클라우드 네이티브 애플리케이션 데이터를 백업 및 복원합니다

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-backup-recovery/concept-protect-cloud-app-data-to-cloud.html on April 18, 2024. Always check docs.netapp.com for the latest.

목차

클라우드 네이티브 애플리케이션 데이터를 백업 및 복원합니다 1
클라우드 네이티브 애플리케이션 데이터 보호 1
클라우드 네이티브 Oracle 데이터베이스 백업 5
클라우드 네이티브 SAP HANA 데이터베이스 백업 17
REST API를 사용하여 클라우드 네이티브 SQL Server 데이터베이스를 백업합니다 26
클라우드 네이티브 Oracle 데이터베이스 복원 38
클라우드 네이티브 SAP HANA 데이터베이스 복원 40
Microsoft SQL Server 데이터베이스를 복원합니다 42
클라우드 네이티브 Oracle 데이터베이스 클론 45
SAP HANA 타겟 시스템을 업데이트하세요 53
클라우드 네이티브 애플리케이션 데이터 보호 관리 55

클라우드 네이티브 애플리케이션 데이터를 백업 및 복원합니다

클라우드 네이티브 애플리케이션 데이터 보호

애플리케이션을 위한 BlueXP 백업 및 복구는 NetApp 클라우드 스토리지에서 실행되는 애플리케이션을 위한 애플리케이션 정합성이 보장되는 데이터 보호 기능을 제공합니다. BlueXP 백업 및 복구는 다음과 같은 애플리케이션에 대해 효율적이고 일관된 정책 기반 보호 기능을 제공합니다.

- NetApp ONTAP, Cloud Volumes ONTAP 및 Azure NetApp Files용 Amazon FSx에 상주하는 Oracle 데이터베이스입니다
- Azure NetApp Files에 상주하는 SAP HANA 시스템
- Amazon FSx for NetApp ONTAP에 상주하는 Microsoft SQL Server 데이터베이스

있습니다

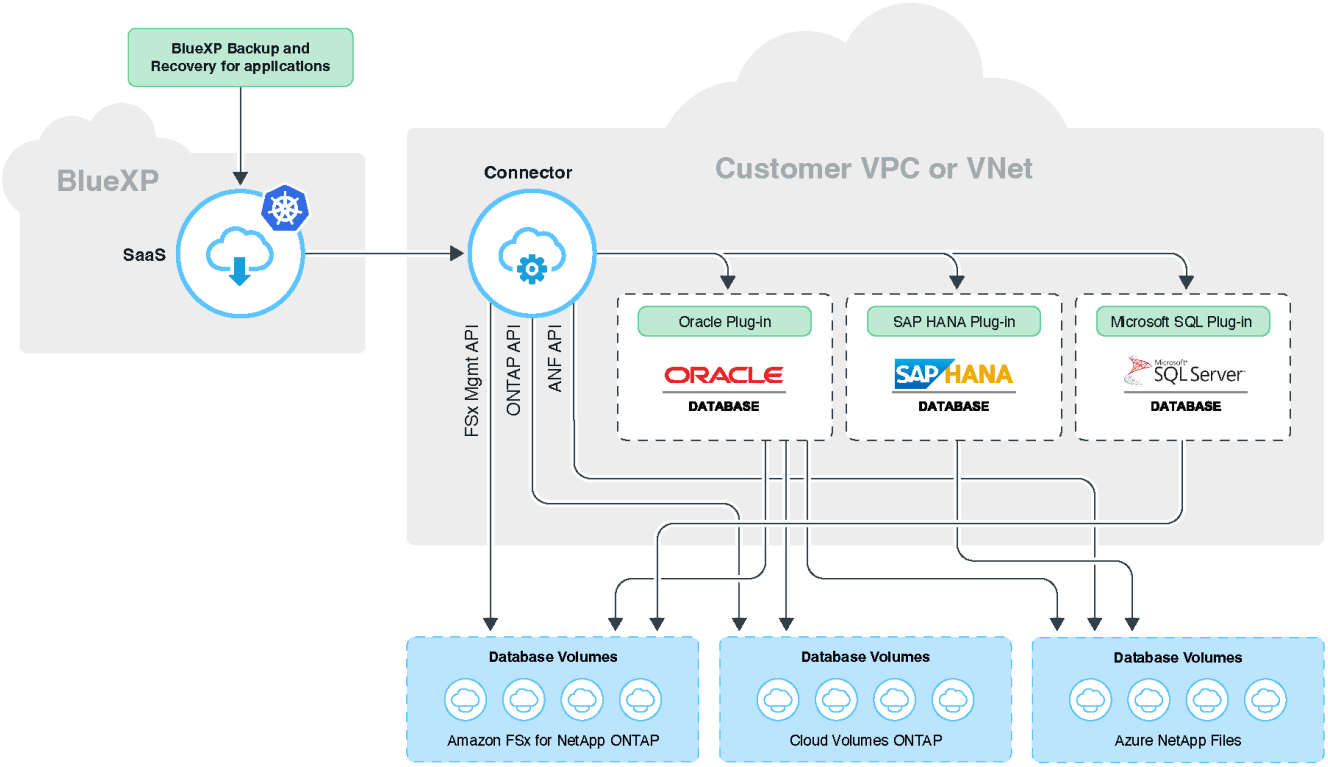
애플리케이션 아키텍처에 대한 BlueXP 백업 및 복구에는 다음과 같은 구성 요소가 포함됩니다.

- BlueXP 백업 및 복구는 NetApp에서 SaaS 서비스로 호스팅하는 데이터 보호 서비스 세트이며, BlueXP SaaS 플랫폼을 기반으로 합니다.

  NetApp 클라우드 스토리지에 상주하는 애플리케이션에 대해 데이터 보호 워크플로우를 조정합니다.

- BlueXP UI는 응용 프로그램에 대한 데이터 보호 기능을 제공하며 BlueXP UI에서 액세스할 수 있습니다.
- BlueXP Connector는 클라우드 네트워크에서 실행되며 스토리지 시스템 및 애플리케이션별 플러그인과 상호 작용하는 구성 요소입니다.
- 애플리케이션별 플러그인은 각 애플리케이션 호스트에서 실행되며 데이터 보호 작업을 수행하는 동안 호스트에서 실행 중인 데이터베이스와 상호 작용하는 구성 요소입니다.

다음 이미지는 각 구성 요소와 이러한 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



사용자가 요청한 요청의 경우 BlueXP UI는 BlueXP SaaS와 통신하며, 요청 프로세스의 유효성을 확인할 때 이 기능을 사용합니다. 요청이 백업, 복원 또는 클론과 같은 워크플로우를 실행하는 경우 SaaS 서비스는 워크플로우를 시작하고 필요한 경우 통화를 BlueXP Connector로 전달합니다. 그런 다음 Connector는 워크플로우 작업을 실행하는 과정에서 스토리지 시스템 및 애플리케이션별 플러그인과 통신합니다.

커넥터는 애플리케이션 또는 다른 애플리케이션과 동일한 VPC 또는 VNET에 구축할 수 있습니다. 커넥터와 응용 프로그램이 서로 다른 네트워크에 있는 경우 이들 간에 네트워크 연결을 설정해야 합니다.

> 단일 BlueXP 커넥터는 여러 스토리지 시스템 및 여러 애플리케이션 플러그인과 통신할 수 있습니다. Connector와 애플리케이션 호스트 간에 연결이 있는 경우 애플리케이션을 관리하려면 단일 커넥터가 필요합니다.

> BlueXP SaaS 인프라는 지역 내의 가용성 영역 장애에 대한 복원력을 제공합니다. 새로운 지역으로 페일오버하여 지역 내 장애를 지원하며 이 페일오버에는 약 2시간의 다운타임이 발생합니다.

Oracle 데이터베이스 보호

피처

- 호스트 추가 및 플러그인 구축

  UI, 스크립트 또는 수동으로 플러그인을 배포할 수 있습니다.

- Oracle 데이터베이스 자동 검색
- NetApp ONTAP, Cloud Volumes ONTAP 및 Azure NetApp Files용 Amazon FSx에 상주하는 Oracle 데이터베이스 백업

    - 전체(데이터 + 제어 + 아카이브 로그 파일) 백업
    - 필요 시 백업
    - 시스템 정의 또는 사용자 지정 정책을 기반으로 예약된 백업

      정책에서 시간별, 일별, 주별 및 월별 등 다양한 예약 빈도를 지정할 수 있습니다. 또한 백업 성공 후 실행될 사후 스크립트를 지정하여 스냅샷을 보조 스토리지에 복제할 수도 있습니다.

- Oracle RMAN을 사용하여 Azure NetApp Files에서 Oracle 데이터베이스 백업을 카탈로그로 작성할 수 있습니다
- 정책을 기반으로 백업을 유지합니다
- NetApp ONTAP, Cloud Volumes ONTAP 및 Azure NetApp Files용 Amazon FSx에 상주하는 Oracle 데이터베이스를 복원하는 중입니다
    - 지정된 백업에서 전체 Oracle 데이터베이스(데이터 파일 + 제어 파일)를 복원합니다
    - SCN, 종료 시점, 사용 가능한 모든 로그 및 복구 옵션이 없을 때까지 Oracle 데이터베이스를 복구합니다
- Azure NetApp Files에서 Oracle 데이터베이스를 대체 위치로 복구
- NetApp ONTAP용 Amazon FSx 및 Cloud Volumes ONTAP에 상주하는 Oracle 데이터베이스를 소스 또는 대체 타겟 호스트에 클론 복제할 수 있습니다
    - 기본 원클릭 클론
    - 사용자 지정 클론 사양 파일을 사용한 고급 클론 생성
    - 클론 엔터티 이름은 자동으로 생성되거나 소스와 동일할 수 있습니다
    - 클론 계층 보기
    - 복제된 데이터베이스를 삭제하는 중입니다
- 백업, 복원, 클론 및 기타 작업 모니터링
- 대시보드에 보호 요약 표시
- 이메일을 통해 알림 전송
- 호스트 플러그인을 업그레이드합니다

제한 사항

- Oracle 11g를 지원하지 않습니다
- 에서는 백업에 대한 마운트, 카탈로그 및 검증 작업을 지원하지 않습니다
- RAC 및 Data Guard에서 Oracle을 지원하지 않습니다
- Cloud Volumes ONTAP HA의 경우 네트워크 인터페이스 IP 중 하나만 사용됩니다. IP 연결이 끊기거나 IP에 액세스할 수 없는 경우 데이터 보호 작업이 실패합니다.
- NetApp ONTAP 또는 Cloud Volumes ONTAP용 Amazon FSx의 네트워크 인터페이스 IP 주소는 BlueXP 계정 및 지역에서 고유해야 합니다.

SAP HANA 데이터베이스 보호

피처

- SAP HANA 시스템을 수동으로 추가합니다

- SAP HANA 데이터베이스 백업
  - 필요 시 백업(파일 기반 및 스냅샷 복사본 기반)
  - 시스템 정의 또는 사용자 지정 정책을 기반으로 예약된 백업

    정책에서 시간별, 일별, 주별 및 월별 등 다양한 예약 빈도를 지정할 수 있습니다.

  - HANA 시스템 복제(HSR) 인식
- 정책을 기반으로 백업을 유지합니다
- 지정된 백업에서 전체 SAP HANA 데이터베이스를 복원하는 중입니다
- HANA 비 데이터 볼륨 및 글로벌 비 데이터 볼륨 백업 및 복원
- Prescript 및 PostScript는 백업 및 복원 작업에 환경 변수 사용을 지원합니다
- 사전 종료 옵션을 사용하여 실패 시나리오에 대한 작업 계획을 작성합니다

제한 사항

- HSR 구성의 경우 2노드 HSR만 지원됩니다(1개의 기본 및 1개의 보조).
- 복원 작업 중에 PS가 실패할 경우 잔상이 트리거되지 않습니다

Microsoft SQL Server 데이터베이스 보호

피처

- 호스트를 수동으로 추가하고 플러그인을 구축합니다
- 데이터베이스를 수동으로 검색합니다
- Amazon FSx for NetApp ONTAP에 상주하는 SQL Server 인스턴스를 백업합니다
  - 필요 시 백업
  - 정책을 기반으로 예약된 백업
  - Microsoft SQL Server 인스턴스의 로그 백업
- 데이터베이스를 원래 위치로 복원합니다

제한 사항

- 백업은 SQL Server 인스턴스에 대해서만 지원됩니다
- FCI(Failover Cluster Instance) 구성은 지원되지 않습니다
- BlueXP UI는 SQL 데이터베이스별 작업을 지원하지 않습니다

  모든 Microsoft SQL Server 데이터베이스별 작업은 REST API를 실행하여 수행됩니다.

- 대체 위치로 복구할 수 없습니다

클라우드 네이티브 **Oracle** 데이터베이스 백업

빠른 시작

다음 단계를 수행하여 빠르게 시작하십시오.

1 구성에 대한 지원을 확인합니다

- 운영 체제:
  - RHEL 7.5 이상 및 8.x
  - OL 7.5 이상 및 8.x
  - SLES 15 SP4
- NetApp 클라우드 스토리지:
  - NetApp ONTAP용 Amazon FSx
  - Cloud Volumes ONTAP
  - Azure NetApp Files
- 스토리지 레이아웃:
  - NFS v3 및 v4.1(dNFS 포함)
  - iSCSI with ASM(ASMFD, ASMLib 및 ASMUDEV)

> Azure NetApp Files는 SAN 환경을 지원하지 않습니다.

- 데이터베이스 레이아웃: Oracle Standard 및 Oracle Enterprise Standalone(레거시 및 멀티 테넌트 CDB 및 PDB)
- 데이터베이스 버전: 19c 및 21c

2 **BlueXP**에 등록하십시오

BlueXP는 웹 기반 콘솔에서 액세스할 수 있습니다. BlueXP를 시작할 때 첫 번째 단계는 기존 NetApp Support 사이트 자격 증명을 사용하거나 NetApp 클라우드 로그인을 생성하여 등록하는 것입니다. 자세한 내용은 을 참조하십시오 "BlueXP에 등록하십시오".

3 **BlueXP**에 로그인합니다

BlueXP에 등록하면 웹 기반 콘솔에서 로그인할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP에 로그인합니다".

4 **BlueXP** 계정을 관리합니다

사용자, 서비스 계정, 작업 영역 및 커넥터를 관리하여 계정을 관리할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP 계정을 관리합니다".

ONTAP에 대해 FSx를 구성합니다

BlueXP를 사용하면 ONTAP 작업 환경에 FSx를 생성하여 볼륨 및 추가 데이터 서비스를 추가하고 관리해야 합니다. 또한 BlueXP에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 AWS에 Connector를 만들어야 합니다.

ONTAP 작업 환경을 위한 FSx를 생성합니다

데이터베이스가 호스팅되는 ONTAP 작업 환경용 FSx를 만들어야 합니다. 자세한 내용은 을 참조하십시오 "ONTAP용 Amazon FSx를 시작하십시오" 및 "ONTAP 작업 환경을 위한 Amazon FSx를 생성하고 관리합니다".

BlueXP 또는 AWS를 사용하여 ONTAP 작업 환경을 위한 FSx를 생성할 수 있습니다. AWS를 사용하여 생성한 경우 BlueXP에서 ONTAP 시스템용 FSx를 검색해야 합니다.

커넥터를 작성합니다

계정 관리자는 AWS에서 Connector를 생성하여 BlueXP가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

자세한 내용은 을 참조하십시오 "BlueXP에서 AWS에 커넥터 생성".

- 동일한 커넥터를 사용하여 ONTAP 작업 환경 및 데이터베이스에 대한 FSx를 모두 관리해야 합니다.
- 동일한 VPC(Virtual Private Cloud)에 ONTAP 작업 환경 및 데이터베이스를 위한 FSx가 있는 경우 동일한 VPC에 커넥터를 배포할 수 있습니다.
- ONTAP 작업 환경 및 다른 VPC에 데이터베이스를 위한 FSx가 있는 경우:
  - ONTAP용 FSx에서 NAS(NFS) 워크로드를 구성한 경우, 두 VPC 중 하나에 커넥터를 생성할 수 있습니다.
  - SAN 워크로드만 구성되어 있고 NAS(NFS) 워크로드를 사용할 계획이 없는 경우, ONTAP용 FSx 시스템이 생성되는 VPC에 커넥터를 생성해야 합니다.

> NAS(NFS) 워크로드를 사용하려면 VPC 데이터베이스와 Amazon VPC 간에 전송 게이트웨이가 있어야 합니다. 부동 IP 주소인 NFS IP 주소는 전송 게이트웨이를 통해서만 다른 VPC에서 액세스할 수 있습니다. VPC를 피해서 유동 IP 주소에 액세스할 수 없습니다.

Connector를 생성한 후 * Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하고 화면의 지시에 따라 작업 환경을 추가합니다. Connector와 Oracle 데이터베이스 호스트 및 FSx 작업 환경이 연결되어 있는지 확인합니다. Connector는 FSx 작업 환경의 클러스터 관리 IP 주소에 연결할 수 있어야 합니다.

- Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하여 작업 환경을 추가합니다.

  커넥터에서 데이터베이스 호스트 및 FSx for ONTAP 작업 환경과의 연결이 있는지 확인합니다. 커넥터는 ONTAP 작업 환경의 FSx의 클러스터 관리 IP 주소에 연결해야 합니다.

- 커넥터 > 커넥터 관리 * 를 클릭하고 커넥터 이름을 선택하여 커넥터 ID를 복사합니다.

Cloud Volumes ONTAP를 구성합니다

BlueXP를 사용하면 Cloud Volumes ONTAP 작업 환경을 만들어 볼륨 및 추가 데이터 서비스를

추가하고 관리해야 합니다. 또한 BlueXP에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 클라우드 환경에 대한 Connector를 만들어야 합니다.

Cloud Volumes ONTAP 작업 환경을 생성합니다

기존 Cloud Volumes ONTAP 시스템을 검색하고 BlueXP에 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 "기존 Cloud Volumes ONTAP 시스템을 BlueXP에 추가".

커넥터를 작성합니다

클라우드 환경을 위한 Cloud Volumes ONTAP를 몇 가지 단계로 시작할 수 있습니다. 자세한 내용은 다음 중 하나를 참조하십시오.

- "AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다"
- "Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다"
- "Google Cloud에서 Cloud Volumes ONTAP를 빠르게 시작합니다"

동일한 커넥터를 사용하여 Cloud Volumes ONTAP 작업 환경과 데이터베이스를 모두 관리해야 합니다.

- 동일한 VPC(가상 프라이빗 클라우드) 또는 VNET에 Cloud Volumes ONTAP 작업 환경과 데이터베이스가 있는 경우 동일한 VPC 또는 VNET에 커넥터를 배포할 수 있습니다.
- Cloud Volumes ONTAP 작업 환경과 데이터베이스가 서로 다른 VPC 또는 VNets에 있는 경우 VPC 또는 VNets를 살펴보는지 확인합니다.

Azure NetApp Files를 구성합니다

BlueXP를 사용하면 Azure NetApp Files 작업 환경을 만들어 볼륨 및 추가 데이터 서비스를 추가하고 관리해야 합니다. 또한 Azure에서 Connector를 만들어 BlueXP가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

Azure NetApp Files 작업 환경을 생성합니다

데이터베이스가 호스팅되는 Azure NetApp Files 작업 환경을 만들어야 합니다. 자세한 내용은 을 참조하십시오 "Azure NetApp Files에 대해 자세히 알아보십시오" 및 "Azure NetApp Files 작업 환경을 만듭니다".

커넥터를 작성합니다

BlueXP 계정 관리자는 Azure에 Connector를 배포하여 BlueXP가 공용 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

자세한 내용은 을 참조하십시오 "BlueXP에서 Azure에 커넥터를 만듭니다".

- 커넥터에서 데이터베이스 호스트로의 연결이 있는지 확인합니다.
- 동일한 VNet(가상 네트워크)에 Azure NetApp Files 작업 환경과 데이터베이스가 있는 경우 동일한 VNET에 커넥터를 배포할 수 있습니다.
- Azure NetApp Files 작업 환경과 데이터베이스가 서로 다른 VNets에 있고 Azure NetApp Files에 NAS(NFS) 워크로드가 구성되어 있는 경우 VNets 중 하나에 커넥터를 생성할 수 있습니다.

커넥터를 만든 후 * Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하여 작업 환경을 추가합니다.

Oracle용 SnapCenter 플러그인을 설치하고 데이터베이스 호스트를 추가합니다

각 Oracle 데이터베이스 호스트에 Oracle용 SnapCenter 플러그인을 설치하고, 데이터베이스 호스트를 추가하고, 호스트에서 데이터베이스를 검색하여 정책을 할당하고, 백업을 생성해야 합니다.

- 데이터베이스 호스트에 대해 SSH가 설정된 경우 다음 방법 중 하나를 사용하여 플러그인을 설치할 수 있습니다.
  - SSH 옵션을 사용하여 플러그인을 설치하고 UI에서 호스트를 추가합니다. 자세한 정보.
  - 스크립트를 사용하여 플러그인을 설치하고 수동 옵션을 사용하여 UI에서 호스트를 추가합니다. 자세한 정보.
- SSH가 비활성화된 경우 수동으로 플러그인을 설치하고 수동 옵션을 사용하여 UI에서 호스트를 추가합니다. 자세한 정보.

필수 구성 요소

호스트를 추가하기 전에 필수 구성 요소가 충족되었는지 확인해야 합니다.

- 작업 환경과 커넥터를 만들어야 합니다.
- Connector가 Oracle 데이터베이스 호스트에 연결되어 있는지 확인합니다.

  연결 문제를 해결하는 방법에 대한 자세한 내용은 을 참조하십시오 "BlueXP 커넥터 호스트에서 애플리케이션 데이터베이스 호스트로의 연결을 확인하지 못했습니다".

  커넥터를 분실하거나 새 커넥터를 만든 경우 커넥터를 기존 응용 프로그램 리소스에 연결해야 합니다. 커넥터 업데이트에 대한 지침은 을 참조하십시오 "커넥터 세부 정보를 업데이트합니다".

- BlueXP 사용자에게 "계정 관리자" 역할이 있는지 확인합니다.
- 데이터 보호 작업을 위해 애플리케이션 호스트에 루트가 아닌(sudo) 계정이 있는지 확인합니다.
- 각 Oracle 데이터베이스 호스트에 Java 11(64비트) Oracle Java 또는 OpenJDK가 설치되어 있고 JAVA_HOME 변수가 적절하게 설정되어 있는지 확인합니다.
- SSH 기반 설치를 수행하는 경우 커넥터에 SSH 포트에 대한 통신이 활성화되어 있는지 확인합니다(기본값: 22).
- 데이터 보호 작업이 작동하려면 커넥터에 플러그인 포트(기본값: 8145)에 대한 통신이 활성화되어 있는지 확인합니다.
- 최신 버전의 플러그인이 설치되어 있는지 확인합니다. 플러그인을 업그레이드하려면 를 참조하십시오 Oracle 데이터베이스용 SnapCenter 플러그인을 업그레이드하십시오.

SSH 옵션을 사용하여 **UI**에서 호스트를 추가합니다

단계

1. BlueXP UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.

   호스트를 이미 추가했고 다른 호스트를 추가하려면 * 응용 프로그램 * > * 데이터베이스 관리 * > * 추가 * 를 클릭한 다음 5단계를 진행합니다.

2. 응용 프로그램 검색 * 을 클릭합니다.
3. Cloud Native * 를 선택하고 * Next * 를 클릭합니다.

   이 계정의 모든 사용자에 대해 예약된 데이터 보호 작업을 수행하기 위해 *SnapCenter* 시스템_역할이 있는 서비스 계정(*_SnapCenter-account-<accountid>*)이 생성됩니다. 서비스 계정(*SnapCenter-account-<accountid>*)은 예약된 백업 작업을 실행하는 데 사용됩니다. 서비스 계정을 삭제해서는 안 됩니다. 계정 * > * 계정 관리 * > * 회원 * 을 클릭하여 서비스 계정을 볼 수 있습니다.

4. 애플리케이션 유형으로 Oracle을 선택합니다.
5. 호스트 세부 정보 페이지에서 다음을 수행합니다.

   a. SSH * 를 사용하여 * 를 선택합니다.
   b. 플러그인을 설치할 호스트의 FQDN 또는 IP 주소를 지정합니다.

      Connector가 FQDN 또는 IP 주소를 사용하여 데이터베이스 호스트와 통신할 수 있는지 확인합니다.

   c. 플러그인 패키지를 호스트에 복사할 때 사용하는 비 루트(sudo) 사용자를 지정합니다.

      루트 사용자는 지원되지 않습니다.

   d. SSH 및 플러그인 포트를 지정합니다.

      기본 SSH 포트는 22이고 플러그인 포트는 8145입니다.

   플러그인을 설치한 후 애플리케이션 호스트에서 SSH 포트를 닫을 수 있습니다. 데이터 보호 작업에 SSH 포트가 필요하지 않습니다.

   a. 커넥터 를 선택합니다.
   b. (선택 사항) Connector와 호스트 간에 키 없는 인증이 활성화되지 않은 경우 호스트와 통신하는 데 사용할 SSH 개인 키를 지정해야 합니다.

      SSH 개인 키는 애플리케이션의 어느 곳에나 저장되지 않으며 다른 작업에 사용되지 않습니다.

   c. 다음 * 을 클릭합니다.
6. 구성 페이지에서 다음을 수행합니다.

   a. Oracle 데이터베이스를 실행하는 Linux 시스템에 로그인하여 Oracle 데이터베이스 호스트에서 SnapCenter 사용자에 대한 sudo 액세스를 구성합니다.
   b. BlueXP UI에 표시된 텍스트를 복사합니다.
   c. Linux 시스템에서 _/etc/sudoers.d/snapcenter_file을 생성하고 복사한 텍스트를 붙여 넣습니다.
   d. BlueXP UI에서 확인란을 선택하고 * 다음 * 을 클릭합니다.
7. 세부 정보를 검토하고 * 응용 프로그램 검색 * 을 클릭합니다.

   - 플러그인이 설치되면 검색 작업이 시작됩니다.
   - 검색 작업을 완료하면 호스트의 모든 데이터베이스가 표시됩니다. 데이터베이스에 대한 OS 인증이 비활성화된 경우 * 구성 * 을 클릭하여 데이터베이스 인증을 활성화합니다. 자세한 내용은 을 참조하십시오 Oracle 데이터베이스 자격 증명을 구성합니다.

- Settings * 를 클릭하고 * Hosts * 를 선택하여 모든 호스트를 봅니다.
- 설정 * 을 클릭하고 * 정책 * 을 선택하여 미리 구성된 정책을 봅니다. 사전 구성된 정책을 검토하여 요구 사항에 맞게 정책을 편집하거나 새 정책을 생성할 수 있습니다.

수동 옵션을 사용하여 **UI**에서 호스트를 추가하고 스크립트를 사용하여 플러그인을 설치합니다

Oracle 호스트 비루트 사용자 계정에 대한 SSH 키 기반 인증을 구성하고 다음 단계를 수행하여 플러그인을 설치합니다.

시작하기 전에

커넥터에 대한 SSH 연결이 활성화되어 있는지 확인합니다.

단계

1. BlueXP UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
2. 응용 프로그램 검색 * 을 클릭합니다.
3. Cloud Native * 를 선택하고 * Next * 를 클릭합니다.

   이 계정의 모든 사용자에 대해 예약된 데이터 보호 작업을 수행하기 위해 *SnapCenter* 시스템_역할이 있는 서비스 계정(*_SnapCenter-account-<accountid>*)이 생성됩니다. 서비스 계정(*SnapCenter-account-<accountid>*)은 예약된 백업 작업을 실행하는 데 사용됩니다. 서비스 계정을 삭제해서는 안 됩니다. 계정 * > * 계정 관리 * > * 회원 * 을 클릭하여 서비스 계정을 볼 수 있습니다.

4. 애플리케이션 유형으로 Oracle을 선택합니다.
5. 호스트 세부 정보 페이지에서 다음을 수행합니다.
   a. 수동 * 을 선택합니다.
   b. 플러그인이 설치된 호스트의 FQDN 또는 IP 주소를 지정합니다.

      Connector가 FQDN 또는 IP 주소를 사용하여 데이터베이스 호스트와 통신할 수 있는지 확인합니다.

   c. 플러그인 포트를 지정합니다.

      기본 포트는 8145입니다.

   d. 플러그인 패키지를 호스트에 복사할 때 사용하는 비 루트(sudo) 사용자를 지정합니다.
   e. 커넥터 를 선택합니다.
   f. 호스트에 플러그인이 설치되어 있는지 확인하려면 확인란을 선택합니다.
   g. 다음 * 을 클릭합니다.
6. 구성 페이지에서 다음을 수행합니다.
   a. Oracle 데이터베이스를 실행하는 Linux 시스템에 로그인하여 Oracle 데이터베이스 호스트에서 SnapCenter 사용자에 대한 sudo 액세스를 구성합니다.
   b. BlueXP UI에 표시된 텍스트를 복사합니다.
   c. Linux 시스템에서 _/etc/sudoers.d/snapcenter_file을 생성하고 복사한 텍스트를 붙여 넣습니다.
   d. BlueXP UI에서 확인란을 선택하고 * 다음 * 을 클릭합니다.
7. Connector VM에 로그인합니다.

8. Connector에 제공된 스크립트를 사용하여 플러그인을 설치합니다.
```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

   이전 커넥터를 사용하는 경우 다음 명령을 실행하여 플러그인을 설치합니다.
```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

이름	설명	필수입니다	기본값
plugin_host 를 선택합니다	Oracle 호스트를 지정합니다	예	-
host_user_name	Oracle 호스트에 대한 SSH 권한이 있는 SnapCenter 사용자를 지정합니다	예	-
host_ssh_key입니다	SnapCenter 사용자의 SSH 키를 지정하며 Oracle 호스트에 연결하는 데 사용됩니다	예	-
plugin_port 를 선택합니다	플러그인에서 사용하는 포트를 지정합니다	아니요	8145
host_ssh_port	Oracle 호스트의 SSH 포트를 지정합니다	아니요	22

   예를 들면 다음과 같습니다.

   - `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
   - `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. BlueXP UI에서 세부 정보를 검토하고 * 응용 프로그램 검색 * 을 클릭합니다.
   - 검색 작업을 완료하면 호스트의 모든 데이터베이스가 표시됩니다. 데이터베이스에 대한 OS 인증이 비활성화된 경우 * 구성 * 을 클릭하여 데이터베이스 인증을 활성화합니다. 자세한 내용은 을 참조하십시오 Oracle 데이터베이스 자격 증명을 구성합니다.
   - Settings * 를 클릭하고 * Hosts * 를 선택하여 모든 호스트를 봅니다.
   - 설정 * 을 클릭하고 * 정책 * 을 선택하여 미리 구성된 정책을 봅니다. 사전 구성된 정책을 검토하여 요구 사항에

맞게 정책을 편집하거나 새 정책을 생성할 수 있습니다.

수동 옵션을 사용하여 **UI**에서 호스트를 추가하고 플러그인을 수동으로 설치합니다

Oracle 데이터베이스 호스트에서 SSH 키 기반 인증이 활성화되지 않은 경우 다음 수동 단계를 수행하여 플러그인을 설치한 다음 수동 옵션을 사용하여 UI에서 호스트를 추가해야 합니다.

단계

1. BlueXP UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
2. 응용 프로그램 검색 * 을 클릭합니다.
3. Cloud Native * 를 선택하고 * Next * 를 클릭합니다.

   이 계정의 모든 사용자에 대해 예약된 데이터 보호 작업을 수행하기 위해 *SnapCenter* 시스템_역할이 있는 서비스 계정*(_SnapCenter-account-<accountid>*)이 생성됩니다. 서비스 계정(*SnapCenter-account-<accountid>*)은 예약된 백업 작업을 실행하는 데 사용됩니다. 서비스 계정을 삭제해서는 안 됩니다. 계정 * > * 계정 관리 * > * 회원 * 을 클릭하여 서비스 계정을 볼 수 있습니다.

4. 애플리케이션 유형으로 Oracle을 선택합니다.
5. Host details * 페이지에서 다음 작업을 수행합니다.
   a. 수동 * 을 선택합니다.
   b. 플러그인이 설치된 호스트의 FQDN 또는 IP 주소를 지정합니다.

      FQDN 또는 IP 주소를 사용하여 Connector가 데이터베이스 호스트와 통신할 수 있는지 확인합니다.

   c. 플러그인 포트를 지정합니다.

      기본 포트는 8145입니다.

   d. 플러그인 패키지를 호스트에 복사할 때 사용할 sudo non-root(sudo) 사용자를 지정합니다.
   e. 커넥터 를 선택합니다.
   f. 호스트에 플러그인이 설치되어 있는지 확인하려면 확인란을 선택합니다.
   g. 다음 * 을 클릭합니다.
6. 구성 페이지에서 다음을 수행합니다.
   a. Oracle 데이터베이스를 실행하는 Linux 시스템에 로그인하여 Oracle 데이터베이스 호스트에서 SnapCenter 사용자에 대한 sudo 액세스를 구성합니다.
   b. BlueXP UI에 표시된 텍스트를 복사합니다.
   c. Linux 시스템에서 _/etc/sudoers.d/snapcenter_file을 생성하고 복사한 텍스트를 붙여 넣습니다.
   d. BlueXP UI에서 확인란을 선택하고 * 다음 * 을 클릭합니다.
7. Connector VM에 로그인합니다.
8. SnapCenter Linux 호스트 플러그인 바이너리를 다운로드합니다. S UDO Docker Exec - IT cloudmanager_scs_cloud curl-X get 'http://127.0.0.1/deploy/downloadLinuxPlugin'`

   플러그인 바이너리는 *CD/var/lib/docker/volumes/service-manager[1]-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker PS|grep-Po "cloudmanager_scs_cloud:. *?"|SED-e's/ *$/"|cut-F2-d":")/SC-Linux-host-plugin*

9. SCP 또는 다른 대체 방법을 사용하여 각 Oracle 데이터베이스 호스트에 대해 */home/<non root user (sudo)>/.SC_NetApp_path*의 위 경로에서 *copy_snapcenter_linux_host_plugin_scs.bin*
10. 비 루트(sudo) 계정을 사용하여 Oracle 데이터베이스 호스트에 로그인합니다.
11. 디렉토리를 _/home/<non root user>/.sc_netapp/_로 변경하고 다음 명령을 실행하여 바이너리에 대한 실행 권한을 활성화합니다.
    ```
    chmod +x snapcenter_linux_host_plugin_scs.bin
    ```
12. sudo SnapCenter 사용자로 Oracle 플러그인을 설치합니다.
    ```
    ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
    ```
13. copy_certificate.pem_from_<base_mount_path>/client/certificate/_path 커넥터 VM의 경로를 플러그인 호스트의 _/var/opt/snapcenter/spl/etc/_로 복사합니다.
14. _/var/opt/snapcenter/spl/etc_로 이동하고 keytool 명령을 실행하여 certificate.pem을 가져옵니다.
    ```
    keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
    -deststorepass snapcenter -noprompt
    ```
15. SPL을 다시 시작합니다:'stemctl restart SPL'
16. Connector에서 아래 명령을 실행하여 커넥터에서 플러그인에 연결할 수 있는지 확인합니다.
    ```
    docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
    plug-in host>:<plug-in port>/PluginService/Version --cert
    /config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```
17. BlueXP UI에서 세부 정보를 검토하고 * 응용 프로그램 검색 * 을 클릭합니다.
    - 검색 작업을 완료하면 호스트의 모든 데이터베이스가 표시됩니다. 데이터베이스에 대한 OS 인증이 비활성화된 경우 * 구성 * 을 클릭하여 데이터베이스 인증을 활성화합니다. 자세한 내용은 을 참조하십시오 Oracle 데이터베이스 자격 증명을 구성합니다.
    - Settings * 를 클릭하고 * Hosts * 를 선택하여 모든 호스트를 봅니다.
    - 설정 * 을 클릭하고 * 정책 * 을 선택하여 미리 구성된 정책을 봅니다. 사전 구성된 정책을 검토하여 요구 사항에 맞게 정책을 편집하거나 새 정책을 생성할 수 있습니다.

Oracle 데이터베이스 자격 증명을 구성합니다

Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용되는 데이터베이스 자격 증명을 구성해야 합니다.

단계

1. 데이터베이스에 대한 OS 인증이 비활성화된 경우 * 구성 * 을 클릭하여 데이터베이스 인증을 수정합니다.
2. 사용자 이름, 암호 및 포트 세부 정보를 지정합니다.

   데이터베이스가 ASM에 있는 경우 ASM 설정도 구성해야 합니다.

   Oracle 사용자는 sysdba 권한을 가지고 ASM 사용자는 sysasm 권한을 가지고 있어야 합니다.

3. 구성 * 을 클릭합니다.

Oracle 데이터베이스용 **SnapCenter** 플러그인을 업그레이드하십시오

Oracle용 SnapCenter 플러그인을 업그레이드하여 최신 새 기능 및 향상된 기능에 액세스해야 합니다. BlueXP UI에서 또는 명령줄을 사용하여 업그레이드할 수 있습니다.

시작하기 전에

- 호스트에서 실행 중인 작업이 없는지 확인합니다.

단계

1. 백업 및 복구 * > * 응용 프로그램 * > * 호스트 * 를 클릭합니다.
2. 전체 상태 열을 확인하여 호스트에 대해 플러그인 업그레이드를 사용할 수 있는지 확인합니다.
3. UI 또는 명령줄을 사용하여 플러그인을 업그레이드합니다.

UI를 사용하여 업그레이드합니다	명령줄을 사용하여 업그레이드합니다

a. 을 클릭합니다 ••• 호스트에 해당되며 * Upgrade Plug-in * 을 클릭합니다.
b. 구성 페이지에서 다음을 수행합니다.
i. Oracle 데이터베이스를 실행하는 Linux 시스템에 로그인하여 Oracle 데이터베이스 호스트에서 SnapCenter 사용자에 대한 sudo 액세스를 구성합니다.
ii. BlueXP UI에 표시된 텍스트를 복사합니다.
iii. Linux 시스템에서 _/etc/sudoers.d/snapcenter_file을 편집하고 복사된 텍스트를 붙여 넣습니다.
iv. BlueXP UI에서 확인란을 선택하고 * 업그레이드 * 를 클릭합니다.
	a. Connector VM에 로그인합니다.
	b. 다음 스크립트를 실행합니다.
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	
	이전 Connector를 사용하는 경우 다음 명령을 실행하여 플러그인을 업그레이드합니다.
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

클라우드 네이티브 **Oracle** 데이터베이스 백업

미리 구성된 정책 또는 사용자가 생성한 정책을 할당하여 예약된 백업 또는 필요 시 백업을 생성할 수 있습니다.

Oracle RMAN(Recovery Manager)을 사용하여 정책을 생성하는 동안 카탈로그 작성을 설정한 경우 Oracle 데이터베이스 백업을 카탈로그로 작성할 수도 있습니다. RMAN(RMAN) 카탈로그는 Azure NetApp Files에 있는 데이터베이스에만 지원됩니다. 나중에 블록 레벨 복구 또는 테이블스페이스 시점 복구 작업에 카탈로그 작성된 백업을 사용할 수 있습니다. 카탈로그를 작성하려면 데이터베이스가 마운트됨 또는 상위 상태여야 합니다.

Oracle 데이터베이스를 보호하기 위한 정책을 수립합니다

사전 구성된 정책을 편집하지 않으려는 경우 정책을 생성할 수 있습니다.

- 단계 *

1. 응용 프로그램 페이지의 설정 드롭다운 목록에서 * 정책 * 을 선택합니다.
2. Create policy * 를 클릭합니다.
3. 정책 이름을 지정합니다.
4. (선택 사항) 백업 이름의 형식을 편집합니다.
5. 스케줄 및 보존 세부 정보를 지정합니다.
6. 스케줄로 _DAILY_와 _weekly_를 선택한 경우 RMAN 카탈로그 작성을 활성화하려면 * Oracle Recovery Manager(RMAN) * 를 사용하여 카탈로그 백업 * 을 선택합니다.
7. (선택 사항) 스냅샷을 보조 스토리지에 복사하는 등 성공적인 백업 이후에 실행될 스크립트 후 경로 및 사후 스크립트의 시간 초과 값을 입력합니다.

   필요에 따라 인수를 지정할 수도 있습니다.

   사후 스크립트는 */var/opt/snapcenter/SPL/scripts* 경로에 유지해야 합니다.

   사후 스크립트는 일련의 환경 변수를 지원합니다.

환경 변수	설명
SC_ORACLE_SID입니다	Oracle 데이터베이스의 SID를 지정합니다.
sc_host를 참조하십시오	데이터베이스의 호스트 이름을 지정합니다
SC_BACKUP_NAME입니다	백업의 이름을 지정합니다. 데이터 백업 이름과 로그 백업 이름은 구분 기호를 사용하여 연결됩니다.
sc_backup_policy_name입니다	백업을 생성하는 데 사용되는 정책의 이름을 지정합니다.
sc_primary_data_volume_full_path를 입력합니다	구분 기호로 ","를 사용하여 연결된 데이터 볼륨 경로를 지정합니다. Azure NetApp Files 볼륨의 경우 "/"를 사용하여 정보가 연결됩니다. */subscription/{subscription_id}/resourceGroups/{resource_group}/providers/{provider}/netAppAccounts/{anfaccount}/capacity_pool}/volumes/{VolumeName}*

환경 변수	설명
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH를 선택합니다	구분 기호로 ","를 사용하여 연결된 아카이브 로그 볼륨 경로를 지정합니다. Azure NetApp Files 볼륨의 경우 "/"를 사용하여 연결된 정보 */subscription/{subscription_id}/resourceGroups/{resource_group}/providers/{provider}/netAppAccounts/{anfaccount}/capacity_pool}/volumes/{VolumeName}*

1. Create * 를 클릭합니다.

RMAN 카탈로그 저장소를 구성합니다

복구 카탈로그 데이터베이스를 RMAN 카탈로그 저장소로 구성할 수 있습니다. 리포지토리를 구성하지 않으면 기본적으로 타겟 데이터베이스의 제어 파일이 RMAN 카탈로그 리포지토리가 됩니다.

시작하기 전에

RMAN 카탈로그 데이터베이스에 대상 데이터베이스를 수동으로 등록해야 합니다.

단계

1. 응용 프로그램 페이지에서 을 클릭합니다 ••• > * 세부 정보 보기 *.
2. 데이터베이스 세부 정보 섹션에서 을 클릭합니다 RMAN 카탈로그 리포지토리를 구성합니다.
3. RMAN을 사용하여 백업을 카탈로그화할 자격 증명과 카탈로그 복구 데이터베이스의 TNS(Transparent Network Substrate) 이름을 지정합니다.
4. 구성 * 을 클릭합니다.

Oracle Database 백업을 생성합니다

미리 구성된 정책을 할당하거나 정책을 생성한 다음 데이터베이스에 할당할 수 있습니다. 정책이 할당되면 정책에 정의된 일정에 따라 백업이 생성됩니다.

> NetApp ONTAP 또는 Cloud Volumes ONTAP용 Amazon FSx에서 ASM 디스크 그룹을 생성할 때 디스크 그룹 전체에 공통 볼륨이 없는지 확인합니다. 각 디스크 그룹에는 전용 볼륨이 있어야 합니다.

- 단계 *

1. 응용 프로그램 페이지에서 정책을 사용하여 데이터베이스가 보호되지 않는 경우 * 정책 할당 * 을 클릭합니다.

   하나 이상의 정책을 사용하여 데이터베이스를 보호하는 경우 를 클릭하여 더 많은 정책을 할당할 수 있습니다 ••• > * 정책 할당 *.

2. 정책을 선택하고 * Assign * 을 클릭합니다.

   백업은 정책에 정의된 일정에 따라 생성됩니다. 정책에서 RMAN 카탈로그를 활성화한 경우 워크플로우 끝에 있는 백업이 별도의 작업으로 카탈로그 작업을 시작합니다. 카탈로그 작업 진행률은 Job Monitor에서 확인할 수 있습니다. 카탈로그 작성 성공 시 * 백업 세부 정보 * 는 각 백업에 대한 카탈로그 상태를 표시합니다.

서비스 계정(*SnapCenter-account-<account_id>*)은 예약된 백업 작업을 실행하는 데 사용됩니다.

Oracle 데이터베이스의 필요 시 백업을 생성합니다

정책을 할당한 후 애플리케이션의 필요 시 백업을 생성할 수 있습니다.

- 단계 *
  1. 응용 프로그램 페이지에서 을 클릭합니다 ••• 응용 프로그램에 해당하는 을 클릭하고 * On-Demand Backup * 을 클릭합니다.
  2. 여러 정책이 애플리케이션에 할당된 경우 정책, 보존 계층을 선택한 다음 * 백업 생성 * 을 클릭합니다.

     정책에서 RMAN 카탈로그를 활성화한 경우 워크플로우 끝에 있는 백업이 별도의 작업으로 카탈로그 작업을 시작합니다. 카탈로그 작성 진행률은 Job Monitor에서 확인할 수 있습니다. 카탈로그 작성 성공 시 * 백업 세부 정보 * 는 각 백업에 대한 카탈로그 상태를 표시합니다.

제한 사항

- 에서는 FSx 볼륨이 중복되어 있는 여러 ASM 디스크 그룹에 상주하는 Oracle 데이터베이스에 대한 정합성 보장 그룹 스냅샷을 지원하지 않습니다
- Oracle 데이터베이스가 NetApp ONTAP 또는 Cloud Volumes ONTAP용 Amazon FSx에 있고 ASM에 구성되어 있는 경우 SVM 이름이 FSx 시스템 전체에서 고유한지 확인합니다. FSx 시스템 간에 SVM 이름이 동일한 경우 이러한 SVM에 상주하는 Oracle 데이터베이스 백업도 지원되지 않습니다.
- 큰 데이터베이스(250GB 이상)를 복원한 후 같은 데이터베이스에서 전체 온라인 백업을 수행하는 경우 다음 오류로 인해 작업이 실패할 수 있습니다.
  ```
  failed with status code 500, error
  {\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
  snapshot. Reason: Snapshot operation not allowed due to clones backed by
  snapshots. Try again after sometime.
  ```

  이 문제를 해결하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "스냅샷이 백업한 클론으로 인해 스냅샷 작업이 허용되지 않습니다".

클라우드 네이티브 **SAP HANA** 데이터베이스 백업

빠른 시작

다음 단계를 수행하여 빠르게 시작하십시오.

1 구성에 대한 지원을 확인합니다

- 운영 체제:
  - RHEL 7.6 이상
  - SAP-HANA SPS07용 RHEL 8.1 이상
  - SLES 12 SP5 이상 및 15 SPX 플랫폼은 SAP HANA 인증을 받았습니다

- NetApp 클라우드 스토리지: Azure NetApp Files
- 스토리지 레이아웃: 데이터 및 로그 파일의 경우 Azure는 NFSv4.1만 지원합니다.
- 데이터베이스 레이아웃:
  - SAP HANA 다중 테넌트 데이터베이스 컨테이너(MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7(단일 또는 다중 테넌트 포함
  - SAP HANA 단일 호스트 시스템, SAP HANA 다중 호스트 시스템, HANA 시스템 복제
- 데이터베이스 호스트의 SAP HANA 플러그인

2 **BlueXP**에 등록하십시오

BlueXP는 웹 기반 콘솔에서 액세스할 수 있습니다. BlueXP를 시작할 때 첫 번째 단계는 기존 NetApp Support 사이트 자격 증명을 사용하거나 NetApp 클라우드 로그인을 생성하여 등록하는 것입니다. 자세한 내용은 을 참조하십시오 "BlueXP에 등록하십시오".

3 **BlueXP**에 로그인합니다

BlueXP에 등록하면 웹 기반 콘솔에서 로그인할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP에 로그인합니다".

4 **BlueXP** 계정을 관리합니다

사용자, 서비스 계정, 작업 영역 및 커넥터를 관리하여 계정을 관리할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP 계정을 관리합니다".

Azure NetApp Files를 구성합니다

BlueXP를 사용하면 Azure NetApp Files 작업 환경을 만들어 볼륨 및 추가 데이터 서비스를 추가하고 관리해야 합니다. 또한 Azure에서 Connector를 만들어 BlueXP가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

Azure NetApp Files 작업 환경을 생성합니다

데이터베이스가 호스팅되는 Azure NetApp Files 작업 환경을 만들어야 합니다. 자세한 내용은 을 참조하십시오 "Azure NetApp Files에 대해 자세히 알아보십시오" 및 "Azure NetApp Files 작업 환경을 만듭니다".

커넥터를 작성합니다

BlueXP 계정 관리자는 Azure에 Connector를 배포하여 BlueXP가 공용 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

자세한 내용은 을 참조하십시오 "BlueXP에서 Azure에 커넥터를 만듭니다".

- 커넥터에서 데이터베이스 호스트로의 연결이 있는지 확인합니다.
- 동일한 VNet(가상 네트워크)에 Azure NetApp Files 작업 환경과 데이터베이스가 있는 경우 동일한 VNET에 커넥터를 배포할 수 있습니다.

- Azure NetApp Files 작업 환경과 데이터베이스가 서로 다른 VNets에 있고 Azure NetApp Files에 NAS(NFS) 워크로드가 구성되어 있는 경우 VNets 중 하나에 커넥터를 생성할 수 있습니다.

커넥터를 만든 후 * Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하여 작업 환경을 추가합니다.

SAP HANA용 SnapCenter 플러그인을 설치하고 데이터베이스 호스트를 추가합니다

각 SAP HANA 데이터베이스 호스트에 SAP HANA용 SnapCenter 플러그인을 설치해야 합니다. SAP HANA 호스트에 SSH 키 기반 인증이 활성화되어 있는지 여부에 따라 플러그인 설치 방법 중 하나를 따를 수 있습니다.

- 데이터베이스 호스트에 SSH가 설정되어 있으면 SSH 옵션을 사용하여 플러그인을 설치할 수 있습니다. 자세한 정보.
- SSH가 비활성화된 경우 플러그인을 수동으로 설치합니다. 자세한 정보.

필수 구성 요소

호스트를 추가하기 전에 필수 구성 요소가 충족되었는지 확인해야 합니다.

- 각 SAP HANA 데이터베이스 호스트에 Java 11(64비트) Oracle Java 또는 OpenJDK가 설치되어 있는지 확인합니다.
- 작업 환경을 추가하고 Connector를 만들어야 합니다.
- Connector가 SAP HANA 데이터베이스 호스트에 연결되어 있는지 확인합니다.

  연결 문제를 해결하는 방법에 대한 자세한 내용은 을 참조하십시오 "BlueXP 커넥터 호스트에서 애플리케이션 데이터베이스 호스트로의 연결을 확인하지 못했습니다".

  커넥터를 분실하거나 새 커넥터를 만든 경우 커넥터를 기존 응용 프로그램 리소스에 연결해야 합니다. 커넥터 업데이트에 대한 지침은 을 참조하십시오 "커넥터 세부 정보를 업데이트합니다".

- BlueXP 사용자에게 "계정 관리자" 역할이 있는지 확인합니다.
- SnapCenter 사용자를 생성하고 비루트(sudo) 사용자에 대해 sudo를 구성해야 합니다. 자세한 내용은 을 참조하십시오 "SnapCenter 사용자에 대해 sudo를 구성합니다."
- 데이터베이스 호스트를 추가하기 전에 SAP HANA용 SnapCenter 플러그인을 설치해야 합니다.
- SAP HANA 데이터베이스 호스트를 추가하는 동안 HDB 사용자 저장소 키를 추가해야 합니다. HDB 보안 사용자 저장소 키는 SAP HANA 데이터베이스 호스트의 연결 정보를 클라이언트에 안전하게 저장하는 데 사용되며 HDBSQL 클라이언트는 보안 사용자 저장소 키를 사용하여 SAP HANA 데이터베이스 호스트에 연결합니다.
- HANA 시스템 복제(HSR)의 경우 HANA 시스템을 보호하려면 운영 및 보조 HANA 시스템을 모두 수동으로 등록해야 합니다.

  ⓘ 호스트 이름은 HSR 복제에 사용되는 호스트의 호스트 이름과 같아야 합니다.

- SSH 기반 설치를 수행하는 경우 커넥터에 SSH 포트에 대한 통신이 활성화되어 있는지 확인합니다(기본값: 22).
- 데이터 보호 작업이 작동하려면 커넥터에 플러그인 포트(기본값: 8145)에 대한 통신이 활성화되어 있는지 확인합니다.

- 최신 버전의 플러그인이 설치되어 있는지 확인합니다. 플러그인을 업그레이드하려면 를 참조하십시오 SAP HANA 데이터베이스용 SnapCenter 플러그인을 업그레이드하십시오.

SnapCenter 사용자에 대해 **sudo**를 구성합니다

root(sudo) 사용자가 아닌 사용자를 만들어 플러그인을 설치합니다.

단계

1. Connector VM에 로그인합니다.
2. SnapCenter Linux 호스트 플러그인 바이너리를 다운로드합니다. S UDO Docker Exec - IT cloudmanager_scs_cloud curl-X get 'http://127.0.0.1/deploy/downloadLinuxPlugin'`
3. sudoer.txt * 의 내용을 */var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/$(sudo Docker PS | grep-po "cloudManager_scs_cloud:. *? "|SED-e's/ *$/"|cut-F2-d":")/SC-Linux-host-plugin*
4. 루트 사용자 계정을 사용하여 SAP HANA 시스템 호스트에 로그인합니다.
5. 3단계에서 복사한 텍스트를 _/etc/sudoers.d/snapcenter_file에 복사하여 비루트 사용자에 대한 sudo 액세스를 구성합니다.

   /etc/sudoers.d/snapcenter_file에 추가한 줄에서 _<LINUXUSER>_를 루트가 아닌 사용자로 바꾸고 _<USER_HOME_DIRECTORY>_를 _HOME/<non-root-user>_로 바꿉니다.

스크립트를 사용하여 플러그인을 설치합니다

SAP HANA 호스트 비루트 사용자 계정에 대한 SSH 키 기반 인증을 구성하고 다음 단계를 수행하여 플러그인을 설치합니다.

시작하기 전에

커넥터에 대한 SSH 연결이 활성화되어 있는지 확인합니다.

단계

1. Connector VM에 로그인합니다.
2. Connector에 제공된 스크립트를 사용하여 플러그인을 설치합니다.
   ```
   sudo bash /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

   이전 커넥터를 사용하는 경우 다음 명령을 실행하여 플러그인을 설치합니다.
   ```
   sudo
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

이름	설명	필수입니다	기본값
plugin_host 를 선택합니다	SAP HANA 호스트를 지정합니다	예	-

이름	설명	필수입니다	기본값
host_user_name	SAP HANA 호스트에 대한 SSH 권한이 있는 SnapCenter 사용자를 지정합니다	예	-
host_ssh_key입니다	SnapCenter 사용자의 SSH 키를 지정하며 SAP HANA 호스트에 연결하는 데 사용됩니다	예	-
plugin_port 를 선택합니다	플러그인에서 사용하는 포트를 지정합니다	아니요	8145
host_ssh_port	SAP HANA 호스트의 SSH 포트를 지정합니다	아니요	22

예를 들어, 'sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh — host 10.0.1.1 — username SnapCenter — sshkey/netapp-ssh.ppk

플러그인을 설치한 후에는 다음을 수행해야 합니다 SAP HANA 데이터베이스 호스트를 추가합니다.

플러그인을 수동으로 설치합니다

HANA 호스트에 SSH 키 기반 인증이 설정되어 있지 않은 경우 아래의 수동 단계를 수행하여 플러그인을 설치해야 합니다.

- 단계 *
  1. Connector VM에 로그인합니다.
  2. SnapCenter Linux 호스트 플러그인 바이너리를 다운로드합니다. S UDO Docker Exec - IT cloudmanager_scs_cloud curl-X get 'http://127.0.0.1/deploy/downloadLinuxPlugin'`

     플러그인 바이너리는 _ cd /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/*data/$(sudo docker PS | grep-Po "cloudmanager_scs_cloud:. *? "|SED-e's/ *$/'|cut-F2-d":")/SC-Linux-host-plugin*
  3. SCP 또는 다른 대체 방법을 사용하여 각 SAP HANA 데이터베이스 호스트에 대한 */home/<non root user (sudo)>/.SC_NetApp_path*의 위 경로에서 *copy_snapcenter_linux_host_plugin_scs.bin*
  4. 비 루트(sudo) 계정을 사용하여 SAP HANA 데이터베이스 호스트에 로그인합니다.
  5. 디렉토리를 _/home/<non root user>/.sc_netapp/_로 변경하고 다음 명령을 실행하여 바이너리에 대한 실행 권한을 활성화합니다.
     ```
     chmod +x snapcenter_linux_host_plugin_scs.bin
     ```
  6. sudo SnapCenter 사용자로 SAP HANA 플러그인을 설치합니다.
     ```
     ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
     ```
  7. copy_certificate.pem_from_<base_mount_path>/client/certificate/_path 커넥터 VM의 경로를 플러그인

호스트의 _/var/opt/snapcenter/spl/etc/_로 복사합니다.

8. /var/opt/snapcenter/spl/etc_로 이동하고 keytool 명령을 실행하여 인증서를 가져옵니다.
```
keytool -import -alias agentcert -file certificate.pem -keystore
keystore.jks -deststorepass snapcenter -noprompt
```
9. SPL을 다시 시작합니다:'stemctl restart SPL'
10. Connector에서 아래 명령을 실행하여 커넥터에서 플러그인에 연결할 수 있는지 확인합니다.
```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
plug-in host>:<plug-in port>/PluginService/Version --cert
config/client/certificate/certificate.pem --key
/config/client/certificate/key.pem
```

플러그인을 설치한 후에는 다음을 수행해야 합니다 SAP HANA 데이터베이스 호스트를 추가합니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인을 업그레이드하십시오

최신 새 기능 및 향상된 기능을 이용하려면 SAP HANA용 SnapCenter 플러그인을 업그레이드해야 합니다.

- 시작하기 전에 *
- 호스트에서 실행 중인 작업이 없는지 확인합니다.
- 단계 *
  1. SnapCenter 사용자에 대해 sudo를 구성합니다. 자세한 내용은 을 참조하십시오 SnapCenter 사용자에 대해 sudo를 구성합니다.
  2. 다음 스크립트를 실행합니다.
```
/var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.
sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

     이전 Connector를 사용하는 경우 다음 명령을 실행하여 플러그인을 업그레이드합니다.
```
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_pl
ugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
--upgrade
```

SAP HANA 데이터베이스 호스트를 추가합니다

정책을 할당하고 백업을 생성하려면 SAP HANA 데이터베이스 호스트를 수동으로 추가해야 합니다. SAP HANA 데이터베이스 호스트에 대한 자동 검색은 지원되지 않습니다.

- 단계 *
  1. BlueXP * UI에서 * Protection * > * Backup and Recovery * > * Applications * 를 선택합니다.
  2. Discover Applications * 를 선택합니다.
  3. Cloud Native * > * SAP HANA * 를 선택하고 * Next * 를 선택합니다.
  4. 응용 프로그램 * 페이지에서 * 시스템 추가 * 를 선택합니다.
  5. 시스템 세부 정보 * 페이지에서 다음 작업을 수행합니다.

a. 시스템 유형 을 멀티 테넌트 데이터베이스 컨테이너 또는 글로벌 비 데이터 볼륨 으로 선택합니다.
b. SAP HANA 시스템 이름을 입력합니다.
c. SAP HANA 시스템의 SID를 지정합니다.
d. (선택 사항) OSDB 사용자를 수정합니다.
e. HANA 시스템이 HANA 시스템 복제로 구성된 경우 * HSR(HANA 시스템 복제) 시스템 * 을 활성화합니다.
f. HDB 보안 사용자 저장소 키 * 텍스트 상자를 선택하여 사용자 저장소 키 세부 정보를 추가합니다.

   키 이름, 시스템 세부 정보, 사용자 이름 및 암호를 지정하고 * 키 추가 * 를 클릭합니다.

사용자 저장소 키를 삭제하거나 수정할 수 있습니다.

6. 다음 * 을 선택합니다.
7. 호스트 세부 정보 * 페이지에서 다음 작업을 수행합니다.
   a. Add new host * 또는 * use existing host * 를 선택합니다.
   b. USING SSH * 또는 * Manual * 을 선택합니다.

      수동 의 경우 호스트 FQDN 또는 IP, 커넥터, 사용자 이름, SSH 포트, 플러그인 포트를 입력합니다. 필요에 따라 SSH 개인 키를 추가하고 검증합니다.

SSH의 경우 호스트 FQDN 또는 IP, 커넥터, 사용자 이름 및 플러그인 포트를 입력합니다.

   a. 다음 * 을 선택합니다.
      1. 호스트 구성 * 페이지에서 구성 요구 사항이 충족되는지 확인합니다.

         확인란을 선택하여 확인합니다.

      2. 다음 * 을 선택합니다.
      3. Storage Footprint * 페이지에서 * Add Storage * 를 선택하고 다음을 수행합니다.
   b. 작업 환경을 선택하고 NetApp 계정을 지정합니다.

      왼쪽 탐색 창에서 BlueXP * Canvas * 를 선택하여 새 작업 환경을 추가합니다.

   c. 필요한 볼륨을 선택합니다.
   d. Add Storage * 를 선택합니다.
      1. 모든 세부 정보를 검토하고 * Add System * 을 선택합니다.

UI에서 SAP HANA 시스템을 수정하거나 제거할 수 있습니다.

SAP HANA 시스템을 제거하기 전에 관련된 모든 백업을 삭제하고 보호를 제거해야 합니다.

비 데이터 볼륨 추가

멀티 테넌트 데이터베이스 컨테이너 유형 SAP HANA 시스템을 추가한 후 HANA 시스템의 비 데이터 볼륨을 추가할 수 있습니다.

사용 가능한 SAP HANA 데이터베이스를 검색하고 나면 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을

수행할 수 있습니다.

- 단계 *
  1. BlueXP * UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
  2. 응용 프로그램 검색 * 을 클릭합니다.
  3. Cloud Native * > * SAP HANA * 를 선택하고 * Next * 를 클릭합니다.
  4. 응용 프로그램 * 페이지에서 을 클릭합니다 ••• 비 데이터 볼륨을 추가하려는 시스템에 해당하는 * 시스템 관리 * > * 비 데이터 볼륨 * 을 선택합니다.

글로벌 비 데이터 볼륨 추가

멀티 테넌트 데이터베이스 컨테이너 유형 SAP HANA 시스템을 추가한 후 HANA 시스템의 글로벌 비 데이터 볼륨을 추가할 수 있습니다.

- 단계 *
  1. BlueXP * UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
  2. 응용 프로그램 검색 * 을 클릭합니다.
  3. Cloud Native * > * SAP HANA * 를 선택하고 * Next * 를 클릭합니다.
  4. 응용 프로그램 * 페이지에서 * 시스템 추가 * 를 클릭합니다.
  5. 시스템 세부 정보 * 페이지에서 다음 작업을 수행합니다.
     a. 시스템 유형 드롭다운에서 * 글로벌 비 데이터 볼륨 * 을 선택합니다.
     b. SAP HANA 시스템 이름을 입력합니다.
  6. . 호스트 세부 정보 * 페이지에서 다음 작업을 수행합니다.
     a. SAP HANA 시스템의 관련 SID를 지정합니다.
     b. 플러그인 호스트를 선택합니다
     c. 다음 * 을 클릭합니다.
     d. 모든 세부 정보를 검토하고 * 시스템 추가 * 를 클릭합니다.

클라우드 네이티브 **SAP HANA** 데이터베이스 백업

미리 구성된 정책 또는 생성한 정책을 할당하여 백업을 생성할 수 있습니다.

SAP HANA 데이터베이스를 보호하기 위한 정책을 수립합니다

사전 구성된 정책을 사용하거나 편집하지 않으려는 경우 정책을 생성할 수 있습니다.

1. 응용 프로그램 * 페이지의 설정 드롭다운 목록에서 * 정책 * 을 선택합니다.
2. Create policy * 를 클릭합니다.
3. 정책 이름을 지정합니다.
4. (선택 사항) 스냅샷 복사본 이름의 형식을 편집합니다.
5. 정책 유형을 선택합니다.

6. 스케줄 및 보존 세부 정보를 지정합니다.
7. (선택 사항) 스크립트를 지정합니다. "사전 스크립트 및 포스트스크립트"
8. Create * 를 클릭합니다.

사전 스크립트 및 포스트스크립트

정책을 생성하는 동안 처방자, postscript 및 종료 스크립트를 제공할 수 있습니다. 이러한 스크립트는 데이터 보호 작업 중에 HANA 호스트에서 실행됩니다.

스크립트에 대해 지원되는 형식은 .sh, python 스크립트, perl 스크립트 등이 있습니다.

prescpt 및 PostScript는 호스트 관리자가 에 등록해야 합니다 `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` 파일.

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

환경 변수

백업 워크플로우의 경우, 다음 환경 변수를 prescpt 및 PostScript의 일부로 사용할 수 있습니다.

환경 변수	설명
SID	복원을 위해 선택한 HANA 데이터베이스의 시스템 식별자입니다
백업 이름	복원 작업에 대해 선택한 백업 이름입니다
UserStoreKeyNames를 참조하십시오	HANA 데이터베이스용 사용자 저장소 키를 구성했습니다
OSDBUser	HANA 데이터베이스에 대해 OSDBUser를 구성했습니다
정책 이름	예약된 백업 전용입니다
schedule_type입니다	예약된 백업 전용입니다

SAP HANA 데이터베이스의 백업을 생성합니다

미리 구성된 정책을 할당하거나 정책을 생성한 다음 데이터베이스에 할당할 수 있습니다. 정책이 할당되면 정책에 정의된 일정에 따라 백업이 생성됩니다.

- 시작하기 전에 *

SAP HANA 데이터베이스 호스트를 추가해야 합니다."SAP HANA 데이터베이스 호스트를 추가합니다"

- 이 작업에 대한 정보 *

HANA 시스템 복제(HSR)의 경우 예약된 백업 작업은 운영 HANA 시스템에 대해서만 트리거되며, 시스템이 보조 HANA 시스템으로 페일오버되면 기존 스케줄이 현재 운영 HANA 시스템에 대한 백업을 트리거합니다. 운영 HANA 시스템과 보조 HANA 시스템 모두에 정책이 할당되지 않은 경우 페일오버 후 일정이 실패합니다.

HSR 시스템에 서로 다른 정책이 할당된 경우 기본 및 보조 HANA 시스템에 대해 예약된 백업이 트리거되고 보조 HANA 시스템에 대한 백업이 실패합니다.

- 단계 *

1. 응용 프로그램 페이지에서 정책을 사용하여 데이터베이스가 보호되지 않는 경우 * 정책 할당 * 을 클릭합니다.

   데이터베이스가 하나 이상의 정책을 사용하여 보호되지만 필요한 경우 를 클릭하여 추가 정책을 계속 할당할 수 있습니다 ••• > * 정책 할당 *.

2. 정책을 선택하고 * Assign * 을 클릭합니다.

   백업은 정책에 정의된 일정에 따라 생성됩니다.

   ⓘ 서비스 계정(*SnapCenter-account-<account_id>*)은 예약된 백업 작업을 실행하는 데 사용됩니다.

SAP HANA 데이터베이스의 온디맨드 백업 생성

정책을 할당한 후 애플리케이션의 필요 시 백업을 생성할 수 있습니다.

- 단계 *

1. 응용 프로그램 * 페이지에서 을 클릭합니다 ••• 응용 프로그램에 해당하는 을 클릭하고 * On-Demand Backup * 을 클릭합니다.
2. 필요 시 백업 유형을 선택합니다.
3. 정책 기반 백업의 경우 정책, 보존 계층을 선택한 다음 * 백업 생성 * 을 클릭합니다.
4. 한 번 스냅샷 복사본 기반 또는 파일 기반 을 선택합니다. 다음 단계를 수행합니다.
   a. 보존 값을 선택하고 백업 이름을 지정합니다.
   b. (선택 사항) 스크립트의 스크립트 및 경로를 지정합니다.

      자세한 내용은 을 참조하십시오 "사전 스크립트 및 포스트스크립트"

   c. 백업 생성 * 을 클릭합니다.

REST API를 사용하여 클라우드 네이티브 SQL Server 데이터베이스를 백업합니다

빠른 시작

다음 단계를 수행하여 빠르게 시작하십시오.

1 구성에 대한 지원을 확인합니다

- 운영 체제:
  - Windows 2016
  - 윈도우즈 2019
  - Windows 2022
- NetApp 클라우드 스토리지:Amazon FSx for NetApp ONTAP
- 스토리지 레이아웃: SAN(iSCSI)

  NAS 구성은 지원되지 않습니다.

- 데이터베이스 버전:
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2022
- 데이터베이스 구성:
  - 독립 실행형

2 **BlueXP**에 등록하십시오

BlueXP는 웹 기반 콘솔에서 액세스할 수 있습니다. BlueXP를 시작할 때 첫 번째 단계는 기존 NetApp Support 사이트 자격 증명을 사용하거나 NetApp 클라우드 로그인을 생성하여 등록하는 것입니다. 자세한 내용은 을 참조하십시오 "BlueXP에 등록하십시오".

3 **BlueXP**에 로그인합니다

BlueXP에 등록하면 웹 기반 콘솔에서 로그인할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP에 로그인합니다".

4 **BlueXP** 계정을 관리합니다

사용자, 서비스 계정, 작업 영역 및 커넥터를 관리하여 계정을 관리할 수 있습니다. 자세한 내용은 을 참조하십시오 "BlueXP 계정을 관리합니다".

ONTAP에 대해 **FSx**를 구성합니다

BlueXP를 사용하면 ONTAP 작업 환경에 FSx를 생성하여 볼륨 및 추가 데이터 서비스를 추가하고 관리해야 합니다. 또한 BlueXP에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 AWS에 Connector를 만들어야 합니다.

ONTAP 작업 환경을 위한 **FSx**를 생성합니다

데이터베이스가 호스팅되는 ONTAP 작업 환경용 FSx를 만들어야 합니다. 자세한 내용은 을 참조하십시오 "ONTAP용

Amazon FSx를 시작하십시오" 및 "ONTAP 작업 환경을 위한 Amazon FSx를 생성하고 관리합니다".

BlueXP 또는 AWS를 사용하여 ONTAP 작업 환경을 위한 FSx를 생성할 수 있습니다. AWS를 사용하여 생성한 경우 BlueXP에서 ONTAP 시스템용 FSx를 검색해야 합니다.

커넥터를 작성합니다

계정 관리자는 AWS에서 Connector를 생성하여 BlueXP가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있도록 해야 합니다.

자세한 내용은 을 참조하십시오 "BlueXP에서 AWS에 커넥터 생성".

- 동일한 커넥터를 사용하여 ONTAP 작업 환경 및 데이터베이스에 대한 FSx를 모두 관리해야 합니다.
- 동일한 VPC(Virtual Private Cloud)에 ONTAP 작업 환경 및 데이터베이스를 위한 FSx가 있는 경우 동일한 VPC에 커넥터를 배포할 수 있습니다.
- ONTAP 작업 환경 및 다른 VPC에 데이터베이스를 위한 FSx가 있는 경우:
  - ONTAP용 FSx에서 NAS(NFS) 워크로드를 구성한 경우, 두 VPC 중 하나에 커넥터를 생성할 수 있습니다.
  - SAN 워크로드만 구성되어 있고 NAS(NFS) 워크로드를 사용할 계획이 없는 경우, ONTAP용 FSx 시스템이 생성되는 VPC에 커넥터를 생성해야 합니다.

> NAS(NFS) 워크로드를 사용하려면 VPC 데이터베이스와 Amazon VPC 간에 전송 게이트웨이가 있어야 합니다. 부동 IP 주소인 NFS IP 주소는 전송 게이트웨이를 통해서만 다른 VPC에서 액세스할 수 있습니다. VPC를 피해서 유동 IP 주소에 액세스할 수 없습니다.

Connector를 생성한 후 * Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하고 화면의 지시에 따라 작업 환경을 추가합니다. Connector와 Oracle 데이터베이스 호스트 및 FSx 작업 환경이 연결되어 있는지 확인합니다. Connector는 FSx 작업 환경의 클러스터 관리 IP 주소에 연결할 수 있어야 합니다.

- Storage * > * Canvas * > * My Working Environments * > * Add Working Environment * 를 클릭하여 작업 환경을 추가합니다.

  커넥터에서 데이터베이스 호스트 및 FSx for ONTAP 작업 환경과의 연결이 있는지 확인합니다. 커넥터는 ONTAP 작업 환경의 FSx의 클러스터 관리 IP 주소에 연결해야 합니다.

- 커넥터 > 커넥터 관리 * 를 클릭하고 커넥터 이름을 선택하여 커넥터 ID를 복사합니다.

SQL Server용 SnapCenter 플러그인 설치 및 데이터베이스 호스트 추가

각 SQL 데이터베이스 호스트에 SnapCenter Plug-in for SQL Server를 설치하고, 데이터베이스 호스트를 추가하고, 데이터베이스 인스턴스를 검색하고, 데이터베이스 인스턴스에 대한 자격 증명을 구성해야 합니다.

SQL Server용 SnapCenter 플러그인을 설치합니다

플러그인 * snapcenter_service_windows_host_plugin.exe * 를 다운로드한 다음 자동 설치 프로그램 명령을 실행하여 데이터베이스 호스트에 플러그인을 설치해야 합니다.

시작하기 전에

- 다음 필수 구성 요소가 충족되는지 확인해야 합니다.
  - Net 4.7.2가 설치되어 있습니다
  - PowerShell 4.0이 설치되어 있습니다
  - 최소 5GB의 디스크 공간을 사용할 수 있습니다
  - 최소 RAM 크기 4GB 사용 가능
- API를 실행하여 고객 온보딩을 완료해야 합니다. 자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant

단계

1. Connector 호스트에서 API를 실행하여 플러그인을 다운로드합니다.
   ```
   docker exec -it cloudmanager_scs_cloud curl
   'http://127.0.0.1/api/v2/pluginpackage/windows'
   ```

   파일 위치는 _/var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/<agent_version>/sc-windows-host-plugin/snapcenter_service_windows_host_plugin.exe_입니다.

2. SCP 또는 다른 방법을 사용하여 커넥터에서 각 MSSQL 서버 데이터베이스 호스트로 _snapcenter_service_windows_host_plugin.exe_를 복사합니다.
3. 플러그인을 설치합니다.
   '"C://<install_folder>/snapcenter_service_windows_host_plugin.exe" /silent/debuglog "C://<install_folder>/HA_Suite_Silent_Install_scsql_fresh.log" /log "C://install_folder/"BI_SNAPCENTENTENTPORT=8145 ISER 설치 = SCSQL'
4. 자체 서명된 인증서를 _/var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/client/certificate/certificate.pem_에서 MSSQL 서버 데이터베이스 호스트로 복사합니다.

   기본 인증서를 사용하지 않는 경우 자체 서명된 인증서 또는 CA 서명된 인증서를 생성할 수도 있습니다.

5. 커넥터 호스트에서 인증서를 .pem에서 .crt 형식으로 변환합니다.
   'openssl x509-outform der-in certificate.pem-out certificate.crt'
6. 인증서를 두 번 클릭하여 * 개인 * 및 * 신뢰할 수 있는 루트 인증 기관 * 저장소에 추가합니다.

SQL Server 데이터베이스 호스트를 추가합니다

호스트 FQDN을 사용하여 MSSQL 데이터베이스 호스트를 추가해야 합니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts' 를 참조하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/AddHosts

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
주소	문자열	참
커넥터_ID	문자열	참
플러그인_유형	문자열	참
설치 방법	문자열	참
plugin_port 를 선택합니다	번호	참
사용자 이름	문자열	참

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

추가된 **SQL Server** 데이터베이스 호스트를 봅니다

이 API를 실행하여 추가된 모든 SQL Server 데이터베이스 호스트를 볼 수 있습니다.

'snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts' 다운로드하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts

응답

API가 정상적으로 실행되면 응답 코드 200이 출력된다.

예:

```
{
  "num_records": 1,
    "total_records": 1,
    "records": [
        {
            "id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "addr": "scspa2722211001.rtp.openenglab.netapp.com",
            "status": "Running",
            "connector_id": "fBf8Iwbp4BscBfD02qBwWm6I03gGAesRclients",
            "plugin_port": 8145,
            "plugins": [
                {
                    "type": "mssql"
                }
            ],
            "os_type": "windows",
            "platform": "onprem",
            "username": "administrator",
            "operating_mode": "production"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


데이터베이스 인스턴스를 검색합니다

이 API를 실행하고 호스트 ID를 입력하여 모든 MSSQL 인스턴스를 검색할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery' 를 참조하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
host_id입니다	문자열	참

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

검색된 데이터베이스 인스턴스를 봅니다

이 API를 실행하여 검색된 모든 데이터베이스 인스턴스를 볼 수 있습니다.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances' 다운로드하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/GetMSSQLInstancesRequest

응답

API가 정상적으로 실행되면 응답 코드 200이 출력된다.

예:

```
{
    "num_records": 2,
    "total_records": 2,
    "records": [
        {
            "id": "953e66de-10d9-4fd9-bdf2-bf4b0eaabfd7",
            "name": "scspa2722211001\\NAMEDINSTANCE1",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Running",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        },
        {
            "id": "18e1b586-4c89-45bd-99c8-26268def787c",
            "name": "scspa2722211001",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Stopped",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        }
    ],
    "_links": {
        "next": {}
    }
}
```


데이터베이스 인스턴스 자격 증명을 구성합니다

이 API를 실행하여 데이터베이스 인스턴스의 자격 증명을 확인하고 설정할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration' 를 참조하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
host_id입니다	문자열	참
인스턴스_ID	문자열	참
사용자 이름	문자열	참
암호	문자열	참
auth_mode(인증 모드	문자열	참

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

클라우드 네이티브 **Microsoft SQL Server** 데이터베이스를 백업

생성한 정책을 할당하여 예약된 백업 또는 필요 시 백업을 생성할 수 있습니다.

백업 정책을 생성합니다

이 API를 실행하여 백업 정책을 생성할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies' 를 참조하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
이름	문자열	참
백업 유형	문자열	참
Copy_only_backup(복사 전용 백업)	문자열	거짓
시스템 정의입니다	문자열	거짓
백업_이름_형식	문자열	참
schedule_type입니다	문자열	참
start_time을 선택합니다	번호	참
시간_간격	번호	참
분_간격	번호	참
retention_type을 선택합니다	문자열	참
retention_count입니다	번호	참
end_time을 선택합니다	번호	참

응답

API가 정상적으로 실행되면 응답 코드 201이 표시됩니다.

예:

```
{
    "_links": {
    "self": {
        "href": "/api/resourcelink"
      }
    }
}
```

SQL 데이터베이스 인스턴스에 정책을 할당합니다

이 API를 실행하여 SQL 데이터베이스 인스턴스에 정책을 할당할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment' 를 참조하십시오

여기서, _id_는 DISCOVER 데이터베이스 인스턴스 API를 실행하여 얻은 MSSQL 인스턴스 ID입니다. 자세한 내용은 을 참조하십시오 "데이터베이스 인스턴스를 검색합니다".

여기서 ID 배열이 입력됩니다. 예를 들면 다음과 같습니다.

```
[
  "c9f3e68d-1f9c-44dc-b9af-72a9dfc54320"
]
```

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

필요 시 백업을 생성합니다

이 API를 실행하여 주문형 백업을 생성할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups' 를 참조하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/CreateMSSQLBackupRequest

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
ID입니다 MSSQL 데이터베이스 인스턴스의 ID입니다.	문자열	참
resource_type입니다	문자열	참
policy_id입니다	문자열	참
schedule_type입니다	문자열	참

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

백업을 봅니다

이러한 API를 실행하여 모든 백업을 나열하고 특정 백업의 세부 정보를 볼 수도 있습니다.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups' 다운로드하십시오

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}' 다운로드하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/MSSQLGetBackupsRequest

응답

API가 정상적으로 실행되면 응답 코드 200이 출력된다.

예:

```
{
    "total_records": 1,
    "num_records": 1,
    "records": [
        {
            "backup_id": "602d7796-8074-43fc-a178-eee8c78566ac",
            "resource_id": "a779578d-cf78-46f3-923d-b9223255938c",
            "backup_name":
"Hourly_policy2_scspa2722211001_NAMEDINSTANCE1_2023_08_08_07_02_01_81269_0
",
            "policy_name": "policy2",
            "schedule_type": "Hourly",
            "start_time": "2023-08-08T07:02:10.203Z",
            "end_time": "0001-01-01T00:00:00Z",
            "backup_status": "success",
            "backup_type": "FullBackup"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

클라우드 네이티브 **Oracle** 데이터베이스 복원

클라우드 네이티브 **Oracle** 데이터베이스를 원래 위치로 복원합니다

데이터가 손실된 경우 데이터 파일, 제어 파일 또는 둘 모두를 원래 위치로 복원한 다음 데이터베이스를 복구할 수 있습니다.

시작하기 전에

Oracle 21c 데이터베이스가 시작 상태인 경우 복원 작업이 실패합니다. 다음 명령을 실행하여 데이터베이스를 복원해야 합니다.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```

단계

1. 을 클릭합니다 ••• 복원하려는 데이터베이스에 해당하는 을 클릭하고 * 복원 * 을 클릭합니다.
2. 데이터베이스를 복원할 복원 지점을 선택하고 * 원래 위치로 복원 * 을 클릭합니다.
3. 복원 범위 섹션에서 다음 작업을 수행합니다.

만약...	수행할 작업...
데이터 파일만 복구하려는 경우	모든 데이터 파일 * 을 선택합니다.
컨트롤 파일만 복구하려는 경우	제어 파일 * 을 선택합니다
데이터 파일과 제어 파일을 모두 복원하려고 합니다	모든 데이터 파일 * 및 * 제어 파일 * 을 선택합니다.

강제 데이터 이동 없이 복원 * 확인란을 선택할 수도 있습니다.

Amazon FSx for NetApp ONTAP 또는 Cloud Volumes ONTAP SAN 레이아웃에서 Oracle용 SnapCenter 플러그인이 ASM 디스크 그룹에서 Oracle 데이터 파일 이외의 외부 파일을 찾으면 연결 및 복사 복원 방법을 수행합니다. 외부 파일은 다음 유형 중 하나 이상이 될 수 있습니다.

- 매개 변수
- 암호
- 보관 로그
- 온라인 로그
- ASM 매개 변수 파일입니다.

  강제 데이터 이동 없이 복원 * 옵션은 매개 변수, 암호 및 아카이브 로그 유형의 외부 파일을 재정의합니다. 원본 위치 복원 강제 * 옵션을 선택한 경우 최신 백업을 사용해야 합니다.

4. 복구 범위 섹션에서 다음 작업을 수행합니다.

만약...	수행할 작업...
마지막 트랜잭션으로 복구하려고 합니다	모든 로그 * 를 선택합니다.
특정 SCN(시스템 변경 번호)으로 복구하려는 경우	SCN * 까지 * 를 선택하고 SCN을 지정합니다.
특정 날짜 및 시간으로 복구하려는 경우	날짜 및 시간 * 을 선택합니다.
복구하기를 원하지 않습니다	No recovery * 를 선택합니다.

선택한 복구 범위의 경우 * Archive Log Files Locations * 필드에서 복구에 필요한 아카이브 로그가 포함된 위치를 선택적으로 지정할 수 있습니다.

복구 후 데이터베이스를 읽기-쓰기 모드로 열려면 이 확인란을 선택합니다.

5. 다음 * 을 클릭하고 세부 정보를 검토합니다.
6. 복원 * 을 클릭합니다.

클라우드 네이티브 **Oracle** 데이터베이스를 대체 위치로 복원합니다

데이터가 손실된 경우 Oracle 데이터베이스를 Azure NetApp Files의 대체 위치로만 복원할 수 있습니다. 대체 위치는 다른 호스트 또는 동일한 호스트에 있을 수 있습니다.

시작하기 전에

- Oracle 21c 데이터베이스가 시작 상태인 경우 복원 작업이 실패합니다. 다음 명령을 실행하여 데이터베이스를 복원해야 합니다.

  ```
  cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
  /opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
  ```

- 대체 호스트의 Oracle 버전이 원래 호스트의 버전과 동일한지 확인해야 합니다.

이 작업에 대해

복원 작업을 시작하는 동안 Oracle Home, 최대 볼륨 처리량, Oracle SID 및 데이터베이스 자격 증명을 제외한 구성을 수정할 수 없습니다.

전체 복구는 기본적으로 _ until cancel_set을 true로 설정하여 활성화됩니다.

복원된 데이터베이스에 대해 보관 로그 모드가 기본적으로 해제되어 있습니다. 필요한 경우 아카이브 로그 모드를 활성화하고 아카이브 로그를 NetApp 볼륨에 유지할 수 있습니다.

단계

1. 을 클릭합니다 ••• 복원하려는 데이터베이스에 해당하는 을 클릭하고 * 복원 * 을 클릭합니다.
2. 데이터베이스를 복원할 복원 지점을 선택하고 * 대체 위치로 복원 * > * 다음 * 을 클릭합니다.
3. 구성 페이지에서 대체 위치, SID, ORACLE_Home, 데이터베이스 자격 증명 및 스토리지 처리량의 세부 정보를 지정합니다.

   데이터베이스 자격 증명의 경우 OS 사용자 인증이 비활성화된 경우 시스템 사용자가 동일한 호스트 또는 대상 호스트의 복원된 데이터베이스에 연결할 수 있도록 암호를 제공해야 합니다.

4. 다음 * 을 클릭하고 세부 정보를 검토한 후 * 복원 * 을 클릭합니다.

   복구 작업의 진행 상황은 Job Monitor 페이지에서 볼 수 있습니다. 작업이 완료된 후 * Discovery 새로 고침 * 을 클릭하여 복원된 데이터베이스를 확인합니다. 그러나 대체 위치로 복원되는 데이터베이스는 보호할 수 없습니다.

클라우드 네이티브 **SAP HANA** 데이터베이스 복원

데이터가 손실된 경우 데이터 및 비 데이터 파일을 복원한 다음 데이터베이스를 복구할 수 있습니다.

- 시작하기 전에 *
- SAP HANA 시스템은 중지된 상태여야 합니다.
- SAP HANA 시스템이 실행 중이면 처방된 내용을 제공하여 시스템을 중지할 수 있습니다.
- 이 작업에 대한 정보 *
- 볼륨에 대해 ANF 백업을 활성화하면 단일 파일 SnapRestore 작업이 수행됩니다.

- 비 데이터 볼륨 및 글로벌 비 데이터 볼륨의 경우 연결 및 복제 복원 작업이 수행됩니다.
  - 연결 및 복사 복원 작업에 대한 서비스 품질(QoS) 값은 비 데이터 볼륨 또는 글로벌 비 데이터 볼륨의 소스 볼륨에서 선택됩니다.

> QoS는 "Manual" 유형의 용량 풀에만 적용할 수 있습니다.

- 단계 *
  1. 을 클릭합니다 ••• 복원하려는 데이터베이스에 해당하는 * 세부 정보 보기 * 를 클릭합니다.
  2. 을 클릭합니다 ••• 복원하려는 데이터 백업에 해당하고 * 복원 * 을 클릭합니다.
  3. 시스템 복원 * 페이지에서 스크립트를 입력합니다. "사전 스크립트 및 포스트스크립트"

     복원 워크플로의 경우 다음 환경 변수를 처방과 PS의 일부로 사용할 수 있습니다.

환경 변수	설명
SID	복원을 위해 선택한 HANA 데이터베이스의 시스템 식별자입니다
백업 이름	복원 작업에 대해 선택한 백업 이름입니다
UserStoreKeyNames를 참조하십시오	HANA 데이터베이스용 사용자 저장소 키를 구성했습니다
OSDBUser	HANA 데이터베이스에 대해 OSDBUser를 구성했습니다

  1. 복원 * 을 클릭합니다.
- 다음 단계 *

복원 후 SAP HANA 시스템을 수동으로 복구하거나 SAP HANA 시스템 복구를 수행하는 PostScript를 제공합니다.

비 데이터 볼륨 복원

- 이 작업에 대한 정보 *

연결 및 복사 복원 작업의 경우 Microsoft Azure 포털로 이동하여 볼륨을 선택하고 * Edit * 를 클릭한 다음 * Hide snapshot path * 를 활성화합니다.

- 단계 *
  1. 응용 프로그램 * 페이지의 드롭다운 상자에서 비 데이터 볼륨 을 선택합니다.
  2. 을 클릭합니다 ••• 복원하려는 백업에 해당하는 을 클릭하고 * 복원 * 을 클릭합니다.

글로벌 비 데이터 볼륨 복원

- 이 작업에 대한 정보 *

연결 및 복사 복원 작업의 경우 Microsoft Azure 포털로 이동하여 볼륨을 선택하고 * Edit * 를 클릭한 다음 * Hide snapshot path * 를 활성화합니다.

- 단계 *
  1. Applications * 페이지에서 복원하려는 글로벌 비 데이터 볼륨을 클릭합니다.
  2. 을 클릭합니다 ••• 복원하려는 글로벌 비 데이터 볼륨에 해당하는 * 복원 * 을 클릭합니다.

Microsoft SQL Server 데이터베이스를 복원합니다

Microsoft SQL Server 데이터베이스를 동일한 호스트에 복구할 수 있습니다. 먼저 데이터베이스 목록을 가져온 다음 데이터베이스를 복원해야 합니다.

데이터베이스 목록을 봅니다

이 API를 실행하여 데이터베이스 목록을 볼 수 있습니다.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases' 다운로드하십시오

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest

응답

API가 정상적으로 실행되면 응답 코드 200이 출력된다.

예:

```
{
    "num_records": 3,
    "total_records": 3,
    "records": [
        {
            "id": "348901e5-aeaa-419f-88b1-80240de3b1fe",
            "name": "DB4",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "c79d33ab-7322-4ed6-92f5-51ad7a6944e0",
            "name": "DB5",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "40d6f35a-f4fb-48bc-8e0a-0ac93ddf0888",
            "name": "model",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.015625,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "System",
            "recovery_mode": "Full"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

MSSQL 데이터베이스를 복원 및 복구합니다

이 API를 실행하여 MSSQL 데이터베이스를 복원할 수 있습니다.

'POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore' 를 참조하십시오

여기서, _id_는 View 데이터베이스 API를 실행하여 얻은 MSSQL 데이터베이스 ID입니다. 자세한 내용은 을 참조하십시오 데이터베이스 목록을 봅니다.

자세한 내용은 다음을 참조하십시오. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest

이 API를 사용하면 BlueXP UI의 * Job Monitor * 탭에서 추적할 수 있는 작업이 생성됩니다.

매개 변수

이름	유형	필수 요소입니다
backup_id입니다	문자열	참
Overwrite_database(데이터베이스 덮어쓰기	불입니다	참
retain_replication_settings를 선택합니다	불입니다	거짓
recovery_mode(복구 모드	문자열 지원되는 3개의 문자열은 *Operational*, *Nonoperational* 및 _ReadOnly_입니다.	참
실행 취소_파일_디렉토리	문자열	참
restore_type 을 선택합니다	문자열	참

응답

API가 정상적으로 실행되면 응답 코드 202가 출력된다.

예:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

클라우드 네이티브 **Oracle** 데이터베이스 클론

클론 개념 및 요구 사항

NetApp ONTAP 또는 Cloud Volumes ONTAP용 Amazon FSx에 상주하는 Oracle 데이터베이스를 소스 데이터베이스 호스트 또는 대체 호스트에 데이터베이스 백업을 사용하여 복제할 수 있습니다. 운영 스토리지 시스템에서 백업을 클론 복제할 수 있습니다.

데이터베이스를 클론 복제하기 전에 클론 개념을 이해하고 모든 요구 사항이 충족되었는지 확인해야 합니다.

Oracle 데이터베이스 클론 생성 요구 사항

Oracle 데이터베이스를 복제하기 전에 필수 구성 요소가 완료되었는지 확인해야 합니다.

- 데이터베이스 백업을 만들어야 합니다. 클론 생성 작업을 성공적으로 수행하려면 온라인 데이터 및 로그 백업을 성공적으로 생성해야 합니다.
- ASM_diskstring 매개 변수에서 다음을 구성해야 합니다.
  - AFD: * ASMFD를 사용하는 경우
  - ORCL: * ASMlib를 사용하는 경우
  - /dev/<exact_device_location> ASMUDEV를 사용하는 경우
- 대체 호스트에서 클론을 생성하는 경우 대체 호스트는 다음 요구 사항을 충족해야 합니다.
  - 대체 호스트에 플러그인을 설치해야 합니다.
  - Oracle 소프트웨어는 대체 호스트에 설치해야 합니다.
  - iSCSI SAN 스토리지에 상주하는 데이터베이스를 클론 생성하는 경우 클론 호스트에서 스토리지에서 LUN을 검색할 수 있어야 합니다. 대체 호스트에 클론을 생성하는 경우 스토리지와 대체 호스트 간에 iSCSI 세션이 설정되었는지 확인합니다.
  - 소스 데이터베이스가 ASM 데이터베이스인 경우:
    - ASM 인스턴스는 클론이 수행될 호스트에서 실행 중이어야 합니다.
    - 클론 데이터베이스의 아카이브 로그 파일을 전용 ASM 디스크 그룹에 배치하려면 클론 작업 전에 ASM 디스크 그룹을 프로비저닝해야 합니다.

- 데이터 디스크 그룹의 이름은 구성할 수 있지만 클론이 수행될 호스트의 다른 ASM 디스크 그룹에서 해당 이름을 사용하지 않도록 해야 합니다.
- ASM 디스크 그룹에 상주하는 데이터 파일은 클론 워크플로우의 일부로 프로비저닝됩니다.

제한 사항

- Azure NetApp Files에 있는 데이터베이스의 복제는 지원되지 않습니다.
- Qtree에 상주하는 데이터베이스의 복제는 지원되지 않습니다.
- 복제된 데이터베이스 백업은 지원되지 않습니다.
- Amazon FSx for NetApp ONTAP에서 일일 자동 백업을 사용하는 경우, FSx가 복제된 볼륨에 백업을 생성했기 때문에 FSx for NetApp ONTAP의 복제된 볼륨을 BlueXP UI에서 삭제할 수 없습니다.
  FSx UI에서 볼륨에 대한 모든 백업을 삭제한 후 복제된 볼륨을 삭제한 다음 force 옵션을 사용하여 BlueXP UI에서 클론을 삭제해야 합니다.

복제 방법

기본 방법을 사용하거나 클론 사양 파일을 사용하여 클론을 생성할 수 있습니다.

기본 방법을 사용하여 클론을 생성합니다

소스 데이터베이스와 선택한 백업을 기반으로 기본 구성으로 클론을 생성할 수 있습니다.

- 데이터베이스 매개 변수, 홈 및 OS 사용자는 기본적으로 소스 데이터베이스를 사용합니다.
- 데이터 파일 경로는 선택한 명명 체계에 따라 이름이 지정됩니다.
- 사전 스크립트, 사후 스크립트 및 SQL 문을 지정할 수 없습니다.
- 복구 옵션은 기본적으로 취소까지 * 이며 * 복구를 위해 데이터 백업과 연결된 로그 백업을 사용합니다

사양 파일을 사용하여 클론을 생성합니다

클론 사양 파일에서 구성을 정의하고 이를 사용하여 데이터베이스를 복제할 수 있습니다. 사양 파일을 다운로드하여 요구 사항에 맞게 수정한 다음 파일을 업로드할 수 있습니다. "자세한 정보".

사양 파일에 정의되어 있고 수정할 수 있는 다양한 매개변수는 다음과 같습니다.

매개 변수	설명
control_files.(제어 파일	클론 데이터베이스에 대한 제어 파일의 위치입니다. 제어 파일 수는 소스 데이터베이스와 동일합니다. 제어 파일 경로를 재정의하려면 다른 제어 파일 경로를 제공할 수 있습니다. 파일 시스템 또는 ASM 디스크 그룹이 호스트에 있어야 합니다.

매개 변수	설명
REDO_LOGS 를 선택합니다	REDO 로그의 위치, 크기, REDO 그룹 수입니다. 데이터베이스를 복제하려면 최소 2개의 REDO 로그 그룹이 필요합니다. redo 로그 파일 경로를 재정의하려면 redo 로그 파일 경로를 소스 데이터베이스와 다른 파일 시스템으로 사용자 지정할 수 있습니다. 파일 시스템이나 ASM 디스크 그룹이 호스트에 있어야 합니다.
ORACLE_VERSION	타겟 호스트에 있는 Oracle의 버전입니다.
ORACLE_HOME	타겟 호스트의 Oracle Home입니다.
archive_log_mode를 활성화합니다	클론 데이터베이스의 아카이브 로그 모드를 제어합니다
database_parameters 를 선택합니다	복제된 데이터베이스에 대한 데이터베이스 매개 변수입니다
sql_statements 를 참조하십시오	클론 생성 후 데이터베이스에서 실행할 SQL 문입니다
OS_USER_DETAIL	타겟 클론 데이터베이스의 Oracle OS 사용자입니다
database_port 를 선택합니다	호스트에서 OS 인증이 비활성화된 경우 데이터베이스와 통신하는 데 사용되는 포트입니다.
ASM_PORT	create clone input에 자격 증명이 제공된 경우 ASM 데이터베이스와 통신하는 데 사용되는 포트입니다.
skip_recovery 를 선택합니다	복구 작업을 수행하지 않습니다.
SCN 까지	데이터베이스를 지정된 SCN(시스템 변경 번호)까지 복구합니다.
종료 시간	데이터베이스를 지정된 날짜 및 시간까지 복구합니다. 허용되는 형식은 _mm/dd/yyyy hh:mm:ss_입니다.
취소 시까지(_C)	클론 생성을 위해 선택한 데이터 백업과 연결된 로그 백업을 마운트하여 복구합니다. 로그 파일이 없거나 손상될 때까지 복제된 데이터베이스가 복구됩니다.
log_paths 를 참조하십시오	복제된 데이터베이스를 복구하는 데 사용할 아카이브 로그 경로의 추가 위치입니다.

매개 변수	설명
source_location을 선택합니다	소스 데이터베이스 호스트의 디스크 그룹 또는 마운트 지점의 위치입니다.
clone_location을 선택합니다	소스 위치에 해당하는 타겟 호스트에서 생성해야 하는 디스크 그룹 또는 마운트 지점의 위치입니다.
location_type을 입력합니다	ASM_diskgroup 또는 마운트 지점이 될 수 있습니다. 이 값은 파일을 다운로드할 때 자동으로 채워집니다. 이 매개 변수를 편집하면 안 됩니다.
pre_script(사전 스크립트)	클론을 생성하기 전에 타겟 호스트에서 실행할 스크립트입니다.
post_script 를 입력합니다	클론을 생성한 후 타겟 호스트에서 실행할 스크립트입니다.
경로	클론 호스트에 있는 스크립트의 절대 경로입니다. 스크립트는 /var/opt/snapcenter/spl/scripts 또는 이 경로 내의 폴더에 저장해야 합니다.
시간 초과	타겟 호스트에서 실행 중인 스크립트에 대해 지정된 시간 초과 시간입니다.
인수	스크립트에 지정된 인수입니다.

클론 명명 체계

클론 명명 체계는 클론 생성된 데이터베이스의 마운트 지점 및 디스크 그룹 이름을 정의합니다. 동일한 * 또는 * 자동 생성 * 을 선택할 수 있습니다.

동일한 명명 체계

클론 명명 체계를 * 동일 * 으로 선택하면 마운트 지점의 위치와 클론 생성된 데이터베이스의 디스크 그룹 이름이 소스 데이터베이스와 동일합니다.

예를 들어, 소스 데이터베이스의 마운트 지점이 _/NetApp_sourcedb/data_1, +Data1_DG_인 경우 클론 복제된 데이터베이스의 마운트 지점은 SAN의 NFS 및 ASM에 대해 동일하게 유지됩니다.

- 제어 파일 및 redo 파일의 수와 경로 같은 구성은 소스와 동일합니다.

> REDO 로그 또는 제어 파일 경로가 비 데이터 볼륨에 있는 경우 사용자는 ASM 디스크 그룹 또는 마운트 지점을 타겟 호스트에 프로비저닝해야 합니다.

- Oracle OS 사용자 및 Oracle 버전은 소스 데이터베이스와 동일합니다.

- 클론 스토리지 볼륨 이름은 sourceVolNameSCS_Clone_CurrentTimeStampNumber 형식으로 지정됩니다.

  예를 들어 소스 데이터베이스의 볼륨 이름이 _sourceVolName_인 경우 복제된 볼륨 이름은 _sourceVolNameSCS_Clone_1661420020304608825_가 됩니다.

  CurrentTimeStamNumber _ 는 볼륨 이름의 고유성을 제공합니다.

자동으로 생성된 명명 체계

클론 생성 스키마를 * Auto-Generated * 로 선택하면 마운트 지점의 위치와 클론 데이터베이스의 디스크 그룹 이름에 접미사가 추가됩니다.

- 기본 클론 방법을 선택한 경우 접미사가 * 클론 SID * 가 됩니다.
- 지정 파일 방법을 선택한 경우 접미사는 클론 사양 파일을 다운로드하는 동안 지정된 * 접미사 * 가 됩니다.

예를 들어 소스 데이터베이스의 마운트 지점이 _/netapp_sourcedb/data_1_이고 * 클론 SID * 또는 * 접미사 * 가 _HR_인 경우 복제된 데이터베이스의 마운트 지점은 _/netapp_sourcedb/data_1_HR_입니다.

- 제어 파일 및 redo 로그 파일 수는 소스와 동일합니다.
- 모든 REDO 로그 파일 및 제어 파일은 복제된 데이터 마운트 지점 중 하나 또는 데이터 ASM 디스크 그룹에 위치합니다.
- 클론 스토리지 볼륨 이름은 sourceVolNameSCS_Clone_CurrentTimeStampNumber 형식으로 지정됩니다.

  예를 들어 소스 데이터베이스의 볼륨 이름이 _sourceVolName_인 경우 복제된 볼륨 이름은 _sourceVolNameSCS_Clone_1661420020304608825_가 됩니다.

  CurrentTimeStamNumber _ 는 볼륨 이름의 고유성을 제공합니다.

- NAS 마운트 지점의 형식은 _SourceNASMountPoint_suffix_입니다.
- ASM 디스크 그룹의 형식은 _SourceDiskgroup_suffix_입니다.

  클론 diskgroup의 문자 수가 25보다 크면 _SC_hashcode_suffix_가 됩니다.

데이터베이스 매개 변수

다음 데이터베이스 매개 변수의 값은 클론 명명 체계와 관계없이 소스 데이터베이스의 값과 동일합니다.

- log_archive_format 을 참조하십시오
- audit_trail을 선택합니다
- 프로세스
- pga_aggregate_target 을 선택합니다
- remote_login_passwordfile 을 참조하십시오
- undo_tablespace 를 선택합니다
- open_cursors

- SGA_TARGET
- db_block_size를 입력합니다

다음 데이터베이스 매개 변수의 값은 클론 SID를 기반으로 접미사와 함께 추가됩니다.

- audit_file_dest={sourcedatabase_parametervalue}_suffix입니다
- log_archive_dest_1={sourcedatabase_oraclehome}_suffix

클론별 정의 정의 정의 지정 및 **PS**에 대해 지원되는 사전 정의된 환경 변수입니다

데이터베이스를 복제하는 동안 처방과 PS를 실행할 때 지원되는 미리 정의된 환경 변수를 사용할 수 있습니다.

- sc_original_SID는 소스 데이터베이스의 SID를 지정합니다. 이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다. 예: NFSB32
- sc_original_host는 소스 호스트의 이름을 지정합니다. 이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다. 예: asmrac1.gdl.englab.netapp.com
- SC_ORACLE_HOME은 대상 데이터베이스의 Oracle 홈 디렉토리 경로를 지정합니다. 예: /ora01/app/oracle/product/18.1.0/db_1
- sc_backup_name은 백업의 이름을 지정합니다. 이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다. 예:
  - 데이터베이스가 ARCHIVELOG 모드에서 실행되지 않는 경우: data@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - 데이터베이스가 ARCHIVELOG 모드에서 실행 중인 경우: data@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|log@RG2_scspr2417819002_07-20-2021_12.16.48.48.98.9267_1, RG2_12.919002_16.7_27_2267_2021-48.27_2267_207_2021
- sc_original_os_user 소스 데이터베이스의 운영 체제 소유자를 지정합니다. 예: Oracle
- sc_original_OS_group은 소스 데이터베이스의 운영 체제 그룹을 지정합니다. 예: oinstall
- SC_TARGET_SID는 복제된 데이터베이스의 SID를 지정합니다. PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다. 이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다. 예: clonedb
- SC_TARGET_HOST는 데이터베이스를 복제할 호스트의 이름을 지정합니다. 이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다. 예: asmrac1.gdl.englab.netapp.com
- SC_TARGET_OS_USER는 복제된 데이터베이스의 운영 체제 소유자를 지정합니다. PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다. 예: Oracle
- SC_TARGET_OS_GROUP은 복제된 데이터베이스의 운영 체제 그룹을 지정합니다. PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다. 예: oinstall
- SC_TARGET_DB_PORT는 복제된 데이터베이스의 데이터베이스 포트를 지정합니다. PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다. 예: 1521

지원되는 구분 기호

- @는 데이터를 데이터베이스 이름과 분리하고 값을 키와 분리하는 데 사용됩니다. 예: data@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- 는 SC_BACKUP_NAME 매개 변수에 대해 서로 다른 두 엔터티 간에 데이터를 분리하는 데 사용됩니다. 예: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- , 은 같은 키에 대한 변수 집합을 구분하는 데 사용됩니다. 예: data@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 | log@RG2_scspr2417819002_07-20-2021_12.16.4267_1, RG2_scprsprs2417819002_07-21-21-2021_12.48.9267_1, squ2287_2407_2407_2427_2407_24222_242267_42.722_242267_1

클라우드 네이티브 **Oracle** 데이터베이스 클론

NetApp ONTAP 또는 Cloud Volumes ONTAP용 Amazon FSx에 상주하는 Oracle 데이터베이스를 소스 데이터베이스 호스트 또는 대체 호스트에 데이터베이스 백업을 사용하여 복제할 수 있습니다.

다음과 같은 이유로 데이터베이스를 복제할 수 있습니다.

- 응용 프로그램 개발 주기 동안 현재 데이터베이스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면 다음을 수행합니다.
- 데이터 추출 및 조작 도구를 사용하여 데이터 웨어하우스를 채웁니다.
- 실수로 삭제 또는 변경된 데이터를 복구합니다.

시작하기 전에

클론 개념을 이해하고 모든 요구 사항이 충족되는지 확인해야 합니다. "자세한 정보".

단계

1. 을 클릭합니다 ••• 복제할 데이터베이스에 해당하는 을 클릭하고 * 세부 정보 보기 * 를 클릭합니다.
2. 을 클릭합니다 ••• 데이터 백업에 해당하고 * Clone * 을 클릭합니다.
3. 클론 세부 정보 페이지에서 클론 옵션 중 하나를 선택합니다.
4. 선택한 옵션에 따라 다음 작업을 수행합니다.

다음을 선택한 경우...	수행할 작업...
• 기본 *	a. 클론 호스트를 선택합니다. 대체 호스트에서 클론을 생성하려면 소스 데이터베이스 호스트의 버전과 Oracle 및 OS 버전이 동일한 호스트를 선택합니다. b. 클론의 SID를 지정합니다. c. 클론 명명 스키마를 선택합니다. 데이터베이스가 소스 호스트에 클론 생성된 경우 클론 명명 체계가 자동으로 생성됩니다. 데이터베이스가 대체 호스트에 클론 복제되면 클론 명명 체계가 동일합니다. d. Oracle 홈 경로를 지정합니다. e. (선택 사항) 데이터베이스 자격 증명을 지정합니다. ◦ 데이터베이스 자격 증명: OS 사용자 인증이 비활성화된 경우 시스템 사용자가 동일한 호스트 또는 대상 호스트의 복제된 데이터베이스에 연결할 수 있도록 암호를 제공해야 합니다. ◦ ASM 자격 증명: 대상 호스트에서 OS 사용자 인증을 사용하지 않도록 설정한 경우 sysasm 권한이 있는 사용자의 자격 증명을 제공하여 타겟 호스트의 ASM 인스턴스에 연결해야 합니다. ⓘ 수신기가 타겟 호스트에서 실행 중인지 확인합니다. f. 다음 * 을 클릭합니다. g. 클론 * 을 클릭합니다.

다음을 선택한 경우...	수행할 작업...
• 규격 파일 *	a. 사양 파일을 다운로드하려면 * 파일 다운로드 * 를 클릭합니다. b. 클론 명명 스키마를 선택합니다. 자동 생성 * 을 선택한 경우 접미사를 지정해야 합니다. c. 요구 사항에 따라 사양 파일을 편집하고 * 찾아보기 * 버튼을 클릭하여 업로드하십시오. d. 클론 호스트를 선택합니다. 대체 호스트에서 클론을 생성하려면 소스 데이터베이스 호스트의 버전과 Oracle 및 OS 버전이 동일한 호스트를 선택합니다. e. 클론의 SID를 지정합니다. f. (선택 사항) 데이터베이스 자격 증명을 지정합니다. ◦ 데이터베이스 자격 증명: OS 사용자 인증이 비활성화된 경우 시스템 사용자가 동일한 호스트 또는 대상 호스트의 복제된 데이터베이스에 연결할 수 있도록 암호를 제공해야 합니다. ◦ ASM 자격 증명: 대상 호스트에서 OS 사용자 인증을 사용하지 않도록 설정한 경우 sysasm 권한이 있는 사용자의 자격 증명을 제공하여 타겟 호스트의 ASM 인스턴스에 연결해야 합니다. ⓘ 수신기가 타겟 호스트에서 실행 중인지 확인합니다. g. 다음 * 을 클릭합니다. h. 클론 * 을 클릭합니다.

5. 을 클릭합니다 + Filter by * 옆의 * Clone options * > * Clones * 를 선택하여 클론을 봅니다.

SAP HANA 타겟 시스템을 업데이트하세요

SAP HANA 소스 시스템의 데이터로 SAP HANA 타겟 시스템을 업데이트할 수 있습니다. 현재 운영 데이터를 테스트 시스템에 제공하는 데 사용할 수 있습니다. BlueXP 백업 및 복구를 사용하면 소스 시스템에서 스냅샷 복사본을 선택하고 스냅샷 복사본을 기반으로 새 Azure NetApp Files 볼륨을 생성할 수 있습니다. 예제 스크립트를 사용할 수 있습니다. 이 스크립트는 데이터베이스 호스트에서 SAP HANA 데이터베이스를 복구하는 데 필요한 작업을 실행합니다.

- 시작하기 전에 *
- 첫 번째 업데이트 작업을 실행하기 전에 SAP HANA 타겟 시스템을 설치해야 합니다.
- 소스 및 타겟 HANA 시스템을 BlueXP 백업 및 복구에 수동으로 추가해야 합니다.
- 소스 및 타겟 시스템에서 SAP HANA 데이터베이스 버전이 동일한지 확인합니다.
- 사용할 업데이트 스크립트를 결정해야 합니다. 새로 고침 스크립트는 솔루션 기술 보고서에서 사용할 수 있습니다.

  "자동화 스크립트 예"

  새로 고침 스크립트를 사용자 지정할 수 있습니다.

- 다음 환경 변수는 처방과 PS의 일부로 사용할 수 있습니다.
  - Cloned_volumes_mount_path 를 참조하십시오
  - <SOURCEVOLUME>_destination을 선택합니다
  - hana_database_type을 선택합니다
  - tenant_database_name입니다
- 플러그인을 3.0 버전으로 업그레이드해야 합니다.
- 마운트 경로는 소스 및 타겟 SAP HANA 시스템의 데이터 볼륨에 대해 동일해야 합니다.
- 첫 번째 새로 고침 작업을 수행하기 전에 '/etc/fstab' 파일에 타겟 SAP HANA 시스템의 데이터 볼륨에 대한 항목이 없는지 확인하십시오.
- 이 작업에 대한 정보 *
- 시스템 새로 고침은 멀티 테넌트 데이터베이스 컨테이너 HANA 시스템에 대해서만 지원됩니다.
- 기존 정책은 시스템 새로 고침 후 유효합니다.
- 생성된 새 볼륨에는 <sourcevolumename>-<timestamp> 명명 규칙이 적용됩니다
  - 타임스탬프 형식: <year> <month> <day>-<hour> <minute> <second>

    예를 들어 소스 볼륨이 vol1인 경우 업데이트된 볼륨 이름은 vol1-20230109-184501이 됩니다

> 새 볼륨은 타겟 볼륨과 동일한 용량 풀에 배치됩니다.

- 접합 경로는 볼륨 이름과 동일합니다.
- 새 볼륨의 "최대 처리량 수"는 수동 QoS(서비스 품질) 용량 풀이 있는 대상 시스템의 볼륨에서 선택됩니다. 자동 QoS 용량 풀의 경우 처리량은 소스 볼륨의 용량으로 정의됩니다.
- 시스템 새로 고침 중에 볼륨의 자동 마운트 및 마운트 해제는 스크립트 대신 워크플로우를 사용하여 수행됩니다.
- 단계 *
  1. BlueXP UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
  2. 응용 프로그램 * 페이지에서 을 클릭합니다 ••• 아이콘을 클릭하여 새로 고칠 시스템에 해당하는 작업을 선택하고 * 시스템 새로 고침 * 을 선택합니다.
  3. 시스템 새로 고침 * 페이지에서 다음 작업을 수행합니다.
     a. 소스 시스템 및 스냅샷 복사본을 선택합니다.

b. (선택 사항) 새 볼륨에 액세스할 수 있는 내보내기 주소를 입력합니다.

c. (선택 사항) 최대 스토리지 처리량(MIB)을 입력합니다.

d. ppt, postscript 및 on failure 스크립트 경로를 입력합니다. On failure 스크립트는 시스템 새로 고침 작업이 실패한 경우에만 실행됩니다.

e. 새로 고침 * 을 클릭합니다.

클라우드 네이티브 애플리케이션 데이터 보호 관리

작업을 모니터링합니다

작업 환경에서 시작된 작업의 상태를 모니터링할 수 있습니다. 이렇게 하면 성공적으로 완료된 작업, 현재 진행 중인 작업 및 실패한 작업을 볼 수 있으므로 문제를 진단하고 해결할 수 있습니다.

> 예약된 작업은 작업 완료 시간에서 최대 5분이 지연되면 BlueXP 작업 모니터 페이지에 표시됩니다.

자세한 내용은 을 참조하십시오 "작업 상태를 모니터링합니다".

Oracle 데이터베이스 호스트의 유지 관리

관리자는 데이터베이스 호스트를 유지 관리 모드로 수동으로 전환하여 호스트에 대한 유지 보수 작업을 수행할 수 있습니다. 업그레이드하는 동안 호스트는 자동으로 유지 관리 모드로 전환되고 업그레이드 후에는 호스트가 운영 모드로 자동 전환됩니다.

호스트를 유지 관리 모드로 전환하면 주문형 작업이 실패하고 예약된 작업이 생략됩니다.

> 호스트를 유지 관리 모드로 전환하기 전에 호스트의 리소스에 대해 실행 중인 작업이 있는지 확인할 수 없습니다.

단계

1. BlueXP UI에서 * 보호 * > * 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다
2. 애플리케이션 유형으로 * Oracle * 을 선택합니다.
3. 설정 * > * 호스트 * 를 클릭합니다.
4. 다음 작업 중 하나를 수행합니다.

만약...	수행할 작업...
호스트를 유지 관리 모드로 전환하려고 합니다	을 클릭합니다 ••• 호스트에 해당 * Enable maintenance mode * 를 선택합니다.
호스트를 유지 관리 모드에서 나오려고 합니다	을 클릭합니다 ••• 유지 보수 중인 호스트에 대해 * Disable maintenance mode * 를 선택합니다.

감사 데이터

API를 직접 실행하거나 UI를 사용하여 BlueXP 백업 및 복구 애플리케이션의 외부에서 노출된 API를 호출할 경우 헤더, 역할, 요청 본문 등의 요청 세부 정보가 API 정보는 BlueXP 타임라인에 기록되고 감사 항목은 타임라인에 영구적으로 유지됩니다. API 호출의 상태 및 오류 응답도 작업 완료 후 감사합니다. 작업과 같은 비동기 API 응답의 경우 작업 ID도 응답의 일부로 기록됩니다.

애플리케이션의 BlueXP 백업 및 복구는 호스트 IP, 요청 본문, 작업 이름, 트리거된 항목, 일부 헤더, API의 작동 상태를 확인할 수 있습니다.

백업 세부 정보를 봅니다

생성된 총 백업 수, 백업 생성에 사용되는 정책, 데이터베이스 버전 및 에이전트 ID를 볼 수 있습니다.

단계

1. 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다.
2. 을 클릭합니다 ••• 해당 응용 프로그램에 대해 * 세부 정보 보기 * 를 클릭합니다.

> 상담원 ID는 커넥터에 연결됩니다. SAP HANA 호스트를 등록하는 동안 사용된 커넥터가 더 이상 존재하지 않으면 새 Connector의 에이전트 ID가 다르기 때문에 해당 애플리케이션의 후속 백업이 실패합니다. 호스트에서 커넥터 ID를 수정해야 합니다. 자세한 내용은 을 참조하십시오 커넥터 세부 정보를 업데이트합니다.

클론을 삭제합니다

더 이상 필요하지 않은 경우 클론을 삭제할 수 있습니다.

단계

1. 을 클릭합니다 + Filter by * 옆에 * Clone options * > * Clone Parents * 를 선택합니다.
2. 을 클릭합니다 ••• 해당 응용 프로그램에 대해 * 세부 정보 보기 * 를 클릭합니다.
3. 데이터베이스 세부 정보 페이지에서 을 클릭합니다 + Filter by * 옆의 * Clone * 을 선택합니다.
4. 을 클릭합니다 ••• 삭제할 클론에 대해 * Delete * 를 클릭합니다.
5. (선택 사항) * 강제 삭제 * 확인란을 선택합니다.

커넥터 세부 정보를 업데이트합니다

애플리케이션 호스트를 등록하는 동안 사용된 커넥터가 더 이상 존재하지 않거나 손상된 경우 새 커넥터를 배포해야 합니다. 새 커넥터를 배포한 후에는 * connector-update * API를 실행하여 이전 커넥터를 사용하여 등록된 모든 호스트의 커넥터 세부 정보를 업데이트해야 합니다.

Oracle 또는 SAP HANA 호스트에 대한 커넥터 세부 정보를 업데이트한 후 다음을 수행하여 커넥터 세부 정보가 성공적으로 업데이트되었는지 확인하십시오.

단계

1. BlueXP Connector VM에 로그인하고 다음 단계를 수행하십시오.

a. Connector에서 아래 명령을 실행하여 커넥터에서 플러그인에 연결할 수 있는지 확인합니다.
```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/getVersion
--cert/config/client/certificate/certificate.pem
--key/config/client/certificate/key.pem
```

b. 기본 마운트 경로를 가져옵니다. 'SUDO Docker 볼륨 ls | grep scs_cloud_volume | awk {'print$2'} | xargs sudo Docker 볼륨 검사 | grep mountpoint'

c. 플러그인 호스트의 _/var/opt/snapcenter/spl/etc/_에 커넥터 VM의 _<base_mount_path>/client/certificate/_path 에서 certificate.pem을 복사합니다.

2. 플러그인 호스트에 로그인하고 다음 단계를 수행하십시오.

a. /var/opt/snapcenter/spl/etc_로 이동한 후 keytool 명령을 실행하여 certificate.pem 파일을 가져옵니다.
```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
```

b. SPL을 다시 시작합니다:'stemctl restart SPL'

c. 다음 중 하나를 수행합니다.

현재 사용 중인 경우...	수행할 작업...
Oracle 데이터베이스 호스트	i. 를 모두 확인하십시오 "필수 구성 요소" 충족됩니다. ii. 백업 및 복구 * > * 응용 프로그램 * 을 클릭합니다 iii. 을 클릭합니다 ••• 해당 응용 프로그램에 대해 * 세부 정보 보기 * 를 클릭합니다. iv. 커넥터 ID * 를 수정합니다.

현재 사용 중인 경우...	수행할 작업...
SAP HANA 데이터베이스 호스트	i. 를 모두 확인하십시오 "필수 구성 요소" 충족됩니다. ii. 다음 명령을 실행합니다. `curl --location --request PATCH 'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \ --header 'x-account-id: <CM account-id>' \ --header 'Authorization: Bearer token' \ --header 'Content-Type: application/json' \ --data-raw '{ "old_connector_id": "Old connector id that no longer exists", "new_connector_id": "New connector Id"}'` 모든 호스트에 SAP HANA용 SnapCenter 플러그인이 설치되어 실행 중이며 새 커넥터에서 모두 연결할 수 있는 경우 커넥터 세부 정보가 성공적으로 업데이트됩니다.

CA 서명 인증서를 구성합니다

환경에 추가 보안을 포함하려는 경우 CA 서명 인증서를 구성할 수 있습니다.

BlueXP Connector에 CA 서명 인증서를 구성합니다

커넥터는 자체 서명된 인증서를 사용하여 플러그인과 통신합니다. 자체 서명된 인증서는 설치 스크립트에 의해 키 저장소로 가져옵니다. 다음 단계를 수행하여 자체 서명된 인증서를 CA 서명 인증서로 바꿀 수 있습니다.

단계

1. Connector가 플러그인과 연결할 때 CA 인증서를 클라이언트 인증서로 사용하려면 Connector에서 다음 단계를 수행하십시오.
   a. Connector에 로그인합니다.
   b. 다음 명령을 실행하여 _<base_mount_path>_를 가져옵니다.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

c. 커넥터의 _<base_mount_path>/client/certificate_에 있는 기존 파일을 모두 삭제합니다.

d. CA 서명 인증서와 키 파일을 커넥터의 _<base_mount_path>/client/certificate_에 복사합니다.

   파일 이름은 certificate.pem 및 key.pem 이어야 합니다. certificate.pem에는 중간 CA 및 루트 CA와 같은 전체 인증서 체인이 있어야 합니다.

e. name certificate.p12를 사용하여 인증서의 PKCS12 형식을 생성하고 _<base_mount_path>/client/certificate_에 유지합니다.

   예: openssl pkcs12-inkey key.pem-in certificate.pem-export-out certificate.p12

2. 플러그인 호스트에서 다음 단계를 수행하여 Connector에서 보낸 인증서의 유효성을 확인합니다.

   a. 플러그인 호스트에 로그인합니다.

   b. Connector에서 모든 중간 CA 및 루트 CA에 대한 certificate.pem 및 인증서를 _/var/opt/snapcenter/spl/etc/_의 플러그인 호스트로 복사합니다.

      중간 CA 및 루트 CA 인증서의 형식은 .crt 형식이어야 합니다.

   c. /var/opt/snapcenter/spl/etc_로 이동한 후 keytool 명령을 실행하여 certificate.pem 파일을 가져옵니다.
      ```
      keytool -import -alias agentcert -file certificate.pem -keystore
      keystore.jks -deststorepass snapcenter -noprompt
      ```

   d. 루트 CA 및 중간 인증서를 가져옵니다. 키 도구-가져오기-trustcacerts-keystore keystore.jks-storepass SnapCenter-alias trustedca-file<certificate.crt>

      certificate.crt는 루트 CA 및 중간 CA의 인증서를 나타냅니다.

   e. SPL을 다시 시작합니다:'stemctl restart SPL'

플러그인에 대해 **CA** 서명 인증서를 구성합니다

CA 인증서의 이름은 플러그인 호스트의 Cloud Backup에 등록된 이름과 같아야 합니다.

단계

1. 플러그인 호스트에서 다음 단계를 수행하여 CA 인증서를 사용하여 플러그인을 호스트합니다.

   a. SPL의 keystore_/var/opt/snapcenter/SPL/etc_가 포함된 폴더로 이동합니다.

   b. alias_splkeystore_로 인증서와 키를 모두 포함하는 인증서의 PKCS12 형식을 만듭니다.

      certificate.pem에는 중간 CA 및 루트 CA와 같은 전체 인증서 체인이 있어야 합니다.

   예: openssl pkcs12-inkey key.pem-in certificate.pem-export-out certificate.p12-name splkeystore

   a. 위의 단계에서 만든 CA 인증서를 추가합니다.
      ```
      keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12
      -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
      -destalias splkeystore -noprompt
      ```

   b. 인증서를 확인합니다. 키툴-리스트-v-keystore keystore.jks

c. SPL을 다시 시작합니다:'stemctl restart SPL'

2. Connector가 플러그인의 인증서를 확인할 수 있도록 Connector에서 다음 단계를 수행합니다.

   a. 커넥터 에 비 루트 사용자로 로그인합니다.

   b. 다음 명령을 실행하여 _<base_mount_path>_를 가져옵니다.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
   sudo docker volume inspect | grep Mountpoint
   ```

   c. 서버 디렉터리 아래에 루트 CA 및 중간 CA 파일을 복사합니다.
   ```
   cd <base_mount_path>
   mkdir server
   ```

   CA 파일은 PEM 형식이어야 합니다.

   d. cloudmanager_scs_cloud에 연결하고 _config.yml_에서 * enableCACert * 를 * true * 로 수정합니다. 'SUDO Docker Exec - cloudmanager_SCS_cloud SED-I's/enableCACert: false/enableCACert: true/g'/opt/NetApp/cloudmanager-SCS-cloud/config/config.yml'

   e. cloudmanager_scs_cloud 컨테이너를 다시 시작합니다. 'SUDO Docker restart cloudmanager_scs_cloud'를 선택합니다

REST API 액세스

애플리케이션을 클라우드로 보호하는 REST API는 다음 사이트에서 확인할 수 있습니다. https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/.

REST API에 액세스하려면 통합 인증이 있는 사용자 토큰을 얻어야 합니다. 사용자 토큰을 얻는 방법에 대한 자세한 내용은 을 참조하십시오 "통합 인증을 사용하여 사용자 토큰을 생성합니다".

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.