ONTAP를 사용하여 데이터를 관리합니다

ASA r2

NetApp
September 26, 2024

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 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.