ASA r2 설명서

ASA r2

NetApp
September 26, 2024

목차

ASA r2 설명서

릴리스 정보

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.

플랫폼

업데이트	설명
구입하십시오	다음과 같은 새로운 NetApp ASA R2 시스템을 사용할 수 있습니다. 이러한 플랫폼은 SAN 전용 고객의 요구사항에 맞게 간소화된 환경을 제공하는 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.

시작하십시오

ASA R2 스토리지 시스템에 대해 알아보십시오

새로운 NetApp ASA R2 시스템(ASA A1K, ASA A70 및 ASA A90)은 SAN 전용 고객의 요구 사항에 맞는 간소화된 환경을 제공하는 통합된 하드웨어 및 소프트웨어 솔루션을 제공합니다.

ASA R2 시스템은 단일 HA 쌍 구축에서 모든 SAN 프로토콜(iSCSI, FC, NVMe/FC, NVMe/TCP)을 지원합니다. SCSI(iSCSI 및 FC) 프로토콜은 호스트와 스토리지 간의 모든 경로가 액티브/최적화되도록 다중 경로를 위해 대칭 액티브-액티브 아키텍처를 사용합니다. NVMe 프로토콜은 호스트와 스토리지 간의 직접 경로를 지원합니다.

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 스토리지 유닛 및 정합성 보장 그룹을 사용하여 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 개별적으로 백업하는 대신 정합성 보장 그룹을 백업하여 전체 데이터베이스를 보호할 수 있습니다.

도난 또는 랜섬웨어와 같은 악의적인 공격으로부터 데이터를 보호하기 위해 ASA R2 시스템은 온보드 키 관리자, 이중 계층 암호화, 무단 변경 방지 스냅샷, 다중 요소 인증 및 다중 관리자 검증을 지원합니다.

ASA R2 시스템은 기존 ASA, AFF 또는 FAS 시스템과의 혼합을 지원하지 않습니다.

를 참조하십시오

- ASA R2 시스템 지원 및 제한 사항에 대한 자세한 내용은 을 "NetApp Hardware Universe를 참조하십시오 "참조하십시오.
- 에 대해 자세히 "새로운 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.

하드웨어를 설치하고 설정합니다

"설치 및 설정" ASA R2 시스템을 ONTAP 환경에서 HA 페어로 구축할 수 있습니다.

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
- NS224 스토리지 쉘프 ID를 설정하기 위한 종이 클립 또는 끝이 뾰족한 볼펜
- Phillips #2 드라이버

인양 주의 사항

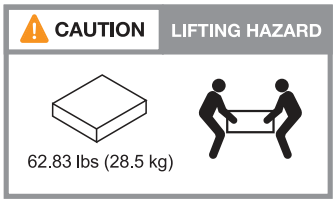
ASA R2 스토리지 시스템과 NS224 스토리지 쉘프는 무겁습니다. 이러한 품목을 들어 올리거나 이동할 때는 주의를 기울이십시오.

스토리지 시스템 중량

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

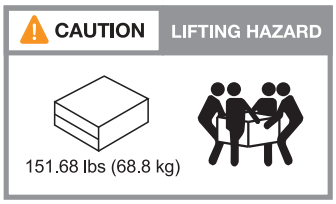
ASA A1K 를 참조하십시오

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



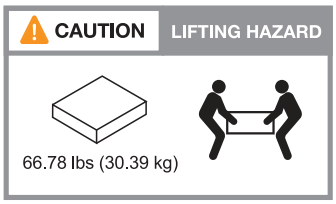
ASA A70 및 **ASA A90**

ASA A70 스토리지 시스템 또는 ASA A90 스토리지 시스템의 무게는 최대 68.8kg(151.68파운드)입니다. 시스템을 인양하려면 4명 또는 유압 리프트를 사용합니다.



보관 선반 무게

NS224 보관 선반은 무게가 최대 30.29kg(66.78lbs)입니다. 보관 선반을 들어 올리려면 두 사람이 함께 있거나 유압식 리프트를 사용하십시오. 선반 무게의 균형을 잃지 않도록 모든 구성 요소를 보관 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" 사이트가 ASA R2 스토리지 시스템의 환경 및 전기 요구 사항을 충족하는지 확인합니다.
2. 충분한 랙 공간이 있는지 확인합니다.
   - 스토리지 시스템용 HA 구성의 4U입니다
   - NS224 스토리지 쉘프당 2U
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.

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

   다음 항목은 상자에 표시될 수 있는 내용 중 일부입니다.

   상자에 들어 있는 모든 항목이 포장 명세서의 목록과 일치하는지 확인합니다. 불일치 사항이 있는 경우 추가 조치를 위해 메모하십시오.

* 하드웨어 *	* 케이블 *	
• 베젤 • 케이블 관리 장치 • 수행할 수 있습니다 • 지침이 포함된 레일 키트(옵션) • 스토리지 쉘프	• 관리 이더넷 케이블(RJ-45 케이블) • 네트워크 케이블 • 전원 코드 • 스토리지 케이블(추가 스토리지를 주문한 경우) • USB-C 직렬 포트 케이블	

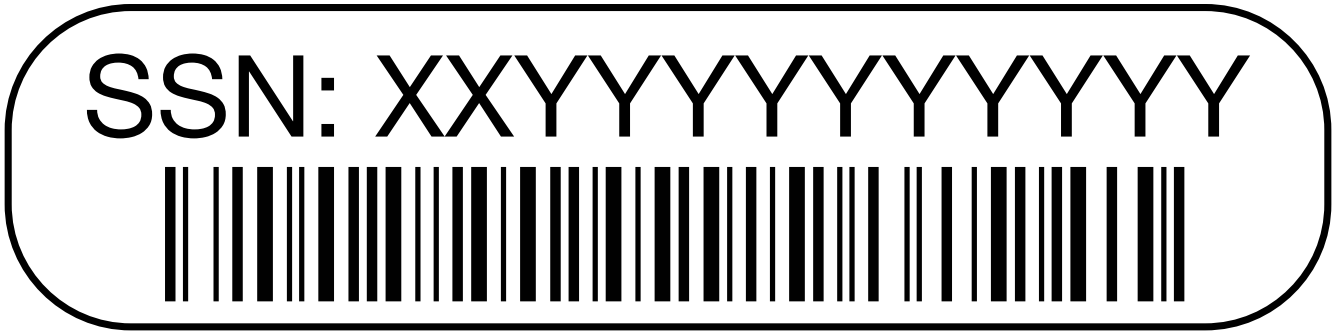
3단계**:** 스토리지 시스템을 등록합니다

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.

   포장 명세서, 확인 이메일 또는 컨트롤러의 시스템 관리 모듈에서 포장을 푼 후 번호를 찾을 수 있습니다.



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. 그렇지 않은 경우 새 NetApp 고객에 대한 지침을 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. 함께 제공된 장착 나사를 사용하여 저장 장치 시스템을 캐비닛이나 텔코 랙에 고정합니다.

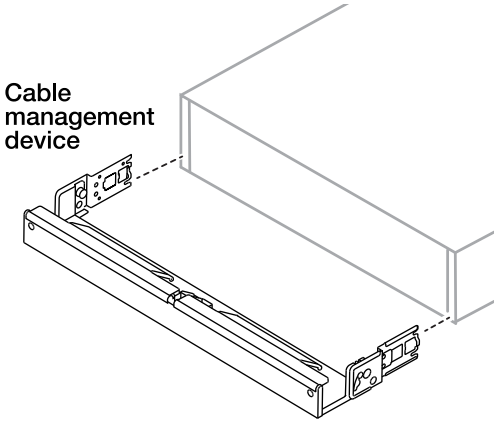
3. 스토리지 쉘프를 설치합니다.

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.

4. 케이블 관리 장치를 기억 장치 시스템 후면에 연결하십시오.



5. 베젤을 스토리지 시스템의 전면에 장착합니다.

다음 단계

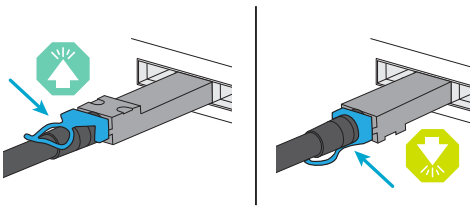
ASA R2 시스템용 하드웨어를 설치한 후에는"ASA R2 시스템의 컨트롤러와 스토리지 쉘프를 케이블로 연결합니다"

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

케이블 커넥터의 당김 탭 방향이 올바른지 케이블 다이어그램의 그림 화살표를 확인합니다.



- 커넥터를 삽입할 때 딸깍 소리가 들려야 합니다. 딸깍 소리가 느껴지지 않으면 커넥터를 분리하고 케이블 헤드를 뒤집은 다음 다시 시도하십시오.
- 광 스위치에 연결하는 경우 포트에 케이블을 연결하기 전에 SFP(Small Form-Factor Pluggable) 트랜시버를 컨트롤러 포트에 삽입합니다.

1단계**:** 스토리지 컨트롤러를 네트워크에 연결합니다

컨트롤러를 서로 또는 호스트 네트워크에 직접 연결합니다.

시작하기 전에

스토리지 시스템을 호스트 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.

ASA A1K 를 참조하십시오

스토리지 컨트롤러를 서로 연결하여 ONTAP 클러스터 연결을 생성한 다음, 각 컨트롤러의 이더넷 포트를 호스트 네트워크에 연결합니다.

단계

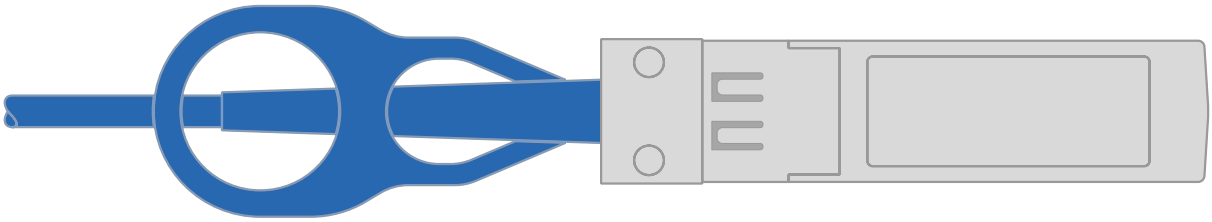
1. 클러스터/HA 인터커넥트 케이블을 사용하여 포트 E1A에 E1A를 연결하고 포트 e7a에 e7a를 연결합니다.

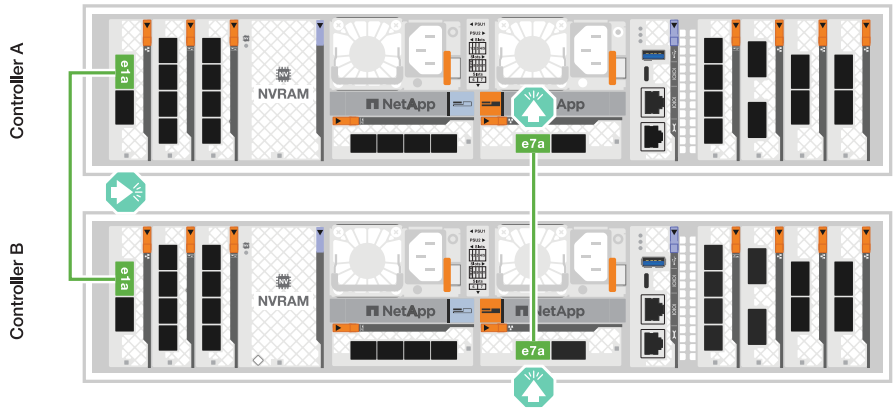
   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트를 공유합니다.

   a. 컨트롤러 A의 포트 E1A를 컨트롤러 B의 포트 E1A에 연결합니다

   b. 컨트롤러 A의 포트 e7a를 컨트롤러 B의 포트 E1A에 연결합니다

   - 클러스터/HA 인터커넥트 케이블 *





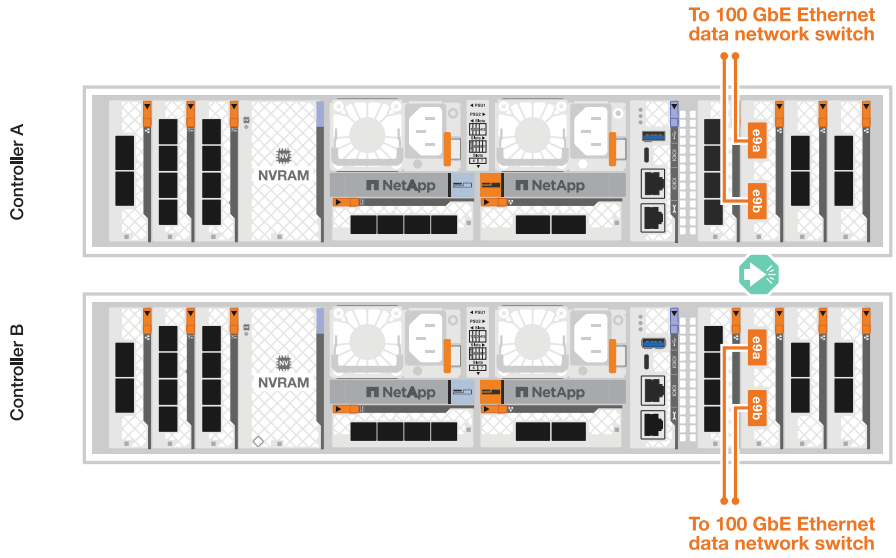
2. 이더넷 모듈 포트를 호스트 네트워크에 연결합니다.

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

   a. 그림과 같이 이더넷 데이터 네트워크 스위치에 e9a 및 e9b 포트를 연결합니다.

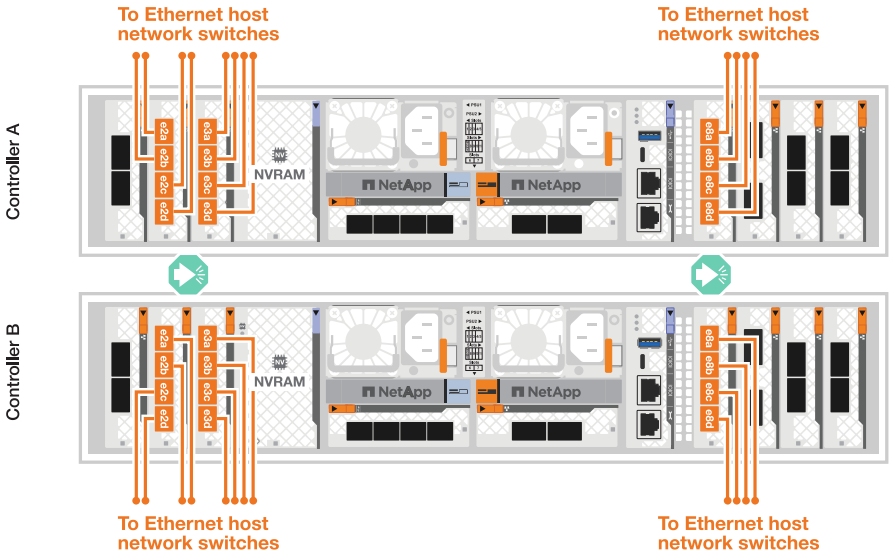
   클러스터 및 HA 트래픽에 시스템 성능을 극대화하려면 호스트 네트워크 연결에 포트 e1b 및 e7b 포트를 사용하지 마십시오. 성능을 최대화하려면 별도의 호스트 카드를 사용하십시오.

   - 100 GbE 케이블 *



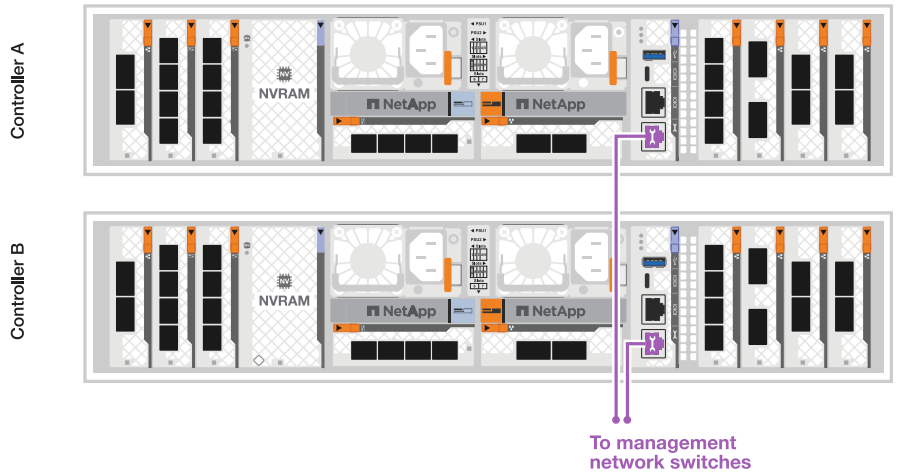
b. 10/25 GbE 호스트 네트워크 스위치를 연결합니다.

- 10/25GbE 호스트 *



3. 1000BASE-T RJ-45 케이블을 사용하여 컨트롤러 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

◦ 1000BASE-T RJ-45 케이블 *



아직 전원 코드를 연결하지 마십시오.

ASA A70 및 **ASA A90**

스토리지 컨트롤러를 서로 연결하여 ONTAP 클러스터 연결을 생성한 다음, 각 컨트롤러의 이더넷 포트를 호스트 네트워크에 연결합니다.

단계

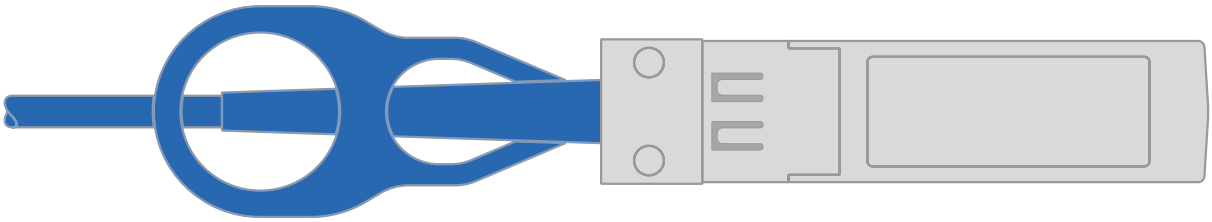
1. 클러스터/HA 인터커넥트 케이블을 사용하여 포트 E1A에 E1A를 연결하고 포트 e7a에 e7a를 연결합니다.

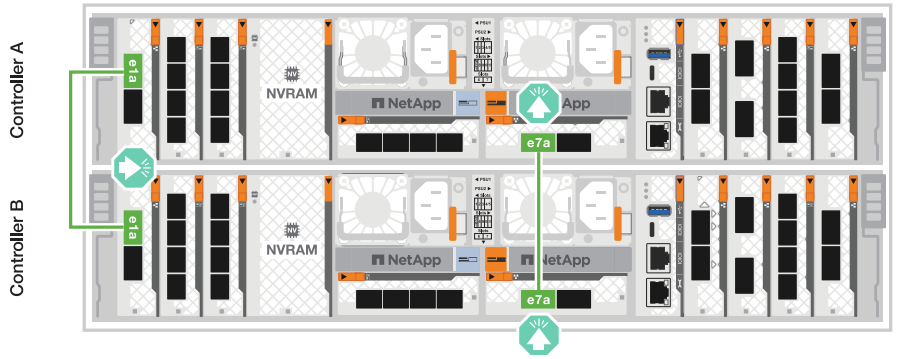
   클러스터 인터커넥트 트래픽과 HA 트래픽은 동일한 물리적 포트를 공유합니다.

   a. 컨트롤러 A의 포트 E1A를 컨트롤러 B의 포트 E1A에 연결합니다

   b. 컨트롤러 A의 포트 e7a를 컨트롤러 B의 포트 E1A에 연결합니다

   - 클러스터/HA 인터커넥트 케이블 *





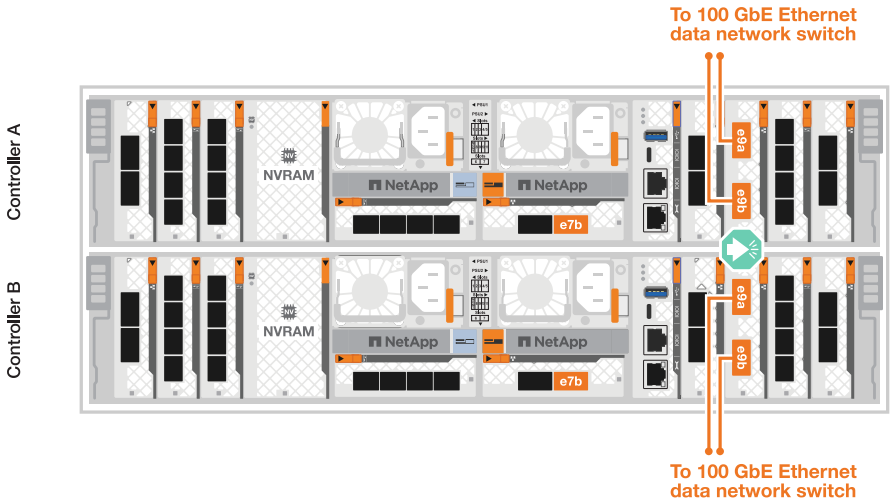
2. 이더넷 모듈 포트를 호스트 네트워크에 연결합니다.

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

a. 그림과 같이 이더넷 데이터 네트워크 스위치에 e9a 및 e9b 포트를 연결합니다.

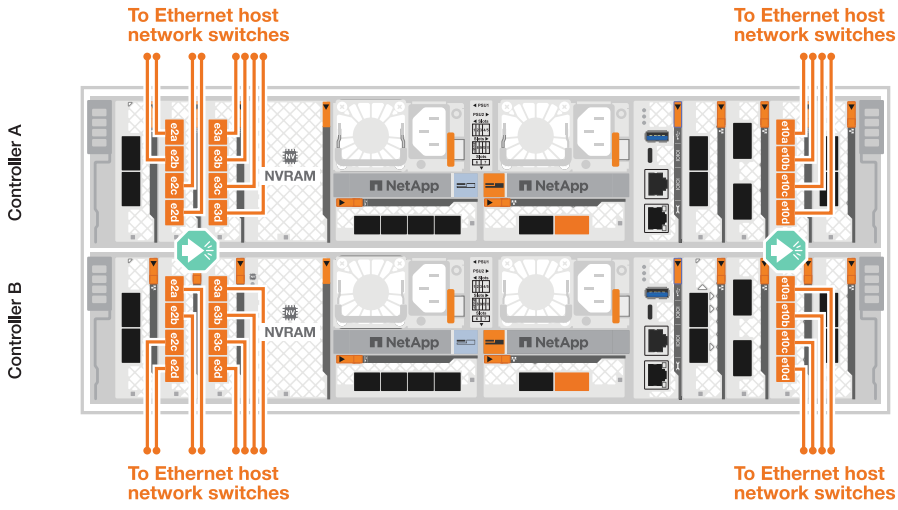
> 클러스터 및 HA 트래픽에 시스템 성능을 극대화하려면 호스트 네트워크 연결에 포트 e1b 및 e7b 포트를 사용하지 마십시오. 성능을 최대화하려면 별도의 호스트 카드를 사용하십시오.

- 100 GbE 케이블 *



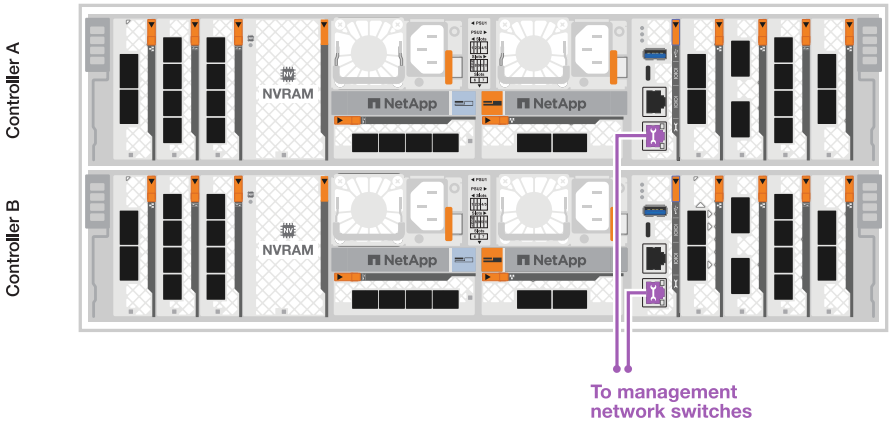
b. 10/25 GbE 호스트 네트워크 스위치를 연결합니다.

- 4포트, 10/25 GbE 호스트 *



3. 1000BASE-T RJ-45 케이블을 사용하여 컨트롤러 관리(렌치) 포트를 관리 네트워크 스위치에 연결합니다.

◦ 1000BASE-T RJ-45 케이블 *



아직 전원 코드를 연결하지 마십시오.

2단계**:** 스토리지 컨트롤러를 스토리지 쉘프에 연결합니다

다음 케이블 연결 절차는 컨트롤러를 1개 쉘프 및 2개 쉘프에 연결하는 방법을 보여줍니다. 최대 4개의 쉘프를 컨트롤러에 직접 연결할 수 있습니다.

ASA A1K 를 참조하십시오

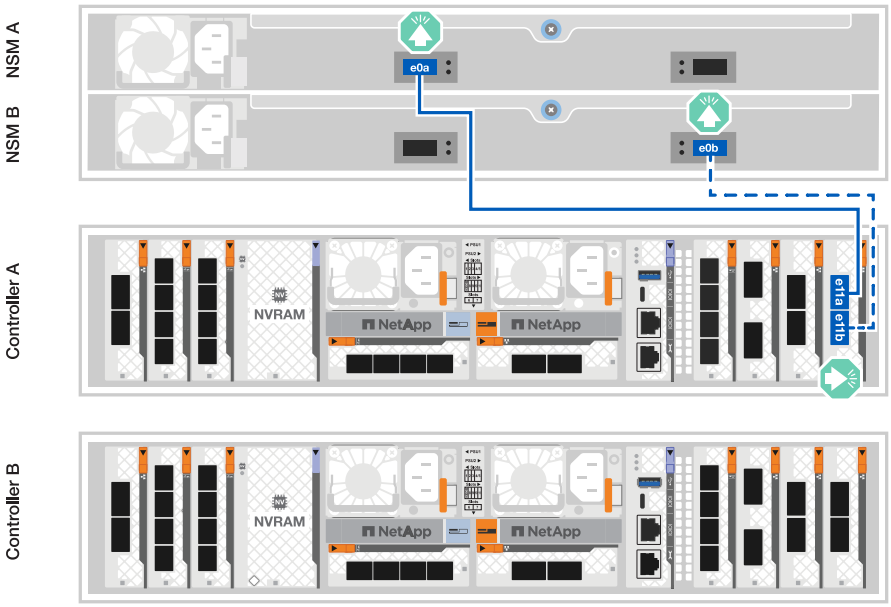
설정에 맞는 다음 케이블 연결 옵션 중 하나를 선택합니다.

옵션 **1:** 컨트롤러를 **NS224** 스토리지 쉘프 **1**개에 연결합니다

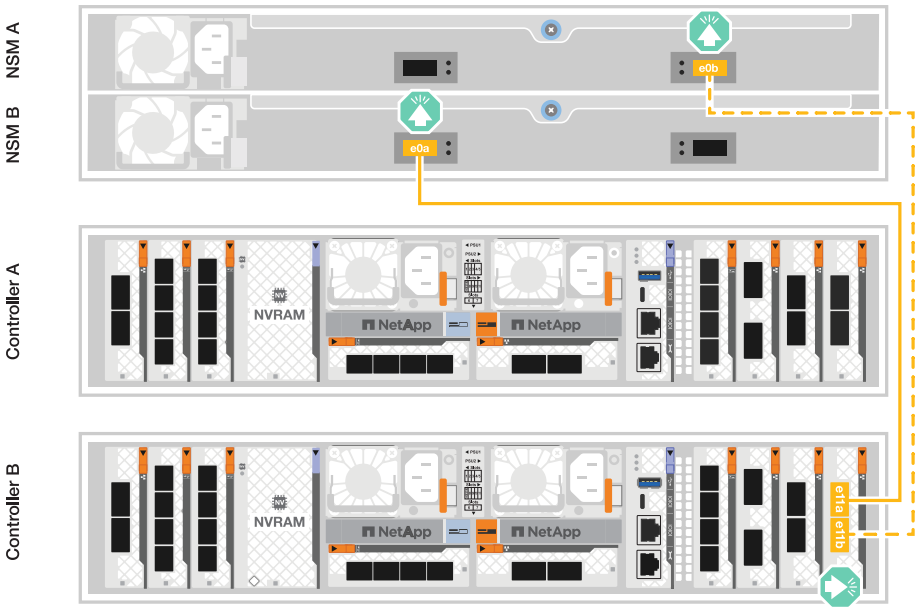
각 컨트롤러를 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

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.

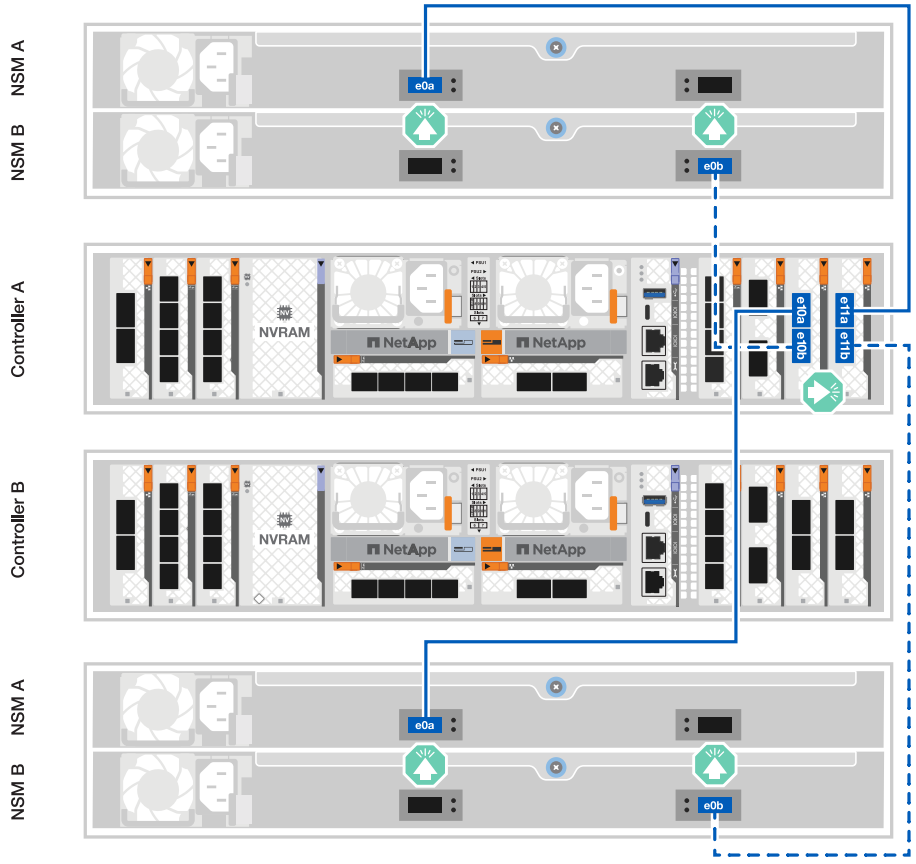


옵션 **2:** 컨트롤러를 **NS224** 스토리지 쉘프 **2**개에 연결합니다

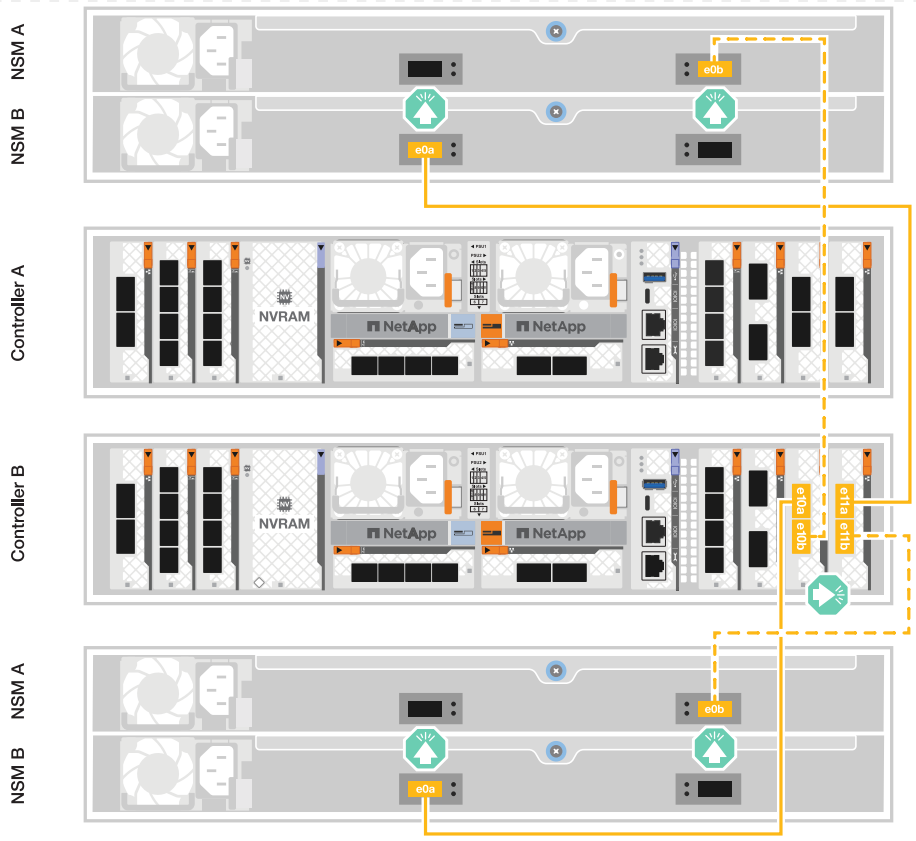
각 컨트롤러를 두 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

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.



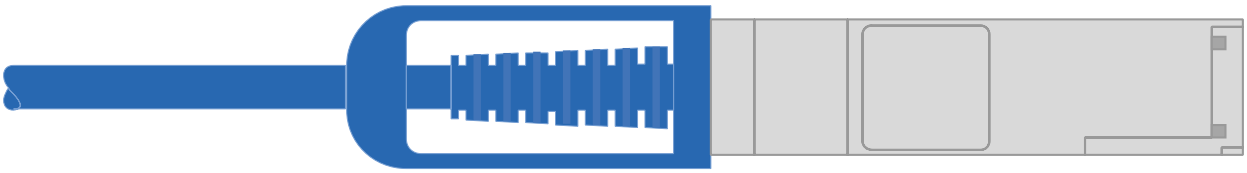
ASA A70 및 **ASA A90**

설정에 맞는 다음 케이블 연결 옵션 중 하나를 선택합니다.

옵션 **1:** 컨트롤러를 **NS224** 스토리지 쉘프 **1**개에 연결합니다

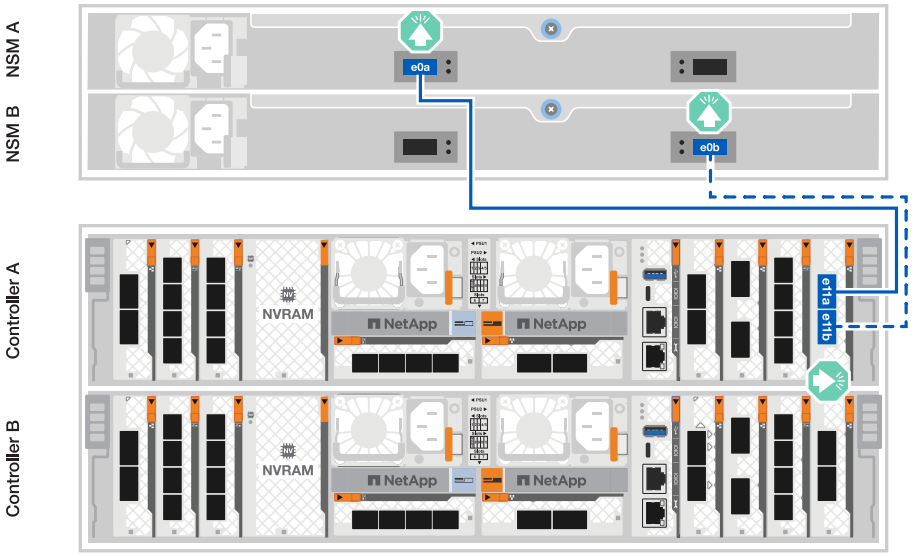
각 컨트롤러를 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

- 100 GbE QSFP28 구리 케이블 *

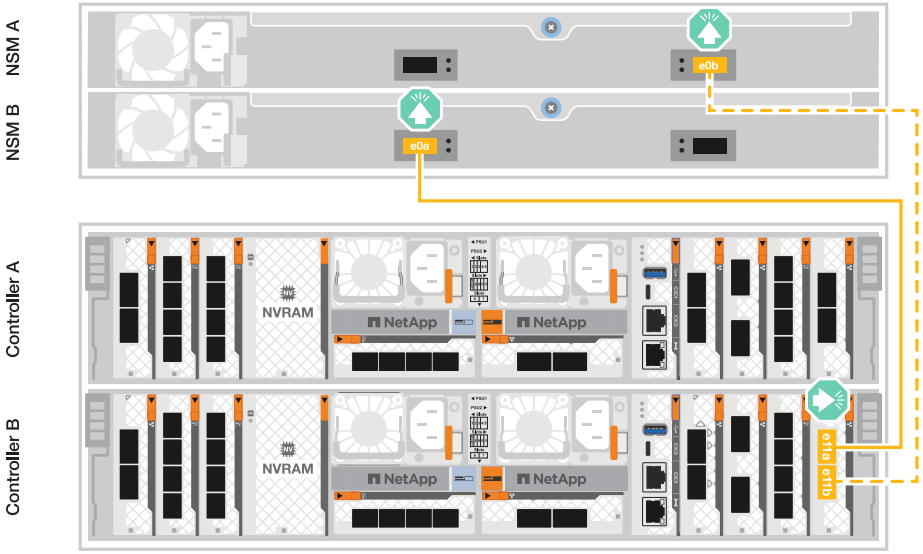


단계

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



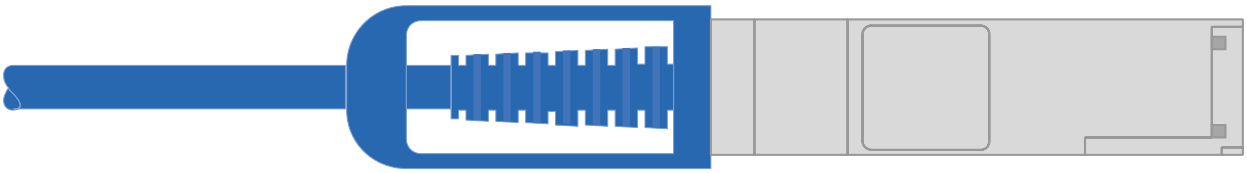
3. 컨트롤러 B 포트 e11a를 NSM B 포트 e0a에 연결합니다.
4. 컨트롤러 B 포트 e11b를 NSM A 포트 e0b에 연결합니다.


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

옵션 **2:** 컨트롤러를 **NS224** 스토리지 쉘프 **2**개에 연결합니다

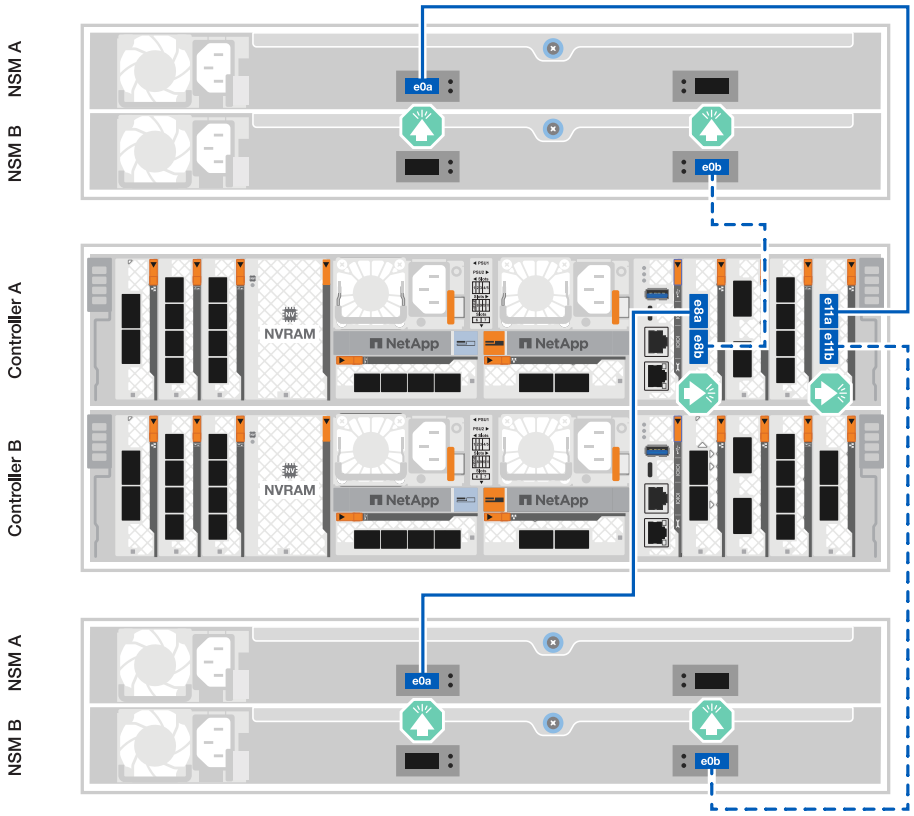
각 컨트롤러를 두 NS224 쉘프의 NSM 모듈에 연결합니다. 그래픽은 각 컨트롤러의 케이블 연결을 보여줍니다. 컨트롤러 A 케이블은 파란색으로 표시되고 컨트롤러 B 케이블은 노란색으로 표시됩니다.

- 100 GbE QSFP28 구리 케이블 *



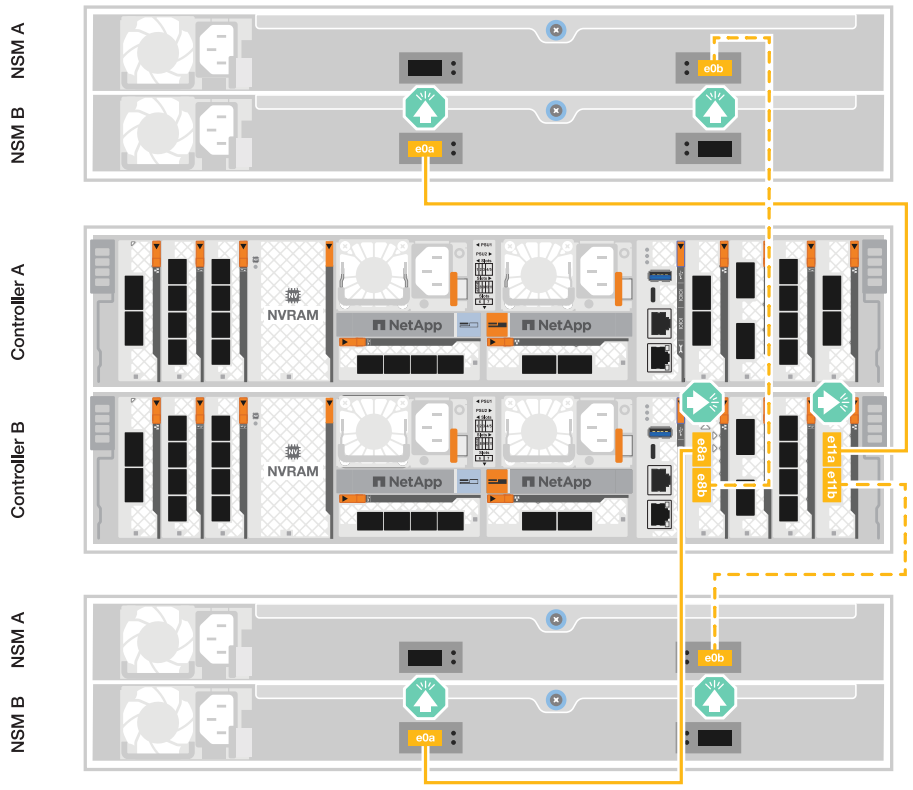
단계

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.



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 NS224 쉘프는 고유한 쉘프 ID로 구별됩니다. 이 ID는 쉘프가 스토리지 시스템 설정 내에서 구분되도록 합니다. 기본적으로 쉘프 ID는 '00' 및 '01'로 할당되지만 스토리지 시스템 전체에서 고유성을 유지하기 위해 이러한 ID를 조정해야 할 수도 있습니다.

이 작업에 대해

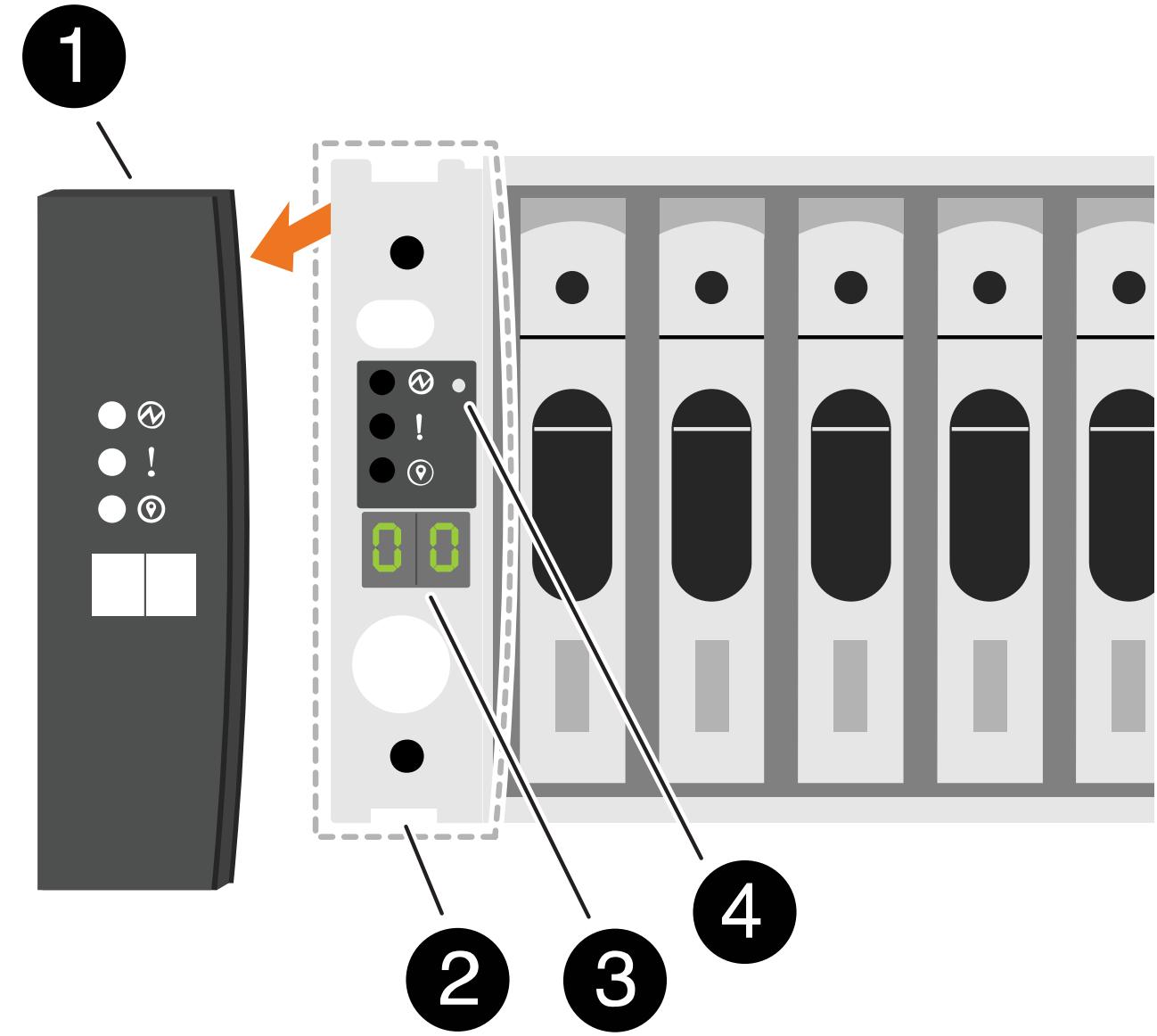
- 유효한 쉘프 ID는 00부터 99까지입니다.
- 쉘프 ID가 적용되려면 쉘프의 전원을 껐다가 다시 켜기(두 전원 코드를 모두 뽑은 다음, 적절한 시간을 기다린 다음 다시 꽂아야 합니다).

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

	선반 면판
	쉘프 ID 번호입니다
	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

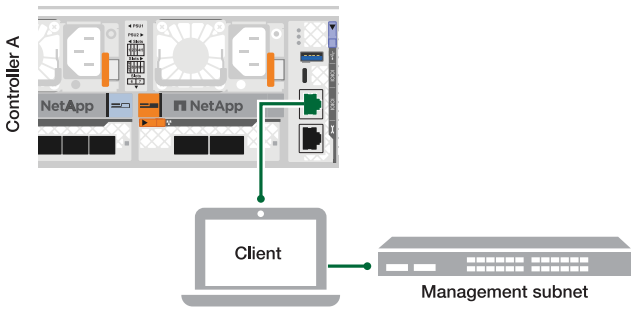
스토리지 쉘프를 켜고 고유한 ID를 할당한 후 스토리지 컨트롤러의 전원을 켭니다.

단계

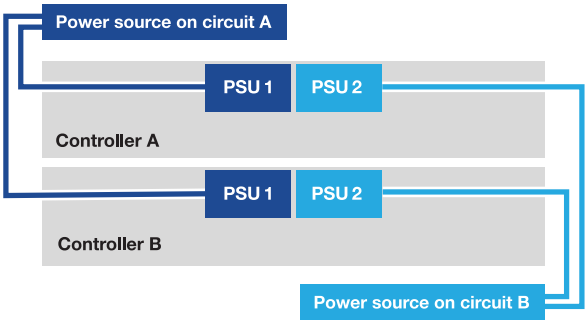
1. 랩톱을 직렬 콘솔 포트에 연결합니다. 이렇게 하면 컨트롤러가 켜져 있을 때 부팅 순서를 모니터링할 수 있습니다.
   a. 노트북의 직렬 콘솔 포트를 N-8-1에서 115,200보드로 설정합니다.

      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.



   d. 관리 서브넷에 있는 주소를 사용하여 랩톱에 TCP/IP 주소를 할당합니다.
2. 전원 코드를 컨트롤러 전원 공급 장치에 연결한 다음 다른 회로의 전원 공급 장치에 연결합니다.



- 스토리지 시스템 부팅이 시작됩니다. 초기 부팅에는 최대 8분이 소요될 수 있습니다.
- LED가 깜박이고 팬이 시작되면서 컨트롤러에 전원이 들어오고 있음을 나타냅니다.
- 처음 시동할 때 팬에서 소음이 많이 발생할 수 있습니다. 시동 중 팬 소음이 정상입니다.

3. 각 전원 공급 장치의 고정 장치를 사용하여 전원 케이블을 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.

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.

SAN 호스트에서 ASA R2 스토리지 시스템으로의 데이터 액세스가 가능합니다

데이터 액세스를 설정하려면 ONTAP와 함께 올바르게 작동하는 데 중요한 SAN 클라이언트의 특정 매개 변수 및 설정이 올바르게 구성되었는지 확인해야 합니다. VMware를 사용 중인 경우 가상 시스템을 마이그레이션해야 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

VM 워크로드를 ASA 스토리지 시스템에서 ASA R2 스토리지 시스템으로 마이그레이션해야 하는 경우, NetApp 를 사용하여 "VMware vSphere vMotion을 참조하십시오"무중단 실시간 데이터 마이그레이션을 수행하는 것이 좋습니다.

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 유닛은 SAN 호스트에서 데이터 작업을 위해 스토리지 공간을 사용할 수 있도록 합니다. 스토리지 유닛은 SCSI 호스트용 LUN 또는 NVMe 호스트용 NVMe 네임스페이스를 가리킵니다. 클러스터가 SCSI 호스트를 지원하도록 구성된 경우 LUN을 생성하라는 메시지가 표시됩니다. 클러스터가 NVMe 호스트를 지원하도록 구성된 경우 NVMe 네임스페이스를 생성하라는 메시지가 표시됩니다. ASA R2 스토리지 유닛의 최대 용량은 128TB입니다.

"NetApp Hardware Universe를 참조하십시오"ASA R2 시스템의 최신 스토리지 한도는 을 참조하십시오.

스토리지 유닛 생성 프로세스의 일부로 호스트 이니시에이터가 스토리지 유닛에 추가 및 매핑됩니다. 또한 "호스트 이니시에이터를 추가합니다""지도"스토리지 유닛을 생성한 후 스토리지 유닛에 연결할 수도 있습니다.

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.

4. 스토리지 유닛 용량을 입력한 다음 호스트 운영 체제를 선택합니다.
5. 자동으로 선택된 * 호스트 매핑 * 을 적용하거나 매핑할 스토리지 유닛에 대해 다른 호스트 그룹을 선택합니다.

    ◦ 호스트 매핑 * 은 새 스토리지 유닛이 매핑될 호스트 그룹을 나타냅니다. 새 스토리지 유닛에 대해 선택한 호스트 유형에 대해 기존 호스트 그룹이 있는 경우 기존 호스트 그룹이 호스트 매핑에 대해 자동으로 선택됩니다. 호스트 매핑에 대해 자동으로 선택된 호스트 그룹을 수락하거나 다른 호스트 그룹을 선택할 수 있습니다.

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

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.
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 제한, 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.

옵션을 선택합니다	단계
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.
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 NQN은 정규화된 도메인 이름 뒤에 <nqn.yyyy-mm>로 포맷되어야 합니다. 연도는 1970년 이후여야 합니다. 총 최대 길이는 223자입니다. 유효한 NVMe 이니시에이터의 예는 nqn.2014-08.com.example:string 입니다

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.

호스트 그룹을 생성합니다

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 생성했으며 이제 스토리지 유닛에 매핑할 수 있습니다.

스토리지 유닛을 호스트에 매핑합니다

ASA R2 스토리지 유닛을 생성하고 호스트 이니시에이터를 추가한 후에는 호스트를 스토리지 유닛에 매핑하여 데이터 서비스를 시작해야 합니다. 스토리지 유닛은 스토리지 유닛 생성 프로세스의 일부로 호스트에 매핑됩니다. 또한 언제든지 기존 스토리지 유닛을 새 호스트 또는 기존 호스트에 매핑할 수 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.

옵션을 선택합니다	단계
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.

ASA R2 스토리지 시스템에서 스토리지 유닛을 수정합니다

ASA R2 시스템의 성능을 최적화하려면 스토리지 유닛을 수정하여 용량을 늘리거나 QoS 정책을 업데이트하거나 유닛에 매핑된 호스트를 변경해야 할 수 있습니다. 예를 들어, 새로운 중요 애플리케이션 워크로드를 기존 스토리지 유닛에 추가하는 경우 새 애플리케이션에 필요한 성능 수준을 지원하기 위해 스토리지 유닛에 적용되는 QoS(서비스 품질) 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 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 스토리지 유닛이 복제 관계에 있는 정합성 보장 그룹에 있는 경우 "정합성 보장 그룹에서 스토리지 유닛을 제거합니다"삭제하기 전에 삭제해야 합니다.

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.

ASA R2 스토리지 제한

최적의 성능, 구성 및 지원을 위해 ASA R2 스토리지 제한을 숙지해야 합니다.

ASA R2 시스템은 다음을 지원합니다.

클러스터당 최대 노드 수	2
최대 저장 장치 크기	128TB

를 참조하십시오

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

데이터 보호

스냅샷을 생성하여 ASA R2 스토리지 시스템에 데이터를 백업합니다

ASA R2 시스템에서 데이터를 백업하려면 스냅샷을 생성해야 합니다. ONTAP 시스템 관리자를 사용하여 단일 스토리지 유닛의 수동 스냅샷을 생성하거나 정합성 보장 그룹을 생성하고 여러 스토리지 유닛의 자동 스냅샷을 동시에 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.

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 각 유닛은 동일한 용량과 동일한 호스트 운영 체제로 생성됩니다. 각 장치에 다른 용량을 할당하려면 * 추가 옵션 * 을 선택한 다음 * 다른 용량 추가 * 를 선택합니다.

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

다음 단계

보호할 스토리지 유닛이 포함된 정합성 보장 그룹을 생성했습니다. 이제 스냅샷을 생성할 준비가 되었습니다.

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

보호할 스토리지 유닛이 포함된 정합성 보장 그룹을 생성했습니다. 이제 스냅샷을 생성할 준비가 되었습니다.

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 생성할 수 있습니다. 필요 시 스냅샷으로 보호하기 위해 스토리지 유닛이 정합성 보장 그룹의 구성원일 필요는 없습니다. 정합성 보장 그룹의 구성원인 스토리지 유닛의 필요 시 스냅샷을 생성하는 경우 정합성 보장 그룹의 다른 스토리지 유닛은 필요 시 스냅샷에 포함되지 않습니다. 정합성 보장 그룹의 필요 시 스냅샷을 생성하는 경우 정합성 보장 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.

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 시스템의 스냅샷 복제는 다른 ASA R2 스토리지 시스템에서만 지원됩니다. ASA R2 시스템에서 현재 ASA, AFF 또는 FAS 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.

1단계**:** 클러스터 피어 관계를 생성합니다

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

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**:** 필요에 따라 복제 정책을 생성합니다

스냅샷 복제 정책은 ASA R2 클러스터에서 수행된 업데이트가 원격 사이트에 복제되는 시점을 정의합니다.

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 * 을 선택합니다.

옵션을 선택합니다	단계
데이터를 소스에 쓴 후 원격 사이트에 복사합니다.	a. Asynchronous * 를 선택합니다. b. 소스에서 스냅숏 전송 * 에서 기본 전송 일정을 수락하거나 다른 전송 일정을 선택합니다. c. 모든 스냅샷을 전송하거나 전송할 스냅샷을 결정하는 규칙을 생성하려면 선택합니다. d. 필요한 경우 네트워크 압축을 활성화합니다.
소스 사이트와 원격 사이트에 동시에 데이터 쓰기	a. Synchronous * 를 선택합니다.

6. 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

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. source_consistency 그룹은 복제할 로컬 클러스터의 정합성 보장 그룹을 나타냅니다. 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.

ASA R2 스토리지 시스템에서 Kubernetes 애플리케이션을 보호합니다

Astra Control Center를 사용하여 Kubernetes 애플리케이션을 보호하십시오. Astra Control Center를 사용하면 애플리케이션 및 데이터를 Kubernetes 클러스터 간에 마이그레이션하고, NetApp SnapMirror 기술을 사용하여 애플리케이션을 원격 시스템으로 복제하고, 스테이징에서 운영 환경으로 애플리케이션을 복제할 수 있습니다.

를 참조하십시오

"Astra Control을 사용하여 Kubernetes 애플리케이션을 보호하는 방법에 대해 자세히 알아보십시오"..

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.

ASA R2 스토리지 시스템에서 ONTAP 정합성 보장 그룹을 관리합니다

정합성 보장 그룹은 단일 유닛으로 관리되는 스토리지 유닛의 모음입니다. 일관성 그룹을 사용하여 스토리지 관리를 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. 스토리지 유닛을 개별적으로 백업하지 않고 정합성 보장 그룹으로 백업하면 모든 유닛에 대해 일관된 백업이 가능하지만 개별적으로 백업하면 정합성이 보장되지 않을 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. 편집 * 을 선택합니다.

다음 단계

스냅샷을 통해 데이터가 보호되므로 "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.

정합성 보장 그룹에 스토리지 유닛을 추가합니다

정합성 보장 그룹에 스토리지 유닛을 추가하여 정합성 보장 그룹에서 관리하는 스토리지 양을 확장합니다.

정합성 보장 그룹에 기존 스토리지 유닛을 추가하거나 새 스토리지 유닛을 생성하여 정합성 보장 그룹에 추가할 수

있습니다.

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.

   하나 이상의 유닛을 생성하는 경우 각 유닛은 동일한 용량과 동일한 호스트 운영 체제로 생성됩니다. 각 유닛에 다른 용량을 할당하려면 * 다른 용량 추가 * 를 선택하여 각 유닛에 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

스토리지 유닛을 삭제하려는 경우, 스토리지 유닛을 다른 정합성 보장 그룹의 일부로 관리하려는 경우 또는 스토리지 유닛에 포함된 데이터를 더 이상 보호할 필요가 없는 경우 정합성 보장 그룹에서 스토리지 유닛을 제거해야 합니다. 정합성 보장 그룹에서 스토리지 유닛을 제거하면 스토리지 유닛과 정합성 보장 그룹 간의 관계가 끊어지지만 스토리지 유닛은 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.

일관성 그룹을 삭제합니다

일관성 그룹의 구성원을 더 이상 단일 단위로 관리할 필요가 없는 경우 해당 일관성 그룹을 삭제할 수 있습니다. 정합성 보장 그룹을 삭제한 후에는 이전에 그룹에 속한 스토리지 유닛이 클러스터에서 활성 상태로 유지됩니다.

시작하기 전에

삭제하려는 일관성 그룹이 복제 관계에 있는 경우 일관성 그룹을 삭제하기 전에 관계를 해제해야 합니다. 이전에 복제 정합성 보장 그룹을 삭제한 후에는 정합성 보장 그룹에 있던 스토리지 유닛이 클러스터에서 활성 상태로 유지되고 복제된 복제본이 원격 클러스터에 남아 있습니다.

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 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 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.
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.

ASA R2 스토리지 시스템에서 랜섬웨어 공격을 방어합니다

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 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.

관리 및 모니터링

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.

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.

IP 데이터 LIF가 생성되면 기본적으로 iSCSI 및 NVMe/TCP 트래픽을 모두 처리할 수 있습니다. FC 및 NVMe/FC 트래픽에는 대해 별도의 데이터 LIF를 생성해야 합니다.

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.

LIF(네트워크 인터페이스) 수정

LIF는 필요에 따라 사용하지 않도록 설정하거나 이름을 바꿀 수 있습니다. LIF IP 주소 및 서브넷 마스크를 변경할 수도 있습니다.

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 볼 때 매일 동시에 성능이 저하된다는 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 절약되는 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 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

새 드라이브를 노드 또는 쉘프에 설치하기 전에 NetApp Hardware Universe를 사용하여 추가하려는 드라이브가 ASA R2 플랫폼에서 지원되는지 확인하고 새 드라이브에 대한 올바른 슬롯을 식별하십시오. 드라이브를 추가할 수 있는 올바른 슬롯은 플랫폼 모델과 ONTAP 버전에 따라 다릅니다. 경우에 따라 특정 슬롯에 순차적으로 드라이브를 추가해야 할 수도 있습니다.

단계

1. 로 이동합니다"NetApp Hardware Universe를 참조하십시오".
2. 제품 * 에서 하드웨어 구성을 선택합니다.
3. ASA R2 플랫폼을 선택합니다.
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. 플랫폼 전면에서 베젤을 조심스럽게 분리합니다.
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 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. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮ 다음 * 사용 * 을 선택합니다.
3. EULA를 읽고 동의합니다.
4. 기본값을 그대로 사용하여 펌웨어 및 시스템 파일을 자동으로 업데이트합니다. 필요한 경우 알림을 표시하거나 권장 업데이트를 자동으로 해제하려면 을 선택합니다.
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

권장 업데이트를 설치하기 전에 유연하게 볼 수 있도록 하려면 자동 업데이트를 사용하지 않도록 설정합니다. 자동 업데이트를 비활성화하는 경우 펌웨어 및 시스템 파일 업데이트를 수동으로 수행해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮다음 * 사용 안 함 * 을 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. 자동 업데이트 * 옆에 있는 * 를 선택한 ⋮다음 * 모든 자동 업데이트 보기 * 를 선택합니다.

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. 자동 업데이트 * 옆에 있는 * ⋮자동 업데이트 * 를 선택한 다음 * 자동 업데이트 편집 * 을 선택합니다.
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. System Manager에서 * 클러스터 > 개요 * 를 선택한 다음 * 업데이트 * 를 선택합니다.
3. 펌웨어 업데이트 * 를 선택하고 선택합니다 + Update firmware .

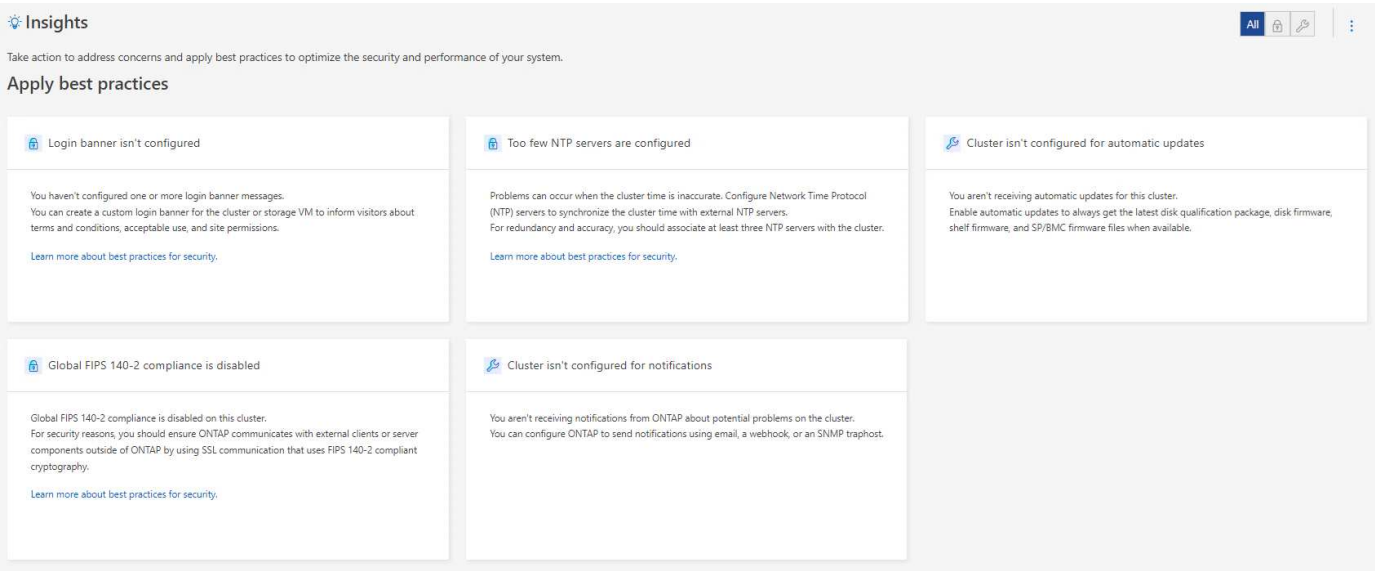
결과

펌웨어가 업데이트됩니다.

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.
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 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 CSR 선택합니다.
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 문서 유지 관리" 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 All-Flash 플랫폼을 기반으로 구축된 SAN 전용 환경을 위한 하드웨어 및 소프트웨어 통합 솔루션을 제공합니다. ASA R2 시스템은 스토리지 계층 구현 시 다른 ONTAP 시스템(ASA, AFF 및 FAS)과 다르며 지원되는 프로토콜 및 ONTAP 성격 구현 시 서로 다릅니다.

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. 다른 모든 ONTAP 시스템(ASA, AFF, FAS)에서 실행되는 ONTAP는 _ 유니파이드 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 입력합니다. `san config show`

ONTAP 스토리지 시스템의 특성은 변경할 수 없습니다.

통합 ONTAP 속성을 실행하는 ONTAP 시스템의 스토리지 계층에서는 애그리게이트를 스토리지의 기본 유닛으로 사용합니다. Aggregate는 스토리지 시스템에서 사용 가능한 특정 디스크 세트를 소유합니다. Aggregate는 소유한 디스크의 공간을 LUN 및 네임스페이스를 위한 볼륨에 할당합니다. 유니파이드 ONTAP 사용자는 CLI(Command Line Interface)를 사용하여 애그리게이트, 볼륨, LUN 및 네임스페이스를 생성하고 수정할 수 있습니다.

ASA R2 시스템의 스토리지 계층에서는 애그리게이트 대신 스토리지 가용성 영역을 사용합니다. 스토리지 가용 영역은 스토리지 시스템의 모든 가용 디스크에 액세스할 수 있는 공통 스토리지 풀입니다. 스토리지 가용성 영역은 ASA R2 HA 쌍의 두 노드에 표시됩니다. LUN 또는 NVMe 네임스페이스를 기반으로 하는 스토리지 유닛이 생성되면 ONTAP은 스토리지 가용성 영역에 VM(스토리지 가상 머신)이 포함된 볼륨을 자동으로 생성하여 스토리지 유닛을 수용합니다. 스토리지 관리에 대한 이 자동화되고 단순한 접근 방식으로 인해 특정 System Manager 옵션, ONTAP 명령 및 REST API 엔드포인트를 사용할 수 없거나 ASA R2 시스템에서 사용이 제한되었습니다. 예를 들어, ASA R2 시스템의 경우 볼륨 생성 및 관리가 자동화되므로 * Volumes * 메뉴가 System Manager에 나타나지 않고 `volume create` 명령이 지원되지 않습니다.

ASA R2 스토리지는 다음과 같은 측면에서 다른 ONTAP 스토리지 시스템과 비교됩니다.

	ASA r2 를 참조하십시오	**ASA**	**AFF**	**FAS**
• ONTAP 성격 *	ASA r2 를 참조하십시오	ASA	통합	통합

	ASA r2 를 참조하십시오	ASA	AFF	FAS
• SAN 프로토콜 지원 *	예	예	예	예
• NAS 프로토콜 지원 *	아니요	아니요	예	예
• 스토리지 계층 지원 *	스토리지 가용 영역	애그리게이트	애그리게이트	애그리게이트

다음 ASA 플랫폼은 ASA R2 시스템으로 분류됩니다.

- ASA A1K 를 참조하십시오
- ASA A70 를 참조하십시오
- ASA A90 를 참조하십시오

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 시스템의 차이점을 요약합니다

ONTAP CLI(Command Line Interface) 및 REST API와 관련된 ASA R2 시스템과 FAS, AFF 및 ASA 시스템의 주요 차이점은 아래에 설명되어 있습니다.

프로토콜 서비스를 통한 기본 **SVM** 생성

새로운 클러스터에는 SAN 프로토콜이 활성화된 기본 데이터 SVM이 자동으로 포함됩니다. IP 데이터 LIF는 iSCSI 및 NVMe/TCP 프로토콜을 지원하며 `default-data-blocks` 기본적으로 서비스 정책을 사용합니다.

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

용 스토리지 유닛은 항상 ASA R2 스토리지 시스템에서 씬 프로비저닝됩니다. 일반 프로비저닝은 지원되지 않습니다.

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.

- iSCSI LIF 페일오버
- FabricPool
- LUN 일반 프로비저닝
- MetroCluster
- 오브젝트 프로토콜
- ONTAP S3 SnapMirror 및 S3 API
- SnapMirror에서 클라우드로
- SnapMirror에서 비 ASA R2 시스템으로 마이그레이션
- 선택적 LUN 맵(SLM)

ASA R2 시스템은 다음을 지원합니다.

- SnapLock
- 이중 계층 암호화

를 참조하십시오

- "NetApp Hardware Universe를 참조하십시오"ASA R2 하드웨어 지원 및 제한 사항에 대한 자세한 내용은 를 참조하십시오.
- "스냅샷을 잠그는 방법에 대해 알아봅니다" ASA R2 시스템에서.
- "이중 레이어 암호화를 적용하는 방법에 대해 알아봅니다" ASA R2 시스템의 데이터로 이동합니다.

ASA R2 스토리지 시스템에 대한 ONTAP CLI 지원

ASA R2 시스템은 스토리지 시스템에서 사용할 수 있는 특정 디스크 세트를 소유하는 기존 애그리게이트 대신 _ 스토리지 가용 영역 _ 을(를) 사용합니다. 스토리지 가용 영역은 스토리지 시스템의 모든 가용 디스크에 액세스할 수 있는 공통 스토리지 풀입니다. 스토리지 가용성 영역은 ASA R2 HA 쌍의 두 노드에 표시됩니다. 스토리지 유닛(LUN 또는 NVMe 네임스페이스)이 생성되면 ONTAP은 스토리지 가용성 영역에 스토리지 가상 머신(VM)이 포함된 볼륨을 자동으로 생성하여 스토리지 유닛을 수용합니다.

이처럼 스토리지 관리가 단순화되어 `storage aggregate` ASA R2 시스템에서는 명령이 지원되지 않습니다. 특정 `lun` 및 `volume` 명령 및 매개 변수에 대한 지원도 제한됩니다.

다음 명령 및 명령 세트는 R2의 ASA에서 지원되지 않습니다.

지원되지 않는 **<code> LUN </code>** 명령입니다

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  이 명령은 LUN 이름 바꾸기/SVM NVMe 네임스페이스 이름 바꾸기로 대체됩니다.

- `lun transition`

지원되지 않는 **<code> volume </code>** 명령 및 매개 변수입니다

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  다음 매개 변수와 함께 사용할 때는 이 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

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> storage </code>** 명령입니다

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

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.

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

는 기술 지원 부서에서 ASA R2 시스템으로부터 AutoSupport 메시지를 수신할 수 있으며, 문제가 발생한 경우 지원을 위해 필요한 데이터를 보유하고 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 확인해야 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.