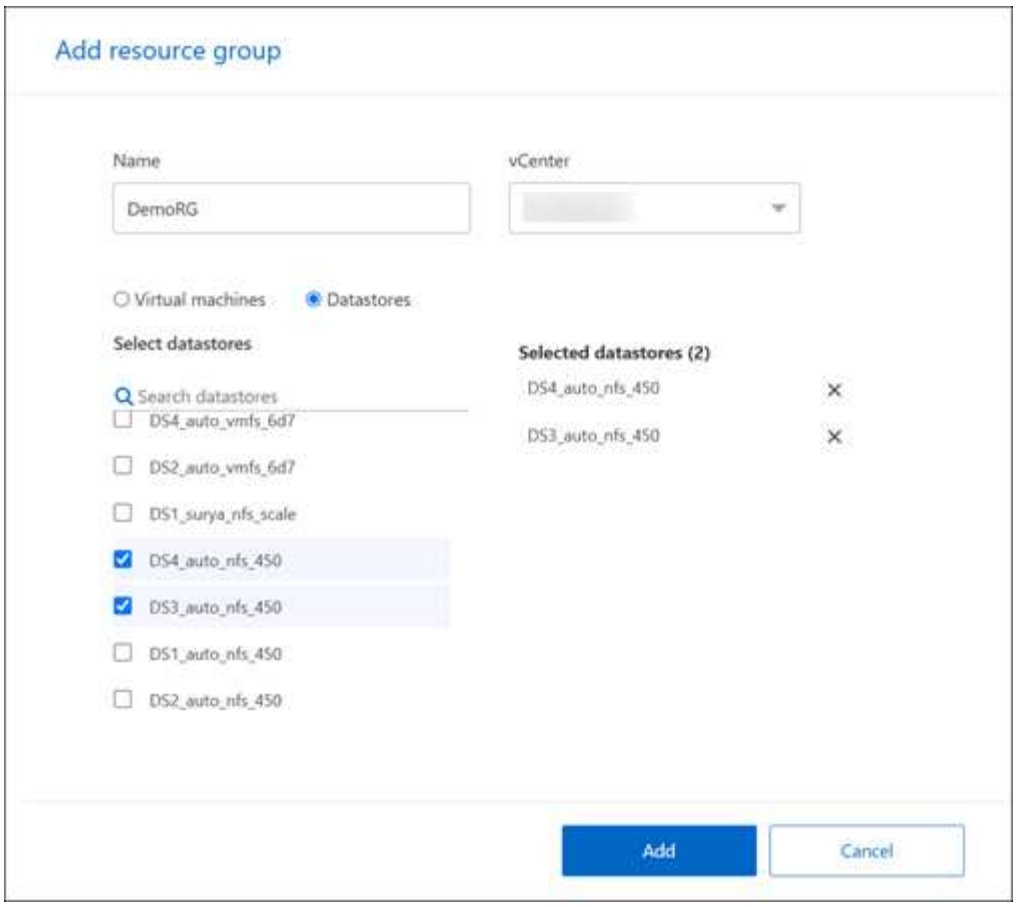
단계

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.

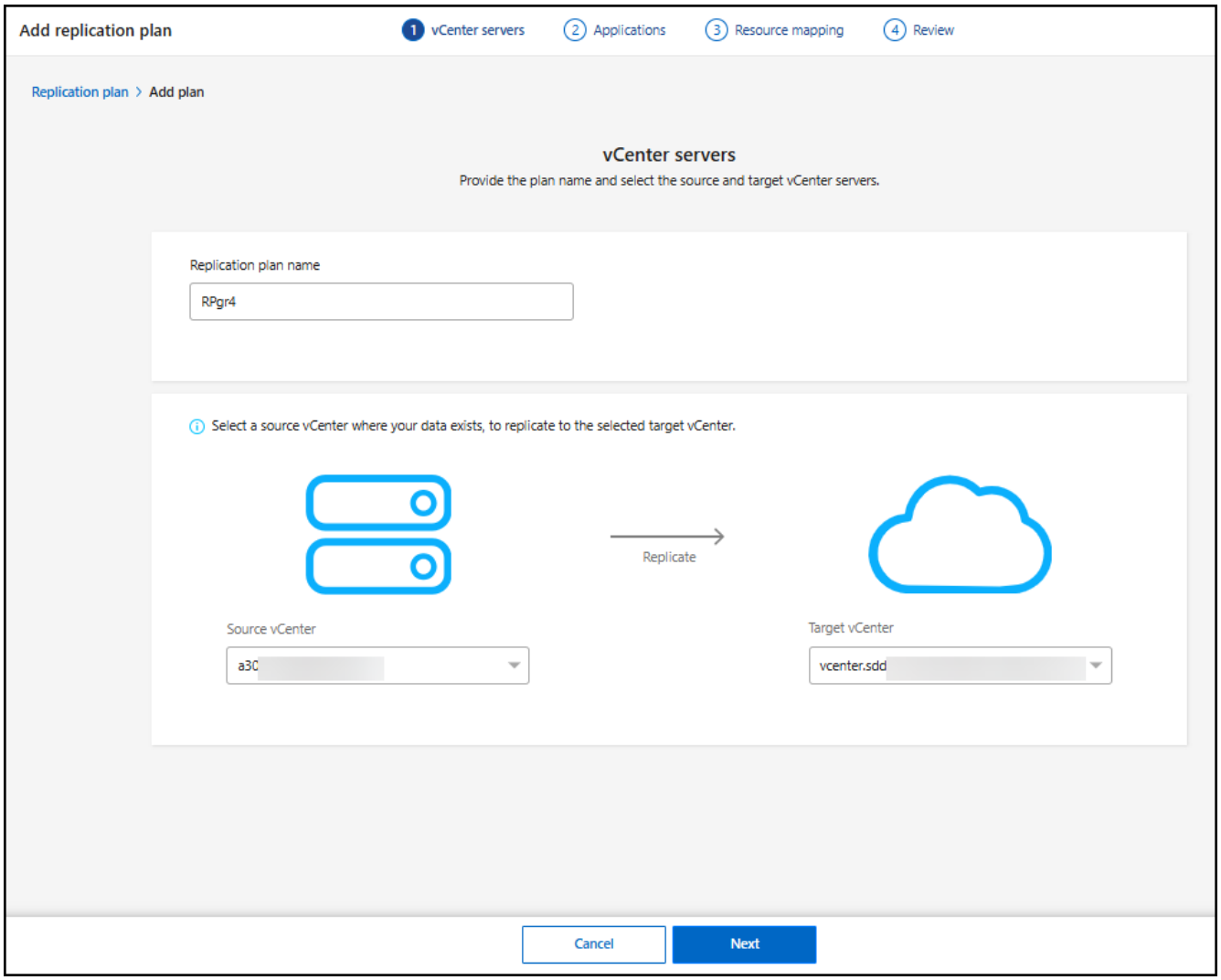
- 계획의 모든 VM에 대해 동일한 자격 증명을 사용합니다.
- 계획에 있는 모든 VM에 동일한 스크립트를 사용합니다.
- 계획에 있는 모든 VM에 대해 동일한 서브넷, DNS 및 게이트웨이를 사용합니다.

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.

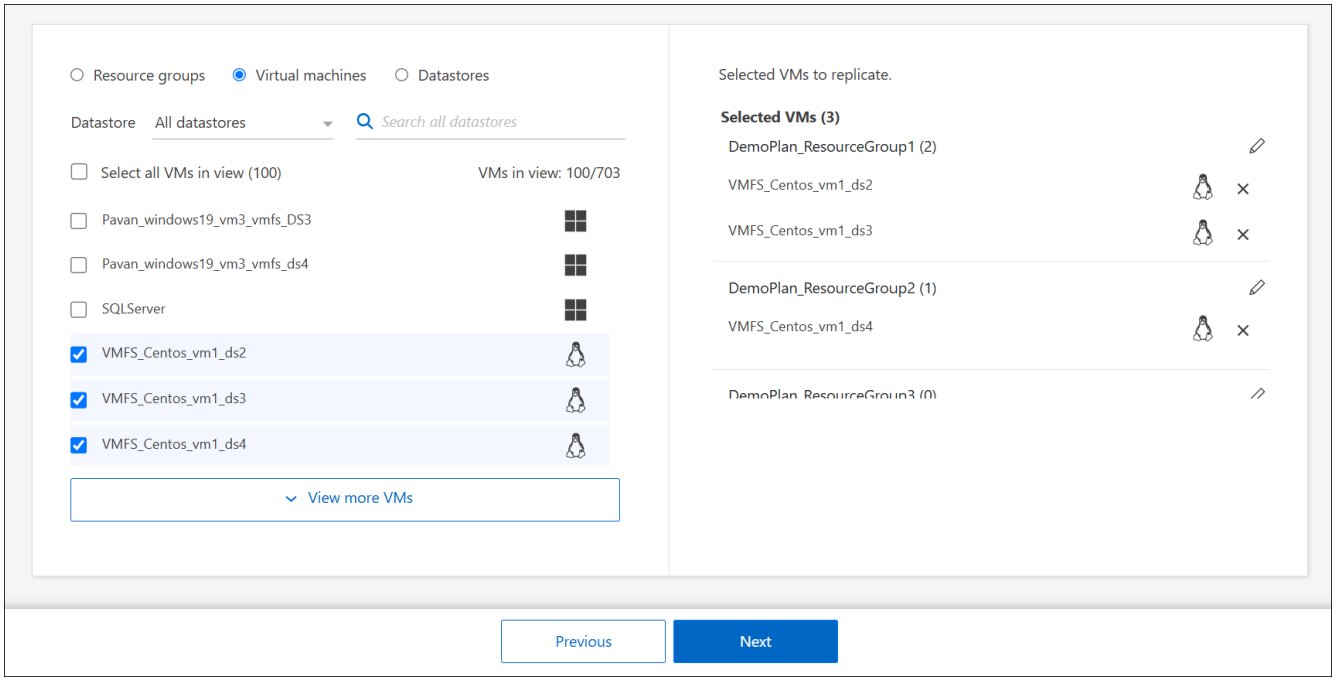
단계

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.

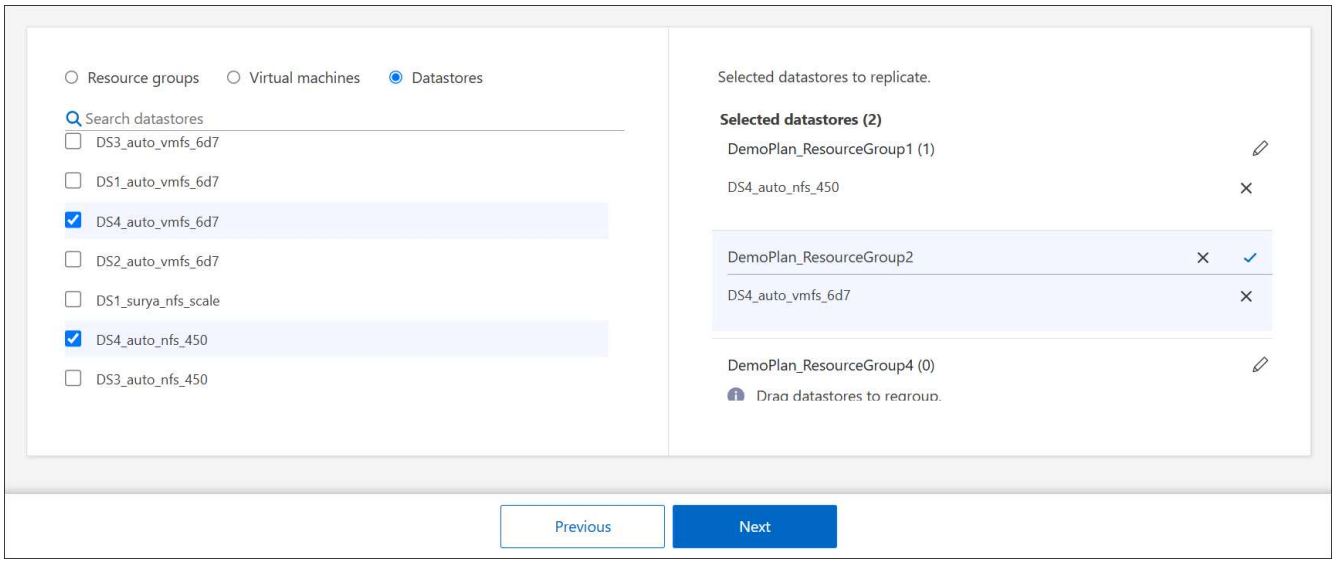
   소스 vCenter는 온프레미스 vCenter에 있어야 합니다. 대상 vCenter는 동일 사이트 또는 원격 사이트에 있는 두 번째 온프레미스 vCenter이거나, VMware Cloud on AWS와 같은 클라우드 기반 소프트웨어 정의 데이터 센터(SDDC)일 수 있습니다. 두 vCenter 모두 재해 복구 작업 환경에 이미 추가되어 있어야 합니다.

   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.

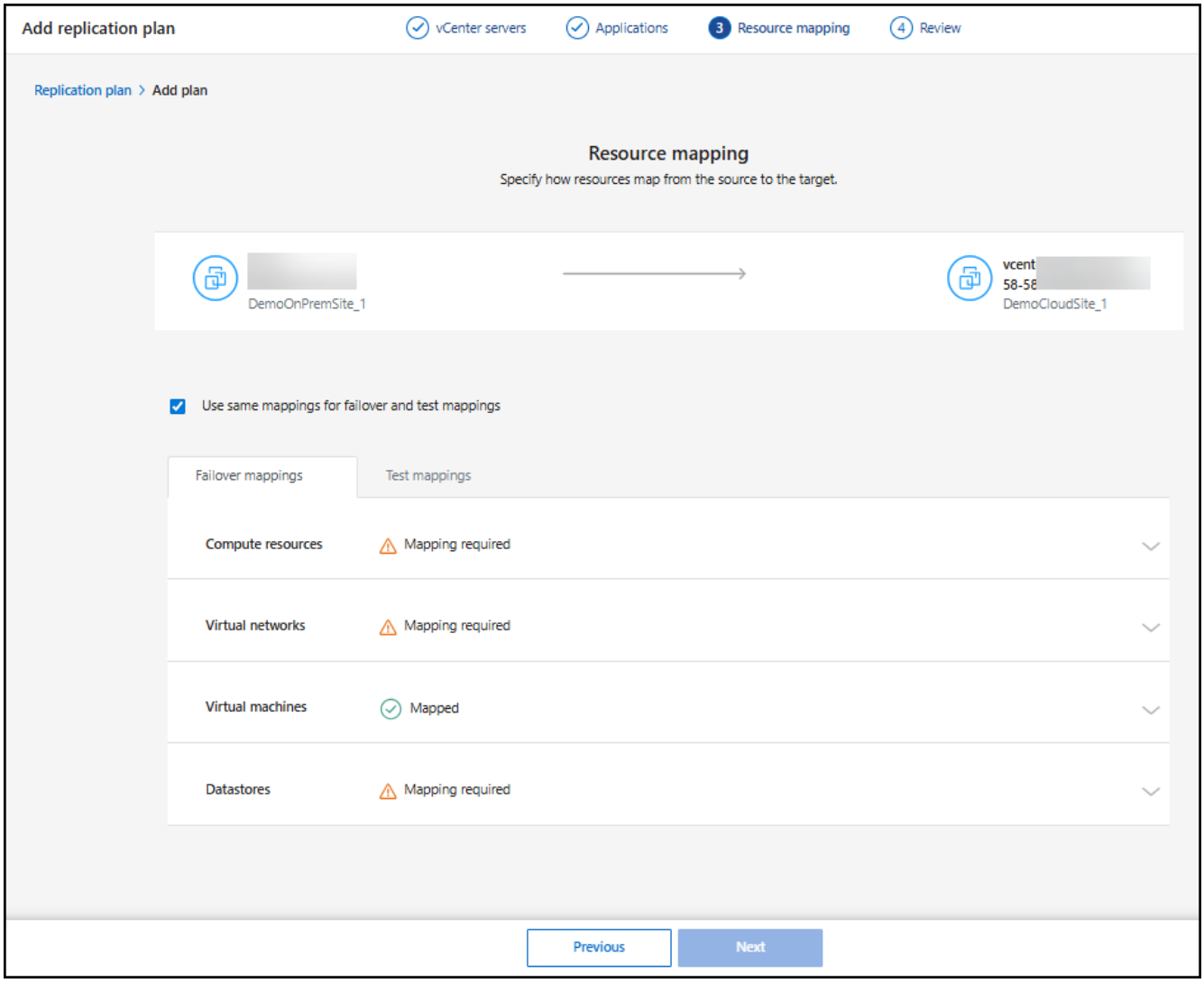
DR 계획의 일부로 테스트 장애 조치를 수행하려는 경우 장애 조치 테스트 중에 시작된 VM이 프로덕션 VM을 방해하지 않도록 테스트 장애 조치 매핑 세트를 제공해야 합니다. 테스트 VM에 다른 IP 주소를 제공하거나 테스트 VM의 가상 NIC를 프로덕션과 분리되어 있지만 IP 구성은 동일한 다른 네트워크(버블 또는 테스트 네트워크라고 함)에 매핑하여 이를 달성할 수 있습니다.

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.

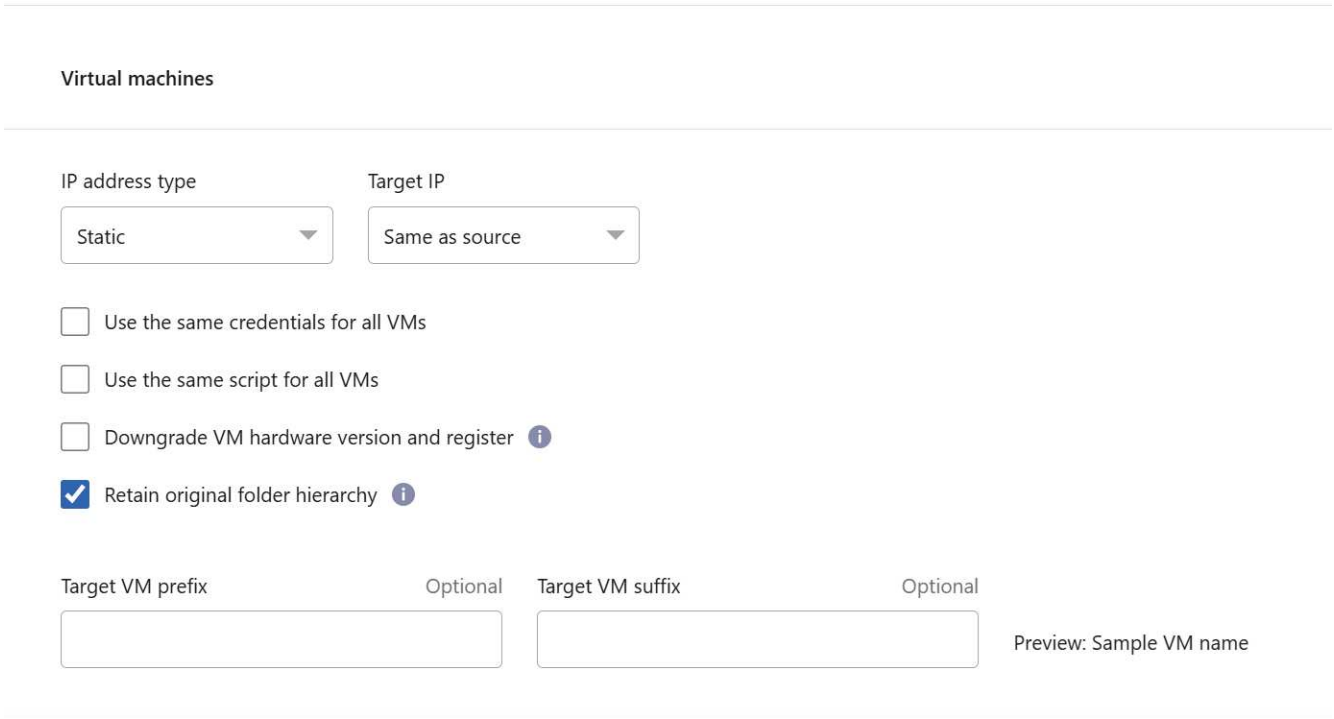
네트워크 설정 재해 복구는 VM 네트워크에 대한 광범위한 구성 옵션을 지원합니다. 대상 사이트에 소스 사이트의 프로덕션 가상 네트워크와 다른 TCP/IP 설정을 사용하는 가상 네트워크가 있는 경우 이를 변경해야 할 수도 있습니다.

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.

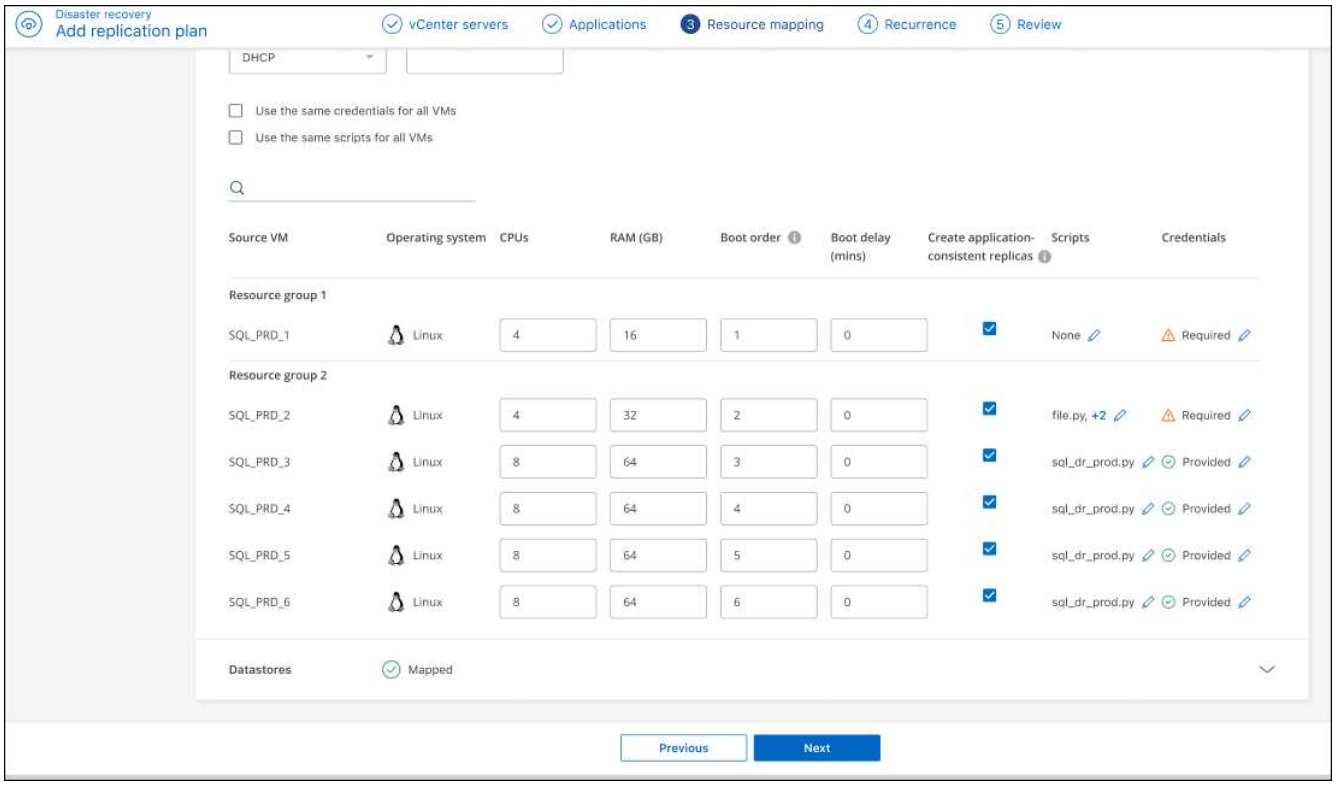
원래 폴더 계층 구조를 무시하려면 이 상자의 선택을 취소하세요.

- 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.

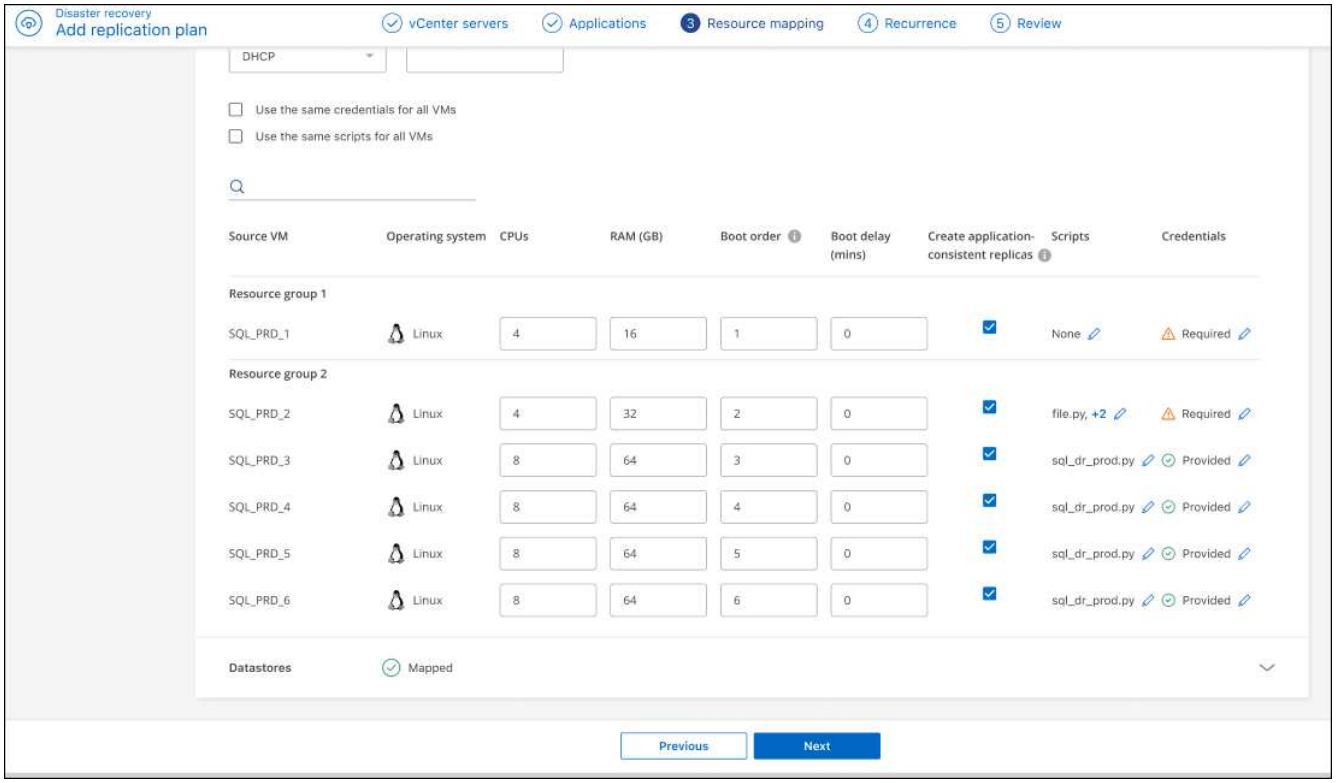
  - 순차 부팅: 각 VM에 고유한 번호를 지정하여 지정된 순서대로 부팅합니다(예: 1, 2, 3, 4, 5).
  - 동시 부팅: 모든 VM에 동일한 번호를 할당하여 동시에 부팅합니다(예: 1,1,1,1,2,2,3,4,4).

- 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.

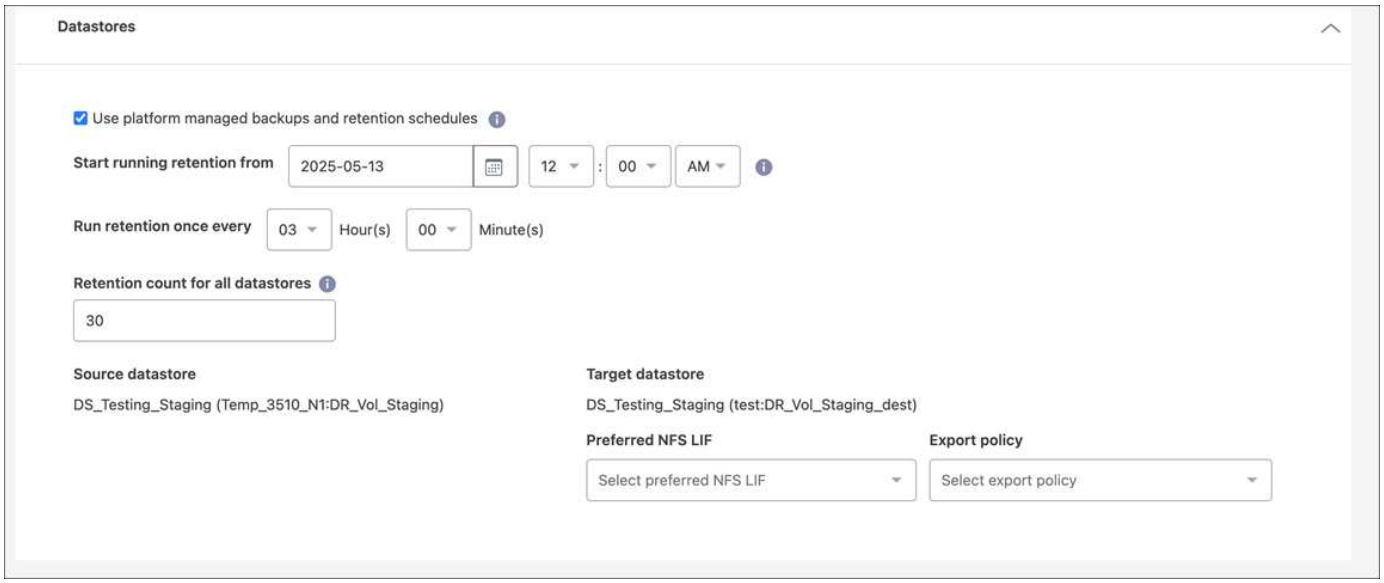
VM과 호스팅 데이터 저장소의 애플리케이션 일관성 복제본을 활성화하려면 각 VM에 대해 애플리케이션 일관성 복제본 만들기 옆의 상자를 선택하고 적절한 권한이 있는 게스트 로그인 자격 증명을 제공합니다.

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

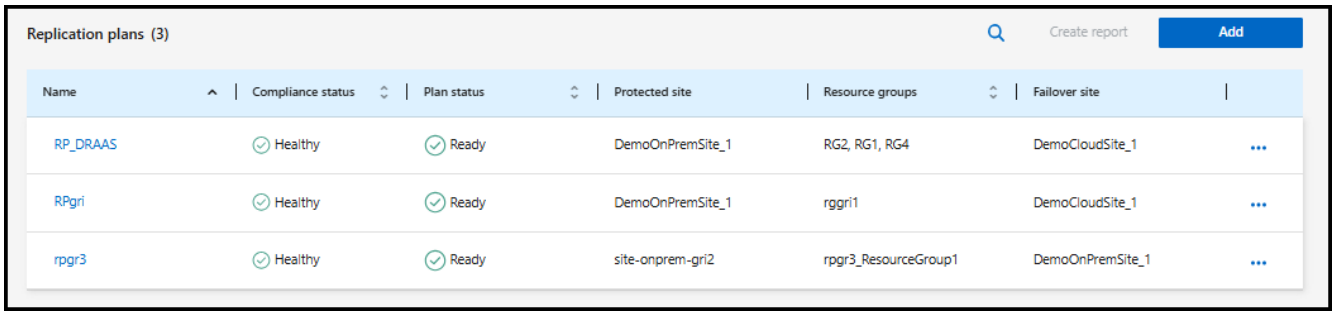
계획에 지정된 대상으로 가상 머신의 장애 조치를 테스트할 수 있습니다.

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.

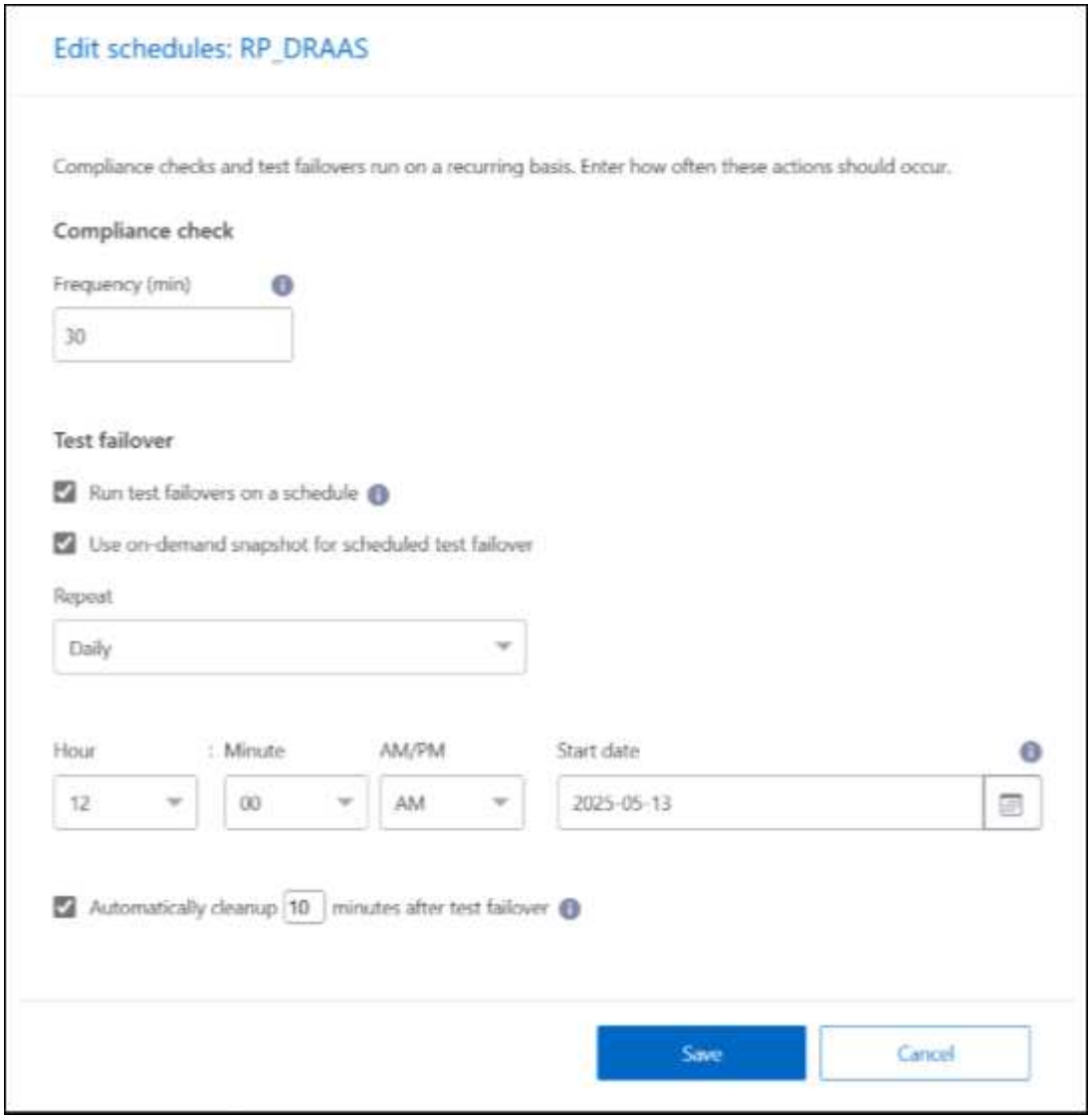
일정에 따라 장애 조치 테스트가 실행되고 워크로드가 복제 계획에 지정된 대상으로 이동하는지 확인합니다.

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.

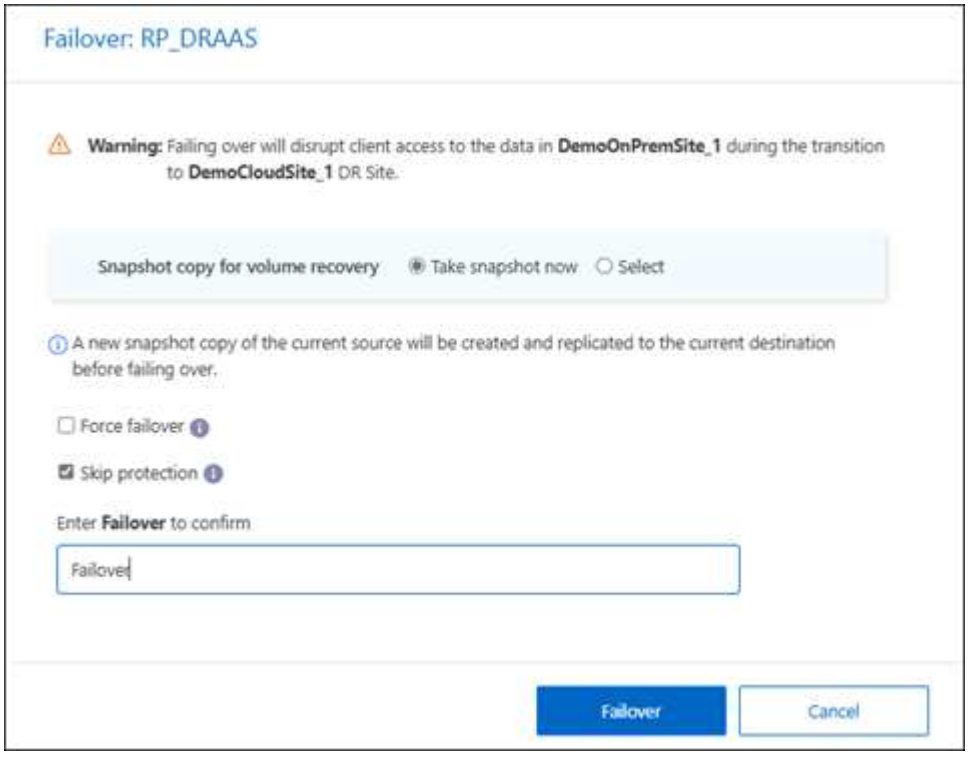
- 대상 가상 머신은 vCenter에 새로운 데이터 저장소로 등록됩니다.
- 대상 가상 머신은 리소스 그룹 페이지에서 캡처한 부팅 순서에 따라 전원이 켜집니다.
- 소스 vCenter가 여전히 활성 상태인 경우 장애 조치 중인 모든 소스 측 VM의 전원을 끕니다.
- "애플리케이션 일관성"으로 표시된 VM에서 지원되는 모든 데이터베이스 애플리케이션을 취소합니다.
- 소스 vCenter 및 ONTAP 클러스터가 여전히 활성 상태인 경우, 장애 조치 상태에서 모든 변경 사항을 원래 소스 사이트로 복제하기 위해 역방향 SnapMirror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

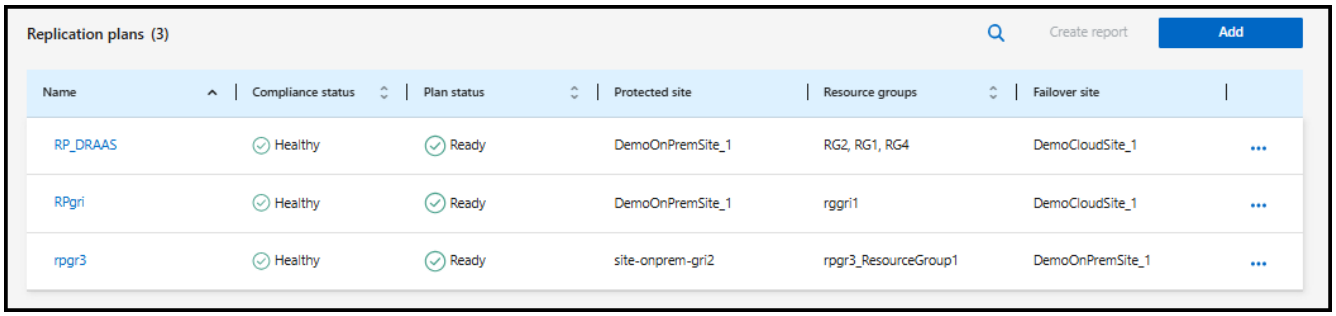
복제 계획을 비활성화, 활성화 및 삭제할 수 있습니다. 일정을 변경할 수 있습니다.

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.

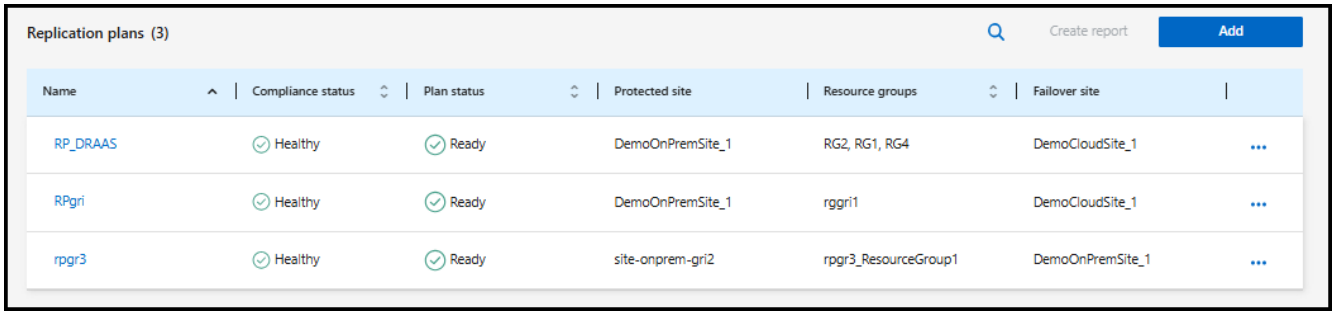
필요에 따라 스냅샷 조정

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.

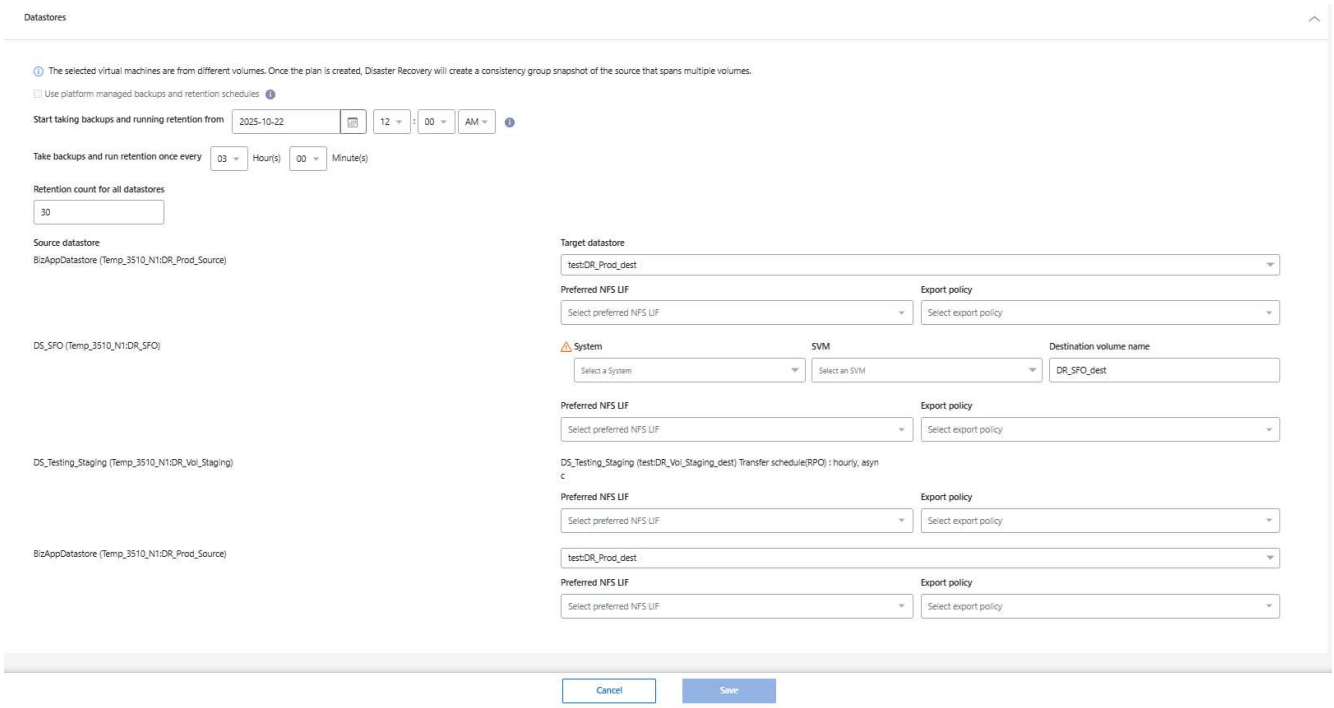
장애 조치 일정에 대한 보존 횟수 변경

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.