ASA r2 설명서

ASA r2

NetApp
February 25, 2026

목차

ASA r2 설명서 1
릴리스 정보 2
ASA r2 시스템용 ONTAP 9.18.1의 새로운 기능 2
데이터 보호 2
네트워킹 2
SAN 데이터 마이그레이션 2
보안 2
스토리지 효율성 2
ASA r2 시스템용 ONTAP 9.17.1의 새로운 기능 3
SAN 데이터 마이그레이션 3
데이터 보호 3
스토리지 관리 3
ASA R2 시스템을 위한 ONTAP 9.16.1의 새로운 기능 4
시스템 4
데이터 보호 4
프로토콜 지원 4
스토리지 효율성 4
ASA R2 시스템을 위한 ONTAP 9.16.0의 새로운 기능 5
시스템 5
시스템 관리자 5
스토리지 관리 5
데이터 보안 6
ASA R2 시스템에 영향을 주는 ONTAP 제한 및 기본값 변경 6
ONTAP 제한 변경 사항 6
시작하십시오 7
ASA R2 스토리지 시스템에 대해 알아보십시오 7
ASA R2 스토리지 시스템의 빠른 시작 8
ASA R2 시스템을 설치합니다 8
ASA R2 스토리지 시스템의 설치 및 설정 워크플로우 8
ASA R2 스토리지 시스템의 설치 요구 사항 9
ASA R2 스토리지 시스템 설치를 준비합니다 11
ASA R2 스토리지 시스템을 설치합니다 14
ASA R2 스토리지 시스템용 하드웨어를 케이블로 연결합니다 15
ASA R2 스토리지 시스템의 전원을 켭니다 49
ASA R2 시스템을 설정합니다 55
ASA R2 스토리지 시스템에서 ONTAP 클러스터를 설정합니다 55
ASA R2 시스템을 사용한 SAN 호스트 구성 57
SAN 호스트에서 ASA R2 스토리지 시스템으로의 데이터 액세스가 가능합니다 58
ONTAP를 사용하여 데이터를 관리합니다 60

ASA R2 스토리지 시스템 비디오 데모 60
스토리지 관리 60
ASA R2 시스템에서 ONTAP SAN 스토리지를 프로비저닝합니다 60
ASA R2 스토리지 시스템에 데이터를 복제합니다 66
호스트 그룹 관리 70
스토리지 유닛 관리 71
스토리지 VM 마이그레이션 73
ASA R2 스토리지 제한 78
데이터 보호 79
스냅샷을 생성하여 ASA R2 스토리지 시스템에 데이터를 백업합니다 79
스냅샷 예약 관리 84
ASA r2 스토리지 시스템에서 클러스터 간 스토리지 VM 피어 관계 생성 86
스냅샷 복제를 설정합니다 86
SnapMirror Active Sync 설정 92
SnapMirror 활성 동기화 관리 96
ASA R2 스토리지 시스템에서 데이터를 복구합니다 100
일관성 그룹을 관리합니다 102
ASA R2 스토리지 시스템에서 ONTAP 데이터 보호 정책 및 일정을 관리합니다 109
데이터 보호 111
ASA R2 스토리지 시스템에서 유휴 데이터를 암호화합니다 111
ONTAP R2 시스템의 주요 관리자 간에 ASA 데이터 암호화 키를 마이그레이션합니다 112
랜섬웨어 공격을 방어하십시오 114
ASA R2 스토리지 시스템에서 NVMe 연결을 보호합니다 120
ASA R2 스토리지 시스템에서 IP 연결을 보호합니다 120
관리 및 모니터링 122
ONTAP 업그레이드 및 되돌리기 122
ASA R2 스토리지 시스템에서 ONTAP를 업그레이드합니다 122
ASA r2 스토리지 시스템에서 ONTAP 되돌리기 122
ASA R2 스토리지 시스템에서 펌웨어를 업데이트합니다 123
ASA R2 스토리지 시스템에서 스토리지 VM에 대한 클라이언트 액세스를 관리합니다 124
스토리지 VM을 생성합니다 125
IPspace 생성 125
서브넷을 생성합니다 126
LIF(네트워크 인터페이스) 생성 126
LIF(네트워크 인터페이스) 수정 129
ASA R2 스토리지 시스템에서 클러스터 네트워킹을 관리합니다 130
브로드캐스트 도메인을 추가합니다 130
포트를 다른 브로드캐스트 도메인에 재할당합니다 131
VLAN을 생성합니다 131
사용량을 모니터링하고 용량을 늘립니다 132
ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 성능을 모니터링합니다 132

ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 활용도를 모니터링합니다 133
ASA R2 스토리지 시스템에서 스토리지 용량을 늘립니다 134
ASA R2 스토리지 시스템 인사이트를 통해 클러스터 보안 및 성능을 최적화합니다 135
ASA R2 스토리지 시스템에서 클러스터 이벤트 및 작업을 봅니다 136
클러스터 이벤트 및 감사 로그에 대한 이메일 알림을 보냅니다 137
노드 관리 137
ASA R2 노드를 ONTAP 클러스터에 추가합니다 137
ASA R2 스토리지 시스템에서 노드를 재부팅합니다 138
ASA R2 스토리지 시스템에서 노드 이름을 바꿉니다 138
ASA R2 스토리지 시스템에서 사용자 계정 및 역할을 관리합니다 138
Active Directory 도메인 컨트롤러 액세스를 구성합니다 139
LDAP를 구성합니다 139
SAML 인증을 구성합니다 139
사용자 계정 역할을 생성합니다 140
관리자 계정을 만듭니다 140
ASA R2 스토리지 시스템에서 보안 인증서를 관리합니다 141
인증서 서명 요청을 생성합니다 141
신뢰할 수 있는 인증 기관을 추가합니다 141
신뢰할 수 있는 인증 기관을 갱신하거나 삭제합니다 141
클라이언트/서버 인증서 또는 로컬 인증 기관을 추가합니다 142
클라이언트/서버 인증서 또는 로컬 인증 기관을 갱신하거나 삭제합니다 142
ASA R2 스토리지 시스템에서 호스트 접속을 확인합니다 143
ASA R2 스토리지 시스템을 유지 관리합니다 144
자세한 정보 145
ONTAP 파워 유저를 위한 ASA R2 145
ASA R2 시스템을 다른 ONTAP 시스템과 비교합니다 145
ASA R2 스토리지 시스템에 대한 ONTAP 소프트웨어 지원 및 제한 사항 147
ASA R2 스토리지 시스템에 대한 ONTAP CLI 지원 148
ASA R2에 대한 REST API 지원 153
ASA r2 시스템에서 지원되는 일반적인 ONTAP 기능 155
데이터 보호 155
데이터 보안 155
네트워킹 156
SAN 프로토콜 156
시스템 관리자 157
도움을 받으십시오 158
ASA R2 스토리지 시스템에서 AutoSupport를 관리합니다 158
AutoSupport 연결을 테스트합니다 158
AutoSupport 받는 사람을 추가합니다 158
AutoSupport 데이터를 전송합니다 159
지원 케이스 생성을 억제합니다 159

지원 케이스 생성을 재개합니다 . . . 159
ASA R2 스토리지 시스템에 대한 지원 사례를 제출하고 확인합니다 . . . 159
법적 고지 . . . 161
저작권 . . . 161
상표 . . . 161
특허 . . . 161
개인 정보 보호 정책 . . . 161
오픈 소스 . . . 161
ONTAP . . . 161

ASA r2 설명서

릴리스 정보

ASA r2 시스템용 ONTAP 9.18.1의 새로운 기능

ASA r2 시스템을 위한 ONTAP 9.18.1에서 사용할 수 있는 새로운 기능에 대해 알아보세요.

데이터 보호

업데이트	설명
"SnapMirror Active Sync 구성에 대한 지원이 향상되었습니다."	SnapMirror Active Sync에 대한 지원이 2노드 클러스터에서 4노드 클러스터로 증가했습니다.

네트워킹

업데이트	설명
"IPsec 하드웨어 오프로드 IPv6 지원"	IPsec 하드웨어 오프로드 지원이 IPv6로 확장되었습니다.
"OpenSSL PQC 알고리즘"	ONTAP SSL을 위한 포스트퀀텀 컴퓨팅 암호화 알고리즘을 지원합니다. 이러한 알고리즘은 미래의 양자 컴퓨팅 공격에 대한 추가적인 보호 기능을 제공하며, SSL FIPS 모드가 비활성화된 경우 사용할 수 있습니다.

SAN 데이터 마이그레이션

업데이트	설명
"스토리지 VM 마이그레이션 지원"	ASA 클러스터에서 ASA r2 클러스터로 스토리지 가상 머신(VM)을 중단 없이 마이그레이션할 수 있습니다. 이를 통해 데이터 무결성을 유지하고 애플리케이션에 영향을 미치지 않으면서 블록 워크로드를 ASA r2 시스템으로 옮길 수 있습니다. 마이그레이션 프로세스는 기존 호스트 매핑과 LUN 구성을 유지하도록 설계되어 마이그레이션 중 운영상의 노력과 위험을 줄여줍니다.

보안

업데이트	설명
"자동 ARP/AI 활성화 지원"	새로운 9.18.1 ASA r2 클러스터를 초기화하거나 클러스터를 9.18.1로 업그레이드하면 12시간의 유예 기간 후 새로 생성된 모든 스토리지 유닛에서 ARP/AI가 기본적으로 자동 활성화됩니다. 유예 기간 동안 ARP/AI를 비활성화하지 않으면 유예 기간이 종료될 때 새로 생성된 스토리지 유닛에 대해 클러스터 전체에서 활성화됩니다.

스토리지 효율성

업데이트	설명
"NVMe 복사 오프로드 지원"	NVMe 복사 오프로드를 사용하면 NVMe 호스트가 CPU에서 ONTAP 스토리지 컨트롤러의 CPU로 복사 작업을 오프로드할 수 있습니다. 호스트는 애플리케이션 워크로드를 위해 CPU 리소스를 예약하는 동시에 한 NVMe 네임스페이스에서 다른 네임스페이스로 데이터를 복사할 수 있습니다.
"스냅샷 예약 수정 및 자동 스냅샷 삭제 지원"	스냅샷 예약을 수정하고 자동 스냅샷 삭제를 활성화하여 ASA r2 스토리지 유닛에서 스냅샷에 사용되는 공간의 양을 제한할 수 있습니다. 스냅샷 예약이 자동 스냅샷 삭제로 설정된 경우, 스냅샷에 사용된 공간이 스냅샷 예약 공간을 초과하면 오래된 스냅샷이 자동으로 삭제됩니다. 이렇게 하면 사용자 데이터를 위한 저장 장치의 공간을 스냅샷이 차지하지 못하게 하여 애플리케이션 중단을 방지할 수 있습니다.

ASA r2 시스템용 ONTAP 9.17.1의 새로운 기능

ASA r2 시스템을 위한 ONTAP 9.17.1에서 사용할 수 있는 새로운 기능에 대해 알아보세요.

SAN 데이터 마이그레이션

업데이트	설명
"타사 스토리지 시스템에서 데이터 마이그레이션 지원"	ASA r2 시스템에서는 FLI(Foreign LUN Import)를 사용한 SAN 데이터 마이그레이션이 지원됩니다. FLI를 사용하면 타사 스토리지 시스템의 LUN에서 ASA r2 시스템으로 데이터를 마이그레이션할 수 있습니다.

데이터 보호

업데이트	설명
"인공 지능(ARP/AI)을 통한 자율 랜섬웨어 보호 지원"	ARP/AI는 ASA r2 스토리지 유닛에서 활성화할 수 있습니다. ARP/AI는 학습 기간 없이 잠재적인 랜섬웨어 공격을 탐지하고 보고하여 추가적인 데이터 보호 기능을 제공합니다.
"NVMe 프로토콜에 대한 SnapMirror Active Sync 지원"	SnapMirror Active Sync는 2노드 ONTAP 클러스터에 대해 NVMe/TCP 및 NVMe/FC 호스트 액세스를 사용하는 VMware 워크로드 지원을 추가합니다. VMware 워크로드의 NVMe/TCP 지원은 VMware 버그 ID: TR1049746 해결 여부에 따라 달라집니다
"복제 관계에서 일관성 그룹에 대한 지오메트리 변경 지원"	ASA r2 시스템은 SnapMirror 활성 동기화 관계나 비동기 복제 관계에서 일관성 그룹에 대한 기하학적 변경을 지원하며, SnapMirror 활성 동기화 관계를 삭제하거나 비동기 관계를 끊지 않습니다. 기본 일관성 그룹에서 기하학적 변경이 발생하면 변경 사항이 보조 일관성 그룹에 복제됩니다.
"자식 일관성 그룹의 비동기 복제 지원"	비동기 복제 정책은 계층적 관계의 일관성 그룹에 적용될 수 있습니다.

스토리지 관리

업데이트	설명
"자동 작업 부하 분산 지원"	HA 쌍의 노드 간에 작업 부하가 자동으로 균형을 이루어 성능과 리소스 활용도가 최적화됩니다.

ASA R2 시스템을 위한 ONTAP 9.16.1의 새로운 기능

ASA R2 시스템을 위한 ONTAP 9.16.1에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

시스템

업데이트	설명
시스템	다음 NetApp ASA r2 시스템은 ONTAP 9.16.1부터 지원됩니다. 이러한 시스템은 SAN 전용 고객의 요구 사항에 맞춰 간소화된 환경을 만드는 통합 하드웨어 및 소프트웨어 솔루션을 제공합니다. • ASA A50 • ASA A30 • ASA A20 • ASA C30

데이터 보호

업데이트	설명
"키 관리자 간 암호화 키 마이그레이션 지원"	ONTAP 온보드 키 관리자에서 클러스터 수준의 외부 키 관리자로 전환할 경우 ONTAP CLI(Command Line Interface)를 사용하여 한 키 관리자에서 다른 키 관리자로 암호화 키를 손쉽게 마이그레이션할 수 있습니다.
"계층적 정합성 보장 그룹 지원"	계층적 일관성 그룹을 사용하면 여러 하위 일관성 그룹이 포함된 부모 일관성 그룹을 생성할 수 있습니다. 따라서 복잡한 데이터 구조에 대한 데이터 보호 및 관리가 간소화됩니다.

프로토콜 지원

업데이트	설명
"대칭 액티브/액티브 다중 경로에 대한 NVMe 지원"	NVMe/FC 및 NVMe/TCP는 이제 다중 경로를 위한 대칭 액티브-액티브 아키텍처를 지원하므로 호스트와 스토리지 간의 모든 경로가 액티브 /최적화됩니다.

스토리지 효율성

업데이트	설명
"스토리지 유닛의 자동 재조정 지원"	ONTAP은 최적의 성능 및 용량 활용도를 위해 스토리지 가용성 영역에서 스토리지 유닛의 균형을 자동으로 조정합니다.

업데이트	설명
"NVMe 공간 할당 취소가 기본적으로 활성화되어 있습니다"	NVMe 네임스페이스에 대해 공간 할당("홀 펀칭" 및 "매핑 해제"라고도 함)이 기본적으로 활성화됩니다. 공간 할당 해제를 통해 호스트가 네임스페이스에서 사용되지 않는 블록을 할당 해제하여 공간을 재확보할 수 있습니다. 특히, 데이터 회전율이 높은 파일 시스템의 경우 전체적인 스토리지 효율성이 크게 향상됩니다.

ASA R2 시스템을 위한 ONTAP 9.16.0의 새로운 기능

ASA R2 시스템을 위한 ONTAP 9.16.0에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

시스템

업데이트	설명
시스템	다음 NetApp ASA r2 시스템을 사용할 수 있습니다. 이러한 시스템은 SAN 전용 고객의 요구 사항에 맞춰 간소화된 환경을 만드는 통합 하드웨어 및 소프트웨어 솔루션을 제공합니다. • ASA A1K 를 참조하십시오 • ASA A70 를 참조하십시오 • ASA A90 를 참조하십시오

시스템 관리자

업데이트	설명
"SAN 전용 고객에 대한 원활한 지원"	System Manager를 활용하면 필수 SAN 기능을 지원하는 동시에 SAN 환경에서 지원되지 않는 기능을 쉽게 파악할 수 있습니다.

스토리지 관리

업데이트	설명
"단순화된 스토리지 관리"	ASA R2 시스템에서는 스토리지 유닛과 정합성 보장 그룹을 사용하여 스토리지 관리를 간소화합니다. • 스토리지 유닛 _ 은(는) 데이터 작업을 위해 SAN 호스트에서 사용할 수 있는 스토리지 공간을 만듭니다. 스토리지 유닛은 SCSI 호스트용 LUN 또는 NVMe 호스트용 NVMe 네임스페이스를 가리킵니다. • _A 정합성 보장 그룹 _ 은(는) 단일 유닛으로 관리되는 스토리지 유닛의 모음입니다.

데이터 보안

업데이트	설명
"온보드 키 관리자 및 이중 계층 암호화"	ASA R2 시스템은 온보드 키 관리자와 이중 계층(하드웨어 및 소프트웨어) 암호화를 지원합니다.

ASA R2 시스템에 영향을 주는 ONTAP 제한 및 기본값 변경

ASA R2 시스템에 영향을 주는 제한 및 기본값 변경 사항에 대해 알아봅니다. NetApp은 고객이 각 ONTAP 릴리스에서 가장 중요한 기본 및 제한 변경 사항을 이해할 수 있도록 돕기 위해 노력하고 있습니다.

ONTAP 제한 변경 사항

피처	제한 변경	릴리스에서 변경...
클러스터당 스토리지 VM	HA 쌍당 지원되는 스토리지 가상 머신(VM)의 최대 수가 32개에서 256개로 늘어났습니다.	ONTAP 9.18.1
SnapMirror 활성 동기화	SnapMirror 활성 동기화 지원이 2노드 클러스터에서 4노드 클러스터로 확대되었습니다.	ONTAP 9.18.1
클러스터당 노드 수	클러스터당 최대 노드 수가 2개에서 12개로 늘어났습니다. ⓘ 클러스터에서 노드가 3개 이상인 ONTAP 9.16.1을 실행 중인 경우 ONTAP 9.16.0으로 되돌릴 수 없습니다.	ONTAP 9.16.1
보관 장치	HA 쌍당 2500개에서 HA 쌍당 10,000개로 스토리지 유닛의 최대 수가 증가합니다.	ONTAP 9.16.1

시작하십시오

ASA R2 스토리지 시스템에 대해 알아보십시오

NetApp ASA R2 시스템은 통합 하드웨어 및 소프트웨어 솔루션을 제공하여 SAN 전용 고객의 요구 사항에 맞는 간소화된 환경을 제공합니다.

ASA r2 시스템으로 분류되는 것은 다음과 같습니다.

- ASA A1K 를 참조하십시오
- ASA A90 를 참조하십시오
- ASA A70 를 참조하십시오
- ASA A50
- ASA A30
- ASA A20
- ASA C30

ASA r2 시스템은 모든 SAN 프로토콜(iSCSI, FC, NVMe/FC, NVMe/TCP)을 지원합니다. iSCSI, FC, NVMe/FC 및 NVMe/TCP 프로토콜은 다중 경로를 위한 대칭적 액티브-액티브 아키텍처를 지원하므로 호스트와 스토리지 간의 모든 경로가 활성/최적화됩니다. iSCSI 및 NVMe/TCP 프로토콜은 호스트와 스토리지 간의 직접 연결을 지원합니다. 파이버 채널 및 NVMe/FC 프로토콜의 경우 직접 연결이 지원되지 않습니다.

ASA R2 시스템에서 ONTAP 소프트웨어 및 System Manager를 간소화하여 필수 SAN 기능을 지원하는 동시에 SAN 환경에서 지원되지 않는 기능을 제거합니다.

ASA R2 시스템에서는 정합성 보장 그룹이 포함된 스토리지 유닛을 사용합니다.

- 스토리지 유닛 _ 은(는) 데이터 작업을 위해 SAN 호스트에서 사용할 수 있는 스토리지 공간을 만듭니다. 스토리지 유닛은 SCSI 호스트용 LUN 또는 NVMe 호스트용 NVMe 네임스페이스를 가리킵니다.
- _A 정합성 보장 그룹 _ 은(는) 단일 유닛으로 관리되는 스토리지 유닛의 모음입니다.

ASA r2 시스템은 일관성 그룹이 있는 스토리지 유닛을 사용하여 스토리지 관리와 데이터 보호를 간소화합니다. 예를 들어, 일관성 그룹에 10개의 저장 장치로 구성된 데이터베이스가 있고 전체 데이터베이스를 백업해야 한다고 가정해 보겠습니다. 각 저장 장치를 개별적으로 백업하는 대신 일관성 그룹을 백업하여 전체 데이터베이스를 보호할 수 있습니다.

도난이나 랜섬웨어와 같은 악의적인 공격으로부터 데이터를 보호하기 위해 ASA r2 시스템은 온보드 키 관리자, 이중 계층 암호화, 다중 인증 및 다중 관리자 검증을 지원합니다. 보조 ASA r2 시스템에서는 변조 방지 스냅샷도 지원됩니다.

ASA r2 시스템은 ASA, AFF 또는 FAS 시스템과의 클러스터 혼합을 지원하지 않습니다.

를 참조하십시오

- ASA R2 시스템 지원 및 제한 사항에 대한 자세한 내용은 을 "NetApp Hardware Universe를 참조하십시오 "참조하십시오.
- 에 대해 자세히 "ASA R2 시스템을 ASA 시스템과 비교한 것입니다"알아보십시오.
- 에 대해 자세히 "NetApp ASA"알아보십시오.

ASA R2 스토리지 시스템의 빠른 시작

ASA R2 시스템을 설치하고 실행하려면 하드웨어 구성 요소를 설치하고, 클러스터를 설정하고, 호스트에서 스토리지 시스템으로의 데이터 액세스를 설정하고, 스토리지를 프로비저닝해야 합니다.

1 하드웨어를 설치하고 설정합니다

"설치 및 설정" ASA R2 시스템을 ONTAP 환경에 구축합니다.

2 클러스터 설정

System Manager를 사용하여 에 대한 빠르고 쉬운 프로세스를 "ONTAP 클러스터를 설정합니다"안내합니다.

3 데이터 액세스를 설정합니다

"ASA R2 시스템을 SAN 클라이언트에 연결합니다"..

4 스토리지를 프로비저닝합니다

"스토리지 프로비저닝" SAN 클라이언트에 데이터를 제공하기 시작합니다.

다음 단계

이제 System Manager를 사용하여 를 통해 데이터를 보호할 수 "스냅샷을 생성하는 중입니다"있습니다.

ASA R2 시스템을 설치합니다

ASA R2 스토리지 시스템의 설치 및 설정 워크플로우

ASA R2 시스템을 설치 및 구성하려면 하드웨어 요구 사항을 검토하고, 사이트를 준비하고, 하드웨어 구성 요소를 설치 및 케이블 연결하고, 시스템의 전원을 켜고, ONTAP 클러스터를 설정합니다.

1 **"하드웨어 설치 요구 사항을 검토합니다"**

하드웨어 요구 사항을 검토하여 ASA R2 스토리지 시스템을 설치합니다.

2 **"ASA R2 스토리지 시스템 설치를 준비합니다"**

ASA R2 시스템 설치를 준비하려면 현장 준비, 환경 및 전기 요구 사항 확인, 충분한 랙 공간 확보 등이 필요합니다. 그런 다음 장비의 포장을 풀고 내용물을 포장 명세서와 비교하고 하드웨어를 등록하여 지원 혜택을 받으십시오.

3 **"ASA R2 스토리지 시스템용 하드웨어를 설치합니다"**

하드웨어를 설치하려면 스토리지 시스템 및 셸프용 레일 키트를 설치한 다음 스토리지 시스템을 캐비닛이나 텔코 랙에 설치하고 고정합니다. 그런 다음 선반을 레일에 밀어 넣습니다. 마지막으로 케이블 관리 장치를 스토리지 시스템 후면에 연결하여 케이블을 체계적으로 배선합니다.

4 **"ASA R2 스토리지 시스템의 컨트롤러와 스토리지 쉘프를 케이블로 연결합니다"**

하드웨어를 케이블로 연결하려면 먼저 스토리지 컨트롤러를 네트워크에 연결한 다음, 컨트롤러를 스토리지 쉘프에 연결합니다.

5 **"ASA R2 스토리지 시스템의 전원을 켭니다"**

컨트롤러의 전원을 켜기 전에 각 NS224 쉘프의 전원을 켜고 고유한 쉘프 ID를 할당하여 각 쉘프가 설정 내에서 고유하게 식별되는지 확인하십시오.

ASA R2 스토리지 시스템의 설치 요구 사항

ASA R2 스토리지 시스템 및 스토리지 셸프에 필요한 장비 및 인양 주의 사항을 검토합니다.

설치에 필요한 장비

ASA R2 스토리지 시스템을 설치하려면 다음과 같은 장비와 툴이 필요합니다.

- 웹 브라우저에 액세스하여 스토리지 시스템을 구성합니다
- 정전기 방전(ESD) 스트랩
- 플래시
- USB/직렬 연결이 있는 랩톱 또는 콘솔
- 보관 선반 ID 설정을 위한 종이 클립 또는 끝이 뾰족한 볼펜
- Phillips #2 드라이버

인양 주의 사항

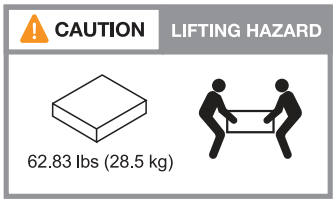
ASA R2 스토리지 시스템과 스토리지 쉘프는 무겁습니다. 이러한 품목을 들어 올리거나 이동할 때는 주의를 기울이십시오.

스토리지 시스템 중량

ASA R2 스토리지 시스템을 이동하거나 들어올릴 때 필요한 예방 조치를 취하십시오.

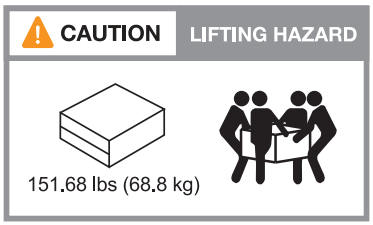
A1K를 참조하십시오

ASA A1K 저장 장치 시스템의 무게는 최대 28.5kg(62.83파운드)입니다. 보관 시스템을 인양하려면 두 사람 또는 유압 리프트를 사용합니다.



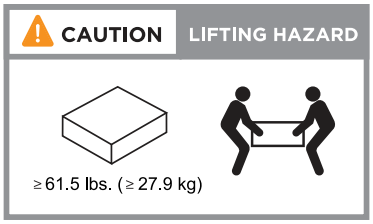
A70 및 **A90**

ASA A70 또는 ASA A90 저장 장치 시스템의 무게는 최대 68.8kg(151.68파운드)입니다. 보관 시스템을 인양하려면 네 명 또는 유압 리프트를 사용합니다.



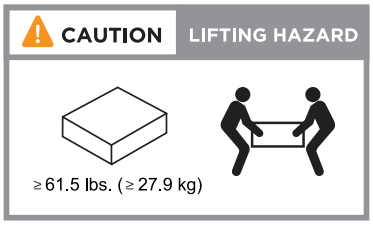
A20, A30, A50을 지원합니다

ASA A20, ASA A30 또는 ASA A50 저장 장치 시스템의 무게는 최대 27.9kg(61.5lbs)입니다. 보관 시스템을 인양하려면 두 사람 또는 유압 리프트를 사용합니다.



C30를 참조하십시오

ASA C30 저장 장치 시스템의 무게는 최대 27.9kg(61.5파운드)입니다. 보관 시스템을 인양하려면 두 사람 또는 유압 리프트를 사용합니다.

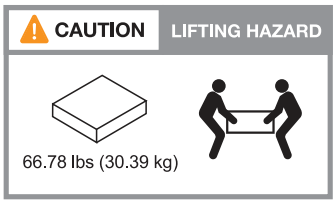


보관 선반 중량

선반을 옮기거나 들어올릴 때 필요한 예방 조치를 취하십시오.

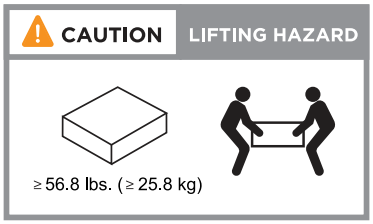
NS224 쉘프

NS224 선반의 무게는 최대 30.29kg(66.78lbs)입니다. 선반을 인양하려면 두 사람이 함께 작업하거나 유압식 리프트를 사용하십시오. 선반 무게의 균형을 맞추기 위해 모든 구성 요소를 선반(전면 및 후면 모두)에 보관하십시오.



NSM100B 모듈 포함 **NS224** 쉘프

NSM100B 모듈이 포함된 NS224 선반의 무게는 최대 25.8kg(56.8파운드)입니다. 선반을 인양하려면 두 사람이 함께 작업하거나 유압식 리프트를 사용하십시오. 선반 무게의 균형을 맞추기 위해 모든 구성 요소를 선반(전면 및 후면 모두)에 보관하십시오.



관련 정보

- "안전 정보 및 규정 고지"

다음 단계

하드웨어 요구 사항을 검토한 후"ASA R2 스토리지 시스템 설치를 준비합니다"

ASA R2 스토리지 시스템 설치를 준비합니다

사이트 준비, 상자 포장 풀기, 포장 명세서와 상자 내용물 비교, 지원 혜택에 액세스할 수 있도록 시스템을 등록하여 ASA R2 스토리지 시스템 설치를 준비합니다.

1단계**:** 사이트를 준비합니다

ASA R2 스토리지 시스템을 설치하려면 사용하려는 사이트와 캐비닛 또는 랙이 구성에 맞는 사양을 충족하는지 확인하십시오.

단계

1. 를 사용하여 "NetApp Hardware Universe를 참조하십시오" 작업장이 기억 장치 시스템의 환경 및 전기 요구 사항을 충족하는지 확인합니다.
2. 스토리지 시스템, 셸프 및 모든 스위치를 저장할 수 있는 충분한 캐비닛 또는 랙 공간이 있는지 확인합니다.

A1K를 참조하십시오

- HA 구성이 4U입니다
- NS224 스토리지 쉘프당 2U
- 대부분의 스위치는 1U

A70 및 **A90**

- HA 구성이 4U입니다
- NS224 스토리지 쉘프당 2U
- 대부분의 스위치는 1U

A20, A30, A50을 지원합니다

- 스토리지 시스템의 경우 2U
- NS224 스토리지 쉘프당 2U
- 대부분의 스위치는 1U

C30를 참조하십시오

- 스토리지 시스템의 경우 2U
- NS224 스토리지 쉘프당 2U
- 대부분의 스위치는 1U

3. 필요한 네트워크 스위치를 설치합니다.

   설치 지침 및 호환성 정보는 를 "스위치 설명서" "NetApp Hardware Universe를 참조하십시오" 참조하십시오.

2단계**:** 상자의 포장을 풉니다

ASA R2 스토리지 시스템에 사용할 사이트와 캐비닛 또는 랙이 필요한 사양을 충족하는지 확인한 후 모든 상자의 포장을 풀고 내용물을 포장 명세서에 있는 항목과 비교합니다.

단계

1. 모든 상자를 조심스럽게 열고 정리된 방식으로 내용물을 배치합니다.
2. 포장을 푼 내용물과 포장 명세서의 목록을 비교합니다. 불일치 사항이 있는 경우 추가 조치를 위해 메모하십시오.

   배송 상자 측면의 QR 코드를 스캔하여 포장 목록을 얻을 수 있습니다.

   다음 항목은 상자에 표시될 수 있는 내용 중 일부입니다.

* 하드웨어 *	* 케이블 *	

• 베젤 • 수행할 수 있습니다 • 지침이 포함된 레일 키트(옵션) • 보관 선반(추가 저장 장치를 주문한 경우)	• 관리 이더넷 케이블(RJ-45 케이블) • 네트워크 케이블 • 전원 코드 • 스토리지 케이블(추가 스토리지를 주문한 경우) • USB-C 직렬 포트 케이블	

3단계**:** 스토리지 시스템을 등록합니다

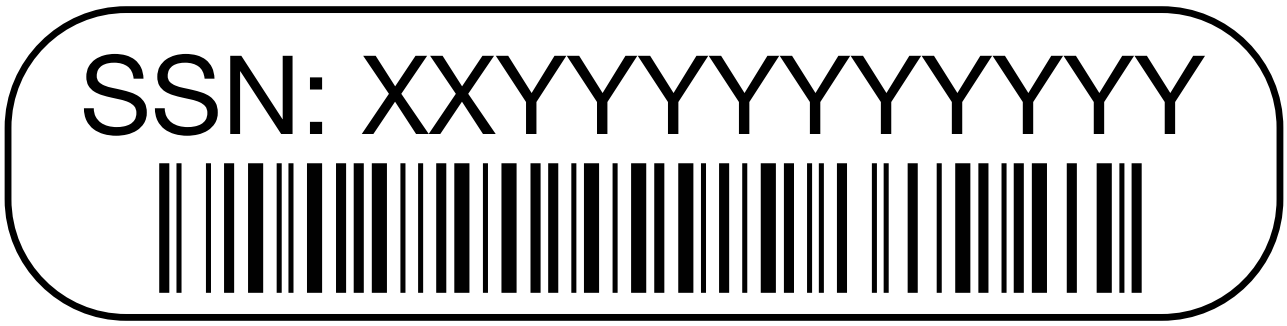
사이트가 ASA R2 스토리지 시스템 사양에 대한 요구 사항을 충족하는지 확인하고 주문한 모든 부품이 있는지 확인한 후에는 시스템을 등록해야 합니다.

단계

1. 스토리지 시스템의 일련 번호를 찾습니다.

   일련 번호는 다음 위치에서 찾을 수 있습니다.

   - 포장 명세서
   - 확인 이메일에 입력합니다
   - 각 컨트롤러 또는 일부 시스템의 경우, 각 컨트롤러의 시스템 관리 모듈에 표시됩니다



2. 로 이동합니다 "NetApp Support 사이트".
3. 다음과 같이 스토리지 시스템을 등록해야 하는지 확인합니다.

귀하의 경우...	다음 단계를 따르십시오...
더 많은 워크로드 추가)	a. 사용자 이름과 암호를 사용하여 로그인합니다. b. 시스템 * > * 내 시스템 * 을 선택합니다. c. 새 일련 번호가 나열되는지 확인합니다. d. 일련 번호가 목록에 없으면 신규 NetApp 고객에 대한 지침을 따르십시오.

귀하의 경우...	다음 단계를 따르십시오...
신규 NetApp 고객	a. 지금 등록 * 을 클릭하고 계정을 만듭니다. b. 시스템 * > * 시스템 등록 * 을 선택합니다. c. 스토리지 시스템의 일련 번호와 요청된 세부 정보를 입력합니다. 등록이 승인되면 필요한 소프트웨어를 다운로드할 수 있습니다. 승인 프로세스는 최대 24시간이 걸릴 수 있습니다.

다음 단계

ASA R2 하드웨어를 설치할 준비가 되면"ASA R2 스토리지 시스템용 하드웨어를 설치합니다"

ASA R2 스토리지 시스템을 설치합니다

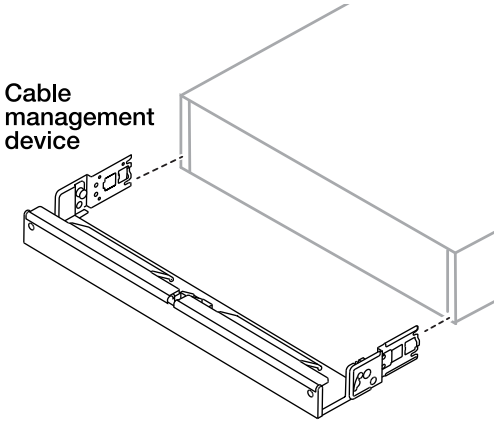
ASA R2 스토리지 시스템을 설치할 준비가 되면 시스템용 하드웨어를 설치합니다. 먼저 레일 키트를 설치합니다. 그런 다음 스토리지 시스템을 캐비닛이나 통신 랙에 설치하고 고정합니다.

시작하기 전에

- 지침이 레일 키트와 함께 포장되어 있는지 확인하십시오.
- 보관 시스템 및 보관 선반의 무게와 관련된 안전 문제에 유의하십시오.
- 스토리지 시스템을 통과하는 공기 흐름은 베젤 또는 엔드 캡이 설치된 전면에서 유입되고 포트가 있는 후면에서 배출됩니다.

단계

1. 키트와 함께 제공되는 지침에 따라 필요에 따라 스토리지 시스템 및 스토리지 셸프용 레일 키트를 설치합니다.
2. 스토리지 시스템을 캐비닛 또는 통신 랙에 설치하고 고정합니다.
   a. 기억 장치 시스템을 캐비닛 또는 통신 랙의 중간에 있는 레일에 놓은 다음, 하단에서 기억 장치 시스템을 지지하고 제자리에 밀어 넣습니다.
   b. 캐비닛이나 통신 랙의 가이드 핀이 스토리지 시스템 가이드 슬롯에 안전하게 들어맞는지 확인하세요.
   c. 함께 제공된 장착 나사를 사용하여 저장 장치 시스템을 캐비닛이나 텔코 랙에 고정합니다.
3. 베젤을 스토리지 시스템의 전면에 장착합니다.
4. ASA R2 시스템에 케이블 관리 장치가 함께 제공된 경우 스토리지 시스템 뒷면에 연결합니다.



5. 스토리지 쉘프를 설치하고 고정하십시오.

   a. 보관 선반의 후면을 레일에 놓은 다음 하단에서 선반을 지지하고 캐비닛이나 텔코 랙에 밀어 넣습니다.

      여러 스토리지 쉘프를 설치하는 경우 첫 번째 스토리지 쉘프를 컨트롤러 바로 위에 배치하십시오. 두 번째 스토리지 쉘프를 컨트롤러 바로 아래에 배치합니다. 추가 스토리지 셸프에 대해 이 패턴을 반복합니다.

   b. 함께 제공된 장착 나사를 사용하여 저장 장치 쉘프를 캐비닛이나 텔코 랙에 고정합니다.

다음 단계

ASA R2 시스템용 하드웨어를 설치한 후에는"ASA R2 시스템의 컨트롤러와 스토리지 쉘프를 케이블로 연결합니다"

ASA R2 스토리지 시스템용 하드웨어를 케이블로 연결합니다

ASA R2 스토리지 시스템용 랙 하드웨어를 설치한 후 컨트롤러의 네트워크 케이블을 설치하고 컨트롤러와 스토리지 쉘프 간에 케이블을 연결합니다.

시작하기 전에

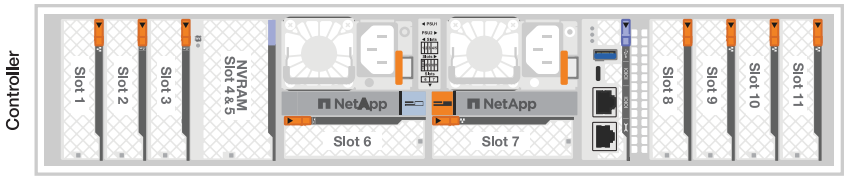
스토리지 시스템을 네트워크 스위치에 연결하는 방법에 대한 자세한 내용은 네트워크 관리자에게 문의하십시오.

이 작업에 대해

- 다음 절차는 일반적인 구성을 보여 줍니다. 특정 케이블 연결은 스토리지 시스템용으로 주문한 구성 요소에 따라 다릅니다. 포괄적인 구성 및 슬롯 우선 순위에 대한 자세한 내용은 을 "NetApp Hardware Universe를 참조하십시오"참조하십시오.
- 클러스터/HA 및 호스트 네트워크 케이블 연결 절차는 일반적인 구성을 보여줍니다.

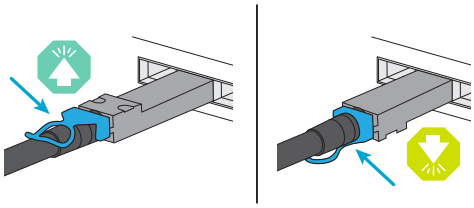
  케이블링 절차에서 구성이 보이지 않으면 다음으로 이동하세요. "NetApp Hardware Universe를 참조하십시오" 스토리지 시스템을 올바르게 케이블로 연결하기 위한 포괄적인 구성 및 슬롯 우선순위 정보를 확인하세요.

- ASA A1K, ASA A70 또는 ASA A90 스토리지 시스템이 있는 경우 I/O 슬롯은 1~11까지 번호가 매겨집니다.



- 케이블 연결 그래픽에는 포트에 커넥터를 삽입할 때 케이블 커넥터 당김 탭의 올바른 방향(위 또는 아래)을 나타내는 화살표 아이콘이 있습니다.

  커넥터를 삽입할 때 딸깍 소리가 들려야 합니다. 딸깍 소리가 안 되면 커넥터를 제거하고 뒤집은 다음 다시 시도하십시오.



- 광 스위치에 케이블로 연결하는 경우 광 트랜시버를 컨트롤러 포트에 삽입한 후 스위치 포트에 연결합니다.

1단계**:** 클러스터**/HA** 연결 케이블 연결

컨트롤러를 ONTAP 클러스터에 케이블로 연결합니다. 이 절차는 스토리지 시스템 모델 및 입출력 모듈 구성에 따라 다릅니다.

클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트를 공유합니다.

A1K를 참조하십시오

ONTAP 클러스터 연결을 생성합니다. 스위치가 없는 클러스터의 경우 컨트롤러를 서로 연결합니다. 스위치 클러스터의 경우 컨트롤러를 클러스터 네트워크 스위치에 연결합니다.

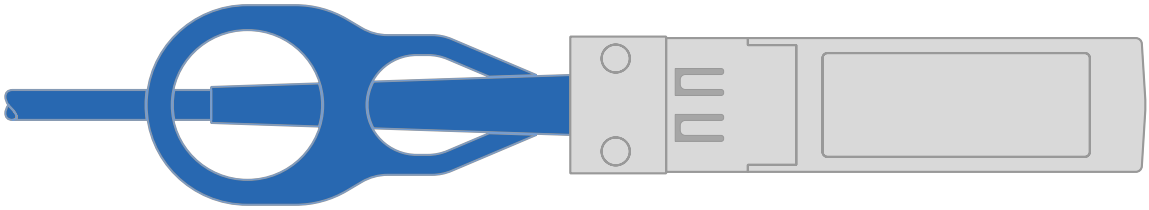
스위치가 없는 클러스터 케이블 연결

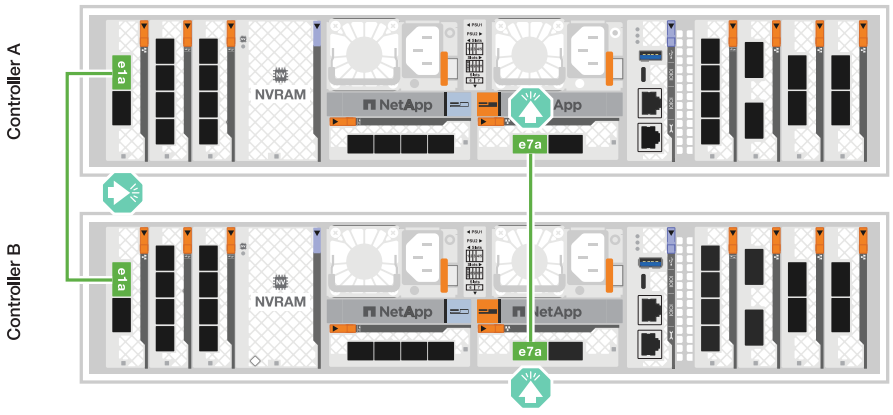
클러스터/HA 인터커넥트 케이블을 사용하여 포트 E1A에 E1A를 연결하고 포트 e7a에 e7a를 연결합니다.

단계

1. 컨트롤러 A의 포트 E1A를 컨트롤러 B의 포트 E1A에 연결합니다
2. 컨트롤러 A의 포트 e7a를 컨트롤러 B의 포트 E1A에 연결합니다

    ◦ 클러스터/HA 인터커넥트 케이블 *





스위치 클러스터 케이블링

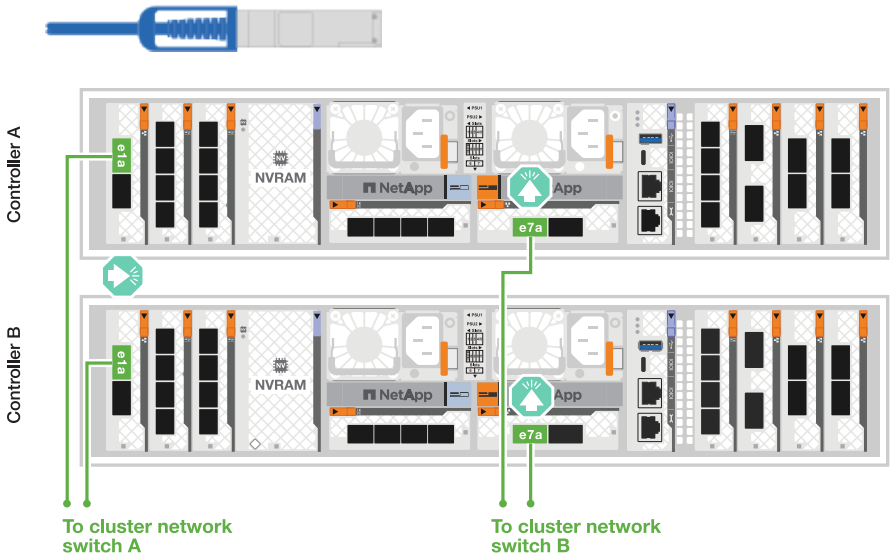
100 GbE 케이블을 사용하여 포트 E1A를 E1A에 연결하고 포트 e7a를 e7a에 연결합니다.

스위치 클러스터 구성은 9.16.1 이상에서 지원됩니다.

단계

1. 컨트롤러 A의 포트 E1A와 컨트롤러 B의 포트 E1A를 클러스터 네트워크 스위치 A에 연결합니다
2. 컨트롤러 A의 포트 e7a와 컨트롤러 B의 포트 e7a를 클러스터 네트워크 스위치 B에 연결합니다

◦ 100 GbE 케이블 *



A70 및 **A90**

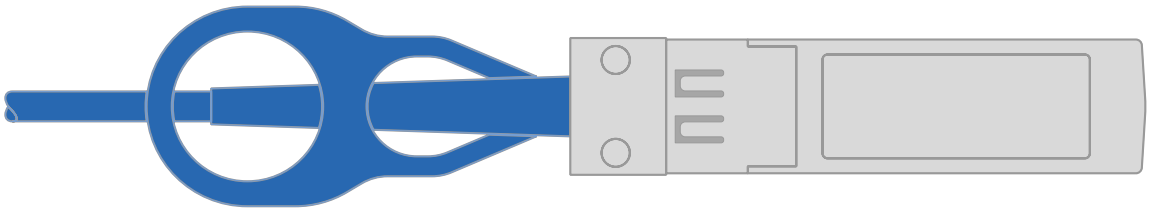
ONTAP 클러스터 연결을 생성합니다. 스위치가 없는 클러스터의 경우 컨트롤러를 서로 연결합니다. 스위치 클러스터의 경우 컨트롤러를 클러스터 네트워크 스위치에 연결합니다.

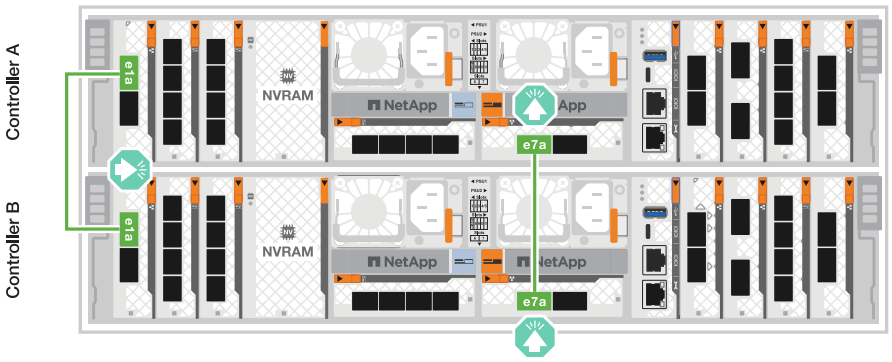
클러스터/HA 인터커넥트 케이블을 사용하여 포트 E1A에 E1A를 연결하고 포트 e7a에 e7a를 연결합니다.

단계

1. 컨트롤러 A의 포트 E1A를 컨트롤러 B의 포트 E1A에 연결합니다
2. 컨트롤러 A의 포트 e7a를 컨트롤러 B의 포트 E1A에 연결합니다

◦ 클러스터/HA 인터커넥트 케이블 *





스위치 클러스터 케이블링

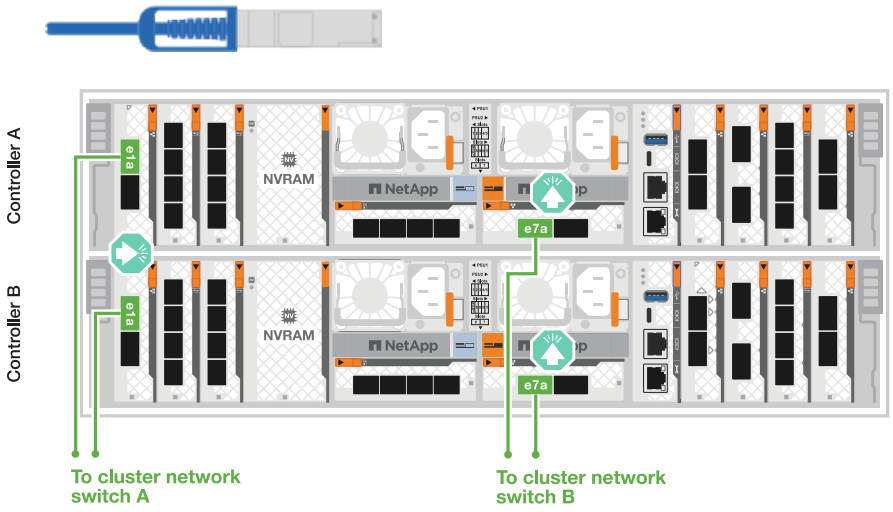
100 GbE 케이블을 사용하여 포트 E1A를 E1A에 연결하고 포트 e7a를 e7a에 연결합니다.

스위치 클러스터 구성은 9.16.1 이상에서 지원됩니다.

단계

1. 컨트롤러 A의 포트 E1A와 컨트롤러 B의 포트 E1A를 클러스터 네트워크 스위치 A에 연결합니다
2. 컨트롤러 A의 포트 e7a와 컨트롤러 B의 포트 e7a를 클러스터 네트워크 스위치 B에 연결합니다

◦ 100 GbE 케이블 *



A20, A30, A50을 지원합니다

ONTAP 클러스터 연결을 생성합니다. 스위치가 없는 클러스터의 경우 컨트롤러를 서로 연결합니다. 스위치 클러스터의 경우 컨트롤러를 클러스터 네트워크 스위치에 연결합니다.

클러스터/HA 케이블링 예제는 일반적인 구성을 보여줍니다.

여기에 구성이 보이지 않으면 다음으로 이동하세요. "NetApp Hardware Universe를 참조하십시오" 스토리지 시스템에 케이블을 연결하기 위한 포괄적인 구성 및 슬롯 우선순위 정보를 확인하세요.

스위치 없는 클러스터 케이블 연결

컨트롤러를 서로 연결하여 ONTAP 클러스터 연결을 생성합니다.

2포트 **40/100 GbE** 입출력 모듈 **2**개가 장착된 **ASA A30** 및 **ASA A50**

단계

1. 클러스터/HA 인터커넥트 연결:

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 2와 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

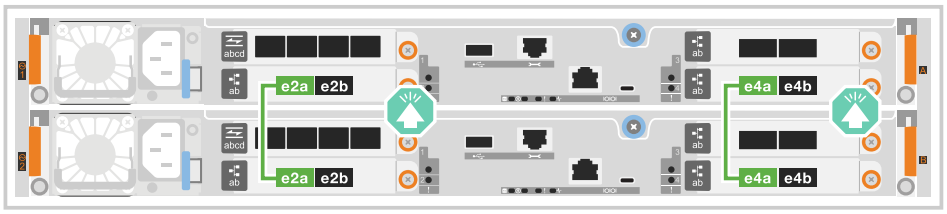
   a. 컨트롤러 A 포트 e2a를 컨트롤러 B 포트 e2a에 연결합니다.

   b. 컨트롤러 A 포트 e4a를 컨트롤러 B 포트 e4a에 연결합니다.

   입출력 모듈 포트 e2b 및 e4b는 사용되지 않으며 호스트 네트워크 연결에 사용할 수 있습니다.

   - 100 GbE 클러스터/HA 인터커넥트 케이블 *

Controller A



Controller B

ASA A30 및 **ASA A50**(2포트 **40/100 GbE** 입출력 모듈 **1**개 포함

단계

1. 클러스터/HA 인터커넥트 연결:

클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

a. 컨트롤러 A 포트 e4a를 컨트롤러 B 포트 e4a에 연결합니다.

b. 컨트롤러 A 포트 e4b를 컨트롤러 B 포트 e4b에 연결합니다.

- 100 GbE 클러스터/HA 인터커넥트 케이블 *

Controller A

Controller B

2포트 **10/25 GbE** 입출력 모듈 **1**개가 포함된 **ASA A20**

단계

1. 클러스터/HA 인터커넥트 연결:

클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 10/25GbE입니다.

a. 컨트롤러 A 포트 e4a를 컨트롤러 B 포트 e4a에 연결합니다.

b. 컨트롤러 A 포트 e4b를 컨트롤러 B 포트 e4b에 연결합니다.

- 25GbE 클러스터/HA 인터커넥트 케이블 *

Controller A

Controller B

• 스위치 클러스터 케이블 연결 *

컨트롤러를 클러스터 네트워크 스위치에 연결하여 ONTAP 클러스터 연결을 생성합니다.

2포트 **40/100 GbE** 입출력 모듈 **2**개가 있는 **ASA A30** 또는 **ASA A50**

단계

1. 클러스터/HA 인터커넥트 연결 케이블 연결:

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 2와 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

   a. 컨트롤러 A 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

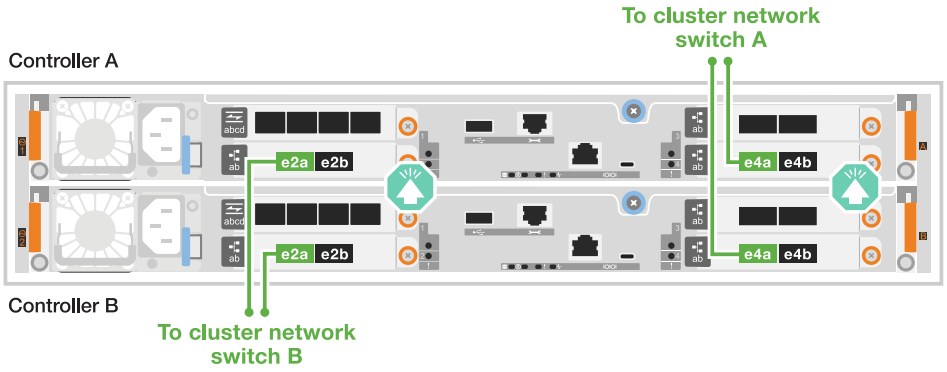
   b. 컨트롤러 A 포트 e2a를 클러스터 네트워크 스위치 B에 연결합니다.

   c. 컨트롤러 B 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   d. 컨트롤러 B 포트 e2a를 클러스터 네트워크 스위치 B에 연결합니다.

   입출력 모듈 포트 e2b 및 e4b는 사용되지 않으며 호스트 네트워크 연결에 사용할 수 있습니다.

   ▪ 40/100 GbE 클러스터/HA 인터커넥트 케이블 *



2포트 40/100 GbE 입출력 모듈 1개가 있는 ASA A30 또는 ASA A50

단계

1. 컨트롤러를 클러스터 네트워크 스위치에 케이블 연결합니다.

> 클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

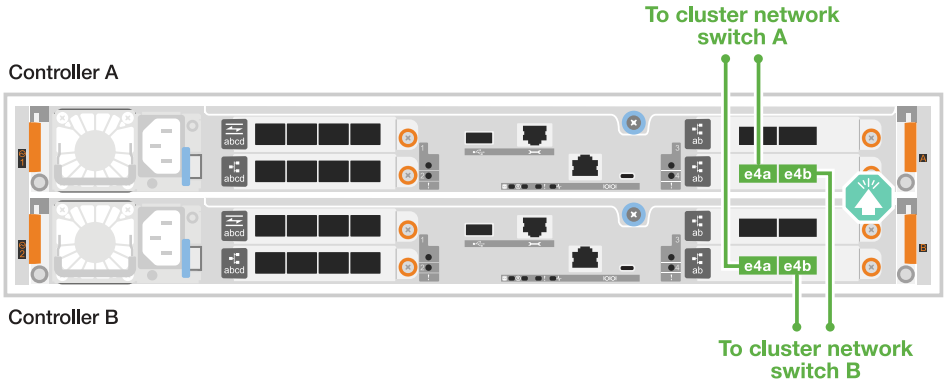
a. 컨트롤러 A 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

b. 컨트롤러 A 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

c. 컨트롤러 B 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

d. 컨트롤러 B 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

- 40/100 GbE 클러스터/HA 인터커넥트 케이블 *



2포트 10/25 GbE 입출력 모듈 1개가 포함된 ASA A20

1. 컨트롤러를 클러스터 네트워크 스위치에 케이블 연결합니다.

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 10/25GbE입니다.

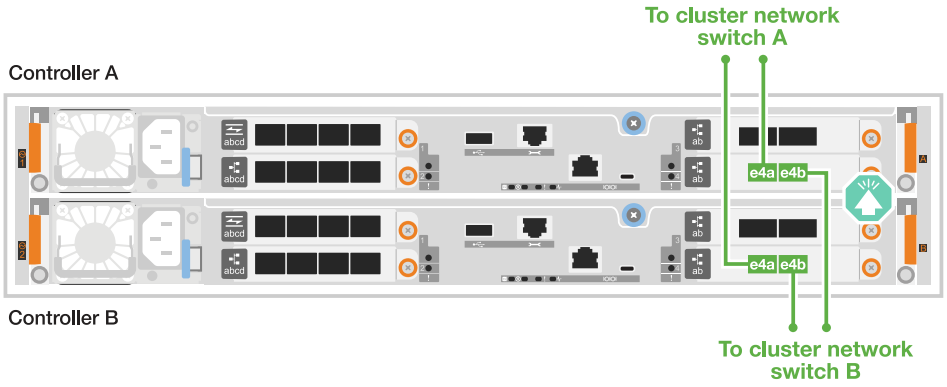
   a. 컨트롤러 A 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   b. 컨트롤러 A 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

   c. 컨트롤러 B 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   d. 컨트롤러 B 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

   - 10/25GbE 클러스터/HA 인터커넥트 케이블 *



ONTAP 클러스터 연결을 생성합니다. 스위치가 없는 클러스터의 경우 컨트롤러를 서로 연결합니다. 스위치 클러스터의 경우 컨트롤러를 클러스터 네트워크 스위치에 연결합니다.

클러스터/HA 케이블링 예제는 일반적인 구성을 보여줍니다.

여기에 구성이 보이지 않으면 다음으로 이동하세요. "NetApp Hardware Universe를 참조하십시오" 스토리지 시스템에 케이블을 연결하기 위한 포괄적인 구성 및 슬롯 우선순위 정보를 확인하세요.

스위치 없는 클러스터 케이블 연결

컨트롤러를 서로 연결하여 ONTAP 클러스터 연결을 생성합니다.

2개의 **2**포트 **40/100 GbE I/O** 모듈이 있는 **ASA C30**

단계

1. 클러스터/HA 인터커넥트 연결 케이블 연결:

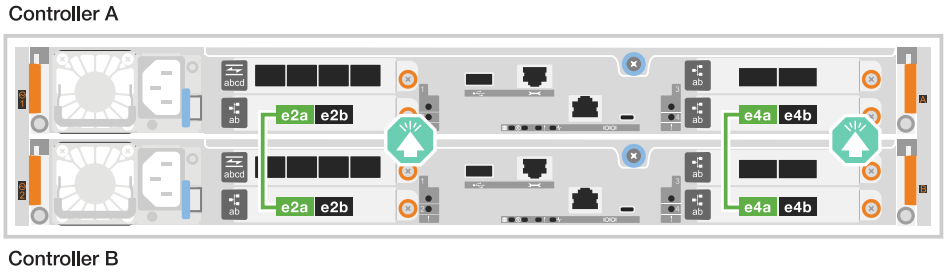
   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 2와 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

   a. 컨트롤러 A 포트 e2a를 컨트롤러 B 포트 e2a에 연결합니다.

   b. 컨트롤러 A 포트 e4a를 컨트롤러 B 포트 e4a에 연결합니다.

   입출력 모듈 포트 e2b 및 e4b는 사용되지 않으며 호스트 네트워크 연결에 사용할 수 있습니다.

   - 100 GbE 클러스터/HA 인터커넥트 케이블 *



2포트 40/100 GbE 입출력 모듈 1개가 포함된 ASA C30

단계

1. 클러스터/HA 인터커넥트 연결 케이블 연결:

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

   a. 컨트롤러 A 포트 e4a를 컨트롤러 B 포트 e4a에 연결합니다.

   b. 컨트롤러 A 포트 e4b를 컨트롤러 B 포트 e4b에 연결합니다.

   - 100 GbE 클러스터/HA 인터커넥트 케이블 *

Controller A

Controller B

- 스위치 클러스터 케이블 연결 *

컨트롤러를 클러스터 네트워크 스위치에 연결하여 ONTAP 클러스터 연결을 생성합니다.

2개의 2포트 40/100 GbE I/O 모듈이 있는 ASA C30

단계

1. 클러스터/HA 인터커넥트 연결 케이블 연결:

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 2와 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

   a. 컨트롤러 A 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

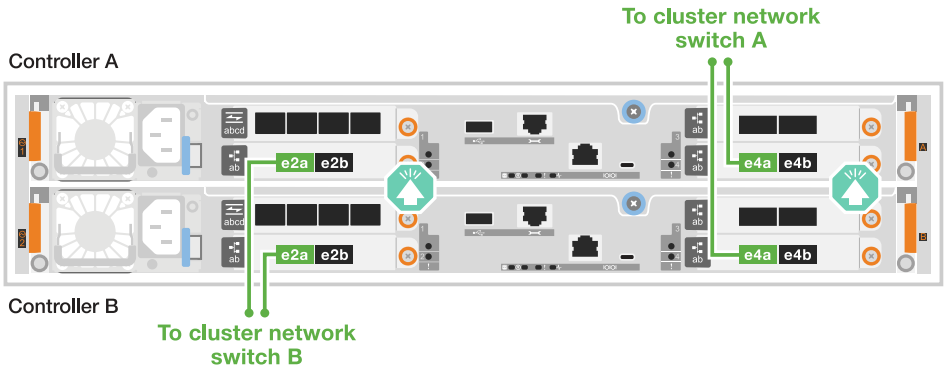
   b. 컨트롤러 A 포트 e2a를 클러스터 네트워크 스위치 B에 연결합니다.

   c. 컨트롤러 B 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   d. 컨트롤러 B 포트 e2a를 클러스터 네트워크 스위치 B에 연결합니다.

   입출력 모듈 포트 e2b 및 e4b는 사용되지 않으며 호스트 네트워크 연결에 사용할 수 있습니다.

   - 40/100 GbE 클러스터/HA 인터커넥트 케이블 *



2포트 **40/100 GbE** 입출력 모듈 **1**개가 포함된 **ASA C30**

단계

1. 컨트롤러를 클러스터 네트워크 스위치에 연결합니다.

   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트(슬롯 4의 I/O 모듈)를 공유합니다. 포트는 40/100 GbE입니다.

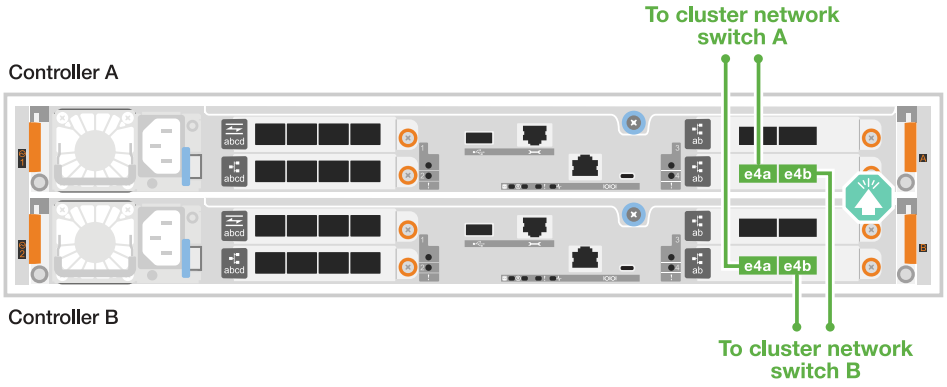
   a. 컨트롤러 A 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   b. 컨트롤러 A 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

   c. 컨트롤러 B 포트 e4a를 클러스터 네트워크 스위치 A에 연결합니다.

   d. 컨트롤러 B 포트 e4b를 클러스터 네트워크 스위치 B에 연결합니다.

   - 40/100 GbE 클러스터/HA 인터커넥트 케이블 *



2단계**:** 호스트 네트워크 연결 케이블 연결

컨트롤러를 호스트 네트워크에 연결합니다.

이 절차는 스토리지 시스템 모델 및 입출력 모듈 구성에 따라 다릅니다.

A1K를 참조하십시오

이더넷 모듈 포트를 호스트 네트워크에 연결합니다.

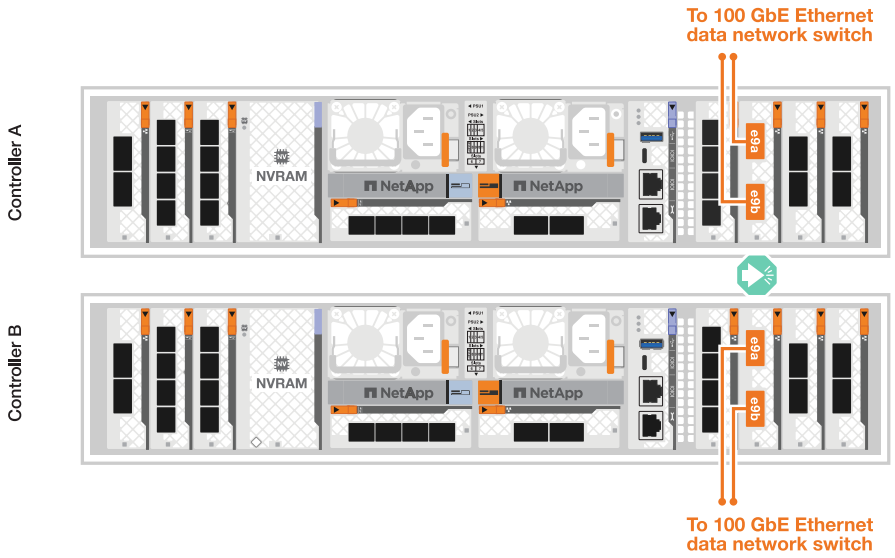
다음은 몇 가지 일반적인 호스트 네트워크 케이블 연결의 예입니다. 특정 시스템 구성은 를 "NetApp Hardware Universe를 참조하십시오" 참조하십시오.

단계

1. 이더넷 데이터 네트워크 스위치에 e9a 및 e9b 포트를 연결합니다.

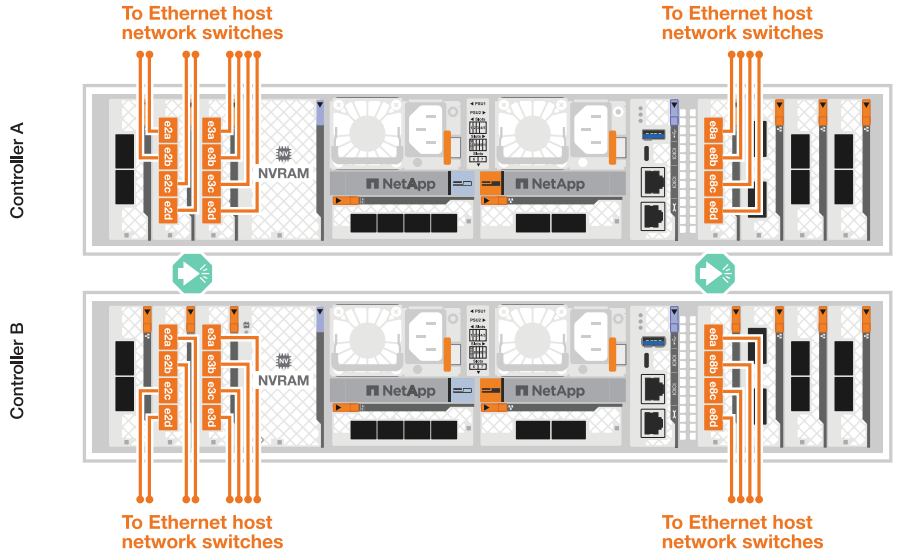
   클러스터 및 HA 트래픽에 시스템 성능을 극대화하려면 호스트 네트워크 연결에 포트 e1b 및 e7b 포트를 사용하지 마십시오. 성능을 최대화하려면 별도의 호스트 카드를 사용하십시오.

   ◦ 100 GbE 케이블 *



2. 10/25 GbE 호스트 네트워크 스위치를 연결합니다.

   ◦ 10/25GbE 호스트 *



A70 및 **A90**

이더넷 모듈 포트를 호스트 네트워크에 연결합니다.

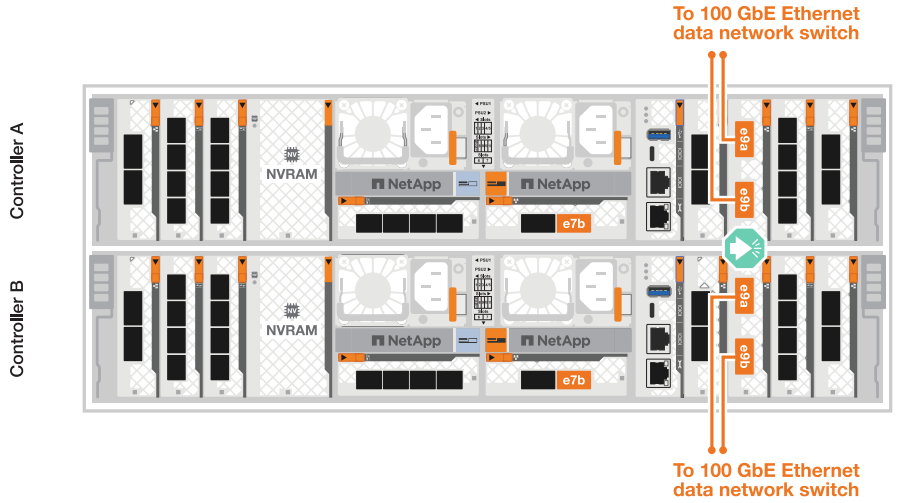
다음은 몇 가지 일반적인 호스트 네트워크 케이블 연결의 예입니다. 특정 시스템 구성은 를 "NetApp Hardware Universe를 참조하십시오" 참조하십시오.

단계

1. 이더넷 데이터 네트워크 스위치에 e9a 및 e9b 포트를 연결합니다.

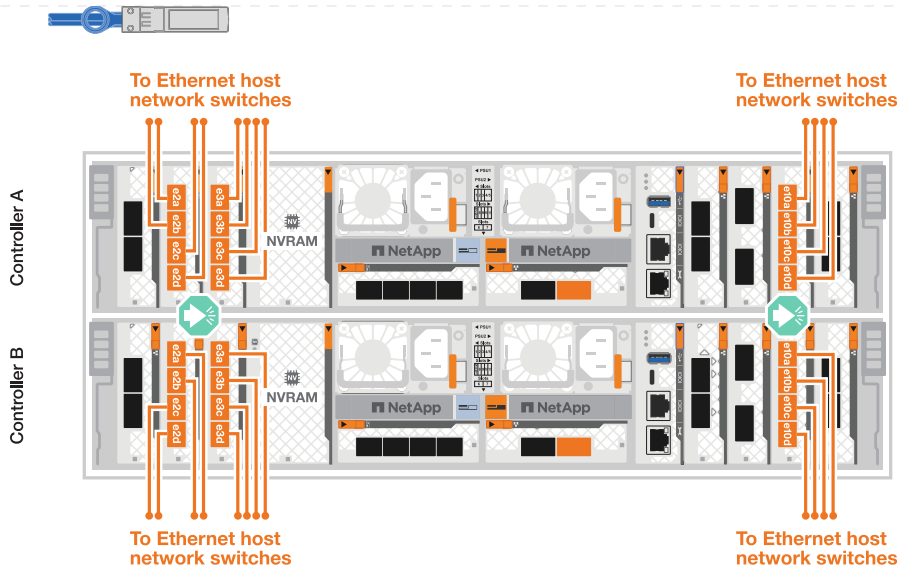
   클러스터 및 HA 트래픽에 시스템 성능을 극대화하려면 호스트 네트워크 연결에 포트 e1b 및 e7b 포트를 사용하지 마십시오. 성능을 최대화하려면 별도의 호스트 카드를 사용하십시오.

   ◦ 100 GbE 케이블 *



2. 10/25 GbE 호스트 네트워크 스위치를 연결합니다.

   ◦ 4포트, 10/25 GbE 호스트 *



A20, A30, A50을 지원합니다

이더넷 모듈 포트 또는 FC(Fibre Channel) 모듈 포트를 호스트 네트워크에 연결합니다.

호스트 네트워크 케이블링 예는 일반적인 구성을 보여줍니다.

여기에 구성이 보이지 않으면 다음으로 이동하세요. "NetApp Hardware Universe를 참조하십시오" 스토리지 시스템에 케이블을 연결하기 위한 포괄적인 구성 및 슬롯 우선순위 정보를 확인하세요.

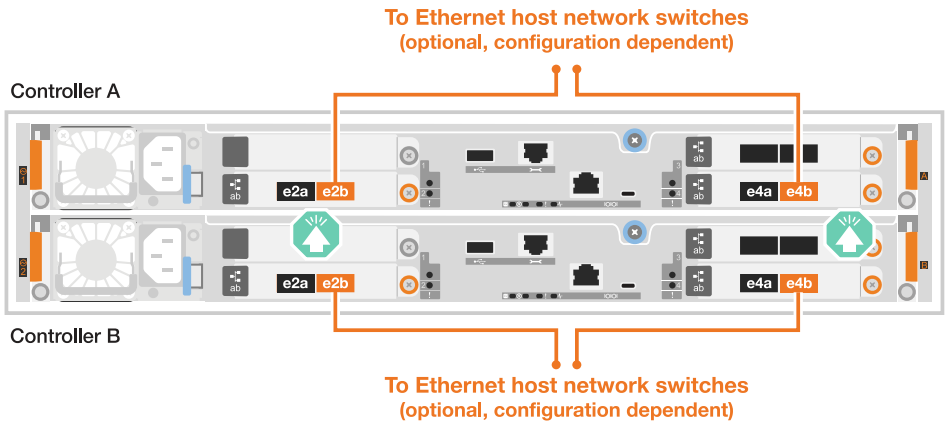
• 이더넷 호스트 케이블 연결 *

2포트 **40/100 GbE** 입출력 모듈 **2**개가 장착된 **ASA A30** 및 **ASA A50**

각 컨트롤러에서 포트 e2b 및 e4b를 이더넷 호스트 네트워크 스위치에 연결합니다.

슬롯 2 및 4의 입출력 모듈 포트는 40/100 GbE(호스트 접속은 40/100 GbE)입니다.

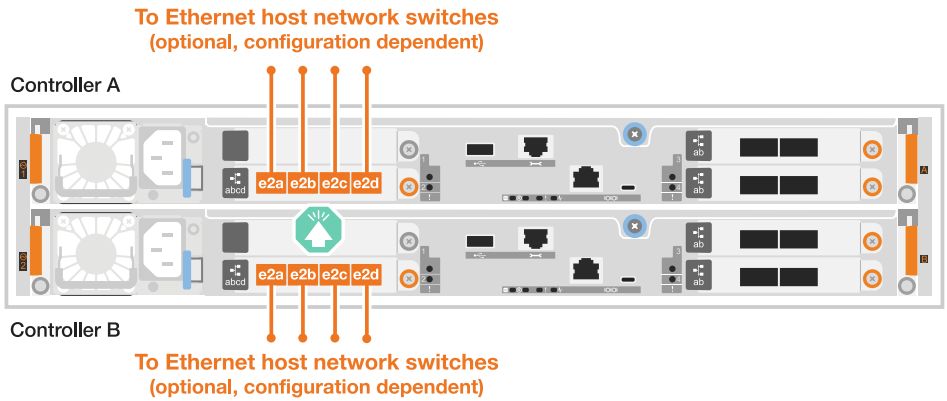
• 40/100 GbE 케이블 *



4포트 **10/25 GbE I/O** 모듈 **1**개가 포함된 **ASA A20, A30** 및 **A50**

각 컨트롤러에서 포트 e2a, e2b, E2C 및 e2D를 이더넷 호스트 네트워크 스위치에 연결합니다.

• 10/25 GbE 케이블 *

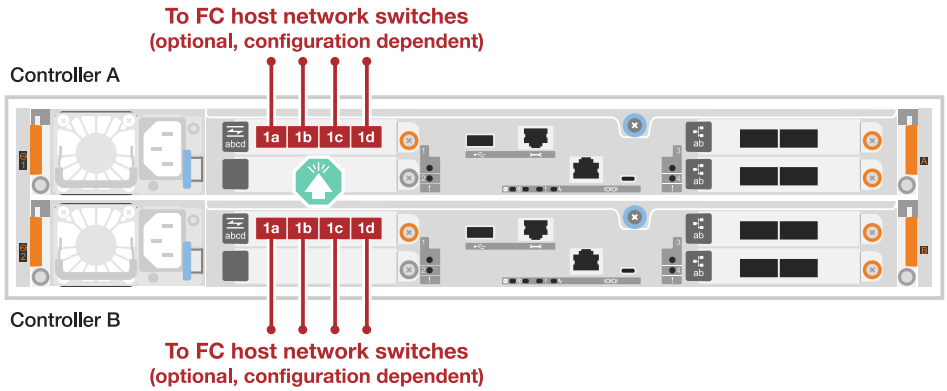


• FC 호스트 케이블 연결 *

4포트 64Gb/s FC I/O 모듈 1개가 포함된 ASA A20, A30 및 A50

각 컨트롤러에서 포트 1a, 1b, 1c 및 1d 를 FC 호스트 네트워크 스위치에 연결합니다.

• 64 Gb/s FC 케이블 *



이더넷 모듈 포트 또는 FC(Fibre Channel) 모듈 포트를 호스트 네트워크에 연결합니다.

호스트 네트워크 케이블링 예는 일반적인 구성을 보여줍니다.

여기에 구성이 보이지 않으면 다음으로 이동하세요. "NetApp Hardware Universe를 참조하십시오" 스토리지 시스템에 케이블을 연결하기 위한 포괄적인 구성 및 슬롯 우선순위 정보를 확인하세요.

• 이더넷 호스트 케이블 연결 *

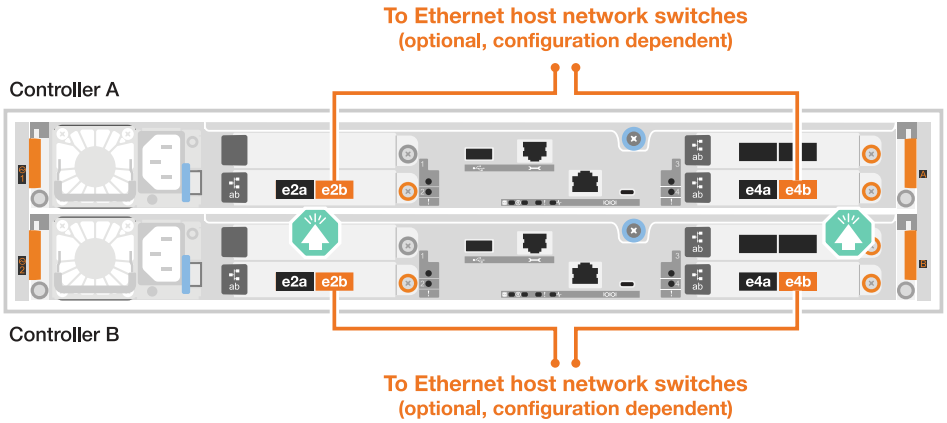
2개의 **2**포트 **40/100 GbE I/O** 모듈이 있는 **ASA C30**

단계

1. 각 컨트롤러에서 이더넷 호스트 네트워크 스위치에 케이블 포트 e2b 및 e4b를 연결합니다.

   슬롯 2 및 4의 입출력 모듈 포트는 40/100 GbE(호스트 접속은 40/100 GbE)입니다.

   ◦ 40/100 GbE 케이블 *

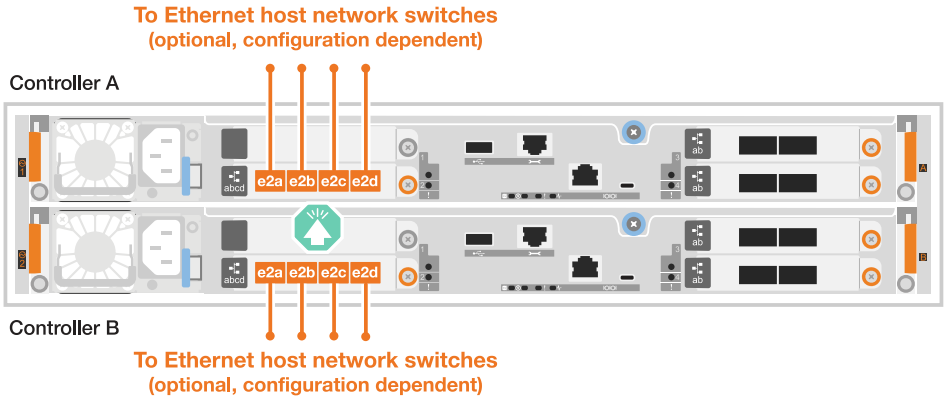


4포트 10/25 GbE 입출력 모듈 1개가 포함된 ASA C30

단계

1. 각 컨트롤러에서 이더넷 호스트 네트워크 스위치에 케이블 포트 e2a, e2b, E2C 및 e2D를 연결합니다.

   ◦ 10/25 GbE 케이블 *

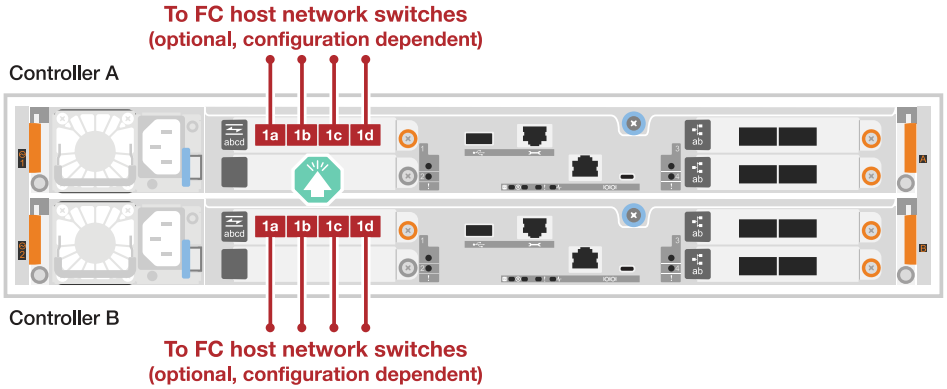


4포트 64Gb/s FC I/O 모듈 1개가 포함된 ASA C30

단계

1. 각 컨트롤러에서 포트 1a, 1b, 1c 및 1d를 FC 호스트 네트워크 스위치에 연결합니다.

   ◦ 64 Gb/s FC 케이블 *



3단계**:** 관리 네트워크 연결 케이블 연결

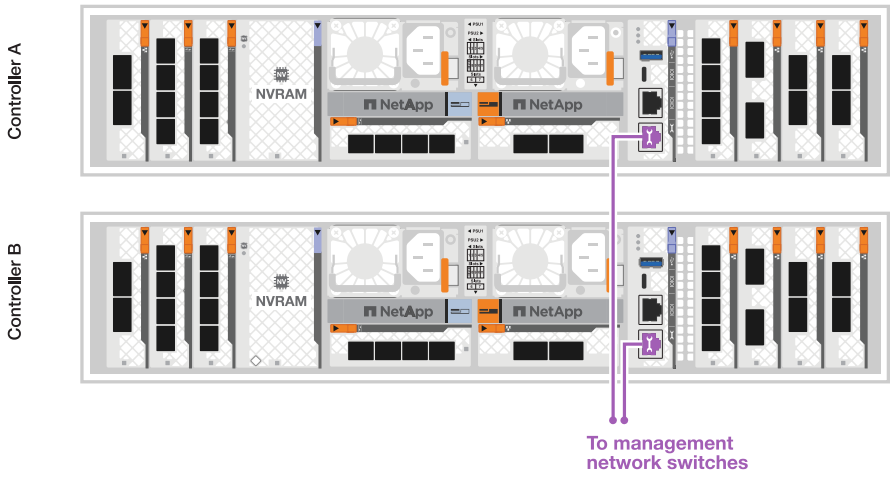
컨트롤러를 관리 네트워크에 연결합니다.

스토리지 시스템을 관리 네트워크 스위치에 연결하는 방법에 대한 자세한 내용은 네트워크 관리자에게 문의하십시오.

A1K를 참조하십시오

1000BASE-T RJ-45 케이블을 사용하여 각 컨트롤러의 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

- 1000BASE-T RJ-45 케이블 *

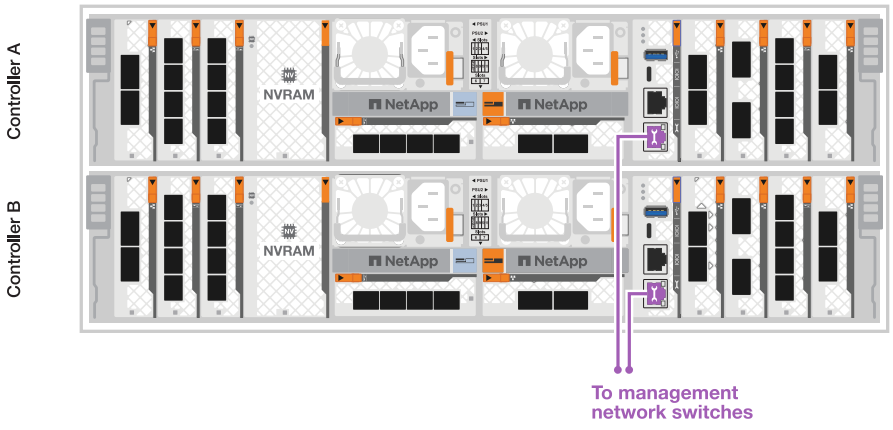


아직 전원 코드를 연결하지 마십시오.

A70 및 **A90**

1000BASE-T RJ-45 케이블을 사용하여 각 컨트롤러의 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

- 1000BASE-T RJ-45 케이블 *

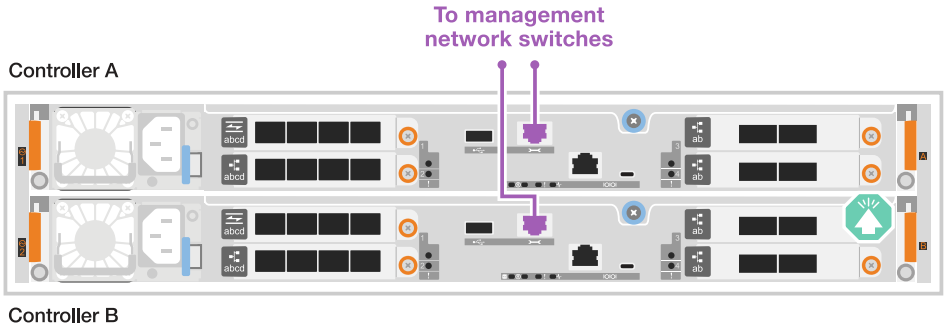


아직 전원 코드를 연결하지 마십시오.

A20, A30, A50을 지원합니다

각 컨트롤러의 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

- 1000BASE-T RJ-45 케이블 *

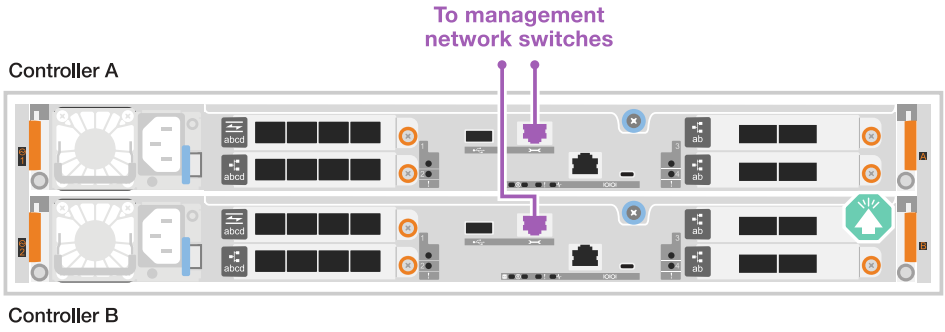


아직 전원 코드를 연결하지 마십시오.

C30를 참조하십시오

각 컨트롤러의 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

- 1000BASE-T RJ-45 케이블 *



아직 전원 코드를 연결하지 마십시오.

4단계**:** 선반 연결 케이블 연결

다음 케이블 연결 절차는 컨트롤러를 스토리지 쉘프에 연결하는 방법을 보여줍니다.

스토리지 시스템에서 지원되는 최대 쉘프 수와 광 및 스위치 연결과 같은 모든 케이블 옵션은 을 참조하십시오."NetApp Hardware Universe를 참조하십시오"

A1K를 참조하십시오

AFF A1K 스토리지 시스템은 NSM100 또는 NSM100B 모듈을 사용하여 NS224 선반을 지원합니다. 두 모듈의 주요 차이점은 다음과 같습니다.

- NSM100 쉘프 모듈은 내장 포트 e0a 및 e0b를 사용합니다.
- NSM100B 쉘프 모듈은 슬롯 1의 포트 e1a와 e1b를 사용합니다.

다음 케이블링 예는 쉘프 모듈 포트를 참조할 때 NS224 쉘프에 있는 NSM100 모듈을 보여줍니다.

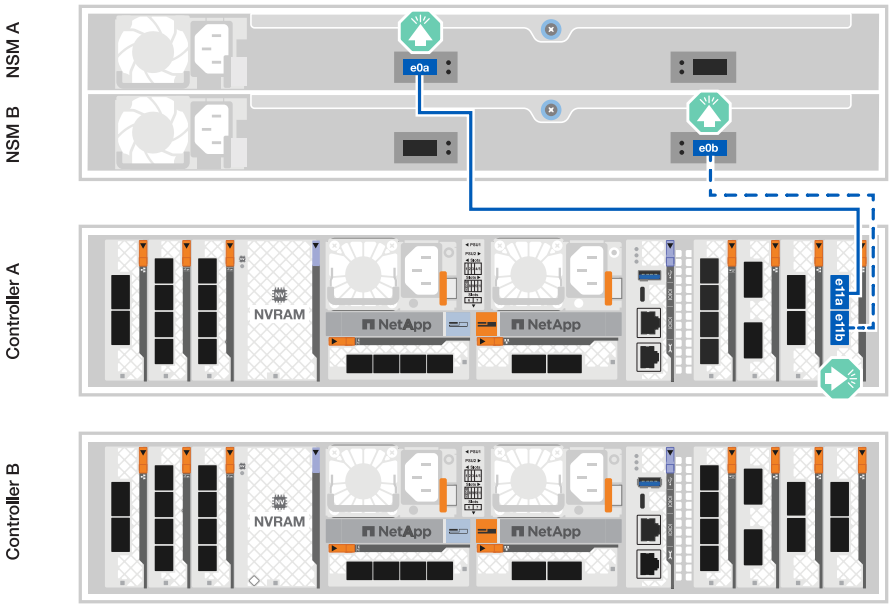
설정에 맞는 다음 케이블 연결 옵션 중 하나를 선택합니다.

옵션 **1: NS224** 스토리지 쉘프 **1**개

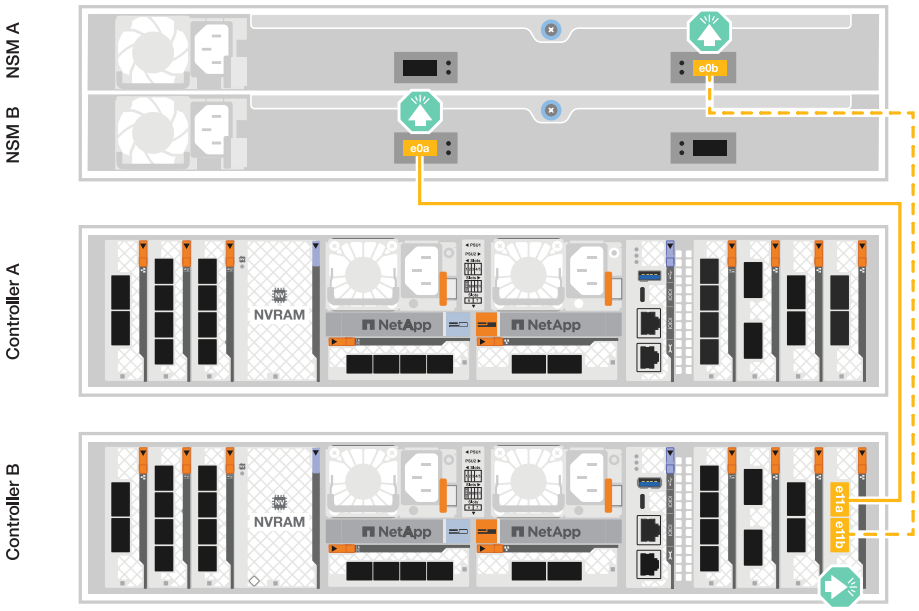
각 컨트롤러를 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

단계

1. 컨트롤러 A에서 다음 포트를 연결합니다.
   a. 포트 e11a를 NSM A 포트 e0a에 연결합니다.
   b. 포트 e11b를 포트 NSM B 포트 e0b에 연결합니다.



2. 컨트롤러 B에서 다음 포트를 연결합니다.
   a. 포트 e11a를 NSM B 포트 e0a에 연결합니다.
   b. 포트 e11b를 NSM A 포트 e0b에 연결합니다.

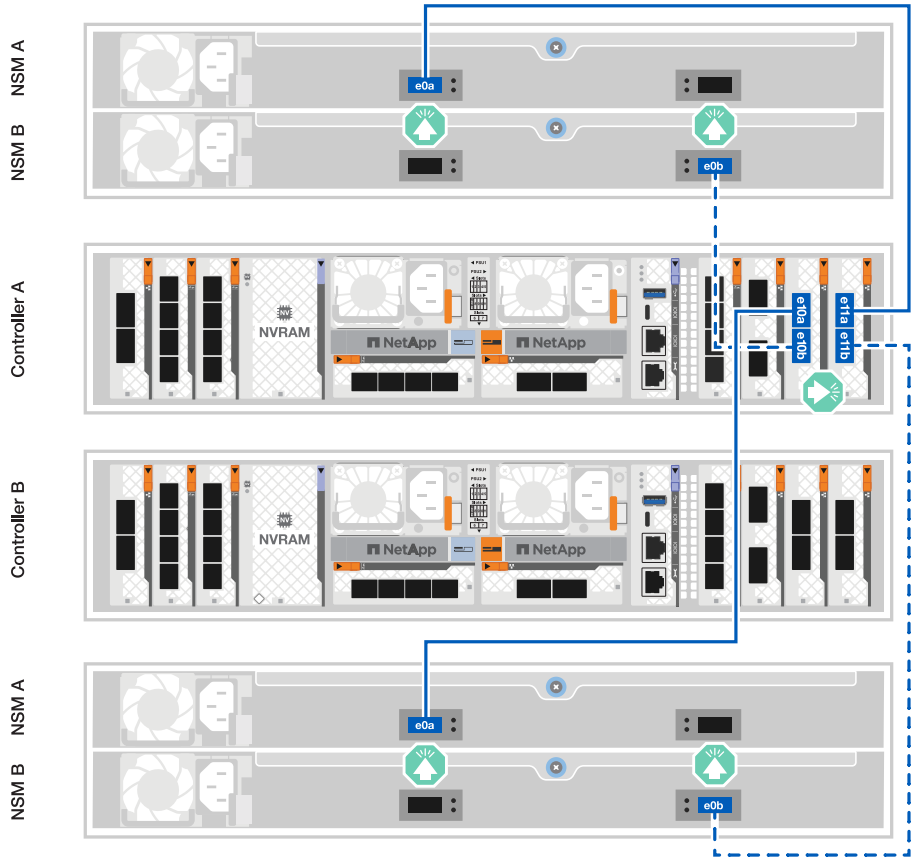


옵션 **2: NS224** 스토리지 쉘프 **2**개

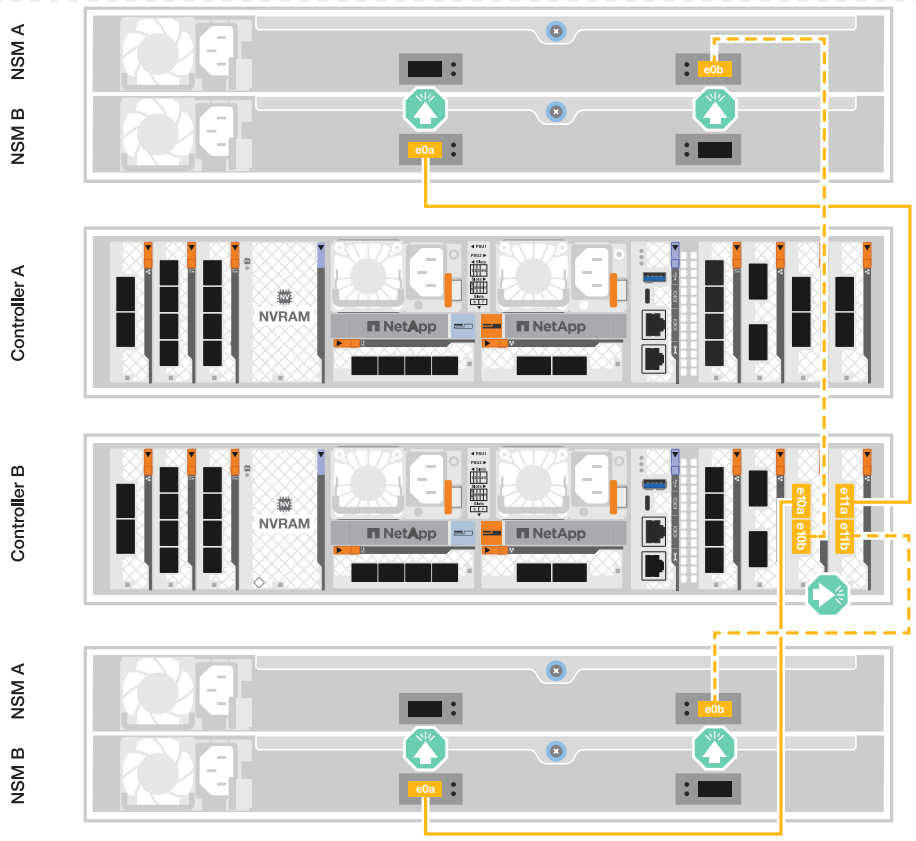
각 컨트롤러를 두 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

단계

1. 컨트롤러 A에서 다음 포트를 연결합니다.
   a. 포트 e11a를 쉘프 1 NSM A 포트 e0a에 연결합니다.
   b. 포트 e11b를 쉘프 2 NSM B 포트 e0b에 연결합니다.
   c. 포트 e10a를 쉘프 2 NSM A 포트 e0a에 연결합니다.
   d. 포트 e10b를 쉘프 1 NSM A 포트 e0b에 연결합니다.



2. 컨트롤러 B에서 다음 포트를 연결합니다.
   a. 포트 e11a를 쉘프 1 NSM B 포트 e0a에 연결합니다.
   b. 포트 e11b를 쉘프 2 NSM A 포트 e0b에 연결합니다.
   c. 포트 e10a를 쉘프 2 NSM B 포트 e0a에 연결합니다.
   d. 포트 e10b를 쉘프 1 NSM A 포트 e0b에 연결합니다.



A70 및 **A90**

AFF A70 및 90 스토리지 시스템은 NSM100 또는 NSM100B 모듈을 사용하여 NS224 선반을 지원합니다. 두 모듈의 주요 차이점은 다음과 같습니다.

- NSM100 선반 모듈은 내장 포트 e0a 및 e0b를 사용합니다.
- NSM100B 쉘프 모듈은 슬롯 1의 포트 e1a와 e1b를 사용합니다.

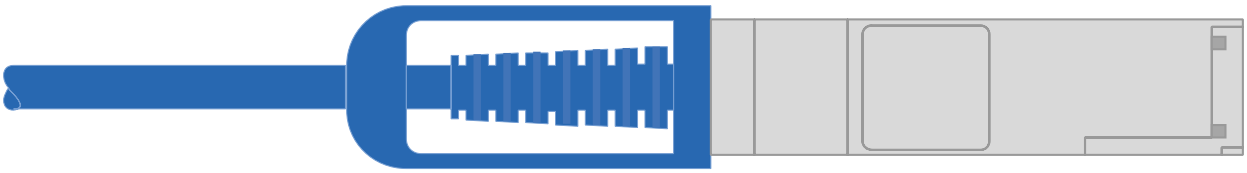
다음 케이블링 예는 쉘프 모듈 포트를 참조할 때 NS224 쉘프에 있는 NSM100 모듈을 보여줍니다.

설정에 맞는 다음 케이블 연결 옵션 중 하나를 선택합니다.

옵션 **1: NS224** 스토리지 쉘프 **1**개

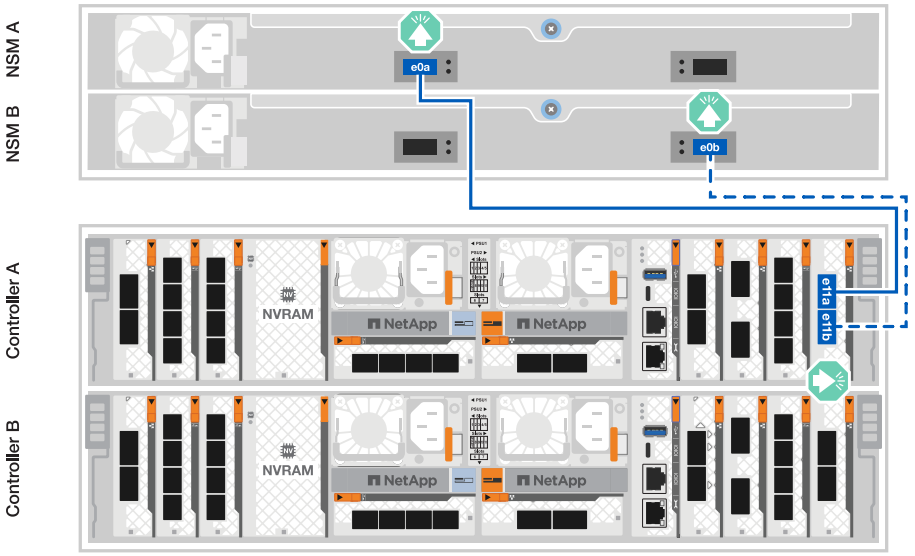
각 컨트롤러를 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

- 100 GbE QSFP28 구리 케이블 *

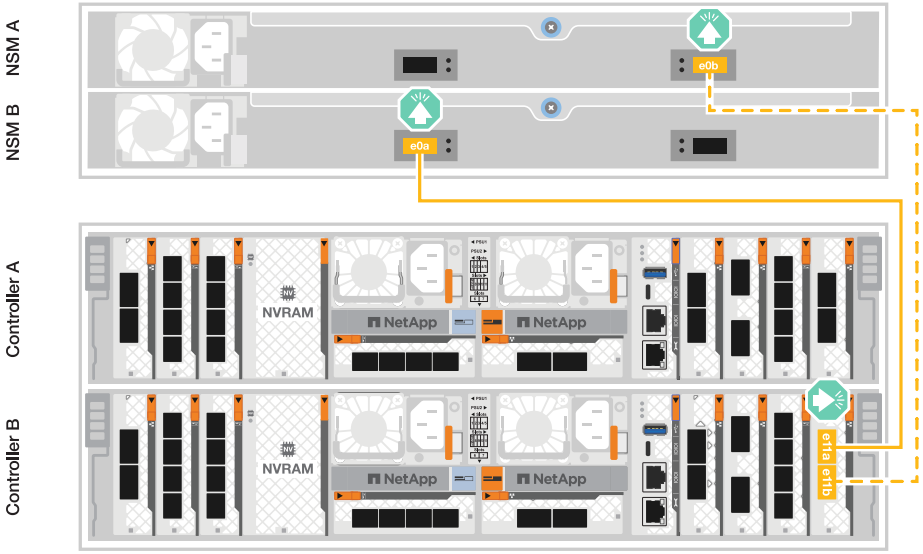


단계

1. 컨트롤러 A 포트 e11a를 NSM A 포트 e0a에 연결합니다.
2. 컨트롤러 A 포트 e11b를 포트 NSM B 포트 e0b에 연결합니다.



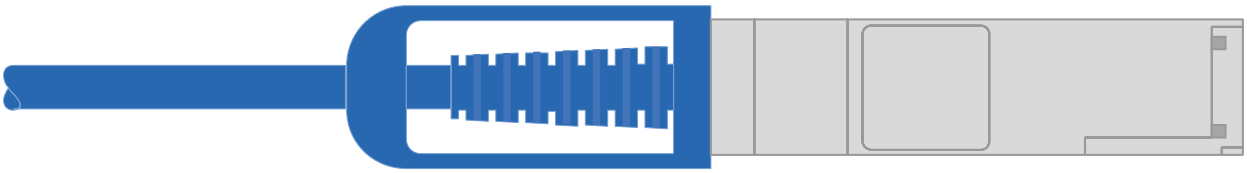
3. 컨트롤러 B 포트 e11a를 NSM B 포트 e0a에 연결합니다.
4. 컨트롤러 B 포트 e11b를 NSM A 포트 e0b에 연결합니다.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e11a
e11b

옵션 **2: NS224** 스토리지 쉘프 **2**개

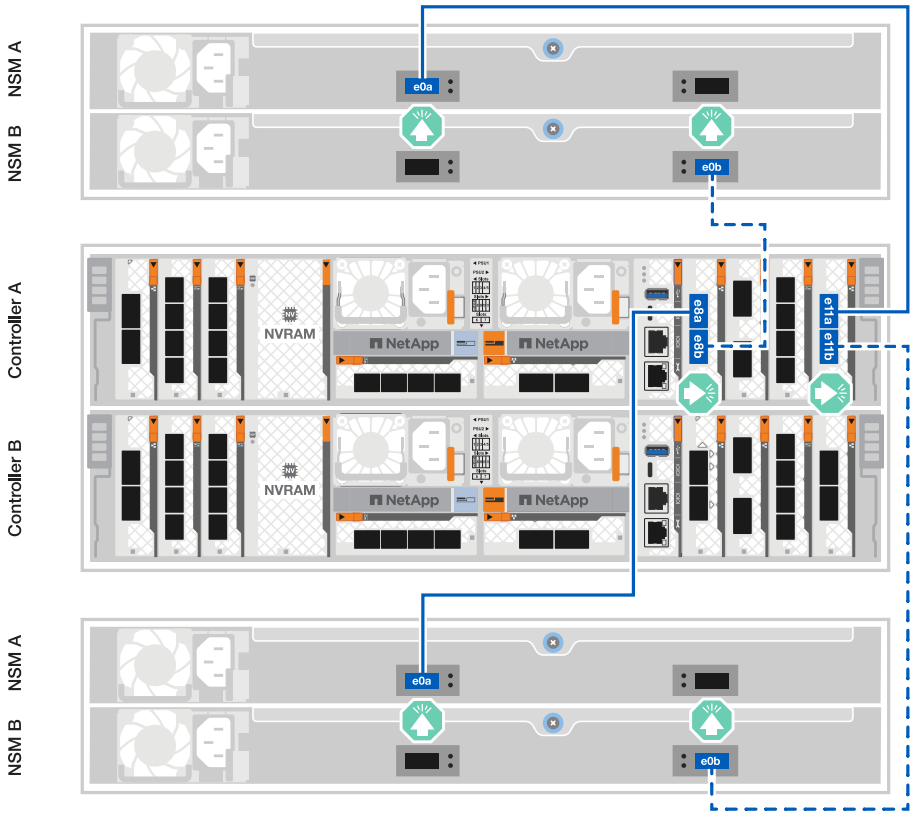
각 컨트롤러를 두 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

- 100 GbE QSFP28 구리 케이블 *



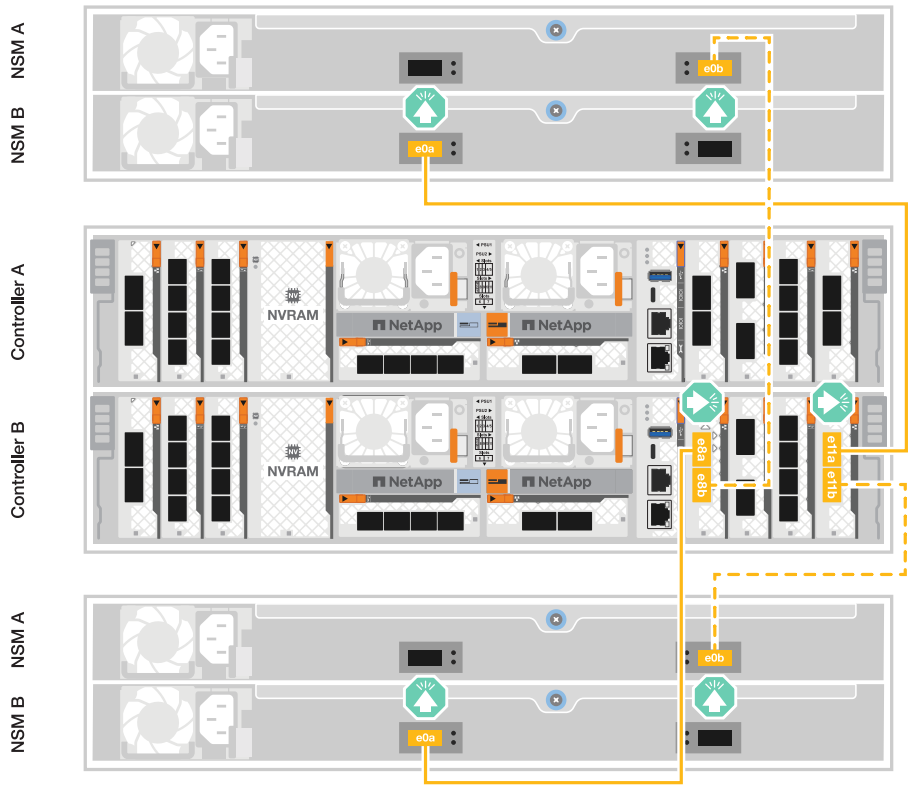
단계

1. 컨트롤러 A에서 다음 포트를 연결합니다.
   a. 포트 e11a를 쉘프 1, NSM A 포트 e0a에 연결합니다.
   b. 포트 e11b를 쉘프 2,NSM B 포트 e0b에 연결합니다.
   c. 포트 e8a를 쉘프 2, NSM A 포트 e0a에 연결합니다.
   d. 포트 e8b를 쉘프 1,NSM B 포트 e0b에 연결합니다.



2. 컨트롤러 B에서 다음 포트를 연결합니다.
   a. 포트 e11a를 쉘프 1, NSM B 포트 e0a에 연결합니다.
   b. 포트 e11b를 쉘프 2,NSM A 포트 e0b에 연결합니다.
   c. 포트 e8a를 쉘프 2, NSM B 포트 e0a에 연결합니다.

d. 포트 e8b를 쉘프 1,NSM A 포트 e0b에 연결합니다.



A20, A30, A50을 지원합니다

NS224 쉘프 케이블 연결 절차는 NSM100 모듈 대신 NSM100B 모듈을 사용합니다. 케이블 연결은 사용된 NSM 모듈의 종류와 관계없이 동일하며, 포트 이름만 다릅니다.

- NSM100B 모듈은 슬롯 1의 I/O 모듈에서 포트 e1a 및 e1b를 사용합니다.
- NSM100 모듈은 내장(온보드) 포트 e0a 및 e0b를 사용합니다.

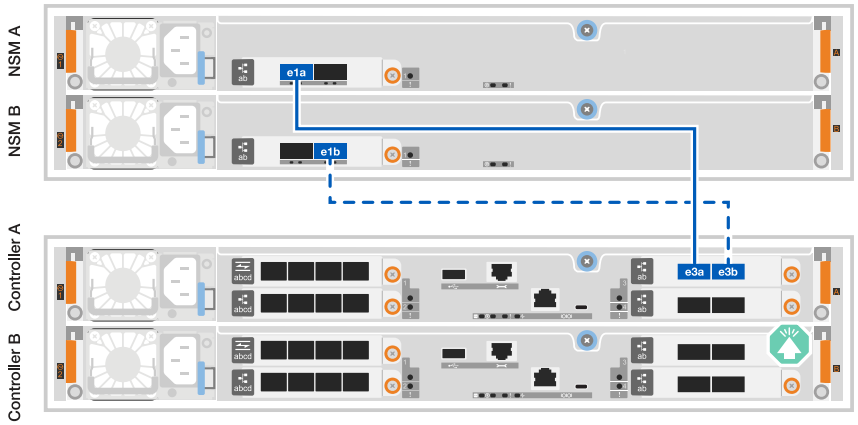
스토리지 시스템과 함께 제공된 스토리지 케이블을 사용하여 NS224 선반의 각 NSM 모듈에 각 컨트롤러를 케이블로 연결합니다. 스토리지 케이블의 케이블 유형은 다음과 같습니다.

- 100 GbE QSFP28 구리 케이블 *

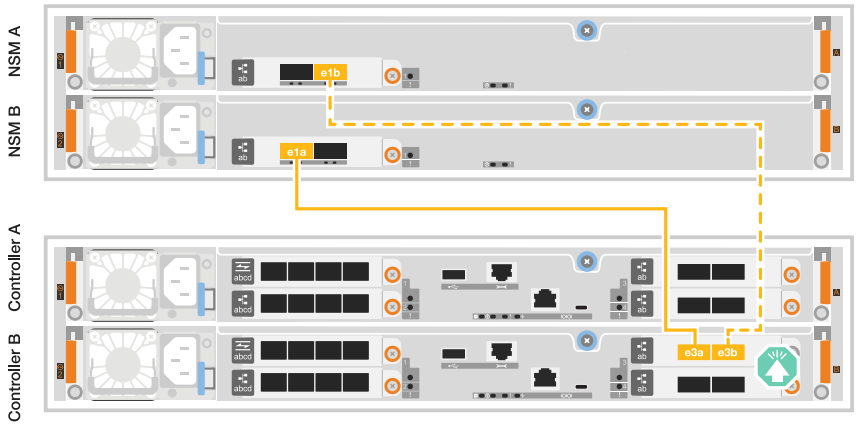
그래픽은 컨트롤러 A 케이블을 파란색으로, 컨트롤러 B 케이블은 노란색으로 표시합니다.

단계

1. 컨트롤러 A를 쉘프에 연결:
   a. 컨트롤러 A 포트 e3a를 NSM A 포트 e1a에 연결합니다.
   b. 컨트롤러 A 포트 e3b를 NSM B 포트 e1b에 연결합니다.



2. 컨트롤러 B를 쉘프에 연결:
   a. 컨트롤러 B 포트 e3a를 NSM B 포트 e1a에 연결합니다.
   b. 컨트롤러 B 포트 e3b를 NSM A 포트 e1b에 연결합니다.



C30를 참조하십시오

NS224 쉘프 케이블 연결 절차는 NSM100 모듈 대신 NSM100B 모듈을 사용합니다. 케이블 연결은 사용된 NSM 모듈의 종류와 관계없이 동일하며, 포트 이름만 다릅니다.

- NSM100B 모듈은 슬롯 1의 I/O 모듈에서 포트 e1a 및 e1b를 사용합니다.
- NSM100 모듈은 내장(온보드) 포트 e0a 및 e0b를 사용합니다.

스토리지 시스템과 함께 제공된 스토리지 케이블을 사용하여 NS224 선반의 각 NSM 모듈에 각 컨트롤러를 케이블로 연결합니다. 스토리지 케이블의 케이블 유형은 다음과 같습니다.

- 100 GbE QSFP28 구리 케이블 *

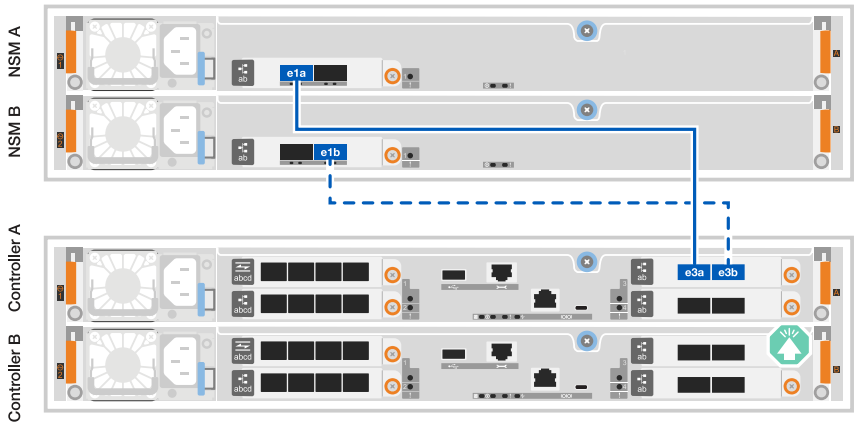
그래픽은 컨트롤러 A 케이블을 파란색으로, 컨트롤러 B 케이블은 노란색으로 표시합니다.

단계

1. 컨트롤러 A를 쉘프에 연결:

a. 컨트롤러 A 포트 e3a를 NSM A 포트 e1a에 연결합니다.

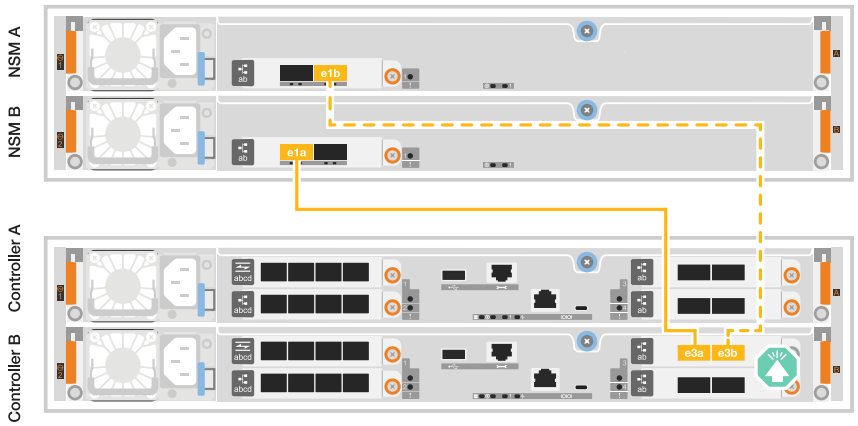
b. 컨트롤러 A 포트 e3b를 NSM B 포트 e1b에 연결합니다.



2. 컨트롤러 B를 쉘프에 연결:

a. 컨트롤러 B 포트 e3a를 NSM B 포트 e1a에 연결합니다.

b. 컨트롤러 B 포트 e3b를 NSM A 포트 e1b에 연결합니다.



다음 단계

스토리지 컨트롤러를 네트워크에 연결한 다음, 컨트롤러를 스토리지 쉘프에 연결한 후에"ASA R2 스토리지 시스템의 전원을 켭니다"

ASA R2 스토리지 시스템의 전원을 켭니다

ASA R2 스토리지 시스템용 랙 하드웨어를 설치하고 컨트롤러 및 스토리지 쉘프용 케이블을 설치한 후에는 스토리지 쉘프와 컨트롤러의 전원을 켜야 합니다.

1단계: 쉘프 전원을 켜고 쉘프 **ID**를 할당합니다

각 쉘프는 고유한 쉘프 ID로 구분됩니다. 이 ID는 쉘프가 스토리지 시스템 설정 내에서 구분되도록 합니다.

이 작업에 대해

- 유효한 쉘프 ID는 01부터 99까지입니다.

  컨트롤러 내에 통합된 내부 쉘프(스토리지)가 있는 경우 고정 쉘프 ID 00이 할당됩니다.

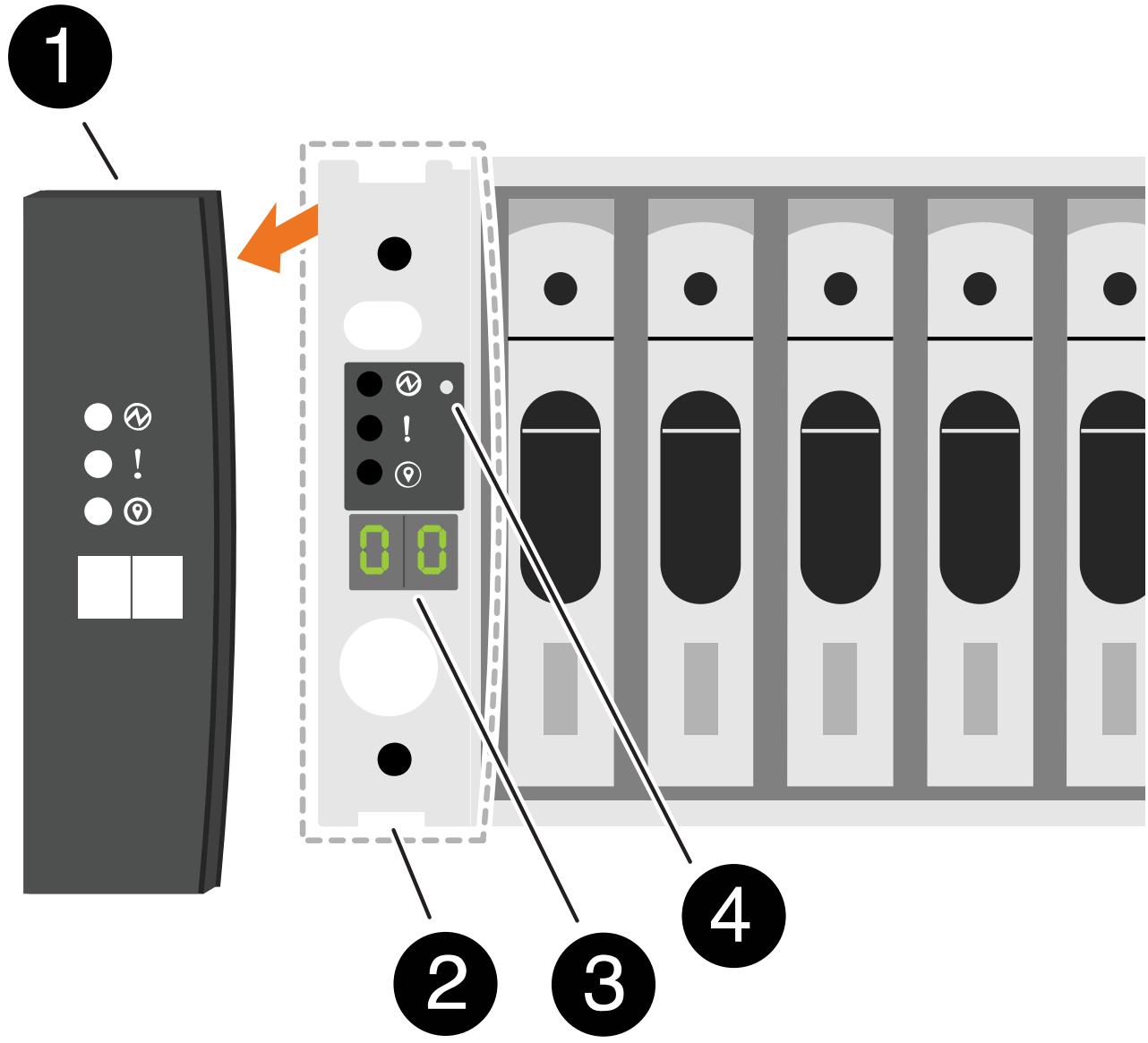
- 쉘프 ID가 적용되려면 쉘프의 전원을 껐다가 다시 켜기(두 전원 코드를 모두 뽑은 다음, 적절한 시간을 기다린 다음 다시 꽂아야 합니다).

단계

1. 전원 코드를 선반에 먼저 연결하고 전원 코드 고정대로 제자리에 고정한 다음 전원 코드를 다른 회로의 전원에 연결하여 선반의 전원을 켭니다.

   셸프의 전원이 켜지고 전원에 연결되면 자동으로 부팅됩니다.

2. 왼쪽 끝 캡을 제거하여 전면판 뒤의 셸프 ID 버튼에 액세스합니다.



1	선반 엔드 캡

2	선반 면판
3	쉘프 ID 번호입니다
4	쉘프 ID 버튼

3. 쉘프 ID의 첫 번째 번호를 변경합니다.

   a. 종이 클립의 곧게 편 끝이나 끝이 뾰족한 볼 포인트 펜을 작은 구멍에 삽입하여 선반 ID 버튼을 누릅니다.

   b. 디지털 디스플레이에서 첫 번째 숫자가 깜박일 때까지 쉘프 ID 버튼을 계속 눌렀다가 놓습니다.

      숫자가 깜박일 때까지 최대 15초가 걸릴 수 있습니다. 그러면 쉘프 ID 프로그래밍 모드가 활성화됩니다.

      ⓘ ID가 깜박이는 데 15초 넘게 걸린 경우 쉘프 ID 버튼을 다시 길게 눌러 완전히 누르십시오.

   c. 쉘프 ID 버튼을 눌렀다가 놓으면 0에서 9 사이의 원하는 번호에 도달할 때까지 번호가 앞으로 이동합니다.

      각 누름 및 해제 시간은 1초 단위로 짧게 설정할 수 있습니다.

   첫 번째 숫자가 계속 깜박입니다.

4. 쉘프 ID의 두 번째 번호를 변경합니다.

   a. 디지털 디스플레이에서 두 번째 숫자가 깜박일 때까지 버튼을 계속 누릅니다.

      숫자가 깜박일 때까지 최대 3초가 걸릴 수 있습니다.

   디지털 디스플레이의 첫 번째 숫자가 깜박임을 멈춥니다.

   a. 쉘프 ID 버튼을 눌렀다가 놓으면 0에서 9 사이의 원하는 번호에 도달할 때까지 번호가 앞으로 이동합니다.

      두 번째 숫자가 계속 깜박입니다.

5. 원하는 번호를 잠그고 두 번째 숫자의 깜박임이 멈출 때까지 쉘프 ID 버튼을 길게 눌러 프로그래밍 모드를 종료합니다.

   숫자가 깜박임을 멈추는 데 최대 3초가 걸릴 수 있습니다.

   디지털 디스플레이의 두 숫자가 깜박이기 시작하고 약 5초 후에 황색 LED가 켜지면서 보류 중인 쉘프 ID가 아직 적용되지 않았음을 알려줍니다.

6. 쉘프 ID가 적용되도록 쉘프 전원을 10초 이상 껐다가 다시 켭니다.

   a. 쉘프의 두 전원 공급 장치에서 전원 코드를 뽑습니다.

   b. 10초 동안 기다립니다.

   c. 전원 코드를 쉘프 전원 공급 장치에 다시 꽂아 전원을 껐다가 다시 켭니다.

      전원 코드를 연결하면 전원 공급 장치가 켜집니다. 이중 LED가 녹색으로 켜집니다.

7. 왼쪽 엔드 캡을 다시 장착합니다.

2단계**:** 컨트롤러의 전원을 켭니다

스토리지 쉘프를 켜고 고유한 ID를 할당한 후 스토리지 컨트롤러의 전원을 켭니다.

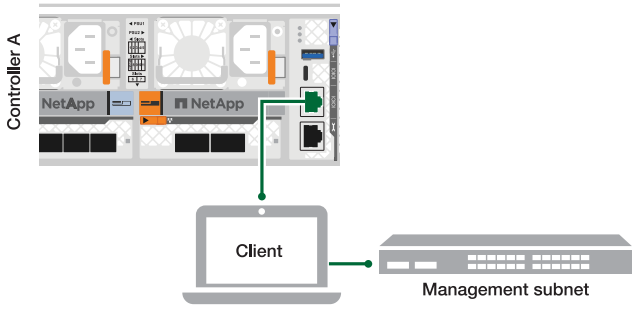
단계

1. 랩톱을 직렬 콘솔 포트에 연결합니다. 이렇게 하면 컨트롤러의 전원이 켜져 있을 때 부팅 순서를 모니터링할 수 있습니다.
   a. 노트북의 직렬 콘솔 포트를 N-8-1에서 115,200보드로 설정합니다.

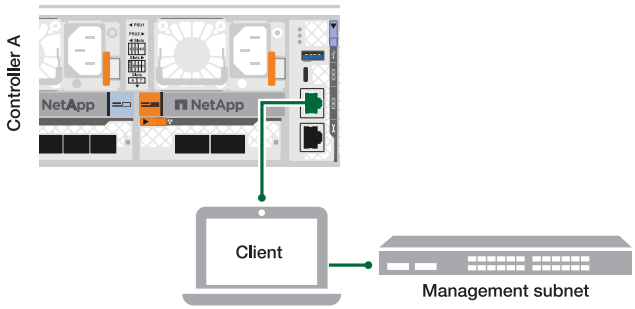
      직렬 콘솔 포트를 구성하는 방법에 대한 지침은 노트북의 온라인 도움말을 참조하십시오.

   b. 콘솔 케이블을 랩톱에 연결하고 스토리지 시스템과 함께 제공된 콘솔 케이블을 사용하여 컨트롤러의 시리얼 콘솔 포트를 연결합니다.
   c. 랩톱을 관리 서브넷의 스위치에 연결합니다.

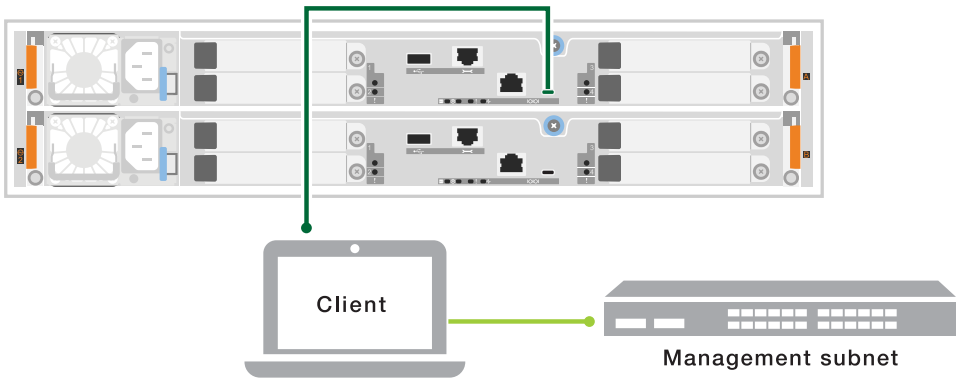
A1K를 참조하십시오



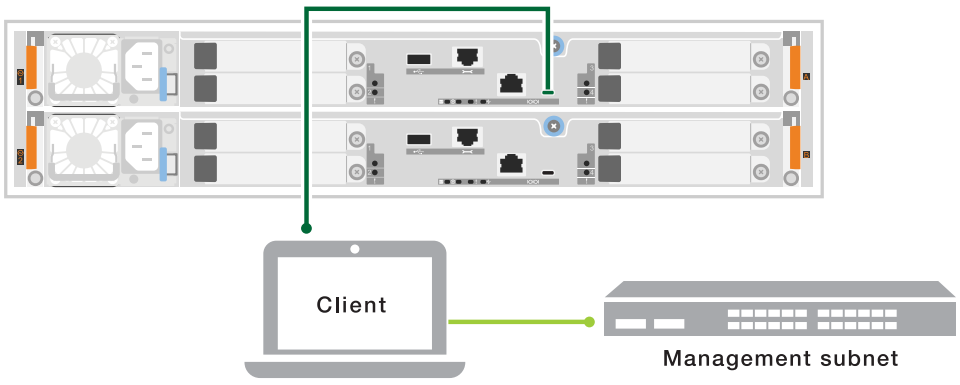
A70 및 **A90**



A20, A30, A50을 지원합니다



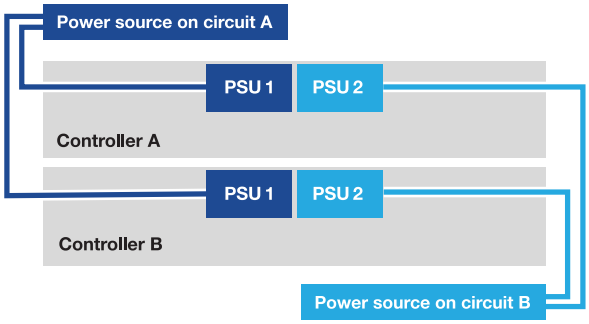
C30를 참조하십시오



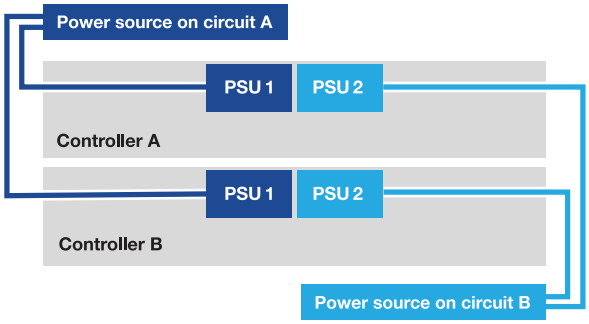
2. 관리 서브넷에 있는 주소를 사용하여 랩톱에 TCP/IP 주소를 할당합니다.

3. 전원 코드를 컨트롤러 전원 공급 장치에 연결한 다음 다른 회로의 전원 공급 장치에 연결합니다.

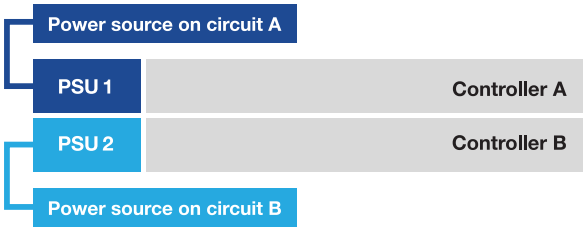
A1K를 참조하십시오



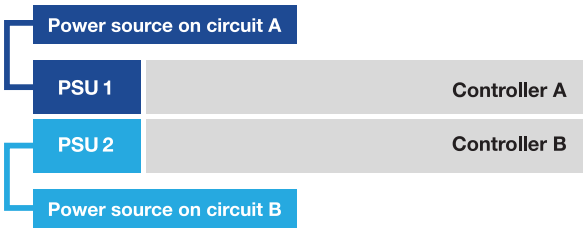
A70 및 **A90**



A20, A30, A50을 지원합니다



C30를 참조하십시오



- 시스템이 부팅 프로세스를 시작합니다. 초기 부팅 순서는 8분 정도 걸릴 수 있습니다.
- 부팅 프로세스 중에 LED가 깜박이고 팬이 활성화되어 컨트롤러의 전원이 켜지는 것을 확인할 수 있습니다.
- 처음 시동할 때 팬에서 높은 수준의 소음이 발생할 수 있습니다. 시동 중 팬 소음이 정상입니다.
- ASA A20, A30, A50 및 ASA C30 스토리지 시스템의 경우 시스템 섀시 전면의 선반 ID 디스플레이가 켜지지 않습니다.

4. 각 전원 공급 장치의 고정 장치를 사용하여 전원 코드를 고정합니다.

다음 단계

ASA R2 스토리지 시스템을 켜면 "ONTAP ASA R2 클러스터를 설정합니다"됩니다.

ASA R2 시스템을 설정합니다

ASA R2 스토리지 시스템에서 ONTAP 클러스터를 설정합니다

ONTAP System Manager는 ONTAP ASA R2 클러스터를 설정하는 빠르고 쉬운 워크플로를 안내합니다.

클러스터 설정 중에 기본 데이터 스토리지 가상 머신(VM)이 생성됩니다. 필요에 따라 DNS(Domain Name System)를 설정하여 호스트 이름을 확인하고, 클러스터가 시간 동기화에 NTP(Network Time Protocol)를 사용하도록 설정하고, 저장된 데이터의 암호화를 사용하도록 설정할 수 있습니다.

특정 상황에서는 다음과 같은 조치가 필요할 수 있습니다. "ONTAP 명령줄 인터페이스(CLI)를 사용하여 클러스터를 설정하십시오.". 예를 들어 보안 프로토콜 때문에 랩톱을 관리 스위치에 연결할 수 없거나 Windows가 아닌 운영 체제를 사용하는 경우 CLI를 사용해야 합니다.

시작하기 전에

다음 정보를 수집합니다.

- 클러스터 관리 IP 주소입니다

  클러스터 관리 IP 주소는 클러스터 관리자가 관리 스토리지 VM에 액세스하고 클러스터를 관리하는 데 사용하는 클러스터 관리 인터페이스에 대한 고유한 IPv4 주소입니다. 조직의 IP 주소 할당 담당자로부터 이 IP 주소를 얻을 수 있습니다.

- 네트워크 서브넷 마스크

  클러스터 설정 중에 ONTAP은 해당 구성에 적합한 네트워크 인터페이스 세트를 권장합니다. 필요한 경우 권장 사항을 조정할 수 있습니다.

- 네트워크 게이트웨이 IP 주소입니다
- 파트너 노드 IP 주소입니다
- DNS 도메인 이름입니다
- DNS 이름 서버 IP 주소입니다
- NTP 서버 IP 주소입니다
- 데이터 서브넷 마스크

단계

1. 클러스터 네트워크를 검색합니다
   a. 랩톱을 관리 스위치에 연결하고 네트워크 컴퓨터 및 장치에 액세스합니다.
   b. 파일 탐색기를 엽니다.
   c. 네트워크 * 를 선택한 다음 마우스 오른쪽 버튼을 클릭하고 * 새로 고침 * 을 선택합니다.
   d. ONTAP 아이콘 중 하나를 선택한 다음 화면에 표시된 인증서를 수락합니다.

System Manager가 열립니다.

2. 암호 * 에서 관리자 계정에 대한 강력한 암호를 만듭니다.

   암호는 8자 이상이어야 하며 문자와 숫자를 하나 이상 포함해야 합니다.

3. 암호를 다시 입력하여 확인한 후 * Continue * 를 선택합니다.
4. 네트워크 주소 * 에 스토리지 시스템 이름을 입력하거나 기본 이름을 그대로 사용합니다.

   기본 스토리지 시스템 이름을 변경하는 경우 새 이름은 문자로 시작해야 하며 44자 미만이어야 합니다. 이름에 마침표(.), 하이픈(-) 또는 밑줄(_)을 사용할 수 있습니다.

5. 파트너 노드의 클러스터 관리 IP 주소, 서브넷 마스크, 게이트웨이 IP 주소 및 IP 주소를 입력한 다음 * Continue * 를 선택합니다.
6. 네트워크 서비스 * 에서 * 호스트 이름을 확인하기 위해 도메인 이름 시스템(DNS)을 사용하고 * 네트워크 시간 프로토콜(NTP)을 사용하여 시간을 동기화하려면 * 원하는 옵션을 선택합니다.

   DNS를 사용하도록 선택한 경우 DNS 도메인 및 이름 서버를 입력합니다. NTP를 사용하도록 선택한 경우 NTP 서버를 입력한 다음 * 계속 * 을 선택합니다.

7. Encryption * 에 Onboard Key Manager(OKM)에 대한 암호를 입력합니다.

   기본적으로 Onboard Key Manager(OKM)를 사용하여 유휴 데이터 암호화가 선택됩니다. 외부 키 관리자를 사용하려면 선택 사항을 업데이트합니다.

   선택적으로 클러스터 설정이 완료된 후 암호화에 대해 클러스터를 구성할 수 있습니다.

8. Initialize * 를 선택합니다.

   설정이 완료되면 클러스터의 관리 IP 주소로 리디렉션됩니다.

9. 네트워크 * 아래에서 * 프로토콜 구성 * 을 선택합니다.

IP(iSCSI 및 **NVMe/TCP)**를 구성하려면 다음을 수행합니다**.**	**FC** 및 **NVMe/FC**를 구성하려면 다음을 수행합니다**.**
a. IP * 를 선택한 다음 * IP 인터페이스 구성 * 을 선택합니다. b. Add a subnet * 을 선택합니다. c. 서브넷의 이름을 입력한 다음 서브넷 IP 주소를 입력합니다. d. 서브넷 마스크를 입력하고 선택적으로 게이트웨이를 입력한 다음 * 추가 * 를 선택합니다. e. 방금 만든 서브넷을 선택한 다음 * 저장 * 을 선택합니다. f. 저장 * 을 선택합니다.	a. FC * 를 선택한 다음 * Configure FC interfaces * 및/또는 * Configure NVMe/FC interfaces * 를 선택합니다. b. FC 및/또는 NVMe/FC 포트를 선택한 다음 * Save * 를 선택합니다.

10. 필요한 경우 를 다운로드하고 "ActiveIQ Config Advisor"실행하여 구성을 확인합니다.

ActiveIQ Config Advisor 는 일반적인 구성 오류를 확인하는 NetApp 시스템용 툴입니다.

다음 단계

이제 "데이터 액세스를 설정합니다"SAN 클라이언트에서 ASA R2 시스템으로 전환할 준비가 되었습니다.

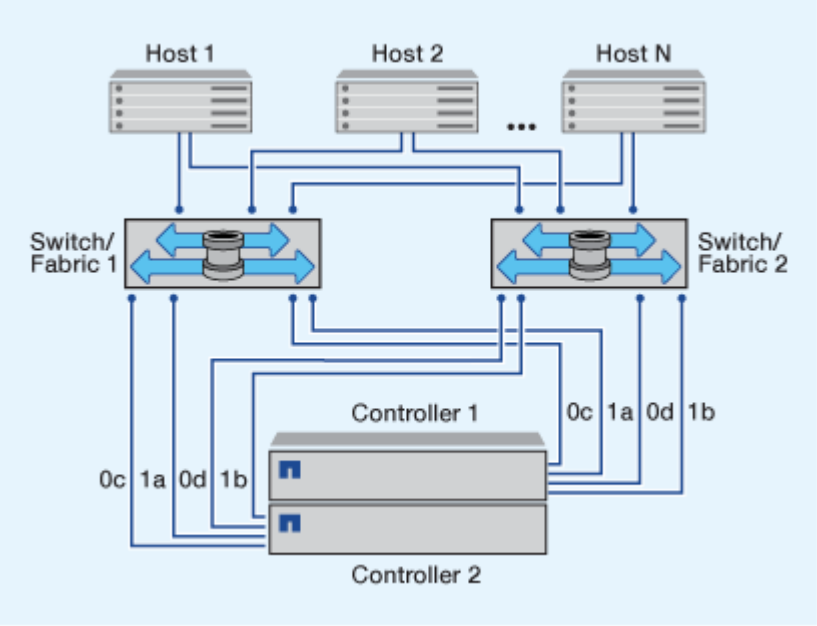
ASA R2 시스템을 사용한 SAN 호스트 구성

ASA R2 시스템은 SAN 호스트 구성에 대해 다른 모든 ONTAP 시스템과 동일한 권장 사항 및 지침을 따릅니다.

스토리지 시스템을 하나 이상의 SAN 호스트에 연결하려면 두 개 이상의 스위치를 사용하는 것이 좋습니다. iSCSI 구성의 경우 호스트, 스위치 및 스토리지 시스템을 연결하는 네트워크 토폴로지를 _network_라고 합니다. FC 및 FC-NVMe 구성의 경우 이 동일한 네트워크 토폴로지를 a_fabric_이라고 합니다.

다중 네트워크/다중 패브릭 구성(둘 이상의 스위치를 사용하는 구성)은 스위치와 스토리지 계층 모두에서 이중화를 제공하기 때문에 권장됩니다. 이러한 이중화를 통해 스토리지 시스템의 내결함성 기능을 강화하고 무중단 운영을 지원할 수 있습니다.

다음 그림은 두 개의 패브릭을 사용하여 단일 HA 쌍에 액세스하는 여러 호스트로 구성된 FC 구성의 예입니다. FC 대상 포트 번호(0c, 0d, 1a, 1b)도 예입니다. 실제 포트 번호는 시스템 모델과 확장 어댑터를 사용하는지 여부에 따라 달라집니다.



에 대해 자세히 "iSCSI 호스트에 대한 SAN 구성"알아보십시오. 에 대해 자세히 "FC 및 FC/NVMe 호스트에 대한 SAN 구성"알아보십시오.

FC 호스트에 대한 조닝 권장 사항

조닝을 사용하도록 FC 호스트를 구성해야 합니다. ASA R2 시스템은 다른 모든 ONTAP 시스템과 동일한 FC 호스트 조닝 권장 사항 및 지침을 따릅니다.

존은 Fabric 내에서 하나 이상의 포트를 논리적으로 그룹화한 것입니다. 장치가 서로를 검색하고 세션을 설정하여 통신할 수 있도록 하려면 두 포트 모두 공통 영역 멤버십이 있어야 합니다.

에 대해 자세히 "FC/FC-NVMe 조닝"알아보십시오.

SAN 호스트에서 ASA R2 스토리지 시스템으로의 데이터 액세스가 가능합니다

데이터 액세스를 설정하려면 ONTAP에서 올바르게 작동하기 위해 SAN 클라이언트의 중요 매개변수 및 설정이 올바르게 구성되어 있는지 확인해야 합니다. VMware 환경을 위한 스토리지를 제공하는 경우 간단히 ASA R2 스토리지를 관리할 수 있도록 OTV 10.3을 설치해야 합니다.

SAN 호스트에서 데이터 액세스 설정

SAN 호스트에서 ASA R2 시스템에 대한 데이터 액세스를 설정하는 데 필요한 구성은 호스트 운영 체제 및 프로토콜에 따라 다릅니다. 최상의 성능과 성공적인 페일오버를 위해서는 올바른 구성이 중요합니다.

"VMware vSphere SCSI 클라이언트""VMware vSphere NVMe 클라이언트""기타 SAN 클라이언트"ASA R2 시스템에 접속하도록 호스트를 적절히 구성하려면 에 대한 ONTAP SAN 호스트 설명서를 참조하십시오.

VMware 가상 시스템을 마이그레이션합니다

ASA 스토리지 시스템에서 ASA r2 스토리지 시스템으로 VM 작업 부하를 마이그레이션해야 하는 경우 NetApp 다음을 권장합니다."VMware vSphere vMotion을 참조하십시오" 데이터의 실시간, 중단 없는 마이그레이션을 수행합니다.

ASA r2 스토리지 유닛은 기본적으로 씬 프로비저닝됩니다. VM 워크로드를 마이그레이션할 때 가상 디스크(VMDK)도 씬 프로비저닝해야 합니다.

관련 정보

- 자세히 알아보세요 "vSphere에 ONTAP 사용하는 이점" .
- 에 대해 알아보세요"ONTAP 사용한 VMware 라이브 사이트 복구" .
- 에 대해 알아보세요"vSphere 환경을 위한 지속적인 가용성 솔루션" .
- 자세히 알아보세요"ONTAP SAN ASA 스토리지 시스템에 Broadcom VMware ESXi iSCSI MPIO를 설정하는 방법" .

타사 스토리지 시스템에서 데이터 마이그레이션

ONTAP 9.17.1부터 FLI(Foreign LUN Import)를 사용하여 타사 스토리지 시스템의 LUN에서 ASA r2 시스템으로 데이터를 마이그레이션할 수 있습니다. FLI를 사용하여 데이터 마이그레이션을 수행하면 마이그레이션 프로세스 중 데이터 손실 및 다운타임 위험을 줄이는 데 도움이 됩니다.

FLI는 온라인 및 오프라인 마이그레이션을 모두 지원합니다. 온라인 마이그레이션에서는 클라이언트 시스템이 온라인 상태를 유지하는 동안 타사 스토리지 시스템에서 ONTAP 스토리지 시스템으로 데이터가 복사됩니다. 온라인 마이그레이션은 Windows, Linux 및 ESXi 호스트 운영 체제에서 지원됩니다. 오프라인 마이그레이션에서는 클라이언트 시스템이 오프라인 상태로 전환되고, LUN 데이터가 타사 스토리지 시스템에서 ONTAP 스토리지 시스템으로 복사된 후 클라이언트 시스템이 다시 온라인 상태로 전환됩니다.

- 수행 방법을 알아보세요 "FLI 오프라인 마이그레이션" .
- 수행 방법을 알아보세요 "FLI 온라인 마이그레이션" .

ASA R2 시스템을 VMware 환경에서 스토리지 공급자로 구성합니다

VMware용 ONTAP 툴을 사용하면 ASA R2 시스템을 VMware 환경에서 스토리지 공급자로 쉽게 설정할 수 있습니다.

VMware vSphere용 ONTAP 툴은 VMware ESXi 호스트에서 가상 머신을 쉽게 관리할 수 있도록 vCSA(vCenter Server Virtual Appliance)와 함께 작동하는 툴 세트입니다.

ASA R2 시스템은 "VMware vSphere 10.3용 ONTAP 툴"이상에서 지원됩니다.

다음 작업을 수행하는 방법 및 사용 방법에 대해 "VMware용 ONTAP 툴을 구축합니다"알아봅니다.

- "vCenter Server 인스턴스를 추가합니다"
- "ESXi 호스트 설정을 구성합니다"
- "ASA R2 스토리지 시스템 및 호스트를 검색합니다"

다음 단계

"스토리지 용량 할당"SAN 호스트에서 스토리지 유닛에 데이터를 읽고 쓸 수 있도록 할 준비가 되었습니다.

ONTAP를 사용하여 데이터를 관리합니다

ASA R2 스토리지 시스템 비디오 데모

ONTAP System Manager를 사용하여 ASA R2 스토리지 시스템에서 일반적인 작업을 빠르고 쉽게 수행하는 방법을 보여주는 짧은 비디오를 보십시오.

ASA R2 시스템에서 SAN 프로토콜을 구성합니다

"비디오 스크립트"

ASA R2 시스템에서 SAN 스토리지를 프로비저닝합니다

"비디오 스크립트"

ASA R2 시스템에서 원격 클러스터로 데이터를 복제합니다

"비디오 스크립트"

스토리지 관리

ASA R2 시스템에서 ONTAP SAN 스토리지를 프로비저닝합니다

스토리지를 프로비저닝할 때 SAN 호스트가 ASA R2 스토리지 시스템에서 데이터를 읽고 쓸 수 있습니다. 스토리지를 프로비저닝하려면 ONTAP 시스템 관리자를 사용하여 스토리지 유닛을 생성하고 호스트 이니시에이터를 추가한 후 호스트를 스토리지 유닛에 매핑합니다. 읽기/쓰기 작업을 설정하려면 호스트에서 단계를 수행해야 합니다.

스토리지 유닛을 생성합니다

ASA r2 시스템에서 스토리지 장치는 SAN 호스트에 데이터 작업을 위한 스토리지 공간을 제공합니다. 저장 장치는 SCSI 호스트의 경우 LUN을 의미하고, NVMe 호스트의 경우 NVMe 네임스페이스를 의미합니다. 클러스터가 SCSI 호스트를 지원하도록 구성된 경우 LUN을 생성하라는 메시지가 표시됩니다. 클러스터가 NVMe 호스트를 지원하도록 구성된 경우 NVMe 네임스페이스를 만들라는 메시지가 표시됩니다.

ASA r2 스토리지 유닛의 최대 용량은 128TB입니다. 를 참조하십시오"NetApp Hardware Universe를 참조하십시오" ASA r2 시스템의 최신 저장 한도에 대해서는 다음을 참조하세요.

스토리지 장치 생성 프로세스의 일부로 호스트 이니시에이터를 스토리지 장치에 추가하고 매핑합니다. 당신도 할 수 있습니다"추가하다" 그리고"지도" 저장 장치를 만든 후 호스트 이니시에이터를 생성합니다.

ONTAP 9.18.1부터 스토리지 유닛을 생성할 때 스냅샷 예약을 수정하고 자동 스냅샷 삭제를 활성화할 수 있습니다. 스냅샷 예약은 스냅샷을 위해 특별히 예약된 저장 장치의 공간입니다. 스냅샷 예약이 자동 스냅샷 삭제로 설정된 경우, 스냅샷에 사용된 공간이 스냅샷 예약 공간을 초과하면 오래된 스냅샷이 자동으로 삭제됩니다.

"ASA r2 시스템의 스냅샷 예약에 대해 자세히 알아보세요.".

스토리지 유닛은 기본적으로 씬 프로비저닝 방식으로 구성됩니다. 씬 프로비저닝을 사용하면 스토리지 유닛이 할당된 크기까지 확장될 수 있지만 공간을 미리 예약하지는 않습니다. 필요에 따라 사용 가능한 여유 공간에서 공간이 동적으로

할당됩니다. 이를 통해 사용 가능한 공간을 _과잉 프로비저닝_하여 스토리지 효율성을 높일 수 있습니다. 예를 들어 1TB의 여유 공간이 있고 1TB 스토리지 유닛 4개를 생성해야 한다고 가정해 보겠습니다. 시스템에 3TB의 추가 스토리지 용량을 즉시 추가하는 대신 스토리지 유닛을 생성하고 공간 사용량을 모니터링한 다음 스토리지 유닛이 실제 공간을 사용함에 따라 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 "씬 프로비저닝"을 참조하십시오.

단계

1. System Manager에서 * Storage * 를 선택한 다음 를 + Add 선택합니다.
2. 새 스토리지 유닛의 이름을 입력합니다.
3. 만들려는 단위 수를 입력합니다.

   두 개 이상의 스토리지 유닛을 생성하는 경우 각 유닛은 동일한 용량, 호스트 운영 체제 및 호스트 매핑을 사용하여 생성됩니다.

   스토리지 가용성 영역 전체에서 워크로드 밸런싱을 최적화하려면 짝수 개의 스토리지 유닛을 만듭니다.

4. 스토리지 유닛 용량을 입력한 다음 호스트 운영 체제를 선택합니다.

   스토리지 유닛을 두 개 이상 생성하는 경우, 각 유닛은 동일한 용량으로 생성됩니다. 충분한 사용 가능한 공간을 확보하려면 생성할 스토리지 유닛 수에 원하는 용량을 곱하십시오. 사용 가능한 공간이 부족한 상태에서 오버 프로비저닝을 선택한 경우, 공간 부족으로 인한 데이터 손실을 방지하기 위해 사용률을 면밀히 모니터링하십시오.

5. 자동으로 선택된 * 호스트 매핑 * 을 적용하거나 매핑할 스토리지 유닛에 대해 다른 호스트 그룹을 선택합니다.

   *호스트 매핑*은 새로운 저장 장치가 매핑될 호스트 그룹을 의미합니다. 새 스토리지 유닛에 대해 선택한 호스트 유형에 대한 기존 호스트 그룹이 있는 경우, 호스트 매핑을 위해 기존 호스트 그룹이 자동으로 선택됩니다. 자동으로 선택된 호스트 그룹을 수락하거나 다른 호스트 그룹을 선택할 수 있습니다.

   지정한 운영 체제에서 실행 중인 호스트에 대한 기존 호스트 그룹이 없는 경우 ONTAP에서 자동으로 새 호스트 그룹을 생성합니다.

6. 다음 중 하나를 수행하려면 * 추가 옵션 * 을 선택하고 필요한 단계를 완료합니다.

옵션을 선택합니다	단계
기본 QoS(Quality of Service) 정책을 변경합니다 기본 QoS 정책이 스토리지 유닛이 생성되는 스토리지 가상 머신(VM)에 이전에 설정되지 않은 경우 이 옵션을 사용할 수 없습니다.	a. 스토리지 및 최적화 * 에서 * 서비스 품질(QoS) * 옆의 를 선택합니다 ⌄. b. 기존 QoS 정책을 선택합니다.

옵션을 선택합니다	단계
새 QoS 정책을 생성합니다	a. 스토리지 및 최적화 * 에서 * 서비스 품질(QoS) * 옆의 를 선택합니다 . b. Define new policy * 를 선택합니다. c. 새 QoS 정책의 이름을 입력합니다. d. QoS 한도, QoS 보장 또는 둘 다를 설정합니다. i. (선택 사항) * Limit * 아래에 최대 처리량 제한, 최대 IOPS 제한 또는 둘 모두를 입력합니다. 스토리지 유닛의 최대 처리량과 IOPS를 설정하면 중요 워크로드의 성능이 저하되지 않도록 시스템 리소스에 대한 영향이 제한됩니다. ii. 필요한 경우 * Guarantee * 에 최소 처리량, 최소 IOPS 또는 둘 모두를 입력합니다. 스토리지 유닛에 대해 최소 처리량과 IOPS를 설정하면 경쟁 워크로드의 수요에 관계없이 최소 성능 목표를 달성할 수 있습니다. e. 추가 * 를 선택합니다.
기본 성능 서비스 수준을 변경합니다.	a. Storage and optimization * 에서 * Performance service level * 옆에 있는 를 선택합니다 . b. 성능 * 을 선택합니다. ASA r2 시스템은 두 가지 성능 수준을 제공합니다. 기본 성능 수준은 *극단*으로, 사용 가능한 가장 높은 수준입니다. 수준을 *성능*으로 낮출 수 있습니다.
기본 스냅샷 예약을 수정하고 자동 스냅샷 삭제를 활성화합니다.	a. *스냅샷 예약 %*에서 스냅샷에 할당하려는 저장 장치 공간의 백분율에 대한 숫자 값을 입력합니다. b. *오래된 스냅샷을 자동으로 삭제*를 선택합니다.
새 SCSI 호스트를 추가합니다	a. 호스트 정보 * 에서 연결 프로토콜로 * SCSI * 를 선택합니다. b. 호스트 운영 체제를 선택합니다. c. Host Mapping * 아래에서 * New hosts * 를 선택합니다. d. FC * 또는 * iSCSI * 를 선택합니다. e. 기존 호스트 이니시에이터를 선택하거나 * Add initiator * 를 선택하여 새 호스트 이니시에이터를 추가합니다. 유효한 FC WWPN의 예는 "01:02:03:04:0a:0b:0c:0d"입니다. 유효한 iSCSI 이니시에이터 이름의 예로는 "iqn.1995-08.com.example:string" 및 "eui.0123456789abcdef"가 있습니다.

옵션을 선택합니다	단계
새 SCSI 호스트 그룹을 생성합니다	a. 호스트 정보 * 에서 연결 프로토콜로 * SCSI * 를 선택합니다. b. 호스트 운영 체제를 선택합니다. c. 호스트 매핑 * 아래에서 * 새 호스트 그룹 * 을 선택합니다. d. 호스트 그룹의 이름을 입력한 다음 그룹에 추가할 호스트를 선택합니다.
새 NVMe 하위 시스템을 추가합니다	a. 호스트 정보 * 에서 연결 프로토콜로 * NVMe * 를 선택합니다. b. 호스트 운영 체제를 선택합니다. c. 호스트 매핑 * 아래에서 * 새 NVMe 하위 시스템 * 을 선택합니다. d. 하위 시스템의 이름을 입력하거나 기본 이름을 그대로 사용합니다. e. 이니시에이터의 이름을 입력합니다. f. 대역내 인증 또는 TLS(전송 계층 보안)를 활성화하려면 을 선택한 다음 옵션을 선택합니다. 대역 내 인증을 통해 NVMe 호스트와 ASA R2 시스템 간에 안전한 양방향 및 단방향 인증을 수행할 수 있습니다. TLS는 NVMe/TCP 호스트와 ASA R2 시스템 간에 네트워크를 통해 전송되는 모든 데이터를 암호화합니다. g. 이니시에이터를 추가하려면 * 이니시에이터 추가 * 를 선택하십시오. 호스트 NQN을 <nqn.yyyy-mm> 다음에 정규화된 도메인 이름으로 포맷합니다. 연도는 1970년 또는 그 이후여야 합니다. 총 최대 길이는 223이어야 합니다. 유효한 NVMe 이니시에이터의 예는 nqn.2014-08.com.example:string입니다.

7. 추가 * 를 선택합니다.

다음 단계

스토리지 유닛이 생성되어 호스트에 매핑됩니다. 이제 "스냅샷을 생성합니다"ASA R2 시스템의 데이터를 보호할 수 있습니다.

를 참조하십시오

에 대해 자세히 "ASA R2 시스템에서 스토리지 가상 머신을 사용하는 방법"알아보십시오.

호스트 이니시에이터를 추가합니다

언제든지 ASA R2 시스템에 새 호스트 이니시에이터를 추가할 수 있습니다. 이니시에이터는 호스트가 스토리지 유닛을 액세스하고 데이터 작업을 수행할 수 있도록 합니다.

시작하기 전에

호스트 이니시에이터를 추가하는 동안 호스트 구성을 대상 클러스터로 복제하려면 클러스터가 복제 관계에 있어야 합니다. 선택적으로 "복제 관계를 생성합니다"호스트를 추가한 후에 수행할 수 있습니다.

SCSI 또는 NVMe 호스트에 대한 호스트 이니시에이터를 추가합니다.

SCSI 호스트

단계

1. Host * 를 선택합니다.
2. SCSI * 를 선택한 다음 를 + Add 선택합니다.
3. 호스트 이름을 입력하고 호스트 운영 체제를 선택한 다음 호스트 설명을 입력합니다.
4. 호스트 구성을 대상 클러스터로 복제하려면 * Replicate host configuration * 을 선택한 다음 대상 클러스터를 선택합니다.

   호스트 구성을 복제하려면 클러스터가 복제 관계에 있어야 합니다.

5. 새 호스트 또는 기존 호스트를 추가합니다.

새 호스트를 추가합니다	기존 호스트를 추가합니다
a. New hosts * 를 선택합니다. b. FC * 또는 * iSCSI * 를 선택한 다음 호스트 이니시에이터를 선택합니다. c. 필요에 따라 * 호스트 근접성 구성 * 을 선택합니다. ONTAP는 호스트 근접성을 구성하여 데이터 경로를 최적화하고 지연 시간을 줄이기 위해 호스트에 가장 가까운 컨트롤러를 식별할 수 있습니다. 이 옵션은 데이터를 원격 위치에 복제된 경우에만 적용됩니다. 스냅샷 복제를 설정하지 않은 경우에는 이 옵션을 선택할 필요가 없습니다. d. 새 이니시에이터를 추가해야 하는 경우 * 이니시에이터 추가 * 를 선택합니다.	a. Existing hosts * 를 선택합니다. b. 추가할 호스트를 선택합니다. c. 추가 * 를 선택합니다.

6. 추가 * 를 선택합니다.

다음 단계

SCSI 호스트가 ASA R2 시스템에 추가되고 호스트를 스토리지 유닛에 매핑할 준비가 되었습니다.

NVMe 호스트

단계

1. Host * 를 선택합니다.
2. NVMe * 를 선택한 다음 를 선택합니다 + Add .
3. NVMe 하위 시스템의 이름을 입력하고 호스트 운영 체제를 선택한 다음 설명을 입력합니다.
4. Add initiator * 를 선택합니다.

다음 단계

NVMe 호스트가 ASA R2 시스템에 추가되고, 호스트를 스토리지 유닛에 매핑할 수 있습니다.

스토리지 유닛을 호스트에 매핑합니다

ASA r2 스토리지 유닛을 생성하고 호스트 이니시에이터를 추가한 후 호스트를 스토리지 유닛에 매핑하여 데이터 제공을 시작합니다. 저장 장치는 저장 장치 생성 프로세스의 일부로 호스트에 매핑됩니다. 언제든지 기존 스토리지 장치를 새 호스트나 기존 호스트에 매핑할 수도 있습니다.

단계

1. 스토리지 * 를 선택합니다.
2. 매핑할 스토리지 유닛의 이름 위로 마우스를 가져갑니다.
3. 을 선택한 다음 * 호스트에 매핑 * 을 선택합니다.
4. 스토리지 유닛에 매핑할 호스트를 선택한 다음 * Map * 을 선택합니다.

다음 단계

스토리지 유닛이 호스트에 매핑되어 호스트에서 프로비저닝 프로세스를 완료할 준비가 되었습니다.

호스트측 프로비저닝을 완료합니다

스토리지 유닛을 생성하고 호스트 이니시에이터를 추가하고 스토리지 유닛을 매핑한 후에는 호스트에서 ASA R2 시스템에서 데이터를 읽고 쓰기 전에 수행해야 하는 단계가 있습니다.

단계

1. FC 및 FC/NVMe의 경우 WWPN을 기준으로 FC 스위치를 조닝합니다.

   이니시에이터당 하나의 존을 사용하고 각 존에 모든 타겟 포트를 포함합니다.

2. 새 저장 장치를 확인해 보십시오.
3. 스토리지 유닛을 초기화하고 파일 시스템을 생성합니다.
4. 호스트가 스토리지 유닛의 데이터를 읽고 쓸 수 있는지 확인합니다.

다음 단계

프로비저닝 프로세스를 완료했으며 데이터 서비스를 시작할 준비가 되었습니다. 이제 "스냅샷을 생성합니다"ASA R2 시스템의 데이터를 보호할 수 있습니다.

를 참조하십시오

호스트측 구성에 대한 자세한 내용은 "ONTAP SAN 호스트 설명서"해당 호스트의 를 참조하십시오.

ASA R2 스토리지 시스템에 데이터를 복제합니다

데이터 클론 생성은 ONTAP System Manager를 사용하여 ASA R2 시스템에서 스토리지 유닛 및 정합성 보장 그룹의 복제본을 생성하며, 이 복제본은 애플리케이션 개발, 테스트, 백업, 데이터 마이그레이션 또는 기타 관리 기능에 사용할 수 있습니다.

스토리지 유닛 복제

스토리지 유닛을 클론하면 ASA R2 시스템에서 클론한 스토리지 유닛의 쓰기 가능한 시점 복제본인 새 스토리지 유닛을 생성합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 복제할 스토리지 유닛의 이름 위에 마우스를 놓습니다.
3. 를 선택한 다음 * Clone * 을 선택합니다.
4. 클론으로 생성될 새 스토리지 유닛의 기본 이름을 그대로 사용하거나 새 스토리지 유닛을 입력합니다.
5. 호스트 운영 체제를 선택합니다.

   클론에 대한 새 스냅샷은 기본적으로 생성됩니다.

6. 기존 스냅샷을 사용하거나, 새 호스트 그룹을 생성하거나, 새 호스트를 추가하려면 * More Options * 를 선택합니다.

옵션을 선택합니다	단계
기존 스냅샷을 사용합니다	a. 복제할 스냅샷 * 아래에서 * 기존 snaphot 사용 * 을 선택합니다. b. 클론에 사용할 스냅샷을 선택합니다.
새 호스트 그룹을 생성합니다	a. 호스트 매핑 * 아래에서 * 새 호스트 그룹 * 을 선택합니다. b. 새 호스트 그룹의 이름을 입력한 다음 그룹에 포함할 호스트 이니시에이터를 선택합니다.
새 호스트를 추가합니다	a. Host mapping * 아래에서 * New hosts * 를 선택합니다. b. 새 호스트의 이름을 입력한 다음 * FC * 또는 * iSCSI * 를 선택합니다. c. 기존 이니시에이터 목록에서 호스트 이니시에이터를 선택하거나 * Add * 를 선택하여 호스트의 새 이니시에이터를 추가합니다.

7. 클론 * 을 선택합니다.

다음 단계

클론한 스토리지 유닛과 동일한 새 스토리지 유닛을 생성했습니다. 이제 필요에 따라 새 저장 장치를 사용할 준비가 되었습니다.

클론 정합성 보장 그룹

일관성 그룹을 클론 복제하면 클론 복제된 일관성 그룹에 구조, 스토리지 유닛 및 데이터가 동일한 새 일관성 그룹을 생성합니다. 일관성 그룹 클론을 사용하여 애플리케이션 테스트를 수행하거나 데이터를 마이그레이션할 수 있습니다. 예를 들어, 일관성 그룹 밖으로 운영 워크로드를 마이그레이션해야 한다고 가정합니다. 정합성 보장 그룹을 클론하여 운영 워크로드의 복제본을 생성하여 마이그레이션이 완료될 때까지 백업으로 유지할 수 있습니다.

클론은 클론 복제할 일관성 그룹의 스냅샷에서 생성됩니다. 클론 생성 프로세스가 기본적으로 시작되는 시점에 클론에 사용되는 스냅샷이 생성됩니다. 기존 스냅샷을 사용하도록 기본 동작을 수정할 수 있습니다.

스토리지 유닛 매핑은 클론 생성 프로세스의 일부로 복사됩니다. 스냅샷 정책은 클론 복제 프로세스의 일부로 복사되지 않습니다.

ASA R2 시스템에 로컬로 저장된 정합성 보장 그룹 또는 원격 위치에 복제된 정합성 보장 그룹에서 클론을 생성할 수 있습니다.

로컬 스냅샷을 사용하여 클론을 생성합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 클론 복제할 일관성 그룹 위에 마우스를 놓습니다.
3. 를 선택한 다음 * Clone * 을 선택합니다.
4. 일관성 그룹 클론의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
5. 호스트 운영 체제를 선택합니다.
6. 소스 정합성 보장 그룹에서 클론을 분리하고 디스크 공간을 할당하려면 * Split clone * 을 선택합니다.
7. 기존 스냅샷을 사용하려면 새 호스트 그룹을 생성하거나 클론에 새 호스트를 추가하려면 * More Options * 를 선택합니다.

옵션을 선택합니다	단계
기존 스냅샷을 사용합니다	a. 복제할 스냅샷 * 아래에서 * 기존 스냅샷 사용 * 을 선택합니다. b. 클론에 사용할 스냅샷을 선택합니다.
새 호스트 그룹을 생성합니다	a. 호스트 매핑 * 아래에서 * 새 호스트 그룹 * 을 선택합니다. b. 새 호스트 그룹의 이름을 입력한 다음 그룹에 포함할 호스트 이니시에이터를 선택합니다.
새 호스트를 추가합니다	a. Host mapping * 아래에서 * New hosts * 를 선택합니다. b. 새 호스트 이름을 입력한 다음 * FC * 또는 * iSCSI * 를 선택합니다. c. 기존 이니시에이터 목록에서 호스트 이니시에이터를 선택하거나 * 이니시에이터 추가 * 를 선택하여 호스트의 새 이니시에이터를 추가합니다.

8. 클론 * 을 선택합니다.

원격 스냅샷을 사용하여 클론을 생성합니다

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. 복제할 * 소스 * 에 마우스를 갖다 댑니다.
3. 를 선택한 다음 * Clone * 을 선택합니다.
4. 소스 클러스터 및 스토리지 VM을 선택한 다음 새 정합성 보장 그룹의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
5. 복제할 스냅샷을 선택한 다음 * Clone * 을 선택합니다.

다음 단계

원격 위치에서 일관성 그룹을 클론 복제했습니다. ASA R2 시스템에서 새 정합성 보장 그룹을 로컬에서 사용하여 필요한 대로 사용할 수 있습니다.

다음 단계

데이터를 보호하려면 "스냅샷을 생성합니다"클론 복제된 일관성 그룹이 있어야 합니다.

정합성 보장 그룹 클론을 분할합니다

일관성 그룹 클론을 분할하면 소스 일관성 그룹에서 클론을 분리하고 클론에 대한 디스크 공간을 할당합니다. 클론은 소스 정합성 보장 그룹과 별개로 사용할 수 있는 독립 실행형 정합성 보장 그룹이 됩니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 분할할 일관성 그룹 클론 위로 마우스를 이동합니다.
3. Split clone * 을 선택합니다.
4. 분할 * 을 선택합니다.

결과

클론이 소스 정합성 보장 그룹에서 분리되고 클론에 대해 디스크 공간이 할당됩니다.

호스트 그룹 관리

ASA r2 시스템에서 호스트 그룹을 만듭니다.

ASA R2 시스템에서 *host group* 은(는) 스토리지 유닛에 대한 호스트 액세스를 제공하는 데 사용되는 메커니즘입니다. 호스트 그룹은 SCSI 호스트용 igroup 또는 NVMe 호스트용 NVMe 서브시스템을 참조합니다. 호스트는 호스트가 속한 호스트 그룹에 매핑된 스토리지 유닛만 볼 수 있습니다. 호스트 그룹이 스토리지 유닛에 매핑되면 그룹의 구성원인 호스트가 스토리지 유닛에 디렉토리 및 파일 구조를 마운트(생성)할 수 있습니다.

호스트 그룹은 스토리지 유닛을 생성할 때 자동으로 또는 수동으로 생성됩니다. 필요에 따라 다음 단계를 사용하여 스토리지 유닛을 생성하기 전이나 후에 호스트 그룹을 생성할 수 있습니다.

단계

1. System Manager에서 * Host * 를 선택합니다.
2. 호스트 그룹에 추가할 호스트를 선택합니다.

   첫 번째 호스트를 선택하면 호스트 그룹에 추가하는 옵션이 호스트 목록 위에 나타납니다.
3. 호스트 그룹에 추가 * 를 선택합니다.
4. 호스트를 추가할 호스트 그룹을 검색하여 선택합니다.

다음 단계

호스트 그룹을 생성했으므로 이제 다음을 수행할 수 있습니다. "저장 장치에 매핑합니다" .

ASA r2 시스템에서 호스트 그룹 삭제

ASA r2 시스템에서 호스트 그룹은 호스트에게 스토리지 유닛에 대한 액세스 권한을 부여하는 데 사용되는 메커니즘입니다. 호스트 그룹은 SCSI 호스트의 경우 igroup, NVMe 호스트의 경우 NVMe 하위 시스템을 나타냅니다. 호스트는 자신이 속한 호스트 그룹에 매핑된 스토리지 유닛만 볼 수 있습니다. 그룹 내 호스트가 해당 그룹에 매핑된 스토리지 유닛에 더 이상 액세스하지 못하도록 하려면 호스트 그룹을 삭제하는 것이 좋습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. *호스트 매핑*에서 삭제하려는 호스트 그룹을 선택합니다.
3. *매핑된 저장소*를 선택하세요.
4. *더보기*를 선택한 다음, *삭제*를 선택하세요.
5. 계속 진행하시겠습니까? 확인을 선택한 후 *삭제*를 선택하세요.

다음 단계

호스트 그룹이 삭제되었습니다. 그룹에 속했던 호스트는 더 이상 호스트 그룹에 매핑된 스토리지 유닛에 액세스할 수 없습니다.

스토리지 유닛 관리

ASA R2 스토리지 시스템에서 스토리지 유닛을 수정합니다

ASA r2 시스템의 성능을 최적화하려면 스토리지 유닛의 용량을 늘리거나, QoS 정책을 업데이트하거나, 유닛에 매핑된 호스트를 변경하는 등의 수정이 필요할 수 있습니다. 예를 들어, 기존 스토리지 유닛에 새롭고 중요한 애플리케이션 워크로드가 추가되는 경우, 새 애플리케이션에 필요한 성능 수준을 지원하기 위해 스토리지 유닛에 적용된 QoS(Quality of Service) 정책을 변경해야 할 수 있습니다.

용량 증가

스토리지 유닛에 쓰기 가능한 공간이 부족할 때 발생할 수 있는 데이터 액세스 손실을 방지하려면 스토리지 유닛의 크기를 전체 용량에 도달하기 전에 늘립니다. 스토리지 유닛의 용량은 ONTAP에서 허용하는 최대 크기인 128TB로 늘릴 수 있습니다.

호스트 매핑을 수정합니다

스토리지 유닛에 매핑되는 호스트를 수정하여 워크로드의 균형을 조정하거나 시스템 리소스를 재구성합니다.

QoS 정책을 수정합니다

QoS(서비스 품질) 정책은 경쟁 워크로드로 인해 중요 워크로드의 성능이 저하되지 않도록 보장합니다. QoS 정책을 사용하여 QoS throughput_limit_와 QoS throughput_guarantee_를 설정할 수 있습니다.

- QoS 처리량 제한

  QoS throughput_limit_은 워크로드의 처리량을 최대 IOPS 또는 MBps 또는 IOPS 및 MBps로 제한하여 워크로드가 시스템 리소스에 미치는 영향을 제한합니다.

- QoS 처리량 보장

  QoS throughput_guarantee_는 중요 워크로드의 처리량이 최소 IOPS 또는 MBps 또는 IOPS 및 MBps 이하로 떨어지지 않도록 보장하여 경쟁 워크로드의 수요에 관계없이 중요 워크로드가 최소 처리량 목표를 충족합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 편집할 스토리지 유닛의 이름 위로 마우스를 가져갑니다.
3. 을 선택한 다음 * 편집 * 을 선택합니다.
4. 필요에 따라 스토리지 유닛 매개 변수를 업데이트하여 용량을 늘리고, QoS 정책을 변경하고, 호스트 매핑을 업데이트합니다.

다음 단계

스토리지 유닛의 크기를 늘린 경우 호스트에서 크기 변경을 인식하려면 호스트에서 스토리지 유닛을 다시 검색해야 합니다.

ASA R2 스토리지 시스템에서 스토리지 유닛 이동

스토리지 가용 영역의 공간이 부족한 경우 스토리지 유닛을 다른 스토리지 가용 영역으로 이동하여 클러스터 전체의 스토리지 사용률을 조정할 수 있습니다.

스토리지 유닛이 온라인 상태이고 데이터를 제공하는 동안 스토리지 유닛을 이동할 수 있습니다. 이동 작업은 무중단으로 수행됩니다.

시작하기 전에

- ONTAP 9.16.1 이상을 실행 중이어야 합니다.
- 클러스터는 4개 이상의 노드로 구성되어야 합니다.

단계

1. System Manager에서 * Storage * 를 선택한 다음 이동할 스토리지 유닛을 선택합니다.
2. 을 선택한 다음 * Move * 를 선택합니다.
3. 스토리지 유닛을 이동할 스토리지 가용 영역을 선택한 다음 * Move * 를 선택합니다.

ASA R2 스토리지 시스템에서 스토리지 유닛을 삭제합니다

유닛에 포함된 데이터를 더 이상 유지 관리할 필요가 없는 경우 스토리지 유닛을 삭제합니다. 더 이상 필요하지 않은 스토리지 유닛을 삭제하면 다른 호스트 애플리케이션에 필요한 공간을 확보하는 데 도움이 됩니다.

시작하기 전에

삭제하려는 저장 장치가 복제 관계에 있는 일관성 그룹에 있는 경우 다음을 수행해야 합니다."정합성 보장 그룹에서 스토리지 유닛을 제거합니다" 삭제하기 전에.

단계

1. System Manager에서 * Storage * 를 선택합니다.

2. 삭제할 스토리지 유닛의 이름 위로 마우스를 가져갑니다.
3. 을 선택한 다음 * 삭제 * 를 선택합니다.
4. 삭제를 취소할 수 없음을 확인합니다.
5. 삭제 * 를 선택합니다.

다음 단계

삭제된 스토리지 유닛에서 확보한 공간을 "크기를 늘립니다"추가 용량이 필요한 스토리지 유닛으로 사용할 수 있습니다.

스토리지 VM 마이그레이션

ASA 클러스터에서 **ASA r2** 클러스터로 스토리지 **VM** 마이그레이션

ONTAP 9.18.1부터 모든 ASA 클러스터에서 모든 ASA r2 클러스터로 스토리지 가상 머신(VM)을 중단 없이 마이그레이션할 수 있습니다. ASA 클러스터에서 ASA r2 클러스터로 마이그레이션하면 SAN 전용 환경에서 ASA r2 시스템의 간소화되고 효율적인 아키텍처를 채택할 수 있습니다.

ASA 와 ASA r2 스토리지 시스템 간의 스토리지 VM 마이그레이션은 다음과 같이 지원됩니다.

다음 **ASA** 시스템 중 하나에서:	다음 **ASA r2** 시스템 중 하나:
• ASA C800 • ASA C400 • ASA C250 • ASA A900 • ASA A800 • ASA A400 • ASA A250 • ASA A150 • ASA AFF A800 • ASA AFF A700 • ASA AFF A400 • ASA AFF A250 • ASA AFF A220	• ASA A1K 를 참조하십시오 • ASA C30 • ASA A90 를 참조하십시오 • ASA A70 를 참조하십시오 • ASA A50 • ASA A30 • ASA A20

ASA 및 ASA r2 시스템의 최신 목록은 다음을 참조하세요."NetApp Hardware Universe를 참조하십시오" . ASA r2 시스템은 NetApp Hardware Universe 에 "ASA A-시리즈/C-시리즈(신제품)"로 나열되어 있습니다.

ASA 클러스터에서만 스토리지 VM을 ASA r2 클러스터로 마이그레이션할 수 있습니다. 다른 유형의 ONTAP 시스템에서의 마이그레이션은 지원되지 않습니다.

시작하기 전에

ASA r2 클러스터와 ASA 클러스터의 모든 노드는 ONTAP 9.18.1 이상을 실행해야 합니다. 클러스터 노드의 ONTAP 9.18.1 패치 버전은 다를 수 있습니다.

1단계: ASA 스토리지 VM 상태 확인

ASA 시스템에서 스토리지 VM을 마이그레이션하기 전에 NVMe 네임스페이스나 vVols 이 없어야 하며 스토리지 VM의 각 볼륨에는 LUN이 하나만 있어야 합니다. NVMe 네임스페이스 및 vVols 마이그레이션은 지원되지 않습니다. ASA r2 시스템의 아키텍처에서는 볼륨에 단일 LUN이 포함되어야 합니다.

단계

1. 스토리지 VM에 NVMe 네임스페이스가 없는지 확인하세요.

   ```
   vserver nvme namespace show -vserver <storage_VM>
   ```

   항목이 표시되면 NVMe 개체가 있어야 합니다."변환됨" LUN으로 이동하거나 제거함. 를 참조하십시오 `vserver nvme namespace delete` 그리고 `vserver nvme subsystem delete` 명령"ONTAP 명령 참조입니다" 자세한 내용은.

2. 스토리지 VM에 vVols 없는지 확인하세요.

   ```
   lun show -verser <storage_VM> -class protocol-endpoint,vvol
   ```

   vVols 이 있는 경우 다른 스토리지 VM에 복사한 다음 마이그레이션할 스토리지 VM에서 삭제해야 합니다. 를 참조하십시오 `lun copy` 그리고 `lun delete` 명령"ONTAP 명령 참조입니다" 자세한 내용은.

3. 스토리지 VM의 각 볼륨에 단일 LUN이 포함되어 있는지 확인하세요.

   ```
   lun show -verser <storage_VM>
   ```

   볼륨에 두 개 이상의 LUN이 포함된 경우 다음을 사용하십시오. `volume create` 그리고 `lun move` 볼륨 대 LUN 비율을 1:1로 만드는 명령입니다. 를 참조하십시오"ONTAP 명령 참조입니다" 자세한 내용은.

다음 단계

이제 ASA 와 ASA r2 클러스터 간에 클러스터 피어 관계를 생성할 준비가 되었습니다.

2단계: ASA 와 ASA r2 클러스터 간 클러스터 피어 관계 생성

ASA 클러스터에서 ASA r2 클러스터로 스토리지 VM을 마이그레이션하려면 먼저 피어 관계를 만들어야 합니다. 피어 관계는 ONTAP 클러스터와 스토리지 VM이 안전하게 데이터를 교환할 수 있도록 하는 네트워크 연결을 정의합니다.

시작하기 전에

다음 방법 중 하나를 사용하여 피어링 중인 클러스터의 모든 노드에 클러스터 간 LIF를 생성해야 합니다.

- "공유 데이터 포트에서 클러스터 간 LIF 구성"
- "전용 데이터 포트에 클러스터 간 LIF 구성"

- "사용자 정의 IP 공간에서 클러스터 간 LIF 구성"

단계

1. ASA r2 클러스터에서 ASA 클러스터와 피어 관계를 만들고 암호를 생성합니다.

```
cluster peer create -peer-addrs <ASA_cluster_LIF_IPs> -generate
-passphrase
```

다음 예제에서는 클러스터 1과 클러스터 2 사이에 클러스터 피어 관계를 만들고 시스템에서 생성한 암호를 만듭니다.

```
cluster1::> cluster peer create -peer-addrs 10.98.191.193 -generate
-passphrase
Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
            Peer Cluster Name: cluster2
            Initial Allowed Vserver Peers: -
            Expiration Time: 6/7/2017 09:16:10 +5:30
            Intercluster LIF IP: 10.140.106.185
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. 생성된 암호를 복사합니다.
3. ASA 클러스터에서 ASA r2 클러스터와 피어 관계를 만듭니다.

```
cluster peer create -peer-addrs <ASA_r2_LIF_IPs>
```

4. ASA r2 클러스터에서 생성된 암호를 입력하세요.
5. 클러스터 피어 관계가 생성되었는지 확인하세요.

```
cluster peer show
```

다음 예에서는 피어링에 성공한 클러스터에 대한 예상 출력을 표시합니다.

```
cluster1::> cluster peer show

Peer Cluster Name   Cluster Serial Number   Availability
Authentication
-----------------   ---------------------   --------------
--------------
cluster2             1-80-123456             Available      ok
```

결과

ASA 및 ASA r2 클러스터는 피어링되어 있으며 스토리지 VM 데이터를 안전하게 전송할 수 있습니다.

다음 단계

이제 ASA 스토리지 VM을 마이그레이션할 준비가 되었습니다.

3단계: ASA 에서 ASA r2 클러스터로 스토리지 VM 마이그레이션 준비

ASA 클러스터에서 ASA r2 클러스터로 스토리지 가상 머신(VM)을 마이그레이션하기 전에 마이그레이션 사전 검사를 실행하고 필요한 문제를 해결해야 합니다. 사전 검사를 성공적으로 통과할 때까지 마이그레이션을 수행할 수 없습니다.

단계

1. ASA r2 클러스터에서 마이그레이션 사전 검사를 실행합니다.

```
vserver migrate start -vserver <storage_VM> -source-cluster
<asa_cluster> -check-only true
```

   ASA 클러스터를 마이그레이션하기 위해 문제를 해결해야 하는 경우 문제와 해결 방법이 표시됩니다. 문제를 해결하고 사전 점검을 성공적으로 완료될 때까지 반복합니다.

다음 단계

이제 ASA 클러스터에서 ASA r2 클러스터로 스토리지 VM을 마이그레이션할 준비가 되었습니다.

4단계: ASA 스토리지 VM을 ASA r2 클러스터로 마이그레이션

ASA 클러스터를 준비하고 ASA r2 클러스터와 필요한 클러스터 피어 관계를 만든 후 스토리지 VM 마이그레이션을 시작할 수 있습니다.

스토리지 VM 마이그레이션을 수행할 때는 CPU 워크로드를 실행할 수 있도록 ASA 클러스터와 ASA r2 클러스터 모두에 30%의 CPU 여유 공간을 두는 것이 가장 좋습니다.

이 작업에 대해

스토리지 VM 마이그레이션 후 클라이언트는 자동으로 ASA r2 클러스터로 전환되고 ASA 클러스터의 스토리지 VM은 자동으로 제거됩니다. 자동 전환 및 자동 스토리지 VM 제거는 기본적으로 활성화되어 있습니다. 선택적으로 두 가지 모두 비활성화하고 전환 및 스토리지 VM 제거를 수동으로 수행할 수 있습니다.

시작하기 전에

- ASA r2 클러스터에는 마이그레이션된 스토리지 VM을 보관할 수 있는 충분한 여유 공간이 있어야 합니다.
- ASA 스토리지 VM에 암호화된 볼륨이 포함되어 있는 경우 ASA r2 시스템의 온보드 키 관리자 또는 외부 키 관리자를 클러스터 수준에서 구성해야 합니다.
- 다음 작업은 소스 ASA 클러스터에서 실행할 수 없습니다.
  - 장애 조치 작업
  - 와플리론
  - 지문
  - 볼륨 이동, 리호스팅, 복제, 생성, 변환 또는 분석

단계

1. ASA r2 클러스터에서 스토리지 VM 마이그레이션을 시작합니다.

```
vserver migrate start -vserver <storage_VM_name> -source-cluster
<ASA_cluster>
```

자동 컷오버를 비활성화하려면 다음을 사용하세요. `-auto-cutover false` 매개변수. ASA 스토리지 VM의 자동 제거를 비활성화하려면 다음을 사용하세요. `-auto-source-cleanup false` 매개변수.

2. 마이그레이션 상태 모니터링

```
vserver migrate show -vserver <storage_VM_name>
```

마이그레이션이 완료되면 *상태*가 *마이그레이션 완료*로 표시됩니다.

자동 전환이 시작되기 전에 마이그레이션을 일시 중지하거나 취소해야 하는 경우 다음을 사용하세요. `vserver migrate pause` 그리고 `vserver migrate abort` 명령. 취소하기 전에 마이그레이션을 일시 중지해야 합니다. 전환이 시작된 후에는 마이그레이션을 취소할 수 없습니다.

결과

스토리지 VM은 ASA 클러스터에서 ASA r2 클러스터로 마이그레이션됩니다. 스토리지 VM의 이름과 UUID, 데이터 LIF 이름, IP 주소, 볼륨 이름과 같은 개체 이름은 변경되지 않습니다. 스토리지 VM에 있는 마이그레이션된 객체의 UUID가 업데이트됩니다.

다음 단계

자동 컷오버 및 자동 스토리지 VM 제거를 비활성화한 경우"ASA 클라이언트를 ASA r2 클러스터로 수동으로 전환하고 ASA 클러스터에서 스토리지 VM을 제거합니다." .

ASA r2 시스템으로 마이그레이션 후 클라이언트를 전환하고 소스 스토리지 **VM**을 정리합니다**.**

스토리지 가상 머신(VM)이 ASA 클러스터에서 ASA r2 클러스터로 마이그레이션된 후 기본적으로 클라이언트는 자동으로 ASA r2 클러스터로 전환되고 ASA 클러스터의 스토리지 VM은 자동으로 제거됩니다. 마이그레이션 중에 ASA 스토리지 VM의 자동 전환 및 제거를 비활성화하도록 선택한 경우 마이그레이션이 완료된 후 이러한 단계를 수동으로 수행해야 합니다.

스토리지 **VM** 마이그레이션 후 클라이언트를 **ASA r2** 시스템으로 수동으로 전환

ASA 클러스터에서 ASA r2 클러스터로 스토리지 VM을 마이그레이션하는 동안 자동 클라이언트 전환을 비활성화한 경우, 마이그레이션이 성공적으로 완료된 후 수동으로 전환을 수행하여 ASA r2 스토리지 VM이 클라이언트에 데이터를 제공할 수 있도록 합니다.

단계

1. ASA r2 클러스터에서 클라이언트 전환을 수동으로 실행합니다.

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. 컷오버 작업이 완료되었는지 확인하세요.

```
vserver migrate show
```

결과

ASA r2 클러스터의 스토리지 VM에서 클라이언트로 데이터가 제공됩니다.

다음 단계

이제 소스 ASA 클러스터에서 스토리지 VM을 제거할 준비가 되었습니다.

ASA r2 클러스터로 마이그레이션한 후 ASA 스토리지 VM을 수동으로 제거합니다.

ASA 클러스터에서 ASA r2 클러스터로 스토리지 VM을 마이그레이션하는 동안 자동 소스 정리를 비활성화한 경우, 마이그레이션이 완료된 후 ASA 클러스터에서 스토리지 VM을 제거하여 스토리지 공간을 확보합니다.

시작하기 전에

클라이언트는 ASA r2 클러스터에서 데이터를 제공해야 합니다.

단계

1. ASA 클러스터에서 ASA 스토리지 VM의 상태가 *소스 정리 준비*인지 확인합니다.

```
vserver migrate show
```

2. ASA 스토리지 VM을 제거합니다.

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

결과

ASA 클러스터의 스토리지 VM이 제거되었습니다.

ASA R2 스토리지 제한

최적의 성능, 구성 및 지원을 위해서는 ASA r2 스토리지 한도를 알고 있어야 합니다.

최신 ASA R2 스토리지 제한값의 전체 목록은 을 참조하십시오"NetApp Hardware Universe를 참조하십시오".

ASA r2 시스템은 다음과 같은 저장 한도를 지원합니다.

	HA 쌍당 최대	클러스터당 최대
일관성 그룹	256	256

	HA 쌍당 최대	클러스터당 최대
엔터프라이즈 애플리케이션	100	350
노드	2	12
복제 그룹	50	50
스토리지 가용성 영역 크기	2페타비	2페타비
보관 장치	10,000	30,000
저장 장치 크기	128TB	128TB
일관성 그룹당 저장 단위	256	256
부모 일관성 그룹별 자녀 일관성 그룹	64	64
스토리지 가상 머신	• 256(ONTAP 9.18.1 이상) • 32 (ONTAP 9.17.1 및 이전 버전)	• 256(ONTAP 9.18.1 이상) • 32 (ONTAP 9.17.1 및 이전 버전)
가상 머신	800	1200

SnapMirror 비동기 관계에 대한 제한

다음 제한은 SnapMirror 비동기 복제 관계의 스토리지 유닛과 일관성 그룹에 적용됩니다. 최신 ASA r2 스토리지 한도의 전체 목록은 다음과 같습니다."NetApp Hardware Universe를 참조하십시오" .

최대 한도	**HA** 쌍당	클러스터당
일관성 그룹	250	750
보관 장치	4,000	6,000

SnapMirror 활성 동기화 관계에 대한 제한 사항

다음 제한은 SnapMirror 활성 동기화 복제 관계의 스토리지 유닛과 일관성 그룹에 적용됩니다. SnapMirror 활성 동기화는 ONTAP 9.17.1부터 2노드 클러스터에서만 지원됩니다. ONTAP 9.18.1부터 SnapMirror 활성 동기화가 4노드 클러스터에서 지원됩니다.

최신 ASA r2 스토리지 한도의 전체 목록은 다음과 같습니다."NetApp Hardware Universe를 참조하십시오" .

최대 한도	**HA** 쌍당
일관성 그룹	50
보관 장치	400

데이터 보호

스냅샷을 생성하여 **ASA R2** 스토리지 시스템에 데이터를 백업합니다

ASA r2 시스템의 데이터를 백업하기 위해 스냅샷을 만듭니다. ONTAP 시스템 관리자를 사용하면 단일 스토리지 유닛의 수동 스냅샷을 생성하거나 일관성 그룹을 생성하고 동시에 여러

스토리지 유닛의 자동 스냅샷을 예약할 수 있습니다.

1단계**:** 필요에 따라 정합성 보장 그룹을 생성합니다

정합성 보장 그룹은 단일 유닛으로 관리되는 스토리지 유닛의 모음입니다. 정합성 보장 그룹을 생성하여 여러 스토리지 유닛에 걸쳐 있는 애플리케이션 워크로드의 스토리지 관리 및 데이터 보호를 간소화합니다. 예를 들어 정합성 보장 그룹에 10개의 스토리지 유닛으로 구성된 데이터베이스가 있고 전체 데이터베이스를 백업해야 한다고 가정합니다. 각 스토리지 유닛을 백업하는 대신 정합성 보장 그룹에 스냅샷 데이터 보호 기능을 추가하여 전체 데이터베이스를 백업할 수 있습니다.

새 스토리지 유닛을 사용하여 정합성 보장 그룹을 생성하거나 기존 스토리지 유닛을 사용하여 정합성 보장 그룹을 생성합니다.

ONTAP 9.18.1부터 새 스토리지 유닛으로 일관성 그룹을 생성할 때 스냅샷 예약 비율을 설정하고 자동 스냅샷 삭제를 활성화할 수 있습니다. 스냅샷 예약은 스냅샷을 위해 특별히 예약된 저장 장치의 공간입니다. 스냅샷 예약이 자동 스냅샷 삭제로 설정된 경우, 스냅샷에 사용된 공간이 스냅샷 예약 공간을 초과하면 오래된 스냅샷이 자동으로 삭제됩니다. 부모 일관성 그룹에서 스냅샷 예약 및 자동 스냅샷 삭제가 활성화된 경우 모든 기존 자식 일관성 그룹에서도 활성화됩니다. 새로운 자식 일관성 그룹이 추가되면 부모의 스냅샷 예약 및 스냅샷 삭제 설정은 상속되지 않습니다.

"ASA r2 스토리지 시스템의 스냅샷 예약에 대해 자세히 알아보세요.".

ONTAP 9.16.1부터 새로운 스토리지 유닛을 사용하여 일관성 그룹을 생성할 때 최대 5개의 자식 일관성 그룹을 구성할 수 있습니다. "ASA r2 시스템의 자식 일관성 그룹에 대해 자세히 알아보세요.".

새 저장 장치를 사용합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 를 선택한 + Add 다음 * 새 스토리지 유닛 사용 * 을 선택합니다.
3. 새 스토리지 유닛의 이름, 유닛 수 및 유닛당 용량을 입력합니다.

   두 개 이상의 유닛을 생성하는 경우 기본적으로 각 유닛은 동일한 용량과 동일한 호스트 운영 체제로 생성됩니다. 필요에 따라 각 유닛에 다른 용량을 할당할 수 있습니다.

4. 다음 중 하나를 수행하려면 * 추가 옵션 * 을 선택하고 필요한 단계를 완료합니다.

옵션을 선택합니다	단계
각 스토리지 유닛에 다른 용량을 할당합니다	Add a different capacity * 를 선택합니다.
기본 성능 서비스 수준을 변경합니다	성능 서비스 수준 * 에서 다른 서비스 수준을 선택합니다. ASA r2 시스템은 두 가지 성능 수준을 제공합니다. 기본 성능 수준은 *극단*으로, 사용 가능한 가장 높은 수준입니다. 성능 수준을 *성능*으로 낮출 수 있습니다.
기본 스냅샷 예약을 수정하고 자동 스냅샷 삭제를 활성화합니다.	a. *스냅샷 예약 %*에서 스냅샷에 할당하려는 저장 장치 공간의 백분율에 해당하는 숫자 값을 입력합니다. b. *오래된 스냅샷을 자동으로 삭제*를 선택합니다.
하위 정합성 보장 그룹을 생성합니다	Add child consistency group * 을 선택합니다.

5. 호스트 운영 체제 및 호스트 매핑을 선택합니다.
6. 추가 * 를 선택합니다.

다음 단계

보호하려는 저장 장치를 포함하는 일관성 그룹을 생성했습니다. 이제 스냅샷을 만들 수 있습니다.

기존 스토리지 유닛을 사용합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 을 + Add 선택한 다음 * 기존 스토리지 유닛 사용 * 을 선택합니다.
3. 정합성 보장 그룹의 이름을 입력한 다음 정합성 보장 그룹에 포함할 스토리지 유닛을 검색하여 선택합니다.
4. 추가 * 를 선택합니다.

다음 단계

보호하려는 저장 장치를 포함하는 일관성 그룹을 생성했습니다. 이제 스냅샷을 만들 수 있습니다.

2단계**:** 스냅샷을 생성합니다

스냅샷은 특정 시점으로 스토리지 유닛을 복구하는 데 사용할 수 있는 데이터의 로컬 읽기 전용 복사본입니다.

스냅샷은 필요에 따라 생성하거나 을 기반으로 일정한 간격으로 자동으로 생성할 수 "스냅샷 정책 및 일정"있습니다. 스냅샷 정책 및 스케줄은 스냅샷을 생성할 시기, 보존할 복제본 수, 복제본 이름 지정 방법 및 복제를 위해 스냅샷 레이블을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 사본 2개를 보존하고, 이름을 "daily"(타임스탬프가 추가됨)로 지정하고, 복제를 위해 "daily"로 레이블을 지정할 수 있습니다.

스냅샷 유형입니다

단일 스토리지 유닛 또는 정합성 보장 그룹의 필요 시 스냅샷을 생성할 수 있습니다. 여러 스토리지 유닛이 포함된 정합성 보장 그룹의 자동 스냅샷을 생성할 수 있습니다. 단일 스토리지 유닛의 자동 스냅샷을 생성할 수 없습니다.

- 주문형 스냅샷

  언제든지 스토리지 유닛의 주문형 스냅샷을 만들 수 있습니다. 스토리지 유닛은 주문형 스냅샷으로 보호받기 위해 일관성 그룹의 멤버일 필요는 없습니다. 일관성 그룹의 구성원인 스토리지 유닛의 주문형 스냅샷을 생성하는 경우 일관성 그룹의 다른 스토리지 유닛은 주문형 스냅샷에 포함되지 않습니다. 일관성 그룹의 주문형 스냅샷을 생성하면 일관성 그룹의 모든 스토리지 유닛이 스냅샷에 포함됩니다.

- 자동화된 스냅샷

  자동화된 스냅샷은 스냅샷 정책을 사용하여 생성됩니다. 자동 스냅샷 생성을 위해 스토리지 유닛에 스냅샷 정책을 적용하려면 스토리지 유닛이 정합성 보장 그룹의 구성원이어야 합니다. 정합성 보장 그룹에 스냅샷 정책을 적용하면 정합성 보장 그룹의 모든 스토리지 유닛이 자동화된 스냅샷으로 보호됩니다.

정합성 보장 그룹 또는 스토리지 유닛의 스냅샷을 생성합니다.

일관성 그룹의 스냅샷

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 보호할 일관성 그룹의 이름 위에 마우스를 놓습니다.
3. 를 ⋮ 선택한 다음 * Protect * 를 선택합니다.
4. 즉시 주문형 스냅샷을 생성하려면 * 로컬 보호 * 아래에서 * 지금 스냅샷 추가 * 를 선택합니다.

   로컬 보호는 스토리지 유닛을 포함하는 동일한 클러스터에 스냅샷을 생성합니다.

   a. 스냅샷의 이름을 입력하거나 기본 이름을 그대로 사용하고 필요에 따라 SnapMirror 레이블을 입력합니다.

      SnapMirror 레이블은 원격 대상에서 사용됩니다.

5. 스냅샷 정책을 사용하여 자동화된 스냅샷을 생성하려면 * Schedule snapshots * 를 선택합니다.

   a. 스냅샷 정책을 선택합니다.

      기본 스냅샷 정책을 수락하거나, 기존 정책을 선택하거나, 새 정책을 생성합니다.

옵션을 선택합니다	단계
기존 스냅샷 정책을 선택합니다	⌄기본 정책 옆에 있는 을 선택한 다음 사용할 기존 정책을 선택합니다.
새 스냅샷 정책을 생성합니다	i. 을 + Add 선택한 다음 스냅샷 정책 매개 변수를 입력합니다. ii. 정책 추가 * 를 선택합니다.

6. 스냅샷을 원격 클러스터에 복제하려면 * 원격 보호 * 에서 * 원격 클러스터에 복제 * 를 선택합니다.

   a. 소스 클러스터 및 스토리지 VM을 선택한 다음 복제 정책을 선택합니다.

      복제를 위한 초기 데이터 전송은 기본적으로 즉시 시작됩니다.

7. 저장 * 을 선택합니다.

스토리지 유닛의 스냅샷입니다

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 보호할 스토리지 유닛의 이름 위로 마우스를 가져갑니다.
3. 를 ⋮ 선택한 다음 * Protect * 를 선택합니다. 즉시 주문형 스냅샷을 생성하려면 * 로컬 보호 * 아래에서 * 지금 스냅샷 추가 * 를 선택합니다.

   로컬 보호는 스토리지 유닛을 포함하는 동일한 클러스터에 스냅샷을 생성합니다.

4. 스냅샷의 이름을 입력하거나 기본 이름을 그대로 사용하고 필요에 따라 SnapMirror 레이블을 입력합니다.

   SnapMirror 레이블은 원격 대상에서 사용됩니다.

5. 스냅샷 정책을 사용하여 자동화된 스냅샷을 생성하려면 * Schedule snapshots * 를 선택합니다.

   a. 스냅샷 정책을 선택합니다.

      기본 스냅샷 정책을 수락하거나, 기존 정책을 선택하거나, 새 정책을 생성합니다.

옵션을 선택합니다	단계
기존 스냅샷 정책을 선택합니다	기본 정책 옆에 있는 을 선택한 다음 사용할 기존 정책을 선택합니다.
새 스냅샷 정책을 생성합니다	i. 을 + Add 선택한 다음 스냅샷 정책 매개 변수를 입력합니다. ii. 정책 추가 * 를 선택합니다.

6. 스냅샷을 원격 클러스터에 복제하려면 * 원격 보호 * 에서 * 원격 클러스터에 복제 * 를 선택합니다.

   a. 소스 클러스터 및 스토리지 VM을 선택한 다음 복제 정책을 선택합니다.

      복제를 위한 초기 데이터 전송은 기본적으로 즉시 시작됩니다.

7. 저장 * 을 선택합니다.

다음 단계

스냅샷을 통해 데이터가 보호되므로 이제 "스냅샷 복제를 설정합니다"백업 및 재해 복구를 위해 일관성 그룹을 지리적으로 멀리 떨어진 위치에 복사해야 합니다.

스냅샷 예약 관리

ASA r2 스토리지에서 **ONTAP** 스냅샷 예약에 대해 알아보세요

스냅샷 예약은 스냅샷을 위해 특별히 예약된 저장 장치의 공간입니다. 스냅샷 예약이 자동 스냅샷 삭제로 설정된 경우, 스냅샷에 사용된 공간이 스냅샷 예약 공간을 초과하면 오래된 스냅샷이 자동으로 삭제됩니다. 이렇게 하면 스냅샷이 사용자 데이터용으로 지정된 저장 장치의 공간을 차지하는 것을 방지할 수 있습니다.

스냅샷 예약은 전체 저장 장치 크기의 백분율로 설정됩니다. 예를 들어, 저장 단위가 50GB이고 스냅샷 예약을 10%로 설정하면 스냅샷에 예약된 공간은 5GB가 됩니다. 스냅샷에 사용되는 공간의 양이 5GB로 늘어나면 새로운 스냅샷을 위한 공간을 확보하기 위해 이전 스냅샷이 자동으로 삭제됩니다. 저장 장치 크기가 100GB로 늘어나면 스냅샷 예약 용량도 10GB로 늘어납니다. 설정할 수 있는 최대 스냅샷 예약량은 200%입니다. 저장 장치가 최대 128TB까지 커지면 200% 스냅샷 예약을 통해 완전한 스냅샷을 2개 찍을 수 있습니다.

기본적으로 스냅샷 예약은 0%로 설정되고 스냅샷 자동 삭제는 활성화되어 있지 않습니다.

ONTAP 9.18.1부터 스토리지 유닛을 생성하는 동안 또는 생성한 후, 그리고 일관성 그룹을 생성하는 동안 기본 스냅샷 예약을 수정할 수 있습니다. 기존 스토리지 가상 머신(VM)에서 기본 스냅샷 예약을 수정할 수도 있습니다. ONTAP 9.17.1 및 이전 버전에서는 이러한 설정을 수정할 수 없습니다.

일관성 그룹이 생성될 때 일관성 그룹의 모든 스토리지 유닛에 대해 스냅샷 예약이 동일한 백분율로 설정됩니다. 나중에 추가된 모든 저장 장치에는 스냅샷 예약을 개별적으로 설정해야 합니다.

ASA r2 스토리지 시스템에서 스냅샷 예약 수정

스냅샷 예약은 스냅샷을 위해 특별히 예약된 저장 장치의 공간입니다. 기본적으로 스냅샷 예약은 0%로 설정됩니다. ONTAP 9.18.1부터 스토리지 유닛의 기본 스냅샷 예약을 수정하고 자동 스냅샷 삭제를 활성화할 수 있습니다. 스냅샷의 자동 삭제는 기본적으로 비활성화되어 있습니다. 스냅샷 예약 값이 설정되고 자동 스냅샷 삭제가 활성화된 경우, 스냅샷에 사용된 공간이 스냅샷 예약 값을 초과하면 이전 스냅샷이 자동으로 삭제됩니다. 이렇게 하면 스냅샷이 사용자 데이터용으로 지정된 저장 장치의 공간을 차지하는 것을 방지할 수 있습니다.

"ASA r2 스토리지 시스템의 스냅샷 예약에 대해 자세히 알아보세요.".

스토리지 유닛의 스냅샷 예약 수정

다양한 스냅샷 예약 값을 설정하려면 각 저장 장치를 개별적으로 구성하세요. 모든 스토리지 유닛에 동일한 값을 사용하려면 스토리지 VM에서 스냅샷 예약을 수정합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 스냅샷 예약을 설정하려는 저장 장치 이름 위에 마우스를 올려놓습니다.
3. 선택하다 ⋮ 을 클릭한 다음, *편집*을 선택하세요.
4. *스냅샷 예약 %*에서 스냅샷에 할당하려는 저장 장치 공간의 백분율에 해당하는 숫자 값을 입력합니다.
5. *이전 스냅샷을 자동으로 삭제*가 선택되어 있는지 확인하세요.
6. 저장 * 을 선택합니다.

결과

스냅샷 예약은 지정한 비율로 설정됩니다. 스냅샷에 사용되는 공간의 양이 예약 공간에 도달하면 오래된 스냅샷은 자동으로 삭제됩니다.

스토리지 **VM**에서 스냅샷 예약 수정

스토리지 VM의 모든 스토리지 유닛에 대해 동일한 스냅샷 예약을 설정하려면 스토리지 VM에 원하는 백분율을 적용합니다. . 스냅샷 예약이 스토리지 VM에 적용되면 스토리지 VM 내에서 새로 생성된 모든 스토리지 유닛에 적용됩니다. 설정을 수정하기 전에 생성된 저장 장치에는 적용되지 않습니다.

단계

1. 시스템 관리자에서 *클러스터 > 스토리지 VM*을 선택한 다음 *설정*을 선택합니다.
2. 정책*에서 *스냅샷 옆에서 다음을 선택하세요. ⋮ ; 그런 다음 *스냅샷 예약 기본값 설정/편집*을 선택합니다.
3. *스냅샷 예약 %*에서 스냅샷에 할당하려는 저장 장치 공간의 백분율에 해당하는 숫자 값을 입력합니다.
4. *이전 스냅샷을 자동으로 삭제*가 선택되어 있는지 확인하세요.
5. 저장 * 을 선택합니다.

결과

새로 생성된 스토리지 유닛에 대한 스냅샷 예약은 사용자가 지정한 비율로 설정됩니다. 해당 저장 장치에서 스냅샷에 의해 사용된 공간의 양이 예약 공간에 도달하면 오래된 스냅샷은 자동으로 삭제됩니다.

ASA r2 스토리지 시스템에서 클러스터 간 스토리지 VM 피어 관계 생성

피어 관계는 클러스터와 스토리지 가상 머신(VM)이 안전하게 데이터를 교환할 수 있도록 하는 네트워크 연결을 정의합니다. SnapMirror 사용하여 서로 다른 클러스터의 스토리지 VM 간에 피어 관계를 생성하면 데이터 보호 및 재해 복구가 가능합니다.

"동료 관계에 대해 자세히 알아보세요" .

시작하기 전에

스토리지 VM 피어 관계를 생성하려면 먼저 로컬 클러스터와 원격 클러스터 간에 클러스터 피어 관계를 설정해야 합니다. "클러스터 피어 관계 생성" 아직 하지 않았다면.

단계

1. 시스템 관리자에서 *보호 > 개요*를 선택합니다.
2. *스토리지 VM 피어*에서 *스토리지 VM 피어 추가*를 선택합니다.
3. 로컬 클러스터에서 스토리지 VM을 선택한 다음, 원격 클러스터에서 스토리지 VM을 선택합니다.
4. *스토리지 VM 피어 추가*를 선택합니다.

스냅샷 복제를 설정합니다

ASA R2 스토리지 시스템에서 원격 클러스터로 스냅샷 복제

스냅샷 복제는 ASA R2 시스템의 정합성 보장 그룹이 지리적으로 멀리 떨어진 위치에 복제되는 프로세스입니다. 초기 복제 후 정합성 보장 그룹에 대한 변경 사항은 복제 정책에 따라 원격 위치에 복제됩니다. 복제된 정합성 보장 그룹을 재해 복구 또는 데이터 마이그레이션에 사용할 수 있습니다.

ASA r2 스토리지 시스템에 대한 스냅샷 복제는 다른 ASA r2 스토리지 시스템에서만 지원됩니다. ASA r2 시스템에서 ASA, AFF 또는 FAS 시스템으로, 또는 ASA, AFF 또는 FAS 시스템에서 ASA r2 시스템으로 스냅샷을 복제할 수 없습니다.

스냅샷 복제를 설정하려면 ASA R2 시스템과 원격 위치 간에 복제 관계를 설정해야 합니다. 복제 관계는 복제 정책에 의해 관리됩니다. 모든 스냅샷을 복제하는 기본 정책은 클러스터 설정 중에 생성됩니다. 기본 정책을 사용하거나 필요에 따라 새 정책을 생성할 수 있습니다.

ONTAP 9.17.1부터 계층적 관계의 일관성 그룹에 비동기 복제 정책을 적용할 수 있습니다. ONTAP 9.16.1에서는 계층적 관계에 있는 일관성 그룹에 대해 비동기 복제가 지원되지 않습니다.

"계층적(부모/자식) 일관성 그룹에 대해 자세히 알아보세요." .

1단계**:** 클러스터 피어 관계를 생성합니다

데이터를 원격 클러스터에 복제하여 데이터를 보호하려면 로컬 및 원격 클러스터 간에 클러스터 피어 관계를 생성해야 합니다.

시작하기 전에

클러스터 피어링을 위한 전제 조건은 ASA r2 시스템과 다른 ONTAP 시스템에서 동일합니다. "클러스터 피어링의 전제 조건 검토" .

단계

1. 로컬 클러스터의 System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 클러스터 피어 * 옆에 있는 * Intercluster Settings * 에서 * Add a cluster peer * 를 선택한 다음 * Add a cluster peer * 를 선택합니다.
3. lauch remote cluster * 를 선택합니다. 그러면 원격 클러스터를 인증하는 데 사용할 암호가 생성됩니다.
4. 원격 클러스터에 대한 암호를 생성한 후 로컬 클러스터의 * Passphrase * 에 붙여 넣습니다.
5. + Add 를 선택한 다음 인터클러스터 네트워크 인터페이스 IP 주소를 입력합니다.
6. 클러스터 피어링 시작 * 을 선택합니다.

다음 단계

원격 클러스터가 있는 로컬 ASA R2 클러스터를 피어링했습니다. 이제 복제 관계를 생성할 수 있습니다.

2단계**:** 선택적으로 사용자 정의 복제 정책을 만듭니다**.**

복제 정책은 ASA r2 클러스터에서 수행된 업데이트가 원격 사이트에 복제되는 시점을 정의합니다. ONTAP 에는 복제 관계에 사용할 수 있는 다양한 사전 정의된 데이터 보호 정책이 포함되어 있습니다. 미리 정의된 정책이 요구 사항을 충족하지 못하는 경우 사용자 정의 복제 정책을 만들 수 있습니다.

에 대해 알아보세요"사전 정의된 ONTAP 데이터 보호 정책" .

단계

1. System Manager에서 * 보호 > 정책 * 을 선택한 다음 * 복제 정책 * 을 선택합니다.
2. 을 + Add 선택합니다.
3. 복제 정책의 이름을 입력하거나 기본 이름을 그대로 사용한 다음 설명을 입력합니다.
4. 정책 범위 * 를 선택합니다.

   복제 정책을 전체 클러스터에 적용하려면 * Cluster * 를 선택합니다. 복제 정책을 특정 스토리지 VM의 스토리지 유닛에만 적용하려면 * Storage VM * 을 선택합니다.

5. *정책 유형*에서 *비동기*를 선택합니다.

   비동기 정책을 사용하면 데이터가 소스에 기록된 후 원격 사이트로 복사됩니다. ASA r2 시스템에서는 동기 복제가 지원되지 않습니다.

6. 소스에서 스냅숏 전송 * 에서 기본 전송 일정을 수락하거나 다른 전송 일정을 선택합니다.
7. 모든 스냅샷을 전송하거나 전송할 스냅샷을 결정하는 규칙을 생성하려면 선택합니다.
8. 필요한 경우 네트워크 압축을 활성화합니다.
9. 저장 * 을 선택합니다.

다음 단계

복제 정책을 생성했으므로 이제 ASA R2 시스템과 원격 위치 간에 복제 관계를 생성할 준비가 되었습니다.

를 참조하십시오

에 대해 자세히 "클라이언트 액세스를 위한 스토리지 VM입니다"알아보십시오.

3단계**:** 복제 관계를 생성합니다

스냅샷 복제 관계는 정합성 보장 그룹을 원격 클러스터에 복제할 수 있도록 ASA R2 시스템과 원격 위치 간에 접속을 설정합니다. 복제된 정합성 보장 그룹을 재해 복구 또는 데이터 마이그레이션에 사용할 수 있습니다.

랜섬웨어 공격으로부터 보호하기 위해 복제 관계를 설정할 때 대상 스냅샷을 잠그도록 선택할 수 있습니다. 잠긴 스냅샷은 실수로 또는 악의적으로 삭제할 수 없습니다. 스토리지 유닛이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수 있습니다.

시작하기 전에

- "복제 정책에 대해 알아보세요" .

  복제 관계를 생성할 때 복제 관계에 적합한 복제 정책을 선택해야 합니다. 미리 정의된 정책을 사용하거나 사용자 지정 정책을 만들 수 있습니다.

- 대상 스냅샷을 잠그려면 "스냅샷 준수 클록을 초기화합니다"복제 관계를 생성하기 전에 작업을 수행해야 합니다.

잠긴 대상 스냅샷을 사용하거나 사용하지 않고 복제 관계를 생성합니다.

잠긴 스냅샷 사용

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 일관성 그룹을 선택합니다.
3. 를 선택한 다음 * Protect * 를 선택합니다.
4. Remote protection * 아래에서 * Replicate to a remote cluster * 를 선택합니다.
5. 복제 정책 * 을 선택합니다.

   반드시 _vault_replication 정책을 선택해야 합니다.

6. Destination settings * 를 선택합니다.
7. 삭제를 방지하려면 * 대상 스냅샷을 잠금 * 을 선택합니다
8. 최대 및 최소 데이터 보존 기간을 입력합니다.
9. 데이터 전송 시작을 지연시키려면 * 즉시 전송 시작 * 을 선택 취소합니다.

   초기 데이터 전송은 기본적으로 즉시 시작됩니다.

10. 선택적으로 기본 전송 일정을 무시하려면 * Destination settings * 를 선택한 다음 * Override transfer schedule * 을 선택합니다.

    전송 일정이 지원되려면 30분 이상이어야 합니다.

11. 저장 * 을 선택합니다.

잠긴 스냅샷 없음

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. 로컬 대상 또는 로컬 소스와의 복제 관계를 생성하려면 선택합니다.

옵션을 선택합니다	단계
로컬 목적지	a. Local Destinations * 를 선택한 후 를 Replicate 선택합니다. b. 소스 정합성 보장 그룹을 검색하여 선택합니다. source_consistency 그룹은 복제할 로컬 클러스터의 정합성 보장 그룹을 나타냅니다.

옵션을 선택합니다	단계
로컬 소스	a. Local sources * 를 선택한 다음 를 Replicate 선택합니다. b. 소스 정합성 보장 그룹을 검색하여 선택합니다. c. Replication destination * 에서 복제할 클러스터를 선택한 다음 스토리지 VM을 선택합니다.

3. 복제 정책을 선택합니다.
4. 데이터 전송 시작을 지연시키려면 * Destination settings * 를 선택한 다음 * Start transfer immediately * 를 선택 취소합니다.

   초기 데이터 전송은 기본적으로 즉시 시작됩니다.

5. 선택적으로 기본 전송 일정을 무시하려면 * Destination settings * 를 선택한 다음 * Override transfer schedule * 을 선택합니다.

   전송 일정이 지원되려면 30분 이상이어야 합니다.

6. 저장 * 을 선택합니다.

다음 단계

복제 정책 및 관계를 생성했으므로 초기 데이터 전송은 복제 정책에 정의된 대로 시작됩니다. 필요에 따라 복제 페일오버를 테스트하여 ASA R2 시스템이 오프라인 상태가 되는 경우 페일오버가 성공적으로 수행되는지 확인할 수 있습니다.

4단계**:** 복제 장애 조치를 테스트합니다

필요에 따라 소스 클러스터가 오프라인 상태인 경우 원격 클러스터의 복제된 스토리지 유닛에서 데이터를 성공적으로 제공할 수 있는지 확인합니다.

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. 테스트할 복제 관계 위로 마우스를 가져간 다음 을 ⋮ 선택합니다.
3. 테스트 대체 작동 * 을 선택합니다.
4. 장애 조치 정보를 입력한 다음 * Test failover * 를 선택합니다.

다음 단계

이제 재해 복구를 위해 스냅샷 복제를 통해 데이터를 보호하므로 "유휴 데이터 암호화"ASA R2 시스템의 디스크가 용도 변경, 반환, 위치 오류 또는 도난된 경우에도 데이터를 읽을 수 없습니다.

미리 정의된 **ONTAP** 데이터 보호 정책에 대해 알아보세요

복제 정책은 ASA r2 클러스터에서 수행된 업데이트가 원격 사이트에 복제되는 시점을 정의합니다. ONTAP 에는 복제 관계에 사용할 수 있는 다양한 사전 정의된 데이터 보호 정책이

포함되어 있습니다.

미리 정의된 정책이 귀하의 요구 사항을 충족하지 못하는 경우"사용자 정의 복제 정책 생성" .

ASA r2 시스템은 동기 복제를 지원하지 않습니다.

ASA r2 시스템은 다음과 같은 사전 정의된 보호 정책을 지원합니다.

정책	설명	정책 유형
비동기	최신 활성 파일 시스템과 일일 및 주간 스냅샷을 시간별 전송 일정에 따라 미러링하기 위한 통합 SnapMirror 비동기 및 볼트 정책입니다.	비동기
자동화된 이중 장애 복구	RTO가 0인 SnapMirror 동기식 및 양방향 동기화 복제 정책입니다.	SnapMirror 액티브 싱크
클라우드백업기본	일일 규칙이 있는 금고 정책.	비동기
데일리백업	일일 규칙과 일일 이체 일정이 있는 금고 정책입니다.	비동기
DPDefault	모든 스냅샷과 최신 활성 파일 시스템을 미러링하기 위한 SnapMirror 비동기 정책입니다.	비동기
미러올스냅샷	모든 스냅샷과 최신 활성 파일 시스템을 미러링하기 위한 SnapMirror 비동기 정책입니다.	비동기
MirrorAllSnapshotsDiscardNetwork	SnapMirror 네트워크 구성을 제외한 모든 스냅샷과 최신 활성 파일 시스템을 미러링하는 비동기 정책입니다.	비동기
미러앤볼트	최신 활성 파일 시스템과 일일 및 주간 스냅샷을 미러링하기 위한 통합 SnapMirror 비동기 및 볼트 정책입니다.	비동기
MirrorAndVaultDiscardNetwork	네트워크 구성을 제외한 최신 활성 파일 시스템과 일일 및 주간 스냅샷을 미러링하기 위한 통합 SnapMirror 비동기 및 볼트 정책입니다.	비동기
미러최신	최신 활성 파일 시스템을 미러링하기 위한 SnapMirror 비동기 정책입니다.	비동기
Unified7year	7년 보존이 적용되는 통합 SnapMirror 정책입니다.	비동기
XDP기본	일일 및 주간 규칙이 있는 금고 정책입니다.	비동기

ASA r2 시스템에서 비동기 복제 관계 해제

특정 상황에서는 비동기 복제 관계를 해제해야 할 수도 있습니다. 예를 들어, ONTAP 9.16.1을 실행 중이고 비동기 복제 관계에 있는 일관성 그룹의 크기를 늘리려면 일관성 그룹의 크기를 수정하기 전에 먼저 관계를 해제해야 합니다.

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. 지역 목적지 또는 *지역 소스*를 선택하세요.
3. 끊고 싶은 관계 옆에서 선택하세요 ; 그런 다음 *중단*을 선택합니다.

4. *휴식*을 선택하세요.

결과

기본 및 보조 일관성 그룹 간의 비동기 관계가 끊어졌습니다.

SnapMirror Active Sync 설정

SnapMirror Active Sync 설정 워크플로

ONTAP SnapMirror 액티브 싱크 데이터 보호 기능은 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 운영될 수 있도록 지원하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 페일오버되도록 지원합니다. SnapMirror 액티브 싱크를 사용하면 페일오버를 트리거하는 데 수동 작업이나 사용자 지정 스크립팅이 필요하지 않습니다.

ASA r2 시스템에서 SnapMirror 활성 동기화를 구성하기 위한 시스템 관리자 절차는 통합 ONTAP 개성을 실행하는 NetApp FAS, AFF 및 ASA 시스템과 다르지만 SnapMirror 활성 동기화의 요구 사항, 아키텍처 및 작동은 동일합니다.

ONTAP 9.18.1부터 SnapMirror 활성 동기화가 4노드 구성에서 지원됩니다. ONTAP 9.17.1에서는 SnapMirror 활성 동기화가 2노드 구성에서만 지원됩니다.

"ASA r2 시스템에서 SnapMirror Active Sync를 사용한 재해 복구에 대해 자세히 알아보세요."

ASA r2 시스템에서 SnapMirror Active Sync는 대칭형 액티브/액티브 구성을 지원합니다. 대칭형 액티브/액티브 구성에서는 두 사이트 모두 액티브 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다.

자세히 알아보세요 "대칭 활성/활성 구성" .

1 **SnapMirror Active Sync**를 구성할 준비를 합니다.

에게 "SnapMirror Active Sync 구성을 준비합니다" ASA r2 시스템에서는 구성 전제 조건을 검토하고, 호스트 운영 체제에 대한 지원을 확인하고, 특정 구성에 영향을 줄 수 있는 개체 제한을 알고 있어야 합니다.

2 클러스터 구성을 확인하세요.

SnapMirror Active Sync를 구성하기 전에 다음을 수행해야 합니다. "ASA r2 클러스터가 적절한 피어링 관계에 있고 기타 구성 요구 사항을 충족하는지 확인하세요." .

3 **ONTAP Mediator**를 설치하세요.

ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용하여 클러스터 상태를 모니터링하고 비즈니스 연속성을 유지할 수 있습니다. ONTAP Mediator를 사용하는 경우 "설치하다" 호스트에서 ONTAP Cloud Mediator를 사용하는 경우 이 단계를 건너뛸 수 있습니다.

4 자체 서명 인증서를 사용하여 **ONTAP Mediator** 또는 **ONTAP Cloud Mediator**를 구성합니다.

당신은해야합니다 "ONTAP Mediator 또는 ONTAP Cloud Mediator 구성" 클러스터 모니터링을 위해 SnapMirror Active Sync와 함께 사용하려면 먼저 다음 단계를 따라야 합니다.

5 SnapMirror Active Sync를 구성합니다.

"SnapMirror 활성 동기화 구성" 재해 발생 시 보조 사이트에 데이터 사본을 생성하고 호스트 애플리케이션이 자동으로 투명하게 장애 조치되도록 합니다.

관련 정보

- "SnapMirror Active Sync에 대해 자세히 알아보세요" .
- "ONTAP 성격에 대해 자세히 알아보세요". *

ASA r2 시스템에서 **SnapMirror Active Sync**를 구성할 준비를 합니다.

ASA r2 시스템에서 SnapMirror Active Sync를 구성하려면 구성 전제 조건을 검토하고, 호스트 운영 체제에 대한 지원을 확인하고, 특정 구성에 영향을 줄 수 있는 개체 제한을 알아야 합니다.

단계

1. SnapMirror Active Sync를 검토하세요 "전제 조건" .
2. "호스트 운영 체제가 지원되는지 확인하세요." SnapMirror Active Sync용.
3. 검토하다 "객체 한계" 구성에 영향을 줄 수 있습니다.
4. ASA r2 시스템에서 SnapMirror Active Sync에 대한 호스트 프로토콜 지원을 확인하세요.

   ASA r2 시스템에서 SnapMirror Active Sync에 대한 지원은 ONTAP 버전과 호스트 프로토콜에 따라 다릅니다.

ONTAP 부터 시작하여…	**SnapMirror Active Sync**는 다음을 지원합니다…
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP
9.16.0	• iSCSI • FC

ASA r2 시스템의 **SnapMirror Active Sync**에 대한 **NVMe** 프로토콜 제한

NVMe 호스트가 있는 ASA r2 시스템에서 SnapMirror 활성 동기화를 구성하기 전에 특정 NVMe 프로토콜 제한 사항을 알아야 합니다.

NVMe 하위 시스템의 모든 NVMe 스토리지 장치는 동일한 일관성 그룹의 구성원이어야 하며 모두 동일한 SnapMirror 활성 동기화 관계에 속해야 합니다.

SnapMirror Active Sync에서는 NVMe/FC 및 NVMe/TCP 프로토콜이 다음과 같이 지원됩니다.

- 2노드 클러스터에서만
- ESXi 호스트에서만

- 대칭 활성/활성 구성에만 해당

  NVMe 호스트에서는 비대칭 액티브/액티브 구성이 지원되지 않습니다.

NVMe를 사용한 SnapMirror 액티브 동기화는 다음을 지원하지 않습니다.

- 두 개 이상의 일관성 그룹에 매핑된 하위 시스템

  일관성 그룹은 여러 하위 시스템에 매핑될 수 있지만, 각 하위 시스템은 하나의 일관성 그룹에만 매핑될 수 있습니다.

- SnapMirror 활성 동기화 관계에서 일관성 그룹 확장
- SnapMirror 활성 동기화 관계에 없는 NVMe 스토리지 장치를 복제된 하위 시스템에 매핑
- 일관성 그룹에서 스토리지 유닛 제거
- 일관성 그룹 지오메트리 변경
- "Microsoft 오프로드 데이터 전송(ODX)"

다음 단계

SnapMirror Active Sync를 활성화하는 데 필요한 준비를 완료한 후에는 다음을 수행해야 합니다. "클러스터 구성을 확인하세요" .

SnapMirror Active Sync를 구성하기 전에 **ASA r2** 클러스터 구성을 확인하세요**.**

SnapMirror 액티브 싱크는 장애 조치 발생 시 데이터를 보호하기 위해 피어링된 클러스터를 사용합니다. SnapMirror 액티브 싱크를 구성하기 전에 ASA r2 클러스터가 지원되는 피어링 관계에 있는지, 그리고 기타 구성 요구 사항을 충족하는지 확인해야 합니다.

단계

1. 클러스터 간에 클러스터 피어링 관계가 있는지 확인합니다.

   SnapMirror Active Sync에서는 클러스터 피어 관계를 위해 기본 IP 공간이 필요합니다. 사용자 지정 IP 공간은 지원되지 않습니다.

   "클러스터 피어 관계 생성" .

2. 각 클러스터의 스토리지 가상 머신(VM) 간에 피어 관계가 있는지 확인합니다.

   "클러스터 간 스토리지 VM 피어 관계 생성" .

3. 클러스터의 각 노드에 최소한 하나의 LIF가 생성되었는지 확인하세요.

   "LIF 생성".

4. 필요한 저장 장치가 생성되어 호스트 그룹에 매핑되었는지 확인합니다.

   "저장 공간을 만드세요" 그리고 "저장 장치를 호스트 그룹에 매핑합니다." .

5. 새로운 저장 장치를 발견하려면 애플리케이션 호스트를 다시 검사하세요.

다음 단계

클러스터 구성을 확인한 후에는 준비가 됩니다. "ONTAP Mediator 설치" .

ASA r2 시스템에 **ONTAP Mediator** 설치

ASA r2 시스템에 ONTAP Mediator를 설치하려면 다른 모든 ONTAP 시스템에 ONTAP Mediator를 설치하는 데 사용하는 것과 동일한 절차를 따라야 합니다.

ONTAP Mediator를 설치하는 과정에는 설치 준비, 저장소 액세스 활성화, ONTAP Mediator 패키지 다운로드, 코드 서명 확인, 호스트에 패키지 설치, 설치 후 작업 수행이 포함됩니다.

ONTAP Mediator를 설치하려면 다음을 따르세요. "이 워크플로"

다음 단계

ONTAP Mediator가 설치된 후에는 다음을 수행해야 합니다. "자체 서명 인증서를 사용하여 ONTAP Mediator 구성" .

ASA r2 시스템에서 **ONTAP Mediator** 또는 **ONTAP Cloud Mediatior** 구성

SnapMirror Active Sync를 사용하여 클러스터 모니터링을 시작하려면 먼저 ONTAP Mediator 또는 ONTAP Cloud Mediator를 구성해야 합니다. ONTAP Mediator와 ONTAP Cloud Mediator는 모두 SnapMirror Active Sync 관계에서 ONTAP 클러스터가 사용하는 고가용성(HA) 메타데이터를 위한 영구적이고 펜싱된 저장소를 제공합니다. 또한, 두 Mediator 모두 쿼럼 결정을 지원하는 동기식 노드 상태 쿼리 기능을 제공하고 컨트롤러 활성 상태 감지를 위한 ping 프록시 역할을 합니다.

시작하기 전에

ONTAP Cloud Mediator를 사용하는 경우 ASA r2 시스템이 필요한 사항을 충족하는지 확인하십시오. "전제 조건" .

단계

1. 시스템 관리자에서 *보호 > 개요*를 선택합니다.
2. 오른쪽 창의 *중재자*에서 *중재자 추가*를 선택합니다.
3. *중개자 유형*을 선택하세요.
4. 클라우드 중재자의 경우 조직 ID, 클라이언트 ID, 클라이언트 비밀번호를 입력하세요. 온프레미스 중재자의 경우 IP 주소, 포트, 중재자 사용자 이름, 중재자 비밀번호를 입력하세요.
5. 적격 클러스터 피어 목록에서 클러스터 피어를 선택하거나 *클러스터 피어 추가*를 선택하여 새 피어를 추가합니다.
6. 인증서 정보를 추가합니다
   - 자체 서명된 인증서를 사용하는 경우 해당 내용을 복사하세요. `intermediate.crt` 파일을 인증서 필드에 붙여 넣거나 *가져오기*를 선택하여 이동합니다. `intermediate.crt` 파일을 열고 인증서 정보를 가져옵니다.
   - 타사 인증서를 사용하는 경우 인증서 정보를 인증서 필드에 입력하세요.
7. 추가 * 를 선택합니다.

다음 단계

중재자를 초기화한 후에는 다음을 수행할 수 있습니다. "SnapMirror Active Sync 구성" 재해 발생 시 보조 사이트에 데이터 사본을 생성하고 호스트 애플리케이션이 자동으로 투명하게 장애 조치될 수 있도록 합니다.

ASA r2 시스템에서 **SnapMirror Active Sync** 구성

SnapMirror 활성 동기화를 구성하여 보조 사이트에 데이터 사본을 만들고 재해 발생 시 호스트 애플리케이션이 자동으로 투명하게 장애 조치될 수 있도록 합니다.

ASA r2 시스템에서 SnapMirror Active Sync는 대칭형 액티브/액티브 구성을 지원합니다. 대칭형 액티브/액티브 구성에서는 두 사이트 모두 액티브 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다.

iSCSI 또는 FC 프로토콜을 사용하고 VMware Sphere용 ONTAP 도구를 사용하는 경우 선택적으로 다음을 수행할 수 있습니다. "VM ware용 ONTAP 도구를 사용하여 SnapMirror 활성 동기화를 구성합니다." .

시작하기 전에

"일관성 그룹 만들기" 기본 사이트에 새 스토리지 유닛을 추가하세요. 비균일 대칭형 액티브/액티브 구성을 생성하려면 보조 사이트에도 새 스토리지 유닛을 사용하여 일관성 그룹을 생성하세요.

자세히 알아보세요 "비균일한" 대칭적인 활성/활성 구성.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. SnapMirror Active Sync로 보호하려는 일관성 그룹의 이름 위에 마우스를 올려놓습니다.
3. 선택하다 ⋮ 그런 다음 *보호*를 선택하세요.
4. Remote protection * 아래에서 * Replicate to a remote cluster * 를 선택합니다.
5. 기존 클러스터 피어를 선택하거나 *새 피어 추가*를 선택하세요.
6. 스토리지 VM을 선택하세요.
7. 복제 정책에 대해 *AutomatedFailOverDuplex*를 선택합니다.
8. 비균일 대칭 활성/활성 구성을 생성하는 경우 *대상 설정*을 선택한 다음 이 절차를 시작하기 전에 생성하는 새 대상 일관성 그룹의 이름을 입력합니다.
9. 저장 * 을 선택합니다.

결과

SnapMirror Active Sync는 재해 발생 시 거의 0에 가까운 복구 지점 목표(RPO)와 거의 0에 가까운 복구 시간 목표(RTO)로 작업을 계속할 수 있도록 데이터를 보호하도록 구성되어 있습니다.

SnapMirror 활성 동기화 관리

ASA r2 시스템에서 타사 인증서를 사용하도록 **ONTAP Mediator** 또는 **ONTAP Cloud Mediator**를 재구성합니다**.**

ONTAP Mediator 또는 ONTAP Cloud Mediator를 자체 서명 인증서로 구성하는 경우 타사 인증서를 사용하도록 Mediator를 재구성할 수 있습니다. 보안상의 이유로 귀하의 조직에서는 타사 인증서를 선호하거나 요구할 수 있습니다.

1단계**:** 중재자 구성 제거

중재자를 재구성하려면 먼저 클러스터에서 현재 구성을 제거해야 합니다.

단계

1. 시스템 관리자에서 *보호 > 개요*를 선택합니다.
2. 오른쪽 창의 *중재자*에서 다음을 선택하세요. 제거하려는 중재자 구성이 있는 클러스터 피어 옆에 있는 *제거*를 선택합니다.

   여러 개의 중재자가 설치되어 있고 모든 구성을 제거하려면 다음을 선택하십시오. 중재자 옆에 있는 *제거*를 선택하세요.

3. *제거*를 선택하여 중재자 구성을 제거할 것인지 확인하세요.

2단계**:** 자체 서명 인증서 제거

중재자 구성을 제거한 후에는 클러스터에서 연관된 자체 서명 인증서를 제거해야 합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. *보안*에서 *인증서*를 선택합니다.
3. 제거할 인증서를 선택하세요.
4. 을 선택한 다음 * 삭제 * 를 선택합니다.

3단계**:** 타사 인증서로 중재자를 다시 설치합니다**.**

연관된 자체 서명 인증서를 제거한 후에는 타사 인증서로 중재자를 다시 구성할 수 있습니다.

단계

1. *보호 > 개요*를 선택합니다.
2. 오른쪽 창의 *중재자*에서 *중재자 추가*를 선택합니다.
3. *중개자 유형*을 선택하세요.
4. 클라우드 중재자의 경우 조직 ID, 클라이언트 ID, 클라이언트 비밀번호를 입력하세요. 온프레미스 중재자의 경우 IP 주소, 포트, 중재자 사용자 이름 및 중재자 비밀번호를 입력합니다.
5. 적격 클러스터 피어 목록에서 클러스터 피어를 선택하거나 *클러스터 피어 추가*를 선택하여 새 피어를 추가합니다.
6. *인증서*에서 타사 인증서 정보를 입력합니다.
7. 추가 * 를 선택합니다.

결과

ONTAP Mediator 또는 ONTAP Cloud Mediator가 타사 인증서를 사용하도록 재구성되었습니다. 이제 중재자를 사용하여 SnapMirror 활성 동기화 관계를 관리할 수 있습니다.

SnapMirror 활성 동기화 관계에서 **ASA r2** 클러스터의 계획된 장애 조치 수행

SnapMirror 액티브 싱크는 보조 사이트에 데이터 사본을 생성하고 재해 발생 시 호스트 애플리케이션이 자동으로 투명하게 장애 조치를 수행하도록 하여 비즈니스 크리티컬 애플리케이션의 지속적인 가용성을 보장합니다. 장애 조치 프로세스를 테스트하거나 기본 사이트의 유지 관리를 위해 SnapMirror 액티브 싱크 관계에 대한 계획된 장애 조치를 수행해야 할 수도 있습니다.

시작하기 전에

- SnapMirror 활성 동기화 관계는 동기화되어야 합니다.
- 저장 장치 이동과 같은 중단 없는 작업이 진행 중일 때는 계획된 장애 조치를 시작할 수 없습니다.
- ONTAP Mediator 또는 ONTAP Cloud Mediator가 구성되고 연결되어 있으며 쿼럼에 있어야 합니다.

단계

1. *보호 > 복제*를 선택합니다.
2. 장애 조치하려는 SnapMirror 활성 동기화 관계를 선택합니다.
3. 선택하다 ⋮ ; 그런 다음 *장애 조치*를 선택합니다.

다음 단계

사용하세요 `snapmirror failover show` ONTAP 명령줄 인터페이스(CLI)에서 명령을 사용하여 장애 조치 상태를 모니터링합니다.

ASA r2 클러스터의 계획되지 않은 장애 조치 후 **SnapMirror** 활성 동기화 관계를 다시 설정합니다**.**

ASA r2 시스템에서 SnapMirror 액티브 동기화는 대칭형 액티브/액티브 구성을 지원합니다. 대칭형 액티브/액티브 구성에서는 양쪽 사이트 모두 활성 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다. 소스 클러스터에 장애가 발생하거나 격리되면 중재자는 자동 계획되지 않은 페일오버(AUFO)를 트리거하고 소스 클러스터가 복구될 때까지 타겟 클러스터에서 모든 I/O를 처리합니다.

SnapMirror 활성 동기화 관계에서 AUFO가 발생하는 경우, 관계를 다시 설정하고 원래 소스 클러스터가 다시 온라인 상태가 되면 해당 클러스터에서 작업을 재개해야 합니다.

시작하기 전에

- SnapMirror 활성 동기화 관계는 동기화되어야 합니다.
- 저장 장치 이동과 같은 중단 없는 작업이 진행 중일 때는 계획된 장애 조치를 시작할 수 없습니다.
- ONTAP Mediator는 구성되고 연결되어 있으며 쿼럼에 속해야 합니다.
- 호스트에서 손실된 I/O 경로를 복구하거나 I/O 경로 상태를 업데이트하려면 기본 스토리지 클러스터가 다시 작동을 시작한 후 호스트에서 스토리지/어댑터 재스캔을 수행해야 합니다.

단계

1. *보호 > 복제*를 선택합니다.
2. 다시 설정하려는 SnapMirror 활성 동기화 관계를 선택하세요.
3. 관계 상태가 *동기화됨*으로 표시될 때까지 기다리세요.
4. 선택하다 ⋮ ; 그런 다음 *장애 조치*를 선택하여 원래 기본 클러스터에서 작업을 재개합니다.

ASA r2 시스템에서 **SnapMirror** 활성 동기화 관계 삭제

비즈니스 애플리케이션에 대해 거의 0에 가까운 RPO 및 RTO가 더 이상 필요하지 않은 경우, 연관된 SnapMirror 활성 동기화 관계를 삭제하여 SnapMirror 활성 동기화 보호를 제거해야 합니다. ASA r2 시스템에서 ONTAP 9.16.1을 실행하는 경우 SnapMirror 활성 동기화 관계의

일관성 그룹에 특정 지오메트리 변경을 적용하기 전에 SnapMirror 활성 동기화 관계를 삭제해야 할 수도 있습니다.

1단계**:** 호스트 복제 종료

소스 클러스터의 호스트 그룹이 대상 클러스터로 복제되고 대상 일관성 그룹이 복제된 호스트 그룹에 매핑된 경우 SnapMirror 활성 동기화 관계를 삭제하기 전에 소스 클러스터에서 호스트 복제를 종료해야 합니다.

단계

1. System Manager에서 * Host * 를 선택합니다.
2. 복제를 중지하려는 호스트 그룹이 포함된 호스트 옆에서 다음을 선택합니다. 을 선택한 다음 *편집*을 선택합니다.
3. *호스트 구성 복제*를 선택 해제한 다음, *업데이트*를 선택합니다.

2단계**: SnapMirror** 활성 동기화 관계 삭제

일관성 그룹에서 SnapMirror 활성 동기화 보호를 제거하려면 SnapMirror 활성 동기화 관계를 삭제해야 합니다.

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. 지역 목적지 또는 *지역 소스*를 선택하세요.
3. 제거하려는 SnapMirror 활성 동기화 관계 옆에서 다음을 선택하세요. ; 그런 다음 *삭제*를 선택합니다.
4. *소스 일관성 그룹 기반 스냅샷 해제*를 선택합니다.
5. 삭제 * 를 선택합니다.

결과

SnapMirror 활성 동기화 관계가 제거되고 소스 일관성 그룹 기반 스냅샷이 해제됩니다. 일관성 그룹의 저장 장치는 더 이상 SnapMirror Active Sync로 보호되지 않습니다.

다음 단계

"스냅샷 복제를 설정합니다"백업 및 재해 복구를 위해 일관성 그룹을 지리적으로 멀리 떨어진 위치로 복사합니다.

ASA r2 시스템에서 **ONTAP Mediator** 또는 **ONTAP Cloud Mediator**를 제거합니다**.**

ASA r2 시스템에서는 SnapMirror Active Sync에 한 번에 한 가지 유형의 중재자만 사용할 수 있습니다. 중재자 유형을 변경하기로 선택한 경우 다른 인스턴스를 설치하기 전에 현재 인스턴스를 제거해야 합니다.

단계

ONTAP Mediator 또는 ONTAP Cloud Mediator를 제거하려면 ONTAP 명령줄 인터페이스(CLI)를 사용해야 합니다.

ONTAP 중재자

1. ONTAP Mediator 제거:

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   예:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP 클라우드 중재자

1. ONTAP Cloud Mediator 제거:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   예:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

관련 정보

- "스냅미러 중재자 제거"

ASA R2 스토리지 시스템에서 데이터를 복구합니다

스냅샷으로 보호되는 정합성 보장 그룹 또는 스토리지 유닛의 데이터는 손실되거나 손상된 경우 복구할 수 있습니다.

일관성 그룹 복원

정합성 보장 그룹을 복구하면 정합성 보장 그룹의 모든 스토리지 유닛에 있는 데이터가 스냅샷의 데이터로 대체됩니다. 스냅샷이 생성된 후 스토리지 유닛에 대한 변경 사항은 복구되지 않습니다.

로컬 또는 원격 스냅샷에서 정합성 보장 그룹을 복구할 수 있습니다.

로컬 스냅샷에서 복구합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 복원할 데이터가 포함된 일관성 그룹을 두 번 클릭합니다.

   정합성 보장 그룹 세부 정보 페이지가 열립니다.

3. Snapshots * 를 선택합니다.
4. 복원할 스냅샷을 선택한 다음 을 선택합니다.
5. Restore consistency group from this snapshot * 을 선택한 다음 * Restore * 를 선택합니다.

원격 스냅샷에서 복구합니다

단계

1. System Manager에서 * Protection > Replication * 을 선택합니다.
2. Local Destinations * 를 선택합니다.
3. 복원할 * 소스 * 를 선택한 다음 를 선택합니다.
4. Restore * 를 선택합니다.
5. 데이터를 복구할 클러스터, 스토리지 VM 및 정합성 보장 그룹을 선택합니다.
6. 복원할 스냅샷을 선택합니다.
7. 메시지가 표시되면 "복원"을 입력한 다음 * 복원 * 을 선택합니다.

결과

정합성 보장 그룹이 복구에 사용되는 스냅샷의 시점으로 복원됩니다.

스토리지 유닛을 복구합니다

스토리지 유닛을 복구하면 스토리지 유닛의 모든 데이터가 스냅샷의 데이터로 대체됩니다. 스냅샷이 생성된 후 스토리지 유닛에 대한 변경 사항은 복원되지 않습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 복원할 데이터가 포함된 스토리지 유닛을 두 번 클릭합니다.

   스토리지 유닛 세부 정보 페이지가 열립니다.

3. Snapshots * 를 선택합니다.
4. 복구할 스냅샷을 선택합니다.
5. 를 선택한 다음 * Restore * 를 선택합니다.
6. Use this snapshot to restore the storage unit * 를 선택한 다음 * Restore * 를 선택합니다.

결과

저장소 유닛이 복원에 사용된 스냅샷의 시점으로 복원됩니다.

일관성 그룹을 관리합니다

ASA r2 스토리지 시스템의 **ONTAP** 일관성 그룹에 대해 알아보세요**.**

일관성 그룹은 단일 단위로 관리되는 저장 단위의 모음입니다. 일관성 그룹을 사용하면 스토리지 관리가 간소화됩니다.

예를 들어, 일관성 그룹에 10개의 저장 장치로 구성된 데이터베이스가 있고 전체 데이터베이스를 백업해야 한다고 가정해 보겠습니다. 각 저장 장치를 백업하는 대신 일관성 그룹에 스냅샷 데이터 보호를 추가하기만 하면 전체 데이터베이스를 백업할 수 있습니다. 저장 장치를 개별적으로 백업하는 대신 일관성 그룹으로 백업하면 모든 장치에 대한 일관된 백업이 제공되지만, 장치를 개별적으로 백업하면 불일치가 발생할 가능성이 있습니다.

ONTAP 9.16.1부터 System Manager를 사용하여 ASA r2 시스템에서 계층적 일관성 그룹을 만들 수 있습니다. 계층적 구조에서는 하나 이상의 일관성 그룹이 부모 일관성 그룹 아래의 자식으로 구성됩니다.

계층적 정합성 보장 그룹을 사용하면 각 하위 정합성 보장 그룹에 개별 스냅샷 정책을 적용하고 상위 정합성 보장 그룹을 복제하여 모든 하위 정합성 보장 그룹의 스냅샷을 단일 유닛으로 원격 클러스터에 복제할 수 있습니다. 따라서 복잡한 데이터 구조에 대한 데이터 보호 및 관리가 간소화됩니다. 예를 들어, 애플리케이션 데이터와 `SVM1app_logs` 애플리케이션 로그라는 두 개의 하위 정합성 보장 그룹이 포함된 이라는 부모 정합성 보장 `SVM1app_data` 그룹을 생성한다고 `SVM1_app` 가정합니다. 의 스냅샷은 `SVM1app_data` 15분마다 생성되며, 의 스냅샷은 `SVM1app_logs` 매시간마다 생성됩니다. 부모 정합성 보장 그룹에는 `SVM1_app`, 및 `SVM1app_logs` 의 스냅샷을 24시간마다 원격 클러스터에 복제하는 SnapMirror 정책이 `SVM1app_data` 있습니다. 부모 정합성 보장 `SVM1_app` 그룹은 단일 유닛으로 관리되고 하위 정합성 보장 그룹은 별도의 유닛으로 관리됩니다.

복제 관계의 일관성 그룹

ONTAP 9.17.1부터 관계를 끊거나 삭제하지 않고도 비동기 복제 관계 또는 SnapMirror 활성 동기화 관계의 일관성 그룹에 다음과 같은 지오메트리 변경을 적용할 수 있습니다. 기본 일관성 그룹에서 기하학적 변경이 발생하면 변경 사항이 보조 일관성 그룹에 복제됩니다.

- "저장 장치 크기 수정"저장 장치를 추가하거나 제거하여.
- "단일 일관성 그룹을 홍보합니다."부모 일관성 그룹에.
- "부모 일관성 그룹 강등"단일 일관성 그룹으로.
- "자식 일관성 그룹 분리"부모 일관성 그룹에서.
- "하위 정합성 보장 그룹을 생성합니다"기존 일관성 그룹을 사용합니다.

ONTAP 9.16.1에서는 다음을 수행해야 합니다."비동기 복제 관계를 끊다" 그리고"SnapMirror 활성 동기화 관계 삭제" 일관성 그룹에 기하학적 변경을 하기 전에.

스냅샷을 사용하여 **ASA r2** 시스템의 일관성 그룹을 보호하세요**.**

일관성 그룹에 속한 스토리지 유닛의 데이터를 보호하려면 ASA r2 스토리지 시스템의 일관성 그룹에 대한 스냅샷을 만듭니다. 일관성 그룹의 어떤 저장 장치에 있는 데이터를 더 이상 보호할 필요가 없는 경우 일관성 그룹에서 스냅샷 보호를 제거할 수 있습니다.

일관성 그룹 내 특정 저장 장치의 데이터를 더 이상 보호할 필요가 없는 경우 일관성 그룹에서 해당 저장 장치를 제거할 수 있습니다.

정합성 보장 그룹에 스냅샷 데이터 보호 기능을 추가합니다

정합성 보장 그룹에 스냅샷 데이터 보호를 추가하면 사전 정의된 스케줄에 따라 정합성 보장 그룹의 로컬 스냅샷이 정기적으로 생성됩니다.

"데이터를 복원합니다"손실되거나 손상된 스냅샷을 사용할 수 있습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 보호할 일관성 그룹 위에 마우스를 놓습니다.
3. 을 ⋮선택한 다음 * 편집 * 을 선택합니다.
4. Local protection * 아래에서 * Schedule snapshots * 를 선택합니다.
5. 스냅샷 정책을 선택합니다.

   기본 스냅샷 정책을 수락하거나, 기존 정책을 선택하거나, 새 정책을 생성합니다.

옵션을 선택합니다	단계
기존 스냅샷 정책을 선택합니다	⌄기본 정책 옆에 있는 을 선택한 다음 사용할 기존 정책을 선택합니다.
새 스냅샷 정책을 생성합니다	a. + Add 을 선택한 다음 새 정책 이름을 입력합니다. b. 정책 범위를 선택합니다. c. Schedules * 아래에서 를 선택합니다+ Add . d. Schedule name * 에 나타나는 이름을 선택합니다. 그런 다음 을 ⌄선택합니다. e. 정책 일정을 선택합니다. f. Maximum snapshots * 에 정합성 보장 그룹에 대해 유지할 최대 스냅샷 수를 입력합니다. g. 선택적으로 * SnapMirror label * 아래에 SnapMirror 라벨을 입력합니다. h. 저장 * 을 선택합니다.

6. 저장 * 을 선택합니다.

다음 단계

스냅샷을 통해 데이터가 보호되므로 이제 "스냅샷 복제를 설정합니다"백업 및 재해 복구를 위해 일관성 그룹을 지리적으로 멀리 떨어진 위치에 복사해야 합니다.

정합성 보장 그룹에서 스냅샷 데이터 보호를 제거합니다

정합성 보장 그룹에서 스냅샷 데이터 보호를 제거하면 정합성 보장 그룹의 모든 스토리지 유닛에 대해 스냅샷이 비활성화됩니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 보호를 중지할 일관성 그룹 위로 마우스를 가져갑니다.
3. 을 ⋮ 선택한 다음 * 편집 * 을 선택합니다.
4. Local protection * 아래에서 Schedule snapshots 를 선택 취소합니다.
5. 편집 * 을 선택합니다.

결과

정합성 보장 그룹의 스토리지 유닛에 대해 스냅샷이 생성되지 않습니다.

ASA r2 시스템에서 일관성 그룹의 크기를 수정합니다**.**

일관성 그룹의 저장 장치 수를 수정하여 일관성 그룹의 크기를 늘리거나 줄입니다.

정합성 보장 그룹에 스토리지 유닛을 추가합니다

일관성 그룹에 새 스토리지 장치나 기존 스토리지 장치를 추가하여 일관성 그룹에서 관리하는 스토리지 양을 확장합니다.

ONTAP 9.18.1부터 스냅샷 예약 및 자동 스냅샷 삭제를 설정하여 스토리지 유닛에서 스냅샷이 사용하는 공간의 양을 제한할 수 있습니다. 기존 일관성 그룹에 스토리지 유닛을 추가하면 스냅샷 예약 및 자동 스냅샷 삭제가 기본적으로 다음과 같이 설정됩니다.

추가하면...	스냅샷 예약 비율은...으로 설정됩니다.	자동 스냅샷 삭제는...
새로운 보관 장치	0	장애가 있는
기존 저장 장치	변하지 않은	변하지 않은

저장 장치를 생성할 때 새 저장 장치의 기본 설정을 수정할 수 있습니다. 당신도 할 수 있습니다"기존 저장 장치 수정" 현재 설정을 업데이트합니다.

"ASA r2 스토리지 시스템의 스냅샷 예약에 대해 자세히 알아보세요.".

시작하기 전에

ONTAP 9.16.1을 실행 중이고 확장하려는 일관성 그룹이 SnapMirror 활성 동기화 관계에 있는 경우 다음을 수행해야 합니다."SnapMirror 활성 동기화 관계 삭제" 저장 장치를 추가하기 전에. ONTAP 9.16.1을 실행 중이고 일관성 그룹이 비동기 복제 관계에 있는 경우 다음을 수행해야 합니다."관계를 끊다" 일관성 그룹을 확장하기 전에. ONTAP 9.17.1 및 이후 릴리스에서는 일관성 그룹을 확장하기 전에 SnapMirror 활성 동기화 관계를 삭제하거나 비동기 관계를 끊을 필요가 없습니다.

기존 스토리지 유닛 추가

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 확장할 일관성 그룹 위에 마우스를 놓습니다.
3. 을 선택한 다음 * 확장 * 을 선택합니다.
4. 기존 스토리지 유닛 사용 * 을 선택합니다.
5. 정합성 보장 그룹에 추가할 스토리지 유닛을 선택한 다음 * 확장 * 을 선택합니다.

새 스토리지 유닛을 추가합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 확장할 일관성 그룹 위에 마우스를 놓습니다.
3. 을 선택한 다음 * 확장 * 을 선택합니다.
4. 새 저장 장치 사용 * 을 선택합니다.
5. 생성할 단위 수와 단위당 용량을 입력합니다.

   두 개 이상의 단위를 생성하는 경우 각 단위는 동일한 용량과 동일한 호스트 운영 체제로 생성됩니다. 각 장치에 다른 용량을 할당하려면 *다른 용량 추가*를 선택하여 각 장치에 다른 용량을 할당합니다.

6. 확장 * 을 선택합니다.

다음 단계

새 스토리지 유닛을 생성한 후에는 "호스트 이니시에이터를 추가합니다"및 "새로 생성된 스토리지 유닛을 호스트에 매핑합니다"을 수행해야 합니다. 호스트 이니시에이터를 추가하면 호스트가 스토리지 유닛을 액세스하고 데이터 작업을 수행할 수 있습니다. 스토리지 유닛을 호스트에 매핑하면 스토리지 유닛이 매핑된 호스트에 데이터를 제공하기 시작할 수 있습니다.

다음 단계

정합성 보장 그룹의 기존 스냅샷에는 새로 추가된 스토리지 유닛이 포함되지 않습니다. "즉시 스냅샷을 생성합니다 "다음에 예약된 스냅샷이 자동으로 생성될 때까지 정합성 보장 그룹을 사용하여 새로 추가된 스토리지 유닛을 보호해야 합니다.

정합성 보장 그룹에서 스토리지 유닛을 제거합니다

일관성 그룹에서 저장 장치를 제거하면 해당 저장 장치를 삭제하거나, 다른 일관성 그룹의 일부로 관리하거나, 해당 데이터 보호를 중지할 수 있습니다. 일관성 그룹에서 저장 장치를 제거하면 저장 장치와 일관성 그룹 간의 관계가 끊어지지만 저장 장치는 삭제되지 않습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 스토리지 유닛을 제거할 정합성 보장 그룹을 두 번 클릭합니다.
3. Overview * 섹션의 * Storage Units * 아래에서 제거할 스토리지 유닛을 선택한 다음 * Remove from consistency group * 을 선택합니다.

결과

스토리지 유닛이 더 이상 정합성 보장 그룹의 구성원이 아닙니다.

다음 단계

스토리지 유닛에 대한 데이터 보호를 계속하려면 스토리지 유닛을 다른 정합성 보장 그룹에 추가합니다.

ASA r2 시스템에서 일관성 그룹 삭제

더 이상 일관성 그룹의 구성원을 단일 단위로 관리할 필요가 없는 경우 일관성 그룹을 삭제할 수 있습니다. 일관성 그룹이 삭제된 후에도 이전에 그룹에 속했던 저장 장치는 클러스터에서 활성 상태를 유지합니다. 일관성 그룹이 복제 관계에 있는 경우 복제된 사본은 원격 클러스터에 남아 있습니다.

시작하기 전에

ONTAP 9.16.1을 실행 중이고 삭제하려는 일관성 그룹이 SnapMirror 활성 동기화 관계에 있는 경우 다음을 수행해야 합니다."SnapMirror 활성 동기화 관계 삭제" 일관성 그룹을 삭제하기 전에. ONTAP 9.17.1 및 이후 릴리스에서는 일관성 그룹을 수정하기 전에 이 관계를 삭제할 필요가 없습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 삭제할 일관성 그룹 위에 마우스를 놓습니다.
3. 을 선택한 다음 * 삭제 * 를 선택합니다.
4. 경고를 수락한 다음 * 삭제 * 를 선택합니다.

다음 단계

정합성 보장 그룹을 삭제한 후에는 이전에 정합성 보장 그룹에 속해 있던 스토리지 유닛이 더 이상 스냅샷으로 보호되지 않습니다. 이러한 스토리지 유닛을 다른 정합성 보장 그룹에 추가하여 데이터 손실로부터 보호하는 것이 좋습니다.

ASA r2 시스템에서 계층적 일관성 그룹 관리

ONTAP 9.16.1부터 System Manager를 사용하여 ASA r2 시스템에서 계층적 일관성 그룹을 만들 수 있습니다. 계층적 구조에서는 하나 이상의 일관성 그룹이 부모 일관성 그룹 아래의 자식으로 구성됩니다. 각 자식 일관성 그룹에 개별 스냅샷 정책을 적용하고 부모를 복제하여 모든 자식 일관성 그룹의 스냅샷을 단일 단위로 원격 클러스터에 복제할 수 있습니다. 이를 통해 복잡한 데이터 구조에 대한 데이터 보호 및 관리가 간소화됩니다.

기존 일관성 그룹을 부모 일관성 그룹으로 승격

기존 일관성 그룹을 부모로 승격하면 새 자식 일관성 그룹이 생성되고 승격된 일관성 그룹에 속한 스토리지 유닛이 새 자식 일관성 그룹으로 이동됩니다. 저장 단위는 부모 일관성 그룹과 직접 연관될 수 없습니다.

시작하기 전에

ONTAP 9.16.1을 실행 중이고 승격하려는 일관성 그룹이 SnapMirror 활성 동기화 관계에 있는 경우 다음을 수행해야 합니다."SnapMirror 활성 동기화 관계 삭제" 일관성 그룹이 승격되기 전에. ONTAP 9.16.1을 실행 중이고 일관성 그룹이 비동기 복제 관계에 있는 경우 다음을 수행해야 합니다."관계를 끊다" 일관성 그룹을 홍보하기 전에. ONTAP 9.17.1 및 이후 릴리스에서는 일관성 그룹을 승격하기 전에 SnapMirror 활성 동기화 관계를 삭제하거나 비동기 관계를 끊을 필요가 없습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 부모 일관성 그룹으로 변환할 일관성 그룹 위에 마우스를 놓습니다.
3. 을 선택한 다음 * 부모 정합성 보장 그룹으로 상향 이동 * 을 선택합니다.
4. 새 자식 일관성 그룹의 이름을 입력하거나 기본 이름을 그대로 사용한 다음, 일관성 그룹 구성 요소 유형을 선택합니다.
5. 승격 * 을 선택합니다.

다음 단계

부모 일관성 그룹 아래에 추가적인 자식 일관성 그룹을 만들 수 있습니다. 당신도 할 수 있습니다"스냅샷 복제를 설정합니다" 백업 및 재해 복구를 위해 부모 및 자식 일관성 그룹을 지리적으로 멀리 떨어진 위치로 복사합니다.

부모 일관성 그룹을 단일 일관성 그룹으로 강등합니다

부모 일관성 그룹을 단일 일관성 그룹으로 강등하면 연관된 자식 일관성 그룹의 스토리지 단위가 부모 일관성 그룹에 추가됩니다. 자식 일관성 그룹이 삭제되고 부모 일관성 그룹은 단일 일관성 그룹으로 관리됩니다.

시작하기 전에

ONTAP 9.16.1을 실행 중이고 강등하려는 일관성 그룹이 SnapMirror 활성 동기화 관계에 있는 경우 다음을 수행해야 합니다."SnapMirror 활성 동기화 관계 삭제" 일관성 그룹이 강등되기 전에. ONTAP 9.16.1을 실행 중이고 일관성 그룹이 비동기 복제 관계에 있는 경우 다음을 수행해야 합니다."관계를 끊다" 일관성 그룹을 강등하기 전에. ONTAP 9.17.1 및 이후 릴리스에서는 일관성 그룹을 확장하기 전에 SnapMirror 활성 동기화 관계를 삭제하거나 비동기 관계를 끊을 필요가 없습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 강등할 부모 일관성 그룹 위에 마우스를 놓습니다.
3. 를 선택한 다음 * 단일 정합성 보장 그룹으로 하향 이동 * 을 선택합니다.
4. 하향 이동 * 을 선택합니다

다음 단계

"스냅샷 정책을 추가합니다" 이전에 하위 정합성 보장 그룹에 의해 관리되었던 스토리지 유닛을 보호하기 위해 강등된 정합성 보장 그룹으로 이동합니다.

하위 정합성 보장 그룹을 생성합니다

자식 일관성 그룹을 만들면 각 자식에 개별 스냅샷 정책을 적용할 수 있습니다. ONTAP 9.17.1부터 개별 복제 정책을 각 자식에 직접 적용할 수도 있습니다. ONTAP 9.16.1에서는 복제 정책이 부모 수준에서만 적용될 수 있습니다.

새 일관성 그룹 또는 기존 일관성 그룹에서 하위 일관성 그룹을 생성할 수 있습니다.

방법을 자세히 소개합니다

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 하위 정합성 보장 그룹을 추가할 부모 정합성 보장 그룹 위로 마우스를 가져갑니다.
3. 을 ⋮선택한 다음 * 새 하위 정합성 보장 그룹 추가 * 를 선택합니다.
4. 자식 정합성 보장 그룹의 이름을 입력하거나 기본 이름을 그대로 둔 다음 정합성 보장 그룹 구성 요소 유형을 선택합니다.
5. 기존 스토리지 유닛을 하위 정합성 보장 그룹에 추가하거나 새 스토리지 유닛을 생성하려면 선택합니다.

   새 스토리지 유닛을 생성하는 경우 생성할 유닛 수와 유닛당 용량을 입력한 다음 호스트 정보를 입력합니다.

   두 개 이상의 스토리지 유닛을 생성하는 경우 각 유닛은 동일한 용량과 동일한 호스트 운영 체제로 생성됩니다. 각 유닛에 다른 용량을 할당하려면 * 다른 용량 추가 * 를 선택합니다.

6. 추가 * 를 선택합니다.

방법을 자세히 알아보십시오

시작하기 전에

사용하려는 일관성 그룹이 이미 다른 일관성 그룹의 자식인 경우 다음을 수행해야 합니다."기존 부모 일관성 그룹에서 분리합니다." 새로운 부모 일관성 그룹으로 옮기기 전에.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 하위 일관성 그룹을 만들 기존 일관성 그룹을 선택합니다.
3. ⋮을 선택한 다음 * Move from different consistency group * 을 선택합니다.
4. 하위 일관성 그룹의 새 이름을 입력하거나 기본 이름을 그대로 둔 다음, 일관성 그룹 구성 요소 유형을 선택합니다.
5. 부모 일관성 그룹으로 만들 기존 일관성 그룹을 선택하거나 를 선택하여 새 부모 일관성 그룹을 생성합니다.

   새 부모 일관성 그룹을 생성하기로 선택한 경우 부모 일관성 그룹의 이름을 입력하거나 기본 이름을 그대로 두고 일관성 애플리케이션의 구성 요소 유형을 선택합니다.

6. 이동 * 을 선택합니다.

다음 단계

자식 일관성 그룹을 만든 후에는 다음을 수행할 수 있습니다."개별 스냅샷 보호 정책을 적용합니다" 각 어린이의 일관성 그룹에 대해. 당신도 할 수 있습니다"복제 정책 설정" 부모 및 자식 일관성 그룹을 사용하여 일관성 그룹을 원격 위치로 복제합니다.

부모 정합성 보장 그룹에서 하위 정합성 보장 그룹을 분리합니다

자식 일관성 그룹을 부모 일관성 그룹에서 분리하면 자식 일관성 그룹은 부모 일관성 그룹에서 제거되고 단일 일관성 그룹으로 관리됩니다. 부모에 적용된 복제 정책은 더 이상 분리된 자식 일관성 그룹에 적용되지 않습니다.

시작하기 전에

ONTAP 9.16.1을 실행 중이고 분리하려는 일관성 그룹이 SnapMirror 활성 동기화 관계에 있는 경우 다음을 수행해야 합니다."SnapMirror 활성 동기화 관계 삭제" 일관성 그룹을 분리하기 전에. ONTAP 9.16.1을 실행 중이고 일관성 그룹이 비동기 복제 관계에 있는 경우 다음을 수행해야 합니다."관계를 끊다" 일관성 그룹을 분리하기 전에. ONTAP 9.17.1 및 이후 릴리스에서는 일관성 그룹을 확장하기 전에 SnapMirror 활성 동기화 관계를 삭제하거나 비동기 관계를 끊을 필요가 없습니다.

단계

1. System Manager에서 * 보호 > 일관성 그룹 * 을 선택합니다.
2. 부모 일관성 그룹을 선택합니다.
3. 분리할 하위 정합성 보장 그룹을 선택합니다.
4. 를 선택한 ⋮ 다음 * 모체에서 분리 * 를 선택합니다.
5. 분리할 일관성 그룹의 새 이름을 입력하거나 기본 이름을 그대로 적용하고 일관성 그룹 애플리케이션 유형을 선택합니다.
6. 분리 * 를 선택합니다.

다음 단계

"복제 정책을 설정합니다"분리된 자식 일관성 그룹의 스냅샷을 원격 클러스터에 복제합니다.

ASA R2 스토리지 시스템에서 ONTAP 데이터 보호 정책 및 일정을 관리합니다

스냅샷 정책을 사용하여 자동화된 일정에 따라 일관성 그룹의 데이터를 보호합니다. 스냅샷 정책 내에서 정책 스케줄을 사용하여 스냅샷을 생성하는 빈도를 결정합니다.

새 보호 정책 스케줄을 생성합니다

보호 정책 스케줄은 스냅샷 정책이 실행되는 빈도를 정의합니다. 일, 시간 또는 분 수에 따라 정기적으로 실행되도록 일정을 만들 수 있습니다. 예를 들어, 매 시간마다 실행되도록 스케줄을 생성하거나 하루에 한 번만 실행할 수 있습니다. 또한 특정 요일 또는 월의 특정 시간에 실행되도록 일정을 만들 수도 있습니다. 예를 들어 매달 20일 오전 12시 15분에 실행되도록 일정을 만들 수 있습니다.

다양한 보호 정책 일정을 정의하면 여러 애플리케이션에 대한 스냅샷 빈도를 유연하게 늘리거나 줄일 수 있습니다. 따라서 중요도가 낮은 워크로드에 필요한 것보다 더 높은 수준의 보호 기능과 중요 워크로드에 데이터 손실 위험을 낮출 수 있습니다.

단계

1. 보호 > 정책 * 을 선택한 다음 * 일정 * 을 선택합니다.
2. 을 + Add 선택합니다.
3. 스케줄의 이름을 입력한 다음 스케줄 매개 변수를 선택합니다.
4. 저장 * 을 선택합니다.

다음 단계

새 정책 일정을 생성했으므로 정책 내에서 새로 생성된 일정을 사용하여 스냅샷 생성 시기를 정의할 수 있습니다.

스냅샷 정책을 생성합니다

스냅샷 정책은 스냅샷을 생성하는 빈도, 허용되는 최대 스냅샷 수 및 스냅샷을 보존하는 기간을 정의합니다.

단계

1. System Manager에서 * 보호 > 정책 * 을 선택한 다음 * Snapshot policies * 를 선택합니다.
2. 을 + Add 선택합니다.
3. 스냅샷 정책의 이름을 입력합니다.
4. 클러스터 * 를 선택하여 정책을 전체 클러스터에 적용합니다. 스토리지 VM * 을 선택하여 정책을 개별 스토리지 VM에 적용합니다.
5. Add a schedule * 을 선택한 다음 스냅샷 정책 스케줄을 입력합니다.
6. 정책 추가 * 를 선택합니다.

다음 단계

스냅샷 정책을 생성했으므로 이제 일관성 그룹에 적용할 수 있습니다. 스냅샷 정책에서 설정한 매개 변수에 따라 정합성 보장 그룹의 스냅샷이 생성됩니다.

정합성 보장 그룹에 스냅샷 정책을 적용합니다

정합성 보장 그룹에 스냅샷 정책을 적용하여 정합성 보장 그룹의 스냅샷을 자동으로 생성, 보존 및 레이블을 지정합니다.

단계

1. System Manager에서 * 보호 > 정책 * 을 선택한 다음 * Snapshot policies * 를 선택합니다.
2. 적용할 스냅샷 정책 이름 위로 마우스를 이동합니다.
3. 를 선택한 ⋮ 다음 * 적용 * 을 선택합니다.
4. 스냅샷 정책을 적용할 정합성 보장 그룹을 선택한 다음 * Apply * 를 선택합니다.

다음 단계

스냅샷을 통해 데이터가 보호되므로 이제 "복제 관계를 설정합니다"백업 및 재해 복구를 위해 일관성 그룹을 지리적으로 멀리 떨어진 위치에 복사해야 합니다.

스냅샷 정책을 편집, 삭제 또는 비활성화합니다

스냅샷 정책을 편집하여 정책 이름, 최대 스냅샷 수 또는 SnapMirror 레이블을 수정합니다. 정책 및 관련 백업 데이터를 클러스터에서 제거하는 정책을 삭제합니다. 정책에 지정된 스냅샷 생성 또는 전송을 일시적으로 중지하려면 정책을 비활성화하십시오.

단계

1. System Manager에서 * 보호 > 정책 * 을 선택한 다음 * Snapshot policies * 를 선택합니다.
2. 편집할 스냅샷 정책의 이름 위로 마우스를 가져갑니다.
3. 를 ⋮ 선택한 다음 * 편집 *, * 삭제 * 또는 * 비활성화 * 를 선택합니다.

결과

스냅샷 정책을 수정, 삭제 또는 비활성화했습니다.

복제 정책을 편집합니다

복제 정책을 편집하여 정책 설명, 전송 일정 및 규칙을 수정합니다. 또한 정책을 편집하여 네트워크 압축을 사용하거나 사용하지 않도록 설정할 수도 있습니다.

단계

1. System Manager에서 * 보호 > 정책 * 을 선택합니다.
2. Replication policies * 를 선택합니다.
3. 편집할 복제 정책 위로 마우스를 가져간 다음 을 선택합니다.
4. 편집 * 을 선택합니다.
5. 정책을 업데이트한 다음 * 저장 * 을 선택합니다.

결과

복제 정책을 수정했습니다.

데이터 보호

ASA R2 스토리지 시스템에서 유휴 데이터를 암호화합니다

유휴 상태의 데이터를 암호화할 때 스토리지 미디어가 용도 변경하거나 반환되거나 잘못 배치되거나 도난당하는 경우에는 읽을 수 없습니다. ONTAP System Manager를 사용하여 하드웨어 및 소프트웨어 수준에서 데이터를 암호화하여 이중 계층 보호를 제공할 수 있습니다.

NSE(NetApp 스토리지 암호화)는 자체 암호화 드라이브(SED)를 이용한 하드웨어 암호화를 지원합니다. SED는 데이터가 기록될 때 데이터를 암호화합니다. 각 SED에는 고유한 암호화 키가 포함되어 있습니다. SED에 저장된 암호화된 데이터는 SED의 암호화 키가 없으면 읽을 수 없습니다. SED에서 읽기를 시도하는 노드는 SED의 암호화 키에 액세스하려면 인증을 받아야 합니다. 노드는 키 관리자로부터 인증 키를 받은 다음 SED에 인증 키를 제공하여 인증됩니다. 인증 키가 유효한 경우 SED는 노드에 포함된 데이터에 액세스할 수 있는 암호화 키를 노드에 제공합니다.

ASA r2 시스템에서는 SED가 NVMe 기반 SSD에 대해서만 지원됩니다.

ASA R2 온보드 키 관리자 또는 외부 키 관리자를 사용하여 노드에 인증 키를 제공합니다.

NSE 이외에 소프트웨어 암호화를 사용하여 데이터에 더 많은 보안 계층을 추가할 수도 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션의 * 암호화 * 에서 * 구성 * 을 선택합니다.
3. Key Manager를 설정한다.

옵션을 선택합니다	단계
Onboard Key Manager를 구성합니다	a. Onboard Key Manager * 를 선택하여 키 서버를 추가합니다. b. 암호를 입력합니다.

옵션을 선택합니다	단계
외부 키 관리자를 구성합니다	a. 외부 키 관리자 * 를 선택하여 키 서버를 추가합니다. b. + Add 키 서버를 추가하려면 선택합니다. c. KMIP 서버 CA 인증서를 추가합니다. d. KMIP 클라이언트 인증서를 추가합니다.

4. 소프트웨어 암호화를 활성화하려면 * 듀얼 레이어 암호화 * 를 선택하십시오.
5. 저장 * 을 선택합니다.

다음 단계

이제 저장된 데이터를 암호화했습니다. NVMe/TCP 프로토콜을 사용하는 경우 "네트워크를 통해 전송되는 모든 데이터를 암호화합니다"NVMe/TCP 호스트와 ASA R2 시스템 간에 데이터를 암호화할 수 있습니다.

ONTAP R2 시스템의 주요 관리자 간에 ASA 데이터 암호화 키를 마이그레이션합니다

ASA R2 시스템의 ONTAP 온보드 키 관리자나 외부 키 관리자(또는 둘 다)를 사용하여 데이터 암호화 키를 관리할 수 있습니다. 외부 키 관리자는 스토리지 VM 레벨에서만 사용하도록 설정할 수 있습니다. ONTAP 클러스터 레벨에서 온보드 키 관리자 또는 외부 키 관리자를 사용하도록 설정할 수 있습니다.

에서 키 관리자를 활성화하면...	다음을 사용할 수 있습니다.
클러스터 레벨만 해당	온보드 키 관리자 또는 외부 키 관리자
스토리지 VM 수준만	외부 키 관리자만 해당됩니다
클러스터 및 스토리지 VM 수준 모두	다음 키 관리자 조합 중 하나: • 옵션 1 클러스터 레벨: 온보드 키 관리자 스토리지 VM 수준: 외부 키 관리자 • 옵션 2 클러스터 레벨: 외부 키 관리자 스토리지 VM 수준: 외부 키 관리자

ONTAP 클러스터 레벨에서 주요 관리자 간에 키를 마이그레이션합니다

ONTAP 9.16.1부터는 ONTAP CLI(Command Line Interface)를 사용하여 클러스터 레벨의 키 관리자 간에 키를 마이그레이션할 수 있습니다.

온보드부터 외부까지

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 비활성 외부 키 관리자 구성 생성:

```
security key-manager external create-config
```

3. 외부 키 관리자로 전환합니다.

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Onboard Key Manager 구성을 삭제합니다.

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. 권한 수준을 admin으로 설정합니다.

```
set -privilege admin
```

외부에서 온보드까지

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 비활성 온보드 키 관리자 구성 생성:

```
security key-manager onboard create-config
```

3. Onboard Key Manager 구성을 활성화합니다.

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. 외부 키 관리자 구성을 삭제합니다

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. 권한 수준을 admin으로 설정합니다.

```
set -privilege admin
```

ONTAP 클러스터와 스토리지 **VM** 수준에서 주요 관리자 간에 키를 마이그레이션합니다

ONTAP CLI(Command Line Interface)를 사용하여 클러스터 수준의 키 관리자와 스토리지 VM 레벨의 키 관리자 간에 키를 마이그레이션할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 키를 마이그레이션합니다.

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. 권한 수준을 admin으로 설정합니다.

```
set -privilege admin
```

랜섬웨어 공격을 방어하십시오

ASA r2 스토리지 시스템에 대한 랜섬웨어 공격으로부터 보호하기 위해 변조 방지 스냅샷을 생성합니다.

랜섬웨어 공격에 대한 보호를 강화하기 위해 스냅샷을 원격 클러스터에 복제하고 대상 스냅샷을 잠가 변조 방지를 보장합니다. 잠긴 스냅샷은 실수로 또는 악의적으로 삭제할 수 없습니다. 스토리지 유닛이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수

있습니다.

SnapLock Compliance 클록을 초기화한다

무단 변경 방지 스냅샷을 생성하려면 로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화해야 합니다.

단계

1. 클러스터 > 개요 * 를 선택합니다.
2. 노드 * 섹션에서 * SnapLock Compliance 시계 초기화 * 를 선택합니다.
3. Initialize * 를 선택합니다.
4. 규정 준수 클록이 초기화되었는지 확인
   a. 클러스터 > 개요 * 를 선택합니다.
   b. Nodes * 섹션에서 를 선택한 다음 * SnapLock Compliance Clock * 을 선택합니다.

다음 단계

로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화한 후에는 을(를) 시작할 "잠긴 스냅샷이 있는 복제 관계를 생성합니다"수 있습니다.

ASA r2 스토리지 시스템에서 AI를 사용하여 자율적인 랜섬웨어 보호 기능을 활성화하세요.

ONTAP 9.17.1부터 인공지능(AI)을 활용한 자율형 랜섬웨어 보호(ARP/AI)를 사용하여 ASA r2 시스템의 데이터를 보호할 수 있습니다. ARP/AI는 잠재적인 랜섬웨어 위협을 신속하게 감지하고, 데이터를 보호하기 위해 ARP 스냅샷을 자동으로 생성하며, 의심스러운 활동을 감지하면 시스템 관리자에 경고 메시지를 표시합니다.

ARP는 머신러닝 모델을 활용한 랜섬웨어 분석 기능을 통해 사이버 복원력을 향상시킵니다. 이 모델은 SAN 환경에서 98%의 정확도로 끊임없이 진화하는 랜섬웨어를 탐지합니다. ARP의 머신러닝 모델은 모의 랜섬웨어 공격 전후의 대규모 파일 데이터셋을 기반으로 사전 학습됩니다. 이러한 리소스 집약적인 학습은 ONTAP 외부에서 수행되며, 학습된 모델은 ONTAP에 포함되어 제공됩니다. 이 모델은 접근하거나 수정할 수 없습니다. ARP/AI는 활성화 즉시 작동하며, "학습 기간"가 필요하지 않습니다.

> 어떤 랜섬웨어 탐지 또는 예방 시스템도 랜섬웨어 공격으로부터 완벽한 안전을 보장할 수는 없습니다. 공격이 탐지되지 않을 수도 있지만, ARP/AI는 안티바이러스 소프트웨어가 침입을 탐지하지 못할 경우 중요한 추가 방어 계층 역할을 합니다.

이 작업에 대해

- ARP/AI 지원이 포함되어 있습니다. "ONTAP One 라이센스" .
- ARP/AI는 SnapMirror 액티브 동기화, SnapMirror 동기식 또는 SnapLock으로 보호되는 스토리지 유닛에서 지원되지 않습니다.
- ONTAP 9.18.1부터는 ONTAP 9.18.1로 업그레이드하거나 새로운 ONTAP 9.18.1 ASA r2 클러스터를 초기화한 후 12시간이 지나면 새로 생성되는 모든 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다.
- ARP/AI를 활성화한 후에는 다음을 수행해야 합니다. "보안 파일에 대한 자동 업데이트를 활성화하세요" 자동으로 새로운 보안 업데이트를 받습니다.

클러스터의 모든 스토리지 유닛에서 **ARP/AI** 활성화

ONTAP 9.17.1을 실행 중인 경우 클러스터에 생성된 모든 스토리지 유닛에 대해 기본적으로 ARP/AI를 활성화할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 랜섬웨어 방지 옆에서 ⋮를 선택한 다음 *기존의 모든 스토리지 유닛에서 활성화*를 선택합니다.
3. *활성화*를 선택하세요.

스토리지 **VM**의 모든 스토리지 장치에서 **ARP/AI**를 활성화합니다**.**

ONTAP 9.17.1을 실행 중인 경우 스토리지 가상 머신(VM)에 생성된 모든 스토리지 유닛에 대해 기본적으로 ARP/AI를 활성화할 수 있습니다. 즉, 스토리지 VM에 새로 생성되는 모든 스토리지 유닛에는 ARP/AI가 자동으로 활성화됩니다. 또한 스토리지 VM에 있는 기존 스토리지 유닛에도 ARP/AI를 적용할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. 시스템 관리자에서 *클러스터 > 스토리지 VM*을 선택합니다.
2. ARP/AI를 활성화할 스토리지 VM을 선택합니다.
3. 보안 섹션에서 랜섬웨어 방지 옆을 선택하세요. ⋮ ; 그런 다음 *랜섬웨어 방지 설정 편집*을 선택합니다.
4. *랜섬웨어 방지 기능 활성화*를 선택하세요.

   이렇게 하면 기본적으로 선택된 스토리지 VM에서 생성되는 모든 향후 스토리지 유닛에서 ARP/AI가 활성화됩니다.

5. 선택한 스토리지 VM의 기존 스토리지 장치에 ARP를 적용하려면 *이 스토리지 VM의 모든 해당 기존 스토리지 장치에 이 변경 사항 적용*을 선택합니다.
6. 저장 * 을 선택합니다.

결과

스토리지 VM에서 생성하는 모든 새 스토리지 유닛은 기본적으로 랜섬웨어 공격으로부터 보호되며, 의심스러운 활동은 System Manager에서 보고됩니다.

스토리지 **VM**의 특정 스토리지 장치에 대해 **ARP/AI**를 활성화합니다**.**

ONTAP 9.17.1을 실행 중이고 스토리지 VM의 모든 스토리지 유닛에서 ARP/AI를 활성화하지 않으려면 활성화할 특정 유닛을 선택할 수 있습니다.

ONTAP 9.18.1 이상에서는 모든 새 스토리지 유닛에서 ARP/AI가 기본적으로 활성화됩니다. ARP/AI가 활성화되지 않은 ONTAP 9.17.1에서 생성된 스토리지 유닛이 있는 경우 수동으로 활성화할 수 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.

2. ARP/AI를 활성화할 저장 장치를 선택하세요.
3. 선택하다 ⋮ ; 그런 다음 *랜섬웨어 방지 기능 사용*을 선택합니다.
4. *활성화*를 선택하세요.

결과

선택한 저장 장치는 랜섬웨어 공격으로부터 보호되며, 의심스러운 활동은 시스템 관리자에 보고됩니다.

ASA r2 스토리지 시스템에서 기본 자율형 랜섬웨어 보호 기능을 비활성화하십시오.

새로운 ONTAP 9.18.1 ASA r2 클러스터를 초기화하거나 클러스터를 ONTAP 9.18.1로 업그레이드하면 12시간의 유예 기간 후 모든 새 스토리지 장치에서 ARP/AI가 기본적으로 자동으로 활성화됩니다. 유예 기간 동안 ARP/AI를 비활성화하지 않으면 유예 기간이 종료될 때 새 스토리지 장치에 대해 클러스터 전체에서 활성화됩니다.

ONTAP 9.17.1에서 생성된 스토리지 장치는 ARP/AI용 "수동으로 활성화됨"이어야 합니다.

단계

최초 12시간의 유예 기간 동안 또는 그 이후에 기본 활성화를 비활성화할 수 있습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. ARP 비활성화:
   - 12시간 유예 기간 동안 비활성화하려면:
     i. **Anti-ransomware** 항목에서 *Don't enable*을 선택한 다음 *Disable*을 선택하십시오.
   - 12시간 유예 기간 후 비활성화하려면:
     i. 랜섬웨어 방지 항목에서 ✎ 를 선택한 다음 *새 저장 장치에 대해 활성화*를 선택 해제합니다.
     ii. *저장*을 선택합니다

CLI

1. 기본 활성화 상태를 확인합니다.

```
security anti-ransomware auto-enable show
```

2. 기존 볼륨 및 새 볼륨에 대한 기본 활성화를 비활성화합니다.

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

ASA r2 스토리지 시스템에서 ARP/AI 스냅샷 보존 기간 수정

인공지능(ARP/AI)을 활용한 자율 랜섬웨어 보호 기능이 ASA r2 시스템 스토리지 유닛 하나 이상에서 비정상적인 활동을 감지하면 자동으로 ARP 스냅샷을 생성하여 스토리지 유닛의 데이터를 보호합니다. 스토리지 용량 및 비즈니스 데이터 요구 사항에 따라 기본 ARP 스냅샷 보존 기간을 늘리거나 줄일 수 있습니다. 예를 들어, 비즈니스 크리티컬 애플리케이션의 보존 기간을 늘려 필요한 경우 데이터 복구를 위한 보존 기간을 늘리거나, 비핵심 애플리케이션의 보존 기간을 줄여 스토리지 공간을 절약할 수 있습니다.

ARP 스냅샷의 기본 보존 기간은 비정상적인 활동에 대한 대응 조치에 따라 달라집니다.

만약 당신이 이 작업을 수행한다면...	ARP 스냅샷은 기본적으로 다음 항목에 대해 보관됩니다.
거짓 양성으로 표시	12시간
잠재적인 랜섬웨어 공격으로 표시	7일
즉각적인 조치를 취하지 마십시오	10일

기본 보존 기간은 ONTAP 명령줄 인터페이스(CLI)를 사용하여 수정할 수 있습니다 . "ONTAP 자동 스냅샷에 대한 옵션 수정" 기본 보존 기간을 변경하는 단계는 다음과 같습니다.

ASA r2 스토리지 시스템에서 AI 알림을 통해 자율적인 랜섬웨어 보호에 대응

인공지능(ARP/AI)을 활용한 자율 랜섬웨어 보호 기능이 ASA r2 시스템 스토리지 유닛 하나 이상에서 비정상적인 활동을 감지하면 시스템 관리자 대시보드에 경고가 생성됩니다. 경고를 확인하고 활동을 확인한 후, 필요한 경우 데이터에 대한 잠재적 위협을 차단하기 위한 조치를 취해야 합니다.

ARP/AI 경고 메시지가 표시되면 조치를 취하기 전에 적절한 애플리케이션 무결성 검사기를 사용하여 스토리지 유닛의 데이터 무결성을 확인해야 합니다. 스토리지 유닛의 데이터 무결성을 확인하면 해당 활동이 허용 가능한 수준인지 아니면 잠재적인 랜섬웨어 공격인지 판단하는 데 도움이 됩니다.

비정상적인 활동이 발생하면...	그러면 이렇게 하세요...
허용 가능	해당 활동을 거짓 양성으로 표시합니다.
잠재적인 랜섬웨어 공격	해당 활동을 랜섬웨어 공격의 가능성이 있는 활동으로 표시합니다.
불확정	즉각적인 조치를 취하지 마십시오. 최대 7일 동안 저장 장치를 모니터링하십시오. 저장 장치가 계속 정상적으로 작동하면 해당 활동을 오탐(false positive)으로 표시하십시오. 저장 장치에서 비정상적인 활동이 계속 나타나면 해당 활동을 잠재적인 랜섬웨어 공격으로 표시하십시오.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.

   ARP가 하나 이상의 저장 장치에서 비정상적인 활동을 감지하면 경고 아래에 메시지가 나타납니다.

2. 경고 메시지를 선택하세요.
3. 이벤트 개요*에서 비정상적인 활동이 있는 저장 장치 수를 나타내는 *경고 메시지를 선택합니다.
4. *비정상적인 활동이 있는 보관 장치*에서 보관 장치를 선택하세요.
5. *보안*을 선택하세요.

   저장 장치에 비정상적인 활동이 있는 경우 랜섬웨어 방지 아래에 메시지가 표시됩니다.

6. *작업 선택*을 선택하세요.
7. *거짓 양성으로 표시*를 선택하거나 *잠재적 랜섬웨어 공격으로 표시*를 선택합니다.

다음 단계

스토리지 유닛 활동의 급증(일회성 급증이든 새로운 정상 상태의 특징인 급증이든)을 알고 있다면 안전하다고 보고해야 합니다. 이러한 급증을 수동으로 안전하다고 보고하면 ARP의 위협 평가 정확도를 높이는 데 도움이 됩니다. "알려진 ARP/AI 급증 보고" 방법을 알아보십시오.

ASA r2 스토리지 시스템에서 **AI**를 사용하여 자율 랜섬웨어 보호를 일시 중지하거나 재개하세요**.**

ONTAP 9.17.1부터 인공지능(ARP/AI)을 활용한 자율형 랜섬웨어 보호 기능을 사용하여 ASA r2 시스템의 데이터를 보호할 수 있습니다. 비정상적인 워크로드 이벤트를 계획하는 경우, 랜섬웨어 공격의 오탐지를 방지하기 위해 ARP/AI 분석을 일시적으로 중단할 수 있습니다. 워크로드 이벤트가 완료되면 ARP/AI 분석을 재개할 수 있습니다.

ARP/AI 일시 중지

비정상적인 작업 부하 이벤트를 시작하기 전에 랜섬웨어 공격에 대한 오탐지 방지를 위해 ARP/AI 분석을 일시적으로 중단해야 할 수도 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. ARP/AI를 일시 중지할 저장 장치를 선택하세요.
3. *랜섬웨어 방지 일시 중지*를 선택하세요.

결과

선택한 저장 장치에 대한 ARP/AI 분석이 일시 중지되고, ARP/AI를 재개할 때까지 시스템 관리자에 의심스러운 활동이 보고되지 않습니다.

ARP/AI 재개

비정상적인 작업 부하 중에 ARP/AI를 일시 중지한 경우, 작업이 완료된 후 다시 시작하여 랜섬웨어 공격으로부터 데이터를 보호해야 합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. ARP/AI를 재개할 저장 장치를 선택하세요.
3. *랜섬웨어 방지 재개*를 선택하세요.

결과

잠재적인 랜섬웨어 공격에 대한 분석이 재개되고, 의심스러운 활동이 시스템 관리자에게 보고됩니다.

ASA R2 스토리지 시스템에서 NVMe 연결을 보호합니다

NVMe 프로토콜을 사용하는 경우 대역 내 인증을 구성하여 데이터 보안을 강화할 수 있습니다. 대역 내 인증을 통해 NVMe 호스트와 ASA R2 시스템 간에 안전한 양방향 및 단방향 인증을 수행할 수 있습니다. 모든 NVMe 호스트에서 대역 내 인증을 사용할 수 있습니다. NVMe/TCP 프로토콜을 사용하는 경우 TLS(전송 계층 보안)를 구성하여 NVMe/TCP 호스트와 ASA R2 시스템 간에 네트워크를 통해 전송되는 모든 데이터를 암호화함으로써 데이터 보안을 더욱 강화할 수 있습니다.

단계

1. Hosts * 를 선택한 다음 * NVMe * 를 선택합니다.
2. 을 + Add 선택합니다.
3. 호스트 이름을 입력한 다음 호스트 운영 체제를 선택합니다.
4. 호스트 설명을 입력한 다음 호스트에 접속할 스토리지 VM을 선택합니다.
5. 호스트 이름 옆의 을 선택합니다.
6. 대역내 인증 * 을 선택합니다.
7. NVMe/TCP 프로토콜을 사용하는 경우 * TLS(전송 계층 보안) 필요 * 를 선택합니다.
8. 추가 * 를 선택합니다.

결과

대역 내 인증 및/또는 TLS를 통해 데이터 보안이 강화됩니다.

ASA R2 스토리지 시스템에서 IP 연결을 보호합니다

ASA R2 시스템에서 IP 프로토콜을 사용하는 경우 IP 보안(IPsec)을 구성하여 데이터 보안을 강화할 수 있습니다. IPsec은 전송 중 데이터 암호화, IP 수준에서 네트워크 엔드포인트 간에 흐르는 트래픽에 대한 인증, 데이터에 대한 재생 및 악의적인 가로채기 공격으로부터 보호하는 인터넷 표준입니다.

ASA R2 시스템의 경우 iSCSI 및 NVMe/TCP 호스트에 IPsec을 사용할 수 있습니다.

특정 ASA R2 시스템에서는 암호화 및 무결성 검사와 같은 여러 암호화 작업을 지원되는 NIC(Network Interface Controller) 카드로 오프로드할 수 있습니다. NIC 카드로 오프로드된 작업의 처리량은 약 5% 이하입니다. 이를 통해 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량을 크게 향상시킬 수 있습니다.

ONTAP 9.18.1부터 지원되는 IPsec 하드웨어 오프로드가 IPv6 트래픽으로 확장되었습니다.

다음 NIC 카드는 다음 ASA r2 시스템 및 ONTAP 버전에서 하드웨어 오프로드를 지원합니다.

지원되는 **NIC** 카드	**ASA r2** 시스템	**ONTAP** 버전
X50135A(2p, 40G/100G 이더넷 컨트롤러)	• ASA A1K 를 참조하십시오 • ASA A90 를 참조하십시오 • ASA A70 를 참조하십시오	ONTAP 9.17.1 이상
X60135A(2p, 40G/100G 이더넷 컨트롤러)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 이상
X50131A - (2p, 40G/100G/200g/400G 이더넷 컨트롤러)	• ASA A1K 를 참조하십시오 • ASA A90 를 참조하십시오 • ASA A70 를 참조하십시오	ONTAP 9.16.1 이상
X60132A - (4P, 10G/25G 이더넷 컨트롤러)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 이상

를 참조하십시오"NetApp Hardware Universe를 참조하십시오" 지원되는 시스템과 카드에 대한 자세한 내용은 여기를 참조하세요.

다음 단계

ASA r2 시스템에서 IPsec은 다른 ONTAP 시스템과 동일한 방식으로 구성됩니다. 자세한 내용은 다음을 참조하세요. "ONTAP 네트워크에 대한 IP 보안 구성을 준비합니다.".

관리 및 모니터링

ONTAP 업그레이드 및 되돌리기

ASA R2 스토리지 시스템에서 ONTAP를 업그레이드합니다

ASA R2 시스템에서 ONTAP 소프트웨어를 업그레이드할 때 새롭고 향상된 ONTAP 기능을 활용하여 비용을 절감하고, 중요한 워크로드를 가속화하고, 보안을 강화하고, 조직에서 사용할 수 있는 데이터 보호 범위를 확장할 수 있습니다.

ASA R2 시스템의 ONTAP 소프트웨어 업그레이드는 다른 ONTAP 시스템의 업그레이드와 동일한 프로세스를 따릅니다. Active IQ Digital Advisor(디지털 어드바이저)에 대해 유효한 SupportEdge 계약을 보유한 경우 해야 "Upgrade Advisor로 업그레이드 준비"합니다. Upgrade Advisor는 클러스터를 평가하고 구성에 맞는 업그레이드 계획을 생성하여 불확실성과 위험을 최소화하는 데 도움이 되는 인텔리전스를 제공합니다. Active IQ 디지털 어드바이저에 대해 유효한 SupportEdge 계약이 없는 경우, 해야 "Upgrade Advisor 없이 업그레이드 준비"합니다.

업그레이드를 준비하고 나면 을 사용하여 업그레이드를 수행하는 것이 좋습니다"System Manager에서 자동 무중단 업그레이드(ANDU". ANDU는 ONTAP의 고가용성(HA) 페일오버 기술을 활용하여 업그레이드 중에 클러스터가 중단 없이 데이터를 지속적으로 제공할 수 있도록 보장합니다.

에 대해 자세히 "ONTAP 소프트웨어 업그레이드"알아보십시오.

ASA r2 스토리지 시스템에서 ONTAP 되돌리기

ASA r2 시스템에 대한 ONTAP 소프트웨어 복구는 다른 ONTAP 시스템에 대한 복구와 동일한 프로세스를 따릅니다.

ONTAP 클러스터를 되돌리는 작업은 시스템 중단을 초래할 수 있습니다. 되돌리는 동안 클러스터를 오프라인 상태로 유지해야 합니다. 기술 지원팀의 도움 없이 운영 클러스터를 되돌려서는 안 됩니다. 새 클러스터나 테스트 클러스터는 도움 없이 되돌릴 수 있습니다. 새 시스템이나 테스트 클러스터의 되돌리기가 실패하거나 성공적으로 완료되었지만 운영 환경의 클러스터 성능에 만족하지 못하는 경우 기술 지원팀에 문의하여 도움을 요청하십시오.

"ONTAP 클러스터 되돌리기" .

ASA r2 시스템에 대한 요구 사항 되돌리기

특정 ASA r2 클러스터 구성에서는 ONTAP 소프트웨어 되돌리기를 시작하기 전에 특정 작업을 수행해야 합니다.

ONTAP 9.17.1에서 복귀

ASA r2 시스템에서 ONTAP 9.17.1에서 되돌리는 경우, 되돌리기를 시작하기 전에 다음 작업을 수행해야 합니다.

"동적 공간 균형 조정"이 기능은 ONTAP 9.17.1로 업그레이드하거나 새로운 ONTAP 9.17.1 ASA r2 클러스터를 초기화한 후 14일이 지나면 기본적으로 활성화됩니다. ASA r2 시스템에서 동적 공간 균형 조정을 활성화한 후에는 ONTAP 9.17.1에서 이전 버전으로 되돌릴 수 없습니다.

만약 당신이 가지고 있다면...	되돌리기 전에 다음을 수행해야 합니다.
SnapMirror 활성 동기화 관계의 계층적 일관성 그룹	"SnapMirror 활성 동기화 관계 삭제".

만약 당신이 가지고 있다면...	되돌리기 전에 다음을 수행해야 합니다.
활성 수입 관계	활성 가져오기 관계를 삭제합니다. "수입 관계에 대해 알아보세요".
랜섬웨어 방지 보호 기능 활성화	"랜섬웨어 방지 보호 일시 중지".

ASA R2 스토리지 시스템에서 펌웨어를 업데이트합니다

ONTAP는 기본적으로 ASA R2 시스템에서 펌웨어 및 시스템 파일을 자동으로 다운로드하고 업데이트합니다. 권장 업데이트를 다운로드하여 설치하기 전에 유연하게 확인할 수 있는 경우 ONTAP System Manager를 사용하여 자동화된 업데이트를 사용하지 않도록 설정하거나 업데이트 매개 변수를 편집하여 작업을 수행하기 전에 사용 가능한 업데이트 알림을 표시할 수 있습니다.

자동 업데이트를 활성화합니다

스토리지 펌웨어, SP/BMC 펌웨어 및 시스템 파일에 대한 권장 업데이트는 기본적으로 ASA R2 시스템에 자동으로 다운로드되고 설치됩니다. 자동 업데이트를 사용하지 않도록 설정한 경우 기본 동작을 복원하도록 설정할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. *소프트웨어 업데이트*에서 *활성화*를 선택합니다.
3. EULA를 읽어보세요.
4. 권장 업데이트에 대한 알림 표시*를 기본값으로 설정합니다. 선택적으로, 권장 업데이트를 *자동으로 업데이트 또는 *자동으로 해제*할 수 있습니다.
5. 업데이트 수정이 모든 현재 및 향후 업데이트에 적용됨을 확인하려면 선택합니다.
6. 저장 * 을 선택합니다.

결과

업데이트 선택 항목에 따라 권장 업데이트가 자동으로 다운로드되고 ASA R2 시스템에 설치됩니다.

자동 업데이트를 비활성화합니다

업데이트를 전적으로 직접 관리하려는 경우에만 자동 업데이트를 비활성화하십시오. 자동 업데이트가 꺼지면 시스템에서 업데이트를 알리거나 다운로드하거나 설치하지 않습니다. 모든 업데이트를 수동으로 모니터링, 다운로드, 예약 및 설치할 책임은 사용자에게 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. *소프트웨어 업데이트*에서 *비활성화*를 선택합니다.

결과

자동 업데이트를 사용할 수 없습니다. 권장 업데이트를 정기적으로 확인하고 수동 설치를 수행할지 결정해야 합니다.

자동 업데이트를 봅니다

클러스터에 다운로드되고 자동 설치가 예약된 펌웨어 및 시스템 파일 업데이트 목록을 봅니다. 이전에 자동으로 설치된 업데이트도 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 소프트웨어 업데이트 옆에서 선택하세요 → 을 선택한 다음 *모든 자동 업데이트 보기*를 선택하세요.

자동 업데이트를 편집합니다

스토리지 펌웨어, SP/BMC 펌웨어 및 시스템 파일에 대한 권장 업데이트를 클러스터에 자동으로 다운로드하고 설치하도록 선택하거나 권장 업데이트를 자동으로 해제하도록 선택할 수 있습니다. 업데이트 설치 또는 해제를 수동으로 제어하려면 권장 업데이트가 있을 때 알림을 받도록 선택합니다. 그런 다음 수동으로 선택하여 설치하거나 해제할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 소프트웨어 업데이트 옆에서 선택하세요 → 을 선택한 다음 *다른 모든 업데이트*를 선택하세요.
3. 자동 업데이트 선택 사항을 업데이트합니다.
4. 저장 * 을 선택합니다.

결과

자동 업데이트는 사용자의 선택에 따라 수정됩니다.

펌웨어를 수동으로 업데이트합니다

권장 업데이트를 다운로드 및 설치하기 전에 유연하게 볼 수 있도록 하려면 자동 업데이트를 비활성화하고 펌웨어를 수동으로 업데이트할 수 있습니다.

단계

1. 펌웨어 업데이트 파일을 서버 또는 로컬 클라이언트에 다운로드합니다.
2. 시스템 관리자에서 *클러스터 > 개요*를 선택한 다음 *기타 모든 업데이트*를 선택합니다.
3. 수동 업데이트*에서 *펌웨어 파일 추가*를 선택한 다음, *서버에서 다운로드 또는 *로컬 클라이언트에서 업로드*를 선택합니다.
4. 펌웨어 업데이트 파일을 설치합니다.

결과

펌웨어가 업데이트됩니다.

ASA R2 스토리지 시스템에서 스토리지 VM에 대한 클라이언트 액세스를 관리합니다

ASA R2 시스템의 스토리지 유닛은 스토리지 가상 머신(VM) 내에 포함됩니다. 스토리지 VM은 SAN 클라이언트에 데이터를 제공하는 데 사용됩니다. ONTAP System Manager를 사용하여

SAN 클라이언트가 스토리지 VM에 연결하고 스토리지 유닛의 데이터에 액세스할 수 있도록 LIF(네트워크 인터페이스)를 생성합니다. 선택적으로 서브넷을 사용하여 LIF 생성을 단순화하고 IPspace를 사용하여 스토리지 VM에 자체적인 보안 스토리지, 관리 및 라우팅을 제공할 수 있습니다.

스토리지 VM을 생성합니다

클러스터 설정 중에 기본 데이터 스토리지 가상 머신(VM)이 생성됩니다. 다른 스토리지 VM을 생성하고 선택하지 않는 한 모든 새 스토리지 유닛은 기본 데이터 스토리지 VM 내에 생성됩니다. 추가 스토리지 VM을 생성하여 다양한 애플리케이션, 부서 또는 클라이언트의 스토리지 유닛을 분리할 수 있습니다. 예를 들어 개발 환경용 스토리지 VM과 프로덕션 환경을 위한 다른 스토리지 VM을 만들거나 재무 부서용 스토리지 VM과 마케팅 부서를 위한 다른 스토리지 VM을 만들 수 있습니다.

단계

1. 클러스터 > 스토리지 VM * 을 선택합니다.
2. 을 + Add 선택합니다.
3. 스토리지 VM의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
4. Configure protocols * 에서 스토리지 VM에 사용할 프로토콜을 선택합니다.

   iSCSI 및 NVMe/TCP에 대해 * IP * 를 선택합니다. 파이버 채널에는 * FC * 를, NVMe/FC에는 * FC * 를 선택합니다.

5. 스토리지 VM 관리 * 에서 * 관리자 계정 관리 * 를 선택한 다음 관리자 계정의 사용자 이름과 암호를 입력합니다.
6. 스토리지 VM에 대한 네트워크 인터페이스를 추가합니다.
7. 저장 * 을 선택합니다.

다음 단계

스토리지 VM을 생성했습니다. 이제 스토리지 VM을 에 사용할 수 "스토리지 용량 할당"있습니다.

IPspace 생성

IPspace는 스토리지 VM이 상주하는 별개의 IP 주소 공간입니다. IPspace를 생성하면 스토리지 VM이 자체적인 보안 스토리지, 관리 및 라우팅을 확보할 수 있습니다. 또한 관리자가 분리된 네트워크 도메인의 클라이언트가 동일한 IP 주소 서브넷 범위의 겹치는 IP 주소를 사용할 수 있도록 합니다.

서브넷을 생성하기 전에 IPspace를 생성해야 합니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. IPspaces * 아래에서 를 선택합니다 + Add .
3. IPspace의 이름을 입력하거나 기본 이름을 그대로 사용합니다.

   "ALL"은 시스템이 예약된 이름이므로 IPspace 이름은 "ALL"일 수 없습니다.

4. 저장 * 을 선택합니다.

다음 단계

이제 IPspace를 생성했으므로 이 IPspace를 사용하여 서브넷을 만들 수 있습니다.

서브넷을 생성합니다

서브넷을 사용하면 LIF(네트워크 인터페이스)를 생성할 때 사용할 IPv4 또는 IPv6 주소의 특정 블록을 할당할 수 있습니다. 서브넷을 사용하면 각 LIF에 대한 특정 IP 주소 및 네트워크 마스크 대신 서브넷 이름을 지정할 수 있어 LIF 생성이 단순화됩니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "브로드캐스트 도메인"서브넷을 추가하려는 및 IPspace가 이미 있어야 합니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. 서브넷 * 을 선택한 다음 을 + Add 선택합니다.
3. 서브넷 이름을 입력합니다.

   모든 서브넷 이름은 IPspace 내에서 고유해야 합니다.

4. 서브넷 IP 주소와 서브넷 마스크를 입력합니다.
5. 서브넷의 IP 주소 범위를 지정합니다.

   서브넷의 IP 주소 범위를 지정할 때 IP 주소를 다른 서브넷과 겹치지 마십시오. 네트워크 문제는 서브넷 IP 주소가 중복되고 다른 서브넷이나 호스트가 동일한 IP 주소를 사용하려고 할 때 발생할 수 있습니다.

6. 서브넷의 브로드캐스트 도메인을 선택합니다.
7. 추가 * 를 선택합니다.

다음 단계

LIF 생성을 단순화하는 데 사용할 수 있는 서브넷을 생성했습니다.

LIF(네트워크 인터페이스) 생성

LIF(네트워크 인터페이스)는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 데이터에 액세스하는 데 사용할 포트에 LIF를 생성합니다. 스토리지 VM은 하나 이상의 LIF를 통해 클라이언트에 데이터를 제공합니다. 구성 요소 장애가 발생하는 경우 LIF가 페일오버되거나 다른 물리적 포트로 마이그레이션되어 네트워크 통신이 중단되지 않습니다.

ASA R2 시스템에서 IP, FC 및 NVMe/FC LIF를 생성할 수 있습니다. IP 데이터 LIF는 기본적으로 iSCSI 및 NVMe/TCP 트래픽을 모두 처리할 수 있습니다. FC 및 NVMe/FC 트래픽에는 대해 별도의 데이터 LIF를 생성해야 합니다.

자동 iSCSI LIF 페일오버를 활성화하려면 iSCSI 전용 트래픽에 대해 IP LIF를 생성해야 합니다. 자동 iSCSI LIF 페일오버가 사용되도록 설정된 경우 스토리지 페일오버가 발생하면 IP iSCSI LIF가 홈 노드나 포트에서 HA 파트너 노드 또는 포트로 자동으로 마이그레이션된 다음, 페일오버가 완료된 후 다시 수행됩니다. 또는 IP iSCSI LIF의 포트가 정상 상태가 아닐 경우 LIF는 자동으로 현재 홈 노드의 정상 포트로 마이그레이션된 다음 포트가 다시 정상화되면 원래 포트로 다시 돌아갑니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.
- 클러스터 간 노드 트래픽을 처리하는 LIF는 LIF가 관리 트래픽을 처리하거나 데이터 트래픽을 처리하는 LIF와 같은 서브넷에 있으면 안 됩니다.

단계

1. 네트워크 > 개요 * 를 선택합니다.
2. 네트워크 인터페이스 * 를 선택한 다음 를 + Add 선택합니다.
3. 인터페이스 유형과 프로토콜을 선택한 다음 스토리지 VM을 선택합니다.
4. LIF의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
5. 네트워크 인터페이스의 홈 노드를 선택한 다음 IP 주소와 서브넷 마스크를 입력합니다.
6. 저장 * 을 선택합니다.

결과

데이터 액세스를 위한 LIF를 생성했습니다.

다음 단계

ONTAP 명령줄 인터페이스(CLI)를 사용하여 자동 장애 조치가 포함된 iSCSI 전용 LIF를 만들 수 있습니다.

사용자 정의 **iSCSI** 전용 **LIF** 서비스 정책 만들기

자동 LIF 장애 조치를 통해 iSCSI 전용 LIF를 만들려면 먼저 사용자 지정 iSCSI 전용 LIF 서비스 정책을 만들어야 합니다.

사용자 지정 서비스 정책을 만들려면 ONTAP 명령줄 인터페이스(CLI)를 사용해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 사용자 지정 iSCSI 전용 LIF 서비스 정책을 만듭니다.

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. 서비스 정책이 생성되었는지 확인하세요.

```
network interface service-policy show -policy <service_policy_name>
```

4. 권한 수준을 admin으로 되돌립니다.

```
set -privilege admin
```

자동 **LIF** 장애 조치를 통해 **iSCSI** 전용 **LIF** 만들기

스토리지 VM에 자동 LIF 장애 조치가 활성화되지 않은 iSCSI LIF가 있는 경우, 새로 만든 LIF도 자동 LIF 장애 조치가 활성화되지 않습니다. 자동 LIF 장애 조치가 활성화되지 않고 장애 조치 이벤트가 발생하는 경우 iSCSI LIF가 마이그레이션되지 않습니다.

시작하기 전에

사용자 지정 iSCSI 전용 LIF 서비스 정책을 만들어야 합니다.

단계

1. 자동 LIF 장애 조치를 통해 iSCSI 전용 LIF를 만듭니다.

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

   - 각 노드에 패브릭 A와 패브릭 B에 각각 하나씩, 총 두 개의 iSCSI LIF를 생성하는 것이 좋습니다. 이렇게 하면 iSCSI 트래픽에 대한 중복성과 부하 분산이 가능합니다. 다음 예에서는 각 노드에 두 개씩, 각 패브릭에 하나씩, 총 네 개의 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- VLAN을 사용하는 경우 다음을 조정하세요. `home-port` 예를 들어, 각 iSCSI 패브릭에 대한 VLAN 포트 정보를 포함하는 매개변수 `-home-port e2b-<iSCSI-A-VLAN>` iSCSI 패브릭 A 및 `-home-port e4b-<iSCSI-B-VLAN>` .
- VLAN과 함께 인터페이스 그룹(ifgroups)을 사용하는 경우 다음을 조정하십시오. `home-port` 예를 들어 적절한 VLAN 포트를 포함하는 매개변수 `-home-port a0a-<iSCSI-A-VLAN>` iSCSI 패브릭 A 및 `-home-port a0a-<iSCSI-B-VLAN>` iSCSI 패브릭 B의 경우 `a0a` 는 ifgroup이고 a0a-<iSCSI-A-VLAN>과 a0a-<iSCSI-B-VLAN>은 각각 iSCSI A 패브릭과 iSCSI B 패브릭에 대한 VLAN 포트입니다.

2. iSCSI LIF가 생성되었는지 확인하세요.

```
network interface show -lif iscsi*
```

LIF(네트워크 인터페이스) 수정

LIF는 필요에 따라 사용하지 않도록 설정하거나 이름을 바꿀 수 있습니다. LIF IP 주소 및 서브넷 마스크를 변경할 수도 있습니다.

이 작업에 대해

ONTAP NTP(네트워크 시간 프로토콜)를 활용하여 클러스터 전체에서 시간을 동기화합니다. LIF IP 주소를 변경한 후에는 동기화 실패를 방지하기 위해 NTP 구성을 업데이트해야 할 수도 있습니다. 자세한 내용은 지식 기반 문서를 참조하세요."LIF IP 변경 후 NTP 동기화가 실패합니다." .

단계

1. 네트워크 > 개요 * 를 선택한 다음 * 네트워크 인터페이스 * 를 선택합니다.
2. 편집할 네트워크 인터페이스 위로 마우스를 가져간 다음 을 ⋮ 선택합니다.

3. 편집 * 을 선택합니다.
4. 네트워크 인터페이스를 비활성화하거나, 네트워크 인터페이스의 이름을 바꾸거나, IP 주소를 변경하거나, 서브넷 마스크를 변경할 수 있습니다.
5. 저장 * 을 선택합니다.

결과

LIF가 수정되었습니다.

ASA R2 스토리지 시스템에서 클러스터 네트워킹을 관리합니다

ONTAP System Manager를 사용하여 ASA R2 시스템에서 기본적인 스토리지 네트워크 관리를 수행할 수 있습니다. 예를 들어 브로드캐스트 도메인을 추가하거나 다른 브로드캐스트 도메인에 포트를 재할당할 수 있습니다.

브로드캐스트 도메인을 추가합니다

브로드캐스트 도메인을 사용하면 동일한 계층 2 네트워크에 속하는 네트워크 포트를 그룹화하여 클러스터 네트워크 관리를 간소화할 수 있습니다. 그러면 VM(스토리지 가상 머신)이 데이터 또는 관리 트래픽에 그룹의 포트를 사용할 수 있습니다.

클러스터 설정 중에 "기본" 브로드캐스트 도메인 및 "클러스터" 브로드캐스트 도메인이 생성됩니다. "기본" 브로드캐스트 도메인에는 "기본" IPspace에 있는 포트가 포함되어 있습니다. 이러한 포트는 주로 데이터를 제공하는 데 사용됩니다. 클러스터 관리 및 노드 관리 포트도 이 브로드캐스트 도메인에 있습니다. "클러스터" 브로드캐스트 도메인에는 "클러스터" IPspace에 있는 포트가 포함되어 있습니다. 이러한 포트는 클러스터 통신에 사용되며 클러스터의 모든 노드에 있는 모든 클러스터 포트를 포함합니다.

클러스터가 초기화된 후 추가 브로드캐스트 도메인을 생성할 수 있습니다. 브로드캐스트 도메인을 생성하면 동일한 포트가 포함된 페일오버 그룹이 자동으로 생성됩니다.

이 작업에 대해

브로드캐스트 도메인에 추가된 포트의 MTU(Maximum Transmission Unit)가 브로드캐스트 도메인에 설정된 MTU 값으로 업데이트됩니다.

단계

1. System Manager에서 * 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 * 도메인 아래에서 를 선택합니다 + Add .
3. 브로드캐스트 도메인의 이름을 입력하거나 기본 이름을 그대로 사용합니다.

   모든 브로드캐스트 도메인 이름은 IPspace 내에서 고유해야 합니다.

4. 브로드캐스트 도메인의 IPspace를 선택합니다.

   IPspace 이름을 지정하지 않으면 브로드캐스트 도메인이 "기본" IPspace에 만들어집니다.

5. MTU(Maximum Transmission Unit)를 입력합니다.

   MTU는 브로드캐스트 도메인에서 허용할 수 있는 가장 큰 데이터 패킷입니다.

6. 원하는 포트를 선택한 다음 * 저장 * 을 선택합니다.

결과

새 브로드캐스트 도메인을 추가했습니다.

포트를 다른 브로드캐스트 도메인에 재할당합니다

포트는 하나의 브로드캐스트 도메인에만 속할 수 있습니다. 포트가 속한 브로드캐스트 도메인을 변경하려면 포트를 기존 브로드캐스트 도메인에서 새 브로드캐스트 도메인으로 재할당해야 합니다.

단계

1. System Manager에서 * 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 도메인 * 에서 도메인 이름 옆에 있는 을 선택한 다음 * 편집 * 을 선택합니다.
3. 다른 도메인에 재할당할 이더넷 포트의 선택을 취소합니다.
4. 포트를 재할당할 브로드캐스트 도메인을 선택한 다음 * 재할당 * 을 선택합니다.
5. 저장 * 을 선택합니다.

결과

포트를 다른 브로드캐스트 도메인에 다시 할당했습니다.

VLAN을 생성합니다

VLAN은 브로드캐스트 도메인으로 그룹화된 스위치 포트로 구성됩니다. VLAN을 사용하면 보안을 강화하고, 문제를 격리하고, IP 네트워크 인프라 내에서 사용 가능한 경로를 제한할 수 있습니다.

시작하기 전에

네트워크에 배포된 스위치는 IEEE 802.1Q 표준을 준수하거나 공급업체별로 VLAN을 구현해야 합니다.

이 작업에 대해

- 구성원 포트가 없는 인터페이스 그룹 포트에는 VLAN을 만들 수 없습니다.
- 처음으로 포트를 통해 VLAN을 구성할 때 포트가 다운되어 일시적으로 네트워크 연결이 끊길 수 있습니다. 이후에 동일한 포트에 VLAN을 추가해도 포트 상태는 영향을 받지 않습니다.
- 스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

단계

1. System Manager에서 * 네트워크 > 이더넷 포트 * 를 선택한 다음 를 선택합니다 + VLAN.
2. VLAN에 대한 노드와 브로드캐스트 도메인을 선택합니다.
3. VLAN의 포트를 선택합니다.

   클러스터 LIF를 호스팅하는 포트 또는 클러스터 IPspace에 할당된 포트에 VLAN을 연결할 수 없습니다.

4. VLAN ID를 입력합니다.
5. 저장 * 을 선택합니다.

결과

보안을 강화하고, 문제를 격리하고, IP 네트워크 인프라 내에서 사용 가능한 경로를 제한하기 위해 VLAN을 만들었습니다.

사용량을 모니터링하고 용량을 늘립니다

ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 성능을 모니터링합니다

ONTAP System Manager를 사용하여 클러스터의 전반적인 성능과 특정 스토리지 유닛의 성능을 모니터링하여 지연 시간, IOPS 및 처리량이 중요 비즈니스 애플리케이션에 미치는 영향을 파악할 수 있습니다. 성능은 1시간에서 1년까지 다양한 기간 동안 모니터링할 수 있습니다.

예를 들어, 중요한 애플리케이션에서 높은 지연 시간과 낮은 처리량이 발생한다고 가정합니다. 지난 5일(영업일 기준) 동안 클러스터 성능을 보면 매일 동시에 성능이 저하되는 것을 알 수 있습니다. 이 정보를 사용하여 중요하지 않은 프로세스가 백그라운드에서 실행되기 시작할 때 중요한 애플리케이션이 클러스터 리소스를 두고 경합하고 있는지 확인합니다. 그런 다음 QoS 정책을 수정하여 중요하지 않은 워크로드가 시스템 리소스에 미치는 영향을 제한하고 중요 워크로드가 최소 처리량 목표를 충족하도록 할 수 있습니다.

클러스터 성능을 모니터링합니다

클러스터 성능 메트릭을 사용하여 지연 시간을 최소화하고 중요 애플리케이션의 IOPS 및 처리량을 극대화하기 위해 워크로드를 이동해야 하는지 여부를 결정할 수 있습니다.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.
2. Performance * 에서 클러스터의 지연 시간, IOPS 및 처리량을 시간, 일, 주, 월 또는 연도별로 확인합니다.
3. 성능 데이터를 다운로드하려면 선택합니다.

다음 단계

클러스터 성능 메트릭을 사용하여 QoS 정책을 수정하거나 애플리케이션 워크로드를 조정할 필요가 있는지 분석하여 전체 클러스터 성능을 극대화할 수 있습니다.

스토리지 유닛 성능을 모니터링합니다

스토리지 유닛 성능 메트릭을 사용하여 특정 애플리케이션이 지연 시간, IOPS 및 처리량에 미치는 영향을 확인합니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 모니터링할 스토리지 유닛을 선택한 다음 * Overview * 를 선택합니다.
3. Performance * 에서 시간, 일, 주, 월 또는 연도별로 스토리지 유닛의 지연 시간, IOPS 및 처리량을 확인합니다.
4. 성능 데이터를 다운로드하려면 선택합니다.

다음 단계

스토리지 유닛 성능 메트릭을 사용하여 스토리지 유닛에 할당된 QoS 정책을 수정해야 하는지 여부를 분석하여 지연

시간을 줄이고 IOPS 및 처리량을 극대화합니다.

ASA R2 스토리지 시스템에서 클러스터 및 스토리지 유닛 활용도를 모니터링합니다

ONTAP System Manager를 사용하여 스토리지 활용률을 모니터링하여 현재 및 미래의 워크로드를 처리하는 데 필요한 스토리지 용량을 확보하십시오.

클러스터 활용률을 모니터링합니다

클러스터에서 사용하는 스토리지 양을 정기적으로 모니터링하여 필요한 경우 공간이 부족해지기 전에 클러스터 용량을 확장할 준비가 되었는지 확인합니다.

단계

1. System Manager에서 * 대시보드 * 를 선택합니다.
2. Capacity * 에서 클러스터에서 사용된 물리적 공간의 양과 사용 가능한 공간의 양을 확인합니다.

   데이터 축소율은 스토리지 효율성을 통해 절약된 공간의 양을 나타냅니다.

다음 단계

클러스터에 공간이 부족하거나 향후 요구 사항을 충족할 수 있는 용량이 없는 경우 "새 드라이브를 추가합니다"ASA R2 시스템을 구축하여 스토리지 용량을 늘려야 합니다.

스토리지 가용 영역 활용률 모니터링

ASA R2 시스템의 각 HA 쌍은 _ 스토리지 가용성 영역 _ 이라는 공통 스토리지 풀을 사용합니다. 스토리지 가용 영역은 스토리지 시스템의 모든 가용 디스크에 액세스할 수 있으며 HA 쌍의 두 노드에 표시됩니다.

클러스터에 4개 이상의 노드가 있는 경우 각 HA 쌍의 스토리지 가용성 영역에서 사용하는 공간의 양을 볼 수 있습니다. 2노드 클러스터에는 이 메트릭을 사용할 수 없습니다.

단계

1. System Manager에서 * Cluster * 를 선택한 다음 * Overview * 를 선택합니다.

   스토리지 가용 영역 활용률에 대한 요약이 클러스터의 각 HA 쌍에 대해 표시됩니다.

2. 보다 자세한 메트릭을 원하는 경우 특정 스토리지 가용성을 선택합니다.

   개요 * 아래에 스토리지 가용 영역의 용량, 사용된 공간 및 데이터 축소율이 표시됩니다.

   Storage units * 아래에 스토리지 가용 영역의 모든 스토리지 유닛 목록이 표시됩니다.

다음 단계

스토리지 가용 영역에서 공간이 부족하면 다른 스토리지 가용 영역을 계획하여 클러스터 전체에서 스토리지 사용률의 균형을 조정해야 "저장 장치를 이동합니다"합니다.

스토리지 유닛 사용률을 모니터링합니다

스토리지 유닛에서 사용하는 스토리지 양을 모니터링하여 비즈니스 요구 사항에 따라 스토리지 유닛의 크기를 사전에 늘릴 수 있습니다.

단계

1. System Manager에서 * Storage * 를 선택합니다.
2. 모니터링할 스토리지 유닛을 선택한 다음 * Overview * 를 선택합니다.
3. 스토리지 * 에서 다음을 확인합니다.
   - 저장 장치의 크기입니다
   - 사용된 공간의 양입니다
   - 데이터 축소율

     데이터 축소율은 스토리지 효율성을 통해 절약된 공간의 양을 나타냅니다
   - 스냅샷이 사용되었습니다

     사용된 스냅샷은 스냅샷에 사용되는 스토리지의 양을 나타냅니다.

다음 단계

저장 장치 용량이 거의 다 되면 "스토리지 유닛을 수정합니다"크기를 늘려야 합니다.

ASA R2 스토리지 시스템에서 스토리지 용량을 늘립니다

노드나 쉘프에 드라이브를 추가하여 ASA R2 시스템의 스토리지 용량을 늘립니다.

NetApp Hardware Universe를 사용하여 새 드라이브 설치를 준비합니다

노드나 선반에 새 드라이브를 설치하기 전에 NetApp Hardware Universe 사용하여 추가하려는 드라이브가 ASA r2 시스템에서 지원되는지 확인하고 새 드라이브에 적합한 슬롯을 식별하세요. 드라이브를 추가하는 데 적합한 슬롯은 시스템 모델과 ONTAP 버전에 따라 다릅니다. 어떤 경우에는 특정 슬롯에 드라이브를 순서대로 추가해야 합니다.

단계

1. 로 이동합니다"NetApp Hardware Universe를 참조하십시오".
2. 제품 * 에서 하드웨어 구성을 선택합니다.
3. ASA r2 시스템을 선택하세요.
4. ONTAP 버전을 선택한 다음 * 결과 표시 * 를 선택합니다.
5. 그래픽 아래에서 * 대체 보기를 보려면 여기를 클릭하십시오 * 를 선택한 다음 구성과 일치하는 보기를 선택하십시오.
6. 구성 보기를 사용하여 새 드라이브가 지원되는지, 올바른 설치 슬롯이 지원되는지 확인합니다.

결과

새 드라이브가 지원되는지 확인했으며 설치에 적합한 슬롯을 알고 있습니다.

ASA R2에 새 드라이브를 설치합니다

단일 절차에서 추가해야 하는 최소 드라이브 수는 6개입니다. 단일 드라이브를 추가하면 성능이 저하될 수 있습니다.

이 작업에 대해

각 드라이브에 대해 이 절차의 단계를 반복해야 합니다.

단계

1. 적절하게 접지합니다.
2. 시스템 전면에서 베젤을 조심스럽게 제거합니다.
3. 새 드라이브를 올바른 슬롯에 삽입합니다.
   a. 캠 핸들이 열린 위치에 있는 상태에서 두 손을 사용하여 새 드라이브를 삽입합니다.
   b. 드라이브가 멈출 때까지 누릅니다.
   c. 드라이브가 중간 평면에 완전히 장착되고 핸들이 제자리에 고정되도록 캠 핸들을 닫습니다.

      캠 핸들이 드라이브 면과 올바르게 정렬되도록 캠 핸들을 천천히 닫아야 합니다.
4. 드라이브의 작동 LED(녹색)가 켜져 있는지 확인합니다.
   - LED가 켜져 있으면 드라이브에 전원이 들어옵니다.
   - LED가 깜박이면 드라이브에 전원이 들어오고 I/O가 진행 중인 것입니다. 드라이브 펌웨어를 업데이트하는 경우에도 LED가 깜박입니다.

     현재 펌웨어 버전이 없는 새 드라이브에서 드라이브 펌웨어가 중단 없이 자동으로 업데이트됩니다.
5. 노드가 드라이브 자동 할당으로 구성되어 있는 경우 ONTAP가 새 드라이브를 노드에 자동으로 할당할 때까지 기다릴 수 있습니다. 노드가 드라이브 자동 할당으로 구성되지 않았거나 원하는 경우 드라이브를 수동으로 할당할 수 있습니다.

   새 드라이브는 노드에 할당될 때까지 인식되지 않습니다.

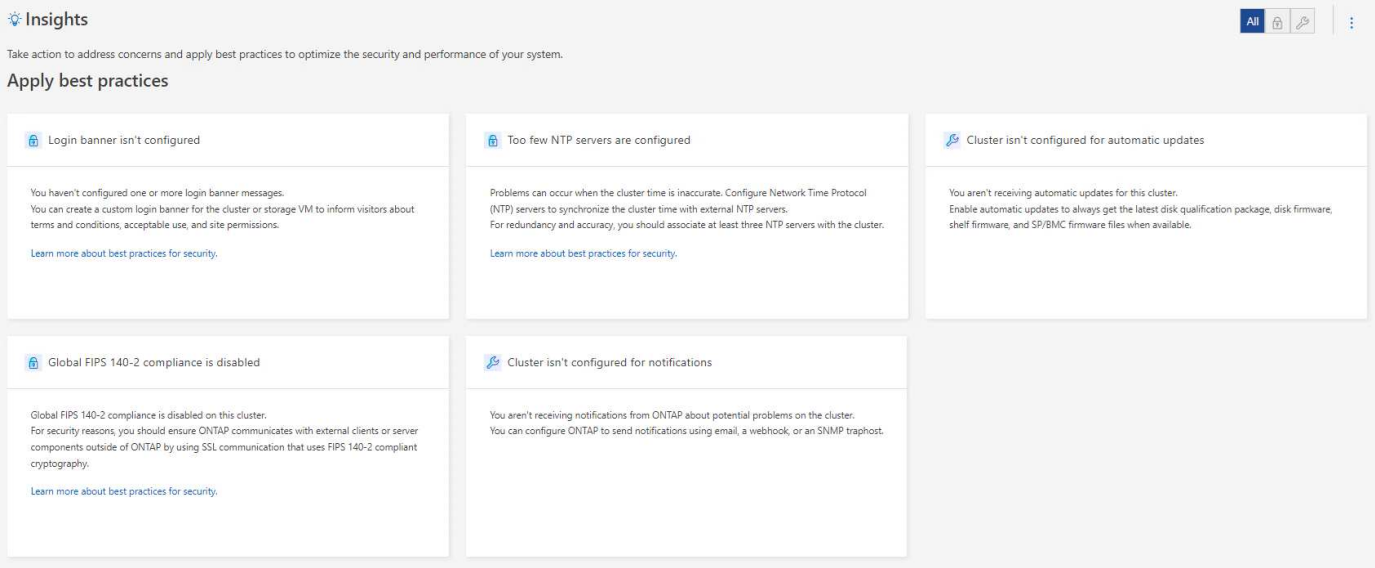
다음 단계

새 드라이브가 인식되면 드라이브가 추가되었고 소유권이 올바르게 지정되었는지 확인합니다.

ASA R2 스토리지 시스템 인사이트를 통해 클러스터 보안 및 성능을 최적화합니다

ONTAP System Manager에서 View_Insights_를 사용하여 ASA R2 시스템에 구현할 수 있는 모범 사례와 구성 수정 사항을 파악하여 클러스터 보안 및 성능을 최적화할 수 있습니다.

예를 들어, 클러스터에 사용하도록 NTP(네트워크 시간 프로토콜) 서버가 구성되어 있다고 가정합니다. 그러나 최적의 클러스터 시간 관리에 필요한 NTP 서버의 수가 권장된 수보다 적다는 사실을 모르고 있습니다. 클러스터 시간이 정확하지 않을 때 발생할 수 있는 문제를 방지하기 위해 Insights에서는 NTP 서버가 너무 적게 구성되어 있음을 알리고 이 문제에 대해 자세히 알아보거나 수정하거나 무시할 수 있는 옵션을 제공합니다.



단계

1. System Manager에서 * Insights * 를 선택합니다.
2. 권장 사항을 검토합니다.

다음 단계

모범 사례를 구현하고 클러스터 보안 및 성능을 최적화하는 데 필요한 작업을 수행합니다.

ASA R2 스토리지 시스템에서 클러스터 이벤트 및 작업을 봅니다

ONTAP System Manager를 사용하면 시스템에서 발생한 오류 또는 경고 목록과 권장 수정 조치를 볼 수 있습니다. 또한 시스템 감사 로그 및 활성, 완료 또는 실패한 작업 목록을 볼 수 있습니다.

단계

1. System Manager에서 * Events & Jobs * 를 선택합니다.
2. 클러스터 이벤트 및 작업을 봅니다.

이 항목을 보려면...	수행할 작업...
클러스터 이벤트입니다	이벤트 * 를 선택한 다음 * 이벤트 로그 * 를 선택합니다.
Active IQ 제안	이벤트 * 를 선택한 다음 * Active IQ Suggestions * 를 선택합니다.
시스템 경고	a. 시스템 알림 * 을 선택합니다. b. 조치를 취할 시스템 알림을 선택합니다. c. 경고를 확인하거나 표시하지 않습니다.
클러스터 작업	작업 * 을 선택합니다.

이 항목을 보려면...	수행할 작업...
감사 로그	Audit logs * 를 선택합니다.

클러스터 이벤트 및 감사 로그에 대한 이메일 알림을 보냅니다

클러스터 이벤트 또는 감사 로그 항목이 있을 때 특정 이메일 주소로 알림을 보내도록 시스템을 구성합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. Notifications management * 옆에 있는 을 선택합니다⋮.
3. 이벤트 목적지를 구성하려면 * 이벤트 목적지 보기 * 를 선택한 다음 * 이벤트 목적지 * 를 선택하십시오. 감사 로그 대상을 구성하려면 * 감사 대상 보기 * 를 선택한 다음 * 감사 로그 대상 * 을 선택합니다.
4. 을 + Add 선택합니다.
5. 목적지 정보를 입력한 다음 * 추가 * 를 선택합니다.

결과

추가한 이메일 주소는 클러스터 이벤트 및 감사 로그에 대해 지정된 이메일 알림을 받습니다.

노드 관리

ASA R2 노드를 ONTAP 클러스터에 추가합니다

ONTAP 9.16.1부터 ASA r2 스토리지 시스템은 클러스터당 최대 12개의 노드를 지원합니다. HA 쌍의 새 노드에 케이블이 연결되고 전원이 켜진 후에는 이를 클러스터에 조인해야 합니다.

시작하기 전에

다음 정보를 수집합니다.

- 노드 IP 주소입니다
- 인터클러스터 네트워크 인터페이스 IP 주소입니다
- 인터클러스터 네트워크 서브넷 마스크입니다
- 인터클러스터 네트워크 게이트웨이입니다
- 온보드 키 관리자(OKM)를 구성하려면 OKM 암호가 필요합니다.

단계

1. System Manager에서 * 클러스터 > 개요 * 를 선택합니다.
2. 클러스터에 연결할 노드 옆에 있는 을 선택한 ⋮다음 * 노드 추가 * 를 선택합니다
3. 각 노드의 IP 주소를 입력합니다.
4. 인터클러스터 네트워크 인터페이스 IP 주소, 서브넷 마스크 및 게이트웨이를 입력합니다.
5. 온보드 키 관리자(OKM)를 구성하려면 OKM 암호를 입력합니다.

◦ 암호화를 위한 온보드 키 관리자 구성 * 이 기본적으로 선택됩니다.

6. 추가 * 를 선택합니다.

결과

새 HA 쌍이 클러스터에 결합되었습니다.

다음 단계

클러스터에 새 HA 쌍을 추가한 후에는 새 노드를 사용할 수 있습니다"SAN 호스트에서 데이터 액세스가 가능합니다".

ASA R2 스토리지 시스템에서 노드를 재부팅합니다

유지보수, 문제 해결, 소프트웨어 업데이트 또는 기타 관리상의 이유로 노드를 재부팅해야 할 수 있습니다. 노드가 재부팅되면 HA 파트너가 자동으로 테이크오버를 실행합니다. 파트너 노드는 재부팅된 노드가 다시 온라인 상태가 된 후에 자동 반환을 수행합니다.

단계

1. System Manager에서 * 클러스터 > 개요 * 를 선택합니다.
2. 재부팅하려는 노드 옆에 있는 을 선택한 다음 * 재부팅 * 을 선택합니다.
3. 노드를 재부팅하는 이유를 입력한 다음 * Reboot * 를 선택합니다.

   재부팅 이유를 입력한 이유는 시스템 감사 로그에 기록됩니다.

다음 단계

노드가 재부팅 중인 동안 HA 파트너가 테이크오버를 수행하여 데이터 서비스가 중단되지 않도록 합니다. 재부팅이 완료되면 HA 파트너가 기브백을 수행합니다.

ASA R2 스토리지 시스템에서 노드 이름을 바꿉니다

ONTAP System Manager를 사용하여 ASA R2 시스템에서 노드 이름을 바꿀 수 있습니다. 조직의 명명 규칙에 맞게 또는 기타 관리 상의 이유로 노드 이름을 변경해야 할 수도 있습니다.

단계

1. System Manager에서 * 클러스터 > 개요 * 를 선택합니다.
2. 이름을 바꾸려는 노드 옆에 있는 을 선택한 다음 * Rename * 을 선택합니다.
3. 노드의 새 이름을 입력한 다음 * Rename * 을 선택합니다.

결과

새 이름이 노드에 적용됩니다.

ASA R2 스토리지 시스템에서 사용자 계정 및 역할을 관리합니다

System Manager를 사용하여 사용자 계정에 대한 Active Directory 도메인 컨트롤러 액세스, LDAP 및 SAML 인증을 구성합니다. 사용자 계정 역할을 생성하여 역할에 할당된 사용자가 클러스터에서 수행할 수 있는 특정 기능을 정의합니다.

Active Directory 도메인 컨트롤러 액세스를 구성합니다

AD 계정 액세스를 설정할 수 있도록 클러스터 또는 스토리지 VM에 대한 AD(Active Directory) 도메인 컨트롤러 액세스를 구성합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션의 * Active Directory * 아래에서 * 구성 * 을 선택합니다.

다음 단계

이제 ASA R2 시스템에서 AD 계정 액세스를 활성화할 수 있습니다.

LDAP를 구성합니다

LDAP(Lightweight Directory Access Protocol) 서버를 구성하여 인증을 위한 사용자 정보를 중앙에서 관리합니다.

시작하기 전에

인증서 서명 요청을 생성하고 CA 서명 서버 디지털 인증서를 추가해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * LDAP * 옆에 있는 를 선택합니다.
3. 필요한 LDAP 서버 및 바인딩 정보를 입력한 다음 * 저장 * 을 선택합니다.

다음 단계

이제 사용자 정보 및 인증에 LDAP를 사용할 수 있습니다.

SAML 인증을 구성합니다

SAML(Security Assertion Markup Language) 인증을 사용하면 Active Directory 및 LDAP와 같은 직접 서비스 공급자 대신 IDP(Secure Identity Provider)에서 사용자를 인증할 수 있습니다.

시작하기 전에

- 원격 인증에 사용하려는 IDP를 구성해야 합니다.

  구성에 대해서는 IDP 설명서를 참조하십시오.

- IDP의 URI가 있어야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * SAML 인증 * 옆에 있는 를 선택합니다.
3. SAML 인증 활성화 * 를 선택합니다.
4. IDP URL 및 호스트 시스템 IP 주소를 입력한 다음 * 저장 * 을 선택합니다.

   확인 창에 메타데이터 정보가 표시되며, 이 정보는 클립보드에 자동으로 복사됩니다.

5. 지정한 IDP 시스템으로 이동한 다음 클립보드에서 메타데이터를 복사하여 시스템 메타데이터를 업데이트합니다.
6. System Manager의 확인 창으로 돌아가서 * I have configured the IDP with the host URI or metadata * 를 선택합니다.
7. SAML 기반 인증을 활성화하려면 * 로그아웃 * 을 선택합니다.

   IDP 시스템에 인증 화면이 표시됩니다.

다음 단계

이제 사용자 계정에 대해 SAML 인증을 사용할 수 있습니다.

사용자 계정 역할을 생성합니다

클러스터 관리자 및 스토리지 VM 관리자의 역할은 클러스터가 초기화될 때 자동으로 생성됩니다. 추가 사용자 계정 역할을 생성하여 역할에 할당된 사용자가 클러스터에서 수행할 수 있는 특정 기능을 정의합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * 사용자 및 역할 * 옆에 있는 를 선택합니다 →.
3. 역할 * 에서 을 + Add 선택합니다.
4. 역할 속성을 선택합니다.

   여러 속성을 추가하려면 을 선택합니다 + Add .
5. 저장 * 을 선택합니다.

결과

새 사용자 계정이 생성되어 ASA R2 시스템에서 사용할 수 있습니다.

관리자 계정을 만듭니다

계정 사용자가 계정에 할당된 역할에 따라 클러스터에서 특정 작업을 수행할 수 있도록 관리자 계정을 생성합니다. 계정 보안을 강화하려면 계정을 만들 때 MFA(다중 요소 인증)를 설정합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * 사용자 및 역할 * 옆에 있는 를 선택합니다 →.
3. 사용자 * 에서 을 선택합니다 + Add .
4. 사용자 이름을 입력한 다음 사용자에게 할당할 역할을 선택합니다.
5. 사용자 로그인 방법과 인증 방법을 선택합니다.
6. MFA를 활성화하려면 를 + Add 선택한 다음 보조 로그인 방법 및 인증 방법을 선택합니다
7. 사용자의 암호를 입력합니다.
8. 저장 * 을 선택합니다.

결과

새 관리자 계정이 생성되어 ASA R2 클러스터에서 사용할 수 있습니다.

ASA R2 스토리지 시스템에서 보안 인증서를 관리합니다

디지털 보안 인증서를 사용하여 원격 서버의 ID를 확인합니다.

OCSP(온라인 인증서 상태 프로토콜)는 SSL 및 TLS(전송 계층 보안) 연결을 사용하여 ONTAP 서비스에서 디지털 인증서 요청 상태를 검증합니다.

인증서 서명 요청을 생성합니다

인증서 서명 요청(CSR)을 생성하여 공용 인증서를 생성하는 데 사용할 수 있는 개인 키를 만듭니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택한 →다음 를 + Generate CSR선택합니다.
3. 주체의 일반 이름을 입력한 다음 국가를 선택합니다.
4. GSR 기본값을 변경하려면 확장 키 사용을 선택하거나 제목 대체 이름을 추가한 ↙↗ More options다음 을 선택하고 원하는 업데이트를 수행합니다.
5. Generate * 를 선택합니다.

결과

공개 인증서를 생성하는 데 사용할 수 있는 CSR을 생성했습니다.

신뢰할 수 있는 인증 기관을 추가합니다

ONTAP TLS(전송 계층 보안)를 사용하는 응용 프로그램에 대해 신뢰할 수 있는 기본 루트 인증서 집합을 제공합니다. 필요에 따라 신뢰할 수 있는 인증 기관을 추가할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 신뢰할 수 있는 인증 기관 * 을 선택합니다.
4. 인증서 세부 정보를 입력하거나 가져온 다음 을 + Add 선택합니다.

결과

신뢰할 수 있는 새 인증 기관을 ASA R2 시스템에 추가했습니다.

신뢰할 수 있는 인증 기관을 갱신하거나 삭제합니다

신뢰할 수 있는 인증 기관은 매년 갱신해야 합니다. 만료된 인증서를 갱신하지 않으려면 삭제해야 합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.

2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 신뢰할 수 있는 인증 기관 * 을 선택합니다.
4. 갱신하거나 삭제할 신뢰 인증 기관을 선택합니다.
5. 인증 기관을 갱신하거나 삭제합니다.

인증 기관을 갱신하려면 다음을 수행합니다.	인증 기관을 삭제하려면 다음을 수행합니다.
a. 을 ⋮ 선택한 다음 * 갱신 * 을 선택합니다. b. 인증서 정보를 입력하거나 가져온 다음 * 갱신 * 을 선택합니다.	a. 을 ⋮ 선택한 다음 * 삭제 * 를 선택합니다. b. 삭제를 확인한 다음 * Delete * 를 선택합니다.

결과

ASA R2 시스템에서 기존의 신뢰할 수 있는 인증 기관을 갱신하거나 삭제했습니다.

클라이언트/서버 인증서 또는 로컬 인증 기관을 추가합니다

클라이언트/서버 인증서 또는 로컬 인증 기관을 추가하여 보안 웹 서비스를 활성화합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 * 인증서 * 옆에 있는 를 선택합니다 →.
3. 클라이언트/서버 인증서 * 또는 * 로컬 인증 기관 * 을 선택합니다.
4. 인증서 정보를 추가한 다음 을 선택합니다 + Add .

결과

새 클라이언트/서버 인증서 또는 지역 기관을 ASA R2 시스템에 추가했습니다.

클라이언트/서버 인증서 또는 로컬 인증 기관을 갱신하거나 삭제합니다

클라이언트/서버 인증서 및 로컬 인증 기관은 매년 갱신해야 합니다. 만료된 인증서 또는 로컬 인증 기관을 갱신하지 않으려면 삭제해야 합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 에서 인증서 옆에 있는 를 →선택합니다.
3. 클라이언트/서버 인증서 * 또는 * 로컬 인증 기관 * 을 선택합니다.
4. 갱신 또는 삭제할 인증서를 선택합니다.
5. 인증 기관을 갱신하거나 삭제합니다.

인증 기관을 갱신하려면 다음을 수행합니다.	인증 기관을 삭제하려면 다음을 수행합니다.
a. 을 선택한 다음 * 갱신 * 을 선택합니다. b. 인증서 정보를 입력하거나 가져온 다음 * 갱신 * 을 선택합니다.	을 선택한 다음 * 삭제 * 를 선택합니다.

결과

ASA R2 시스템에서 기존 클라이언트/서버 인증서 또는 로컬 인증 기관을 갱신하거나 삭제했습니다.

ASA R2 스토리지 시스템에서 호스트 접속을 확인합니다

호스트 데이터 작업에 문제가 있는 경우 ONTAP System Manager를 사용하여 호스트에서 ASA R2 스토리지 시스템으로의 접속이 활성 상태인지 확인할 수 있습니다.

단계

1. System Manager에서 * Host * 를 선택합니다.

   호스트 접속 상태는 호스트 그룹 이름 옆에 다음과 같이 표시됩니다.

   - * OK *: 모든 이니시에이터가 두 노드에 연결되었음을 나타냅니다.
   - 부분적으로 연결됨: 초기자 중 일부가 두 노드에 연결되지 않았음을 나타냅니다.
   - **None Connected**: 연결된 이니시에이터가 없음을 나타냅니다.

다음 단계

호스트에서 업데이트를 수행하여 연결 문제를 수정합니다. ONTAP는 15분마다 연결 상태를 다시 확인합니다.

ASA R2 스토리지 시스템을 유지 관리합니다

로 이동하여 "ASA R2 유지 보수 설명서" ASA R2 시스템 구성 요소에 대한 유지 관리 절차를 수행하는 방법을 알아보십시오.

자세한 정보

ONTAP 파워 유저를 위한 ASA R2

ASA R2 시스템을 다른 ONTAP 시스템과 비교합니다

ASA r2 시스템은 모든 플래시 솔루션을 기반으로 SAN 전용 환경을 위한 하드웨어 및 소프트웨어 솔루션을 제공합니다. ASA r2 시스템은 ONTAP 특성, 스토리지 계층 및 지원 프로토콜 구현 측면에서 다른 ONTAP 시스템(ASA, AFF, FAS)과 차별화됩니다.

ASA r2 시스템으로 분류되는 것은 다음과 같습니다.

- ASA A1K 를 참조하십시오
- ASA A90 를 참조하십시오
- ASA A70 를 참조하십시오
- ASA A50
- ASA A30
- ASA A20
- ASA C30

성격 차이

ASA R2 시스템에서 ONTAP 소프트웨어가 간소화되어 필수 SAN 기능을 지원하는 동시에 SAN 관련 기능이 아닌 기능의 가시성과 가용성을 제한합니다. 예를 들어, ASA R2 시스템에서 실행되는 System Manager에는 NAS 클라이언트의 홈 디렉토리를 생성하는 옵션이 표시되지 않습니다. 이 간소화된 ONTAP 버전은 _ ASA R2 Personality _ 로 식별됩니다. ASA 시스템에서 실행되는 ONTAP는 _ ASA ONTAP Personality _ 로 식별됩니다. AFF 및 FAS ONTAP 시스템에서 실행되는 ONTAP는 _ Unified ONTAP Personality _ 로 식별됩니다. ONTAP 퍼스낼리티의 차이는 ONTAP 명령 참조(man 페이지), REST API 사양 및 해당되는 경우 EMS 메시지에서 참조된다.

ONTAP 스토리지의 특성은 System Manager 또는 ONTAP CLI에서 확인할 수 있습니다.

- System Manager 메뉴에서 * 클러스터 > 개요 * 를 선택합니다.
- CLI에서 다음을 입력하세요. `system node show -personality -is-disaggregated`

ASA r2 시스템의 경우 _개성_은 _ASA r2_이고 _is-disaggregated_의 상태는 _true_입니다.

ONTAP 스토리지 시스템의 특성은 변경할 수 없습니다.

저장 계층 차이점

ASA r2 시스템은 FAS, AFF, ASA 시스템에서 사용하는 저장 계층과 다른 단순화된 저장 계층을 사용합니다.

FAS, AFF 및 **ASA** 시스템

FAS, AFF 및 ASA 시스템의 스토리지 계층은 집계를 스토리지의 기본 단위로 사용합니다. 집계는 스토리지 시스템에서 사용 가능한 특정 디스크 집합을 소유합니다. 집계는 자신이 소유한 디스크의 공간을 LUN 및 네임스페이스 볼륨에 할당합니다. 이러한 시스템을 통해 ONTAP 사용자는 집계, 볼륨, LUN 및 네임스페이스를 생성하고 수정할 수 있습니다.

ASA r2 시스템

ASA r2 시스템의 스토리지 계층은 집계 대신 스토리지 가용성 영역(SAZ)을 사용합니다. 스토리지 가용성 영역은 단일 HA 쌍의 두 노드 모두에서 사용할 수 있는 공통 스토리지 풀입니다. HA 쌍의 두 노드는 공유 스토리지 가용성 영역의 모든 사용 가능한 디스크에 액세스할 수 있습니다. 예를 들어, 2노드 ASA r2 System ONTAP 클러스터에는 클러스터의 두 노드 모두 액세스할 수 있는 스토리지 가용성 영역이 하나 있습니다. 4노드 ASA r2 System ONTAP 클러스터에는 두 개의 스토리지 가용성 영역이 있습니다. 클러스터의 각 HA 쌍은 스토리지 가용성 영역 중 하나에 액세스할 수 있습니다.

스토리지 유닛(LUN 또는 NVMe 네임스페이스 기반)이 생성되면 ONTAP 해당 스토리지 가용 영역에 볼륨을 자동으로 생성하여 스토리지 유닛을 저장합니다. 새로 생성된 볼륨은 최적의 성능과 균형 잡힌 용량 활용을 위해 스토리지 가용 영역 내에 자동으로 배치됩니다. 스토리지 가용 영역 내에서 용량 활용률은 사용자의 ONTAP 버전에 따라 균형을 이룹니다. "ASA r2 클러스터에서 용량 균형 조정에 대해 알아보세요.".

ASA r2 시스템 차이점 요약

ASA r2 시스템은 다음과 같은 면에서 FAS, AFF, ASA 시스템과 다릅니다.

	ASA r2 를 참조하십시오	ASA	AFF	FAS
• ONTAP 성격 *	ASA r2 를 참조하십시오	ASA	통합	통합
• SAN 프로토콜 지원 *	예	예	예	예
• NAS 프로토콜 지원 *	아니요	아니요	예	예
• 스토리지 계층 지원 *	스토리지 가용 영역	애그리게이트	애그리게이트	애그리게이트

이러한 자동화되고 간소화된 스토리지 관리 방식으로 인해 ASA r2 시스템에서는 특정 System Manager 옵션, ONTAP 명령 및 REST API 엔드포인트를 사용할 수 없거나 사용이 제한됩니다. 예를 들어, ASA r2 시스템에서는 볼륨 생성 및 관리가 자동화되어 있기 때문에 System Manager에 볼륨 메뉴가 나타나지 않고 `volume create` 명령이 지원되지 않습니다. "지원되지 않는 ASA r2 명령에 대해 자세히 알아보세요" .

ONTAP CLI(Command Line Interface) 및 REST API와 관련된 ASA R2 시스템과 FAS, AFF 및 ASA 시스템의 주요 차이점은 아래에 설명되어 있습니다.

프로토콜 서비스를 사용한 기본 스토리지 VM 생성

새로운 클러스터에는 SAN 프로토콜이 활성화된 기본 데이터 저장 가상 머신(VM)이 자동으로 포함됩니다. IP 데이터 LIF는 iSCSI 및 NVMe/TCP 프로토콜을 지원하며 다음을 사용합니다. `default-data-blocks` 기본적으로 서비스 정책이 적용됩니다.

자동 볼륨 생성

스토리지 유닛(LUN 또는 네임스페이스)을 생성하면 스토리지 가용 영역에서 볼륨이 자동으로 생성됩니다. 결과적으로 공통 네임스페이스가 단순화됩니다. 스토리지 유닛을 삭제하면 연결된 볼륨이 자동으로 삭제됩니다.

씬 및 일반 프로비저닝으로 변경

스토리지 유닛은 항상 ASA R2 스토리지 시스템에서 씬 프로비저닝됩니다. 일반 프로비저닝은 지원되지 않습니다.

데이터 압축의 변경 사항

온도에 민감한 스토리지 효율성이 ASA R2 시스템에는 적용되지 않습니다. ASA R2 시스템에서 압축은 *hot*(자주 액세스하는) 데이터 또는 *cold*(자주 액세스하지 않는) 데이터를 기반으로 하지 않습니다. 데이터의 콜드 데이터가 될 때까지 기다리지 않고 압축을 시작합니다.

를 참조하십시오

- 에 대해 자세히 "ONTAP 하드웨어 시스템"알아보십시오.
- 에서 ASA 및 ASA R2 시스템에 대한 전체 구성 지원 및 제한 사항을 "NetApp Hardware Universe를 참조하십시오"참조하십시오.
- 에 대해 자세히 "NetApp ASA"알아보십시오.

ASA R2 스토리지 시스템에 대한 ONTAP 소프트웨어 지원 및 제한 사항

ASA R2 시스템은 SAN 솔루션에 대해 광범위한 지원을 제공하지만 특정 ONTAP 소프트웨어 기능은 지원되지 않습니다.

ASA R2 시스템은 다음을 지원하지 않습니다.

- 기본 자동 iSCSI LIF 페일오버

  ASA R2 시스템에서는 기본 네트워킹 LIF가 NVMe와 SCSI 호스트 간에 공유되므로 자동 페일오버를 지원하지 않습니다. 자동 iSCSI LIF 페일오버를 사용하려면 이 "iSCSI 전용 LIF를 생성합니다"필요합니다. 자동 페일오버는 기본적으로 iSCSI 전용 LIFS에서 설정됩니다.

  자동 iSCSI LIF 페일오버가 사용되도록 설정된 경우 스토리지 페일오버가 발생하면 iSCSI LIF가 홈 노드나 포트에서 HA 파트너 노드 또는 포트로 자동으로 마이그레이션된 다음, 페일오버가 완료된 후 다시 수행됩니다. 또는 iSCSI LIF의 포트가 정상 상태가 아닐 경우 LIF는 자동으로 현재 홈 노드의 정상 포트로 마이그레이션된 다음 포트가 다시 정상 상태가 되면 원래 포트로 다시 마이그레이션됩니다.

- FabricPool
- LUN 일반 프로비저닝
- MetroCluster
- 오브젝트 프로토콜
- ONTAP S3 SnapMirror 및 S3 API

ASA R2 시스템은 다음을 지원합니다.

- SnapLock

  "스냅샷을 잠그는 방법에 대해 알아봅니다" ASA R2 시스템에서.

- 이중 계층 암호화

"이중 레이어 암호화를 적용하는 방법에 대해 알아봅니다" ASA R2 시스템의 데이터로 이동합니다.

SnapMirror 복제 지원

SnapMirror 복제는 다음과 같은 제한 사항이 있는 ASA r2 시스템에서 지원됩니다.

- SnapMirror 동기 복제는 지원되지 않습니다.
- SnapMirror Active Sync는 두 개의 ASA r2 시스템 간에만 지원됩니다.

  자세히 알아보세요"ASA r2 시스템의 SnapMirror Active Sync" .

- SnapMirror 비동기 복제는 두 개의 ASA r2 시스템 간에만 지원됩니다. SnapMirror 비동기 복제는 ASA r2 시스템과 ASA, AFF 또는 FAS 시스템 또는 클라우드 사이에서는 지원되지 않습니다.

  자세히 알아보세요"ASA r2 시스템에서 지원되는 SnapMirror 복제 정책" .

를 참조하십시오

- "NetApp Hardware Universe를 참조하십시오"ASA R2 하드웨어 지원 및 제한 사항에 대한 자세한 내용은 를 참조하십시오.

ASA R2 스토리지 시스템에 대한 ONTAP CLI 지원

ASA r2 시스템의 스토리지 계층은 집계 대신 스토리지 가용성 영역(SAZ)을 사용합니다. 스토리지 가용성 영역은 단일 HA 쌍에서 사용할 수 있는 공통 스토리지 풀입니다. HA 쌍의 두 노드는 공유 스토리지 가용성 영역의 모든 사용 가능한 디스크에 액세스할 수 있습니다. 스토리지 유닛(LUN 또는 NVMe 네임스페이스)이 생성되면 ONTAP 해당 스토리지 가용성 영역에 볼륨을 자동으로 생성하여 스토리지 유닛을 저장합니다.

이러한 저장소 관리에 대한 간소화된 접근 방식으로 인해 `storage aggregate` ASA r2 시스템에서는 명령이 지원되지 않습니다. `lun` , `storage` 그리고 `volume` 명령과 매개변수도 제한적이다.

다음 명령 및 명령 세트는 R2의 ASA에서 지원되지 않습니다.

지원되지 않는 **<code> LUN </code>** 명령입니다

- `lun copy`
- `lun geometry`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  > 그만큼 `lun move-in-volume` 명령은 다음으로 대체됩니다. `lun rename` 그리고 `vserver nvme namespace rename` 명령.

- `lun transition`

지원되지 않는 **<code> storage </code>** 명령입니다

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

지원되지 않는 **<code> volume </code>** 명령 집합입니다

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

지원되지 않는 **<code> volume </code>** 명령 및 매개 변수입니다

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  그만큼 `volume modify` 다음 매개변수와 함께 사용하면 명령을 사용할 수 없습니다.

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`
- `volume mount`

- volume move
- volume offline
- volume rehost
- volume rename
- volume restrict
- volume transition-prepare-to-downgrade
- volume unmount

지원되지 않는 **<code>** 볼륨 클론 **</code>** 명령입니다

- volume clone create
- volume clone split

지원되지 않는 **<code> volume SnapLock </code>** 명령입니다

- volume snaplock modify

지원되지 않는 **<code>** 볼륨 스냅샷 **</code>** 명령입니다

- volume snapshot
- volume snapshot autodelete modify
- volume snapshot policy modify

를 참조하십시오

"ONTAP 명령 참조입니다"지원되는 명령의 전체 목록은 를 참조하십시오

CLI를 사용하여 ONTAP ASA R2 클러스터를 설정합니다

권장 "System Manager를 사용하여 ONTAP ASA R2 클러스터를 설정합니다"사항입니다. System Manager는 클러스터를 설정하고 실행하는 데 도움이 되는 빠르고 쉬운 워크플로우를 제공합니다. 하지만 ONTAP 명령 작업에 익숙한 경우 선택적으로 ONTAP CLI(Command Line Interface)를 사용하여 클러스터 설정을 할 수 있습니다. CLI를 사용하여 클러스터를 설정하면 System Manager를 사용하여 설정하는 것보다 더 많은 옵션이나 이점이 없습니다.

클러스터 설정 중에 기본 데이터 스토리지 가상 머신(VM)이 생성되고 초기 스토리지 유닛이 생성되며 데이터 LIF가 자동으로 검색됩니다. 필요에 따라 DNS(Domain Name System)를 활성화하여 호스트 이름을 확인하고, 시간 동기화에 NTS(Network Time Protocol)를 사용하도록 클러스터를 설정하고, 저장된 데이터의 암호화를 활성화할 수 있습니다.

시작하기 전에

다음 정보를 수집합니다.

- 클러스터 관리 IP 주소입니다

클러스터 관리 IP 주소는 클러스터 관리자가 관리 스토리지 VM에 액세스하고 클러스터를 관리하는 데 사용하는 클러스터 관리 인터페이스에 대한 고유한 IPv4 주소입니다. 조직의 IP 주소 할당 담당자로부터 이 IP 주소를 얻을 수 있습니다.

- 네트워크 서브넷 마스크

  클러스터 설정 중에 ONTAP은 해당 구성에 적합한 네트워크 인터페이스 세트를 권장합니다. 필요한 경우 권장 사항을 조정할 수 있습니다.

- 네트워크 게이트웨이 IP 주소입니다
- 파트너 노드 IP 주소입니다
- DNS 도메인 이름입니다
- DNS 이름 서버 IP 주소입니다
- NTP 서버 IP 주소입니다
- 데이터 서브넷 마스크

단계

1. HA Pair의 두 노드 전원을 켭니다.
2. 로컬 네트워크에서 검색된 노드를 표시합니다.

```
system node show-discovered -is-in-cluster false
```

3. 클러스터 설정 마법사를 시작합니다.

```
cluster setup
```

4. AutoSupport 설명을 확인합니다.
5. 노드 관리 인터페이스 포트, IP 주소, 넷마스크 및 기본 게이트웨이의 값을 입력합니다.
6. 명령줄 인터페이스를 사용하여 설치를 계속하려면 * Enter * 를 누른 다음 * create * 를 입력하여 새 클러스터를 생성합니다.
7. 시스템 기본값을 그대로 사용하거나 값을 직접 입력합니다.
8. 첫 번째 노드에서 설정이 완료되면 클러스터에 로그인합니다.
9. 클러스터가 활성 상태이고 첫 번째 노드가 정상 상태인지 확인합니다.

```
system node show-discovered
```

10. 두 번째 노드를 클러스터에 추가합니다.

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. 필요한 경우 클러스터 전체의 시스템 시간을 동기화합니다

대칭 인증 없이 동기화합니다	`cluster time-service ntp server create -server <server_name>`
대칭 인증과 동기화합니다	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. 클러스터가 NTP 서버와 연결되어 있는지 확인합니다.

```
Cluster time-service ntp show
```

12. 필요한 경우 를 다운로드하고 "ActiveIQ Config Advisor"실행하여 구성을 확인합니다.

다음 단계

"데이터 액세스를 설정합니다"SAN 클라이언트에서 시스템으로 전환할 준비가 되었습니다.

ASA R2에 대한 REST API 지원

ASA R2 REST API는 통합된 ONTAP 퍼스낼리티와 함께 제공되는 REST API를 기반으로 하며, ASA R2 퍼스낼리티의 고유한 특성과 기능에 맞게 많은 변경이 적용되었습니다.

API 변경 유형

ASA R2 시스템 REST API와 FAS, AFF 및 ASA 시스템에서 사용할 수 있는 유니파이드 ONTAP REST API 간에는 여러 가지 차이점이 있습니다. 변경 유형을 이해하면 온라인 API 참조 문서를 보다 잘 활용할 수 있습니다.

새로운 **ASA R2** 엔드포인트는 유니파이드 **ONTAP**에서 지원되지 않습니다

유니파이드 ONTAP에서는 사용할 수 없는 ASA R2 REST API에 여러 엔드포인트가 추가되었습니다.

예를 들어, 새로운 블록 볼륨 엔드포인트가 ASA R2 시스템용 REST API에 추가되었습니다. 블록 볼륨 엔드포인트는 LUN 및 NVMe 네임스페이스 개체에 대한 액세스를 제공하여 리소스를 종합적으로 볼 수 있도록 지원합니다. REST API를 통해서만 사용할 수 있습니다.

또 다른 예로, * storage-units * 엔드포인트는 LUN 및 NVMe 네임스페이스를 집계한 보기로 제공합니다. 여러 개의 끝점이 있으며 모두 기반으로 하거나 에서 파생됩니다. `/api/storage/storage-units` `/api/storage/luns`및 도 검토해야 `/api/storage/namespaces` 합니다.

일부 끝점에 사용되는 **HTTP** 메서드에 대한 제한 사항

ASA R2에서 사용할 수 있는 여러 끝점에는 Unified ONTAP와 비교하여 사용할 수 있는 HTTP 메서드가 제한되어 있습니다. 예를 들어, `/api/protocols/nvme/services` ASA R2 시스템에서 엔드포인트를 사용할 때는 POST

및 DELETE가 허용되지 않습니다.

끝점 및 **HTTP** 메서드에 대한 속성 변경

일부 ASA R2 시스템 끝점 및 메서드 조합은 통합 ONTAP 속성에서 사용할 수 있는 정의된 모든 속성을 지원하지 않습니다. 예를 들어, 끝점에서 패치를 사용하는 경우 `/api/storage/volumes/{uuid}` ASA R2에서는 다음을 비롯한 몇 가지 속성이 지원되지 않습니다.

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

내부 처리의 변경

ASA R2가 특정 REST API 요청을 처리하는 방법은 몇 가지 변경되었습니다. 예를 들어, 끝점이 있는 삭제 요청은 `/api/storage/luns/{uuid}` 비동기적으로 처리됩니다.

OAuth 2.0으로 보안 강화

OAuth 2.0은 업계 표준 인증 프레임워크입니다. 서명된 액세스 토큰을 기반으로 보호된 리소스에 대한 액세스를 제한하고 제어하는 데 사용됩니다. System Manager를 사용하여 OAuth 2.0을 구성하여 ASA R2 시스템 리소스를 보호할 수 있습니다.

System Manager로 OAuth 2.0을 설정한 후 REST API 클라이언트의 액세스를 제어할 수 있습니다. 먼저 인증 서버에서 액세스 토큰을 얻어야 합니다. 그런 다음 REST 클라이언트는 HTTP 승인 요청 헤더를 사용하여 토큰을 ASA R2 클러스터에 베어러 토큰으로 전달합니다. 자세한 내용은 을 "OAuth 2.0을 사용한 인증 및 권한 부여" 참조하십시오.

Swagger UI를 통해 **ASA R2 API** 참조 문서에 액세스합니다

ASA R2 시스템에서 Swagger UI를 통해 REST API 참조 문서에 액세스할 수 있습니다.

이 작업에 대해

REST API에 대한 자세한 내용은 ASA R2 참조 문서 페이지에 액세스해야 합니다. 이 과정에서 문자열 * 플랫폼 사양 * 을 검색하여 API 호출 및 속성에 대한 ASA R2 시스템 지원에 대한 세부 정보를 찾을 수 있습니다.

시작하기 전에

다음 항목이 있어야 합니다.

- ASA R2 시스템의 클러스터 관리 LIF의 IP 주소 또는 호스트 이름입니다
- REST API 액세스 권한이 있는 계정의 사용자 이름 및 암호

단계

1. 브라우저에 URL을 입력하고 * Enter *:+를 누릅니다
   `https://<ip_address>/docs/api`
2. 관리자 계정을 사용하여 로그인합니다.

   ASA R2 API 설명서 페이지는 주요 리소스 범주로 구성된 API 호출과 함께 표시됩니다.
3. ASA R2 시스템에만 해당되는 API 호출 예를 보려면 * SAN * 범주로 스크롤한 다음 * Get/storage/storage-units * 를 클릭합니다.

ASA r2 시스템에서 지원되는 일반적인 ONTAP 기능

ASA r2 시스템은 간소화된 버전의 ONTAP 실행하므로 일반적인 ONTAP 작업과 시스템 관리자 기능은 ASA r2 시스템에서 다른 ONTAP 시스템과 동일한 방식으로 수행됩니다.

일반적인 특징과 기능에 대한 자세한 내용은 다음 ONTAP 설명서를 참조하세요.

데이터 보호

ASA r2 시스템에서 지원되는 일반적인 데이터 보호 기능에 대해 자세히 알아보세요.

클러스터링된 외부 키 서버

스토리지 VM에서 클러스터링된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 클러스터형 키 서버를 사용하면 스토리지 VM에서 기본 키 서버와 보조 키 서버를 지정할 수 있습니다. ONTAP 키를 등록할 때 먼저 기본 키 서버에 액세스를 시도한 후 작업이 성공적으로 완료될 때까지 순차적으로 보조 서버에 액세스를 시도하여 키 중복을 방지합니다.

"클러스터형 외부 키 서버를 구성하는 방법을 알아보세요".

휴면 암호화를 위한 외부 키 관리

하나 이상의 KMIP 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다.

- "외부 키 관리 활성화".
- "외부 키 관리(NVE) 활성화" .

데이터 보안

ASA r2 시스템에서 지원되는 일반적인 데이터 보안 기능에 대해 자세히 알아보세요.

관리자 액세스 관리

관리자에게 할당된 역할에 따라 관리자가 수행할 수 있는 기능이 결정됩니다. System Manager는 클러스터 관리자와 스토리지 VM 관리자를 위한 미리 정의된 역할을 제공합니다. 관리자 계정을 생성할 때 역할을 할당하거나 나중에 다른 역할을 할당할 수 있습니다.

- "System Manager를 사용하여 관리자 액세스를 관리하는 방법을 알아보세요.".

클라이언트 인증 및 권한 부여

ONTAP 표준 방법을 사용하여 클라이언트와 관리자가 저장소에 액세스하는 것을 보호하고 바이러스로부터 보호합니다. 저장 중인 데이터의 암호화와 WORM 저장을 위해 고급 기술을 사용할 수 있습니다. ONTAP 신뢰할 수 있는 출처를 통해 클라이언트 컴퓨터와 사용자의 신원을 검증하여 인증합니다. ONTAP 사용자의 자격 증명을 파일이나 디렉토리에 구성된 권한과 비교하여 사용자가 파일이나 디렉토리에 액세스할 수 있도록 권한을 부여합니다.

"클라이언트 인증 및 권한 부여에 대해 알아보세요" .

OAuth 2.0 인증

OAuth 2.0(Open Authorization) 프레임워크를 사용하여 ONTAP 클러스터에 대한 액세스를 제어할 수 있습니다. OAuth 2.0은 서명된 액세스 토큰을 사용하여 보호된 리소스에 대한 액세스를 제한하고 제어합니다.

"OAuth 2.0 인증에 대해 알아보세요" .

SAML 인증 및 관리자 액세스

웹 서비스에 대한 SAML(Security Assertion Markup Language) 인증을 구성하고 활성화할 수 있습니다. SAML은 Active Directory 및 LDAP와 같은 디렉터리 서비스 공급자 대신 외부 ID 공급자(IdP)를 통해 사용자를 인증합니다.

"SAML 인증 구성 방법 알아보기" .

네트워킹

ASA r2 시스템에서 지원되는 일반적인 네트워킹 기능에 대해 자세히 알아보세요.

FIPS 준수

ONTAP 모든 SSL 연결에 대해 연방 정보 처리 표준(FIPS) 140-2를 준수합니다. ONTAP 내에서 SSL FIPS 모드를 켜고 끌 수 있고, SSL 프로토콜을 전역적으로 설정하고, RC4와 같은 취약한 암호를 끌 수 있습니다.

ONTAP 9.18.1부터 SSL에 대한 포스트퀀텀 컴퓨팅 암호화 알고리즘이 지원됩니다. 이러한 알고리즘은 미래의 양자 컴퓨팅 공격에 대한 추가적인 보호 기능을 제공하며, SSL FIPS 모드가 비활성화된 경우 사용할 수 있습니다.

- "모든 SSL 연결에 대한 FIPS를 구성하는 방법을 알아보세요".

링크 집계 그룹**(LAG)**

인터페이스 그룹은 링크 집계 그룹(LAG)이라고도 하며, 동일한 노드에 있는 두 개 이상의 물리적 포트를 단일 논리적 포트로 결합하여 생성됩니다. 논리적 포트는 복원력, 가용성, 부하 공유를 향상시킵니다.

"링크 집계 그룹에 대해 알아보기".

SAN 프로토콜

ASA r2 시스템은 모든 SAN 프로토콜(iSCSI, FC, NVMe/FC, NVMe/TCP)을 지원합니다.

- "iSCSI 프로토콜에 대해 자세히 알아보세요".
- "FC(Fibre Channel) 프로토콜에 대해 자세히 알아보세요".
- "NVMe 프로토콜에 대해 알아보세요".
  - "NVMe 복사 오프로드를 구성하는 방법을 알아보세요".

    ONTAP 9.18.1부터 NVMe 복사 오프로드가 지원됩니다. NVMe 복사 오프로드를 사용하면 NVMe 호스트가 CPU에서 ONTAP 스토리지 컨트롤러의 CPU로 복사 작업을 오프로드할 수 있습니다. 호스트는 애플리케이션 워크로드를 위해 CPU 리소스를 예약하는 동시에 한 NVMe 네임스페이스에서 다른 네임스페이스로 데이터를 복사할 수 있습니다.

  - "NVMe에 대한 공간 할당(맵 해제)에 대해 자세히 알아보세요.".

ONTAP 9.16.1부터 NVMe 네임스페이스에 대한 공간 할당 해제(일명 "홀 펀칭" 및 "언맵"이라고도 함)가 기본적으로 활성화됩니다. 공간 할당 해제를 통해 호스트는 네임스페이스에서 사용되지 않은 블록을 할당 해제하여 공간을 회수할 수 있습니다.

시스템 관리자

시스템 관리자에서 다양한 작업, 개체 및 정보 항목을 검색할 수 있습니다. 특정 항목에 대한 테이블 데이터를 검색할 수도 있습니다.

"시스템 관리자에서 정보를 검색, 필터링 및 정렬하는 방법을 알아보세요.".

도움을 받으십시오

ASA R2 스토리지 시스템에서 AutoSupport를 관리합니다

AutoSupport는 시스템의 상태를 능동적으로 모니터링하고 NetApp 기술 지원, 내부 지원 조직 및 지원 파트너에게 메시지를 자동으로 보내는 메커니즘입니다.

클러스터를 설정할 때 기술 지원에 대한 AutoSupport 메시지는 기본적으로 사용하도록 설정됩니다. 내부 지원 조직에 메시지를 보내려면 올바른 옵션을 설정하고 유효한 메일 호스트가 있어야 합니다. ONTAP는 AutoSupport 메시지를 사용하도록 설정한 후 24시간 후에 보내기 시작합니다.

시작하기 전에

AutoSupport를 관리하려면 클러스터 관리자여야 합니다.

AutoSupport 연결을 테스트합니다

클러스터를 설정한 후에는 AutoSupport 연결을 테스트하여 AutoSupport에서 생성된 메시지를 기술 지원 부서에서 수신하는지 확인해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 옆에 있는 * ⋮ Test connectivity * 를 선택합니다.
3. AutoSupport 메시지의 제목을 입력한 다음 * Send test AutoSupport message * 를 선택합니다.

다음 단계

귀하는 기술 지원 부서에서 ASA R2 시스템으로부터 AutoSupport 메시지를 수신하여 문제가 발생할 경우 도움을 주는 데 필요한 데이터를 확보할 수 있음을 확인했습니다.

AutoSupport 받는 사람을 추가합니다

내부 지원 조직의 구성원을 AutoSupport 메시지를 받는 전자 메일 주소 목록에 추가합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 옆에 있는 * ⋮ 추가 옵션 * 을 선택합니다.
3. 이메일 * 옆에 있는 을 선택한  다음 을 + Add 선택합니다.
4. 받는 사람의 전자 메일 주소를 입력한 다음 받는 사람 범주를 입력합니다.

   파트너의 경우 받는 사람 범주에 * Partner * 를 선택합니다. 내부 지원 조직의 구성원에 대해서는 * 일반 * 을 선택하십시오.

5. 저장 을 선택합니다.

다음 단계

추가한 전자 메일 주소는 특정 받는 사람 범주에 대한 새 AutoSupport 메시지를 받게 됩니다.

AutoSupport 데이터를 전송합니다

ASA R2 시스템에서 문제가 발생할 경우 AutoSupport 데이터는 문제를 식별하고 해결하는 데 걸리는 시간을 크게 줄일 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 옆에 있는 을 선택한 ⋮ 다음 * Generate and send * 를 선택합니다.
3. AutoSupport 메시지의 제목을 입력한 다음 * 보내기 * 를 선택합니다.

다음 단계

귀하의 AutoSupport 데이터는 기술 지원으로 전송됩니다.

지원 케이스 생성을 억제합니다

ASA R2 시스템에서 업그레이드 또는 유지 관리를 수행하는 경우 업그레이드 또는 유지 관리가 완료될 때까지 AutoSupport 지원 케이스를 생성하지 않을 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 옆에 있는 * 를 선택한 ⋮ 다음 * 지원 케이스 생성 기능 억제 * 를 선택합니다.
3. 지원 케이스 생성을 억제할 시간을 지정한 다음, 케이스 생성을 원하지 않는 노드를 선택합니다.
4. 보내기 * 를 선택합니다.

다음 단계

지정한 시간 동안에는 AutoSupport 케이스가 생성되지 않습니다. 지정된 시간이 만료되기 전에 업그레이드 또는 유지 관리를 완료한 경우 지원 케이스 생성을 즉시 재개해야 합니다.

지원 케이스 생성을 재개합니다

업그레이드 또는 유지 관리 창에서 지원 케이스 생성을 제한한 경우, 업그레이드 또는 유지 관리가 완료된 직후 지원 케이스 생성을 재개해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 옆에 있는 * 를 선택한 ⋮ 다음 * 지원 케이스 생성 재개 * 를 선택합니다.
3. 생성된 AutoSupport 케이스를 재개할 노드를 선택합니다.
4. 보내기 * 를 선택합니다.

결과

AutoSupport 케이스는 필요에 따라 ASA R2 시스템에 대해 자동 생성됩니다.

ASA R2 스토리지 시스템에 대한 지원 사례를 제출하고 확인합니다

도움이 필요한 문제가 있는 경우 ONTAP System Manager를 사용하여 기술 지원 부서에

케이스를 제출할 수 있습니다. ONTAP System Manager를 사용하여 종료되었거나 진행 중인 케이스를 볼 수도 있습니다.

"Active IQ에 등록되었습니다" ASA r2 시스템에 대한 지원 사례를 보려면 권한이 있어야 합니다.

단계

1. 지원 케이스를 제출하려면 System Manager에서 * 클러스터 > 지원 * 을 선택한 다음 * NetApp 지원 * 으로 이동 * 을 선택합니다.
2. 이전에 제출한 케이스를 보려면 System Manager에서 * 클러스터 > 지원 * 을 선택한 다음 * 내 케이스 보기 * 를 선택합니다.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

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

상표

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

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

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

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

개인 정보 보호 정책

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

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

ONTAP

"ONTAP 9.16.1 참고 사항"