



데이터 저장소 및 가상 머신 보호 ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

목차

데이터 저장소 및 가상 머신 보호	1
ONTAP tools에서 호스트 클러스터 보호	1
SRA 보호를 사용하여 보호	2
데이터 저장소를 보호하려면 ONTAP tools에서 SRA를 구성하십시오	2
SAN 및 NAS 환경용 ONTAP tools에서 SRA 구성	3
확장성이 높은 환경을 위해 ONTAP tools에서 SRA를 구성합니다	4
ONTAP tools를 사용하여 VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다	5
ONTAP tools에서 SRA 자격 증명 업데이트	6
ONTAP tools에서 보호 사이트 및 복구 사이트를 구성합니다	7
보호 사이트 및 복구 사이트 리소스 구성	8
ONTAP tools에서 복제된 스토리지 시스템을 검증합니다	12
ONTAP 도구의 팬아웃 보호	12

데이터 저장소 및 가상 머신 보호

ONTAP tools에서 호스트 클러스터 보호

ONTAP tools for VMware vSphere는 호스트 클러스터 보호를 관리합니다. 선택한 SVM에 속하고 클러스터의 하나 이상의 호스트에 마운트된 모든 데이터 저장소는 호스트 클러스터로 보호됩니다.

시작하기 전에

호스트 클러스터를 보호하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- 호스트 클러스터에는 단일 SVM의 데이터 저장소만 포함되어 있습니다.
- 호스트 클러스터의 데이터 저장소는 클러스터 외부의 호스트에 마운트되지 않습니다.
- 호스트 클러스터에 마운트된 데이터 저장소는 iSCSI 또는 FC 프로토콜을 사용하는 VMFS 데이터 저장소입니다. vVols, NFS 또는 NVMe/FC 및 NVMe/TCP 프로토콜을 사용하는 VMFS 데이터 저장소는 사용할 수 없습니다.
- 호스트에 마운트된 FlexVol/LUN 볼륨 기반 데이터 저장소는 어떤 일관성 그룹에도 속하지 않습니다.
- 호스트에 마운트된 FlexVol/LUN 볼륨 기반 데이터 저장소는 어떠한 SnapMirror 관계에도 포함되지 않습니다.
- 호스트 클러스터에는 하나 이상의 데이터 저장소가 포함되어 있습니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 클러스터를 마우스 오른쪽 버튼으로 클릭하고 * NetApp ONTAP tools* > *클러스터 보호*를 선택합니다.
3. 클러스터 보호 창에서 시스템은 데이터 저장소 유형과 소스 스토리지 가상 머신(VM) 세부 정보를 자동으로 채웁니다. 보호된 데이터 저장소를 보려면 데이터 저장소 링크를 선택하십시오.
4. *관계 추가*를 선택합니다.
5. **SnapMirror** 관계 추가 창에서 대상 스토리지 **VM***과 *정책 유형을 선택합니다.

정책 유형은 비동기 또는 AutomatedFailOverDuplex일 수 있습니다.

SnapMirror 관계를 AutomatedFailOverDuplex 유형 정책으로 추가할 때, ONTAP tools for VMware vSphere가 배포된 동일한 vCenter에 대상 스토리지 VM을 스토리지 백엔드로 추가해야 합니다.

AutomatedFailOverDuplex 정책 유형에는 균일 호스트 구성과 비균일 호스트 구성이 있습니다. 균일 호스트 구성 토글 버튼을 선택하면 호스트 이니시에이터 그룹 구성이 대상 사이트에 암묵적으로 복제됩니다. 자세한 내용은 ["핵심 개념 및 용어"](#)를 참조하십시오.

6. 비균일 호스트 구성을 선택하는 경우, 해당 클러스터 내의 각 호스트에 대한 호스트 액세스(소스/대상)를 선택합니다.
7. *추가*를 선택합니다.
8. 호스트 클러스터 보호는 호스트 클러스터 보호 수정 작업을 사용하여 편집할 수 있습니다. 관계는 줄임표 메뉴 옵션을 사용하여 편집하거나 삭제할 수 있습니다.
9. 보호 버튼을 선택합니다.

시스템은 vCenter 작업 ID 세부 정보가 포함된 vCenter 작업을 생성하고 최근 작업 패널에 진행 상황을 표시합니다. 이 작업은 비동기 작업이므로 사용자 인터페이스에는 요청 제출 상태만 표시되고 작업 완료를 기다리지 않습니다.

10. 보호된 호스트 클러스터를 보려면 * NetApp ONTAP tools* > 보호 > *호스트 클러스터 관계*로 이동하십시오. 일관성 그룹을 선택하여 용량, 연결된 데이터 저장소 및 하위 일관성 그룹을 확인합니다.



생성 후 1시간 이내에 보호 기능을 해제해야 하는 경우 먼저 스토리지 검색을 실행하십시오.

관련 정보

["VMware vSphere Metro Storage Cluster\(vMSC\)"](#)

SRA 보호를 사용하여 보호

데이터 저장소를 보호하려면 **ONTAP tools**에서 **SRA**를 구성하십시오

ONTAP tools for VMware vSphere는 재해 복구를 구성하기 위해 SRA 기능을 활성화하는 옵션을 제공합니다.

시작하기 전에

- vCenter Server 인스턴스를 설정하고 ESXi 호스트를 구성해야 합니다.
- ONTAP tools for VMware vSphere를 배포해야 합니다.
- SRA 어댑터 .tar.gz 파일을 ["NetApp 지원 사이트"](#)에서 다운로드해야 합니다.
- SRA 워크플로우를 실행하기 전에 소스 및 대상 ONTAP 클러스터 모두에 동일한 사용자 지정 SnapMirror 일정이 있어야 합니다.
- ["ONTAP tools for VMware vSphere 서비스 활성화"](#) SRA 기능을 활성화합니다.

단계

1. URL `https://<srn\_ip>:5480`을 사용하여 VMware Live Site Recovery 어플라이언스 관리 인터페이스에 로그인한 다음 VMware Live Site Recovery 어플라이언스 관리 인터페이스에서 Storage Replication Adapters로 이동합니다.
2. *새 어댑터*를 선택합니다.
3. SRA 플러그인용 .tar.gz 설치 프로그램을 VMware Live Site Recovery에 업로드하십시오.
4. VMware Live Site Recovery 스토리지 복제 어댑터 페이지에서 세부 정보가 업데이트되었는지 확인하려면 어댑터를 다시 스캔하십시오.



장애 조치 후에는 데이터 저장소에 대해 확장, 마운트 및 삭제와 같은 작업이 사용 불가능할 수 있습니다. 데이터 저장소 검색을 수행하여 컨텍스트 메뉴의 적절한 작업을 새로 고치고 표시하십시오.



재보호 작업을 수행할 때마다 양쪽 사이트 모두에서 스토리지 검색을 수행해야 합니다.

SRA 보호 기능을 사용하는 새로운 설정에서는 항상 테스트 페일오버를 실행해야 합니다. 테스트 페일오버를 건너뛰면 재보호 작업이 실패할 수 있습니다.

팬아웃 구성에서 자동 페일오버 듀플렉스 및 비동기 SnapMirror에 대해 SnapMirror 소스가 사이트 B로 변경되는

SnapMirror Active Sync 페일오버 후, 사이트 B와 C 간에 테스트 페일오버를 실행하십시오. 이 단계를 건너뛰면 재보호 작업이 실패할 수 있습니다.

관련 정보

["VMware Site Recovery Manager를 사용하여 NFS 데이터스토어에 대한 재해 복구 구성"](#)

SAN 및 NAS 환경용 ONTAP tools에서 SRA 구성

VMware Live Site Recovery용 스토리지 복제 어댑터(SRA)를 실행하기 전에 스토리지 시스템을 설정해야 합니다.

SAN 환경에 맞게 SRA 구성



SRA 워크플로의 일관성 그룹은 Unified 및 ASA r2 스토리지 시스템 모두에서 SAN 프로토콜(iSCSI 및 Fibre Channel)을 통해서만 지원됩니다.

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware Live Site Recovery: VMware 웹사이트에서는 VMware Live Site Recovery 설치 관련 문서를 제공합니다.

["VMware Live Site Recovery 정보"](#)

- SRA: VMware Live Site Recovery에 어댑터를 설치합니다.

iSCSI 프로토콜 구성의 경우 SRA 워크플로우를 실행하기 전에 다음 사항에 유의하십시오.

- 보호된 사이트: iSCSI 스토리지 어댑터 및 데이터 LIF 세부 정보는 데이터 저장소를 프로비저닝할 때 자동으로 구성됩니다. 수동 구성은 필요하지 않습니다.
- 복구 사이트: 재해 복구를 위한 리소스 매핑에 포함된 각 ESXi 호스트에서 iSCSI 스토리지 어댑터를 수동으로 구성해야 합니다. 각 호스트에서 어댑터를 개별적으로 구성하는 번거로움을 피하려면 SRA 워크플로가 구성된 SVM을 사용하여 복구 사이트에 iSCSI 유형의 자리 표시자 데이터 저장소를 생성하십시오. 이렇게 하면 iSCSI 어댑터와 필요한 데이터 LIF IP 주소가 매핑된 모든 ESXi 호스트에 자동으로 추가됩니다. 자세한 내용은 ["ONTAP tools에서 플레이스홀더 데이터 저장소를 구성합니다"](#)을(를) 참조하십시오.

단계

1. 보호 대상 사이트의 운영 스토리지 시스템에 있는 LUN에 운영 ESXi 호스트가 연결되어 있는지 확인하십시오.
2. 운영 스토리지 시스템에서 LUN이 `ostype` 옵션이 `_VMware_`로 설정된 `igroup`에 있는지 확인합니다.
3. 복구 사이트의 ESXi 호스트가 스토리지 가상 머신(SVM)에 대해 적절한 iSCSI 및 Fibre Channel 연결을 갖추고 있는지 확인하십시오. 보조 사이트의 ESXi 호스트는 보조 사이트 스토리지에 액세스할 수 있어야 하고, 기본 사이트의 ESXi 호스트는 기본 사이트 스토리지에 액세스할 수 있어야 합니다.

이 작업은 ESXi 호스트의 SVM에 로컬 LUN이 연결되어 있는지 확인하거나 `iscsi show initiators` SVM에서 명령을 실행하여 수행할 수 있습니다. iSCSI 연결을 확인하려면 ESXi 호스트에서 매핑된 LUN에 대한 LUN 액세스 권한을 확인하십시오.

NAS 환경에 대한 SRA 구성



SRA 워크플로에서 NFS에 대한 일관성 그룹은 지원되지 않습니다. NFS 데이터 저장소 볼륨이 일관성 그룹에 배치되고 보호되는 경우 장치 검색 작업이 실패합니다. SRA를 사용하여 NFS 데이터 저장소를 보호할 때는 일관성 그룹을 사용하지 마십시오.

시작하기 전에

보호 사이트와 복구 사이트에 다음 프로그램이 설치되어 있어야 합니다.

- VMware Live Site Recovery: VMware Live Site Recovery 설치 관련 문서는 VMware 웹사이트에서 확인하실 수 있습니다 - "[VMware Live Site Recovery 정보](#)"
- SRA: VMware Live Site Recovery 및 SRA 서버에 어댑터를 설치합니다.

단계

1. 보호 대상 사이트의 데이터 저장소에 vCenter Server에 등록된 가상 머신이 있는지 확인하십시오.
2. 보호 대상 사이트의 ESXi 호스트가 스토리지 가상 머신(SVM)에서 NFS 익스포트 볼륨을 마운트했는지 확인하십시오.
3. Array Manager 마법사를 사용하여 VMware Live Site Recovery에 어레이를 추가할 때 **NFS Addresses** 필드에 NFS 익스포트가 있는 유효한 IP 주소가 지정되어 있는지 확인하십시오. **NFS Addresses** 필드에 NFS 호스트 이름 또는 FQDN을 사용하지 마십시오.
4. 복구 사이트의 각 ESXi 호스트에서 ping 명령을 사용하여 호스트에 SVM에서 NFS 내보내기를 제공하는 데 사용되는 IP 주소에 액세스할 수 있는 VMkernel 포트가 있는지 확인하십시오.

확장성이 높은 환경을 위해 ONTAP tools에서 SRA를 구성합니다

대규모 환경에서 최적의 성능을 발휘하려면 스토리지 복제 어댑터(SRA)에 권장되는 설정에 따라 스토리지 시간 초과 간격을 구성해야 합니다.

스토리지 공급자 설정

확장된 환경을 위한 VMware Live Site Recovery의 시간 초과 값은 다음과 같이 설정해야 합니다.

고급 설정	타임아웃 값
StorageProvider.resignatureTimeout	설정값을 900초에서 12000초로 늘립니다.
storageProvider.hostRescanDelaySec	60
storageProvider.hostRescanRepeatCnt	20
storageProvider.hostRescanTimeoutSec	높은 값을 설정합니다(예: 99999).

해당 StorageProvider.autoResignatureMode 옵션도 활성화해야 합니다.

스토리지 공급자 설정 수정에 대한 자세한 내용은 "[스토리지 공급자 설정 변경](#)"를 참조하십시오.

스토리지 설정

타임아웃이 발생하면 `storage.commandTimeout` 및 `storage.maxConcurrentCommandCnt`의 값을 더 높은 값으로 늘리십시오.



지정된 타임아웃 간격은 최대값입니다. 최대 타임아웃 시간이 될 때까지 기다릴 필요는 없습니다. 대부분의 명령은 설정된 최대 타임아웃 간격 내에 완료됩니다.

SAN Provider 설정 수정에 대한 자세한 내용은 ["스토리지 설정 변경"](#)를 참조하십시오.

ONTAP tools를 사용하여 VMware Live Site Recovery 어플라이언스에서 SRA를 구성합니다

VMware Live Site Recovery 어플라이언스를 배포한 후 재해 복구 관리를 활성화하도록 스토리지 복제 어댑터(SRA)를 구성하십시오.

VMware Live Site Recovery 어플라이언스에서 SRA를 구성하면 VMware vSphere용 ONTAP tools 자격 증명이 어플라이언스 내에 저장되어 VMware Live Site Recovery와 SRA 간의 통신이 가능해집니다.

시작하기 전에

- `.tar.gz` 파일을 ["NetApp 지원 사이트"](#)에서 다운로드합니다.
- ONTAP tools Manager에서 SRA 서비스를 활성화하십시오. 자세한 내용은 ["서비스 활성화"](#) 섹션을 참조하십시오.
- vCenter 서버를 ONTAP tools for VMware vSphere 어플라이언스에 추가합니다. 자세한 내용은 ["vCenter 서버 추가"](#) 섹션을 참조하십시오.
- ONTAP tools for VMware vSphere에 스토리지 백엔드를 추가합니다. 자세한 내용은 ["스토리지 백엔드 추가"](#) 섹션을 참조하십시오.



ONTAP tools에서 vCenter 인증서 패치를 적용한 경우, (:5480) 포트를 사용하여 VMware Live Site Recovery 어플라이언스에서 vCenter 구성을 업데이트하십시오. 자세한 내용은 ["Site Recovery Manager 어플라이언스 재구성"](#)을 참조하십시오.

단계

1. VMware Live Site Recovery 어플라이언스 화면에서 스토리지 복제 어댑터 > *새 어댑터*를 선택합니다.
2. `.tar.gz` 파일을 VMware Live Site Recovery에 업로드하십시오.
3. PuTTY와 같은 SSH 클라이언트를 사용하여 관리자 계정으로 VMware Live Site Recovery 어플라이언스에 로그인합니다.
4. 다음 명령을 사용하여 루트 사용자로 전환합니다: `su root`
5. 명령을 실행하여 `cd /var/log/vmware/srm` 로그 디렉토리로 이동합니다.
6. 로그 위치에서 SRA에서 사용하는 Docker ID를 얻으려면 다음 명령을 입력하십시오. `docker ps -l`
7. 컨테이너 ID에 로그인하려면 다음 명령을 입력합니다. `docker exec -it -u srm <container id> sh`
8. 다음 명령을 사용하여 VMware Live Site Recovery를 ONTAP tools for VMware vSphere IP 주소 및 암호로 구성하십시오: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`

- 암호를 입력할 때 작은따옴표로 묶어야 Perl 스크립트가 특수 문자를 구분 기호가 아닌 암호의 일부로 처리합니다.
- 처음 서비스를 활성화할 때 ONTAP tools Manager에서 애플리케이션(VASA Provider/SRA) 사용자 이름과 암호를 설정할 수 있습니다. 이 자격 증명을 사용하여 SRA를 VMware Live Site Recovery에 등록하십시오.
- vCenter GUID를 찾으려면 vCenter 인스턴스를 추가한 후 ONTAP tools Manager의 vCenter 서버 페이지로 이동하십시오. "[vCenter 서버 추가](#)" 섹션을 참조하십시오.

9. 업데이트된 세부 정보가 VMware Live Site Recovery 스토리지 복제 어댑터 페이지에 표시되는지 확인하려면 어댑터를 다시 스캔하십시오.

결과 스토리지 자격 증명이 저장되었음을 나타내는 확인 메시지가 나타납니다. 이제 지정된 IP 주소, 포트 및 자격 증명을 사용하여 SRA로 SRA 서버와 통신할 수 있습니다.

ONTAP tools에서 SRA 자격 증명 업데이트

VMware Live Site Recovery가 SRA와 통신하려면 자격 증명을 수정한 경우 VMware Live Site Recovery 서버에서 SRA 자격 증명을 업데이트해야 합니다.

시작하기 전에

해당 항목에 언급된 단계를 실행했어야 합니다 "[VMware Live Site Recovery 어플라이언스에서 SRA 구성](#)".

단계

1. VMware Live Site Recovery 시스템에서 캐시된 ONTAP tools 자격 증명을 삭제하려면 다음 명령을 실행하십시오.

- `sudo su <enter root password>`
- `docker ps`
- `docker exec -it <container_id> sh`
- `cd conf/`
- `rm -rf *`

2. 새 자격 증명으로 SRA를 구성하려면 Perl 명령을 실행하십시오.

- `cd ..`
- `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` 비밀번호 값 주위에 작은따옴표(')를 붙여야 합니다.

스토리지 자격 증명이 저장되었음을 확인하는 성공 메시지가 표시됩니다. SRA는 제공된 IP 주소, 포트 및 자격 증명을 사용하여 SRA 서버와 통신할 수 있습니다.

인증서 변경 후 **VMware Live Site Recovery** 어플라이언스에서 **vCenter** 재구성

vCenter 인증서가 변경되는 경우(예: vCenter 업그레이드 후) Site Recovery 확장 프로그램에서 지문 불일치 오류가 발생할 수 있습니다. 다음 단계를 수행하여 이 문제를 해결하십시오.

단계

1. VMware Live Site Recovery 어플라이언스에서 vCenter 재구성

- a. 브라우저에서 VMware Live Site Recovery 어플라이언스 관리 인터페이스를 엽니다.
https://<SRM_IP>:5480
- b. * 요약 * 탭을 선택합니다.
- c. vCenter Server 연결에 대해 *재구성*을 선택하십시오.

이 작업은 vCenter에서 최신 인증서 지문을 가져와 수락합니다.

2. 사이트 페어링 재연결(오류가 지속되는 경우)

재구성 후에도 지문 불일치 오류가 계속 발생하는 경우:

- a. vCenter 사용자 인터페이스에 로그인합니다.
- b. **Site Recovery** 확장 프로그램으로 이동합니다.
- c. **Site Pairing** 섹션을 찾으십시오.
- d. 업데이트된 인증서를 사용하여 사이트 페어링을 다시 설정하려면 *다시 연결*을 선택하십시오.

ONTAP tools에서 보호 사이트 및 복구 사이트를 구성합니다

보호 대상 사이트에서 가상 머신 그룹을 보호하려면 보호 그룹을 생성해야 합니다.

새 데이터스토어를 추가할 때 기존 데이터스토어 그룹에 포함시키거나, 새 데이터스토어를 추가하고 보호를 위해 새 볼륨 또는 일관성 그룹을 생성할 수 있습니다. 보호된 일관성 그룹 또는 볼륨에 새 데이터스토어를 추가한 후에 SnapMirror를 업데이트하고 보호 사이트와 복구 사이트 모두에서 스토리지 검색을 수행해야 합니다. 새 데이터스토어가 감지되고 보호되도록 검색을 수동으로 또는 예약된 시간에 실행할 수 있습니다.

보호된 사이트와 복구 사이트 페어링

vSphere Client를 사용하여 생성한 보호 사이트와 복구 사이트를 연결하여 스토리지 복제 어댑터(SRA)가 스토리지 시스템을 검색할 수 있도록 해야 합니다.



스토리지 복제 어댑터(SRA)는 일관성 그룹에서 Automated Failover Duplex 유형의 동기 관계 하나와 비동기 SnapMirror 관계를 사용하여 팬아웃을 지원합니다. 그러나 일관성 그룹에서 두 개의 비동기 SnapMirror 관계를 사용하거나 볼륨에서 SnapMirror 관계를 사용하여 팬아웃하는 것은 지원되지 않습니다. Vault 유형의 SnapMirror 관계는 이러한 팬아웃 제한에 포함되지 않습니다. SRA의 일관성 그룹 지원은 Unified 및 ASA r2 스토리지 시스템의 SAN 프로토콜(iSCSI 및 파이버 채널)로 제한됩니다. NFS의 경우 일관성 그룹이 지원되지 않습니다. NFS 데이터스토어 볼륨이 일관성 그룹에 속한 경우 장치 검색 작업이 실패합니다.

시작하기 전에

- 보호 대상 사이트와 복구 사이트 모두에 VMware Live Site Recovery가 설치되어 있어야 합니다.
- 보호 사이트와 복구 사이트 모두에 SRA가 설치되어 있어야 합니다.

단계

1. vSphere Client 홈 페이지에서 사이트 복구 아이콘을 두 번 클릭한 다음 *사이트*를 선택합니다.
2. 개체 > 작업 > *사이트 페어링*을 선택합니다.
3. **Pair Site Recovery Manager Servers** 대화 상자에서 보호 대상 사이트의 Platform Services Controller 주소를 입력한 다음 *다음*을 선택합니다.

4. Select vCenter Server 섹션에서 다음 작업을 수행합니다.
 - a. 보호 대상 사이트의 vCenter Server가 페어링 대상 후보로 표시되는지 확인하십시오.
 - b. SSO 관리자 자격 증명을 입력한 다음 *완료*를 선택하십시오.
5. 보안 인증서를 수락하라는 메시지가 표시되면 *예*를 선택하십시오.

결과

개체 대화 상자에는 보호된 사이트와 복구 사이트가 모두 표시됩니다.

보호 그룹 구성

시작하기 전에

소스 사이트와 대상 사이트 모두 다음 사항에 맞게 구성되어 있는지 확인해야 합니다.

- 동일한 버전의 VMware Live Site Recovery가 설치되어 있습니다.
- 가상 머신
- 쌍을 이루는 보호 사이트 및 복구 사이트
- 원본 및 대상 데이터 저장소는 각각의 사이트에 마운트되어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *보호 그룹*을 선택합니다.
2. 보호 그룹 창에서 *새로 만들기*를 선택합니다.
3. 보호 그룹의 이름과 설명을 지정하고 방향을 선택한 다음 *다음*을 선택하십시오.
4. **Type** 필드에서 NFS 및 VMFS 데이터 저장소에 대해 *Type field option...*을 데이터 저장소 그룹(어레이 기반 복제)으로 선택합니다. 장애 도메인은 복제가 활성화된 SVM으로 구성됩니다. 피어링만 구현되어 있고 문제가 없는 SVM이 표시됩니다.
5. 복제 그룹 탭에서 활성화된 어레이 쌍 또는 구성한 가상 머신이 포함된 복제 그룹을 선택한 다음 *다음*을 선택합니다.

복제 그룹에 있는 모든 가상 머신이 보호 그룹에 추가됩니다.

6. 기존 복구 계획을 선택하거나 *새 복구 계획에 추가*를 선택하여 새 복구 계획을 생성할 수 있습니다.
7. Ready to complete 탭에서 생성한 보호 그룹의 세부 정보를 검토한 다음 *Finish*를 선택합니다.

보호 사이트 및 복구 사이트 리소스 구성

ONTAP tools에서 네트워크 매핑을 구성합니다

보호 사이트의 각 리소스를 복구 사이트의 적절한 리소스에 매핑할 수 있도록 양쪽 사이트에서 VM 네트워크, ESXi 호스트 및 폴더와 같은 리소스 매핑을 구성해야 합니다.

다음 리소스 구성을 완료해야 합니다.

- 네트워크 매핑
- 폴더 매핑

- 리소스 매핑
- 자리 표시자 데이터 저장소

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 관리 탭에서 네트워크 매핑 > *새로 만들기*를 선택하여 새 네트워크 매핑을 생성합니다.
4. 네트워크 매핑 생성 마법사에서 다음을 수행하십시오.
 - a. *일치하는 이름을 가진 네트워크에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

네트워크 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 네트워크에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 폴더 매핑을 구성합니다

보호 사이트와 복구 사이트 간의 통신을 가능하게 하려면 두 사이트의 폴더를 매핑해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 새 폴더 매핑을 만들려면 관리 탭에서 폴더 매핑 > 폴더 아이콘을 선택합니다.
4. 폴더 매핑 생성 마법사에서 다음 단계를 수행하십시오.
 - a. *이름이 일치하는 폴더에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

폴더 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 폴더에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 리소스 매핑을 구성합니다

보호 사이트와 복구 사이트의 리소스를 매핑하여 가상 머신이 두 호스트 그룹 중 하나로 장애 조치되도록 구성해야 합니다.

시작하기 전에

보호 사이트와 복구 사이트를 연결했어야 합니다.



VMware Live Site Recovery에서 리소스는 리소스 풀, ESXi 호스트 또는 vSphere 클러스터일 수 있습니다.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 관리 탭에서 리소스 매핑 > *새로 만들기*를 선택하여 새 리소스 매핑을 생성합니다.
4. 리소스 매핑 생성 마법사에서 다음 단계를 수행하십시오.
 - a. *일치하는 이름을 가진 리소스에 대한 매핑을 자동으로 준비*를 선택하고 *다음*을 선택합니다.
 - b. 보호 사이트와 복구 사이트에 필요한 데이터 센터 개체를 선택하고 *매핑 추가*를 선택합니다.
 - c. 매핑이 성공적으로 생성되면 *다음*을 선택합니다.
 - d. 이전에 역매핑을 생성하는 데 사용했던 개체를 선택한 다음 *완료*를 선택합니다.

결과

리소스 매핑 페이지에는 보호된 사이트 리소스와 복구 사이트 리소스가 표시됩니다. 환경 내 다른 리소스에 대해서도 동일한 단계를 따르면 됩니다.

ONTAP tools에서 플레이스홀더 데이터 저장소를 구성합니다

보호 대상 가상 머신(VM)을 위해 복구 사이트의 vCenter 인벤토리에 공간을 예약하려면 자리 표시자 데이터 저장소를 구성하십시오. 자리 표시자 VM은 크기가 작고 일반적으로 수백 킬로바이트만 사용하므로 자리 표시자 데이터 저장소에는 최소한의 용량만 필요합니다.

시작하기 전에

- 보호 사이트와 복구 사이트가 연결되어 있는지 확인하십시오.
- 리소스 매핑이 구성되었는지 확인하십시오.

단계

1. vCenter Server에 로그인하고 사이트 복구 > *사이트*를 선택합니다.
2. 보호된 사이트를 선택하고 *관리*를 선택합니다.
3. 관리 탭에서 **Placeholder Datastores** > *New*를 선택하여 새 플레이스홀더 데이터 저장소를 생성합니다.
4. 적절한 데이터 저장소를 선택하고 *확인*을 선택하십시오.



플레이스홀더 데이터스토어는 로컬 또는 원격 스토리지에 있을 수 있지만 복제는 필요하지 않습니다.

5. 3단계부터 5단계까지를 반복하여 복구 사이트에 대한 자리 표시자 데이터 저장소를 구성합니다.

ONTAP 도구의 어레이 관리자를 사용하여 **SRA**를 구성합니다

VMware Live Site Recovery와 스토리지 가상 머신(SVM) 간의 상호 작용을 활성화하려면 VMware Live Site Recovery의 어레이 관리자 마법사를 사용하여 SRA(Storage Replication Adapter)를 구성할 수 있습니다.

시작하기 전에

- VMware Live Site Recovery에서 보호 사이트와 복구 사이트를 페어링했어야 합니다.
- 어레이 관리자를 구성하기 전에 온보딩된 스토리지를 먼저 구성해야 합니다.
- 보호 대상 사이트와 복구 사이트 간의 SnapMirror 관계를 구성하고 복제했어야 합니다.
- 멀티테넌시를 활성화하려면 SVM 관리 LIF를 활성화해야 합니다.

SRA는 클러스터 수준 관리와 SVM 수준 관리를 지원합니다. 클러스터 수준에서 스토리지를 추가하면 클러스터 내의 모든 SVM을 검색하고 작업을 수행할 수 있습니다. SVM 수준에서 스토리지를 추가하면 해당 SVM만 관리할 수 있습니다.

단계

1. VMware Live Site Recovery에서 **Array Managers** > *Add Array Manager*를 선택합니다.
2. VMware Live Site Recovery에서 어레이를 설명하려면 다음 정보를 입력하십시오.
 - a. 표시 이름 필드에 어레이 관리자를 식별할 이름을 입력하십시오.
 - b. **SRA** 유형 필드에서 *NetApp Storage Replication Adapter for ONTAP*를 선택합니다.
 - c. 클러스터 또는 SVM에 연결하기 위한 정보를 입력하십시오.
 - 클러스터에 연결하는 경우 클러스터 관리 LIF를 입력해야 합니다.
 - SVM에 직접 연결하는 경우 SVM 관리 LIF의 IP 주소를 입력해야 합니다.



어레이 관리자를 구성할 때는 ONTAP tools for VMware vSphere에서 스토리지 시스템을 온보딩하는 데 사용된 것과 동일한 연결(IP 주소)을 스토리지 시스템에 사용해야 합니다. 예를 들어, 어레이 관리자 구성이 SVM 범위로 설정된 경우 ONTAP tools for VMware vSphere의 스토리지는 SVM 레벨에서 추가해야 합니다.

- d. 클러스터에 연결하는 경우 **SVM** 이름 필드에 SVM 이름을 지정하거나, 클러스터의 모든 SVM을 관리하려면 비워 두십시오.
- e. 검색할 볼륨을 포함할 볼륨 목록 필드에 입력하십시오.

보호 사이트에 소스 볼륨을 입력하고 복구 사이트에 복제 대상 볼륨을 입력할 수 있습니다.

예를 들어 볼륨 dst_vol1과 SnapMirror 관계로 연결된 볼륨 src_vol1을 검색하려면 보호 사이트 필드에 src_vol1을, 복구 사이트 필드에 dst_vol1을 지정해야 합니다.

- f. (선택 사항) 검색에서 제외할 볼륨을 볼륨 제외 목록 필드에 입력하십시오.

보호 사이트에 소스 볼륨을 입력하고 복구 사이트에 복제 대상 볼륨을 입력할 수 있습니다.

예를 들어, 볼륨 `_dst_vol1_`과 SnapMirror 관계로 연결된 볼륨 `_src_vol1_`을 제외하려면 보호 사이트 필드에 `_src_vol1_`을, 복구 사이트 필드에 `_dst_vol1_`을 지정해야 합니다.

3. *다음*을 선택하십시오.
4. 어레이가 검색되어 어레이 관리자 추가 창 하단에 표시되는지 확인하고 *마침*을 선택합니다.

적절한 SVM 관리 IP 주소와 자격 증명을 사용하여 복구 사이트에 대해서도 동일한 단계를 수행할 수 있습니다. 어레이 관리자 추가 마법사의 어레이 쌍 활성화 화면에서 올바른 어레이 쌍이 선택되었는지, 그리고 활성화 준비가 완료되었는지 확인해야 합니다.

ONTAP tools에서 복제된 스토리지 시스템을 검증합니다

스토리지 복제 어댑터(SRA)를 구성한 후 보호 사이트와 복구 사이트가 성공적으로 페어링되었는지 확인해야 합니다. 복제된 스토리지 시스템은 보호 사이트와 복구 사이트 모두에서 검색 가능해야 합니다.

시작하기 전에

- 스토리지 시스템을 구성해야 합니다.
- VMware Live Site Recovery 어레이 관리자를 사용하여 보호 사이트와 복구 사이트를 페어링했어야 합니다.
- FlexClone 라이선스와 SnapMirror 라이선스는 SRA에 대한 테스트 페일오버 작업 및 페일오버 작업을 수행하기 전에 활성화해야 합니다.
- 원본 사이트와 대상 사이트에 동일한 SnapMirror 정책 및 일정이 설정되어 있어야 합니다.
- 사용자 지정 일정을 사용하는 사용자 지정 SnapMirror 정책을 사용하는 경우 보호 사이트와 복구 사이트 모두에 동일한 일정과 정책을 구성해야 합니다.
- 사용자 지정 SnapMirror 정책(기본 일정 또는 사용자 지정 일정)을 사용하는 경우 새 정책이 인식되도록 ONTAP tools에서 스토리지 검색을 수행해야 합니다. 그렇지 않으면 테스트 페일오버 및 페일오버를 포함한 SRA 워크플로가 실패합니다. 다음 시점에서 스토리지 검색을 수행하십시오.
 - 복구 사이트에서 사용자 지정 정책을 생성한 후
 - 재보호 작업 후에는 보호 대상 사이트에 정책이 다시 생성됩니다.

단계

1. vCenter 서버에 로그인하십시오.
2. **Site Recovery > Array Based Replication** 으로 이동합니다.
3. 필요한 어레이 쌍을 선택하고 해당 세부 정보를 확인하십시오.

스토리지 시스템은 보호 사이트와 복구 사이트에서 **Enabled** 상태로 검색되어야 합니다.

ONTAP 도구의 팬아웃 보호

팬아웃 보호 시나리오에서 일관성 그룹은 첫 번째 대상 ONTAP 클러스터에서는 동기 관계를, 두 번째 대상 ONTAP 클러스터에서는 비동기 관계를 통해 이중으로 보호됩니다. SnapMirror 활성화 동기화 보호 워크플로(생성, 편집, 삭제)는 동기 보호를 유지합니다. VMware Live Site Recovery 어플라이언스 장애 조치 및 재보호 워크플로는 비동기 보호를 유지합니다.



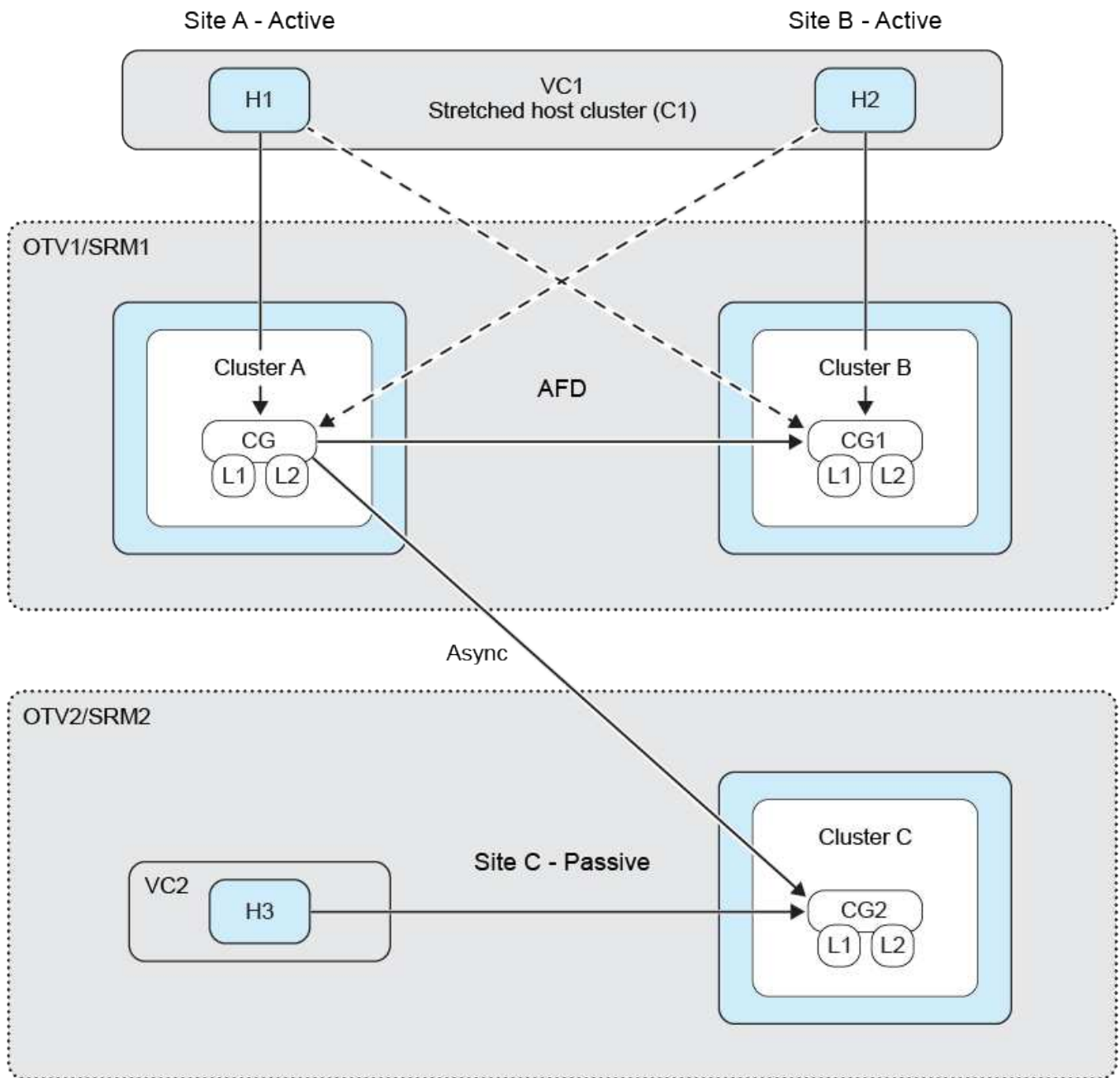
SVM 사용자에게 대해서는 팬아웃이 지원되지 않습니다.

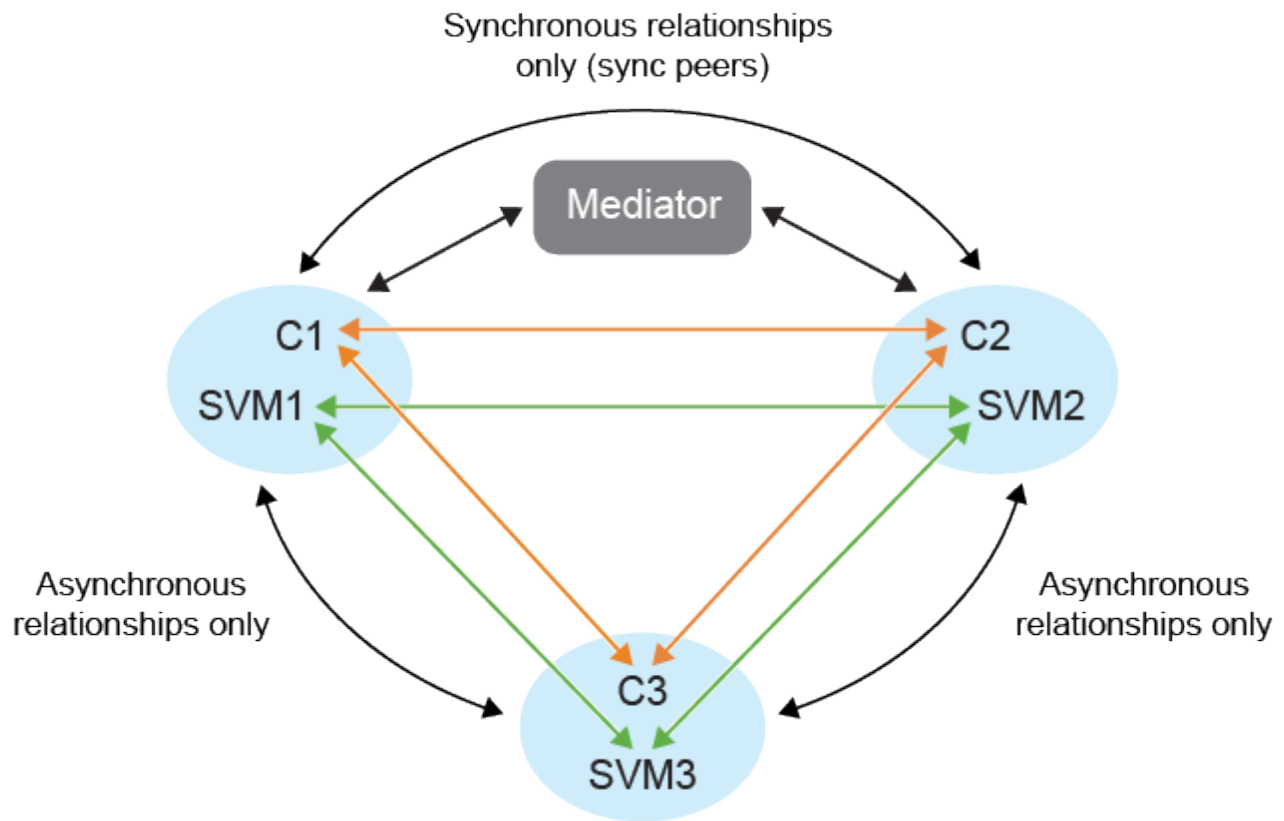
팬아웃 보호를 설정하려면 세 사이트 클러스터와 SVM을 피어링해야 합니다.

예:

만약에	그 다음에
- 소스 일관성 그룹은 클러스터 c1 및 SVM svm1에 있습니다. - 첫 번째 대상 일관성 그룹은 클러스터 c2와 SVM svm2에 있습니다. - 두 번째 대상 일관성 그룹은 클러스터 c3 및 SVM svm3에 있습니다.	- 소스 ONTAP 클러스터의 클러스터 피어링은 (C1, C2) 및 (C1, C3)이 됩니다. - 첫 번째 대상 ONTAP 클러스터에서의 클러스터 피어링은 (C2, C1) 및 (C2, C3)이 될 것이며 - 두 번째 대상 ONTAP 클러스터의 클러스터 피어링은 (C3, C1) 및 (C3, C2)가 됩니다. - 소스 SVM에 대한 SVM 피어링은 (svm1, svm2) 및 (svm1, svm3)이 됩니다. - 첫 번째 목적지 SVM에 대한 SVM 피어링은 (svm2, svm1) 및 (svm2, svm3)이 되고 - 두 번째 대상 SVM에 대한 SVM 피어링은 (svm3, svm1) 및 (svm3, svm2)가 됩니다.

다음 다이어그램은 팬아웃 보호 구성을 보여 줍니다.





단계

1. 새로운 임시 데이터 저장소를 선택하십시오. 단계별 보호를 위한 임시 데이터 저장소 선택 기준은 다음과 같습니다.
 - 보호 대상 호스트 클러스터에 자리 표시자 데이터 저장소를 배치하지 마십시오.
 - 호스트 클러스터에 자리 표시자 데이터 저장소를 포함해야 하는 경우 SnapMirror 활성 동기화 보호를 설정하기 전에 VMware Live Site Recovery 어플라이언스에 추가하십시오. 이렇게 설정하면 자리 표시자 데이터 저장소를 보호 대상에서 제외할 수 있습니다.

자세한 내용은 "[자리 표시자 데이터 저장소 선택](#)"을(를) 참조하십시오.
2. "[보호된 호스트 클러스터 수정](#)"에 따라 호스트 클러스터 보호에 데이터 저장소를 추가하십시오. 비동기 및 동기 정책 유형을 모두 추가하십시오.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.