SnapCenter를 사용한 SAP HANA 백업 및 복구

NetApp solutions for SAP

NetApp
February 25, 2026

목차

SnapCenter를 사용한 SAP HANA 백업 및 복구

ONTAP, Azure NetApp Files 및 FSx for ONTAP 에서 SnapCenter 사용하여 SAP HANA 시스템 보호

스냅샷 기반 백업 및 데이터 복제를 사용하여 NetApp SnapCenter 로 SAP HANA 시스템을 보호하세요. 이 솔루션은 ONTAP AFF 및 ASA 시스템, Azure NetApp Files, Amazon FSx for ONTAP 의 SAP HANA 시스템에 대한 SnapCenter 구성 및 운영 모범 사례를 다루며 여기에는 백업 전략, 일관성 검사, 복구 워크플로가 포함됩니다.

저자: 닐스 바우어, NetApp

SAP 시스템 새로 고침 작업 및 SAP HANA 시스템 복제에 대한 추가적인 사용 사례별 세부 정보는 다음에서 확인할 수 있습니다.

- "SnapCenter를 사용하여 SAP HANA 시스템 복사 및 클론 작업 자동화"
- "SAP HANA 시스템 복제 - SnapCenter를 사용한 백업 및 복구"

SnapCenter 데이터 보호와 NetApp SnapMirror Active Sync를 결합하는 모범 사례는 다음에서 설명합니다.

- "SnapCenter, SnapMirror Active Sync 및 VMware Metro Storage Cluster를 통한 SAP HANA 데이터 보호 및 고가용성"

추가 플랫폼별 모범 사례 문서는 다음에서 제공됩니다.

- "VMware VMFS 및 NetApp ASA 시스템을 사용한 SnapCenter 통한 SAP HANA 데이터 보호"
- "NetApp ONTAP용 Amazon FSx 기반 SAP HANA - SnapCenter를 통한 백업 및 복구"
- "Azure NetApp Files with SnapCenter의 SAP HANA 데이터 보호(블로그 및 비디오)"
- "Azure NetApp Files with SnapCenter에서 SAP 시스템 업데이트 및 클로닝 작업(블로그 및 비디오)"

NetApp Snapshot 기술을 사용한 SAP HANA 데이터 보호에 대해 알아보세요

NetApp Snapshot 기술이 데이터베이스 크기에 관계없이 몇 분 안에 완료되는 백업을 통해 SAP HANA 데이터베이스를 보호하는 방법을 알아보세요. 스냅샷 복사본, 빠른 복구를 위한 SnapRestore , 보조 보호를 위한 SnapVault 또는 Azure NetApp Files 백업을 사용한 복제를 활용한 백업 및 복구 전략에 대해 알아보세요.

오늘날의 기업들은 SAP 애플리케이션에 대해 지속적이고 중단 없는 가용성을 요구합니다. 그들은 일관된 성능 수준을 기대하며, 끊임없이 증가하는 데이터 볼륨과 시스템 백업과 같은 일상적인 유지 관리 업무의 필요성에 대처하기 위해 자동화된 일상 업무가 필요합니다. SAP 데이터베이스 백업을 수행하는 것은 중요한 작업이며, 프로덕션 SAP 시스템의 성능에 상당한 영향을 미칠 수 있습니다.

백업해야 할 데이터 양은 늘어나는 반면 백업 창은 줄어들고 있습니다. 따라서 비즈니스 프로세스에 최소한의 영향만 미치면서 백업을 수행할 수 있는 시기를 찾는 것은 어렵습니다. SAP 시스템을 복구하고 복원하는 데 필요한 시간은 중요한 문제입니다. 비즈니스 비용을 줄이기 위해 SAP 운영 및 비운영 시스템의 가동 중지 시간을 최소화해야 하기

때문입니다.

스냅샷 백업을 사용한 백업 및 복구

NetApp Snapshot 기술을 사용하면 몇 분 안에 데이터베이스 백업을 만들 수 있습니다. 스냅샷 복사본을 만드는 데 필요한 시간은 스냅샷 복사본이 스토리지 플랫폼에서 물리적 데이터 블록을 이동하지 않기 때문에 데이터베이스 크기와 무관합니다. 또한, 스냅샷 기술을 사용해도 모든 작업이 스토리지 시스템에서 실행되므로 라이브 SAP 시스템의 성능에 영향을 미치지 않습니다. 따라서 대화가 가장 많은 기간이나 일괄 작업 기간을 고려하지 않고도 스냅샷 복사본 생성을 예약할 수 있습니다. NetApp 고객의 SAP는 일반적으로 하루 중 여러 번의 온라인 스냅샷 백업을 예약합니다. 예를 들어, 6시간마다 백업하는 것이 일반적입니다. 이러한 스냅샷 백업은 일반적으로 장기 보존을 위해 제거되거나 더 저렴한 스토리지로 계층화되기 전에 기본 스토리지 시스템에 3~5일 동안 보관됩니다.

스냅샷 복사본은 복원 및 복구 작업에도 주요 이점을 제공합니다. 복원 작업은 백업 상태에 따라 파일 시스템의 데이터를 다시 가져옵니다. 복구 작업은 데이터베이스 로그 백업을 사용하여 데이터베이스 상태를 특정 시점으로 롤포워드하는 데 사용됩니다.

NetApp SnapRestore 기술을 사용하면 현재 사용 가능한 스냅샷 백업을 기반으로 전체 데이터베이스 또는 데이터베이스의 일부만 복원할 수 있습니다. 복원 과정은 데이터베이스 크기에 관계없이 몇 초 안에 완료됩니다. 하루 동안 여러 개의 온라인 스냅샷 백업을 만들 수 있으므로, 하루에 한 번 백업하는 기존 방식에 비해 복구 프로세스에 필요한 시간이 크게 줄어듭니다. 최대 24시간이 아닌 몇 시간 전의 스냅샷 복사본으로 복원을 수행할 수 있으므로 전방 복구 중에 적용해야 하는 트랜잭션 로그가 줄어듭니다. 기존 스트리밍 백업에 비해 복원 및 복구에 필요한 시간이 크게 단축됩니다.

스냅샷 백업은 활성 온라인 데이터와 동일한 디스크 시스템에 저장되므로 NetApp 스냅샷 복사 백업을 보조 위치에 대한 백업을 대체하는 것이 아니라 보완하는 용도로 사용할 것을 권장합니다. 대부분의 복원 및 복구 작업은 기본 스토리지 시스템의 SnapRestore 사용하여 관리됩니다. 보조 위치에서 복원하는 작업은 스냅샷 복사본이 들어 있는 기본 스토리지 시스템을 사용할 수 없는 경우에만 필요합니다. 기본 저장소에서 더 이상 사용할 수 없는 백업을 복원해야 하는 경우에도 보조 백업을 사용할 수 있습니다.

보조 위치에 대한 백업은 기본 저장소에 생성된 스냅샷 복사본을 기반으로 합니다. 따라서 SAP 데이터베이스 서버와 네트워크에 부하를 발생시키지 않고 기본 스토리지 시스템에서 직접 데이터를 읽을 수 있습니다. 기본 저장소는 보조 저장소와 직접 통신하고 SnapVault 또는 ANF 백업 기능을 사용하여 백업 데이터를 대상에 복제합니다.

SnapVault 와 ANF 백업은 기존 백업에 비해 상당한 이점을 제공합니다. 모든 데이터가 소스에서 목적지로 전송되는 초기 데이터 전송 후, 이후의 모든 백업은 변경된 블록만 보조 저장소로 복제합니다. 따라서 기본 스토리지 시스템의 부하와 전체 백업에 필요한 시간이 크게 줄어듭니다. 변경된 블록만 대상에 저장되므로, 추가적인 전체 데이터베이스 백업은 디스크 공간을 상당히 적게 차지합니다.

Snapshot 백업 및 복원 작업의 런타임

다음 그림은 스냅샷 백업 작업을 사용하는 고객의 HANA Studio를 보여줍니다. 이 이미지는 스냅샷 백업 기술을 사용하면 HANA 데이터베이스(약 4TB 크기)가 1분 20초 만에 백업되고, 파일 기반 백업 작업으로는 4시간 이상 걸리는 것을 보여줍니다.

전체 백업 워크플로 런타임에서 가장 큰 부분은 HANA 데이터베이스 스냅샷 작업을 실행하는 데 필요한 시간입니다. 스토리지 스냅샷 백업 자체는 HANA 데이터베이스 크기에 관계없이 몇 초 안에 완료됩니다.

[너비=624, 높이=267]

복구 시간 목표 비교

이 섹션에서는 파일 기반 및 스토리지 기반 스냅샷 백업의 복구 시간 목표(RTO)를 비교합니다. RTO는 데이터베이스를 복원하고 복구한 다음 시작하는 데 필요한 시간의 합계로 정의됩니다.

데이터베이스를 복원하는 데 필요한 시간입니다

파일 기반 백업을 사용할 경우 복원 시간은 데이터베이스 및 백업 인프라의 크기에 따라 달라지며, 이 크기는 초당 메가바이트 단위로 복원 속도를 정의합니다. 예를 들어, 인프라에서 250MBps의 속도로 복원 작업을 지원하는 경우 지속성 상태에서 데이터베이스 크기가 4TB로 복원하는 데 약 4.5시간이 걸립니다.

NetApp 스냅샷 백업을 사용하면 복원 시간은 데이터베이스 크기에 관계없이 항상 몇 초 정도 소요됩니다.

데이터베이스 복구에 필요한 시간

복구 시간은 복구 후 적용해야 하는 로그 수에 따라 달라집니다. 이 수는 데이터 백업을 수행하는 빈도에 따라 결정됩니다.

파일 기반 데이터 백업을 사용하면 백업 스케줄이 일반적으로 하루에 한 번 수행됩니다. 백업이 운영 성능을 저하하므로 일반적으로 백업 빈도를 높일 수 없습니다. 따라서 최악의 경우, 하루 동안 기록된 모든 로그는 순방향 복구 중에 적용해야 합니다.

스냅샷 백업은 SAP HANA 데이터베이스의 성능에 영향을 미치지 않으므로 일반적으로 더 높은 빈도로 예약됩니다. 예를 들어, 스냅샷 백업이 6시간마다 예약된 경우, 다음 스냅샷이 생성되기 직전에 오류가 발생하면 최악의 경우 마지막 6시간에 대한 로그를 적용해야 합니다. 최악의 경우, 매일 파일 기반 백업을 하려면 지난 24시간 동안의 로그를 적용해야 합니다.

데이터베이스를 시작하는 데 필요한 시간입니다

데이터베이스 시작 시간은 데이터베이스의 크기와 데이터를 메모리로 로드하는 데 필요한 시간에 따라 달라집니다. 다음 예에서는 데이터가 1000Mbps로 로드될 수 있다고 가정합니다. 4TB를 메모리에 로드하는 데 1시간 10분 정도 소요됩니다. 파일 기반 복구 및 스냅샷 기반 복원 및 복구 작업의 시작 시간은 동일합니다.

복원 및 복구 샘플 계산

다음 그림은 일일 파일 기반 백업과 다양한 일정에 따른 스냅샷 백업을 통한 복원 및 복구 작업을 비교한 것입니다.

처음 두 개의 막대는 하루에 Snapshot 백업을 하나만 하더라도 스냅샷 백업의 복원 작업 속도로 인해 복원 및 복구가 43%로 줄어들었다는 것을 보여 줍니다. 하루에 여러 개의 Snapshot 백업이 생성되는 경우 앞으로 복구 중에 적용해야 할 로그가 줄어들기 때문에 런타임을 더욱 줄일 수 있습니다.

다음 그림에서는 하루에 4~6개의 Snapshot 백업이 가장 적합하다는 것을 보여 줍니다. 이보다 더 높은 빈도는 더 이상 전체 런타임에 큰 영향을 주지 않기 때문입니다.

[너비=624, 높이=326]

신속한 백업 및 클론 복제 작업의 사용 사례와 값

백업 실행은 모든 데이터 보호 전략에서 중요한 부분입니다. 시스템 장애로부터 복구할 수 있도록 정기적으로 백업이 예약됩니다. 이것이 가장 확실한 사용 사례이지만 백업 및 복구 작업의 속도가 더욱 빠른 것이 중요한 다른 SAP 라이프사이클 관리 작업도 있습니다.

SAP HANA 시스템 업그레이드는 업그레이드 전에 온디맨드 백업을 수행하고 업그레이드가 실패할 경우 복원 작업을 수행하는 것이 전체 계획된 가동 중지 시간에 상당한 영향을 미치는 사례입니다. 4TB 데이터베이스의 예를 들어보면, 스냅샷 기반 백업 및 복원 작업을 사용하면 계획된 가동 중지 시간을 8시간 줄일 수 있고, 오류를 분석하고 수정하는 데 8시간을 더 사용할 수 있습니다.

또 다른 사용 사례는 일반적인 테스트 주기로, 다양한 데이터 세트나 매개변수를 사용하여 여러 번의 반복을 거쳐

테스트를 수행해야 하는 경우입니다. 빠른 백업 및 복원 작업을 활용하면 테스트 주기 내에서 저장 지점을 쉽게 만들고 테스트가 실패하거나 반복이 필요한 경우 시스템을 이전 저장 지점으로 재설정할 수 있습니다. 이를 통해 테스트를 더 일찍 완료하거나 동시에 더 많은 테스트를 실시하고 테스트 결과를 개선할 수 있습니다.

[너비=618, 높이=279]

스냅샷 백업이 구현되면 HANA 데이터베이스 복사본이 필요한 여러 다른 사용 사례를 처리하는 데 사용할 수 있습니다. 사용 가능한 스냅샷 백업의 내용을 기반으로 새 볼륨을 만들 수 있습니다. 이 작업의 실행 시간은 볼륨 크기에 관계없이 몇 초입니다.

가장 인기 있는 사용 사례는 SAP 시스템 새로 고침으로, 프로덕션 시스템의 데이터를 테스트 또는 QA 시스템으로 복사해야 하는 경우입니다. ONTAP 또는 ANF 클로닝 기능을 활용하면 몇 초 만에 프로덕션 시스템의 스냅샷 복사본에서 테스트 시스템의 볼륨을 프로비저닝할 수 있습니다. 그런 다음 새 볼륨을 테스트 시스템에 연결하고 HANA 데이터베이스를 복구해야 합니다.

두 번째 사용 사례는 프로덕션 시스템의 논리적 손상을 해결하는 데 사용되는 복구 시스템을 만드는 것입니다. 이 경우, 운영 시스템의 이전 스냅샷 백업을 사용하여 복구 시스템을 시작합니다. 복구 시스템은 손상이 발생하기 전의 데이터가 있는 운영 시스템의 동일한 복제본입니다. 그런 다음 수리 시스템을 사용하여 문제를 분석하고 손상되기 전에 필요한 데이터를 내보냅니다.

마지막 사용 사례는 복제를 중단하지 않고 재해 복구 장애 조치 테스트를 실행하여 재해 복구 설정의 RTO 및 복구 지점 목표(RPO)에 영향을 미치지 않는 기능입니다. ONTAP SnapMirror 복제 또는 ANF 지역 간 복제를 사용하여 데이터를 재해 복구 사이트로 복제하는 경우, 운영 스냅샷 백업도 재해 복구 사이트에서 사용할 수 있으며, 이를 사용하여 재해 복구 테스트를 위한 새 볼륨을 만들 수 있습니다.

[너비=627, 높이=328]

SnapCenter 아키텍처에 대해 알아보세요

SnapCenter 서버, 플러그인 구성 요소, 지원되는 스토리지 플랫폼을 비롯하여 SAP HANA 데이터 보호를 위한 SnapCenter 아키텍처에 대해 알아보세요. SnapCenter ONTAP 시스템, Azure NetApp Files 및 FSx for ONTAP 의 SAP HANA 데이터베이스에 대한 중앙 집중식 백업, 복원 및 복제 관리를 제공합니다.

SnapCenter 는 애플리케이션 일관성을 유지하는 데이터 보호를 위한 통합 플랫폼입니다. SnapCenter 사용자에게 애플리케이션별 백업, 복원 및 복제 작업을 관리하는 기능을 위임하는 동시에 중앙 집중식 제어 및 감독 기능을 제공합니다. NetApp SnapCenter 는 데이터베이스 및 스토리지 관리자가 다양한 애플리케이션과 데이터베이스에 대한 백업, 복원 및 복제 작업을 관리하는 데 사용할 수 있는 단일 도구입니다. SnapCenter NetApp ONTAP 스토리지 시스템은 물론 Azure NetApp Files 와 FSx for ONTAP 도 지원합니다. SnapCenter 사용하면 온프레미스 환경 간, 온프레미스 환경과 클라우드 간, 프라이빗, 하이브리드 또는 퍼블릭 클라우드 간에 데이터를 복제할 수도 있습니다.

SnapCenter SnapCenter 서버와 SnapCenter 플러그인이 포함되어 있습니다. 플러그인은 다양한 애플리케이션과 인프라 구성 요소에 사용할 수 있습니다. SnapCenter 서버는 Windows나 Linux에서 실행될 수 있습니다.

[너비=601, 높이=275]

SAP HANA를 위한 SnapCenter 백업 및 복구에 대해 알아보세요

SnapCenter 스토리지 기반 스냅샷 복사본, 자동화된 보존 관리, NetApp ONTAP, Azure NetApp Files, FSx for NetApp ONTAP 과의 통합을 사용하여 SAP HANA 데이터베이스에

대한 포괄적인 백업 및 복구 기능을 제공합니다. 이 솔루션은 SnapVault 또는 ANF 백업을 사용하여 애플리케이션 일관성 있는 데이터베이스 백업, 비데이터 볼륨 보호, 블록 무결성 검사 및 보조 스토리지로의 복제를 지원합니다.

SAP HANA용 SnapCenter 백업 솔루션은 다음과 같은 영역을 다룹니다.

- 백업 작업, 스케줄링 및 보존 관리
- 스토리지 기반 Snapshot 복사본으로 SAP HANA 데이터 백업
- 저장소 기반 스냅샷 복사본(예: /hana/shared)을 사용한 비데이터 볼륨 백업
- 데이터베이스 블록 무결성 검사 작업
  - 파일 기반 백업 사용
  - SAP HANA hdbpersdiag 도구 사용
- 보조 백업 위치로의 스냅샷 백업 복제
  - SnapVault/ SnapMirror 사용
  - Azure NetApp Files ANF 백업 사용
- SAP HANA 백업 카탈로그 관리
  - HANA 데이터 백업(스냅샷 및 파일 기반)
  - HANA 로그 백업용
- 복원 및 복구 작업
  - 자동 복원 및 복구
  - 단일 테넌트 복원 작업

데이터베이스 데이터 백업은 SAP HANA용 SnapCenter 플러그인과 함께 SnapCenter 에서 실행됩니다. 플러그인은 SAP HANA 내부 데이터베이스 스냅샷을 트리거하여 스토리지 시스템에 생성되는 스냅샷이 SAP HANA 데이터베이스의 애플리케이션 일관성 이미지를 기반으로 하도록 합니다.

SnapCenter SnapVault 또는 SnapMirror 기능을 사용하여 일관된 데이터베이스 이미지를 보조 백업이나 재해 복구 위치로 복제할 수 있도록 합니다. 일반적으로 기본 저장소와 보조 저장소의 백업에는 서로 다른 보존 정책이 정의됩니다. SnapCenter 기본 스토리지에서의 보존을 처리하고, ONTAP 보조 백업 스토리지에서의 보존을 처리합니다.

또한 SnapCenter를 사용하면 모든 SAP HANA 관련 리소스를 완벽하게 백업할 수 있을 뿐만 아니라 스토리지 기반 Snapshot 복사본과 함께 SAP HANA 플러그인을 사용하여 모든 비 데이터 볼륨을 백업할 수 있습니다. 개별 보존 및 보호 정책을 사용할 수 있도록 데이터베이스 데이터 백업과 별도로 비데이터 볼륨을 예약할 수 있습니다.

SAP에서는 스토리지 기반 스냅샷 백업과 지속성 계층의 주간 일관성 검사를 결합할 것을 권장합니다. SnapCenter 내에서 블록 일관성 검사를 실행하려면 파일 기반 백업을 실행하거나 SAP hdbpersdiag 도구를 실행하면 됩니다.

구성된 보존 정책에 따라 SnapCenter 기본 저장소의 데이터 파일 백업, 로그 파일 백업 및 SAP HANA 백업 카탈로그의 정리 작업을 관리합니다.

SnapCenter는 운영 스토리지에서 보존을 처리하고, ONTAP은 보조 백업 보존을 관리합니다.

다음 그림에서는 SnapCenter 백업 및 보존 관리 작업의 개요를 보여 줍니다.

SAP HANA 데이터베이스의 스토리지 기반 스냅샷 백업을 실행할 때 SnapCenter은 다음과 같은 작업을 수행합니다.

- 백업 작업:
  - 지속성 계층에서 애플리케이션 일관성 이미지를 얻기 위해 내부 HANA 데이터베이스 스냅샷을 트리거합니다.
  - 데이터 볼륨의 저장소 기반 스냅샷 백업을 생성합니다.
  - 내부 HANA 데이터베이스 스냅샷을 닫고, 백업 작업을 확인하거나 중단합니다. 이 단계에서는 HANA 백업 카탈로그에 백업을 등록합니다.
- 보존 관리:
  - 정의된 보존 기간을 기준으로 스토리지 스냅샷 백업을 삭제합니다.
  - 스토리지 계층에서 스냅샷을 삭제합니다.
  - SAP HANA 백업 카탈로그 항목을 삭제합니다.
  - 가장 오래된 데이터 백업보다 오래된 모든 로그 백업을 삭제합니다. 로그 백업은 파일 시스템 및 SAP HANA 백업 카탈로그에서 삭제됩니다.

[너비=601, 높이=285]

SnapVault/ SnapMirror 또는 ANF 백업을 사용하여 보조 백업이 구성된 경우 기본 볼륨에서 생성된 스냅샷이 보조 백업 저장소에 복제됩니다. SnapCenter 보조 백업의 가용성에 따라 HANA 백업 카탈로그와 로그 백업 보존을 관리합니다.

[너비=601, 높이=278]

SAP HANA에 대한 SnapCenter 지원 구성에 대해 알아보세요.

SnapCenter 온프레미스 및 클라우드 스토리지 플랫폼 전반에서 광범위한 SAP HANA 시스템 아키텍처와 배포 시나리오를 지원합니다. 각 환경에 지원되는 SAP HANA 구성, 플랫폼 조합, 스토리지 프로토콜, 사용 가능한 백업 및 복원 작업에 대해 알아보세요.

지원되는 SAP HANA 구성

SnapCenter 다음과 같은 HANA 구성과 기능을 지원합니다.

- SAP HANA 단일 호스트 시스템
- SAP HANA 다중 호스트 시스템
  - 설명된 대로 중앙 플러그인 배포가 필요합니다. "SAP HANA용 SnapCenter 플러그인 배포 옵션".
- SAP HANA MDC 시스템
  - 단일 또는 여러 세입자와 함께
- 여러 파티션이 있는 SAP HANA 시스템
- SAP HANA 시스템 복제
- SAP HANA 암호화(데이터, 로그, 백업)

지원되는 플랫폼 및 인프라 구성

SnapCenter 다음과 같은 호스트 플랫폼, 파일 시스템 및 스토리지 플랫폼의 조합을 지원합니다.

호스트 플랫폼	**SAP HANA** 스토리지 연결 및 파일 시스템	저장 플랫폼
VMware	게스트 내 NFS 마운트	ONTAP AFF
VMware	VMFS가 있는 FC 데이터 저장소 + Linux LVM이 있거나 없는 XFS가 있는 VM	ONTAP AFF 또는 ASA
케이비엠	게스트 내 NFS 마운트	ONTAP AFF
베어메탈 서버	NFS 마운트	ONTAP AFF
베어메탈 서버	FC SAN + 및 Linux LVM이 있거나 없는 XFS	ONTAP AFF 또는 ASA (*)
Azure VM	NFS 마운트	Azure NetApp Files
AWS EC2	NFS 마운트	ONTAP 용 FSx

(*): SnapCenter 6.2 릴리스부터 ASA 지원이 가능합니다.

HANA 및 Linux 플러그인은 Intel CPU 플랫폼에서만 사용할 수 있습니다. IBM Power의 Linux의 경우 중앙 HANA 플러그인 배포는 다음에 설명된 대로 설정해야 합니다. "SAP HANA용 SnapCenter 플러그인 배포 옵션".

지원되는 기능 및 작업

약어 설명

- VBSR: 볼륨 기반 SnapRestore + 볼륨 기반 SnapRestore 볼륨을 스냅샷 상태로 되돌립니다.
- SFSR: 단일 파일 SnapRestore + 단일 파일 SnapRestore 볼륨 내의 특정 파일이나 LUN을 복원하는 데 사용할 수 있습니다.

또한 참조하세요 "자동 검색된 SAP HANA 데이터베이스에 대한 복원 작업 유형"

ONTAP AFF 및 **ONTAP** 용 **FSx**

아래 표의 열 1(NFS 마운트)만 FSx for ONTAP 과 관련이 있습니다.

작업	**VMware** 또는 **KVM**을 사용하여 베어 메탈 또는 게스트 내부 **NFS** 마운트	**FC SAN +** 베어 메탈	**FC** 데이터 저장소 **VMware VMFS**
HANA 데이터베이스에 대한 스냅샷 백업 및 복원 작업			
스냅샷 백업	예	예	예
변조 방지 스냅샷	예	예	예
전체 복원	VBSR 또는 SFSR(선택 가능)	완전한 LUN의 SFSR	복제, 마운트, 복사
단일 테넌트 복원	SFSR	복제, 마운트, 복사	복제, 마운트, 복사
* HANA 데이터베이스에 대한 SnapVault 백업 및 복원 작업*			

작업	**VMware** 또는 **KVM**을 사용하여 베어 메탈 또는 게스트 내부 **NFS** 마운트	**FC SAN +** 베어 메탈	**FC** 데이터 저장소 **VMware VMFS**
SnapVault 복제	예	예	예
변조 방지 스냅샷	예	예	예
전체 복원	예	예	복제, 마운트, 복사
단일 테넌트 복원	예	복제, 마운트, 복사	복제, 마운트, 복사
기본 스냅샷 또는 **SnapVault** 대상에서의 **HANA** 복구 작업			
자동 복구 MDC 단일 테넌트	예	예	예
자동 복구 MDC 다중 테넌트	아니요	아니요	아니요
데이터가 아닌 볼륨 백업 및 복원			
스냅샷 백업	예	예	예 (*)
스냅샷에서 복원	VBSR 또는 SFSR(선택 가능)	완전한 LUN의 SFSR	VBSR (*)
SnapVault 복제	예	예	예 (*)
SnapVault 대상에서 복원	예	예	예 (*)
SAP 시스템 새로 고침			
기본 스냅샷에서	예	예 (**)	예 (**)
SnapVault 대상에서	예	예 (**)	예 (**)
HA와 **DR**			
HSR은 스냅샷과 SnapVault 지원합니다.	예	예	예
SC를 사용한 SnapMirror 복제 업데이트	예	예	예
SnapMirror 액티브 싱크	해당 없음	예	예

(*): VMware 통합 없음 - 충돌 이미지 스냅샷 및 전체 볼륨 복원

(**): SnapCenter 릴리스 < 6.2에 필요한 해결 방법

ONTAP ASA

작업	**FC SAN +** 베어 메탈**(*)**	**FC** 데이터 저장소 **VMware VMFS**
HANA 데이터베이스에 대한 스냅샷 백업 및 복원 작업		
스냅샷 백업	예	예
변조 방지 스냅샷	아니요	아니요
전체 복원	완전한 LUN의 SFSR	복제, 마운트, 복사

작업	**FC SAN +** 베어 메탈**(*)**	**FC** 데이터 저장소 **VMware VMFS**
단일 테넌트 복원	복제, 마운트, 복사	복제, 마운트, 복사
* HANA 데이터베이스에 대한 SnapVault 백업 및 복원 작업*		
SnapVault 복제	예	예
변조 방지 스냅샷	아니요	아니요
전체 복원	예	복제, 마운트, 복사
단일 테넌트 복원	복제, 마운트, 복사	복제, 마운트, 복사
기본 스냅샷 또는 **SnapVault** 대상에서의 **HANA** 복구 작업		
자동 복구 MDC 단일 테넌트	예	예
자동 복구 MDC 다중 테넌트	아니요	아니요
데이터가 아닌 볼륨 백업 및 복원		
스냅샷 백업	예	예 (*)
스냅샷에서 복원	완전한 LUN의 SFSR	완전한 LUN의 SFSR (*)
SnapVault 복제	예	예 (*)
SnapVault 대상에서 복원	예	예 (*)
SAP 시스템 새로 고침		
기본 스냅샷에서	예	예 (**)
SnapVault 대상에서	예	예 (**)
HA와 **DR**		
HSR은 스냅샷과 SnapVault 지원합니다.	예	예
SnapCenter 에서 트리거되는 SnapMirror 복제 업데이트	예	예
SnapMirror 액티브 싱크	예	예

(*): SnapCenter 6.2 릴리스부터 지원

(**): SnapCenter 릴리스 < 6.2에 필요한 해결 방법

Azure NetApp Files

작업	**NFS** 마운트
HANA 데이터베이스에 대한 스냅샷 백업 및 복원 작업	
스냅샷 백업	예
변조 방지 스냅샷	아니요
전체 제자리 복원	볼륨 되돌리기 또는 SFSR(선택 가능)

작업	**NFS** 마운트
단일 테넌트 복원	SFSR
HANA 데이터베이스에 대한 **ANF** 백업 및 복원 작업	
ANF 백업 복제	예
변조 방지 스냅샷	아니요
전체 제자리 복원	예
단일 테넌트 복원	예
기본 스냅샷 또는 **ANF** 백업에서 **HANA** 복구 작업	
자동 복구 MDC 단일 테넌트	예
자동 복구 MDC 다중 테넌트	아니요
데이터가 아닌 볼륨 백업 및 복원	
스냅샷 백업	예
스냅샷에서 복원	볼륨 되돌리기
ANF 백업 복제	예
ANF 백업에서 전체 복원	아니요 (*)
SAP 시스템 새로 고침	
기본 스냅샷에서	예
ANF 백업에서	예
HA와 **DR**	
HSR은 스냅샷과 ANF 백업을 지원합니다.	예
SnapCenter 에서 트리거된 지역 간 복제 업데이트	아니요

(*): 현재 버전에서는 Azure Portal 또는 CLI를 사용하여 복원 작업을 수행해야 합니다.

SnapCenter 데이터 보호 개념과 모범 사례에 대해 알아보세요.

SAP HANA 환경을 위한 SnapCenter 배포 옵션, 데이터 보호 전략 및 백업 보존 관리에 대해 알아보세요. SnapCenter 데이터베이스 호스트나 중앙 호스트에 플러그인 배포, 자동 검색 및 수동 구성, 파일 기반 백업이나 hdbpersdiag를 사용한 블록 일관성 검사, 기본 및 보조 스토리지 전반에 걸친 포괄적인 보존 관리를 지원합니다.

SAP HANA용 SnapCenter 플러그인 배포 옵션

다음 그림은 SnapCenter 서버, SAP HANA 데이터베이스 및 스토리지 시스템 간 통신의 논리적 보기를 보여줍니다. SnapCenter 서버는 HANA 및 Linux 플러그인을 활용하여 HANA 데이터베이스와 Linux 운영 체제와 통신합니다.

[너비=601, 높이=199]

SnapCenter 플러그인에 권장되고 기본으로 제공되는 배포 옵션은 HANA 데이터베이스 호스트에 설치하는 것입니다.

이 배포 옵션을 사용하면 SnapCenter 지원 구성 장에서 설명한 모든 구성과 기능이 유효합니다. SnapCenter 플러그인을 HANA 데이터베이스 호스트에 설치할 수 없고 SnapCenter 서버 자체일 수 있는 중앙 플러그인 호스트에서 구성해야 하는 몇 가지 예외가 있습니다. HANA 다중 호스트 시스템이나 IBM Power 플랫폼에서 실행되는 HANA 시스템에는 중앙 플러그인 호스트가 필요합니다. 두 가지 배포 옵션을 혼합하여 사용할 수도 있습니다. 예를 들어 SnapCenter 서버를 다중 호스트 시스템의 중앙 플러그인 호스트로 사용하고 다른 모든 단일 호스트 HANA 시스템의 경우 HANA 데이터베이스 호스트에 플러그인을 배포할 수 있습니다.

SnapCenter 에서는 HANA 리소스를 자동으로 검색하거나 수동으로 구성할 수 있습니다. HANA 및 Linux 플러그인이 데이터베이스 호스트에 배포되면 기본적으로 HANA 시스템이 자동으로 검색됩니다. SnapCenter 자동 검색은 동일한 호스트에서 여러 HANA 설치를 지원하지 않습니다. 중앙 플러그인 호스트를 사용하여 관리되는 HANA 시스템은 SnapCenter 에서 수동으로 구성해야 합니다. 또한, 비데이터 볼륨은 기본적으로 수동으로 구성된 리소스입니다.

	플러그인이 배포됨	**SnapCenter** 리소스
HANA 데이터베이스	데이터베이스 호스트	자동 발견됨
HANA 데이터베이스	중앙 플러그인 호스트	수동 구성됨
비데이터 볼륨	해당 없음	수동 구성됨

SnapCenter HANA 시스템을 위한 중앙 플러그인 배포를 지원하지만 플랫폼 및 기능 지원에는 제한이 있습니다. 다음 인프라 구성 및 작업은 중앙 플러그인 호스트로 구성된 HANA 시스템에서 지원되지 않습니다.

- FC 데이터 저장소를 사용한 VMware
- SnapMirror 액티브 싱크
- 중앙 플러그인 호스트로 사용하는 경우 SnapCenter 서버 고가용성
- HANA 시스템 자동 검색
- 자동화된 HANA 데이터베이스 복구
- 자동화된 SAP 시스템 새로 고침
- 단일 테넌트 복원

SAP HANA 데이터베이스 호스트에 배포된 **HANA**용 **SnapCenter** 플러그인

SnapCenter 서버는 HANA 플러그인을 통해 HANA 데이터베이스와 통신합니다. HANA 플러그인은 HANA hdbsql 클라이언트 소프트웨어를 사용하여 HANA 데이터베이스에 SQL 명령을 실행합니다. HANA hdb 사용자 저장소는 HANA 데이터베이스에 액세스하기 위한 사용자 자격 증명, 호스트 이름 및 포트 정보를 제공하는 데 사용됩니다. SnapCenter Linux 플러그인은 호스트 파일 시스템 작업과 파일 시스템 및 스토리지 리소스의 자동 검색을 처리하는 데 사용됩니다.

HANA 플러그인이 HANA 데이터베이스 호스트에 배포되면 HANA 시스템은 SnapCenter 에서 자동으로 검색되고 SnapCenter 에서 자동 검색된 리소스로 플래그가 지정됩니다.

[너비=601, 높이=304]

SnapCenter 서버 고가용성

SnapCenter 2노드 HA 구성으로 설정할 수 있습니다. 이러한 구성에서는 로드 밸런서(예: F5)를 사용하여 SnapCenter 호스트에 액세스합니다. SnapCenter 저장소(MySQL 데이터베이스)는 SnapCenter 에 의해 두 호스트 간에 복제되므로 SnapCenter 데이터는 항상 동기화됩니다.

HANA 플러그인이 SnapCenter 서버에 설치된 경우 SnapCenter 서버 HA는 지원되지 않습니다. SnapCenter HA에

대한 자세한 내용은 다음에서 확인할 수 있습니다. "고가용성을 위한 SnapCenter 서버 구성".

[너비=601, 높이=307]

중앙 플러그인 호스트

이전 장에서 논의한 대로 중앙 플러그인이 필요합니다.

- HANA 다중 호스트 시스템
- IBM Power에서 실행되는 HANA 시스템

중앙 플러그인 호스트를 사용하는 경우 HANA 플러그인과 SAP HANA hdbsql 클라이언트를 HANA 데이터베이스 호스트 외부의 호스트에 설치해야 합니다. 이 호스트는 SnapCenter 서버 등 Windows 또는 Linux 호스트가 될 수 있습니다.

Windows에서 SnapCenter 서버를 실행하면 Windows 시스템을 중앙 플러그인 호스트로 사용할 수 있습니다. Linux에서 SnapCenter 서버를 실행하는 경우 다른 호스트를 중앙 플러그인 호스트로 사용해야 합니다.

HANA 다중 호스트 시스템의 경우 모든 작업자 및 대기 호스트에 대한 SAP HANA 사용자 저장소 키는 중앙 플러그인 호스트에서 구성해야 합니다. SnapCenter 제공된 각 키를 사용하여 데이터베이스에 연결을 시도하므로 시스템 데이터베이스(HANA 네임 서버)가 다른 호스트로 장애 조치되는 것과 관계없이 독립적으로 작동할 수 있습니다.

[너비=601, 높이=314]

중앙 플러그인 호스트에서 관리하는 여러 개의 단일 호스트 HANA 시스템의 경우, HANA 시스템의 모든 개별 SAP HANA 사용자 저장소 키는 중앙 플러그인 호스트에서 구성되어야 합니다.

[너비=601, 높이=338]

SAP HANA 블록 일관성 검사

SAP에서는 전반적인 백업 전략에 정기적인 HANA 블록 일관성 검사를 포함할 것을 권장합니다. 기존의 파일 기반 백업에서는 이러한 확인 작업이 각 백업 작업마다 수행됩니다. 스냅샷 백업의 경우 스냅샷 백업 작업 외에도 일관성 검사를 실행해야 합니다(예: 주 1회).

기술적으로 블록 일관성 검사를 실행하는 데는 두 가지 옵션이 있습니다.

- 표준 파일 기반 또는 backint 기반 백업 실행
- HANA 도구 hdbpersdiag 실행, 또한 참조하세요. "지속성 일관성 검사 | SAP 도움말 포털"

HANA hdbpersdiag 도구는 HANA 설치의 일부이며, 오프라인 HANA 데이터베이스에 대해 블록 일관성 검사 작업을 실행할 수 있습니다. 따라서 기존 스냅샷 백업을 hdbpersdiag에 제시할 수 있는 스냅샷 백업과 함께 사용하기에 완벽하게 적합합니다.

두 가지 접근 방식을 비교해보면, hdbpersdiag는 HANA 블록 일관성 검사를 위한 파일 기반 백업에 비해 상당한 이점을 가지고 있습니다. 한 가지 차원은 필요한 저장 용량입니다. 파일 기반 백업의 경우 각 HANA 시스템에서 최소한 하나의 백업 크기만큼의 백업을 사용할 수 있어야 합니다. 예를 들어, 지속성 크기가 3TB인 HANA 시스템이 15개 있다면 일관성 검사에만 45TB가 추가로 필요합니다. hdbpersdiag를 사용하면 기존 스냅샷 백업이나 기존 스냅샷 백업의 FlexClone 대상으로 작업이 실행되므로 추가 저장 용량이 필요하지 않습니다. 두 번째 차원은 일관성 검사 작업 중 HANA 호스트의 CPU 부하입니다. 파일 기반 백업에는 HANA 데이터베이스 호스트에서 CPU 사이클이 필요하지만,

hdbpersdiag 처리는 중앙 검증 호스트와 함께 사용하면 HANA 호스트에서 완전히 오프로드될 수 있습니다. 아래 표는 주요 특징을 요약한 것입니다.

	필요한 저장 용량	**HANA** 호스트의 **CPU** 및 네트워크 부하
파일 기반 백업	각 HANA 시스템에 대한 최소 1 x 데이터 백업 크기	높은
HANA 호스트의 스냅샷 디렉토리를 사용하는 hdbpersdiag(NFS 전용)	None	중간
FlexClone 볼륨으로 hdbpersdiag를 실행하는 데 사용되는 중앙 검증 호스트	None	None

NetApp HANA 블록 일관성 검사를 실행하기 위해 hdbpersdiag를 사용할 것을 권장합니다. 구현에 대한 자세한 내용은 다음 장에서 확인할 수 있습니다. "SnapCenter 사용한 블록 일관성 검사".

데이터 보호 전략

SnapCenter 및 SAP HANA 플러그인을 구성하기 전에 다양한 SAP 시스템의 RTO 및 RPO 요구사항을 기준으로 데이터 보호 전략을 정의해야 합니다.

일반적인 접근 방식은 운영, 개발, 테스트 또는 샌드박스 시스템과 같은 시스템 유형을 정의하는 것입니다. 동일한 시스템 유형의 모든 SAP 시스템은 일반적으로 동일한 데이터 보호 매개 변수를 사용합니다.

정의해야 하는 매개 변수는 다음과 같습니다.

- Snapshot 백업을 얼마나 자주 실행해야 합니까?
- Snapshot 복사본 백업을 기본 스토리지 시스템에 얼마나 오래 보관해야 합니까?
- 블록 무결성 검사를 얼마나 자주 실행해야 합니까?
- 1차 백업을 2차 백업 사이트로 복제해야 합니까?
- 백업은 보조 백업 저장소에 얼마 동안 보관해야 합니까?

다음 표는 생산, 개발, 테스트 시스템 유형에 대한 데이터 보호 매개변수의 예를 보여줍니다. 운영 시스템의 경우 높은 백업 빈도가 정의되었으며, 백업은 하루에 한 번씩 보조 백업 사이트에 복제됩니다. 테스트 시스템은 요구 사항이 낮고 백업 복제가 없습니다.

매개 변수	운영 시스템	개발 시스템	시스템을 테스트합니다
백업 빈도	6시간마다	6시간마다	12시간마다
기본 보존	3일	3일	6일
블록 무결성 검사	일주일에 한 번	일주일에 한 번	아니요
보조 백업 사이트로 복제	하루에 한 번	하루에 한 번	아니요
2차 백업 보존	2주	2주	아니요

다음 표는 위의 데이터 보호 매개변수에 대해 구성해야 할 정책과 일정을 보여줍니다.

정책	백업 유형	일정 빈도	기본 보존	**SnapVault** 복제	**2**차 보존
로컬스냅	스냅샷 기반	6시간마다	개수=12	아니요	해당 없음
로컬스냅앤스냅볼트	스냅샷 기반	하루에 한 번	개수=2	예	개수=14
스냅앤콜HDB퍼스디아그	스냅샷 기반	일주일에 한 번	개수=2	아니요	해당 없음

ONTAP 시스템 또는 FSx for ONTAP 의 경우 SnapCenter 에서 SnapVault 업데이트 작업을 실행하기 전에 SnapVault 복제를 위해 ONTAP 에서 데이터 보호 관계를 구성해야 합니다. 2차 보존은 ONTAP 보호 정책에 정의되어 있습니다.

ANF 백업의 경우 SnapCenter 외부에서 추가 구성이 필요하지 않습니다. ANF 백업 보조 보존은 SnapCenter 에서 관리합니다.

이 예제 구성에서는 블록 무결성 검사 작업에 hdbpersdiag가 사용됩니다. 자세한 내용은 장에서 확인할 수 있습니다. "SnapCenter 사용한 블록 일관성 검사".

아래 그림은 일정과 백업 보존 기간을 요약한 것입니다. SnapCenter 사용하여 로그 백업 보존을 관리하는 경우 가장 오래된 스냅샷 백업보다 오래된 모든 로그 백업이 삭제됩니다. 다시 말해, 로그 백업은 사용 가능한 모든 백업을 현재 시점으로 복구하는 데 필요한 기간 동안 보관됩니다.

[너비=601, 높이=192]

암호화 루트 키 백업

HANA 지속성 암호화를 사용하는 경우 표준 데이터 백업 외에도 루트 키의 백업을 만드는 것이 중요합니다. 데이터 볼륨과 HANA 설치 파일 시스템이 손실된 경우 HANA 데이터베이스를 복구하려면 루트 키 백업이 필요합니다. 자세한 내용은 다음을 참조하세요. "SAP HANA 관리 가이드".

루트 키가 변경되면 새로운 루트 키를 사용하여 이전에 생성된 이전 HANA 데이터베이스 백업을 복구할 수 없다는 점을 명심하세요. 백업을 생성할 당시 활성화되어 있던 루트 키가 항상 필요합니다.

백업 작업

SnapCenter 단일 또는 여러 테넌트가 있는 HANA MDC 시스템의 스냅샷 백업 작업을 지원합니다. SnapCenter HANA MDC 시스템의 두 가지 다른 복원 작업도 지원합니다. 전체 시스템, 시스템 DB 및 모든 테넌트를 복원할 수도 있고, 하나의 테넌트만 복원할 수도 있습니다. SnapCenter 이러한 작업을 실행하려면 몇 가지 전제 조건이 있습니다.

MDC 시스템에서는 테넌트 구성이 반드시 정적이지는 않습니다. 세입자를 추가하거나 삭제할 수 있습니다. SnapCenter HANA 데이터베이스가 SnapCenter 에 추가될 때 발견된 구성에 의존할 수 없습니다. 단일 테넌트 복원 작업을 활성화하려면 SnapCenter 각 스냅샷 백업에 포함된 테넌트를 알아야 합니다. 또한 스냅샷 백업에 포함된 각 테넌트에 속하는 파일과 디렉토리를 알아야 합니다.

따라서 SnapCenter 각 백업 작업을 통해 테넌트 정보를 식별합니다. 여기에는 테넌트 이름과 해당 파일 및 디렉토리 정보가 포함됩니다. 단일 테넌트 복원 작업을 지원하려면 이 데이터를 스냅샷 백업 메타데이터에 저장해야 합니다.

애플리케이션 자동 검색의 또 다른 단계는 HANA 시스템 복제(HSR) 기본 또는 보조 노드를 감지하는 것입니다. HANA 시스템이 HSR로 구성된 경우 SnapCenter 각 백업 작업에서 기본 노드를 식별하여 백업 SQL 명령이 HSR 기본

노드에서 실행되도록 해야 합니다. 또한 참조하세요 "SAP HANA 시스템 복제 - SnapCenter를 사용한 백업 및 복구".

SnapCenter 또한 HANA 데이터 볼륨 구성을 감지하고 이를 파일 시스템 및 스토리지 리소스에 매핑합니다. 이러한 접근 방식을 통해 SnapCenter HANA 볼륨 구성 변경(예: 여러 파티션 또는 볼륨 마이그레이션과 같은 스토리지 구성 변경)을 처리할 수 있습니다.

다음 단계는 스냅샷 백업 작업 자체입니다. 이 단계에는 HANA 데이터베이스 스냅샷을 트리거하는 SQL 명령, 스토리지 스냅샷 백업, HANA 스냅샷 작업을 닫는 SQL 명령이 포함됩니다. close 명령을 사용하면 HANA 데이터베이스는 시스템 DB와 각 테넌트의 백업 카탈로그를 업데이트합니다.

하나 이상의 테넌트가 중지된 경우 SAP는 MDC 시스템에 대한 스냅샷 백업 작업을 지원하지 않습니다.

데이터 백업 및 HANA 백업 카탈로그 관리의 보존 관리를 위해 SnapCenter는 첫 번째 단계에서 식별된 시스템 데이터베이스 및 모든 테넌트 데이터베이스에 대해 카탈로그 삭제 작업을 실행해야 합니다. 로그 백업과 마찬가지로 SnapCenter 워크플로도 백업 작업의 일부인 각 테넌트에서 작동해야 합니다.

다음 그림에서는 백업 워크플로우의 개요를 보여 줍니다.

[너비=601, 높이=237]

백업 보존 관리

데이터 백업 보존 관리 및 로그 백업 정리정돈 은 보존 관리를 포함하여 5가지 주요 영역으로 나눌 수 있습니다.

- 운영 스토리지의 로컬 백업
- 파일 기반 백업
- 보조 저장소에서의 백업(SnapVault 또는 ANF 백업)
- SAP HANA 백업 카탈로그 내의 데이터 백업
- SAP HANA 백업 카탈로그 및 파일 시스템의 로그 백업

다음 그림에서는 다양한 워크플로우와 각 작업의 종속 관계를 간략하게 보여 줍니다. 다음 섹션에서는 다양한 작업에 대해 자세히 설명합니다.

[너비=601, 높이=309]

운영 스토리지에서 로컬 백업의 보존 관리

SnapCenter SnapCenter 백업 정책에 정의된 보존 기간에 따라 기본 스토리지와 SnapCenter 저장소에서 스냅샷 복사본을 삭제하여 SAP HANA 데이터베이스 백업과 비데이터 볼륨 백업의 정리 작업을 처리합니다. SnapCenter 의 각 백업 워크플로에는 보존 관리가 포함되어 있습니다. 기본 저장소의 로컬 백업도 SnapCenter 에서 수동으로 삭제할 수 있습니다.

파일 기반 백업의 보존 관리

SnapCenter SnapCenter 백업 정책에 정의된 보존 기간에 따라 파일 시스템의 백업을 삭제하여 파일 기반 백업의 정리 작업을 처리합니다. SnapCenter 의 각 백업 워크플로우에서는 보존 관리 로직이 실행됩니다.

보조 저장소(SnapVault)에서의 백업 보존 관리

보조 저장소(SnapVault)에서 백업의 보존 관리를 담당하는 ONTAP 은 ONTAP 보호 관계에 정의된 보존을 기반으로 관리합니다. SnapCenter 저장소의 보조 저장소에서 이러한 변경 사항을 동기화하기 위해 SnapCenter 예약된 정리 작업을 사용합니다. 이 정리 작업은 모든 SnapCenter 플러그인과 모든 리소스에 대한 모든 보조 저장소 백업을 SnapCenter 저장소와 동기화합니다.

정리 작업은 기본적으로 일주일에 한 번씩 예약됩니다. 이 주간 일정을 적용하면 SnapCenter 와 SAP HANA Studio에서 백업을 삭제하는 데 시간이 걸리는데, 이는 보조 저장소에서 이미 삭제된 백업과 비교했을 때 지연이 발생합니다. 이러한 불일치를 피하기 위해 고객은 일정을 더 자주(예: 하루에 한 번) 변경할 수 있습니다. 정리 작업 일정을 조정하는 방법이나 수동 새로 고침을 트리거하는 방법에 대한 자세한 내용은 다음 장을 참조하십시오. "2차 백업 정리".

2차 저장소(ANF 백업)에서의 백업 보존 관리

ANF 백업의 보존은 SnapCenter 에서 구성하고 처리합니다. SnapCenter SnapCenter 백업 정책에 정의된 보존 기간에 따라 백업을 삭제하여 ANF 백업의 정리 작업을 처리합니다. SnapCenter 의 각 백업 워크플로에는 보존 관리가 포함되어 있습니다.

SAP HANA 백업 카탈로그 내에서 데이터 백업의 보존 관리

SnapCenter 백업, 로컬 스냅샷 또는 파일 기반을 삭제하거나 SnapCenter 보조 저장소에서 백업 삭제를 식별한 경우, 이 데이터 백업은 SAP HANA 백업 카탈로그에서도 삭제됩니다. SnapCenter 기본 저장소에서 로컬 스냅샷 백업에 대한 SAP HANA 카탈로그 항목을 삭제하기 전에 백업이 보조 저장소에 여전히 있는지 확인합니다.

로그 백업의 보존 관리

SAP HANA 데이터베이스는 자동으로 로그 백업을 생성합니다. 이러한 작업은 SAP HANA에 구성된 백업 디렉토리에 각 SAP HANA 서비스에 대한 백업 파일을 생성합니다. 최신 데이터 백업보다 오래된 로그 백업은 더 이상 전방 복구에 필요하지 않으므로 삭제할 수 있습니다. SnapCenter 다음 단계를 실행하여 파일 시스템 수준과 SAP HANA 백업 카탈로그에서 로그 파일 백업의 정리 작업을 처리합니다.

1. SnapCenter SAP HANA 백업 카탈로그를 읽어 가장 오래된 성공적인 데이터 백업의 백업 ID를 가져옵니다.
2. SnapCenter는 SAP HANA 카탈로그에 있는 모든 로그 백업과 이 백업 ID보다 오래된 파일 시스템을 삭제합니다.

SnapCenter는 SnapCenter에서 생성한 백업의 하우스키핑만 처리합니다. SnapCenter 외부에서 추가 파일 기반 백업이 생성되는 경우 파일 기반 백업이 백업 카탈로그에서 삭제되었는지 확인해야 합니다. 이러한 데이터 백업이 백업 카탈로그에서 수동으로 삭제되지 않으면 가장 오래된 데이터 백업이 될 수 있으며, 이 파일 기반 백업이 삭제될 때까지 오래된 로그 백업이 삭제되지 않습니다.

정책 구성에서 주문형 백업에 대한 보존 기간이 정의되어 있더라도, 다른 주문형 백업이 실행될 때만 정리 작업이 수행됩니다. 따라서 주문형 백업은 일반적으로 SnapCenter 에서 수동으로 삭제하여 이러한 백업이 SAP HANA 백업 카탈로그에서도 삭제되고 로그 백업 정리가 이전 주문형 백업을 기반으로 하지 않도록 해야 합니다.

로그 백업 보존 관리는 기본적으로 활성화되어 있습니다. 필요한 경우 자동 로그 백업 정리 비활성화 섹션에 설명된 대로 비활성화할 수 있습니다.

SAP HANA 환경에 대한 SnapCenter 구성에 대해 알아보세요.

2단계 접근 방식을 사용하여 SAP HANA 환경에 맞게 SnapCenter 구성합니다. 공유 리소스(자격 증명, 스토리지 시스템 및 정책)에 대한 초기 구성과 개별 HANA 시스템(호스트 배포, 자동 검색 및 보호 설정)에 대한 리소스별 구성이 있습니다.

여러 HANA 시스템이 있는 SAP HANA 환경에 대한 SnapCenter 구성은 두 가지 주요 영역으로 나눌 수 있습니다.

- 초기 구성
  - 자격 증명, 저장소 및 정책 구성. + 이러한 설정이나 리소스는 일반적으로 여러 HANA 시스템에서 사용됩니다.
- HANA 리소스별 구성
  - 호스트, HANA 및 리소스 보호 구성은 각 HANA 시스템에 대해 개별적으로 수행해야 합니다.

아래 그림은 다양한 구성 구성 요소와 해당 종속성을 보여줍니다.

모든 구성 단계는 다음 항목에서 자세히 설명합니다.

> 문서의 설명과 스크린샷은 SnapCenter 자동으로 검색한 HANA 시스템을 기반으로 합니다. 중앙 플러그인 호스트를 사용하여 수동으로 구성된 리소스에 대한 추가 또는 다른 구성 단계는 다음에서 설명합니다. "중앙 플러그인 호스트 구성".

[너비=601, 높이=319]

SAP HANA에 대한 초기 SnapCenter 설정 구성

Azure 서비스 주체에 대한 자격 증명을 설정하고, 스토리지 시스템을 추가하고, 스냅샷 백업, 블록 무결성 검사 및 보조 복제에 대한 정책을 만들어 SAP HANA 환경에 대한 초기 SnapCenter 설정을 구성합니다.

SnapCenter 초기 구성에는 다음 단계가 포함됩니다.

1. 자격 증명 구성
   a. Azure NetApp Files (ANF)로 구성된 HANA 시스템의 경우 서비스 주체를 준비한 다음 SnapCenter 에서 구성해야 합니다.
   b. HANA 데이터베이스 호스트에 HANA 플러그인을 자동으로 설치하려면 호스트 자격 증명을 제공해야 합니다.
2. 스토리지 시스템 구성
   a. ANF로 구성된 HANA 시스템의 경우, 필요한 NetApp 계정을 선택하여 SnapCenter 구성에 추가할 수 있습니다.
   b. ONTAP 또는 FSx for ONTAP 스토리지 시스템의 경우 SVM이나 전체 스토리지 클러스터를 SnapCenter 에 추가할 수 있습니다.
3. 정책 구성
   a. 스냅샷 기반 백업과 블록 무결성 검사 작업에 대한 정책은 ANF뿐만 아니라 ONTAP 및 FSx for ONTAP 스토리지 시스템에 대해서도 구성할 수 있습니다.
   b. SnapVault 또는 SnapMirror 사용한 변조 방지 스냅샷 및 보조 백업에 대한 정책은 ONTAP 및 FSx for ONTAP

스토리지 시스템에만 구성할 수 있습니다.

c. ANF로 구성된 HANA 시스템의 경우 정책에는 다음이 포함될 수 있습니다. "ANF 백업".

> 동일한 스냅샷 백업 정책은 HANA 데이터베이스뿐만 아니라 HANA 공유 볼륨과 같은 비데이터 볼륨에도 사용할 수 있습니다.

아래 그림은 구성 섹션을 요약한 것입니다.

[너비=601, 높이=158]

다음 장에서는 초기 구성 단계를 설명합니다.

자격 증명 구성

HANA 플러그인 배포를 위한 자격 증명

자격 증명은 설정 섹션에서 자격 증명 탭을 선택하여 구성합니다. + 아이콘을 클릭하면 자격 증명을 추가할 수 있습니다.

[너비=601, 높이=118]

NetApp 모든 HANA 데이터베이스 호스트(예: scuser)에 사용자를 구성하고 설명된 대로 sudo 권한을 구성할 것을 권장합니다. "SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건".

[너비=287, 높이=247]

Azure NetApp Files 에 대한 자격 증명

SnapCenter ANF 볼륨에 필요한 작업을 실행할 수 있도록 Azure 서비스 주체를 준비해야 합니다. 아래 예는 반드시 포함되어야 하는 최소한의 필수 권한을 보여줍니다.

```
    "assignableScopes": [
        "/subscriptions/xxx"
    ],
    "createdBy": "xxx",
    "createdOn": "2025-05-07T07:12:14.451483+00:00",
    "description": "Restricted Access for SnapCenter ",
    "id":
"/subscriptions/xxx/providers/Microsoft.Authorization/roleDefinitions/xxx"
,
    "name": "xxx",
    "permissions": [
        {
            "actions": [
            "Microsoft.NetApp/register/action",
            "Microsoft.NetApp/unregister/action",
            "Microsoft.NetApp/netAppAccounts/read",
            "Microsoft.NetApp/netAppAccounts/getKeyVaultStatus/action",
            "Microsoft.NetApp/netAppAccounts/migrateEncryption/action",
```

```
            "Microsoft.NetApp/netAppAccounts/transitionToCmk/action",
            "Microsoft.NetApp/netAppAccounts/capacityPools/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revert/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/poolChange/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/finalizeRelocation/
action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revertRelocation/ac
tion",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/breakFileLocks/acti
on",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/getGroupIdListForLd
apUser/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/restoreFile
s/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/restoreFi
les/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/getMetad
ata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/volumeQuotaRules/re
ad",
```

```
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/latestRestoreStatus
/current/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/mountTargets/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/restoreStatus/read"
,
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/read",
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/write",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/listVolumes/read",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/volumes/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/write",
            "Microsoft.NetApp/locations/checknameavailability/action",
            "Microsoft.NetApp/locations/checkfilepathavailability/action",
            "Microsoft.NetApp/locations/operationresults/read",
            "Microsoft.NetApp/Operations/read",
            "Microsoft.Resources/resources/read",
            "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
            "Microsoft.Network/virtualNetworks/read",
            "Microsoft.Network/virtualNetworks/subnets/read",
            "Microsoft.Network/virtualNetworks/write",
            "Microsoft.Network/virtualNetworks/subnets/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/delete",

"Microsoft.NetApp/netAppAccounts/backupVaults/backups/restoreFiles/action"
            ],
            "condition": null,
            "conditionVersion": null,
            "dataActions": [],
            "notActions": [],
            "notDataActions": []
        }
    ],
    "roleName": "SnapCenter-Restricted-Access",
    "roleType": "CustomRole",
    "type": "Microsoft.Authorization/roleDefinitions",
```

```
    "updatedBy": "xxx",
    "updatedOn": "2025-05-07T07:12:14.451483+00:00"
}
```

자격 증명은 설정 섹션에서 자격 증명 탭을 선택하여 구성합니다. 자격 증명은 + 아이콘을 클릭하여 구성합니다.

[너비=601, 높이=116]

다음 화면에서는 자격 증명 이름을 제공하고 인증 모드 Azure 자격 증명을 선택해야 합니다. 그런 다음 테넌트 ID, 클라이언트 ID 및 클라이언트 비밀 키를 구성해야 합니다.

[너비=252, 높이=246]

스토리지 시스템 구성

ONTAP 시스템 및 **ONTAP** 용 **FSx**

ONTAP 시스템이나 FSx for ONTAP 클러스터 자격 증명이나 필요한 각 SVM에 대한 자격 증명을 제공하여 SnapCenter 에 추가할 수 있습니다. 클러스터 자격 증명이 제공되면 클러스터의 모든 SVM이 SnapCenter 에 추가됩니다.

우리 연구실 설정에서 SnapCenter 에 스토리지 클러스터를 추가했습니다. ONTAP 클러스터는 ONTAP 스토리지 탭과 ONTAP 클러스터 유형을 선택하여 스토리지 시스템 섹션에서 구성됩니다. + 아이콘을 클릭하면 새로운 클러스터가 추가됩니다.

[너비=601, 높이=117]

다음 화면에서는 클러스터 사용자의 자격 증명을 제공해야 합니다.

클러스터 사용자 admin을 사용하면 안 됩니다. 대신, 설명된 대로 필요한 권한을 가진 새 사용자를 만들어야 합니다. "최소 권한으로 ONTAP 클러스터 역할 생성". ASA 시스템에 필요한 권한은 다음에서 찾을 수 있습니다. "ASA r2 시스템에 대한 ONTAP 클러스터 역할 생성".

[너비=299, 높이=176]

SVM은 ONTAP 스토리지 탭과 ONTAP SVMS 유형을 선택하여 스토리지 시스템 섹션에서 구성됩니다. + 아이콘을 클릭하면 새로운 SVM이 추가됩니다.

다음 화면에서는 클러스터 사용자의 자격 증명을 제공해야 합니다.

SVM 사용자 vsadmin을 사용하면 안 됩니다. 대신, 설명된 대로 필요한 권한을 가진 새 사용자를 만들어야 합니다. "최소 권한으로 SVM 역할 생성". ASA 시스템에 필요한 권한은 다음에서 찾을 수 있습니다. "ASA r2 시스템에 대한 SVM 역할 생성".

SVM의 DNS 이름은 ONTAP 시스템에 구성된 SVM 이름과 일치해야 합니다.

[너비=331, 높이=199]

Azure NetApp Files

ANF 자격 증명이 구성된 후 ANF NetApp 계정을 SnapCenter 에 추가할 수 있습니다. NetApp 계정은 스토리지 시스템 섹션에서 구성하고 Azure NetApp Files 탭을 선택하여 구성합니다. + 아이콘을 클릭하면 새로운 NetApp 계정이 추가됩니다.

[너비=601, 높이=117]

ANF 자격 증명과 구독을 선택한 후 NetApp 계정을 SnapCenter 에 추가할 수 있습니다.

[너비=401, 높이=176]

SnapMirror Active Sync 사용 시 스토리지 구성

특정 저장소 구성 단계는 다음에서 설명됩니다. "SnapMirror Active Sync를 사용한 스토리지 구성".

정책 구성

데이터 보호 전략 정책 섹션에서 설명한 대로 일반적으로 리소스와 독립적으로 구성되며 여러 SAP HANA 시스템에 사용할 수 있습니다.

일반적인 최소 구성은 다음 정책으로 구성됩니다.

- 복제 없이 매시간 백업하기 위한 정책
- SnapVault 또는 ANF 백업 복제를 통한 일일 백업 정책
- 주간 블록 무결성 검사 작업에 대한 정책
  - 파일 기반 백업 사용
  - HANA 도구 hdbpersdiag 사용

다음 섹션에서는 이러한 세 가지 정책의 구성에 대해 설명합니다.

정책은 설정 섹션에서 정책 탭을 선택하여 구성합니다. + 아이콘을 클릭하면 새로운 정책을 구성할 수 있습니다. 아래의 두 스크린샷은 Azure NetApp Files 사용하여 실행되는 HANA 시스템에 대한 정책 목록과 ONTAP 스토리지 시스템 또는 FSx for ONTAP 사용하여 실행되는 HANA 시스템에 대한 정책 목록을 보여줍니다.

[너비=601, 높이=133]

[너비=601, 높이=138]

ONTAP 시스템 및 **FSx for ONTAP** 사용한 스냅샷 백업

ONTAP 시스템이나 FSx for ONTAP 의 스냅샷 백업 정책은 로컬 스냅샷을 복제 또는 스냅샷 잠금(변조 방지 스냅샷) 작업과 결합할 수 있습니다. 이 예에서는 SnapVault 사용하여 보조 저장소로 복제하는 정책을 보여줍니다.

정책 이름과 설명(선택 사항)을 제공합니다.

[너비=376, 높이=103]

ONTAP 스토리지 유형과 스냅샷 정책 범위를 선택합니다.

[너비=385, 높이=97]

이 정책에서는 일일 일정 유형이 구성되었습니다. 매일 스냅샷이 생성되고, 스냅샷 델타는 SnapVault 사용하여 보조 저장소에 복제됩니다.

일정 자체는 개별 HANA 리소스 보호 구성에 따라 구성됩니다.

정책에 구성된 보존은 기본 스냅샷에만 유효합니다. SnapVault 대상의 보존은 HANA 데이터베이스의 개별 볼륨에 대한 ONTAP 복제 관계로 구성됩니다. 이는 챕터에서 설명합니다. "SAP HANA 스냅샷 백업 작업". 정책에 구성된 스냅샷 레이블은 ONTAP 복제 관계에 구성된 레이블과 일치해야 합니다.

스냅샷 잠금(변조 방지 스냅샷)은 확인란을 클릭하고 잠금 기간을 정의하여 활성화할 수 있습니다. 이 기능을 사용하려면 스토리지 시스템에 SnapLock 라이선스가 필요하고 규정 준수 시계가 구성되어 있어야 합니다.

로컬 스냅샷에 대한 정책만 구성하려면 시간별 일정을 적용하고 SnapVault 업데이트 확인란을 비활성화해야 합니다.

[너비=378, 높이=352]

요약 화면에는 구성된 매개변수가 표시됩니다.

[너비=385, 높이=119]

Azure NetApp Files 사용한 스냅샷 백업

Azure NetApp Files 의 스냅샷 백업 정책은 로컬 스냅샷과 ANF 백업을 결합하여 스냅샷 데이터를 Azure Blob에 복제할 수 있습니다. 이 예에서는 ANF 백업을 사용한 복제에 사용되는 정책을 보여줍니다.

정책 이름과 설명(선택 사항)을 제공합니다.

[너비=356, 높이=95]

Azure NetApp Files 저장소 유형과 스냅샷 정책 범위를 선택합니다.

[너비=360, 높이=102]

이 정책에서는 일일 일정 유형이 구성되었습니다. 매일 스냅샷이 생성되고, 스냅샷 델타는 ANF 백업을 사용하여 백업 볼트에 복제됩니다.

일정 자체는 개별 HANA 리소스 보호 구성에 따라 구성됩니다.

정책에 구성된 스냅샷 보존은 ANF 볼륨의 기본 스냅샷에 유효합니다. ANF 백업의 보존 기간은 백업 보존 설정으로 구성됩니다.

로컬 스냅샷에 대한 정책만 구성하려면 시간별 일정을 설정하고 백업 사용 확인란을 비활성화해야 합니다.

[너비=373, 높이=361]

요약 화면에는 구성된 매개변수가 표시됩니다.

[너비=376, 높이=138]

모든 플랫폼에 대한 블록 무결성 검사 작업

HANA 도구 **hdbpersdiag**

자세한 내용은 장에서 설명합니다. "SnapCenter 사용한 블록 일관성 검사".

파일 기반 백업

정책 이름과 설명(선택 사항)을 제공합니다.

[너비=346, 높이=95]

설정에 따라 ONTAP 또는 Azure NetApp Files 저장소 유형을 선택하고 파일 기반 정책 범위를 선택합니다.

[너비=357, 높이=98]

논의된 대로, 일주일에 한 번씩 블록 무결성 검사를 실행하는 것이 좋습니다. 따라서 주간 일정이 선택되었습니다.

일정 자체는 개별 HANA 리소스 보호 구성에 따라 구성됩니다.

파일 기반 백업이 기록되는 파일 시스템은 보존 설정에 정의된 것보다 더 많은 백업을 저장할 수 있는 충분한 용량을 제공해야 합니다. SnapCenter 새 백업이 생성된 후 이전 백업을 삭제하기 때문입니다. 이 예시에서는 두 개의 백업을 위한 공간이 필요하고 그 중 하나는 보존됩니다. 구성 가능한 최소 보존 기간은 0입니다.

[너비=351, 높이=173]

요약 화면에는 구성된 매개변수가 표시됩니다.

[너비=366, 높이=101]

SnapMirror Active Sync를 사용할 때의 정책 구성

특정 정책 구성 단계는 문서에 설명되어 있습니다. "SnapMirror 활성 동기화 정책 구성".

개별 **SAP HANA** 데이터베이스에 대한 **SnapCenter** 리소스 구성

백업 사용자와 사용자 저장소 키를 생성하고, 보조 백업을 위한 스토리지 복제를 설정하고, 자동 검색을 위한 HANA 플러그인을 배포하고, 정책과 일정을 사용하여 리소스 보호를 구성하여 SnapCenter 에서 개별 SAP HANA 데이터베이스를 구성합니다.

SnapCenter 에서 HANA 데이터베이스를 구성하는 단계는 다음과 같습니다.

1. SnapCenter 백업 사용자는 HANA 시스템 데이터베이스에 구성되어야 하며 SAP HANA 사용자 저장소 키는 HANA 데이터베이스 호스트에 설정되어야 합니다.
2. 보조 저장소에 대한 데이터 복제가 필요한 경우 HANA 데이터 볼륨에 대한 ONTAP 저장소 복제를 구성해야 합니다.
3. SnapCenter HANA 플러그인은 HANA 데이터베이스 호스트에 배포되어야 합니다.
    a. 자동 검색 프로세스가 시작됩니다

b. SAP HANA 사용자 저장소 키는 SnapCenter 에서 구성되어야 합니다.

c. 자동 검색의 두 번째 단계가 시작되고 HANA 리소스가 SnapCenter 에 의해 자동으로 추가됩니다.

4. 새로 추가된 HANA 리소스에 대해 HANA 리소스 보호를 구성해야 합니다.

이전 항목에서 설명한 대로 초기 SnapCenter 구성 "SnapCenter 초기 구성" HANA 데이터베이스 리소스를 구성하는 동안 자격 증명, 스토리지 시스템 및 정책이 필요하므로 먼저 이 작업을 수행해야 합니다. 아래 그림은 단계와 종속성을 요약한 것입니다.

아래 그림은 다양한 구성 구성 요소와 종속성을 시각화한 것입니다.

[너비=601, 높이=315] 다음 섹션에서는 필요한 구성 단계에 대한 자세한 설명을 제공합니다.

SAP HANA 백업 사용자 및 SAP HANA 사용자 저장소 구성

NetApp SnapCenter 사용하여 백업 작업을 실행하기 위해 HANA 데이터베이스에 전담 사용자를 구성할 것을 권장합니다. 두 번째 단계로, 이 백업 사용자에 대해 SAP HANA 사용자 저장소 키가 구성되고, SAP HANA 사용자 저장소 키는 SnapCenter 구성에 제공됩니다.

다음 그림은 SAP HANA Studio를 보여줍니다. 이 예제에서는 백업 사용자인 SNAPCENTER를 생성할 수 있습니다.

ⓘ 백업 사용자는 백업 관리자, 카탈로그 읽기, 데이터베이스 백업 관리자 및 데이터베이스 복구 운영자 권한을 갖도록 구성되어야 합니다.

ⓘ 모든 시스템 및 테넌트 데이터베이스에 대한 백업 명령은 시스템 데이터베이스를 통해 실행되므로 백업 사용자는 시스템 데이터베이스에서 생성되어야 합니다.

[너비=601, 높이=382]

HANA 데이터베이스 호스트의 **SAP HANA** 사용자 저장소 구성

SnapCenter <sid>adm 사용자를 사용하여 HANA 데이터베이스와 통신합니다. 따라서 SAP HANA 사용자 저장소 키는 데이터베이스 호스트의 <sid>adm 사용자를 사용하여 구성해야 합니다.

hdbuserstore set <키 이름> <호스트>:<포트> <데이터베이스 사용자> <비밀번호>

SAP HANA MDC 시스템의 경우 HANA 시스템 데이터베이스의 포트는 3<instanceNo>13입니다.

SAP HANA 사용자 저장소 구성 예

출력은 인스턴스 번호 = 00인 HANA 시스템에 대해 구성된 키 SS1KEY를 보여줍니다.

```
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1SAPDBCTRL
ENV : hana-1:30013
USER: SAPDBCTRL
KEY SS1KEY
ENV : hana-1:30013
USER: SNAPCENTER
KEY SYSTEMKEY
ENV : hana-1:30013
USER: SYSTEM
ACTIVE RECORDS : 10
DELETED RECORDS : 15
NUMBER OF COMPLETE KEY: 3
Operation succeed.
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

출력은 인스턴스 번호 = 12인 HANA 시스템에 대해 구성된 키 SM1KEY를 보여줍니다.

```
sm1adm@hana-2:/usr/sap/SM1/HDB12> hdbuserstore list
DATA FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.DAT
KEY FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.KEY
KEY SM1SAPDBCTRL
ENV : hana-2:31213
USER: SAPDBCTRL
KEY SM1KEY
ENV : hana-2:31213
USER: SNAPCENTER
ACTIVE RECORDS : 7
DELETED RECORDS : 9
NUMBER OF COMPLETE KEY: 2
Operation succeed.
sm1adm@hana-2:/usr/sap/SM1/HDB12>
```

스토리지 복제 구성

SnapCenter에서 복제 업데이트를 관리하기 전에 초기 데이터 전송뿐만 아니라 데이터 보호 관계의 구성을 실행해야 합니다.

다음 스크린샷은 ONTAP 시스템 관리자를 사용한 구성을 보여줍니다. ONTAP 시스템용 FSx의 경우 복제는 ONTAP CLI를 사용하여 수행해야 합니다. "개요 - SnapVault를 사용한 백업 복제".

다음 그림은 SAP HANA 시스템 SS1의 데이터 볼륨에 대해 구성된 보호 관계를 보여줍니다. 이 예제에서는 SVM hana-primary의 소스 볼륨 SS1_data_mnt00001이 SVM hana-backup과 대상 볼륨 SS1_data_mnt00001_dst로

복제됩니다.

[너비=601, 높이=183]

다음 그림은 이 랩 설정을 위해 만들어진 보호 정책을 보여줍니다. 보호 관계에 사용되는 보호 정책은 SnapMirror 레이블과 보조 저장소에서의 백업 보존을 정의합니다. 이 예에서 사용된 레이블은 '매일'이고, 보존 기간은 5로 설정되었습니다.

복제 정책의 SnapMirror 레이블은 SnapCenter 정책 구성에 정의된 레이블과 일치해야 합니다.

SnapCenter 이전에 생성된 애플리케이션 일관성 스냅샷을 기반으로 백업 작업의 일부로 SnapVault 업데이트를 트리거하므로 관계 일정은 없음으로 설정해야 합니다.

보조 백업 저장소의 백업 보존은 정책에 정의되어 있으며 ONTAP 에서 제어합니다.

[너비=601, 높이=180]

ANF 백업 구성

ANF 백업에는 특별한 준비가 필요하지 않습니다. ANF 백업이 활성화된 첫 번째 백업이 실행되자마자 SnapCenter 에서 snapcenter-vault라는 이름의 Azure 백업 볼트가 생성됩니다. 이 백업 볼트는 SnapCenter 에서 실행되는 모든 후속 ANF 백업 작업에 사용됩니다.

[너비=601, 높이=227]

SAP HANA용 SnapCenter 플러그인 배포

호스트 요구 사항은 다음에 나열되어 있습니다. "Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항".

HANA 플러그인 배포는 SnapCenter UI의 호스트 섹션에서 추가 버튼을 클릭하여 수행됩니다.

[너비=601, 높이=145]

호스트 추가 화면에서는 배포 프로세스에 사용할 호스트 유형과 이름, 자격 증명을 제공해야 합니다. 또한 SAP HANA 플러그인을 선택해야 합니다. 제출을 클릭하면 배포 프로세스가 시작됩니다.

이 설명에서는 새로운 호스트를 추가하지 않았지만 SnapCenter 에 있는 기존 호스트의 구성을 보여줍니다.

[너비=601, 높이=154]

HANA 자동 검색

HANA 플러그인 배포가 완료되면 자동 검색 프로세스가 시작됩니다. 첫 번째 단계에서는 기본 설정만 검색되고 SnapCenter UI의 리소스 섹션에 빨간색 자물쇠로 표시된 새 리소스를 만듭니다.

[너비=601, 높이=169]

리소스를 클릭하면 이 HANA 데이터베이스에 대한 SAP HANA 사용자 저장소 키를 입력하라는 메시지가 표시됩니다.

[너비=316, 높이=180]

키가 제공된 후 자동 검색 프로세스의 두 번째 단계가 시작됩니다. 자동 검색 프로세스는 HANA 시스템의 모든 테넌트 데이터베이스를 감지하고, 로그 및 카탈로그 백업 구성 세부 정보와 HANA 시스템 복제 역할을 감지합니다. 또한, 저장 공간 세부 정보가 자동으로 검색됩니다. 이러한 설정은 리소스를 선택하고 세부 정보 버튼을 클릭하면 확인할 수 있습니다.

이 자동 검색 프로세스는 각 백업 작업과 함께 실행되므로 백업 작업과 관련된 HANA 시스템의 모든 변경 사항이 자동으로 감지됩니다.

[너비=601, 높이=219]

리소스 보호 구성

자동 검색 프로세스가 완료된 후 리소스를 클릭하면 리소스 보호 구성 화면이 열립니다. 이 문서의 스크린샷은 기존 리소스의 보호 구성을 보여줍니다.

스냅샷에 대한 사용자 정의 이름 형식을 구성합니다. NetApp 어떤 백업이 어떤 정책 및 일정 유형으로 생성되었는지 쉽게 식별할 수 있도록 사용자 지정 스냅샷 이름을 사용할 것을 권장합니다.

다음 그림에 나와 있는 구성에서는 백업 및 스냅샷 복사본 이름의 형식이 다음과 같습니다.

- 예약된 시간별 백업: + SnapCenter_<호스트 이름>_LocalSnap_Hourly_<타임스탬프>
- 예약된 일일 백업: + SnapCenter_<호스트 이름>_LocalSnapAndSnapVault_Daily_<타임스탬프>

[너비=601, 높이=294]

다음 화면에서는 스크립트를 구성할 수 있으며, 이 스크립트는 백업 워크플로의 다양한 단계에서 실행되어야 합니다.

[너비=601, 높이=294]

이제 정책이 리소스에 첨부되고 일정이 정의되었습니다.

이 예에서는 다음을 구성했습니다.

- 매주 일요일에 블록 무결성 검사를 실시합니다.
- 4시간마다 로컬 스냅샷 백업
- SnapVault 복제를 통해 하루에 한 번씩 일일 스냅샷 백업

[너비=601, 높이=294]

이메일 알림을 구성할 수 있습니다.

[너비=601, 높이=294]

리소스 보호 구성이 완료되면 정의된 설정에 따라 예약된 백업이 실행됩니다.

비데이터 볼륨을 백업하도록 **SnapCenter** 구성

실행 파일, 구성 파일, 추적 파일, 애플리케이션 서버 데이터와 같은 비데이터 볼륨을 백업하도록 SnapCenter 구성합니다.

데이터베이스 설치 리소스와 필요한 로그를 계속 사용할 수 있는 경우 데이터베이스 데이터 볼륨을 보호하면 SAP HANA 데이터베이스를 특정 시점으로 복원 및 복구할 수 있습니다.

다른 비데이터 파일을 복원해야 하는 상황에서 복구하기 위해 NetApp SAP HANA 데이터베이스 백업을 보완하기 위해 비데이터 볼륨에 대한 추가 백업 전략을 개발할 것을 권장합니다. 특정 요구 사항에 따라 비데이터 볼륨의 백업은 예약 빈도와 보존 설정이 다를 수 있으며, 비데이터 파일이 얼마나 자주 변경되는지 고려해야 합니다. 예를 들어, HANA 볼륨 /hana/shared에는 실행 파일, 구성 파일뿐만 아니라 SAP HANA 추적 파일도 포함되어 있습니다. 실행 파일은 SAP HANA 데이터베이스가 업그레이드될 때만 변경되지만, SAP HANA 구성 및 추적 파일은 더 높은 백업 빈도가 필요할 수 있습니다. 또한 SnapCenter 사용하여 비데이터 볼륨 백업을 사용하여 SAP 애플리케이션 서버 볼륨을 보호할 수 있습니다.

SnapCenter 비데이터 볼륨 백업을 사용하면 SAP HANA 데이터베이스 백업과 동일한 공간 효율성으로 모든 관련 볼륨의 스냅샷 복사본을 몇 초 안에 생성할 수 있습니다. 차이점은 SAP HANA 데이터베이스와의 상호 작용이 필요 없다는 것입니다.

리소스 탭에서 비 데이터 볼륨 을 선택하고 SAP HANA 데이터베이스 추가 를 클릭합니다.

[너비=601, 높이=173]

[너비=601, 높이=112]

SAP HANA 데이터베이스 추가 대화 상자의 리소스 유형 목록에서 비 데이터 볼륨을 선택합니다. 리소스에 사용할 리소스 및 관련 SID와 SAP HANA 플러그인 호스트의 이름을 지정한 후 다음 을 클릭합니다.

[너비=332, 높이=310]

ONTAP 시스템과 FSx for ONTAP 의 경우 스토리지 유형으로 ONTAP 선택하고 SVM과 스토리지 볼륨을 스토리지 공간으로 추가한 후 다음을 클릭합니다.

[너비=332, 높이=312]

ANF의 경우 스토리지 유형을 선택하고 Azure NetApp Files NetApp 계정 및 용량 풀을 선택한 다음 ANF 볼륨을 스토리지 공간으로 추가하고 다음을 클릭합니다.

[너비=350, 높이=337]

요약 단계에서 마침 을 클릭하여 설정을 저장합니다.

필요한 모든 비데이터 볼륨에 대해 이 단계를 반복합니다. 새 리소스의 보호 구성을 계속합니다.

비데이터 볼륨 리소스에 대한 데이터 보호 구성은 SAP HANA 데이터베이스 리소스에 대한 워크플로와 동일하며 개별 리소스 수준에서 정의할 수 있습니다.

SAP HANA용 SnapCenter 중앙 플러그인 호스트 구성

SAP HANA 다중 호스트 시스템이나 IBM Power 기반 HANA 시스템을 지원하기 위해 중앙 호스트에 SnapCenter HANA 플러그인을 배포합니다. 이 절차에는 Windows 또는 Linux 호스트에 플러그인을 설치하고, SAP HANA hdbsql 클라이언트를 구성하고, 보호된 각 HANA 시스템에 대한 사용자 저장소 키를 설정하는 작업이 포함됩니다.

에서 논의된 바와 같이 "SAP HANA용 SnapCenter 플러그인 배포 옵션"HANA 플러그인은 SAP HANA 다중 호스트 시스템이나 IBM Power 환경의 SAP HANA에 필요한 중앙 플러그인 구성을 지원하기 위해 HANA 데이터베이스 외부에 배포될 수 있습니다.

중앙 플러그인 호스트는 Windows나 Linux 호스트가 될 수 있지만, 일반적으로 SnapCenter 서버 자체가 중앙 플러그인 호스트로 사용됩니다.

중앙 플러그인 호스트 구성은 다음 단계로 구성됩니다.

- SnapCenter HANA 플러그인 배포
- SAP HANA hdbsql 클라이언트 설치 및 구성
- 중앙 플러그인 호스트로 보호되는 각 HANA 시스템에 대한 SAP HANA 사용자 저장소 구성

SnapCenter HANA 플러그인 배포

호스트 요구 사항은 다음에 나열되어 있습니다. "Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항".

중앙 플러그인 호스트가 호스트로 추가되고, SAP HANA 플러그인이 호스트에 설치됩니다. 아래 스크린샷은 Windows에서 실행되는 SnapCenter 서버에 플러그인을 배포하는 모습을 보여줍니다.

1. 호스트 로 이동하고 추가 를 클릭합니다.
2. 필요한 호스트 정보를 제공합니다. 제출 을 클릭합니다.

[너비=601, 높이=166]

SAP HANA hdbsql 클라이언트 소프트웨어 설치 및 구성

SAP HANA hdbsql 클라이언트 소프트웨어는 SAP HANA 플러그인이 설치된 동일한 호스트에 설치해야 합니다. 소프트웨어는 다음에서 다운로드할 수 있습니다. "SAP 지원 포털".

HANA 리소스 구성 중에 구성된 hdbsql OS 사용자는 hdbsql 실행 파일을 실행할 수 있어야 합니다. hdbsql 실행 파일의 경로는 hana.properties 파일이나 OS 사용자의 검색 경로 매개변수(%PATH%, $PATH)에서 구성해야 합니다.

Windows의 중앙 플러그인 호스트:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties

HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

Linux의 중앙 플러그인 호스트:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties

HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

중앙 플러그인 호스트를 위한 **SAP HANA** 사용자 저장소 구성

중앙 플러그인 호스트에서 관리하는 각 HANA 시스템에 대해 SAP HANA 사용자 저장소 키를 구성해야 합니다. 중앙 플러그인 호스트에서 키를 구성하기 전에 다음에서 설명한 대로 데이터베이스 사용자를 생성해야 합니다. "SAP HANA 백업 사용자 및 SAP HANA 사용자 저장소 구성".

SAP HANA 플러그인과 SAP hdbsql 클라이언트가 Windows에 설치된 경우 로컬 시스템 사용자는 hdbsql 명령을 실행하고 기본적으로 리소스 구성에서 구성됩니다. 시스템 사용자는 로그온 사용자가 아니므로 SAP HANA 사용자 저장소 구성은 -u <사용자> 옵션을 사용하여 다른 사용자로 수행해야 합니다.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>
<password>
```

SAP HANA 다중 호스트 설정의 경우 모든 호스트에 대한 SAP HANA 사용자 저장소 키를 구성해야 합니다. SnapCenter 제공된 각 키를 사용하여 데이터베이스에 연결을 시도하므로 시스템 데이터베이스(HANA 네임 서버)가 다른 호스트로 장애 조치되는 것과 관계없이 독립적으로 작동할 수 있습니다. 모든 작업자와 대기 호스트에 대해 SAP HANA 사용자 저장소 키가 구성됩니다. 이 예에서 HANA 데이터베이스 사용자인 SNAPCENTER는 시스템 데이터베이스에 구성된 사용자입니다.

```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.DAT
KEY FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
ENV : hana-4:30013
USER: SNAPCENTER
KEY MS1KEYHOST2
ENV : hana-5:30013
USER: SNAPCENTER
KEY MS1KEYHOST3
ENV : hana-6:30013
USER: SNAPCENTER
KEY SS2KEY
ENV : hana-3:30013
USER: SNAPCENTER

C:\Program Files\sap\hdbclient>
```

HANA 수동 리소스 구성

SnapCenter 에서 리소스 보기의 추가 버튼을 클릭하면 수동으로 구성된 HANA 시스템 리소스가 생성됩니다.

[너비=601, 높이=189]

다음 화면에서는 몇 가지 시스템 매개변수를 제공해야 합니다.

- 플러그인 호스트: 중앙 플러그인 호스트를 선택해야 합니다.
- SAP HANA 사용자 저장소 키: 단일 호스트 HANA 시스템의 경우 중앙 플러그인 호스트에서 준비된 키 이름을 제공해야 합니다. 다중 호스트 HANA 시스템의 경우 시스템의 모든 키를 쉼표로 구분하여 나열해야 합니다.
- HDBSQL OS 사용자: 중앙 플러그인 호스트가 Windows에서 실행되는 경우 사용자는 SYSTEM 사용자로 미리 선택됩니다. 그렇지 않으면 SAP HANA 사용자 저장소 키에 사용된 사용자를 제공해야 합니다.

[너비=384, 높이=357]

다음 단계로 저장 공간을 구성해야 합니다. HANA 시스템에 속하는 모든 ONTAP 또는 ANF 볼륨을 여기에 추가해야 합니다.

[너비=385, 높이=359]

이제 자동 검색된 HANA 시스템과 동일한 방식으로 리소스 보호 구성을 수행할 수 있습니다.

SnapCenter 에서 SAP HANA 스냅샷에 대한 백업 작업에 대해 알아보세요.

SnapCenter 사용하여 SAP HANA 스냅샷 백업을 수행합니다. SnapVault 또는 Azure NetApp Files 백업을 사용한 데이터베이스 스냅샷 백업, 블록 무결성 검사, 비데이터 볼륨 백업 및 백업 복제에 대해 알아보세요.

SnapCenter에서 데이터베이스 백업은 일반적으로 각 HANA 데이터베이스의 리소스 보호 구성 내에 정의된 일정을 사용하여 실행됩니다.

필요 시 데이터베이스 백업은 SnapCenter GUI, PowerShell 명령줄 또는 REST API를 사용하여 수행할 수 있습니다.

SnapCenter 다음과 같은 백업 작업을 지원합니다.

- HANA 데이터베이스 스냅샷 백업 작업
- 블록 무결성 검사 작업
- 비데이터 볼륨의 스냅샷 백업
- HANA 데이터베이스 또는 비데이터 볼륨 백업을 위한 SnapVault 또는 ANF 백업을 사용한 백업 복제

다음 섹션에서는 SnapCenter (HANA 데이터베이스 호스트에 배포된 HANA 플러그인)에서 자동으로 검색된 단일 호스트 HANA 시스템에 대한 다양한 작업을 설명합니다.

SnapCenter 의 SAP HANA 스냅샷 백업

SnapCenter 리소스 토폴로지는 SnapCenter 에서 생성된 백업 목록을 보여줍니다. 다음 그림은 기본 저장소에서 사용 가능한 백업을 보여주며 가장 최근의 백업을 강조 표시합니다.

[너비=601, 높이=293]

보조 저장소의 백업은 Vault 복사본 아이콘을 클릭하면 나열할 수 있습니다.

[너비=601, 높이=294]

다음 스크린샷은 변조 방지 스냅샷이 구성된 시스템 SM1의 백업 목록을 보여줍니다.

[너비=601, 높이=293]

SAP HANA Studio에서 SAP HANA 스냅샷 백업

SAP HANA MDC 시스템의 스토리지 스냅샷을 사용하여 백업을 수행하면 데이터 볼륨의 스냅샷 복사본이 생성됩니다. 이 데이터 볼륨에는 시스템 데이터베이스의 데이터와 모든 테넌트 데이터베이스의 데이터가 포함되어 있습니다. 이러한 물리적 아키텍처를 반영하기 위해 SAP HANA는 SnapCenter 스냅샷 백업을 트리거할 때마다 시스템 데이터베이스와 모든 테넌트 데이터베이스의 결합된 내부 데이터베이스 스냅샷을 내부적으로 수행합니다. 이로 인해 SAP HANA 백업 카탈로그에 여러 개의 별도 백업 항목이 생성됩니다. 하나는 시스템 데이터베이스용이고 다른 하나는 각 테넌트 데이터베이스용입니다.

SAP HANA 백업 카탈로그에서 SnapCenter 백업 이름은 외부 백업 ID(EBID)와 함께 주석 필드로 저장됩니다. 이는 시스템 데이터베이스에 대한 다음 스크린샷과 테넌트 데이터베이스 SS1에 대한 다음 스크린샷에 표시됩니다. 두 그림 모두 주석 필드에 저장된 SnapCenter 백업 이름과 EBID를 강조 표시합니다.

[너비=601, 높이=289]

[너비=601, 높이=296]

SnapCenter 자체 백업만 인식합니다. 예를 들어 SAP HANA Studio를 사용하여 생성된 추가 백업은 SAP HANA 카탈로그에서는 볼 수 있지만 SnapCenter 에서는 볼 수 없습니다. 또한 스토리지 시스템에서 직접 생성된 스냅샷은 SnapCenter 에 표시되지 않습니다.

스토리지 계층의 **SAP HANA** 스냅샷 백업

스토리지 계층의 백업을 보려면 NetApp System Manager를 사용하여 데이터베이스 볼륨을 선택하면 됩니다. 다음 스크린샷은 기본 저장소에서 SS1_data_mnt00001 데이터베이스 볼륨에 대해 사용 가능한 백업을 보여줍니다. 강조 표시된 백업은 이전 이미지에서 SnapCenter 와 SAP HANA Studio에 표시된 백업이며 동일한 명명 규칙을 따릅니다.

[너비=601, 높이=294]

다음 스크린샷은 보조 스토리지 시스템의 복제 대상 볼륨 hana_SS1_data_mnt00001_dest에 대해 사용 가능한 백업을 보여줍니다.

[너비=601, 높이=294]

ANF를 사용한 **SAP HANA** 스냅샷 백업

다음 스크린샷은 Azure NetApp Files 사용한 HANA 시스템의 토폴로지 보기를 보여줍니다. 이 HANA 시스템의 경우 로컬 스냅샷 백업과 ANF 백업을 사용한 백업 복제가 구성되었습니다.

[너비=601, 높이=303]

ANF 볼륨의 스냅샷 백업은 Azure Portal을 사용하여 나열할 수 있습니다.

[너비=601, 높이=258]

백업 아이콘을 클릭하면 ANF 백업으로 복제된 백업을 나열할 수 있습니다.

[너비=601, 높이=304]

ANF 백업은 Azure Portal에도 나열될 수 있습니다.

[너비=601, 높이=216]

비데이터 볼륨의 스냅샷 백업

SnapCenter 리소스 토폴로지는 비데이터 볼륨에 대한 백업 목록을 보여줍니다. 다음 그림에서는 HANA 공유 볼륨의 백업이 나열되어 있습니다.

[너비=601, 높이=294]

HANA 데이터베이스 백업을 위한 백업 워크플로

HANA 데이터베이스 스냅샷 백업을 위한 백업 워크플로는 세 가지 주요 섹션으로 구성됩니다.

- 자동 검색
  - 응용 프로그램 검색, 예:
    - SnapCenter 모든 테넌트 구성 변경 사항을 감지합니다.
    - SnapCenter HANA 시스템 복제 기본 노드를 감지합니다.
  - 파일 시스템 및 스토리지 검색, 예:
    - SnapCenter 볼륨 구성의 변경 사항을 감지합니다.
    - SnapCenter HANA 다중 파티션 구성을 감지합니다.
- HANA 및 스냅샷 백업 작업
  - HANA 데이터베이스 스냅샷 트리거
  - 스토리지 스냅샷 만들기
  - HANA 데이터베이스 스냅샷을 확인하고 HANA 백업 카탈로그에 백업을 등록합니다.
- 보존 관리
  - 정의된 보존 기간을 기준으로 스냅샷 백업을 삭제합니다.
    - SnapCenter 저장소
    - 스토리지
    - HANA 백업 카탈로그
  - 로그 백업 보존 관리
    - 파일 시스템 및 HANA 백업 카탈로그에서 로그 백업 삭제

[너비=339, 높이=475]

비데이터 볼륨에 대한 백업 워크플로

비데이터 볼륨의 경우 백업 워크플로는 스냅샷 작업과 보존 관리 작업으로 구성됩니다.

[너비=329, 높이=404]

2차 백업 정리

에서 설명한 대로 "2차 백업에 대한 보존 관리", 보조 백업 저장소에 대한 데이터 백업의 보존 관리 작업은 ONTAP 에서 처리합니다. SnapCenter 주 단위 기본 일정으로 정리 작업을 실행하여 ONTAP 보조 백업 저장소에서 백업을 삭제했는지 주기적으로 확인합니다.

SnapCenter 정리 작업은 보조 백업 저장소에서 삭제된 백업이 식별된 경우 SnapCenter 저장소와 SAP HANA 백업 카탈로그에서 백업을 삭제합니다.

[너비=601, 높이=158]

[너비=267, 높이=330]

이 예약된 정리가 완료될 때까지 SAP HANA와 SnapCenter 보조 백업 저장소에서 이미 삭제된 백업을 계속 표시합니다. 이렇게 하면 보조 백업 저장소에 있는 해당 저장소 기반 스냅샷 백업이 이미 삭제된 경우에도 추가 로그 백업이 유지됩니다. NetApp 더 이상 필요하지 않은 로그 백업을 피하기 위해 일정을 주간에서 일간으로 변경할 것을

권장합니다.

SnapCenter 정리 작업의 빈도를 변경합니다

SnapCenter 기본적으로 모든 리소스에 대해 주 단위로 정리 작업 SnapCenter_RemoveSecondaryBackup을 실행합니다. 이는 SnapCenter PowerShell cmdlet을 사용하여 변경할 수 있습니다.

```
SnapCenterPS C:\> Open-SmConnection

Enter username/password
User: sapcc\scadmin
Password for user sapcc\scadmin: **********

SnapCenterPS C:\> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"="1"}
-TaskName SnapCenter_RemoveSecondaryBackup

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExist : False
UserName :
Password :
SchedulerType : Daily
RepeatTask_Every_Hour : 1
IntervalDuration :
EndTime :
LocalScheduler : False
AppType : False
AuthMode :
SchedulerSQLInstance : SMCoreContracts.SmObject
MonthlyFrequency :
Hour : 0
Minute : 0
NodeName :
ScheduleID : 0
RepeatTask_Every_Mins :
CronExpression :
CronOffsetInMinutes :
StrStartTime :
StrEndTime :
```

```
ScheduleCategory :
PolicyId : 0
PolicyName :
ProtectionGroupId : 0
ProtectionGroupName :
PluginCode : NONE
PolicyType : None
ReportTriggerName :
PolicyScheduleId : 0
HoursOfTheDay :
DayStartTime :
MinuteOffset : ZeroMinutes
SnapMirrorLabel :
BackupType :
SnapCenterPS C:\>
```

구성은 SnapCenter UI의 모니터 - 일정 보기에서도 확인할 수 있습니다.

[너비=601, 높이=257]

리소스 레벨의 수동 새로 고침

필요한 경우 리소스의 토폴로지 보기에서 보조 백업의 수동 정리를 실행할 수도 있습니다. 다음 스크린샷에 표시된 것처럼, 보조 백업을 선택하면 SnapCenter 보조 백업 저장소에 있는 백업이 표시됩니다. SnapCenter 새로 고침 아이콘을 사용하여 정리 작업을 실행하여 이 리소스의 백업을 동기화합니다.

[너비=601, 높이=291]

SnapCenter 사용하여 SAP HANA 블록 일관성 검사 실행

SAP hdbpersdiag 도구를 사용하거나 파일 기반 백업을 실행하여 SAP HANA 블록 일관성 검사를 실행합니다. 로컬 스냅샷 디렉토리 액세스, FlexClone 볼륨을 갖춘 중앙 검증 호스트, 스케줄링 및 자동화를 위한 SnapCenter 통합을 포함한 구성 옵션에 대해 알아보세요.

아래 표는 사용자 환경에 가장 적합한 블록 일관성 검사 방법을 결정하는 데 도움이 되는 주요 매개변수를 요약한 것입니다.

	로컬 스냅샷 디렉토리를 사용하는 **HANA hdbpersdiag** 도구	중앙 검증 호스트가 있는 **HANA hdbpersdiag** 도구	파일 기반 백업
지원되는 구성	NFS만 베어 메탈, ANF, FSx ONTAP, VMware 또는 KVM 인게스트 마운트	모든 프로토콜 및 플랫폼	모든 프로토콜 및 플랫폼
HANA 호스트의 CPU 부하	중간	None	높은

	로컬 스냅샷 디렉토리를 사용하는 **HANA hdbpersdiag** 도구	중앙 검증 호스트가 있는 **HANA hdbpersdiag** 도구	파일 기반 백업
HANA 호스트의 네트워크 활용	높은	None	높은
실행 시간	스토리지 볼륨의 전체 읽기 처리량을 활용합니다.	스토리지 볼륨의 전체 읽기 처리량을 활용합니다.	일반적으로 대상 시스템의 쓰기 처리량에 의해 제한됨
용량 요구 사항	None	None	HANA 시스템당 최소 1배의 백업 크기
SnapCenter 통합	백업 후 스크립트	복제 생성 및 복제 후 스크립트, 복제 삭제	내장 기능
스케줄링	SnapCenter 스케줄러	클론 생성 및 삭제 워크플로를 실행하기 위한 PowerShell 스크립트, 외부 예약	SnapCenter 스케줄러

다음 장에서는 블록 일관성 검사 작업을 위한 다양한 옵션의 구성과 실행에 대해 설명합니다.

로컬 스냅샷 디렉토리를 사용하여 **hdbpersdiag**로 일관성 검사

SnapCenter 내에서 hdbpersdiag 작업에 대한 전담 정책이 일일 일정과 2개의 보존 기간으로 생성됩니다. 주간 일정을 사용하지 않는 이유는 최소 2개의 스냅샷 백업(최소 보존 기간=2)이 필요하고, 그중 하나는 최대 2주 전까지의 내용이기 때문입니다.

HANA 시스템의 SnapCenter 리소스 보호 구성 내에 hdbpersdiag 도구를 실행하는 백업 후 스크립트가 추가되었습니다. 백업 후 스크립트는 리소스에 대해 구성된 다른 정책과 함께 호출되므로 스크립트에서 현재 활성화된 정책을 확인해야 합니다. 스크립트 내에서 우리는 또한 요일을 확인하고 hdbpersdiag 작업을 일주일에 한 번 일요일에 실행합니다. 그런 다음 현재 스냅샷 백업 디렉토리의 해당 hdb* 디렉토리에 있는 각 데이터 볼륨에 대해 HANA hdbpersdiag가 호출됩니다. hdbpersdiag를 사용하여 일관성 검사를 수행한 결과 오류가 보고되면 SnapCenter 작업이 실패로 표시됩니다.

> 예제 스크립트 call-hdbpersdiag.sh는 그대로 제공되며 NetApp 지원에 포함되지 않습니다. 스크립트는 ng-sapcc@netapp.com으로 이메일을 보내 요청하실 수 있습니다.

아래 그림은 일관성 검사 구현의 상위 수준 개념을 보여줍니다.

[너비=601, 높이=248]

첫 번째 단계로 스냅샷 디렉토리에 대한 액세스를 허용해야 합니다. 이렇게 하면 HANA 데이터베이스 호스트에서 """.snapshot" 디렉토리가 표시됩니다.

- ONTAP 시스템 및 ONTAP 용 FSX: 스냅샷 디렉토리 액세스 볼륨 매개변수를 구성해야 합니다.
- ANF: 스냅샷 경로 볼륨 매개변수를 구성해야 합니다.

다음 단계로, 백업 후 스크립트에 사용된 이름과 일치하는 정책을 구성해야 합니다. 스크립트 예시에서는 이름이 SnapAndCallHdbpersdiag여야 합니다. 앞서 논의한 대로 일일 일정은 주간 일정으로 오래된 스냅샷을 보관하는 것을 피하기 위해 사용됩니다.

[너비=414, 높이=103]

[너비=424, 높이=108]

[너비=433, 높이=336]

리소스 보호 구성 내에서 백업 후 스크립트가 추가되고, 정책이 리소스에 할당됩니다.[너비=601, 높이=294]

[너비=601, 높이=281]

마지막으로, 스크립트는 HANA 호스트의 allowed_commands.config 파일에서 구성되어야 합니다.

```
hana-1:/ # cat /opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag.sh
```

스냅샷 백업 작업은 이제 하루에 한 번 실행되고, 스크립트는 hdbpersdiag 검사가 일요일에 일주일에 한 번만 실행되도록 처리합니다.

스크립트는 데이터 볼륨 암호화에 필요한 "-e" 명령줄 옵션과 함께 hdbpersdiag를 호출합니다. HANA 데이터 볼륨 암호화가 사용되지 않으면 매개변수를 제거해야 합니다.

아래 출력은 스크립트의 로그 파일을 보여줍니다.

```
20251024055824###hana-1###call-hdbpersdiag.sh: Current policy is
SnapAndCallHdbpersdiag
20251024055824###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001
20251024055827###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001/ (4.8 GB,
5100273664 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
```

```
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (94276 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055827###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001.
20251024055827###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003
20251024055828###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003/
(320.0 MB, 335544320 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251024055828###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003.
```

```
20251024055828###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003
20251024055833###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003/
(4.6 GB, 4898947072 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (100817 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055833###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003.
20251024060048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnapAndSnapVault, consistency check is only done with Policy
SnapAndCallHdbpersdiag
20251024080048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnap, consistency check is only done with Policy SnapAndHdbpersdiag
```

중앙 검증 호스트를 사용하여 **hdbpersdiag**로 일관성 검사

아래 그림은 솔루션 아키텍처와 워크플로우에 대한 개략적인 보기를 보여줍니다. 중앙 검증 호스트를 사용하면 검증 호스트를 사용하여 여러 개의 서로 다른 HANA 시스템의 일관성을 확인할 수 있습니다. 이 솔루션은 SnapCenter 복제본 생성 및 삭제 워크플로를 활용하여 HANA 시스템에서 복제된 볼륨을 연결하고 이를 검증 호스트에 연결합니다. HANA hdbpersdiag 도구를 실행하려면 복제 후 스크립트가 사용됩니다. 두 번째 단계로 SnapCenter 복제 삭제 워크플로를 사용하여 복제된 볼륨을 마운트 해제하고 삭제합니다.

HANA 시스템이 데이터 볼륨 암호화로 구성된 경우 hdbpersdiag를 실행하기 전에 소스 HANA 시스템의 암호화 루트 키를 검증 호스트로 가져와야 합니다. 또한 참조하세요 "데이터베이스 복구 전 백업된 루트 키 가져오기 | SAP 도움말 포털"

[너비=601, 높이=257]

HANA 도구 hdbpersdiag는 모든 HANA 설치에 포함되어 있지만 독립형 도구로는 사용할 수 없습니다. 따라서 일반적인 HANA 시스템을 설치하여 중앙 검증 호스트를 준비해야 합니다.

초기 일회성 준비 단계:

- 중앙 검증 호스트로 사용할 SAP HANA 시스템 설치
- SnapCenter 에서 SAP HANA 시스템 구성
  - 검증 호스트에 SnapCenter SAP HANA 플러그인을 배포합니다. SAP HANA 시스템은 SnapCenter 에 의해 자동으로 검색됩니다.
- 초기 설치 후 첫 번째 hdbpersdiag 작업은 다음 단계로 준비됩니다.
  - 대상 SAP HANA 시스템을 종료합니다
  - SAP HANA 데이터 볼륨을 마운트 해제합니다.

대상 시스템에서 실행해야 하는 스크립트를 SnapCenter allowed commands config 파일에 추가해야 합니다.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag-flexclone.sh
```

예제 스크립트 call-hdbpersdiag-flexclone.sh는 그대로 제공되며 NetApp 지원에 포함되지 않습니다. 스크립트는 ng-sapcc@netapp.com으로 이메일을 보내 요청하실 수 있습니다.

수동 워크플로 실행

대부분의 경우 일관성 검사 작업은 다음 장에서 설명하는 대로 예약된 작업으로 실행됩니다. 그러나 수동 작업 흐름을 알고 있으면 자동화 프로세스에 사용되는 매개변수를 이해하는 데 도움이 됩니다.

복제본 생성 워크플로는 시스템에서 확인해야 할 백업을 선택하고 백업에서 복제를 클릭하여 시작됩니다.

[너비=601, 높이=247]

다음 화면에서는 검증 호스트의 호스트 이름, SID 및 스토리지 네트워크 인터페이스를 제공해야 합니다.

검증 호스트에 설치된 HANA 시스템의 SID를 항상 사용하는 것이 중요합니다. 그렇지 않으면 워크플로가 실패합니다.

[너비=431, 높이=115]

다음 화면에서는 call-hdbpersdiag-fleclone.sh 스크립트를 복제 후 명령으로 추가해야 합니다.

[너비=442, 높이=169]

워크플로가 시작되면 SnapCenter 선택한 스냅샷 백업을 기반으로 복제된 볼륨을 생성하고 이를 검증 호스트에 마운트합니다.

참고: 아래의 예시 출력은 저장 프로토콜로 NFS를 사용하는 HANA 시스템을 기반으로 합니다. FC 또는 VMware VMDK를 사용하는 HANA 시스템의 경우 장치는 동일한 방식으로 /hana/data/SID/mnt00001에 마운트됩니다.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 8.0K 16G 1% /dev
tmpfs 25G 0 25G 0% /dev/shm
tmpfs 16G 474M 16G 3% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 9.0G 48G 16% /
/dev/mapper/system-root 60G 9.0G 48G 16% /home
/dev/mapper/system-root 60G 9.0G 48G 16% /.snapshots
/dev/mapper/system-root 60G 9.0G 48G 16% /root
/dev/mapper/system-root 60G 9.0G 48G 16% /opt
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 9.0G 48G 16% /srv
/dev/mapper/system-root 60G 9.0G 48G 16% /usr/local
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 9.0G 48G 16% /var
/dev/mapper/system-root 60G 9.0G 48G 16% /tmp
/dev/sda1 500M 5.1M 495M 2% /boot/efi
192.168.175.117:/QS1_shared/usr-sap 251G 15G 236G 6% /usr/sap/QS1
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
192.168.175.117:/QS1_log_mnt00001 251G 335M 250G 1% /hana/log/QS1/mnt00001
192.168.175.117:/QS1_shared/shared 251G 15G 236G 6% /hana/shared
tmpfs 3.2G 20K 3.2G 1% /run/user/467
tmpfs 3.2G 0 3.2G 0% /run/user/0
192.168.175.117:/SS2_data_mnt00001_Clone_10292511250337819 250G 6.4G 244G
3% /hana/data/QS1/mnt00001
```

아래 출력은 클론 후 명령 call-hdbpersdiag-flexclone.sh의 로그 파일을 보여줍니다.

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (65388 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251029112601###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
```

```
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (79333 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
```

스크립트는 데이터 볼륨 암호화에 필요한 "-e" 명령줄 옵션과 함께 hdbpersdiag를 호출합니다. HANA 데이터 볼륨 암호화가 사용되지 않으면 매개변수를 제거해야 합니다. 클론 후 스크립트가 완료되면 SnapCenter 작업도 완료됩니다.

[너비=279, 높이=344]

다음 단계로 SnapCenter 복제 삭제 워크플로를 실행하여 검증 호스트를 정리하고 FlexClone 볼륨을 삭제합니다.

소스 시스템의 토폴로지 뷰에서 복제본을 선택하고 삭제 버튼을 클릭합니다.

[너비=601, 높이=165]

이제 SnapCenter 검증 호스트에서 복제된 볼륨을 마운트 해제하고 스토리지 시스템에서 복제된 볼륨을 삭제합니다.

PowerShell 스크립트를 사용한 **SnapCenter** 워크플로 자동화

이전 섹션에서는 SnapCenter UI를 사용하여 복제본 생성 및 복제본 삭제 워크플로를 실행했습니다. 모든 워크플로는 PowerShell 스크립트나 REST API 호출을 통해서도 실행될 수 있으므로 추가적인 자동화가 가능합니다. 다음 섹션에서는 SnapCenter 복제본 생성 및 복제본 삭제 워크플로를 실행하는 기본 PowerShell 스크립트 예를 설명합니다.

예제 스크립트 call-hdbpersdiag-flexclone.sh 및 clone-hdbpersdiag.ps1은 그대로 제공되며 NetApp 지원에 포함되지 않습니다. 스크립트는 ng-sapcc@netapp.com으로 이메일을 보내 요청할 수 있습니다.

PowerShell 예제 스크립트는 다음 워크플로를 실행합니다.

- 명령줄 매개변수 SID 및 소스 호스트에 따라 최신 스냅샷 백업을 검색합니다.
- 이전 단계에서 정의한 스냅샷 백업을 사용하여 SnapCenter 복제본 생성 워크플로를 실행합니다. 스크립트에는 대상 호스트 정보와 hdbpersdiag 정보가 정의되어 있습니다. call-hdbpersdiag-flexclone.sh 스크립트는 복제 후 스크립트로 정의되며 대상 호스트에서 실행됩니다.
  - $result = New-SmClone -AppPluginCode hana -BackupName $backupName -Resources @{"Host"="$sourceHost";"UID"="$uid"} -CloneToInstance "$verificationHost" -NFSExportIPs $exportIpTarget -CloneUid $targetUid -PostCloneCreateCommands $postCloneScript
- SnapCenter 복제본 삭제 워크플로를 실행합니다. 아래 텍스트는 SnapCenter 서버에서 실행되는 예제 스크립트의 출력을 보여줍니다.

아래 텍스트는 SnapCenter 서버에서 실행되는 예제 스크립트의 출력을 보여줍니다.

```
C:\Users\scadmin>pwsh -command "c:\netapp\clone-hdbpersdiag.ps1 -sid SS2
-sourceHost hana-3.sapcc.stl.netapp.com"
Starting verification
Connecting to SnapCenter
Validating clone/verification request - check for already existing clones
Get latest back for [SS2] on host [hana-3.sapcc.stl.netapp.com]
Found backup name [SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]
Creating clone from backup [hana-
3.sapcc.stl.netapp.com/SS2/SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]: [hana-7.sapcc.stl.netapp.com/QS1]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Completed]
Removing clone [SS2 - HANA System Replication__clone__169851_MDC_SS2_07-
09-2025_07.44.09]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Completed]
Verification completed

C:\Users\scadmin>
```

스크립트는 데이터 볼륨 암호화에 필요한 "-e" 명령줄 옵션과 함께 hdbpersdiag를 호출합니다. HANA 데이터 볼륨 암호화가 사용되지 않으면 매개변수를 제거해야 합니다.

아래 출력은 call-hdbpersdiag-flexclone.sh 스크립트의 로그 파일을 보여줍니다.

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
```

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
              Logical Pages (65415 pages) OK
                    Logical Pages Linkage OK
Checking entries from restart page...
                       ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                             LobDirectory OK
                     MidSizeLobDirectory OK
                             LobFileIDMap OK
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
```

```
              Logical Pages (4099 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                  UndoContainerDirectory OK
                           DRLoadedTable OK
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                  Default Converter Pages OK
                   Static Converter Pages OK
                 RowStore Converter Pages OK
             Logical Pages (79243 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                       ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                            LobDirectory OK
                           DRLoadedTable OK
                     MidSizeLobDirectory OK
                            LobFileIDMap OK
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
hana-7:/mnt/sapcc-share/hdbpersdiag #
```

파일 기반 백업

SnapCenter 파일 기반 백업이 백업 유형으로 선택된 정책을 사용하여 블록 무결성 검사를 실행할 수 있도록 지원합니다.

이 정책을 사용하여 백업을 예약하면 SnapCenter 시스템과 모든 테넌트 데이터베이스에 대한 표준 SAP HANA 파일

백업을 만듭니다.

SnapCenter는 스냅샷 복사본 기반 백업과 같은 방식으로 블록 무결성 검사를 표시하지 않습니다. 대신 요약 카드에는 파일 기반 백업 수와 이전 백업 상태가 표시됩니다.

[너비=601, 높이=293]

SAP HANA 백업 카탈로그에는 시스템과 테넌트 데이터베이스 모두에 대한 항목이 표시됩니다. 다음 그림에서는 시스템 데이터베이스의 백업 카탈로그에 있는 SnapCenter 블록 무결성 검사를 보여 줍니다.

[너비=601, 높이=293]

블록 무결성 검사가 성공적으로 완료되면 표준 SAP HANA 데이터 백업 파일이 생성됩니다.

[너비=351, 높이=433]

SnapCenter 파일 기반 데이터 백업 작업을 위해 HANA 데이터베이스에 구성된 백업 경로를 사용합니다.

```
hana-1:/hana/shared/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 3717564
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 159744 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1
-rw-r----- 1 ss1adm sapsys 83898368 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_2_1
-rw-r----- 1 ss1adm sapsys 3707777024 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_3_1
SYSTEMDB:
total 3339236
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 163840 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1

-rw-r----- 1 ss1adm sapsys 3405787136 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_1_1
```

SnapCenter 사용하여 SAP HANA 데이터베이스 복원 및 복구

SnapCenter 사용하여 자동 또는 수동 복구 옵션을 통해 SAP HANA 시스템을 복원하고 복구하세요. 여기에는 전체 시스템 복원, ONTAP 의 HANA 데이터베이스, Azure NetApp Files 및 FSx for ONTAP 에 대한 단일 테넌트 복원이 포함됩니다.

SnapCenter 다음과 같은 복원 및 복구 작업을 지원합니다.

- 단일 테넌트가 있는 SAP HANA MDC 시스템
  - 종단 간 자동 복원 및 복구
  - 종단 간 자동 복구 및 수동 복구(선택 가능)
- 여러 테넌트가 있는 SAP HANA MDC 시스템
  - 종단 간 자동 복구, 복구는 수동으로 수행해야 함
- 단일 테넌트의 복원
  - 종단 간 자동 복구, 복구는 수동으로 수행해야 함

ⓘ 자동 복구는 HANA 플러그인이 HANA 데이터베이스 호스트에 배포되고 HANA 시스템이 SnapCenter에 의해 자동으로 검색된 경우에만 지원됩니다. 중앙 플러그인 호스트 구성을 사용하는 경우 SnapCenter 사용하여 복원 작업을 수행한 후 수동으로 복구를 수행해야 합니다.

ⓘ Azure NetApp Files에서는 기본 ANF 볼륨 또는 ANF 백업에 대한 복원 작업이 지원됩니다. 기본 ANF 볼륨의 경우 볼륨 되돌리기가 실행되고, ANF 백업의 경우 단일 파일 복원을 통한 제자리 복원이 실행됩니다. 두 경우 모두 애플리케이션 볼륨 그룹 구성은 유지됩니다.

ⓘ 볼륨 암호화가 활성화되어 있고 SAP 로컬 보안 저장소(LSS)를 사용하는 경우, 백업 이후 LSS의 루트 키 백업 암호가 변경되지 않았다면 SnapCenter를 사용한 복구가 지원됩니다. 암호가 변경되었고 다른 암호를 사용하는 이전 스냅샷을 사용하여 복원 및 복구를 수행하는 경우, 복구는 수동으로 수행해야 하며 복구 명령문에 이전 암호를 제공해야 합니다: "RECOVER DATA USING SNAPSHOT CLEAR LOG ENCRYPTION ROOT KEYS BACKUP PASSWORD 'old-password'"

단일 테넌트가 있는 **SAP HANA MDC** 시스템에 대한 자동 복원 및 복구

복원 작업은 리소스 토폴로지 보기에서 스냅샷 백업을 선택하고 복원을 클릭하여 시작됩니다.

[너비=601, 높이=294]

ANF에서 NFS를 사용하는 HANA 시스템, ONTAP 용 FSx 또는 ONTAP 스토리지 시스템의 경우 기본 볼륨 스냅샷에 대해 볼륨 되돌리기 작업을 포함하거나 포함하지 않고 전체 복원을 선택할 수 있습니다.

- 볼륨 되돌리기 없는 전체 리소스는 SFSR(Single File SnapRestore)을 사용하여 데이터베이스의 모든 파일을 복원합니다.
- 볼륨 되돌리기가 있는 전체 리소스는 볼륨 기반 복원 작업(VBSR)을 사용하여 전체 볼륨을 선택한 스냅샷 상태로 되돌립니다.

ⓘ 활성 SnapVault 또는 SnapMirror 복제 스냅샷보다 오래된 스냅샷으로 복원해야 하는 경우 볼륨 되돌리기를 사용할 수 없습니다.

ⓘ 볼륨 되돌리기 작업은 되돌리기 작업에 선택된 스냅샷보다 최신인 모든 스냅샷 백업을 삭제합니다.

ⓘ SFSR을 사용한 복원은 볼륨 되돌리기 작업만큼 빠르지만 백그라운드 프로세스가 메타데이터 작업을 완료할 때까지 모든 스냅샷 작업이 차단됩니다.

[너비=300]

FC SAN을 사용하는 베어 메탈 호스트의 HANA 시스템의 경우 볼륨 되돌리기(VBSR)가 지원되지 않고 대신 복원 작업에는 항상 SFSR이 사용됩니다. VMFS가 있는 VMware에서 실행되는 HANA 시스템의 경우 복제, 마운트, 복사 작업이 사용됩니다.

[너비=345, 높이=325]

보조 백업에서 복원하려면 보관 위치를 선택해야 합니다.

[너비=345, 높이=323]

복구 범위를 사용하면 로그 백업을 사용하지 않고 '최근 상태로', '특정 시점으로' 또는 저장 지점 복구를 선택할 수 있습니다. 복구 안 함을 선택하면 SnapCenter 복원 작업만 실행하고 복구는 설명된 대로 수동으로 수행해야 합니다. "HANA Studio를 사용한 수동 복구".

SnapCenter SAP HANA에 구성된 경로를 로그 백업 및 카탈로그 백업 위치에 사용합니다. 추가 위치에 계층형 백업이 있는 경우 이러한 추가 경로를 추가할 수 있습니다.

[너비=346, 높이=324]

선택적으로 복원 전후의 스크립트를 추가할 수 있습니다.

[너비=348, 높이=326]

[너비=359, 높이=335]

요약 화면에서 '마침'을 클릭하면 복원 및 복구 작업이 시작됩니다.

[너비=361, 높이=336]

복원 및 복구 워크플로는 세 가지 주요 섹션으로 나눌 수 있습니다.

- HANA 시스템 종료
- 복원 작업
  - 파일 시스템별 준비, 예: 마운트 해제 작업
  - 스냅샷 복원 작업
  - 파일 시스템별 포스트 작업(예: 마운트 작업)
- HANA 복구
  - 시스템 데이터베이스 복구
  - 테넌트 데이터베이스 복구

[너비=357, 높이=439]

HANA Studio를 사용한 수동 복구

SAP HANA Studio와 SnapCenter 사용하여 단일 또는 여러 테넌트가 있는 SAP HANA MDC 시스템을 복원하고 복구하려면 다음 단계를 완료하세요.

1. SAP HANA Studio를 사용하여 복원 및 복구 프로세스 준비:
   a. Recover System Database(시스템 데이터베이스 복구) 를 선택하고 SAP HANA 시스템의 종료를 확인합니다.
   b. 복구 유형을 선택하고 백업 카탈로그 위치를 제공합니다.
   c. 데이터 백업 목록이 표시됩니다. 백업을 선택하여 외부 백업 ID를 확인합니다.
2. SnapCenter를 사용하여 복원 프로세스 수행:
   a. 리소스의 토폴로지 보기에서 기본 저장소에서 복원하려면 로컬 복사본을 선택하고, 보조 백업 저장소에서 복원하려면 볼트 복사본을 선택합니다.
   b. SAP HANA Studio의 외부 백업 ID 또는 설명 필드와 일치하는 SnapCenter 백업을 선택합니다.
   c. 복원 프로세스를 시작합니다.
3. SAP HANA Studio를 사용하여 시스템 데이터베이스에 대한 복구 프로세스 실행:
   a. 백업 목록에서 새로 고침 을 클릭하고 복구에 사용할 수 있는 백업(녹색 아이콘으로 표시됨)을 선택합니다.
   b. 복구 프로세스를 시작합니다. 복구 프로세스가 완료되면 시스템 데이터베이스가 시작됩니다.
4. SAP HANA Studio를 사용하여 테넌트 데이터베이스에 대한 복구 프로세스 실행:
   a. Recover Tenant Database 를 선택하고 복구할 테넌트를 선택합니다.
   b. 복구 유형 및 로그 백업 위치를 선택합니다.
   c. 데이터 백업 목록이 표시됩니다. 데이터 볼륨이 이미 복원되었기 때문에 테넌트 백업은 사용 가능으로 표시됩니다(녹색).
   d. 이 백업을 선택하고 복구 프로세스를 시작합니다. 복구 프로세스가 완료되면 테넌트 데이터베이스가 자동으로 시작됩니다.
5. 여러 테넌트가 있는 HANA 시스템의 경우 각 테넌트에 대해 4단계를 반복합니다.

SAP HANA Cockpit을 사용한 수동 복구는 동일한 단계로 수행됩니다.

다음 섹션에서는 단일 테넌트가 있는 SAP HANA MDC 시스템의 복원 및 복구 작업 단계를 설명합니다.

HANA Studio에서 백업 및 복구와 시스템 데이터베이스 복구를 선택합니다.

[너비=450, 높이=368]

종료 작업을 확인합니다. HANA 시스템이 계속 실행 중인 경우에만 필요합니다.

[너비=349, 높이=83]

복구 작업을 선택하세요. 이 예에서는 가장 최근 상태로 복구하고 싶습니다.

[너비=345, 높이=359]

백업 카탈로그 위치를 제공합니다.

[너비=343, 높이=356]

HANA Studio는 HANA 백업 카탈로그에 저장된 최신 백업을 나열합니다.

백업 카탈로그의 내용을 기반으로 사용 가능한 백업 목록이 표시됩니다. 필요한 백업을 선택하고 외부 백업 ID를 기록해 둡니다. 이 예에서는 가장 최근 백업입니다.

[너비=391, 높이=283]

SnapCenter GUI에서 리소스 토폴로지 보기를 선택하고 복원해야 하는 백업을 선택합니다. 이 예에서는 가장 최근의 기본 백업입니다. 복원 아이콘을 클릭하여 복원을 시작하세요.

[너비=601, 높이=294]

SnapCenter 복원 마법사가 시작됩니다. 볼륨 기반 복원을 사용하려면 복원 유형으로 전체 리소스 및 볼륨 되돌리기를 선택합니다.

[너비=346, 높이=325]

SnapCenter 워크플로에서 복구 작업을 제외하려면 '복구 안 함'을 선택합니다.

[너비=358, 높이=336]

마침을 클릭하여 복원 작업을 시작합니다.

[너비=361, 높이=339]

SnapCenter 복원 작업을 실행 중입니다.

- 파일 시스템별 준비, 예: 마운트 해제 작업
- 스냅샷 복원 작업
- 파일 시스템별 포스트 작업(예: 마운트 작업)

[너비=322, 높이=398]

SnapCenter 에서 스냅샷을 복원하면 HANA 데이터 볼륨의 시스템 및 테넌트 데이터베이스 하위 디렉토리에서 snapshot_databackup_0_1 파일을 사용할 수 있습니다. 이 파일은 HANA 데이터베이스 스냅샷 생성 중에 HANA 데이터베이스에 의해 생성되었습니다. HANA는 백업 작업이 완료되면 파일을 삭제하므로 해당 파일은 스냅샷 백업 내에서만 볼 수 있습니다. 이러한 파일은 모든 복구 작업에 필요합니다. 복구 후 파일은 HANA 데이터베이스에 의해 삭제됩니다.

```
hana-1:~ # cd /hana/data/SS1/mnt00001/
hana-1:/hana/data/SS1/mnt00001 # ls -al *
-rw-r--r-- 1 ss1adm sapsys 16 Aug 26 06:00 nameserver.lck
hdb00001:
total 4992236
drwxr-x--- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r----- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 ss1adm sapsys 5100273664 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 36 Aug 25 10:30 landscape.id
-rw-r----- 1 ss1adm sapsys 163840 Aug 26 06:00 snapshot_databackup_0_1
hdb00002.00003:
total 201420
drwxr-xr-- 2 ss1adm sapsys 4096 Nov 3 2020 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 335544320 Aug 26 06:00 datavolume_0000.dat
hdb00003.00003:
total 4803140
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 4898947072 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 159744 Aug 26 06:00 snapshot_databackup_0_1
hana-1:/hana/data/SS1/mnt00001 #
```

SAP HANA Studio로 이동하여 새로 고침을 클릭하면 사용 가능한 백업 목록이 업데이트됩니다. SnapCenter 로 복원된 백업은 이제 백업 목록에서 녹색 아이콘으로 표시됩니다. 백업을 선택하고 다음을 클릭합니다.

[너비=400, 높이=290]

로그 백업의 위치를 제공합니다. 다음 을 클릭합니다.

SAP HANA Studio는 SAP HANA에 구성된 경로를 로그 백업 및 카탈로그 백업 위치에 사용합니다. 추가 위치에 계층형 백업이 있는 경우 이러한 추가 경로를 추가할 수 있습니다.

[너비=465, 높이=296]

필요에 따라 다른 설정을 선택합니다. Delta 백업 사용 이 선택되어 있지 않은지 확인합니다. 다음 을 클릭합니다.

[너비=466, 높이=296]

복구 설정을 검토하고 마침 을 클릭합니다.

SQL 명령문 표시를 클릭하면 HANA Studio에서 복구 작업에 대해 실행되는 SQL 명령이 표시됩니다.

[너비=464, 높이=295]

복구 프로세스가 시작됩니다. 시스템 데이터베이스 복구가 완료될 때까지 기다리세요.

[너비=376, 높이=239]

SAP HANA Studio에서 시스템 데이터베이스의 항목을 선택하고 Backup Recovery - Recover Tenant Database를 시작합니다.

[너비=476, 높이=315]

복구할 테넌트를 선택하고 다음 을 클릭합니다.

[너비=342, 높이=355]

복구 유형을 지정하고 Next를 클릭합니다.

[너비=343, 높이=356]

백업 카탈로그 위치를 확인하고 Next를 클릭합니다.

[너비=342, 높이=355]

테넌트 데이터베이스가 종료되었는지 확인하세요.

[너비=348, 높이=85]

시스템 데이터베이스를 복구하기 전에 데이터 볼륨을 복원했으므로 테넌트 백업을 즉시 사용할 수 있습니다. 녹색으로 강조 표시된 백업을 선택하고 다음을 클릭합니다.

[너비=433, 높이=349]

로그 백업의 위치를 제공합니다. 다음 을 클릭합니다.

SAP HANA Studio는 SAP HANA에 구성된 경로를 로그 백업 및 카탈로그 백업 위치에 사용합니다. 추가 위치에 계층형 백업이 있는 경우 이러한 추가 경로를 추가할 수 있습니다.

[너비=384, 높이=310]

필요에 따라 다른 설정을 선택합니다. Delta 백업 사용 이 선택되어 있지 않은지 확인합니다. 다음 을 클릭합니다.

[너비=384, 높이=310]

복구 설정을 검토하고 마침 을 클릭합니다.

SQL 명령문 표시를 클릭하면 HANA Studio에서 복구 작업에 대해 실행되는 SQL 명령이 표시됩니다.

[너비=380, 높이=307]

복구가 완료되고 테넌트 데이터베이스가 시작될 때까지 기다립니다.

[너비=378, 높이=305]

테넌트 복구가 완료되면 SAP HANA 시스템이 실행됩니다.

여러 테넌트가 있는 SAP HANA MDC 시스템의 경우 각 테넌트에 대해 테넌트 복구를 반복해야 합니다.

SQL 명령을 사용한 수동 복구

HANA 시스템을 복구하려면 SQL 문을 사용할 수도 있습니다.

먼저 시스템 데이터베이스를 복구해야 합니다.

```
HDBSettings.sh recoverSys.py --command="RECOVER DATABASE UNTIL TIMESTAMP
'2026-08-26 10:55:49' USING CATALOG PATH ('mnt/log-backup/SYSTEMDB') USING
LOG PATH ('mnt/log-backup/SYSTEMDB') USING SNAPSHOT"
```

두 번째 단계로 시스템 데이터베이스에 연결하고 테넌트 데이터베이스 복구를 시작해야 합니다. 이 예에서 테넌트 데이터베이스는 SS1입니다.

```
hdbsql SYSTEMDB=> RECOVER DATABASE FOR SS1 UNTIL TIMESTAMP '2026-08-26
10:55:49' USING CATALOG PATH ('mnt/log-backup/DB_SS1') USING LOG PATH
('mnt/log-backup/DB_SS1') USING SNAPSHOT
```

단일 테넌트 복원 및 복구

SnapCenter 사용한 단일 테넌트 복원 및 복구 작업은 이전 항목에서 설명한 워크플로와 매우 유사합니다. "HANA Studio를 사용한 수동 복구".

SAP HANA Studio 및 SnapCenter를 사용하여 SAP HANA MDC 단일 테넌트 시스템을 복원 및 복구하려면 다음 단계를 수행하십시오.

1. SAP HANA Studio를 사용하여 복원 및 복구 프로세스 준비:
   a. 테넌트 데이터베이스 복구를 선택하고 테넌트 데이터베이스 종료를 확인합니다.
   b. 복구 유형을 선택하고 백업 카탈로그 위치를 제공합니다.
   c. 데이터 백업 목록이 표시됩니다. 백업을 선택하여 외부 백업 ID를 확인합니다.
2. SnapCenter를 사용하여 복원 프로세스 수행:
   a. 리소스의 토폴로지 보기에서 기본 저장소에서 복원하려면 로컬 복사본을 선택하고, 보조 백업 저장소에서 복원하려면 볼트 복사본을 선택합니다.
   b. SAP HANA Studio의 외부 백업 ID 또는 설명 필드와 일치하는 SnapCenter 백업을 선택합니다.
   c. 세입자 복구 프로세스를 시작합니다.
3. SAP HANA Studio를 사용하여 테넌트 데이터베이스에 대한 복구 프로세스 실행:
   a. 백업 목록에서 새로 고침 을 클릭하고 복구에 사용할 수 있는 백업(녹색 아이콘으로 표시됨)을 선택합니다.

b. 복구 프로세스를 시작합니다. 복구 프로세스가 완료되면 테넌트 데이터베이스가 시작됩니다.

비데이터 볼륨 복원

비데이터 볼륨에 대한 복원 작업은 비데이터 볼륨 리소스의 토폴로지 보기에서 스냅샷 백업을 선택하고 복원을 클릭하여 시작됩니다.

[너비=601, 높이=294]

NFS가 있는 비데이터 볼륨의 경우 전체 리소스(VBSR) 또는 파일 수준(SFSR) 복원 작업을 선택할 수 있습니다. 파일 수준 복원의 경우 모든 파일이나 개별 파일을 복원 작업에 대해 정의할 수 있습니다.

[너비=369, 높이=344]

SAP HANA에 대한 고급 SnapCenter 옵션 구성

게스트 내 NFS 마운트에 대한 VMware 경고 메시지 억제, 자동 로그 백업 정리 비활성화, HANA 데이터베이스 연결에 대한 SSL 암호화 활성화 등 SAP HANA 환경에 대한 고급 SnapCenter 설정을 구성합니다.

가상화 환경 및 게스트 내 마운트에 대한 경고 메시지

예를 들어 NFS 게스트 마운트를 사용하여 VMware를 사용하는 경우 SnapCenter SnapCenter VMware 플러그인을 사용해야 한다는 경고 메시지를 표시합니다. 게스트 내 마운트에는 VMWare 플러그인이 필요하지 않으므로 경고 메시지를 무시하고 끌 수 있습니다. 이 경고를 억제하도록 SnapCenter 구성하려면 다음 구성을 적용해야 합니다.

1. 설정 탭에서 전역 설정 을 선택합니다.
2. 하이퍼바이저 설정의 경우 모든 호스트에 대해 VM에 iSCSI Direct Attached Disks 또는 NFS를 가지고 있음 을 선택하고 설정을 업데이트합니다.

[너비=601, 높이=176]

자동 로그 백업 관리 기능을 비활성화합니다

로그 백업 하우스키핑은 기본적으로 활성화되어 있으며 HANA 플러그인 호스트 수준에서 비활성화할 수 있습니다. PowerShell 명령을 사용하세요.

명령 Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}는 이 SAP HANA 호스트에 대한 로그 백업 정리 작업을 비활성화합니다.

HANA 데이터베이스에 대한 보안 통신 지원

HANA 데이터베이스가 보안 통신으로 구성된 경우 SnapCenter 에서 실행되는 hdbsql 명령은 추가 명령줄 옵션을 사용해야 합니다.

SSL 통신을 구성하는 데에는 다양한 옵션이 있습니다. 기본적으로 SnapCenter -e ssltrustcert hdbsql 명령줄 옵션을 사용합니다. 이 옵션을 사용하면 서버 인증서 검증 없이 SSL 통신이 수행되며, 이 옵션은 SSL이 활성화되지 않은 HANA 시스템에서도 작동합니다.

서버 및/또는 클라이언트 측에서 인증서 검증이 필요한 경우 다른 hdbsql 명령줄 옵션이 필요하며, SAP HANA 보안 가이드에 설명된 대로 PSE 환경을 적절히 구성해야 합니다.

이는 필요한 옵션과 함께 hdbsql을 호출하는 래퍼 스크립트를 사용하여 달성할 수 있습니다. hana.properties 파일에서 hdbsql 실행 파일을 구성하는 대신, 래퍼 스크립트가 추가되었습니다.

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

래퍼 스크립트 hdbsqls는 필요한 명령줄 옵션과 함께 hdbsql을 호출합니다.

```
#/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql <command line options> $*
```

HANA 플러그인 호스트에서 자동 검색을 해제합니다

HANA 플러그인 호스트에서 자동 검색을 비활성화하려면 다음 단계를 완료하세요.

1. SnapCenter 서버에서 PowerShell을 엽니다. OpenSmConnection 명령을 실행하여 SnapCenter 서버에 연결하고 로그인 창이 열리면 사용자 이름과 비밀번호를 지정합니다.
2. 자동 검색을 비활성화하려면 Set-SmConfigSettings 명령을 실행합니다.

HANA 호스트 hana-2의 경우 명령은 다음과 같습니다.

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname
hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}

Name Value

---- -----

DISABLE_AUTO_DISCOVERY true

PS C:\Users\administrator.SAPCC>

Verify the configuration by running the Get- SmConfigSettings command.

PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all

Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC Value: 3600000 Details: Plug-
in API operation Timeout

Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC Value: 1800 Details:
Web Service API Timeout

Key: CUSTOMPLUGINS_ALLOWED_CMDS Value: *; Details: Allowed Host OS
Commands

Key: DISABLE_AUTO_DISCOVERY Value: true Details:

Key: PORT Value: 8145 Details: Port for server communication

PS C:\Users\administrator.SAPCC>
```

구성은 호스트의 에이전트 구성 파일에 기록되며 SnapCenter를 사용한 플러그인 업그레이드 후에도 계속 사용할 수 있습니다.

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/agent.properties | grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```