Oracle 데이터 보호

Enterprise applications

NetApp
May 09, 2024

목차

Oracle 데이터 보호

ONTAP을 사용한 Oracle 데이터 보호

NetApp은 가장 미션 크리티컬한 데이터가 데이터베이스에 있다는 것을 알고 있습니다.

데이터에 액세스하지 않고는 기업을 운영할 수 없으며 경우에 따라서는 데이터가 비즈니스를 정의하기도 합니다. 이러한 데이터는 보호해야 합니다. 그러나 데이터 보호는 사용 가능한 백업을 보장하는 것 이상의 의미를 갖습니다. 백업을 안전하게 저장하는 것은 물론 빠르고 안정적으로 수행하는 것입니다.

데이터 보호의 다른 측면은 데이터 복구입니다. 데이터에 액세스할 수 없으면 엔터프라이즈가 영향을 받으며 데이터를 복원하기 전까지 작동하지 않을 수 있습니다. 이 프로세스는 빠르고 안정적이어야 합니다. 마지막으로, 대부분의 데이터베이스는 재해로부터 보호해야 합니다. 즉, 데이터베이스의 복제본을 유지 관리해야 합니다. 복제본이 최신 상태여야 합니다. 또한 복제본을 완벽하게 작동하는 데이터베이스로 빠르고 간단하게 만들 수 있어야 합니다.

이 문서는 이전에 게시된 기술 보고서_TR-4591: Oracle 데이터 보호: 백업, 복구 및 복제 _ 를 대체합니다

계획 수립

적절한 엔터프라이즈 데이터 보호 아키텍처는 다양한 이벤트 중에 데이터 보존, 복구 기능 및 운영 중단에 대한 허용성과 관련된 비즈니스 요구 사항에 따라 달라집니다.

예를 들어, 적용 범위의 애플리케이션, 데이터베이스 및 중요 데이터 세트의 수를 예로 들어 보겠습니다. 관리할 객체가 많지 않기 때문에 단일 데이터 세트에 대해 일반적인 SLA를 준수하는 백업 전략을 구축하는 것은 매우 간단합니다. 데이터 세트의 수가 늘어나면 모니터링이 더 복잡해지고 관리자는 백업 장애를 해결하는 데 더 많은 시간을 소비해야 할 수도 있습니다. 환경이 클라우드에 도달하고 서비스 공급자가 확장됨에 따라 완전히 다른 접근 방식이 필요합니다.

데이터 세트 크기도 전략에 영향을 줍니다. 예를 들어, 데이터 세트가 매우 작기 때문에 100GB 데이터베이스를 사용한 백업 및 복구에 사용할 수 있는 옵션이 많이 있습니다. 기존 툴을 사용하여 백업 미디어에서 데이터를 복제하는 것만으로도 복구에 충분한 RTO를 얻을 수 있습니다. 일반적으로 100TB 데이터베이스에는 다일의 운영 중단이 허용되지 않는 한 100TB 데이터베이스에는 일반적으로 완전히 다른 전략이 필요합니다. 이 경우 기존의 복사본 기반 백업 및 복구 절차가 허용되는 경우가 아니라면 말입니다.

마지막으로, 백업 및 복구 프로세스 자체 이외의 요소가 있습니다. 예를 들어, 중요한 운영 작업을 지원하는 데이터베이스가 있어 숙련된 DBA만 수행하는 드문 이벤트로 간주됩니까? 아니면 데이터베이스가 대규모 개발 환경에 있어서 복구가 자주 발생하고 일반 IT 팀이 관리하는 환경입니까?

Oracle 데이터베이스 RTO, RPO 및 SLA 계획 수립

ONTAP을 사용하면 Oracle 데이터베이스 데이터 보호 전략을 비즈니스 요구 사항에 맞게 쉽게 조정할 수 있습니다.

이러한 요구 사항에는 복구 속도, 허용되는 최대 데이터 손실 및 백업 보존 요구 사항 등의 요인이 포함됩니다. 데이터 보호 계획도 데이터 보존 및 복원에 대한 다양한 규정 요구 사항을 고려해야 합니다. 마지막으로 사용자 또는 애플리케이션 오류로 인해 발생하는 일반적인 복구 방법부터 사이트의 완전한 손실을 포함하는 재해 복구 시나리오에 이르기까지 다양한 데이터 복구 시나리오를 고려해야 합니다.

데이터 보호 및 복구 정책을 조금만 변경하면 스토리지, 백업 및 복구의 전체 아키텍처에 상당한 영향을 줄 수 있습니다.

데이터 보호 아키텍처의 복잡성을 방지하려면 설계 작업을 시작하기 전에 표준을 정의하고 문서화해야 합니다. 불필요한 기능이나 보호 수준은 불필요한 비용과 관리 부담을 초래하며, 초기에 간과한 요구 사항으로 인해 프로젝트가 잘못된 방향으로 진행되거나 최종 설계 변경이 필요할 수 있습니다.

복구 시간 목표

RTO(복구 시간 목표)는 서비스 복구에 허용되는 최대 시간을 정의합니다. 예를 들어 인사 데이터베이스의 RTO는 24시간이 될 수 있습니다. 왜냐하면 업무 중에 이 데이터에 액세스하지 못하는 것이 매우 불편함에도 불구하고 비즈니스가 계속 운영될 수 있기 때문입니다. 반면 은행의 총계정원장을 지원하는 데이터베이스에는 분 또는 초 단위로 측정된 RTO가 있습니다. 실제 서비스 중단과 네트워크 패킷 손실과 같은 일상적인 이벤트를 구분하는 방법이 있어야 하므로 RTO 0은 불가능합니다. 하지만 제로에 가까운 RTO는 일반적인 요구사항입니다.

복구 시점 목표

RPO(복구 지점 목표)는 허용되는 최대 데이터 손실을 정의합니다. 대부분의 경우 RPO는 스냅샷 또는 SnapMirror 업데이트 빈도에 의해서만 결정됩니다.

경우에 따라 RPO를 보다 적극적으로 설정하여 특정 데이터를 보다 자주 보호할 수 있습니다. 데이터베이스 컨텍스트에서 RPO는 일반적으로 특정 상황에서 손실될 수 있는 로그 데이터의 양이 어느 정도인지에 관한 문제입니다. 제품 버그 또는 사용자 오류로 인해 데이터베이스가 손상된 일반적인 복구 시나리오에서 RPO는 0이어야 합니다. 즉, 데이터 손실이 없어야 합니다. 복구 절차에서는 데이터베이스 파일의 이전 복사본을 복원한 다음 로그 파일을 재생하여 데이터베이스 상태를 원하는 시점으로 되돌리는 작업을 수행합니다. 이 작업에 필요한 로그 파일이 이미 원래 위치에 있어야 합니다.

비정상적인 시나리오에서는 로그 데이터가 손실될 수 있습니다. 예를 들어, 우발적 또는 악의적 경우입니다 `rm -rf *` 데이터베이스 파일의 경우 모든 데이터가 삭제될 수 있습니다. 유일한 옵션은 로그 파일을 포함하여 백업에서 복원하는 것이며, 일부 데이터가 손실될 수밖에 없습니다. 기존 백업 환경에서 RPO를 향상시킬 수 있는 유일한 옵션은 로그 데이터의 반복 백업을 수행하는 것입니다. 그러나 지속적인 데이터 이동과 백업 시스템을 지속적으로 실행하는 서비스로 유지 관리하기가 어렵기 때문에 이러한 문제에는 한계가 있습니다. 고급 스토리지 시스템의 이점 중 하나는 파일에 대한 우발적 또는 악의적 손상으로부터 데이터를 보호하여 데이터 이동 없이 더 높은 RPO를 제공하는 기능입니다.

재해 복구

재해 복구에는 물리적 재해 발생 시 서비스를 복구하는 데 필요한 IT 아키텍처, 정책 및 절차가 포함됩니다. 여기에는 홍수, 화재 또는 악의적이거나 과실로 행동하는 사람이 포함될 수 있습니다.

재해 복구는 단순한 복구 절차 그 이상입니다. 다양한 위험을 식별하고, 데이터 복구 및 서비스 연속성 요구 사항을 정의하고, 관련 절차에 따라 올바른 아키텍처를 제공하는 완전한 프로세스입니다.

데이터 보호 요구 사항을 설정할 때는 일반적인 RPO 및 RTO 요구 사항과 재해 복구에 필요한 RPO 및 RTO 요구 사항을 구분해야 합니다. 일부 애플리케이션 환경에서는 비교적 일반적인 사용자 오류부터 데이터 센터 파괴에 이르는 데이터 손실 상황에 대해 0의 RPO와 0에 가까운 RTO가 필요합니다. 그러나 이러한 높은 수준의 보호를 위해서는 비용과 관리 상의 문제가 발생합니다.

일반적으로 비재해 데이터 복구 요구사항은 두 가지 이유로 엄격해야 합니다. 첫째, 애플리케이션 버그와 사용자 오류로 인해 데이터가 손상되는 것은 거의 불가피한 시점까지 예상할 수 있습니다. 둘째, 스토리지 시스템이 폐기되지 않는 한 RPO 0과 낮은 RTO를 제공할 수 있는 백업 전략을 설계하는 것은 쉽지 않습니다. 쉽게 해결할 수 있는 심각한 위험을 해결하지 않을 이유가 없습니다. 따라서 로컬 복구에 대한 RPO 및 RTO 목표를 적극적으로 적용해야 합니다.

재해 복구 RTO 및 RPO 요구 사항은 재해 가능성 및 관련 데이터 손실 또는 비즈니스 중단 결과에 따라 더 크게 달라집니다. RPO 및 RTO 요구 사항은 일반적인 원칙이 아닌 실제 비즈니스 요구 사항을 기반으로 해야 합니다. 여러 논리적 및 물리적 재해 시나리오를 고려해야 합니다.

논리적 재해

논리적 재해에는 사용자, 애플리케이션 또는 OS 버그, 소프트웨어 오작동으로 인한 데이터 손상이 포함됩니다. 논리적 재해에는 바이러스 또는 웜이 있는 외부 사용자에 의한 악의적인 공격이나 응용 프로그램 취약점을 악용하는 공격도 포함될 수 있습니다. 이러한 경우 물리적 인프라스트럭처는 손상되지 않지만 기본 데이터는 더 이상 유효하지 않습니다.

점점 더 일반적인 유형의 논리적 재해를 랜섬웨어라고 하며, 이를 공격 벡터가 데이터를 암호화하는 데 사용됩니다. 암호화는 데이터를 손상시키지 않지만 제3자에게 지불이 이루어질 때까지 데이터를 사용할 수 없게 합니다. 랜섬웨어 해킹을 특별히 도입한 기업이 점점 더 많아지고 있습니다. NetApp는 이러한 위협에 대해 변조 방지 스냅샷을 제공합니다. 따라서 스토리지 관리자도 구성된 만료일 전에 보호된 데이터를 변경할 수 없습니다.

물리적 재해

물리적 재해에는 인프라의 구성 요소가 중복성을 넘어 데이터 손실이나 서비스 손실로 이어지는 장애가 포함됩니다. 예를 들어 RAID 보호는 디스크 드라이브 이중화를 제공하며 HBA를 사용하면 FC 포트 및 FC 케이블 이중화를 제공할 수 있습니다. 이러한 구성 요소의 하드웨어 장애는 예측 가능하며 가용성에 영향을 미치지 않습니다.

엔터프라이즈 환경에서는 일반적으로 예측 가능한 유일한 물리적 재해 시나리오가 사이트의 완전한 손실인 시점까지 중복 구성 요소를 사용하여 전체 사이트의 인프라를 보호할 수 있습니다. 그런 다음 재해 복구 계획이 사이트 간 복제에 달려 있습니다.

동기식 및 비동기식 데이터 보호

이상적인 환경에서는 모든 데이터를 지리적으로 분산된 사이트에 걸쳐 동기식으로 복제합니다. 이러한 복제는 다음과 같은 몇 가지 이유로 항상 실현 가능하지 않거나 가능한 경우가 있습니다.

- 애플리케이션/데이터베이스가 처리를 진행하기 전에 모든 변경 사항을 두 위치에 복제해야 하기 때문에 동기식 복제는 불가피하게 쓰기 지연 시간을 증가시킵니다. 이로 인해 발생할 수 있는 성능 영향은 용납되지 않으므로 동기식 미러링 사용을 배제할 수 있습니다.
- 100% SSD 스토리지의 채택이 증가함에 따라 성능 기대치에는 수십만 IOPS와 1ms 미만의 지연 시간이 포함되므로 쓰기 지연 시간이 더 많이 발생하고 있습니다. 100% SSD 사용의 이점을 최대한 활용하려면 재해 복구 전략을 다시 세워야 할 수 있습니다.
- 데이터 세트는 바이트 측면에서 계속 증가하고 있기 때문에 동기 복제를 지속할 수 있는 충분한 대역폭을 확보하는 데 어려움이 있습니다.
- 또한 데이터 세트가 복잡해지면서 대규모 동기식 복제 관리에 따르는 문제가 발생합니다.
- 클라우드 기반 전략에서는 복제 거리와 지연 시간이 더욱 길어져 동기식 미러링을 사용하는 것이 오히려 사라지는 경우가 많습니다.

NetApp은 가장 까다로운 데이터 복구 요구사항을 위한 동기식 복제 솔루션과 향상된 성능과 유연성을 지원하는 비동기 솔루션을 제공합니다. 또한 NetApp 기술은 Oracle DataGuard와 같은 여러 타사 복제 솔루션과 원활하게 통합됩니다

보존 시간

데이터 보호 전략의 마지막 측면은 데이터 보존 시간이며, 이는 크게 달라질 수 있습니다.

- 일반적으로 운영 사이트에서 14일 야간 백업을 수행하고 보조 사이트에 90일 동안 백업을 저장해야 합니다.
- 많은 고객이 서로 다른 미디어에 저장된 분기별 독립 실행형 아카이브를 생성합니다.
- 데이터베이스를 지속적으로 업데이트하면 기록 데이터가 필요하지 않을 수 있으며, 백업은 며칠 동안만 보존되어야 합니다.

- 규정 요구 사항에 따라 365일 기간 내에 임의의 트랜잭션 시점까지 복구가 필요할 수 있습니다.

ONTAP을 사용한 Oracle 데이터베이스 가용성

ONTAP는 최대한의 Oracle 데이터베이스 가용성을 제공하도록 설계되었습니다. ONTAP 고가용성 기능에 대한 전체 설명은 본 문서의 범위를 벗어나며 그러나 데이터 보호와 마찬가지로 데이터베이스 인프라를 설계할 때는 이 기능에 대한 기본적인 이해가 중요합니다.

HA 쌍

고가용성의 기본 단위는 HA 쌍입니다. 각 쌍에는 NVRAM에 데이터 복제를 지원하는 중복 링크가 포함되어 있습니다. NVRAM은 쓰기 캐시가 아닙니다. 컨트롤러 내의 RAM은 쓰기 캐시 역할을 합니다. NVRAM의 목적은 예기치 않은 시스템 장애를 방지하기 위해 일시적으로 데이터를 저널링하는 것입니다. 이 점에서 데이터베이스 재실행 로그와 유사합니다.

NVRAM과 데이터베이스 재실행 로그를 모두 사용하여 데이터를 빠르게 저장하므로 데이터의 변경사항을 최대한 빠르게 커밋할 수 있습니다. 드라이브(또는 데이터 파일)의 영구 데이터에 대한 업데이트는 ONTAP 플랫폼과 대부분의 데이터베이스 플랫폼 모두에서 체크포인트라는 프로세스 도중 늦게 수행되지 않습니다. 정상 작업 중에는 NVRAM 데이터나 데이터베이스 재실행 로그를 읽지 않습니다.

컨트롤러가 갑자기 실패할 경우 드라이브에 아직 기록되지 않은 NVRAM에 저장된 변경 사항이 보류 중일 수 있습니다. 파트너 컨트롤러는 장애를 감지하고 드라이브를 제어하며 NVRAM에 저장된 필수 변경 사항을 적용합니다.

테이크오버 및 반환

Takeover 및 Giveback은 HA 2노드의 노드 간에 스토리지 리소스에 대한 책임을 지는 프로세스를 의미합니다. Takeover와 반환에는 두 가지 측면이 있습니다.

- 드라이브에 액세스할 수 있는 네트워크 연결 관리
- 드라이브 자체 관리

CIFS 및 NFS 트래픽을 지원하는 네트워크 인터페이스는 홈 위치와 페일오버 위치 모두를 사용하여 구성됩니다. 테이크오버는 원래 위치와 동일한 서브넷에 있는 물리적 인터페이스에서 네트워크 인터페이스를 임시 홈으로 이동하는 것을 포함합니다. 반환에는 네트워크 인터페이스를 원래 위치로 이동하는 것도 포함됩니다. 정확한 동작은 필요에 따라 조정할 수 있습니다.

iSCSI 및 FC와 같은 SAN 블록 프로토콜을 지원하는 네트워크 인터페이스는 테이크오버 및 반환 중에 재배치되지 않습니다. 전체 HA 쌍이 포함된 경로를 사용하여 LUN을 프로비저닝해야 하므로 1차 경로와 2차 경로가 됩니다.

추가 컨트롤러를 위한 추가 경로를 대규모 클러스터에서 노드 간 데이터 재배치를 지원하도록 구성할 수도 있지만 이는 HA 프로세스에 포함되지 않습니다.

Takeover와 Giveback의 두 번째 측면은 디스크 소유권을 이전하는 것입니다. 정확한 프로세스는 Takeover/Giveback 이유 및 실행된 명령줄 옵션을 비롯한 여러 요인에 따라 달라집니다. 목표는 최대한 효율적으로 작업을 수행하는 것입니다. 전체 프로세스에는 몇 분이 필요한 것처럼 보이지만 드라이브 소유권이 노드에서 노드로 전환되는 실제 순간은 일반적으로 초 단위로 측정할 수 있습니다.

인수 시간

테이크오버 및 반환 작업 중에 호스트 I/O가 잠깐 정지되지만 올바르게 구성된 환경에서는 애플리케이션이 중단되어서는 안 됩니다. I/O가 지연되는 실제 전환 프로세스는 일반적으로 몇 초 내로 측정되지만, 호스트에서 데이터 경로의 변경을 인식하고 I/O 작업을 다시 제출하기 위해 추가 시간이 필요할 수 있습니다.

중단 특성은 프로토콜에 따라 다릅니다.

- NFS 및 CIFS 트래픽을 지원하는 네트워크 인터페이스는 새 물리적 위치로 전환한 후 네트워크에 ARP(Address Resolution Protocol) 요청을 발급합니다. 이로 인해 네트워크 스위치가 MAC(Media Access Control) 주소 테이블을 업데이트하고 I/O 처리를 재개합니다 계획된 테이크오버와 반환의 경우 운영 중단은 일반적으로 몇 초 단위로 측정되며, 대부분의 경우 감지할 수 없는 경우가 많습니다. 일부 네트워크는 네트워크 경로의 변화를 완전히 인식하기 위해 더 느려질 수 있으며 일부 운영 체제는 재시도해야 하는 매우 짧은 시간 내에 많은 I/O를 대기시킬 수 있습니다. 이렇게 하면 입출력을 재개하는 데 필요한 시간이 길어질 수 있습니다
- SAN 프로토콜을 지원하는 네트워크 인터페이스는 새 위치로 전환되지 않습니다. 호스트 운영 체제에서 사용 중인 경로를 변경해야 합니다. 호스트에서 관찰되는 입출력 일시 중지는 여러 요인에 따라 달라집니다. 스토리지 시스템 관점에서 볼 때 입출력을 처리할 수 없는 기간은 불과 몇 초입니다. 그러나 다른 호스트 운영 체제마다 재시도하기 전에 I/O가 시간 초과되도록 하려면 추가 시간이 필요할 수 있습니다. 최신 운영 체제는 경로 변경을 훨씬 더 빠르게 인식할 수 있지만, 기존 운영 체제에서는 일반적으로 변경 사항을 인식하는 데 최대 30초가 걸립니다.

아래 표에는 스토리지 시스템에서 애플리케이션 환경에 데이터를 제공할 수 없는 테이크오버가 예상되고 있습니다. 애플리케이션 환경에서 오류가 발생하지 않도록 하려면 테이크오버 대신 IO 처리 중에 잠깐 정지된 상태로 표시되어야 합니다.

	NFS 를 참조하십시오	AFF	ASA
계획된 테이크오버	15초	6-10초	2-3초
계획되지 않은 테이크오버	30초	6-10초	2-3초

체크섬 및 **Oracle** 데이터베이스 무결성

ONTAP 및 지원되는 프로토콜에는 유휴 데이터와 네트워크 네트워크를 통해 전송되는 데이터를 비롯하여 Oracle 데이터베이스 무결성을 보호하는 여러 기능이 포함되어 있습니다.

ONTAP 내의 논리적 데이터 보호는 다음과 같은 세 가지 주요 요구 사항으로 구성됩니다.

- 데이터가 손상되지 않도록 보호해야 합니다.
- 드라이브 장애로부터 데이터를 보호해야 합니다.
- 데이터 변경사항을 손실로부터 보호해야 합니다.

이 세 가지 요구 사항은 다음 섹션에서 설명합니다.

네트워크 손상**:** 체크섬

가장 기본적인 데이터 보호 수준은 데이터와 함께 저장되는 특별한 오류 감지 코드인 체크섬입니다. 네트워크 전송 중 데이터 손상은 체크섬을 사용하여 감지되며 경우에 따라 여러 체크섬을 사용할 수 있습니다.

예를 들어, FC 프레임에는 전송 중에 페이로드가 손상되지 않도록 CRC(Cyclic Redundancy Check)라는 체크섬 유형이 포함되어 있습니다. 송신기는 데이터와 데이터의 CRC를 모두 전송합니다. FC 프레임의 수신기는 수신된

데이터의 CRC를 다시 계산하여 전송된 CRC와 일치하는지 확인합니다. 새로 계산된 CRC가 프레임에 연결된 CRC와 일치하지 않으면 데이터가 손상되고 FC 프레임이 삭제되거나 거부됩니다. iSCSI I/O 작업에는 TCP/IP 및 이더넷 계층에 체크섬이 포함되며, 추가적인 보호를 위해 SCSI 계층에 선택 사항인 CRC 보호 기능이 포함될 수도 있습니다. 와이어의 모든 비트 손상은 TCP 계층 또는 IP 계층에서 감지되어 패킷의 재전송을 초래합니다. FC와 마찬가지로 SCSI CRC의 오류로 인해 작업이 삭제되거나 거부됩니다.

드라이브 손상: 체크섬

또한 체크섬을 사용하여 드라이브에 저장된 데이터의 무결성을 검증합니다. 드라이브에 기록된 데이터 블록은 원래 데이터와 연결된 예측 불가능한 수를 생성하는 체크섬 기능과 함께 저장됩니다. 드라이브에서 데이터를 읽으면 체크섬이 다시 계산되어 저장된 체크섬과 비교됩니다. 일치하지 않으면 데이터가 손상되어 RAID 계층에 의해 복구되어야 합니다.

데이터 손상: 쓰기 손실

감지하기 가장 어려운 유형의 손상 중 하나는 손실되거나 잘못 배치된 쓰기입니다. 쓰기가 확인되면 올바른 위치에 있는 미디어에 기록해야 합니다. 데이터 이동 없는 데이터 손상은 데이터와 함께 저장된 간단한 체크섬을 사용하여 비교적 쉽게 감지할 수 있습니다. 그러나 쓰기가 단순히 손실되는 경우 이전 버전의 데이터가 여전히 존재하고 체크섬이 정확할 수 있습니다. 쓰기가 잘못된 물리적 위치에 배치되면 쓰기가 다른 데이터를 제거했더라도 연결된 체크섬이 저장된 데이터에 대해 다시 한 번 유효합니다.

이 문제에 대한 해결책은 다음과 같습니다.

- 쓰기 작업에는 쓰기를 찾을 위치를 나타내는 메타데이터가 포함되어야 합니다.
- 쓰기 작업에는 버전 식별자가 일부 포함되어 있어야 합니다.

ONTAP에서 블록을 쓰면 해당 블록이 속한 위치에 대한 데이터가 포함됩니다. 후속 읽기에서 블록을 식별하지만 메타데이터에서 위치 456에서 찾은 위치 123에 해당 블록이 속해 있음을 나타내는 경우 쓰기가 잘못 배치된 것입니다.

완전히 손실된 쓰기를 감지하기가 더 어렵습니다. 이 설명은 매우 복잡하지만 기본적으로 ONTAP은 쓰기 작업으로 인해 드라이브의 서로 다른 두 위치에 업데이트가 이루어지도록 메타데이터를 저장하고 있습니다. 쓰기가 손실되면 후속 데이터 읽기와 관련 메타데이터를 읽으면 서로 다른 두 버전 ID가 표시됩니다. 이는 드라이브에서 쓰기가 완료되지 않았음을 나타냅니다.

손실되거나 잘못 배치된 쓰기 손상은 매우 드물지만 드라이브가 계속 증가하고 데이터 세트가 엑사바이트 규모로 증가함에 따라 위험이 증가합니다. 손실된 쓰기 감지 기능은 데이터베이스 워크로드를 지원하는 모든 스토리지 시스템에 포함되어야 합니다.

드라이브 장애: RAID, RAID DP 및 RAID-TEC

드라이브의 데이터 블록이 손상되었거나 전체 드라이브에 장애가 발생하여 완전히 사용할 수 없는 경우 데이터를 다시 구성해야 합니다. 이 작업은 ONTAP에서 패리티 드라이브를 사용하여 수행됩니다. 데이터가 여러 데이터 드라이브에 스트라이핑된 다음 패리티 데이터가 생성됩니다. 원본 데이터와 별도로 저장됩니다.

ONTAP에서는 원래 데이터 드라이브 그룹마다 단일 패리티 드라이브를 사용하는 RAID 4를 사용했습니다. 그 결과, 그룹의 드라이브 중 하나에 장애가 발생하여 데이터가 손실되지 않을 수 있었습니다. 패리티 드라이브에 장애가 발생하면 데이터가 손상되지 않았으며 새 패리티 드라이브를 구성할 수 있습니다. 단일 데이터 드라이브에 장애가 발생하면 나머지 드라이브를 패리티 드라이브와 함께 사용하여 누락된 데이터를 재생성할 수 있습니다.

드라이브 용량이 작을 경우 두 개의 드라이브가 동시에 실패할 가능성이 매우 낮았습니다. 드라이브 용량이 증가함에 따라 드라이브 장애 후 데이터를 재구성하는 데 많은 시간이 필요하게 되었습니다. 이로 인해 두 번째 드라이브 오류로 인해 데이터가 손실되는 기간이 늘어났습니다. 또한 리빌드 프로세스는 나머지 드라이브에서 많은 I/O를 추가로 생성합니다. 드라이브가 노후화되면 추가 로드로 인해 두 번째 드라이브 장애가 발생할 위험도 증가합니다. 마지막으로

RAID 4를 계속 사용하면 데이터 손실 위험이 증가하지 않더라도 데이터 손실의 결과는 더욱 심각해집니다. RAID 그룹 장애 시 손실될 데이터가 많을수록 데이터 복구에 시간이 더 오래 걸리기 때문에 비즈니스 운영이 중단됩니다.

이러한 문제로 인해 NetApp는 RAID 6의 변종인 NetApp RAID DP 기술을 개발하게 되었습니다. 이 솔루션에는 패리티 드라이브가 2개 포함되어 있으므로 RAID 그룹에 있는 두 드라이브가 데이터 손실없이 실패할 수 있습니다. 드라이브의 크기가 계속 커짐에 따라 NetApp는 NetApp RAID-TEC 기술을 개발하여 세 번째 패리티 드라이브를 도입했습니다.

일부 내역 데이터베이스 모범 사례에서는 스트라이프 미러링이라고도 하는 RAID-10을 사용할 것을 권장합니다. 여러 개의 2-디스크 장애 시나리오가 있기 때문에 RAID DP보다 데이터 보호 기능이 떨어지는 반면 RAID DP는 없습니다.

또한 성능 문제로 인해 RAID-10이 RAID-4/5/6 옵션보다 선호됨을 나타내는 몇 가지 과거 데이터베이스 모범 사례가 있습니다. 이러한 권장 사항은 종종 RAID 성능 저하와 관련이 있습니다. 이러한 권장 사항은 일반적으로 정확하지만 ONTAP 내에서 RAID를 구현하는 경우에는 적용되지 않습니다. 성능 문제는 패리티 재생과 관련이 있습니다. 기존 RAID 구현에서 데이터베이스에서 수행하는 일상적인 랜덤 쓰기를 처리하려면 패리티 데이터를 재생성하고 쓰기를 완료하기 위해 여러 디스크 읽기를 수행해야 합니다. 페널티는 쓰기 작업을 수행하는 데 필요한 추가 읽기 IOPS로 정의됩니다.

쓰기 작업은 패리티가 생성된 메모리에서 스테이징된 다음 단일 RAID 스트라이프로 디스크에 기록되므로 ONTAP에서 RAID 패널티가 발생하지 않습니다. 쓰기 작업을 완료하는 데 읽기 작업이 필요하지 않습니다.

요약하면 RAID DP 및 RAID-TEC는 RAID 10과 비교하여 훨씬 더 많은 가용 용량을 제공하고, 드라이브 장애를 방지하며, 성능에 영향을 주지 않습니다.

하드웨어 장애 방지**: NVRAM**

데이터베이스 워크로드를 처리하는 스토리지 어레이는 쓰기 작업을 최대한 빨리 처리해야 합니다. 또한 쓰기 작업은 전원 장애와 같은 예기치 않은 이벤트로 인한 손실로부터 보호해야 합니다. 즉, 쓰기 작업은 적어도 두 위치에 안전하게 저장해야 합니다.

AFF 및 FAS 시스템은 이러한 요구사항을 충족하기 위해 NVRAM을 사용합니다. 쓰기 프로세스는 다음과 같이 작동합니다.

1. 인바운드 쓰기 데이터는 RAM에 저장됩니다.
2. 디스크의 데이터에 필요한 변경 사항은 로컬 및 파트너 노드 모두의 NVRAM으로 저널링됩니다. NVRAM은 쓰기 캐시가 아니라 데이터베이스 재실행 로그와 유사한 저널입니다. 정상적인 상태에서는 읽지 않습니다. I/O 처리 중 전원 장애 발생 후와 같은 복구에만 사용됩니다.
3. 그러면 쓰기가 호스트에 인식됩니다.

이 단계의 쓰기 프로세스는 응용 프로그램 관점에서 완료되며 데이터는 서로 다른 두 위치에 저장되므로 손실로부터 보호됩니다. 최종적으로 변경 사항이 디스크에 기록되지만 이 프로세스는 쓰기 확인 후에 발생하므로 지연 시간에 영향을 주지 않기 때문에 애플리케이션 관점에서 대역 외로 처리됩니다. 이 프로세스는 데이터베이스 로깅과 다시 유사합니다. 데이터베이스 변경 사항은 가능한 한 빨리 재실행 로그에 기록되고 변경 사항은 커밋된 것으로 확인됩니다. 데이터 파일에 대한 업데이트는 훨씬 나중에 수행되며 처리 속도에 직접적인 영향을 주지 않습니다.

컨트롤러 장애가 발생할 경우 파트너 컨트롤러가 필요한 디스크의 소유권을 가져오고 NVRAM에 기록된 데이터를 재생하여 장애가 발생했을 때 전송 중이었던 I/O 작업을 복구합니다.

하드웨어 장애 보호**: NVFAIL**

앞서 설명한 것처럼, 쓰기는 하나 이상의 다른 컨트롤러에서 로컬 NVRAM 및 NVRAM에 로그인되기 전까지는 승인되지 않습니다. 이렇게 하면 하드웨어 장애나 정전이 발생해도 전송 중인 I/O가 손실되지 않습니다 로컬 NVRAM에 장애가 발생하거나 HA 파트너에 대한 연결이 실패하면 전송 중인 이 데이터는 더 이상 미러링되지 않습니다.

로컬 NVRAM에 오류가 보고되면 노드가 종료됩니다. 이 종료를 통해 HA 파트너 컨트롤러로 페일오버됩니다. 오류가 발생한 컨트롤러가 쓰기 작업을 인식하지 못했기 때문에 데이터가 손실되지 않습니다.

페일오버가 강제 적용되지 않는 한 ONTAP는 데이터가 동기화되지 않을 때 페일오버를 허용하지 않습니다. 이러한 방식으로 조건을 강제로 변경하면 데이터가 원래 컨트롤러에 남겨질 수 있으며 데이터 손실이 허용되는 수준임을 알 수 있습니다.

데이터베이스는 디스크에 대규모 내부 데이터 캐시를 유지하기 때문에 페일오버가 강제 적용되는 경우 손상에 특히 취약합니다. 강제 적용 페일오버가 발생하면 이전에 승인되었던 변경사항이 효과적으로 폐기됩니다. 스토리지 어레이의 콘텐츠가 사실상 이전 시간으로 이동하며, 데이터베이스 캐시의 상태는 디스크에 있는 데이터의 상태를 더 이상 반영하지 않습니다.

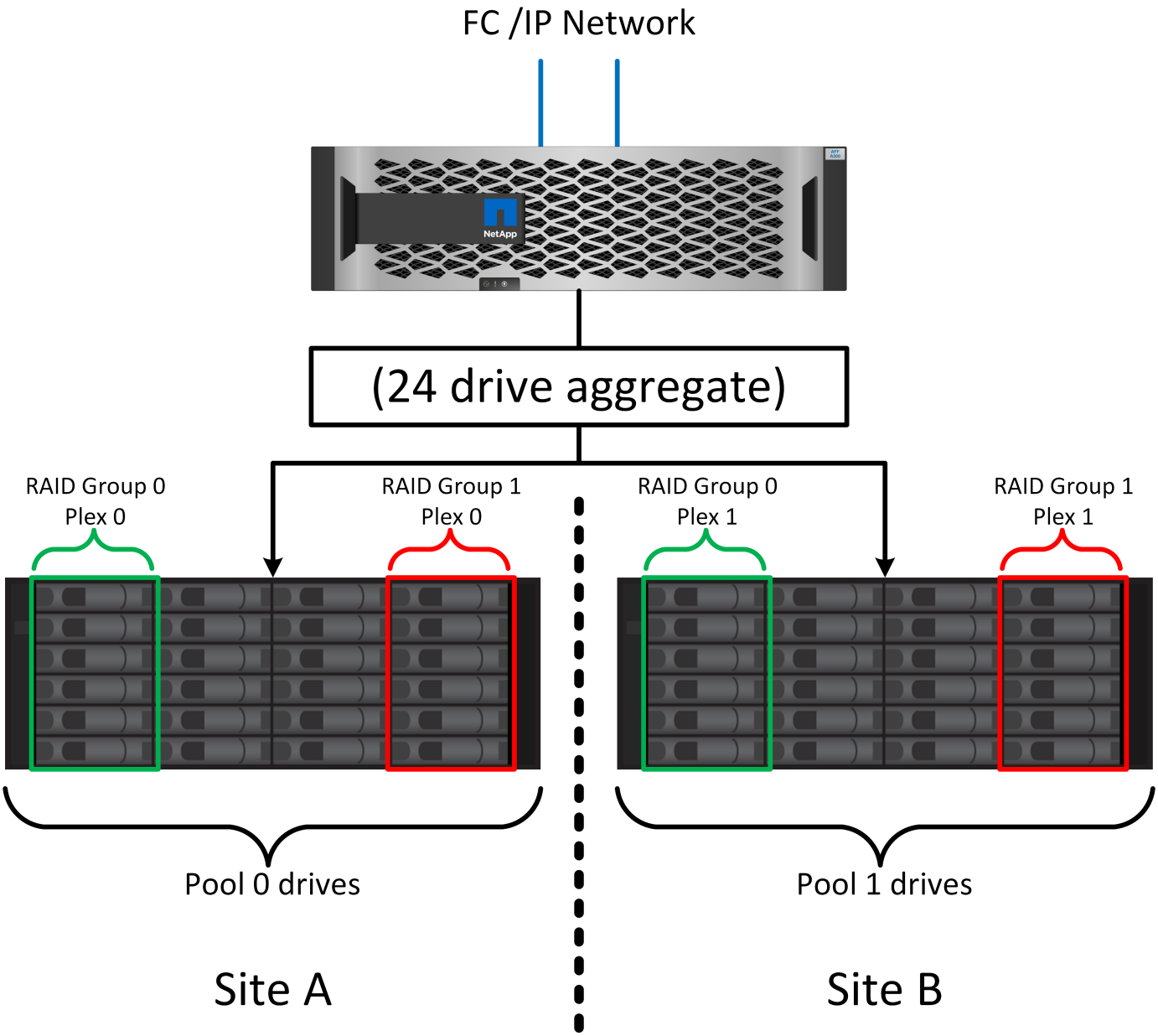
이 상황에서 데이터를 보호하기 위해 ONTAP에서는 NVRAM 장애에 대비하여 특별한 보호를 제공하도록 볼륨을 구성할 수 있습니다. 이 보호 메커니즘이 트리거되면 볼륨이 NVFAIL이라는 상태로 전환됩니다. 이 상태에서는 I/O 오류가 발생하여 오래된 데이터를 사용하지 않도록 애플리케이션이 종료됩니다. 확인된 쓰기가 스토리지 배열에 있어야 하므로 데이터가 손실되지 않아야 합니다.

일반적인 다음 단계는 관리자가 LUN 및 볼륨을 수동으로 다시 온라인 상태로 전환하기 전에 호스트를 완전히 종료하는 것입니다. 이러한 단계에는 일부 작업이 포함될 수 있지만 이 접근 방식은 데이터 무결성을 보장하는 가장 안전한 방법입니다. 모든 데이터에 이 보호가 필요한 것은 아니므로 NVFAIL 동작을 볼륨별로 구성할 수 있습니다.

사이트 및 쉘프 장애 보호: **SyncMirror** 및 플렉스

SyncMirror는 RAID DP 또는 RAID-TEC를 향상하지만 대체하지는 않는 미러링 기술입니다. 2개의 독립적인 RAID 그룹의 콘텐츠를 미러링합니다. 논리적 구성은 다음과 같습니다.

- 드라이브는 위치에 따라 두 개의 풀로 구성됩니다. 하나의 풀은 사이트 A의 모든 드라이브로 구성되고, 두 번째 풀은 사이트 B의 모든 드라이브로 구성됩니다
- 그런 다음 애그리게이트라고 하는 공통 스토리지 풀이 RAID 그룹의 미러링된 세트를 기반으로 생성됩니다. 각 사이트에서 동일한 수의 드라이브가 그려집니다. 예를 들어, 20개 드라이브로 구성된 SyncMirror 애그리게이트는 사이트 A의 드라이브 10개와 사이트 B의 드라이브 10개로 구성됩니다
- 특정 사이트의 각 드라이브 세트는 미러링 사용과 관계없이 하나 이상의 완전히 이중화된 RAID-DP 또는 RAID-TEC 그룹으로 자동으로 구성됩니다. 따라서 사이트 손실 후에도 데이터를 지속적으로 보호할 수 있습니다.



위 그림은 SyncMirror 구성의 예를 보여 줍니다. 24-드라이브 애그리게이트가 사이트 A에 할당된 쉘프의 드라이브 12개와 사이트 B에 할당된 쉘프의 드라이브 12개로 컨트롤러에서 생성되었습니다 드라이브는 두 개의 미러링된 RAID 그룹으로 그룹화되었습니다. RAID Group 0에는 사이트 B의 6개 드라이브 플렉스에 미러링된 사이트 A의 6개 드라이브 플렉스가 포함되어 있습니다 마찬가지로, RAID 그룹 1에는 사이트 B의 6개 드라이브 플렉스에 미러링되는 사이트 A의 6개 드라이브 플렉스가 포함되어 있습니다

SyncMirror는 일반적으로 각 사이트에 하나의 데이터 복사본으로 MetroCluster 시스템에 원격 미러링을 제공하는 데 사용됩니다. 경우에 따라 단일 시스템에서 추가 수준의 이중화를 제공하기 위해 사용되었습니다. 특히, 쉘프 레벨 이중화를 제공합니다. 드라이브 쉘프에는 이미 이중 전원 공급 장치와 컨트롤러가 포함되어 있으며 전반적으로 판금보다 조금 더 크지만, 경우에 따라 추가 보호가 필요할 수 있습니다. 예를 들어, 한 NetApp 고객은 자동차 테스트에 사용되는 모바일 실시간 분석 플랫폼용 SyncMirror를 구축했습니다. 시스템은 독립적인 UPS 시스템의 독립적인 전원 공급으로 공급되는 두 개의 물리적 랙으로 분리되었습니다.

체크섬

체크섬에 대한 주제는 Oracle RMAN 스트리밍 백업을 사용하는 데 익숙한 DBA가 스냅샷 기반 백업으로

마이그레이션하는 데 특히 유용합니다. RMAN은 백업 운영 중에 무결성 점검을 수행하는 기능을 가지고 있습니다. 이것이 유용하기는 하지만 이 기능의 주요 이점은 최신 스토리지 어레이에 사용되지 않는 데이터베이스를 위한 것입니다. Oracle 데이터베이스에 물리적 드라이브를 사용할 때 드라이브가 노후하면 결국 손상이 발생할 확률이 매우 높아지는데, 이 문제는 진정한 스토리지 어레이에서 어레이 기반 체크섬을 통해 해결됩니다.

진정한 스토리지 어레이는 여러 레벨에서 체크섬을 사용하여 데이터 무결성을 보호합니다. IP 기반 네트워크에서 데이터가 손상된 경우 TCP(Transmission Control Protocol) 계층은 패킷 데이터를 거부하고 재전송을 요청합니다. FC 프로토콜은 캡슐화된 SCSI 데이터처럼 체크섬을 포함하고 있습니다. 이것이 어레이에 배치되면 ONTAP에서 RAID 및 체크섬 보호 기능을 수행할 수 있습니다. 대부분의 엔터프라이즈 어레이에서 그렇듯 손상이 발생할 수도 있지만 감지하여 수정할 수 있습니다. 일반적으로 전체 드라이브에 장애가 발생하면 RAID 리빌드가 신속하게 이뤄지며 데이터베이스 무결성은 영향을 받지 않습니다. ONTAP가 드라이브의 데이터가 손상되었음을 의미하는 체크섬 오류를 감지하는 경우가 간혹 있습니다. 그러면 드라이브 작동이 중단되고 RAID 리빌드가 시작됩니다. 여기서도 데이터 무결성은 영향을 받지 않습니다.

또한, Oracle 데이터 파일 및 재실행 로그 아키텍처는 극단적인 환경에서도 최고 수준의 데이터 무결성을 제공하도록 설계되었습니다. 가장 기본적인 레벨에서 Oracle 블록은 거의 모든 I/O에 관한 체크섬과 기본 논리 점검을 포함합니다 Oracle이 충돌하거나 테이블스페이스를 오프라인으로 전환하지 않았다면 데이터는 온전한 상태입니다. 데이터 무결성 점검의 수준은 조정할 수 있으며 쓰기를 확인하도록 Oracle을 구성할 수도 있습니다. 결과적으로 거의 모든 충돌 및 장애 시나리오가 복구될 수 있으며, 극도로 드물긴 하나 복구가 불가능한 상황에서는 손상이 즉시 감지됩니다.

Oracle 데이터베이스를 사용하는 대부분의 NetApp 고객은 스냅샷 기반 백업으로 마이그레이션한 후에 RMAN 및 기타 백업 제품의 사용을 중단합니다. SnapCenter를 통한 블록 레벨 복구를 수행하기 위해 RMAN을 사용할 수 있는 옵션이 여전히 있습니다. 하지만, 일별 기준으로 보면 RMAN, NetBackup 및 기타 제품은 월별 또는 분기별 아카이빙 복사본을 생성하기 위해 가끔씩만 사용됩니다.

어떤 고객은 실행을 선택합니다 `dbv` 정기적으로 기존 데이터베이스에 대한 무결성 검사를 수행합니다. 하지만 NetApp에서는 불필요한 I/O 로드가 생성되기 때문에 이 방식은 권장되지 않습니다. 위에서 설명한 바와 같이 데이터베이스에 이전에 문제가 발생하지 않았다면 의 가능성이 높습니다 `dbv` 문제를 감지하는 것은 거의 0에 가까우며, 이 유틸리티는 네트워크 및 스토리지 시스템에 매우 높은 순차 I/O 로드를 생성합니다. 알려진 Oracle 버그에 관한 노출 같은 손상이 존재한다고 판단할 근거가 있지 않는 한 를 실행할 이유는 없습니다 `dbv`.

백업 및 복구 기초

Oracle 데이터베이스 및 스냅샷 기반 백업

ONTAP에서 Oracle 데이터베이스 데이터 보호의 기반은 NetApp Snapshot 기술입니다.

키 값은 다음과 같습니다.

- * Simplicity. * 스냅샷은 특정 시점의 데이터 컨테이너 내용의 읽기 전용 복사본입니다.
- * 효율성. * 스냅샷은 생성 시점에 공간이 필요하지 않습니다. 공간은 데이터가 변경될 때만 사용됩니다.
- * 관리 효율성. * 스냅샷이 스토리지 OS의 기본 부분이기 때문에 스냅샷을 기반으로 하는 백업 전략은 구성 및 관리가 용이합니다. 스토리지 시스템의 전원이 켜져 있으면 백업을 생성할 준비가 된 것입니다.
- * 확장성. * 파일 및 LUN의 단일 컨테이너에 대해 최대 1024개의 백업을 유지할 수 있습니다. 복잡한 데이터 세트의 경우 일관된 단일 스냅샷 세트로 여러 데이터 컨테이너를 보호할 수 있습니다.
- 볼륨에 1024개의 스냅샷이 포함되어 있는지 여부에 관계없이 성능에 영향을 주지 않습니다.

많은 스토리지 공급업체가 스냅샷 기술을 제공하지만 ONTAP 내 스냅샷 기술은 고유한 특성을 가지고 있으며 엔터프라이즈 애플리케이션 및 데이터베이스 환경에 큰 이점을 제공합니다.

- 스냅샷 복사본은 기본 WAFL(Write Anywhere File Layout)의 일부입니다. 이러한 기술은 애드온 또는 외부 기술이 아닙니다. 따라서 스토리지 시스템이 백업 시스템이므로 관리가 간소화됩니다.
- 스냅샷 복사본은 성능에 영향을 미치지 않습니다. 단, 기본 스토리지 시스템이 가득 찬 스냅샷에 많은 데이터가 저장되는 경우와 같이 일부 에지 사례는 예외입니다.
- "정합성 보장 그룹"이라는 용어는 일관된 데이터 모음으로 관리되는 스토리지 객체 그룹을 지칭하는 데 주로 사용됩니다. 특정 ONTAP 볼륨의 스냅샷은 정합성 보장 그룹 백업을 구성합니다.

ONTAP 스냅샷은 또한 경쟁 기술보다 더 효과적으로 확장할 수 있습니다. 고객은 성능에 영향을 주지 않고 5개, 50개 또는 500개의 스냅샷을 저장할 수 있습니다. 볼륨에 현재 허용되는 최대 스냅숏 수는 1024개입니다. 추가 스냅샷 보존이 필요한 경우 스냅샷을 추가 볼륨에 단계적으로 적용할 수 있는 옵션이 있습니다.

그 결과, ONTAP에서 호스팅되는 데이터 세트를 보호하는 것은 간단하며 확장성이 뛰어납니다. 백업에는 데이터를 이동할 필요가 없으므로 네트워크 전송 속도, 많은 수의 테이프 드라이브 또는 디스크 스테이징 영역의 제한이 아니라 비즈니스 요구에 맞게 백업 전략을 조정할 수 있습니다.

스냅샷이 백업입니까?

스냅샷을 데이터 보호 전략으로 사용하는 것에 대해 자주 묻는 질문 중 하나는 "실제" 데이터와 스냅샷 데이터가 동일한 드라이브에 있다는 사실입니다. 이러한 드라이브가 손실되면 기본 데이터와 백업이 모두 손실됩니다.

이는 유효한 문제입니다. 로컬 스냅샷은 일상적인 백업 및 복구 요구에 사용되며 이러한 측면에서 스냅샷은 백업입니다. NetApp 환경의 모든 복구 시나리오 중 거의 99%가 가장 공격적인 RTO 요구 사항까지도 충족하기 위해 스냅샷에 의존합니다.

하지만 로컬 스냅샷만 사용할 수 있는 백업 전략이 되어서는 안 됩니다. 그렇기 때문에 NetApp에서는 스냅샷을 독립 드라이브 세트에 빠르고 효율적으로 복제할 수 있는 SnapMirror 및 SnapVault 복제 같은 기술을 제공합니다. 스냅샷과 스냅샷 복제를 갖춘 제대로 설계된 솔루션을 사용하면 분기별 아카이브로 테이프 사용을 최소화하거나 완전히 제거할 수 있습니다.

스냅샷 기반 백업

ONTAP Snapshot 복사본을 사용하여 데이터를 보호하는 방법에는 여러 가지가 있으며, 스냅샷은 복제, 재해 복구, 클론 복제를 포함한 다른 ONTAP 기능의 기반입니다. 스냅샷 기술에 대한 전체 설명은 이 문서의 범위를 벗어나지만 다음 섹션에서는 일반적인 개요를 제공합니다.

데이터 세트의 스냅샷을 생성하는 방법에는 두 가지가 있습니다.

- 충돌 시에도 정합성 보장 백업
- 애플리케이션 정합성이 보장되는 백업

데이터 세트의 장애 발생 시 정합성이 보장되는 백업은 단일 시점의 전체 데이터 세트 구조를 캡처하는 것을 의미합니다. 데이터 세트가 단일 NetApp FlexVol 볼륨에 저장된 경우 프로세스는 간단하며 언제든지 스냅샷을 생성할 수 있습니다. 데이터 세트가 여러 볼륨으로 확장되는 경우에는 정합성 보장 그룹(CG) 스냅샷을 생성해야 합니다. CG 스냅샷을 생성하는 옵션에는 NetApp SnapCenter 소프트웨어, 기본 ONTAP 일관성 그룹 기능, 사용자 유지보수 스크립트 등 여러 가지가 있습니다.

충돌 시에도 정합성 보장 백업은 백업 지점 복구가 충분할 때 주로 사용됩니다. 더 세부적인 복구가 필요한 경우 일반적으로 애플리케이션 정합성이 보장되는 백업이 필요합니다.

"애플리케이션 정합성 보장"에서 "정합성 보장"이라는 단어가 잘못된 표현인 경우가 많습니다. 예를 들어 Oracle 데이터베이스를 백업 모드로 설정하는 것을 애플리케이션 정합성 보장 백업이라고 하지만 데이터가 어떤 식으로든

일관되지 않거나 정지되지 않습니다. 백업 내내 데이터가 계속 변경됩니다. 반면 대부분의 MySQL 및 Microsoft SQL Server 백업은 실제로 백업을 실행하기 전에 데이터를 정지합니다. VMware는 특정 파일의 일관성을 유지할 수도 있고 그렇지 않을 수도 있습니다.

정합성 보장 그룹

"정합성 보장 그룹"이란 스토리지 배열이 여러 스토리지 리소스를 단일 이미지로 관리하는 기능을 의미합니다. 예를 들어, 데이터베이스는 10개의 LUN으로 구성될 수 있습니다. 스토리지에서 이러한 10개의 LUN을 일관된 방식으로 백업, 복원 및 복제할 수 있어야 합니다. LUN의 이미지가 백업 시점에 일치하지 않으면 복구할 수 없습니다. 이러한 10개의 LUN을 복제하려면 모든 복제본이 서로 완벽하게 동기화되어야 합니다.

ONTAP에 대해 설명할 때는 "일관성 그룹"이라는 용어가 자주 사용되지 않습니다. 왜냐하면 일관성이 항상 ONTAP 내의 볼륨 및 애그리게이트 아키텍처의 기본 기능이기 때문입니다. 다른 많은 스토리지 시스템은 LUN 또는 파일 시스템을 개별 유닛으로 관리합니다. 그런 다음 데이터 보호를 위해 "정합성 보장 그룹"으로 구성할 수도 있지만 이 작업은 구성에 있어 추가 단계입니다.

ONTAP는 항상 일관된 로컬 및 복제된 데이터 이미지를 캡처할 수 있었습니다. ONTAP 시스템의 다양한 볼륨이 일반적으로 공식적으로 일관성 그룹으로 설명되어 있는 것은 아니지만, 그것이 바로 그러한 볼륨입니다. 해당 볼륨의 스냅샷은 일관성 그룹 이미지이고, 해당 스냅샷에 대한 복원은 일관성 그룹 복원이며, SnapMirror 및 SnapVault에서 모두 일관성 그룹 복제를 제공합니다.

정합성 보장 그룹 스냅샷

일관성 그룹 스냅샷(CG-스냅샷)은 기본 ONTAP 스냅샷 기술의 확장입니다. 표준 스냅샷 작업은 단일 볼륨 내에서 모든 데이터의 일관된 이미지를 생성하지만 여러 볼륨 및 여러 스토리지 시스템에 걸쳐 일관된 스냅샷 세트를 생성해야 하는 경우도 있습니다. 그 결과 하나의 개별 볼륨의 스냅샷과 동일한 방식으로 사용할 수 있는 스냅샷 세트가 생성됩니다. 로컬 데이터 복구에 사용하거나, 재해 복구를 위해 복제하거나, 일관된 단일 유닛으로 복제할 수 있습니다.

CG-스냅샷의 가장 큰 용도는 12개의 컨트롤러를 포함하여 약 1PB의 데이터베이스 환경을 위한 것입니다. 이 시스템에서 생성된 CG 스냅샷이 백업, 복구 및 클론 생성에 사용되었습니다.

대부분의 경우 데이터 세트가 여러 볼륨에 걸쳐 있고 쓰기 순서를 보존해야 하는 경우 선택한 관리 소프트웨어에서 CG 스냅샷이 자동으로 사용됩니다. 이러한 경우 CG-스냅샷의 기술적 세부 사항을 이해할 필요가 없습니다. 그러나 복잡한 데이터 보호 요구 사항이 데이터 보호 및 복제 프로세스를 세부적으로 제어해야 하는 경우도 있습니다. 몇 가지 옵션은 자동화 워크플로우 또는 맞춤형 스크립트를 사용하여 CG-스냅샷 API를 호출하는 것입니다. 최상의 옵션과 CG-스냅샷의 역할을 이해하려면 기술에 대한 자세한 설명이 필요합니다.

CG 스냅샷 세트를 생성하는 프로세스는 2단계로 구성됩니다.

1. 모든 타겟 볼륨에 쓰기 펜싱을 설정합니다.
2. 펜싱된 상태에서 해당 볼륨의 스냅샷을 생성합니다.

쓰기 펜싱은 연속적으로 설정됩니다. 즉, 펜싱 프로세스가 여러 볼륨에 설정되면 나중에 나타나는 볼륨에 계속 커밋되기 때문에 쓰기 I/O가 시퀀스의 첫 번째 볼륨에 고정됩니다. 이는 처음에 쓰기 순서를 보존해야 하는 요구 사항을 위반하는 것처럼 보일 수 있지만, 이는 호스트에서 비동기식으로 실행되며 다른 쓰기에 의존하지 않는 입출력에만 적용됩니다.

예를 들어, 데이터베이스가 많은 비동기식 데이터 파일 업데이트를 발행하고 운영 체제가 I/O를 재주문하고 자체 스케줄러 구성에 따라 업데이트를 완료할 수 있습니다. 애플리케이션 및 운영 체제에서 쓰기 순서를 유지하기 위한 요구 사항을 이미 해제했기 때문에 이러한 유형의 입출력 순서를 보장할 수 없습니다.

반대의 예로 대부분의 데이터베이스 로깅 작업은 동기적입니다. 입출력이 확인되고 이러한 쓰기 순서가 유지되어야 데이터베이스가 더 이상 로그 쓰기를 진행하지 않습니다. 로그 입출력이 펜싱된 볼륨에 도착하면 로그 입출력이 확인되지 않고 애플리케이션이 추가 쓰기를 차단합니다. 마찬가지로 파일 시스템 메타데이터 I/O는 일반적으로

동기식입니다. 예를 들어 파일 삭제 작업은 손실되지 않아야 합니다. xfs 파일 시스템이 있는 운영 체제에서 파일 및 xfs 파일 시스템 메타데이터를 업데이트한 입출력이 펜싱된 볼륨에 있는 해당 파일에 대한 참조를 제거하기 위해 삭제된 경우 파일 시스템 작업이 일시 중지됩니다. 따라서 CG 스냅샷 작업 중에 파일 시스템의 무결성이 보장됩니다.

대상 볼륨에 쓰기 펜싱이 설정된 후에는 스냅샷을 생성할 준비가 됩니다. 볼륨의 상태가 종속 쓰기 관점에서 고정되므로 스냅샷을 정확하게 동시에 생성할 필요가 없습니다. CG-스냅샷을 생성하는 애플리케이션의 결함을 방지하기 위해 초기 쓰기 펜싱에는 구성 가능한 시간 초과가 포함되어 있습니다. 이 시간 초과는 ONTAP가 자동으로 펜싱을 해제하고 정의된 초 후에 쓰기 처리를 재개합니다. 시간 제한 기간이 만료되기 전에 모든 스냅샷이 생성되면 생성된 스냅샷 세트는 유효한 정합성 보장 그룹입니다.

종속 쓰기 순서입니다

기술적 관점에서 정합성 보장 그룹의 핵심은 쓰기 순서, 특히 종속 쓰기 순서를 유지하는 것입니다. 예를 들어, 10개의 LUN에 쓰는 데이터베이스는 이들 모두에 동시에 쓰입니다. 많은 쓰기가 비동기적으로 실행되므로 쓰기 작업이 완료되는 순서는 중요하지 않으며 실제 완료 순서는 운영 체제 및 네트워크 동작에 따라 다릅니다.

데이터베이스에서 추가 쓰기를 진행하려면 디스크에 일부 쓰기 작업이 있어야 합니다. 이러한 중요한 쓰기 작업을 종속 쓰기라고 합니다. 이후의 쓰기 입출력은 디스크에 이러한 쓰기가 있는지에 따라 달라집니다. 이러한 10개 LUN의 모든 스냅샷, 복구 또는 복제는 종속 쓰기 순서가 보장되도록 해야 합니다. 파일 시스템 업데이트는 쓰기 순서 종속 쓰기의 또 다른 예입니다. 파일 시스템 변경 순서를 보존해야 합니다. 그렇지 않으면 전체 파일 시스템이 손상될 수 있습니다.

전략

스냅샷 기반 백업에는 다음과 같은 두 가지 기본 접근 방식이 있습니다.

- 충돌 시에도 정합성 보장 백업
- 스냅샷 보호 핫 백업

데이터베이스의 충돌 시에도 정합성 보장 백업은 데이터 파일, 재실행 로그, 제어 파일을 비롯한 전체 데이터베이스 구조를 단일 지점에서 캡처하는 것을 의미합니다. 데이터베이스를 단일 NetApp FlexVol 볼륨에 저장하면 프로세스가 단순해지며 언제든 스냅샷을 생성할 수 있습니다. 데이터베이스가 여러 볼륨으로 확장되는 경우에는 일관성 그룹(CG) 스냅샷을 생성해야 합니다. CG 스냅샷을 생성하는 옵션에는 NetApp SnapCenter 소프트웨어, 기본 ONTAP 일관성 그룹 기능, 사용자 유지보수 스크립트 등 여러 가지가 있습니다.

스냅샷에서 충돌 시에도 정합성 보장 백업은 백업 지점 복구가 충분할 때 주로 사용됩니다. 경우에 따라 아카이브 로그를 적용할 수 있지만 더 세분화된 시점 복구가 필요한 경우에는 온라인 백업을 적용하는 것이 좋습니다.

스냅샷 기반 온라인 백업의 기본 절차는 다음과 같습니다.

1. 에 데이터베이스를 배치합니다 `backup` 모드를 선택합니다.
2. 데이터 파일을 호스팅하는 모든 볼륨의 스냅샷을 생성합니다.
3. Exit(종료) `backup` 모드를 선택합니다.
4. 명령을 실행합니다 `alter system archive log current` 로그 보관을 수행합니다.
5. 아카이브 로그를 호스팅하는 모든 볼륨의 스냅샷을 생성합니다.

이 절차를 따르면 백업 모드의 데이터 파일과 백업 모드 중에 생성된 주요 아카이브 로그가 포함된 스냅샷 세트가 만들어집니다. 데이터베이스를 복구하는 데에는 두 가지 요구사항이 있는데, 편의를 위해 제어 파일 같은 파일도 보호해야 하지만 데이터 파일과 아카이브 로그를 반드시 보호해야 합니다.

고객마다 전략은 다르겠지만 이 전략은 거의 모든 경우에 결국은 아래에 설명된 동일한 원칙에 기반을 두고 수립됩니다.

스냅샷 기반 복구

Oracle 데이터베이스를 위해 볼륨 레이아웃을 설계할 때 첫 번째 내려야 할 결정은 볼륨 기반 NetApp SnapRestore(VBSR) 기술을 사용할 것이냐입니다.

볼륨 기반 SnapRestore는 볼륨을 이전 시점으로 거의 즉시 되돌릴 수 있게 합니다. 볼륨의 모든 데이터를 되돌릴 수 있기 때문에 VBSR은 모든 사용 사례에는 적합하지 않을 수 있습니다. 예를 들어, 데이터 파일, 재실행 로그, 아카이브 로그를 비롯한 전체 데이터베이스가 단일 볼륨에 저장되고 이 볼륨이 VBSR을 통해 복원되는 경우 최신 아카이브 로그와 재실행 데이터가 삭제되기 때문에 데이터가 손실됩니다.

VBSR은 복원이 필요하지 않습니다. 대부분의 경우 파일을 기반으로 SFSR(Single File SnapRestore)을 사용하거나 스냅샷에서 액티브 파일 시스템으로 파일을 복사하여 데이터베이스를 복원할 수 있습니다.

VBSR은 데이터베이스가 대규모이거나 최대한 빨리 복구해야 할 경우에 적용하는 것이 좋으며 VBSR을 사용할 시 데이터 파일을 격리해야 합니다. NFS 환경에서는 다른 유형의 파일에 의해 손상되지 않은 전용 볼륨에 기존 데이터베이스의 데이터 파일을 저장해야 하며 SAN 환경에서는 전용 FlexVol 볼륨의 전용 LUN에 데이터 파일을 저장해야 합니다. Oracle 자동 스토리지 관리(ASM)와 같은 볼륨 관리자를 사용하는 경우 디스크 그룹도 데이터 파일 전용이어야 합니다.

이런 방식으로 데이터 파일을 격리하면 다른 파일 시스템을 손상시키지 않고 이전 상태로 되돌릴 수 있습니다.

스냅숏 예비 공간입니다

SAN 환경에 있는 Oracle 데이터의 각 볼륨에 대해 를 참조하십시오 `percent-snapshot-space` LUN 환경에서 스냅샷에 대한 공간을 예약하는 것은 유용하지 않으므로 0으로 설정해야 합니다. 부분 예약 공간이 100으로 설정된 경우 LUN이 있는 볼륨의 스냅샷은 전체 데이터의 100% 턴오버를 처리하기 위해 스냅샷 예약 공간을 제외하고 볼륨에서 충분한 여유 공간을 필요로 합니다. 부분 예약이 더 낮은 값으로 설정된 경우 이에 따라 더 적은 양의 여유 공간이 필요하지만 항상 스냅숏 예비 공간이 제외됩니다. 즉, LUN 환경에서 스냅샷 예약 공간이 낭비됩니다.

NFS 환경에는 다음 두 가지 옵션이 있습니다.

- 를 설정합니다 `percent-snapshot-space` 예상되는 스냅샷 공간 소비량을 기준으로 합니다.
- 를 설정합니다 `percent-snapshot-space` 활성 및 스냅샷 공간 소비를 총체적으로 제로화하고 관리합니다.

첫 번째 옵션으로 `percent-snapshot-space` 0이 아닌 값(일반적으로 약 20%)으로 설정됩니다. 그러면 이 공간이 사용자로부터 숨겨집니다. 하지만 이 값은 활용률의 한계를 생성하지 않습니다. 20%가 예약된 데이터베이스에서 턴오버가 30%인 경우 스냅샷 공간은 20% 예약이라는 경계를 넘어 확장할 수 있으며 미예약 공간을 점유할 수 있습니다.

예약을 20%와 같은 값으로 설정할 때 얻을 수 있는 가장 큰 이점은 일부 공간이 스냅샷에 항상 사용 가능한지 확인하는 것입니다. 예를 들어, 20%가 예약된 1TB 볼륨의 경우 데이터베이스 관리자(DBA)는 800GB의 데이터만 저장할 수 있을 것입니다. 이 구성은 스냅샷 소비를 위해 최소 200GB의 공간을 보장합니다.

시기 `percent-snapshot-space` 0으로 설정하면 볼륨의 모든 공간을 최종 사용자가 사용할 수 있어 가시성이 향상됩니다. DBA가 확인했을 때 스냅샷을 활용하는 볼륨이 1TB라면 이 1TB 공간이 액티브 데이터와 스냅샷 턴오버 간에 공유된다는 것을 알아야 합니다.

이 두 옵션 중 최종 사용자가 특별히 선호하는 것은 없습니다.

ONTAP 및 타사 스냅샷

Oracle Doc ID 604683.1은 타사 스냅샷 지원에 관련된 요구사항과 백업 및 복원 작업에 사용할 수 있는 여러 옵션을 설명합니다.

타사 공급업체는 회사의 스냅샷이 다음과 같은 요구 사항을 준수함을 보증해야 합니다.

- 스냅샷이 Oracle에서 권장하는 복원 및 복구 작업에 통합되어야 합니다.
- 스냅샷 지점에서 스냅샷의 데이터베이스 충돌이 일치해야 합니다.
- 쓰기 순서는 각 파일에 대해 스냅샷 내에 보존됩니다.

ONTAP 및 NetApp Oracle 관리 제품은 이러한 요구사항을 준수합니다.

SnapRestore을 사용한 신속한 Oracle 데이터베이스 복구

ONTAP의 빠른 스냅샷 데이터 복원은 NetApp SnapRestore 기술을 통해 수행됩니다.

중요 데이터 세트를 사용할 수 없으면 중요한 비즈니스 운영이 중단됩니다. 테이프는 작동 중지될 수 있으며 디스크 기반 백업에서 복원하는 경우 네트워크를 통해 전송되는 속도가 느려질 수 있습니다. SnapRestore은 데이터 세트를 거의 즉각적으로 복원하여 이러한 문제를 방지합니다. 페타바이트급 데이터베이스도 단 몇 분만에 완벽하게 복원할 수 있습니다.

SnapRestore 파일/LUN 기반과 볼륨 기반에는 두 가지 형식이 있습니다.

- 개별 파일 또는 LUN은 2TB LUN인지 4KB 파일인지에 관계없이 몇 초 이내에 복원할 수 있습니다.
- 파일 또는 LUN의 컨테이너는 10GB 또는 100TB의 데이터이든 몇 초 만에 복원할 수 있습니다.

"파일 또는 LUN 컨테이너"는 일반적으로 FlexVol 볼륨을 의미합니다. 예를 들어, 단일 볼륨에 LVM 디스크 그룹을 구성하는 10개의 LUN이 있거나 볼륨에 1000명의 사용자가 있는 NFS 홈 디렉토리를 저장할 수 있습니다. 각 개별 파일 또는 LUN에 대해 복구 작업을 실행하는 대신 전체 볼륨을 단일 작업으로 복구할 수 있습니다. 이 프로세스는 FlexGroup 또는 ONTAP 일관성 그룹과 같은 여러 볼륨이 포함된 스케일아웃 컨테이너에도 작동합니다.

SnapRestore이 빠르고 효율적으로 작동하는 이유는 기본적으로 특정 시점에 볼륨 콘텐츠에 대한 병렬 읽기 전용 뷰인 스냅샷의 특성 때문입니다. 활성 블록은 변경할 수 있는 실제 블록이지만 스냅샷은 스냅샷이 생성된 시점의 파일 및 LUN을 구성하는 블록 상태에 대한 읽기 전용 뷰입니다.

ONTAP에서는 스냅샷 데이터에 대한 읽기 전용 액세스만 허용하지만, SnapRestore를 사용하여 데이터를 다시 활성화할 수 있습니다. 스냅샷은 데이터의 읽기/쓰기 뷰로 다시 설정되며 데이터를 이전 상태로 되돌립니다. SnapRestore는 볼륨 또는 파일 레벨에서 작동할 수 있습니다. 이 기술은 본질적으로 같으며 몇 가지 사소한 행동 차이가 있습니다.

Volume SnapRestore를 참조하십시오

볼륨 기반 SnapRestore는 전체 데이터 볼륨을 이전 상태로 되돌립니다. 이 작업은 데이터를 이동할 필요가 없습니다. 즉, API 또는 CLI 작업을 처리하는 데 몇 초가 걸릴 수 있지만 복원 프로세스가 기본적으로 즉각적입니다. 1GB의 데이터를 복원하는 것은 1PB의 데이터를 복원하는 것보다 더 복잡하거나 시간이 많이 소요됩니다. 이 기능 은 많은 엔터프라이즈 고객이 ONTAP 스토리지 시스템으로 마이그레이션하는 주된 이유입니다. 또한 가장 큰 데이터 세트에 대해 몇 초 단위의 RTO를 제공합니다.

볼륨 기반 SnapRestore의 한 가지 단점은 볼륨 내의 변경 사항이 시간 경과에 따라 누적된다는 사실에 의해 발생합니다. 따라서 각 스냅샷 및 활성 파일 데이터는 해당 시점까지 이어지는 변경 사항에 따라 달라집니다. 볼륨을 이전 상태로 되돌리면 데이터에 적용된 이후의 모든 변경 내용이 취소됩니다. 그러나 이는 이후에 생성된 스냅샷을 포함한다는 점은 그만큼 분명하지 않습니다. 이것이 항상 바람직한 것은 아닙니다.

예를 들어, 데이터 보존 SLA는 30일 야간 백업을 지정할 수 있습니다. 볼륨 SnapRestore를 사용하여 5일 전에 생성된 스냅샷으로 데이터 세트를 복구하면 지난 5일 동안 생성된 모든 스냅샷이 삭제되어 SLA를 위반하게 됩니다.

이 제한 사항을 해결하는 데 사용할 수 있는 여러 가지 옵션이 있습니다.

1. 전체 볼륨의 SnapRestore를 수행하는 것이 아니라 이전 스냅샷에서 데이터를 복사할 수 있습니다. 이 방법은 보다 작은 데이터 집합에 가장 적합합니다.
2. 스냅샷은 복구하지 않고 클론을 생성할 수 있습니다. 이 접근 방식의 제한 사항은 소스 스냅샷이 클론에 종속된다는 것입니다. 따라서 클론이 삭제되거나 독립 볼륨으로 분할되지 않는 한 삭제할 수 없습니다.
3. 파일 기반 SnapRestore 사용:

파일 **SnapRestore**

파일 기반 SnapRestore는 보다 세부적인 스냅샷 기반 복원 프로세스입니다. 전체 볼륨의 상태를 되돌리는 대신 개별 파일 또는 LUN의 상태를 되돌립니다. 스냅샷을 삭제할 필요가 없으며, 이 작업으로 이전 스냅샷에 대한 종속성이 생성되지 않습니다. 파일 또는 LUN을 활성 볼륨에서 즉시 사용할 수 있습니다.

파일 또는 LUN의 SnapRestore 복원 중에 데이터를 이동할 필요가 없습니다. 그러나 파일 또는 LUN의 기본 블록이 이제 스냅샷과 활성 볼륨 모두에 존재한다는 사실을 반영하려면 일부 내부 메타데이터를 업데이트해야 합니다. 성능에는 영향을 미치지 않겠지만 이 프로세스는 완료될 때까지 스냅샷 생성을 차단합니다. 처리 속도는 복원된 파일의 총 크기에 따라 약 5GBps(시간당 18TB)입니다.

Oracle 데이터베이스 온라인 백업

백업 모드에서 Oracle 데이터베이스를 보호하고 복구하려면 두 세트의 데이터가 필요합니다. 이것이 유일한 Oracle 백업 옵션은 아니지만 가장 일반적입니다.

- 백업 모드의 데이터 파일 스냅샷
- 데이터 파일이 백업 모드일 때 생성된 아카이브 로그입니다

커밋된 모든 트랜잭션을 포함하여 완전한 복구가 필요한 경우 세 번째 항목이 필요합니다.

- 현재 redo 로그 집합입니다

온라인 백업의 복구를 유도하는 방법에는 여러 가지가 있습니다. 많은 고객은 ONTAP CLI를 사용한 다음 Oracle RMAN 또는 sqlplus를 사용하여 복구를 완료함으로써 스냅샷을 복구합니다. 이러한 현상은 데이터베이스 복구 가능성과 빈도가 매우 낮고 숙련된 DBA가 복구 절차를 처리하는 대규모 운영 환경에서 특히 흔합니다. NetApp SnapCenter와 같은 솔루션에는 완벽한 자동화를 위해 명령줄 및 그래픽 인터페이스 모두를 지원하는 Oracle 플러그인이 포함되어 있습니다.

일부 대규모 고객은 예약된 스냅샷을 준비하는 과정에서 특정 시간에 데이터베이스를 백업 모드로 전환하도록 호스트에 기본 스크립트를 구성하여 보다 간단한 접근 방식을 취했습니다. 예를 들어, 명령을 예약합니다 `alter database begin backup` 23:58에 `alter database end backup` 00:02에 스냅샷을 예약한 다음 자정에 스토리지 시스템에서 직접 스냅샷을 예약합니다. 그 결과 외부 소프트웨어 또는 라이센스가 필요 없는 간단하고 확장성이 뛰어난 백업 전략을 구축할 수 있습니다.

데이터 레이아웃

가장 간단한 레이아웃은 데이터 파일을 하나 이상의 전용 볼륨으로 분리하는 것입니다. 다른 파일 형식으로 오염되지 않아야 합니다. 이는 중요한 재실행 로그, 제어 파일 또는 아카이브 로그를 삭제하지 않고 SnapRestore 작업을 통해 데이터 파일 볼륨을 신속하게 복원할 수 있도록 보장하기 위한 것입니다.

SAN은 전용 볼륨 내의 데이터 파일 격리에 대해서도 유사한 요구사항을 가지고 있습니다. Microsoft Windows 같은

운영 체제에서 단일 볼륨에는 각각 NTFS 파일 시스템이 포함된 여러 데이터 파일 LUN이 포함될 수 있습니다. 다른 운영 체제에는 일반적으로 논리적 볼륨 관리자가 있습니다. 예를 들어, Oracle ASM을 사용할 경우 가장 간단한 옵션은 ASM 디스크 그룹의 LUN을 하나의 볼륨으로 백업 및 복원할 수 있는 단일 볼륨으로 제한하는 것입니다. 성능 또는 용량 관리를 위해 추가 볼륨이 필요한 경우 새 볼륨에 추가 디스크 그룹을 생성하면 관리가 더 간단해집니다.

이러한 지침을 따를 경우 정합성 보장 그룹 스냅샷을 수행할 필요 없이 스토리지 시스템에서 스냅샷을 직접 예약할 수 있습니다. Oracle 백업에는 데이터 파일을 동시에 백업할 필요가 없기 때문입니다. 온라인 백업 절차는 몇 시간 내에 테이프로 천천히 스트리밍될 때 데이터 파일을 계속해서 업데이트할 수 있도록 설계되었습니다.

여러 볼륨에 분산된 ASM 디스크 그룹을 사용하는 것과 같은 상황에서는 문제가 발생합니다. 이 경우 ASM 메타데이터가 모든 구성 볼륨에서 일관되도록 CG-스냅샷을 수행해야 합니다.

- 주의: * ASM을 확인합니다 `spfile` 및 `passwd` 파일이 데이터 파일을 호스팅하는 디스크 그룹에 없습니다. 이로 인해 데이터 파일과 데이터 파일만 선택적으로 복원할 수 없습니다.

로컬 복구 절차 **- NFS**

이 절차는 수동으로 또는 SnapCenter와 같은 응용 프로그램을 통해 실행할 수 있습니다. 기본 절차는 다음과 같습니다.

1. 데이터베이스를 종료합니다.
2. 원하는 복원 지점 바로 전에 데이터 파일 볼륨을 스냅샷으로 복구합니다.
3. 원하는 지점으로 아카이브 로그를 재생합니다.
4. 전체 복구가 필요한 경우 현재 redo 로그를 재생합니다.

이 절차에서는 활성 파일 시스템에 원하는 아카이브 로그가 여전히 존재한다고 가정합니다. 그렇지 않은 경우 아카이브 로그를 복원해야 합니다. 그렇지 않으면 RMAN/sqlplus를 스냅샷 디렉토리의 데이터로 리디렉션할 수 있습니다.

또한 데이터베이스의 규모가 작은 경우 최종 사용자가 에서 직접 데이터 파일을 복구할 수 있습니다 `.snapshot` 자동화 툴 또는 스토리지 관리자의 도움 없이 디렉토리를 실행하여 `snaprestore` 명령.

로컬 복구 절차 **- SAN**

이 절차는 수동으로 또는 SnapCenter와 같은 응용 프로그램을 통해 실행할 수 있습니다. 기본 절차는 다음과 같습니다.

1. 데이터베이스를 종료합니다.
2. 데이터 파일을 호스팅하는 디스크 그룹을 중지합니다. 절차는 선택한 논리적 볼륨 관리자에 따라 다릅니다. ASM을 사용할 경우 이 프로세스에서는 디스크 그룹을 마운트 해제해야 합니다. Linux에서는 파일 시스템을 마운트 해제하고 논리적 볼륨 및 볼륨 그룹을 비활성화해야 합니다. 목표는 복구할 타겟 볼륨 그룹의 모든 업데이트를 중지하는 것입니다.
3. 원하는 복원 지점 바로 전에 데이터 파일 디스크 그룹을 스냅샷으로 복원합니다.
4. 새로 복구된 디스크 그룹을 다시 활성화합니다.
5. 원하는 지점으로 아카이브 로그를 재생합니다.
6. 전체 복구가 필요한 경우 모든 재실행 로그를 재생합니다.

이 절차에서는 활성 파일 시스템에 원하는 아카이브 로그가 여전히 존재한다고 가정합니다. 그렇지 않은 경우 아카이브 로그 LUN을 오프라인으로 전환하고 복원을 수행하여 아카이브 로그를 복원해야 합니다. 아카이브 로그를 전용 볼륨으로 분할하는 것이 유용한 예이기도 합니다. 아카이브 로그가 재실행 로그와 볼륨 그룹을 공유하는 경우 전체 LUN 세트를 복원하기 전에 재실행 로그를 다른 위치에 복사해야 합니다. 이 단계는 최종 기록된 트랜잭션의 손실을 방지합니다.

Oracle Database Storage Snapshot Optimized Backups의 약어입니다

데이터베이스를 핫 백업 모드로 설정할 필요가 없기 때문에 Oracle 12c가 출시되었을 때 스냅샷 기반 백업 및 복구가 더욱 간편해졌습니다. 그 결과 스토리지 시스템에서 직접 스냅샷 기반 백업을 예약하고 전체 또는 시점 복구를 수행하는 기능을 유지할 수 있습니다.

핫 백업 복구 절차는 DBA에게 더 익숙하지만 데이터베이스가 핫 백업 모드인 동안 생성되지 않은 스냅샷을 사용할 수 있는 것은 오래되었습니다. Oracle 10g 및 11g를 복구하는 동안 데이터베이스의 일관성을 유지하기 위해 추가 수동 단계가 필요했습니다. Oracle 12c를 사용하면 `sqlplus` 및 `rman` 핫 백업 모드에 있지 않은 데이터 파일 백업에서 아카이브 로그를 재생하는 추가 로직을 포함합니다.

앞에서 설명한 것처럼 스냅샷 기반 핫 백업을 복구하려면 두 가지 데이터 세트가 필요합니다.

- 백업 모드에서 생성된 데이터 파일의 스냅샷입니다
- 데이터 파일이 핫 백업 모드일 때 생성되는 아카이브 로그

복구 중에 데이터베이스는 데이터 파일에서 메타데이터를 읽어 복구에 필요한 아카이브 로그를 선택합니다.

스토리지 스냅샷으로 최적화된 복구에서는 동일한 결과를 얻기 위해 약간 다른 데이터 세트가 필요합니다.

- 데이터 파일의 스냅샷과 스냅샷이 생성된 시간을 식별하는 방법입니다
- 최신 데이터 파일 체크포인트 시점부터 스냅샷의 정확한 시간까지 로그를 아카이빙합니다

복구 중에 데이터베이스는 데이터 파일에서 메타데이터를 읽어 필요한 초기 아카이브 로그를 식별합니다. 전체 또는 특정 시점 복구를 수행할 수 있습니다. 시점 복구를 수행할 때는 데이터 파일의 스냅샷 시간을 알아야 합니다. 지정된 복구 지점은 스냅샷 생성 시간 이후여야 합니다. NetApp에서는 클럭 변동을 고려하여 스냅샷 시간에 최소 몇 분을 추가하는 것이 좋습니다.

자세한 내용은 Oracle 12c 설명서의 다양한 릴리스에서 제공되는 "Recovery using Storage Snapshot Optimization(스토리지 스냅샷 최적화를 사용한 복구)" 항목에 대한 Oracle 설명서를 참조하십시오. 또한 Oracle 타사 스냅샷 지원에 대해서는 Oracle Document ID Doc ID 604683.1을 참조하십시오.

데이터 레이아웃

가장 간단한 레이아웃은 데이터 파일을 하나 이상의 전용 볼륨으로 분리하는 것입니다. 다른 파일 형식으로 오염되지 않아야 합니다. 이는 중요한 redo 로그, 제어 파일 또는 아카이브 로그를 삭제하지 않고 SnapRestore 작업을 통해 데이터 파일 볼륨을 신속하게 복원할 수 있도록 하기 위한 것입니다.

SAN은 전용 볼륨 내의 데이터 파일 격리에 대해서도 유사한 요구사항을 가지고 있습니다. Microsoft Windows 같은 운영 체제에서 단일 볼륨에는 각각 NTFS 파일 시스템이 포함된 여러 데이터 파일 LUN이 포함될 수 있습니다. 다른 운영 체제에서는 일반적으로 논리적 볼륨 관리자도 있습니다. 예를 들어, Oracle ASM을 사용할 경우 가장 간단한 옵션은 디스크 그룹을 하나의 볼륨으로 백업 및 복원할 수 있는 단일 볼륨으로 제한하는 것입니다. 성능 또는 용량 관리를 위해 추가 볼륨이 필요한 경우 새 볼륨에 추가 디스크 그룹을 생성하면 관리가 더 쉬워집니다.

이러한 지침을 따를 경우 정합성 보장 그룹 스냅샷을 수행할 필요 없이 ONTAP에서 스냅샷을 직접 예약할 수 있습니다. 이유는 스냅샷 최적화 백업에는 데이터 파일을 동시에 백업할 필요가 없기 때문입니다.

여러 볼륨에 분산된 ASM 디스크 그룹과 같은 상황에서는 문제가 발생합니다. 이 경우 ASM 메타데이터가 모든 구성 볼륨에서 일관되도록 CG-스냅샷을 수행해야 합니다.

[참고] ASM spfile 및 passwd 파일이 데이터 파일을 호스팅하는 디스크 그룹에 없는지 확인합니다. 이로 인해 데이터

파일과 데이터 파일만 선택적으로 복원할 수 없습니다.

로컬 복구 절차 **- NFS**

이 절차는 수동으로 또는 SnapCenter와 같은 응용 프로그램을 통해 실행할 수 있습니다. 기본 절차는 다음과 같습니다.

1. 데이터베이스를 종료합니다.
2. 원하는 복원 지점 바로 전에 데이터 파일 볼륨을 스냅샷으로 복구합니다.
3. 원하는 지점으로 아카이브 로그를 재생합니다.

이 절차에서는 활성 파일 시스템에 원하는 아카이브 로그가 여전히 존재한다고 가정합니다. 그렇지 않은 경우, 또는 아카이브 로그를 복원해야 합니다 `rman` 또는 `sqlplus` 의 데이터로 이동할 수 있습니다 `.snapshot` 디렉토리.

또한 데이터베이스의 규모가 작은 경우 최종 사용자가 에서 직접 데이터 파일을 복구할 수 있습니다 `.snapshot` 디렉토리에는 자동화 툴 또는 스토리지 관리자의 도움 없이 SnapRestore 명령을 실행할 수 있습니다.

로컬 복구 절차 **- SAN**

이 절차는 수동으로 또는 SnapCenter와 같은 응용 프로그램을 통해 실행할 수 있습니다. 기본 절차는 다음과 같습니다.

1. 데이터베이스를 종료합니다.
2. 데이터 파일을 호스팅하는 디스크 그룹을 중지합니다. 절차는 선택한 논리적 볼륨 관리자에 따라 다릅니다. ASM을 사용할 경우 이 프로세스에서는 디스크 그룹을 마운트 해제해야 합니다. Linux에서는 파일 시스템을 마운트 해제해야 하며 논리적 볼륨 및 볼륨 그룹이 비활성화됩니다. 목표는 복구할 타겟 볼륨 그룹의 모든 업데이트를 중지하는 것입니다.
3. 원하는 복원 지점 바로 전에 데이터 파일 디스크 그룹을 스냅샷으로 복원합니다.
4. 새로 복구된 디스크 그룹을 다시 활성화합니다.
5. 원하는 지점으로 아카이브 로그를 재생합니다.

이 절차에서는 활성 파일 시스템에 원하는 아카이브 로그가 여전히 존재한다고 가정합니다. 그렇지 않은 경우 아카이브 로그 LUN을 오프라인으로 전환하고 복원을 수행하여 아카이브 로그를 복원해야 합니다. 아카이브 로그를 전용 볼륨으로 분할하는 것이 유용한 예이기도 합니다. 아카이브 로그가 재실행 로그와 볼륨 그룹을 공유하는 경우, 최종 기록된 트랜잭션이 손실되지 않도록 전체 LUN 세트를 복원하기 전에 재실행 로그를 다른 곳에 복사해야 합니다.

전체 복구 예

데이터 파일이 손상되었거나 제거되었으며 전체 복구가 필요한 것으로 가정합니다. 이렇게 하는 절차는 다음과 같습니다.

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover automatic;
Media recovery complete.
SQL> alter database open;
Database altered.
SQL>
```

특정 시점 복구 예

전체 복구 절차는 단일 명령입니다. `recover automatic`.

시점 복구가 필요한 경우 스냅샷의 타임스탬프를 알고 있어야 하며 다음과 같이 식별할 수 있습니다.

```
Cluster01::> snapshot show -vserver vserver1 -volume NTAP_oradata -fields
create-time
vserver   volume        snapshot   create-time
--------  ------------  ---------  ------------------------
vserver1  NTAP_oradata  my-backup  Thu Mar 09 10:10:06 2017
```

스냅샷 생성 시간은 3월 9일 및 10:10:06으로 표시됩니다. 안전을 위해 스냅샷 시간에 1분이 추가됩니다.

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover database until time '09-MAR-2017 10:44:15' snapshot time '09-
MAR-2017 10:11:00';
```

이제 복구가 시작됩니다. 또한 스냅샷 시간을 10:11:00, 기록된 시간 1분 후 가능한 클럭 편차를 계산하고 목표 복구 시간을 10:44로 지정했습니다. 그런 다음 sqlplus는 원하는 복구 시간인 10:44에 도달하는 데 필요한 아카이브 로그를 요청합니다.

```
ORA-00279: change 551760 generated at 03/09/2017 05:06:07 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_31_930813377.dbf
ORA-00280: change 551760 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 552566 generated at 03/09/2017 05:08:09 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_32_930813377.dbf
ORA-00280: change 552566 for thread 1 is in sequence #32
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 553045 generated at 03/09/2017 05:10:12 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_33_930813377.dbf
ORA-00280: change 553045 for thread 1 is in sequence #33
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 753229 generated at 03/09/2017 05:15:58 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_34_930813377.dbf
ORA-00280: change 753229 for thread 1 is in sequence #34
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Log applied.
Media recovery complete.
SQL> alter database open resetlogs;
Database altered.
SQL>
```

를 사용하여 스냅샷을 사용하여 데이터베이스 복구를 완료합니다 `recover automatic` 명령에는 특정 라이센스가 필요하지 않지만 를 사용하여 시점 복구가 필요합니다 `snapshot time` Oracle Advanced Compression 라이센스가 필요합니다.

Oracle 데이터베이스 관리 및 자동화 툴

Oracle 데이터베이스 환경에서 ONTAP의 기본적인 가치는 즉각적인 스냅샷 복사본, 간단한 SnapMirror 복제, 효율적인 FlexClone 볼륨 생성 등의 핵심 ONTAP 기술에서 나오는 것입니다.

이러한 핵심 기능을 ONTAP에서 직접 간단히 구성하여 요구사항을 충족하는 경우도 있지만, 더 복잡한 요구사항에는 오케스트레이션 계층이 필요합니다.

SnapCenter

SnapCenter은 NetApp의 대표적인 데이터 보호 제품입니다. 매우 낮은 수준에서 SnapManager 제품은 데이터베이스 백업을 수행하는 방법이라는 측면에서 볼 때 NetApp 제품과 비슷하지만, 처음부터 NetApp 스토리지 시스템의 데이터

보호 관리에 대한 단일 창 방식을 제공하도록 제작되었습니다.

SnapCenter에는 스냅샷 기반 백업 및 복원, SnapMirror 및 SnapVault 복제와 같은 기본 기능과 대기업에서 규모에 따라 운영하는 데 필요한 기타 기능이 포함되어 있습니다. 이러한 고급 기능에는 확장된 역할 기반 액세스 제어(RBAC) 기능, 타사 오케스트레이션 제품과 통합하기 위한 RESTful API, 데이터베이스 호스트에서 SnapCenter 플러그인의 무중단 중앙 관리, 클라우드급 환경에 맞게 설계된 사용자 인터페이스가 포함됩니다.

휴식

ONTAP에는 풍부한 RESTful API 세트도 포함되어 있습니다. 따라서 타사 공급업체에서는 ONTAP과 긴밀히 통합되는 데이터 보호 및 기타 관리 애플리케이션을 구축할 수 있습니다. 또한 RESTful API는 자체 자동화 워크플로우와 유틸리티를 생성하려는 고객이 손쉽게 사용할 수 있습니다.