ONTAP를 사용하여 데이터를 관리합니다

ASA r2

NetApp
February 25, 2026

목차

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.".