시작 개요

NetApp Solutions

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html on April 20, 2024. Always check docs.netapp.com for the latest.

목차

시작 개요 1
온프레미스 1
설치하고 1
온프레미스에서 시작합니다 1
AWS 퍼블릭 클라우드 시작하기 54

시작 개요

이 섹션에서는 이전 섹션에서 설명한 사전 요구 사항을 충족하기 위해 완료해야 하는 작업을 요약합니다. 다음 섹션에서는 사내 및 퍼블릭 클라우드 운영에 모두 필요한 개략적인 작업 목록을 제공합니다. 자세한 프로세스와 절차는 관련 링크를 클릭하여 액세스할 수 있습니다.

온프레미스

- SnapCenter에서 데이터베이스 관리자 사용자를 설정합니다
- SnapCenter 플러그인 설치 필수 구성 요소
- SnapCenter 호스트 플러그인 설치
- DB 리소스 검색
- 스토리지 클러스터 피어링 및 DB 볼륨 복제를 설정합니다
- SnapCenter에 CVO 데이터베이스 스토리지 SVM 추가
- SnapCenter에서 데이터베이스 백업 정책을 설정합니다
- 백업 정책을 구현하여 데이터베이스를 보호합니다
- 백업을 검증합니다

설치하고

- 사전 항공편 확인
- AWS에서 Cloud Manager 및 Cloud Volumes ONTAP를 구축하는 단계
- 데이터베이스 워크로드를 위한 EC2 컴퓨팅 인스턴스 구축

자세한 내용을 보려면 다음 링크를 클릭하십시오.

"온프레미스", "퍼블릭 클라우드 - AWS"

온프레미스에서 시작합니다

NetApp SnapCenter 툴은 RBAC(역할 기반 액세스 제어)를 사용하여 사용자 리소스 액세스 및 권한 부여를 관리하고 SnapCenter 설치를 통해 미리 채워진 역할을 생성합니다. 필요에 따라 사용자 지정 역할을 만들 수도 있습니다.

온프레미스

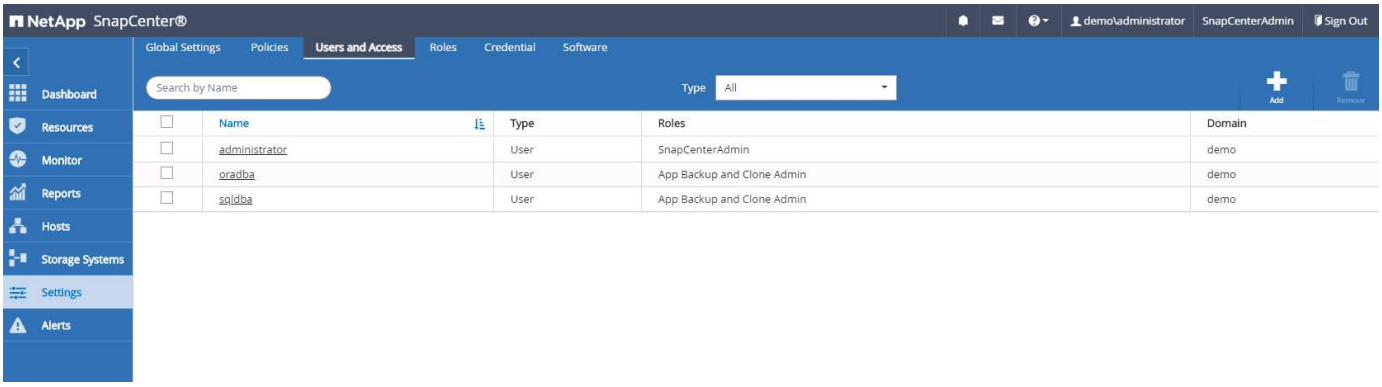
SnapCenter에서 데이터베이스 관리자 설정

데이터베이스 백업, 복원 및/또는 재해 복구를 위해 SnapCenter에서 지원하는 각 데이터베이스 플랫폼에 대해 전용 관리 사용자 ID를 갖는 것이 적합합니다. 단일 ID를 사용하여 모든 데이터베이스를 관리할 수도 있습니다. 테스트 사례 및 데모에서는 Oracle과 SQL Server 모두에 대해 각각 전용 관리 사용자를 생성했습니다.

특정 SnapCenter 리소스는 SnapCenter 관리자 역할만 사용하여 프로비저닝할 수 있습니다. 그러면 액세스를 위해 리소스를 다른 사용자 ID에 할당할 수 있습니다.

사전 설치 및 구성된 사내 SnapCenter 환경에서는 다음 작업이 이미 완료되었을 수 있습니다. 그렇지 않은 경우 다음 단계에 따라 데이터베이스 관리자 사용자를 생성합니다.

1. Windows Active Directory에 관리자 사용자를 추가합니다.
2. SnapCenter CenterAdmin 역할로 부여된 ID를 사용하여 로그인합니다.
3. 설정 및 사용자 아래의 액세스 탭으로 이동하고 추가 를 클릭하여 새 사용자를 추가합니다. 새 사용자 ID는 1단계에서 Windows Active Directory에서 만든 관리자 사용자에게 연결됩니다. . 필요에 따라 사용자에게 적절한 역할을 할당합니다. 필요에 따라 admin 사용자에게 리소스를 할당합니다.



2.SnapCenter 플러그인 설치 필수 구성 요소입니다

SnapCenter는 DB 호스트에서 실행 중인 플러그인 에이전트를 사용하여 백업, 복구, 클론 및 기타 기능을 수행합니다. 플러그인 설치 및 기타 관리 기능을 위해 설정 및 자격 증명 탭에서 구성된 자격 증명을 통해 데이터베이스 호스트 및 데이터베이스에 연결합니다. Linux 또는 Windows와 같은 타겟 호스트 유형과 데이터베이스 유형에 따른 특정 권한 요구 사항이 있습니다.

SnapCenter 플러그인 설치 전에 DB 호스트 자격 증명을 구성해야 합니다. 일반적으로 플러그인 설치를 위한 호스트 연결 자격 증명으로 DB 호스트의 관리자 사용자 계정을 사용합니다. 또한 OS 기반 인증을 사용하여 데이터베이스 액세스에 동일한 사용자 ID를 부여할 수도 있습니다. 반면, DB 관리 액세스를 위해 서로 다른 데이터베이스 사용자 ID를 사용하여 데이터베이스 인증을 사용할 수도 있습니다. OS 기반 인증을 사용하기로 결정한 경우 OS 관리자 사용자 ID에 DB 액세스 권한이 부여되어야 합니다. Windows 도메인 기반 SQL Server 설치의 경우 도메인 관리자 계정을 사용하여 도메인 내의 모든 SQL Server를 관리할 수 있습니다.

SQL Server용 Windows 호스트:

1. 인증에 Windows 자격 증명을 사용하는 경우 플러그인을 설치하기 전에 자격 증명을 설정해야 합니다.
2. 인증에 SQL Server 인스턴스를 사용하는 경우 플러그인을 설치한 후 자격 증명을 추가해야 합니다.
3. 자격 증명을 설정하는 동안 SQL 인증을 사용하도록 설정한 경우 검색된 인스턴스 또는 데이터베이스에 빨간색 잠금 아이콘이 표시됩니다. 잠금 아이콘이 나타나면 인스턴스 또는 데이터베이스 자격 증명을 지정하여 인스턴스 또는 데이터베이스를 리소스 그룹에 성공적으로 추가해야 합니다.
4. 다음 조건이 충족될 경우 sysadmin 액세스 없이 RBAC 사용자에게 자격 증명을 할당해야 합니다.
    - 자격 증명이 SQL 인스턴스에 할당됩니다.
    - SQL 인스턴스 또는 호스트는 RBAC 사용자에게 할당됩니다.
    - RBAC DB 관리자 사용자에게는 리소스 그룹과 백업 권한이 모두 있어야 합니다.

Oracle용 UNIX 호스트:

1. sshd.conf를 편집하고 sshd 서비스를 다시 시작하여 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다. AWS 인스턴스의 암호 기반 SSH 인증은 기본적으로 해제되어 있습니다.
2. 비루트 사용자에 대한 sudo 권한을 구성하여 플러그인 프로세스를 설치 및 시작합니다. 플러그인을 설치하면 프로세스가 효과적인 루트 사용자로 실행됩니다.
3. 설치 사용자에 대한 Linux 인증 모드를 사용하여 자격 증명을 생성합니다.
4. Linux 호스트에 Java 1.8.x(64비트)를 설치해야 합니다.
5. Oracle 데이터베이스 플러그인을 설치하면 Unix용 SnapCenter 플러그인도 설치됩니다.

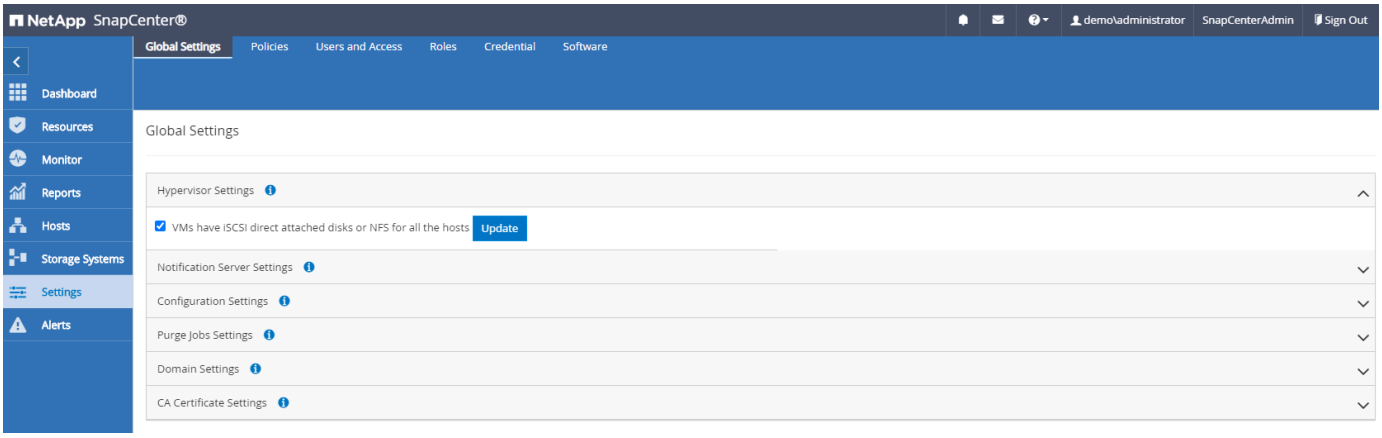
3.SnapCenter 호스트 플러그인 설치

> 클라우드 DB 서버 인스턴스에 SnapCenter 플러그인을 설치하기 전에 컴퓨팅 인스턴스 구축을 위한 관련 클라우드 섹션에 나와 있는 대로 모든 구성 단계를 완료해야 합니다.

다음 단계에서는 SnapCenter 플러그인이 호스트에 설치되어 있는 동안 데이터베이스 호스트를 SnapCenter에 추가하는 방법을 보여 줍니다. 이 절차는 사내 호스트와 클라우드 호스트를 모두 추가하는 데 적용됩니다. 다음 데모에서는 AWS에 상주하는 Windows 또는 Linux 호스트를 추가합니다.

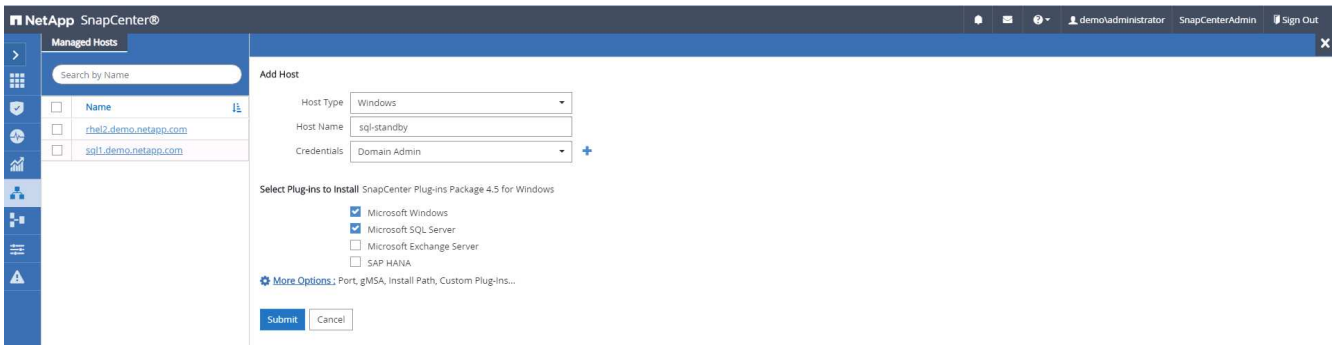
SnapCenter VMware 글로벌 설정을 구성합니다

설정 > 전역 설정 으로 이동합니다. 하이퍼바이저 설정 에서 "VM에 모든 호스트에 대한 iSCSI 직접 연결 디스크 또는 NFS가 있음"을 선택하고 업데이트 를 클릭합니다.



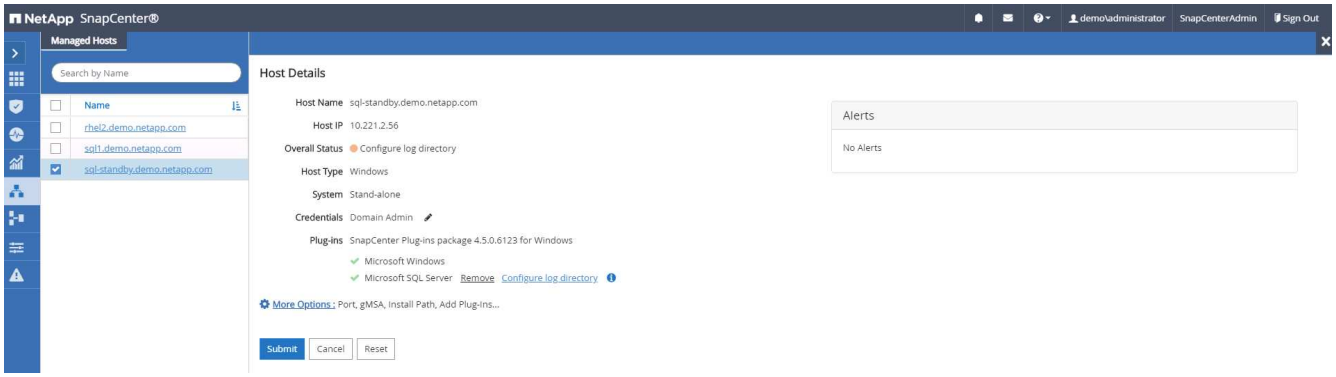
호스트에 Windows 호스트 및 플러그인 설치를 추가합니다

1. SnapCenter에 SnapCenterAdmin 권한으로 사용자 ID를 사용하여 로그인합니다.
2. 왼쪽 메뉴에서 호스트 탭을 클릭한 다음 추가를 클릭하여 호스트 추가 워크플로우를 엽니다.
3. 호스트 유형에 Windows를 선택합니다. 호스트 이름은 호스트 이름 또는 IP 주소일 수 있습니다. 호스트 이름은 SnapCenter 호스트에서 올바른 호스트 IP 주소로 확인되어야 합니다. 2단계에서 생성한 호스트 자격 증명을 선택합니다. 설치할 플러그인 패키지로 Microsoft Windows 및 Microsoft SQL Server를 선택합니다.

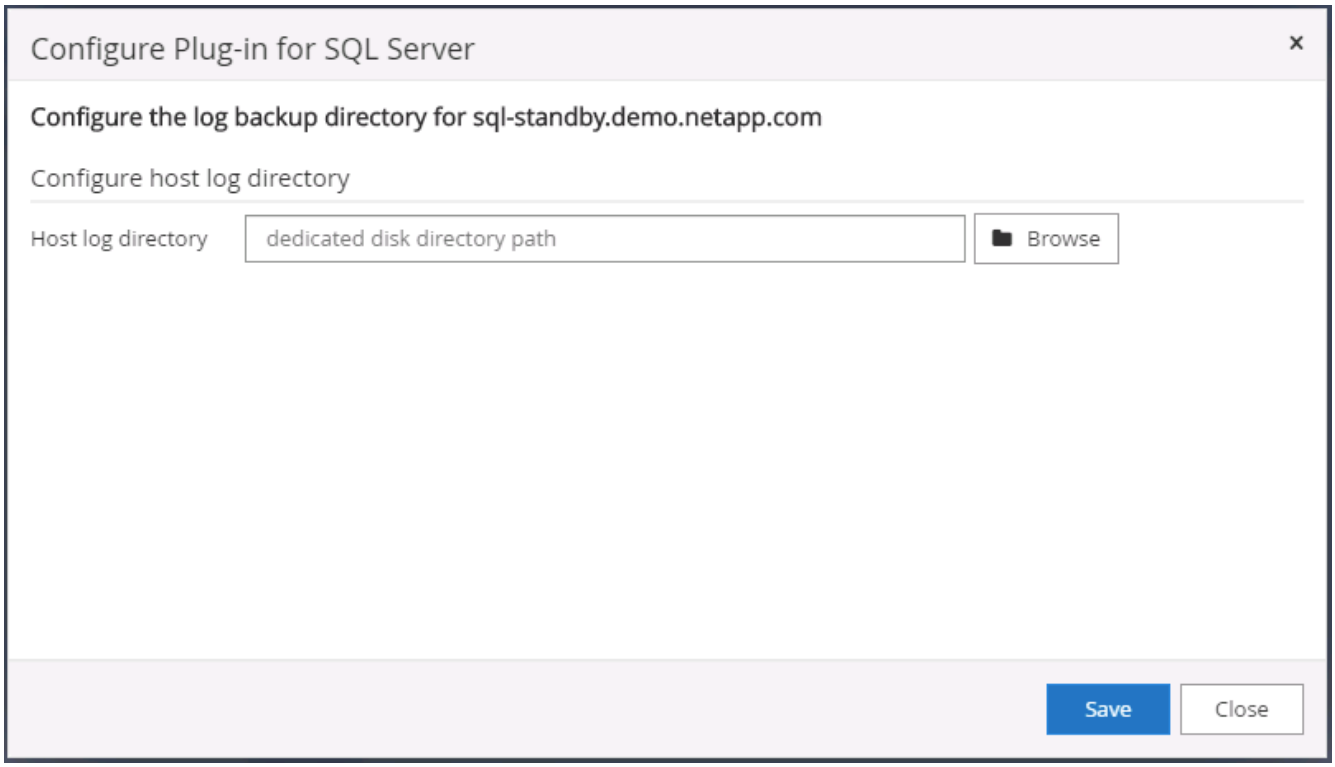


4. Windows 호스트에 플러그인을 설치하면 전체 상태가 "Configure log directory"로 표시됩니다.

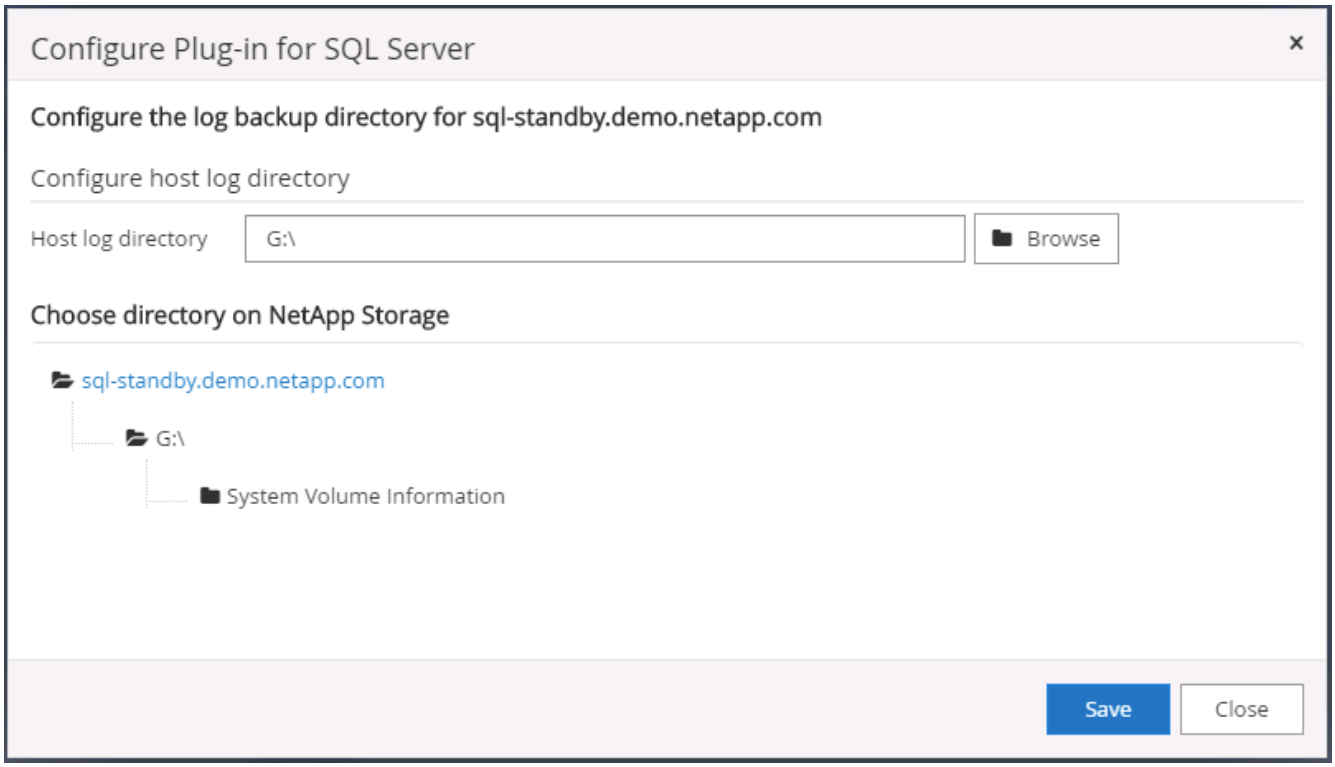
5. 호스트 이름을 클릭하여 SQL Server 로그 디렉토리 구성을 엽니다.



6. "로그 디렉토리 구성"을 클릭하여 "SQL Server용 플러그인 구성"을 엽니다.

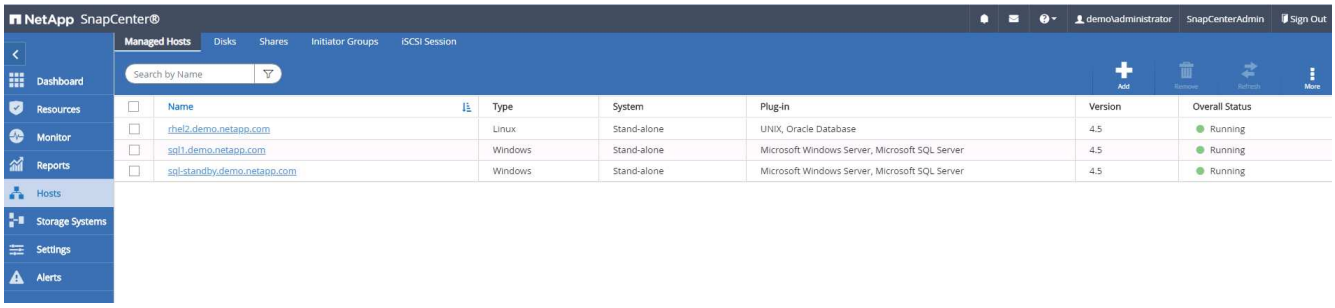


7. 찾아보기 를 클릭하여 로그 디렉토리를 설정할 수 있도록 NetApp 스토리지를 검색합니다. SnapCenter는 이 로그 디렉토리를 사용하여 SQL Server 트랜잭션 로그 파일을 롤업합니다. 저장을 클릭합니다.

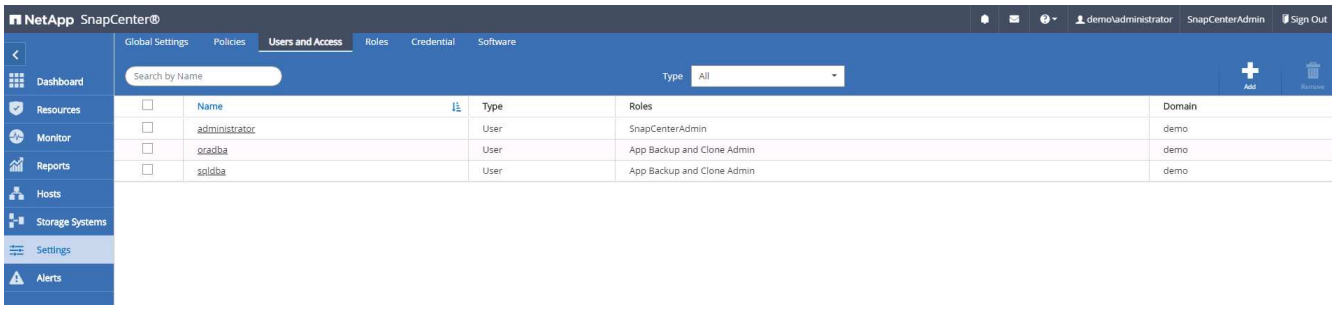


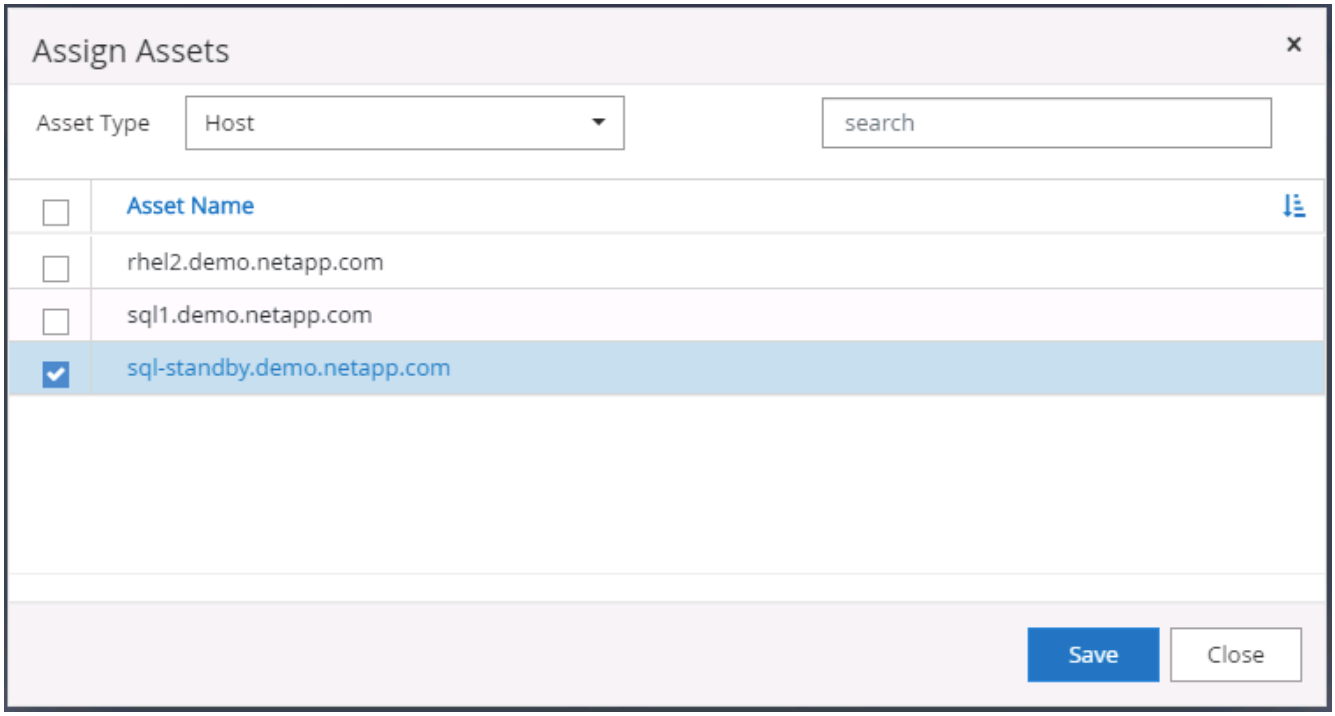
DB 호스트에 프로비저닝된 NetApp 스토리지의 경우 CVO의 6단계에 나와 있는 것처럼 SnapCenter에 스토리지(온프레미스 또는 CVO)를 추가해야 합니다.

8. 로그 디렉토리가 구성된 후 Windows 호스트 플러그인 전체 상태가 실행 중 으로 변경됩니다.



9. 데이터베이스를 관리하는 사용자 ID에 호스트를 할당하려면 설정 및 사용자 아래의 액세스 탭으로 이동하고 데이터베이스 관리 사용자 ID(호스트를 할당해야 하는 sqlldba인 경우)를 클릭한 다음 저장 을 클릭하여 호스트 리소스 할당을 완료합니다.

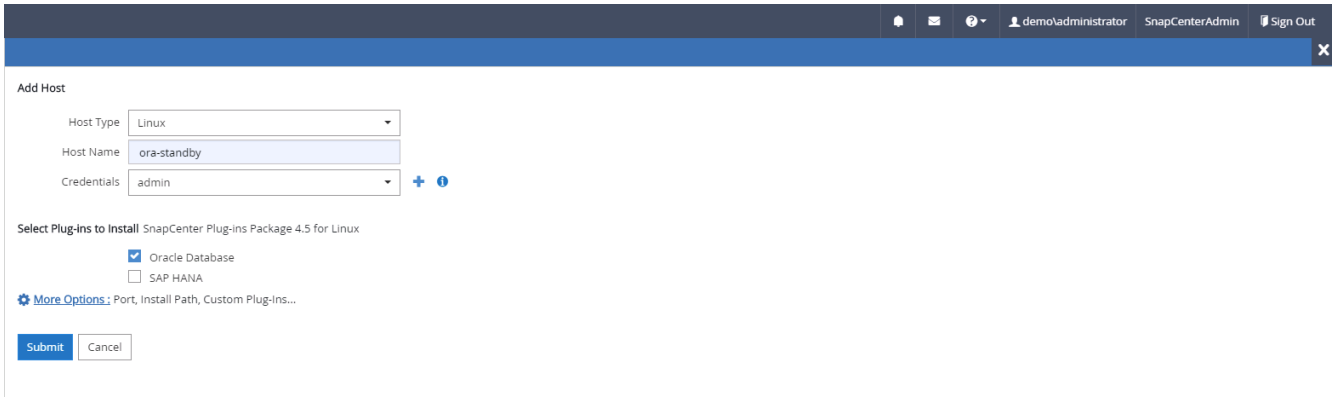




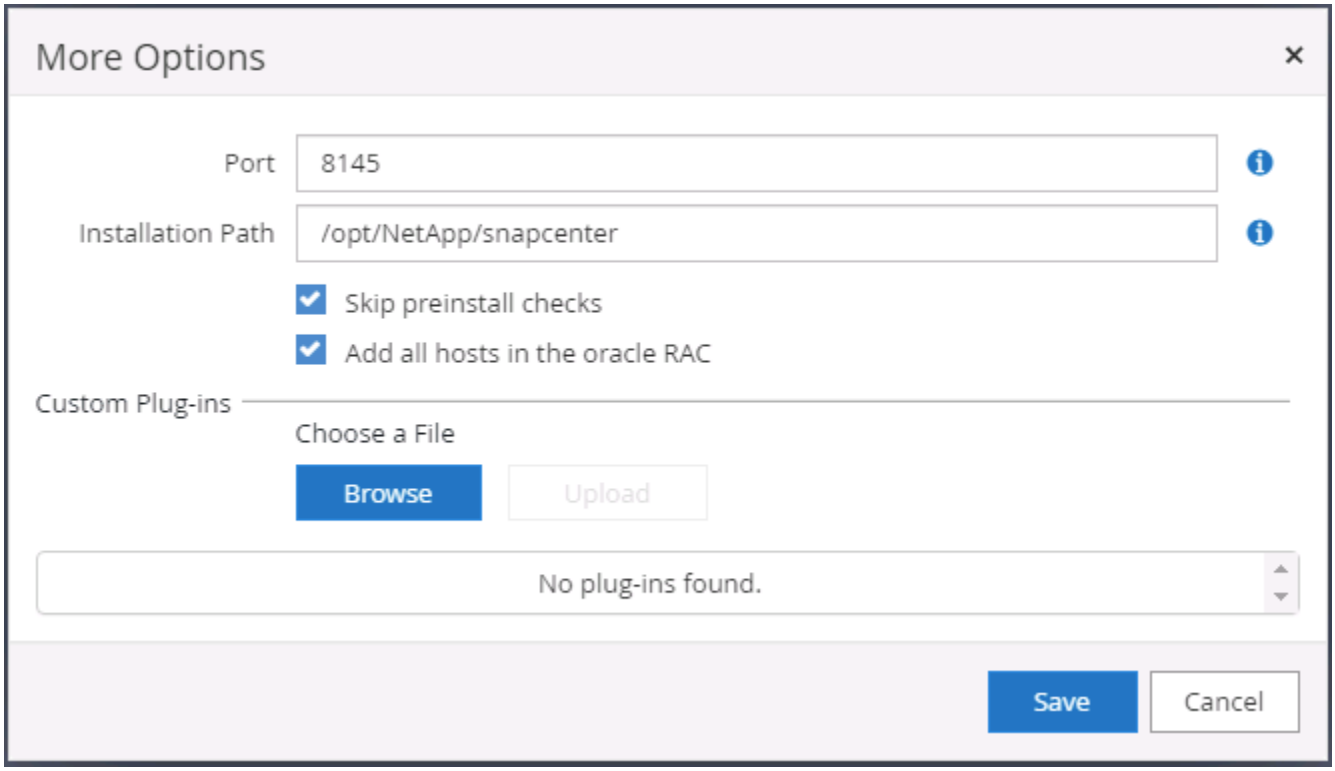
Unix 호스트를 추가하고 호스트에 플러그인을 설치합니다

1. SnapCenter에 SnapCenterAdmin 권한으로 사용자 ID를 사용하여 로그인합니다.
2. 왼쪽 메뉴에서 호스트 탭을 클릭하고 추가 를 클릭하여 호스트 추가 워크플로우를 엽니다.
3. 호스트 유형으로 Linux를 선택합니다. 호스트 이름은 호스트 이름 또는 IP 주소일 수 있습니다. 그러나 SnapCenter 호스트에서 호스트 IP 주소를 수정하려면 호스트 이름을 확인해야 합니다. 2단계에서 만든 호스트 자격 증명을 선택합니다. 호스트 자격 증명에는 sudo 권한이 필요합니다. Oracle Database를 설치할 플러그인으로 선택하여

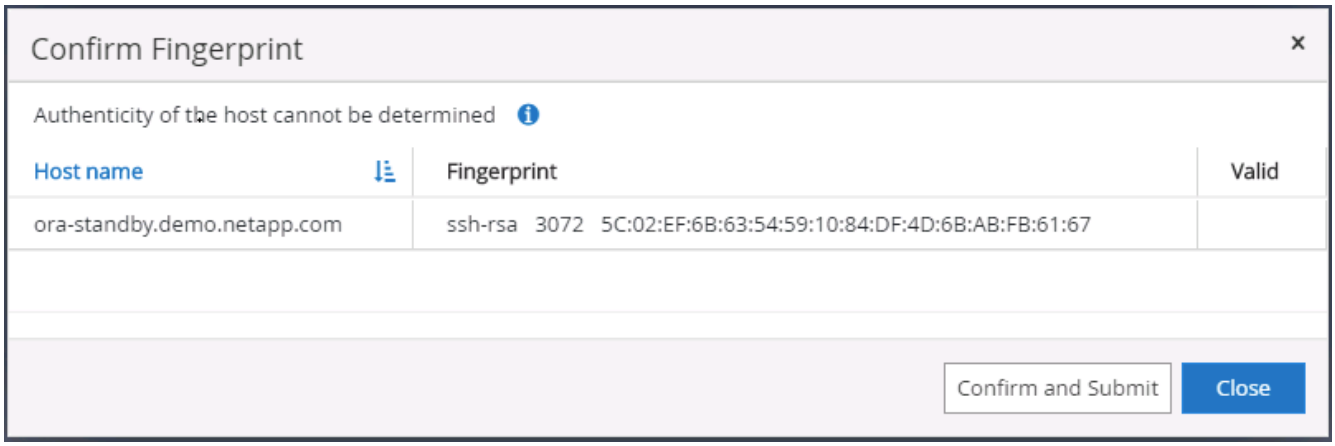
Oracle 및 Linux 호스트 플러그인을 모두 설치합니다.



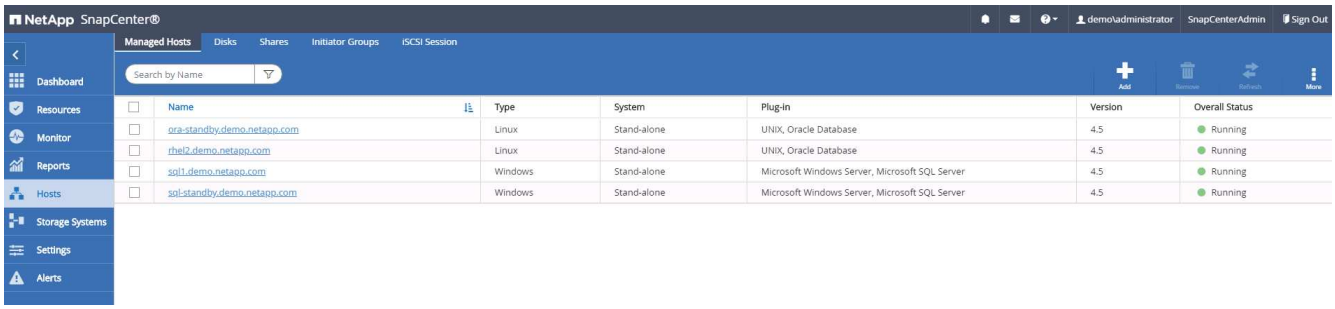
4. 기타 옵션 을 클릭하고 "설치 전 검사 건너뛰기"를 선택합니다. 사전 설치 검사를 건너뛰는 것을 확인하는 메시지가 표시됩니다. 예 를 클릭한 다음 저장 을 클릭합니다.



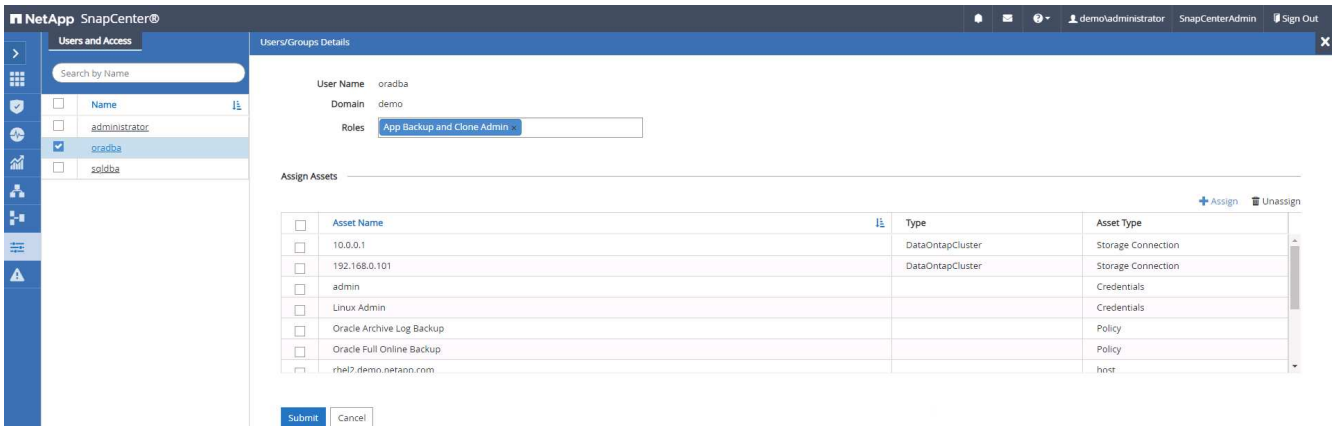
5. 제출 을 클릭하여 플러그인 설치를 시작합니다. 아래와 같이 지문을 확인하라는 메시지가 표시됩니다.

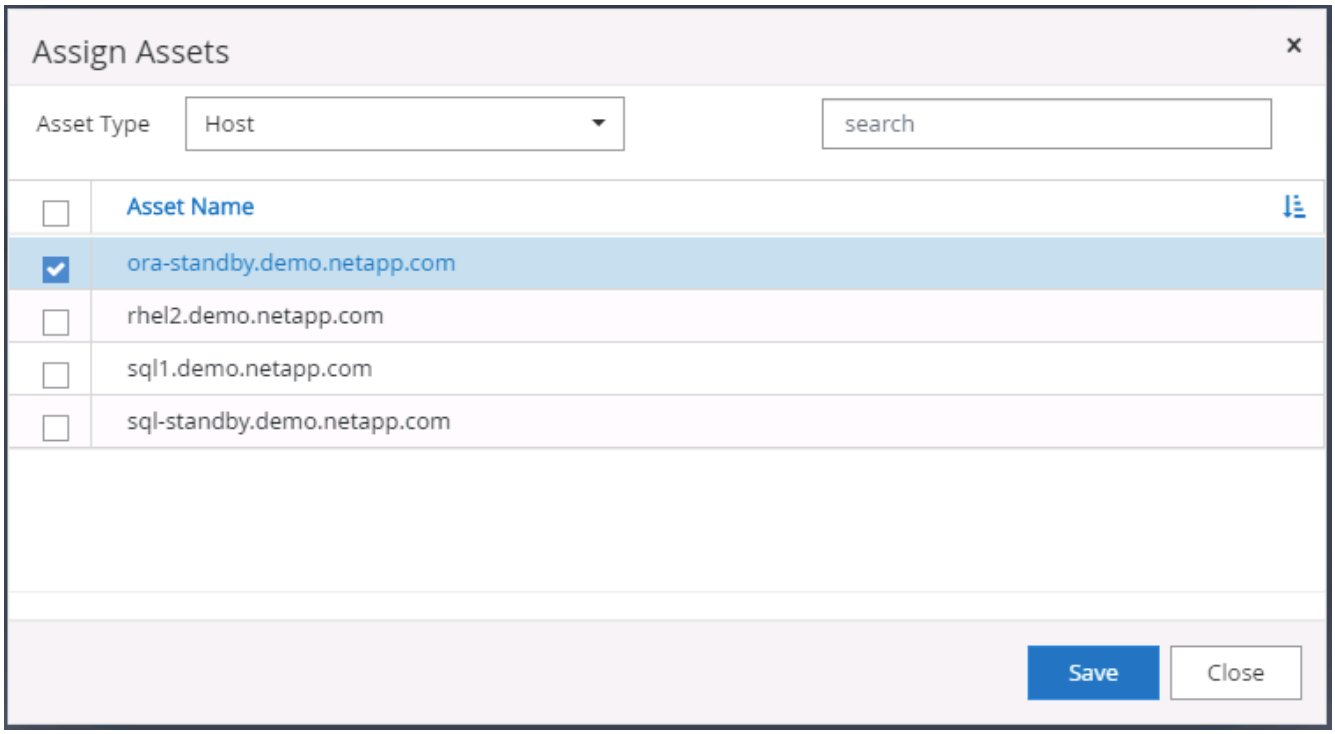


6. SnapCenter는 호스트 검증 및 등록을 수행한 다음 Linux 호스트에 플러그인을 설치합니다. 상태가 플러그인 설치에서 실행 중 으로 변경됩니다.



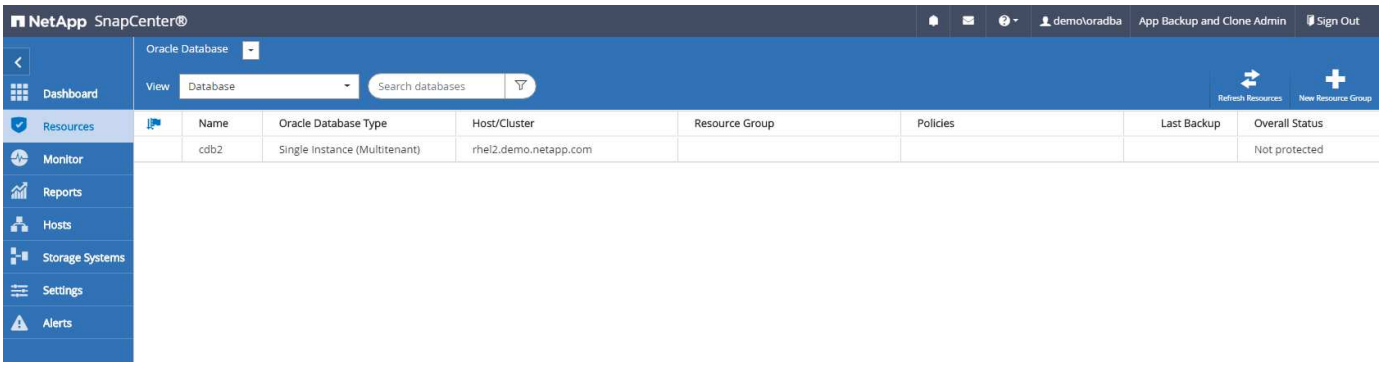
7. 새로 추가된 호스트를 적절한 데이터베이스 관리 사용자 ID(여기서는 oradba)에 할당합니다.





4.데이터베이스 리소스 검색

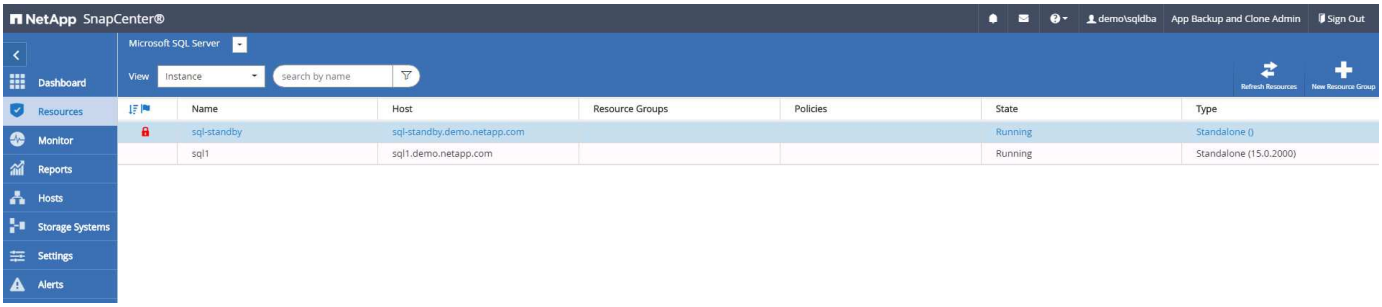
플러그인 설치가 완료되면 호스트의 데이터베이스 리소스를 즉시 검색할 수 있습니다. 왼쪽 메뉴에서 리소스 탭을 클릭합니다. 데이터베이스 플랫폼 유형에 따라 데이터베이스, 리소스 그룹 등과 같은 다양한 보기를 사용할 수 있습니다. 호스트의 리소스가 검색되지 않고 표시되지 않으면 리소스 새로 고침 탭을 클릭해야 할 수도 있습니다.

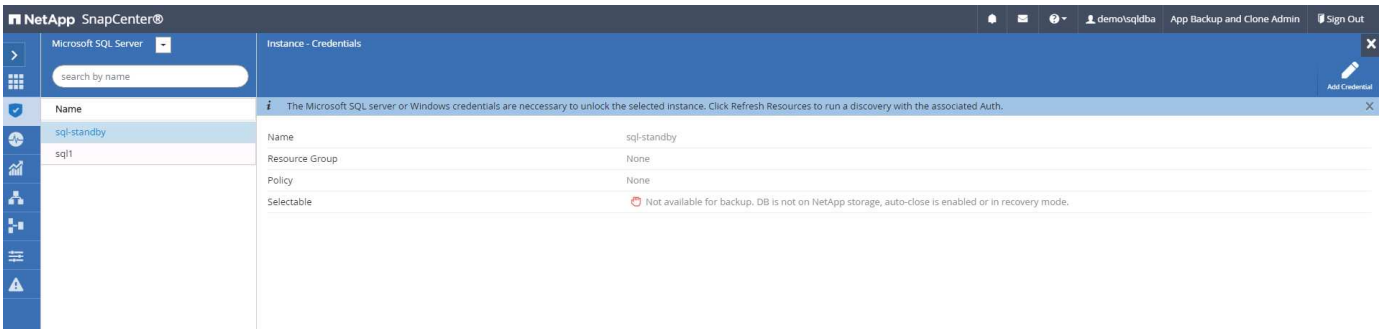


데이터베이스가 처음 검색되면 전체 상태가 "보호되지 않음"으로 표시됩니다. 이전 스크린샷은 아직 백업 정책에 의해 보호되지 않은 Oracle 데이터베이스를 보여 줍니다.

백업 구성 또는 정책을 설정하고 백업을 실행한 경우 데이터베이스의 전체 상태는 백업 상태를 "Backup Succeeded"로 표시하고 마지막 백업의 타임스탬프를 표시합니다. 다음 스크린샷은 SQL Server 사용자 데이터베이스의 백업 상태를 보여 줍니다.

데이터베이스 액세스 자격 증명이 제대로 설정되어 있지 않으면 빨간색 잠금 단추가 데이터베이스에 액세스할 수 없음을 나타냅니다. 예를 들어, Windows 자격 증명에 데이터베이스 인스턴스에 대한 sysadmin 액세스 권한이 없는 경우 데이터베이스 자격 증명을 다시 구성하여 빨간색 잠금을 해제해야 합니다.





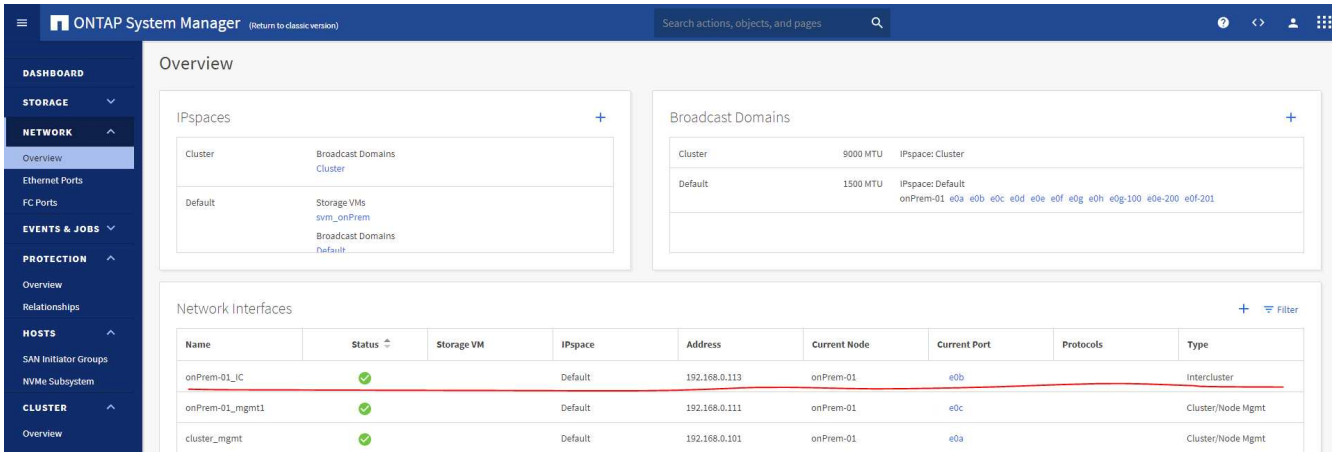
Windows 수준 또는 데이터베이스 수준에서 적절한 자격 증명이 구성되면 빨간색 잠금이 사라지고 SQL Server 유형 정보가 수집 및 검토됩니다.

스토리지 클러스터 피어링 및 **DB** 볼륨 복제를 설정합니다

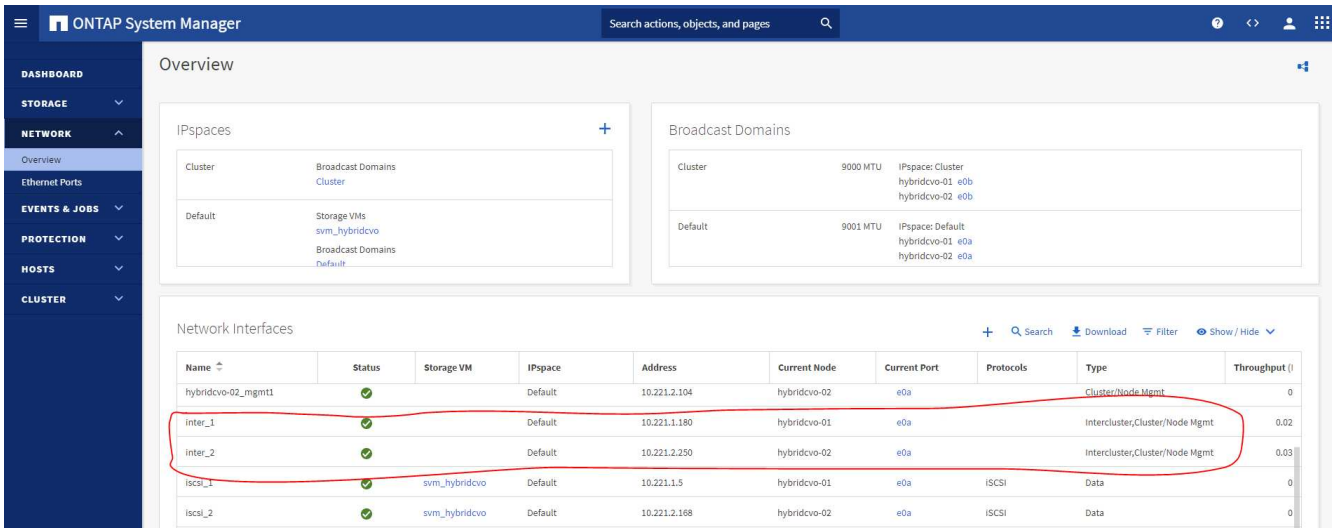
퍼블릭 클라우드를 타겟 대상으로 사용하여 사내 데이터베이스 데이터를 보호하기 위해 NetApp SnapMirror 기술을 사용하여 사내 ONTAP 클러스터 데이터베이스 볼륨을 클라우드의 CVO에 복제합니다. 그런 다음 복제된 타겟 볼륨을 개발/OPS 또는 재해 복구를 위해 복제할 수 있습니다. 다음은 클러스터 피어링을 설정하고 DB 볼륨 복제를 설정하는 상위 단계입니다.

1. 온프레미스 클러스터와 CVO 클러스터 인스턴스 모두에서 클러스터 피어링을 위해 인터클러스터 LIF를 구성합니다. 이 단계는 ONTAP 시스템 관리자로 수행할 수 있습니다. 기본 CVO 배포에는 클러스터 간 LIF가 자동으로 구성됩니다.

   사내 클러스터:



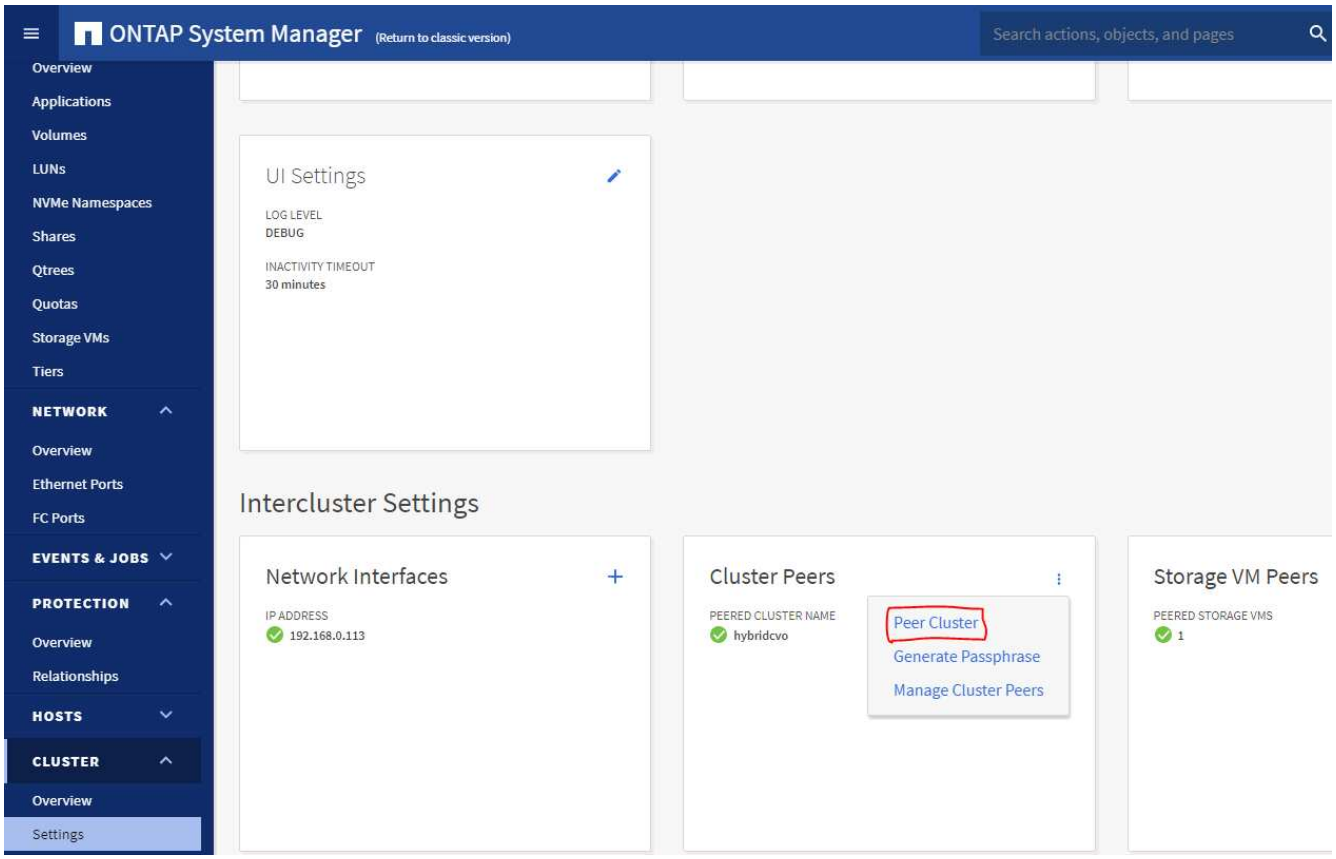
   타겟 CVO 클러스터:



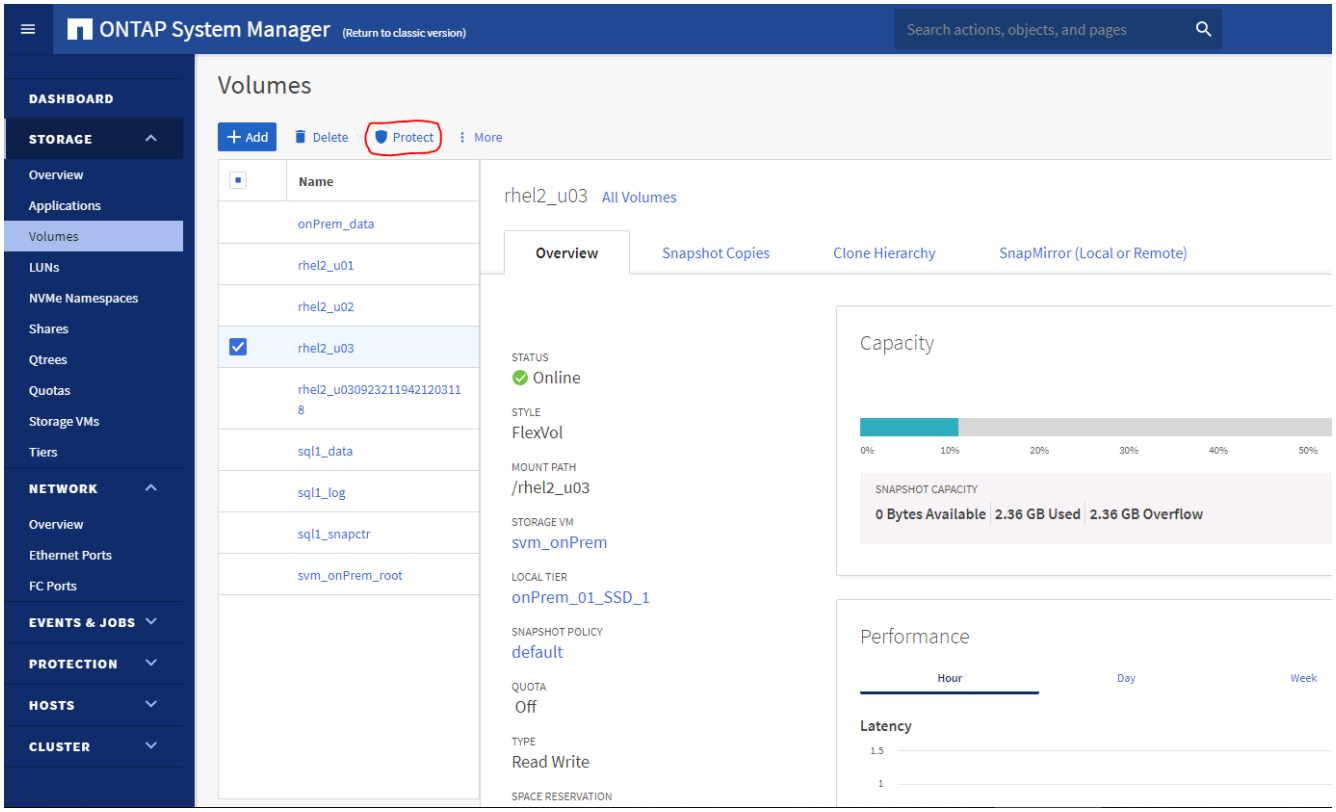
2. 인터클러스터 LIF가 구성된 경우 NetApp Cloud Manager의 끌어서 놓기를 사용하여 클러스터 피어링을 설정하고 볼륨 복제를 설정할 수 있습니다. 을 참조하십시오 "시작하기 - AWS 퍼블릭 클라우드" 를 참조하십시오.

   또는 ONTAP System Manager를 사용하여 다음과 같이 클러스터 피어링을 수행하고 DB 볼륨 복제를 수행할 수 있습니다.

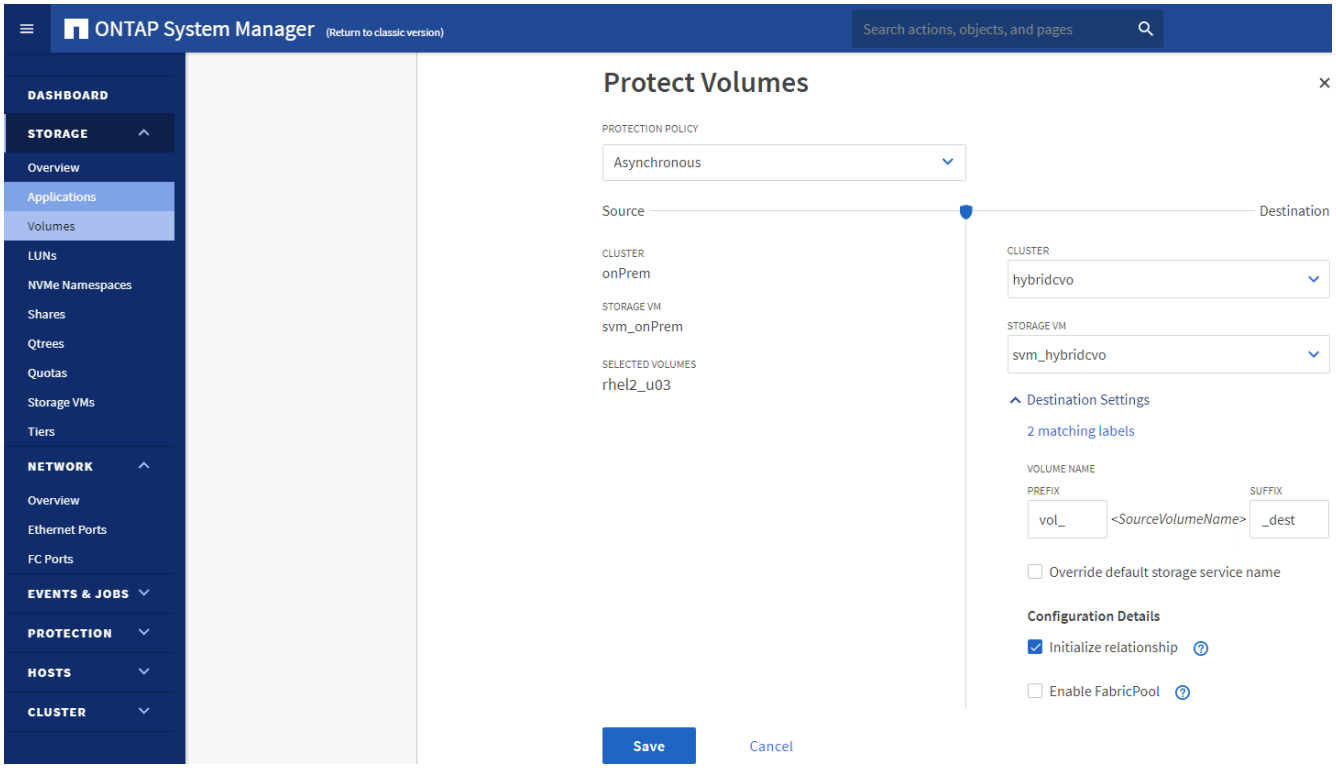
3. ONTAP 시스템 관리자에 로그인합니다. 클러스터 > 설정 으로 이동하고 피어 클러스터 를 클릭하여 클라우드의 CVO 인스턴스로 클러스터 피어링을 설정합니다.



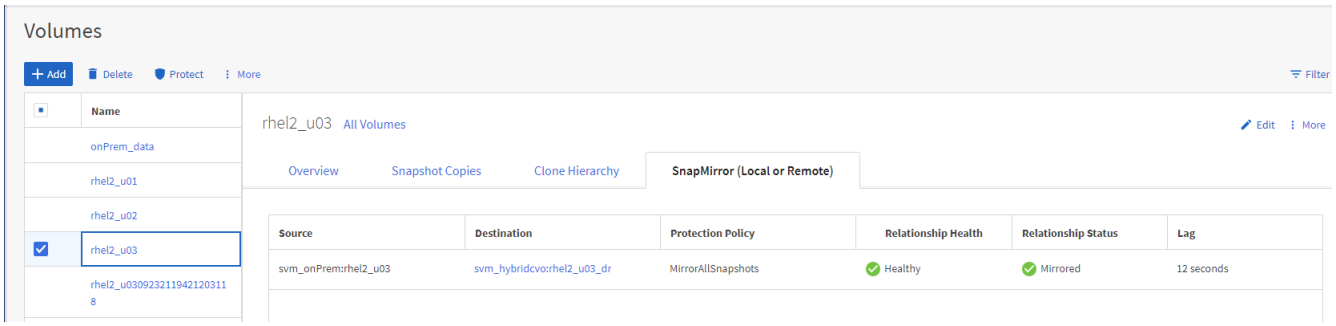
4. 볼륨 탭으로 이동합니다. 복제할 데이터베이스 볼륨을 선택하고 보호 를 클릭합니다.



5. 보호 정책을 Asynchronous로 설정합니다. 대상 클러스터와 스토리지 SVM을 선택합니다.

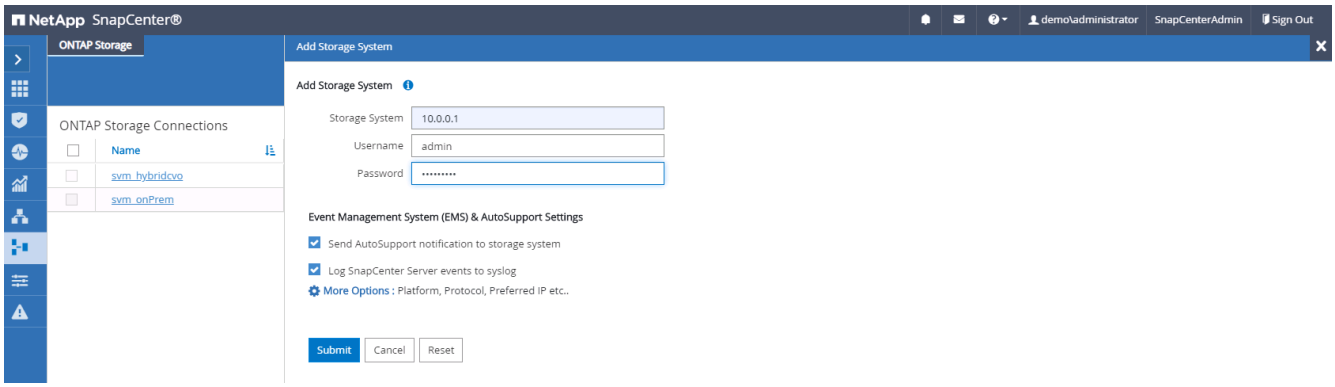


6. 볼륨이 소스와 타겟 간에 동기화되고 복제 관계가 정상 상태인지 확인합니다.

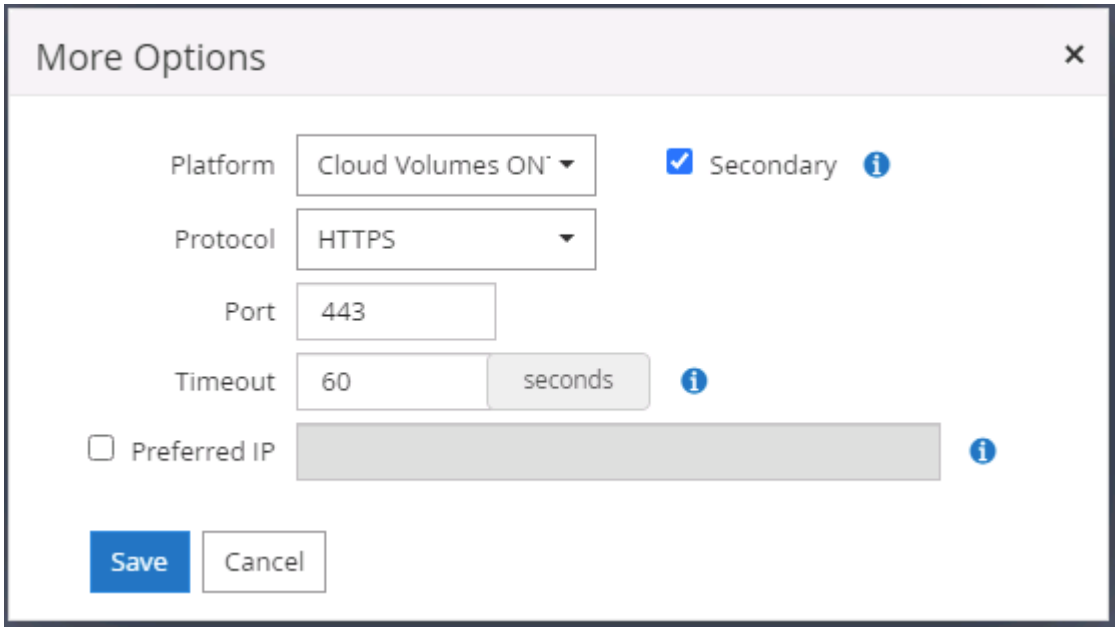


CVO 데이터베이스 스토리지 SVM을 SnapCenter에 추가합니다

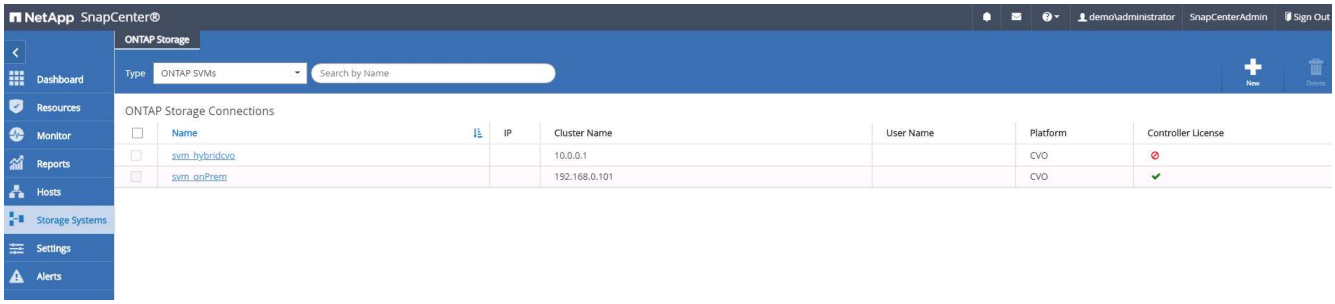
1. SnapCenter에 SnapCenterAdmin 권한으로 사용자 ID를 사용하여 로그인합니다.
2. 메뉴에서 스토리지 시스템 탭을 클릭한 다음 새로 만들기를 클릭하여 복제된 타겟 데이터베이스 볼륨을 SnapCenter에 호스팅하는 CVO 스토리지 SVM을 추가합니다. 스토리지 시스템 필드에 클러스터 관리 IP를 입력하고 적절한 사용자 이름과 암호를 입력합니다.



3. 추가 옵션을 클릭하여 추가 스토리지 구성 옵션을 엽니다. 플랫폼 필드에서 Cloud Volumes ONTAP 를 선택하고 보조 를 선택한 다음 저장 을 클릭합니다.



4. 에 나와 있는 대로 스토리지 시스템을 SnapCenter 데이터베이스 관리 사용자 ID에 할당합니다 3.SnapCenter 호스트 플러그인 설치.

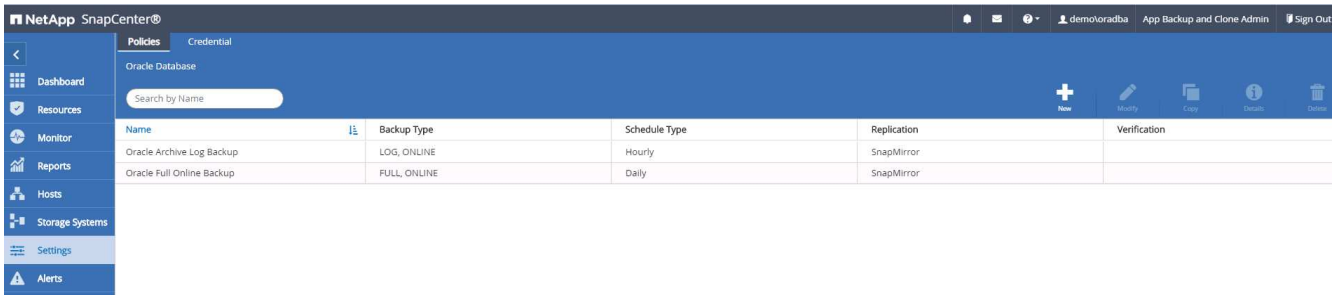


SnapCenter에서 데이터베이스 백업 정책을 설정합니다

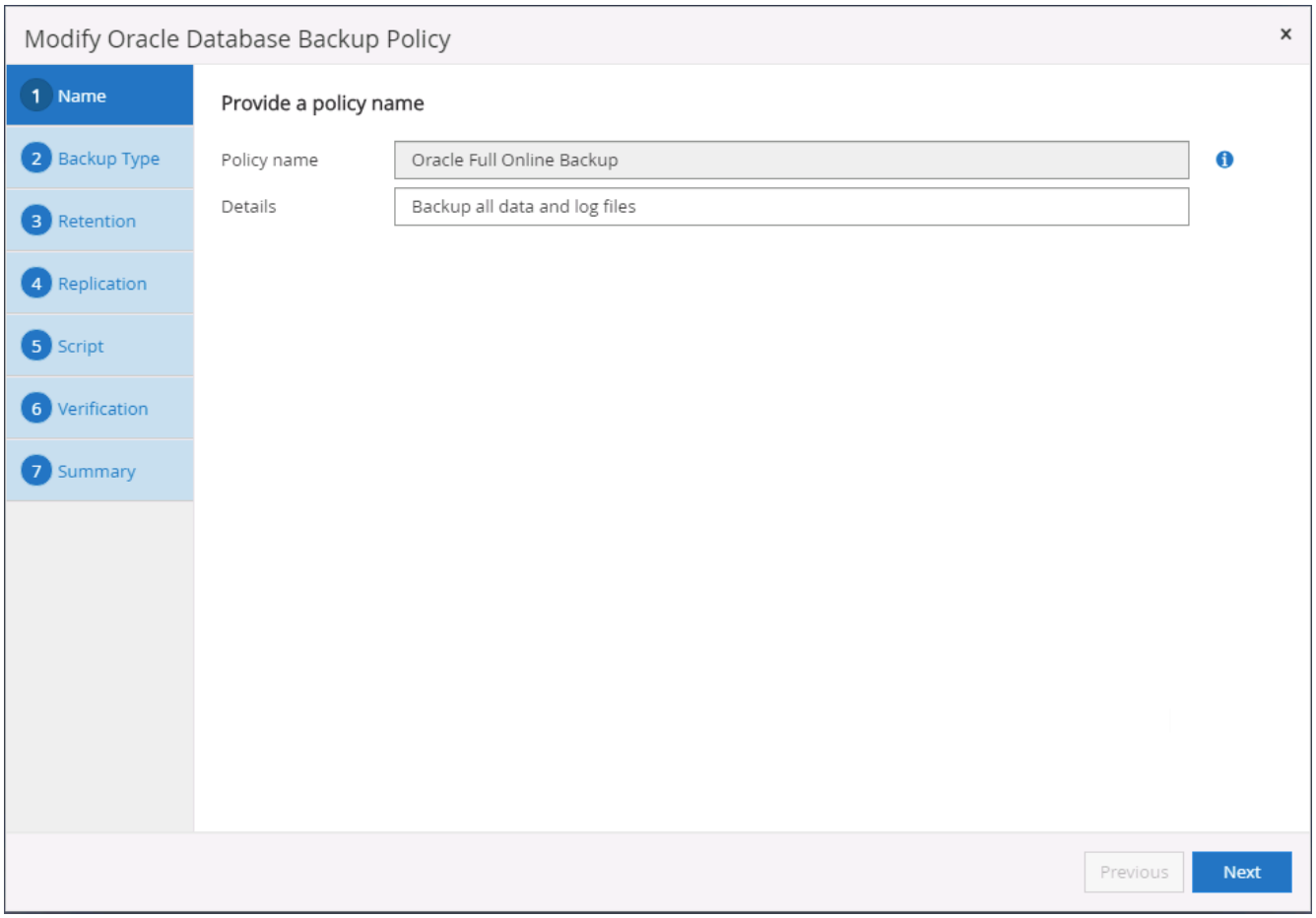
다음 절차에서는 전체 데이터베이스 또는 로그 파일 백업 정책을 만드는 방법을 보여 줍니다. 그런 다음 이 정책을 구현하여 데이터베이스 리소스를 보호할 수 있습니다. RPO(복구 지점 목표) 또는 RTO(복구 시간 목표)는 데이터베이스 및/또는 로그 백업의 빈도를 결정합니다.

Oracle에 대한 전체 데이터베이스 백업 정책을 생성합니다

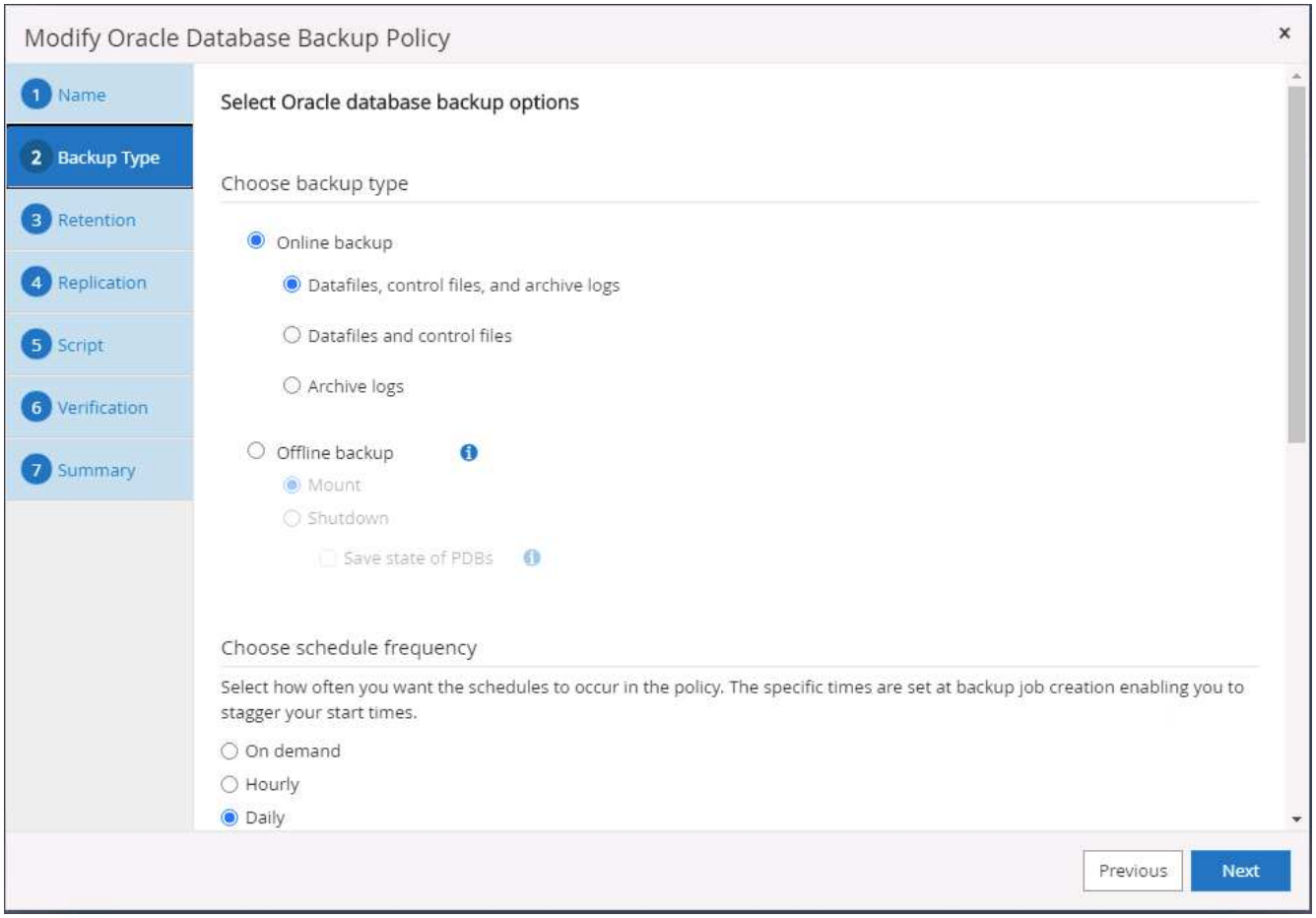
1. SnapCenter에 데이터베이스 관리 사용자 ID로 로그인하고 설정을 클릭한 다음 정책을 클릭합니다.



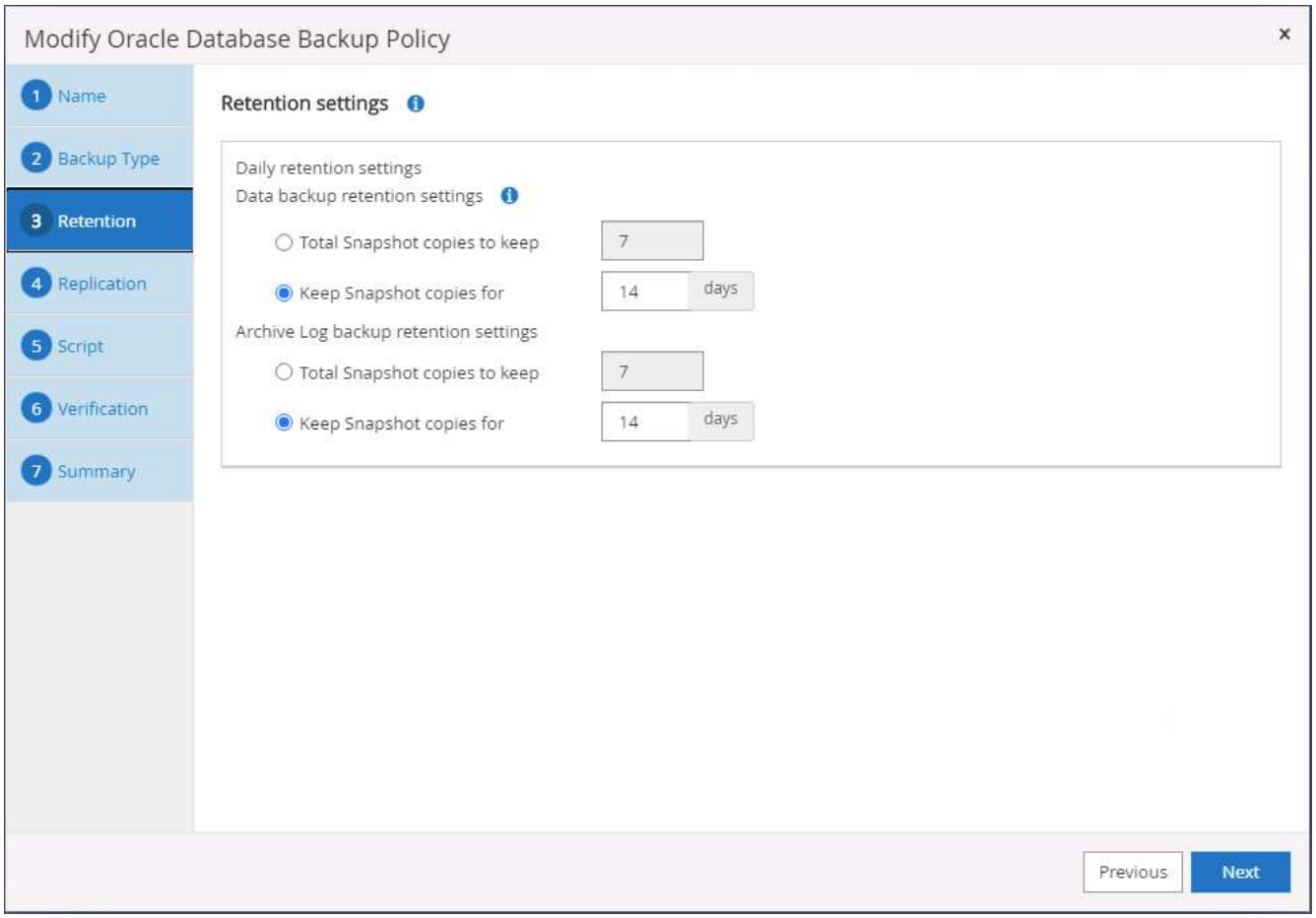
2. New(새로 만들기) 를 클릭하여 새 백업 정책 생성 워크플로우를 시작하거나 수정할 기존 정책을 선택합니다.



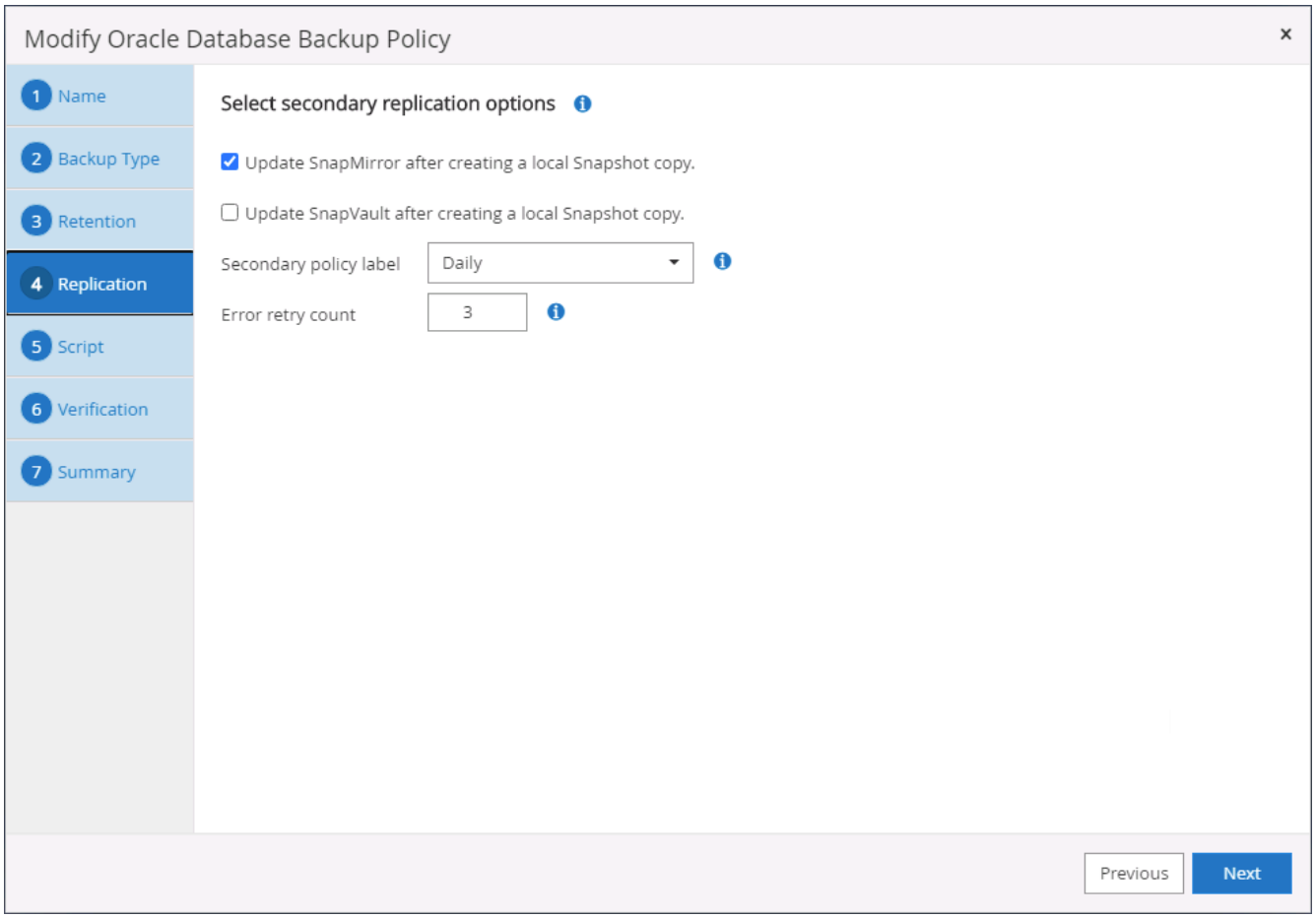
3. 백업 유형 및 스케줄 빈도를 선택합니다.



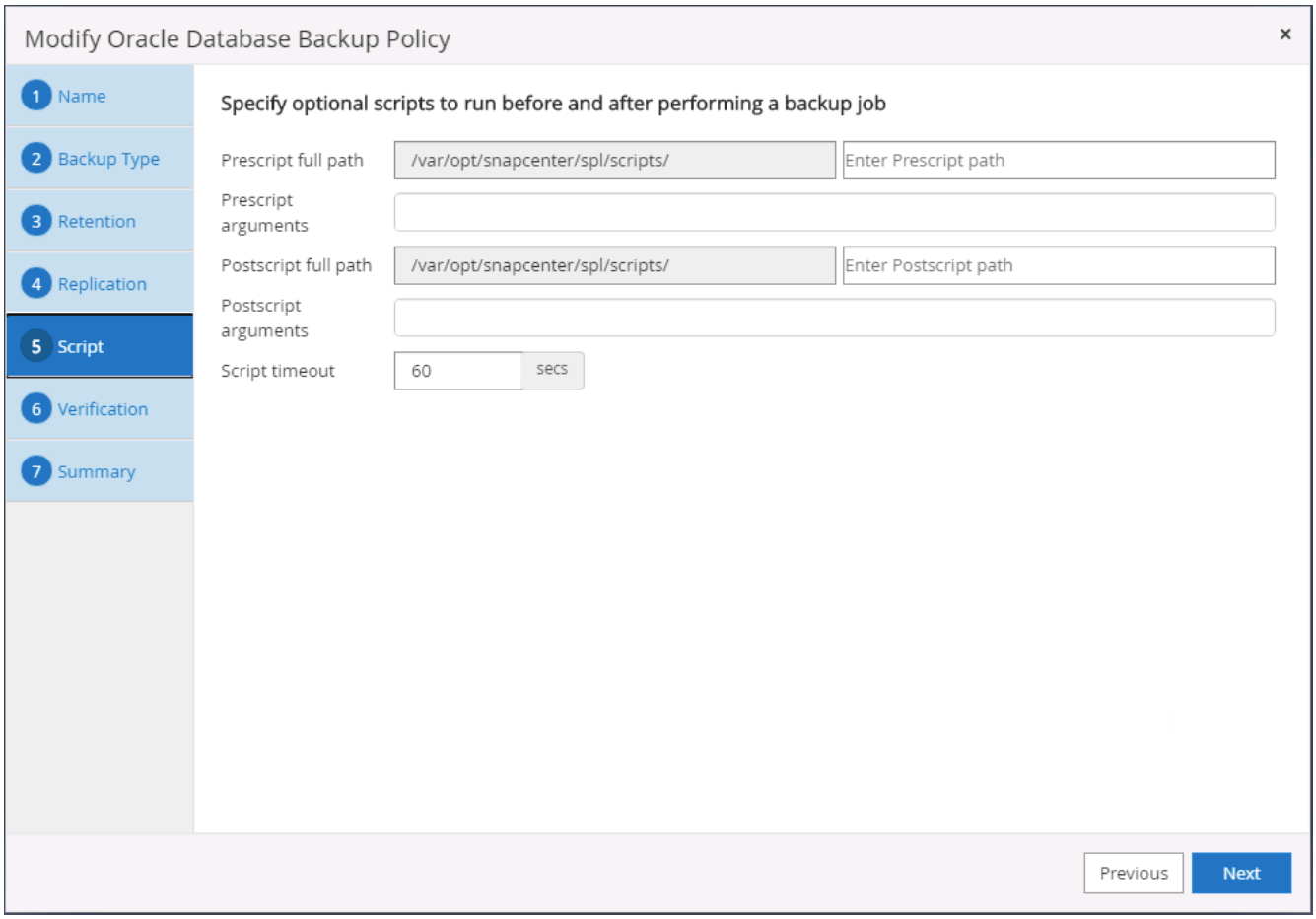
4. 백업 보존 설정을 지정합니다. 이 경우 보관할 전체 데이터베이스 백업 복사본 수가 정의됩니다.



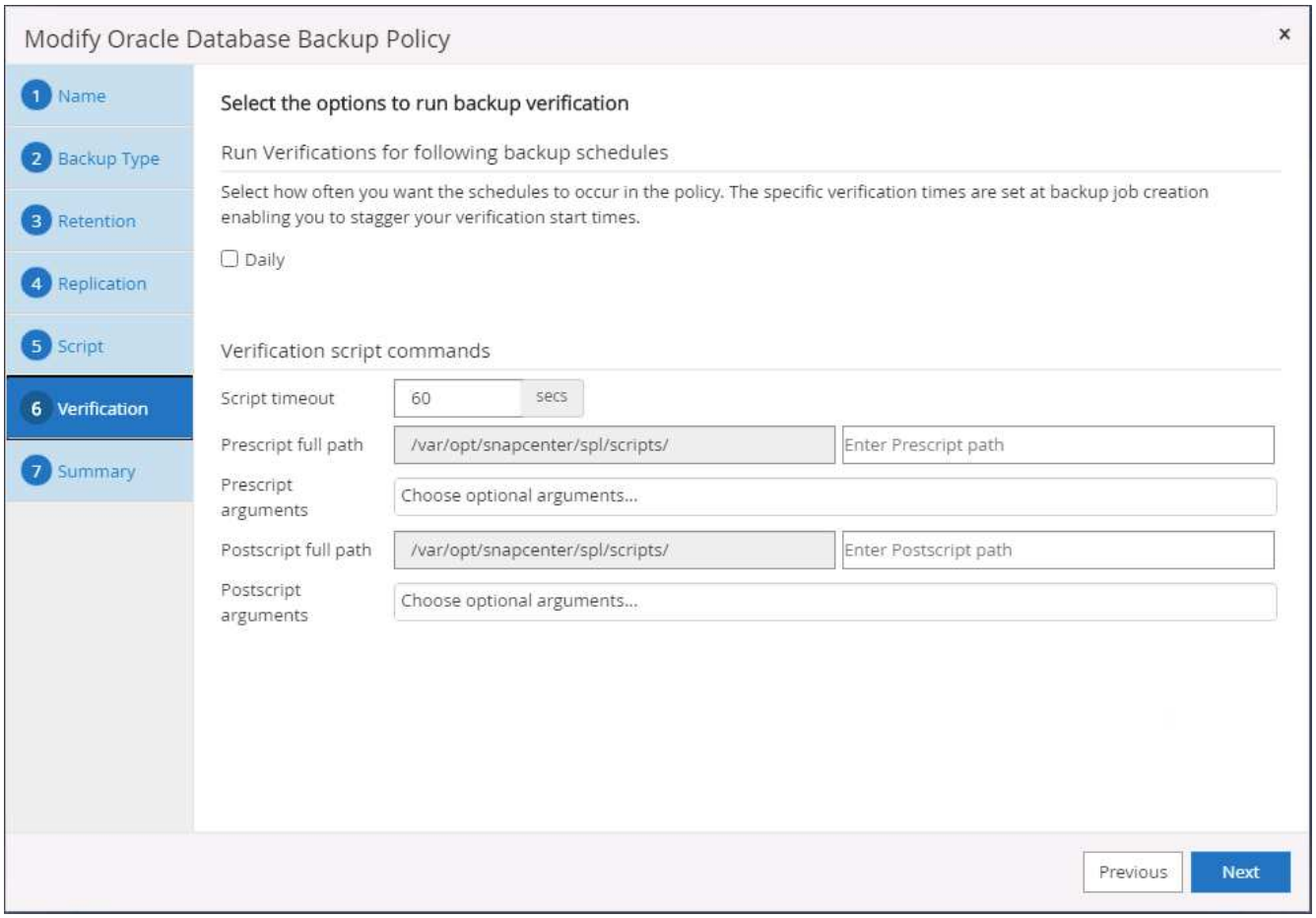
5. 클라우드의 2차 위치에 복제할 로컬 기본 스냅샷 백업을 푸시할 2차 복제 옵션을 선택합니다.



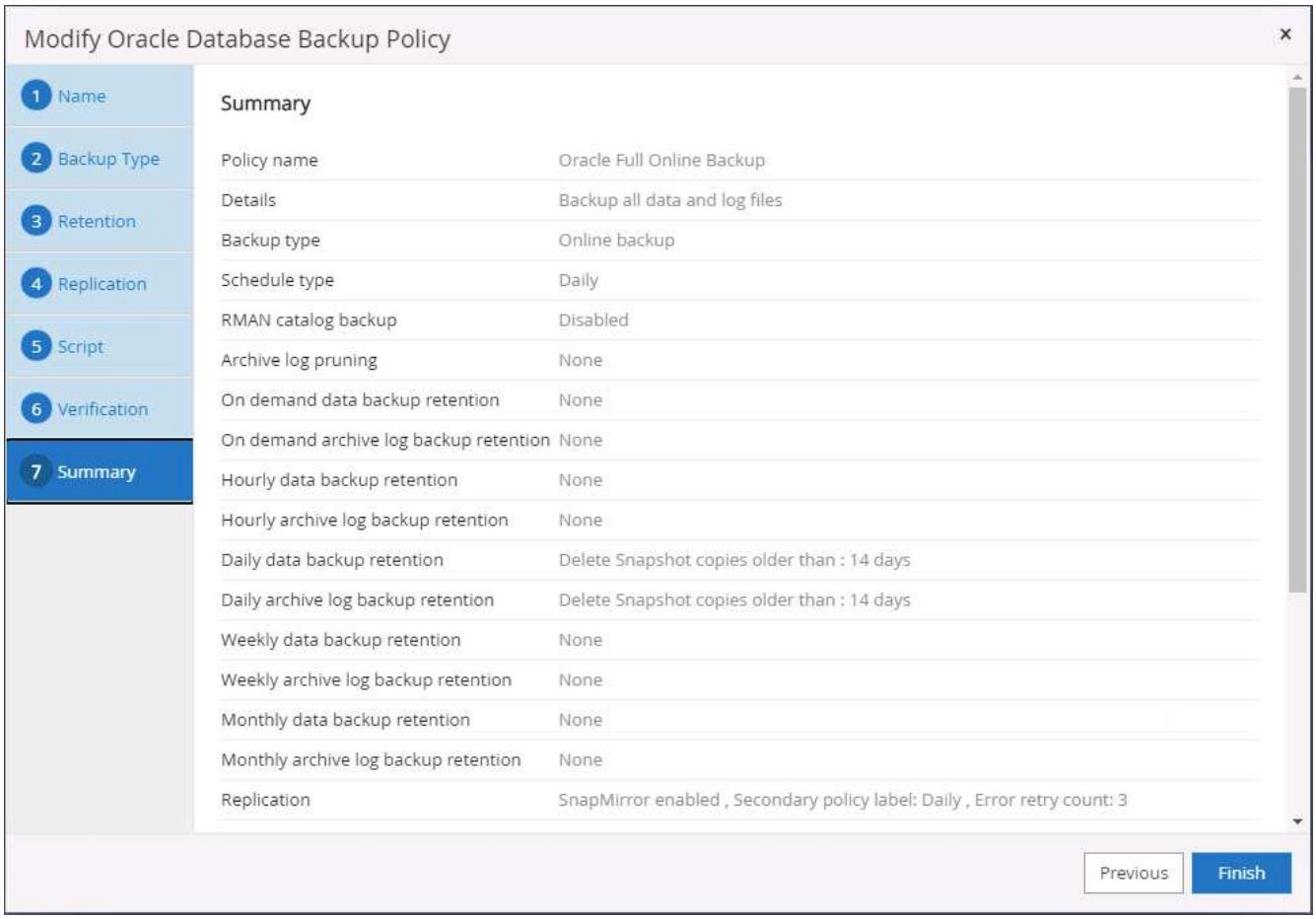
6. 백업 실행 전후에 실행할 선택적 스크립트를 지정합니다.



7. 필요한 경우 백업 검증을 실행합니다.

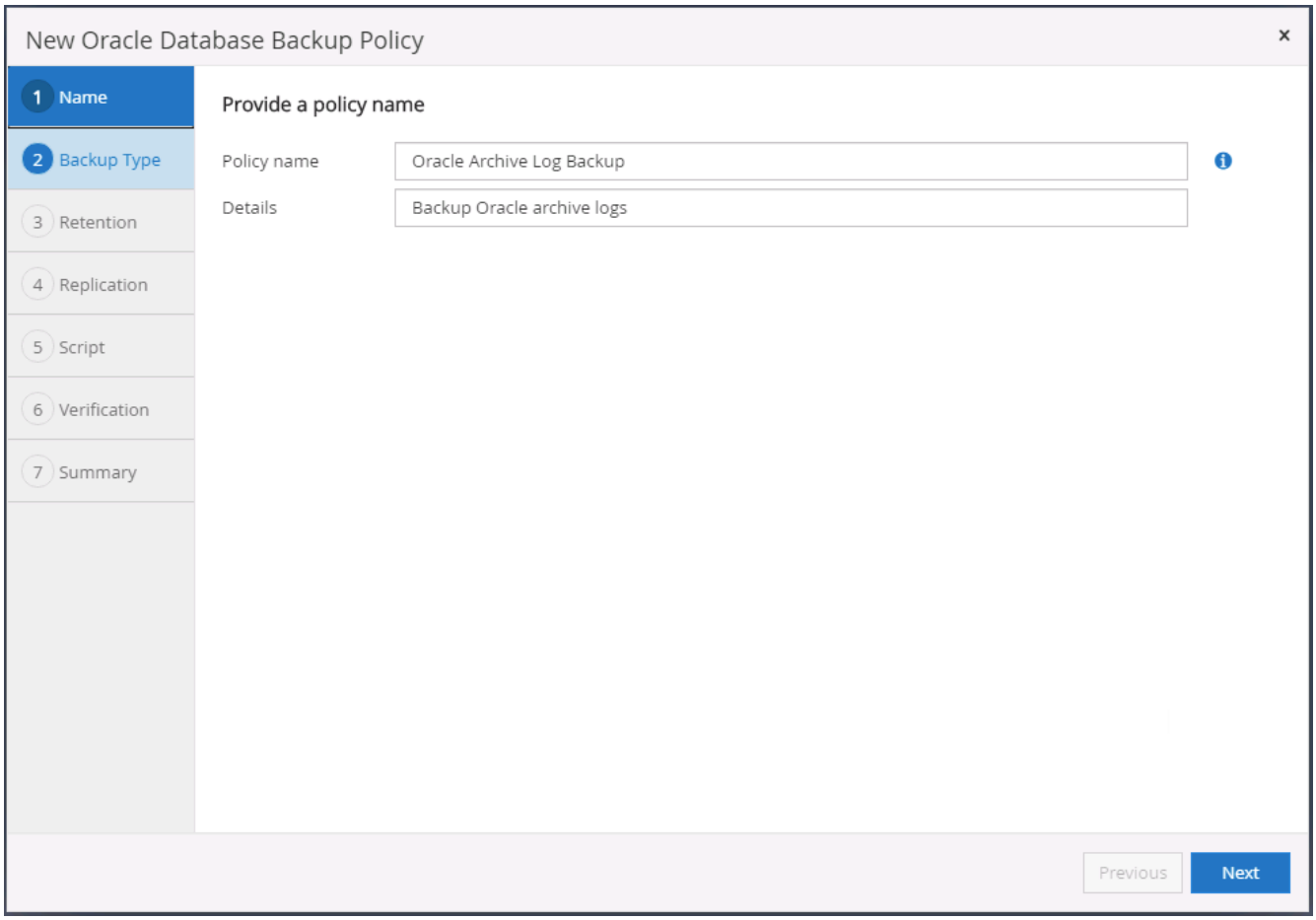

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. 요약.

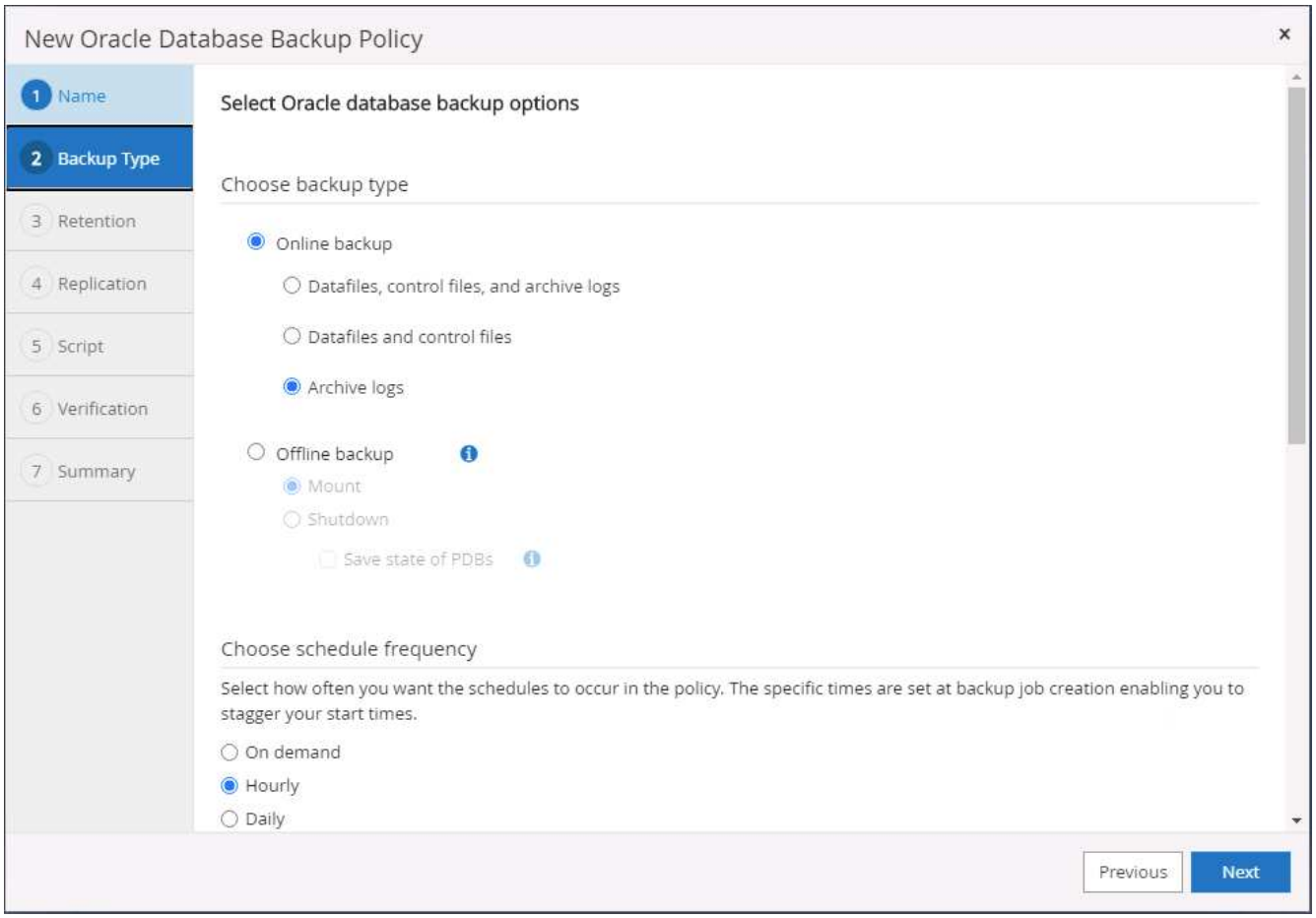


Oracle에 대한 데이터베이스 로그 백업 정책을 생성합니다

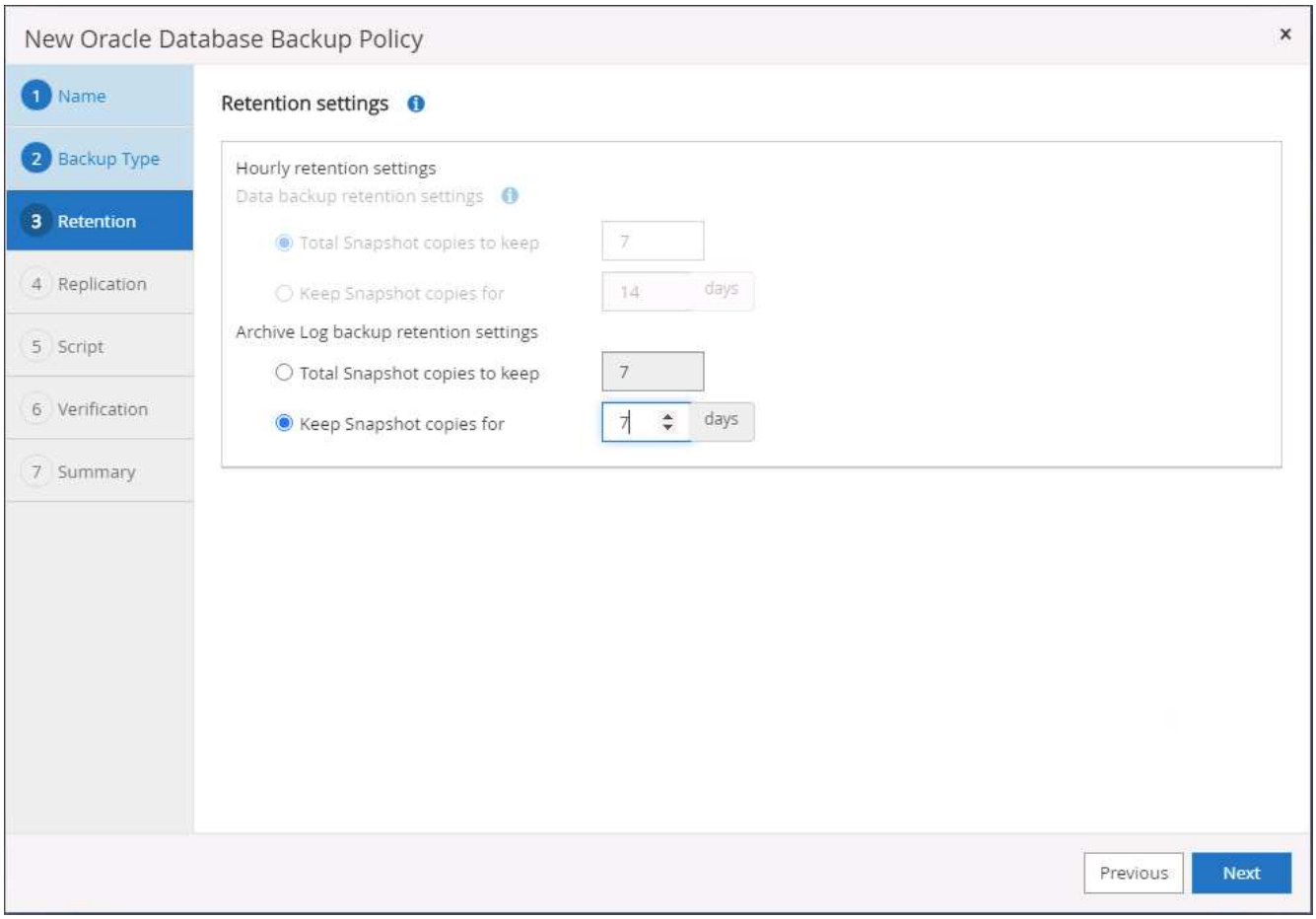
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 설정을 클릭한 다음 정책을 클릭합니다.
2. 새로 만들기 를 클릭하여 새 백업 정책 생성 워크플로우를 시작하거나 수정할 기존 정책을 선택합니다.



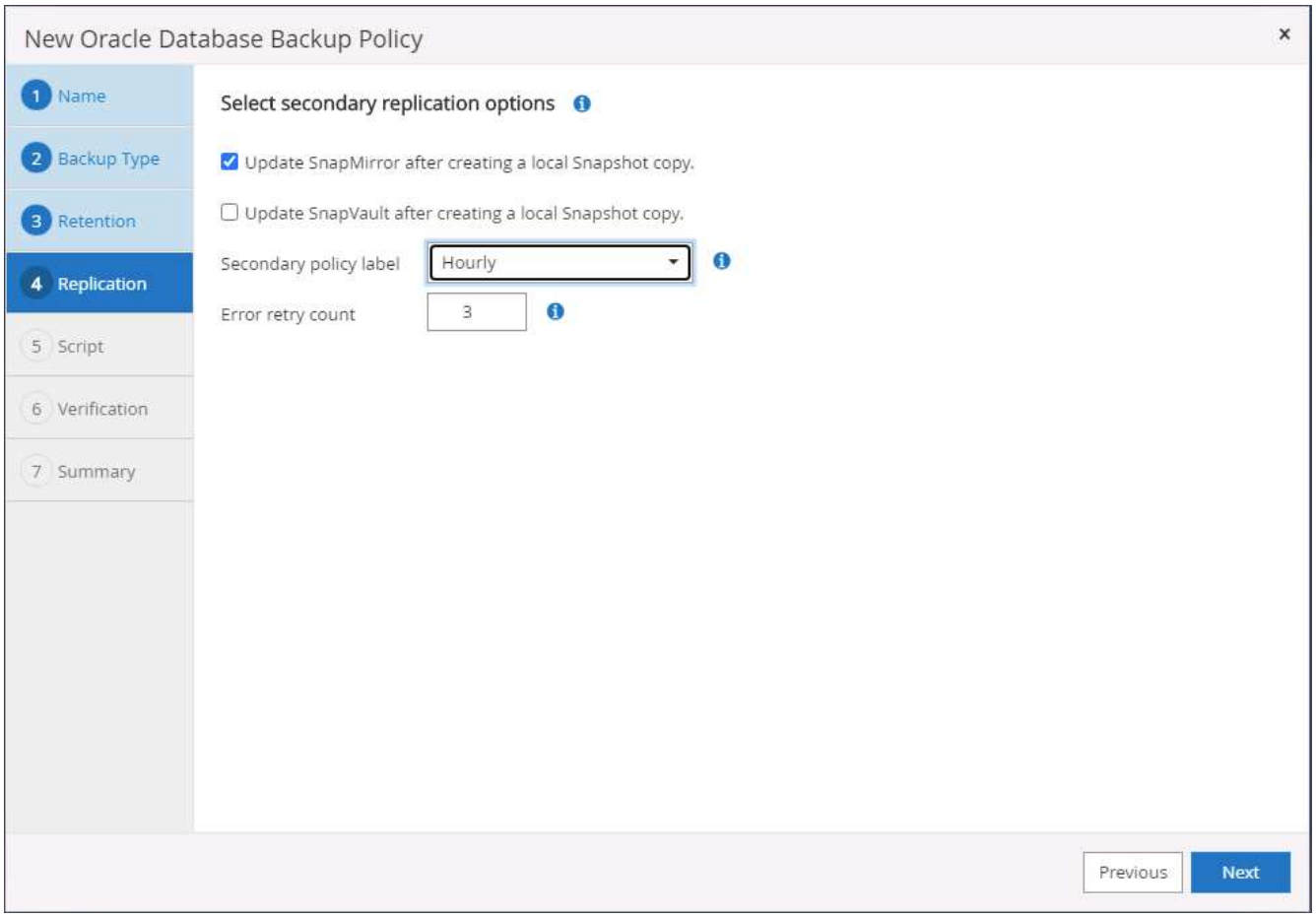
3. 백업 유형 및 스케줄 빈도를 선택합니다.



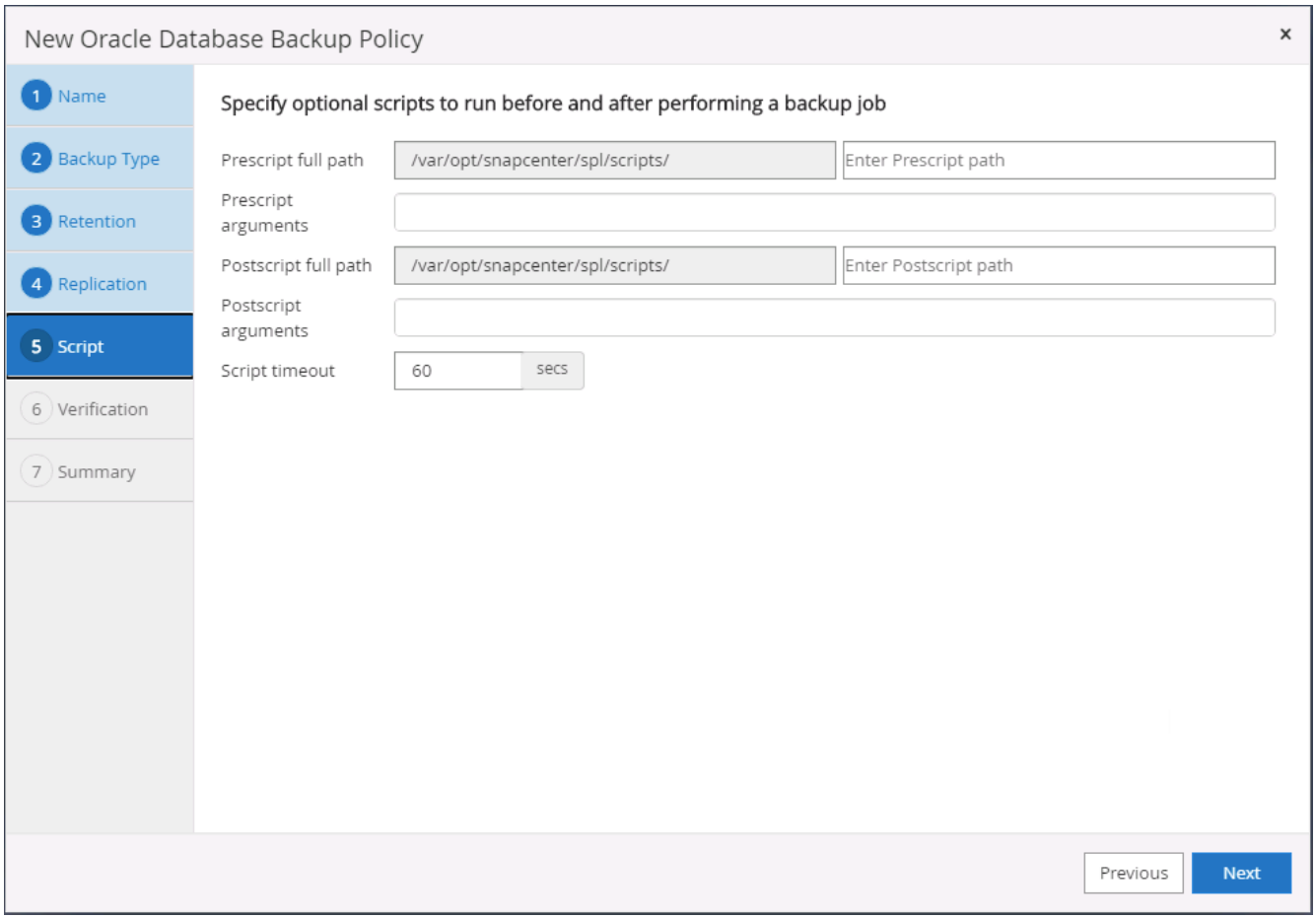
4. 로그 보존 기간을 설정합니다.



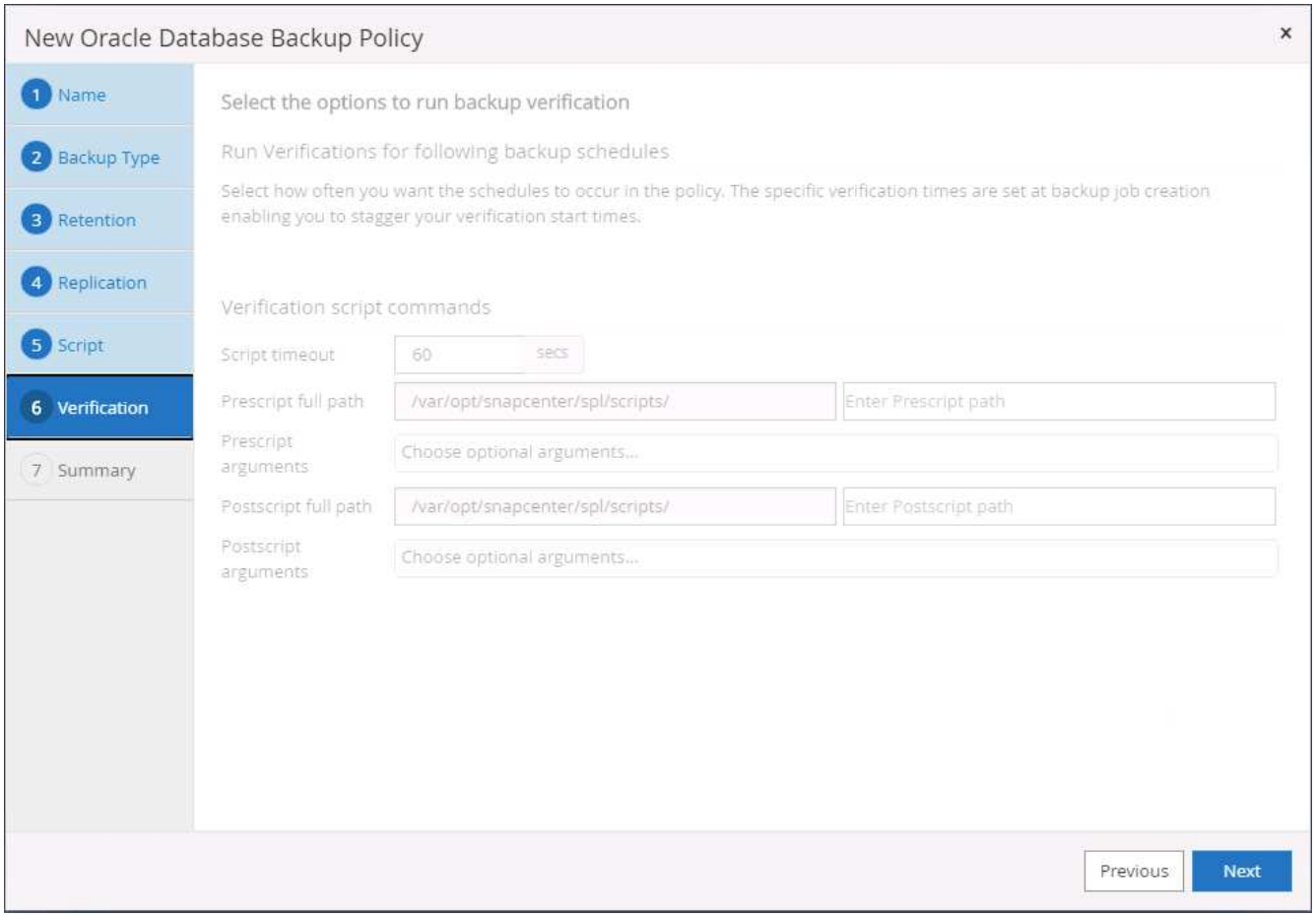
5. 퍼블릭 클라우드의 2차 위치에 복제



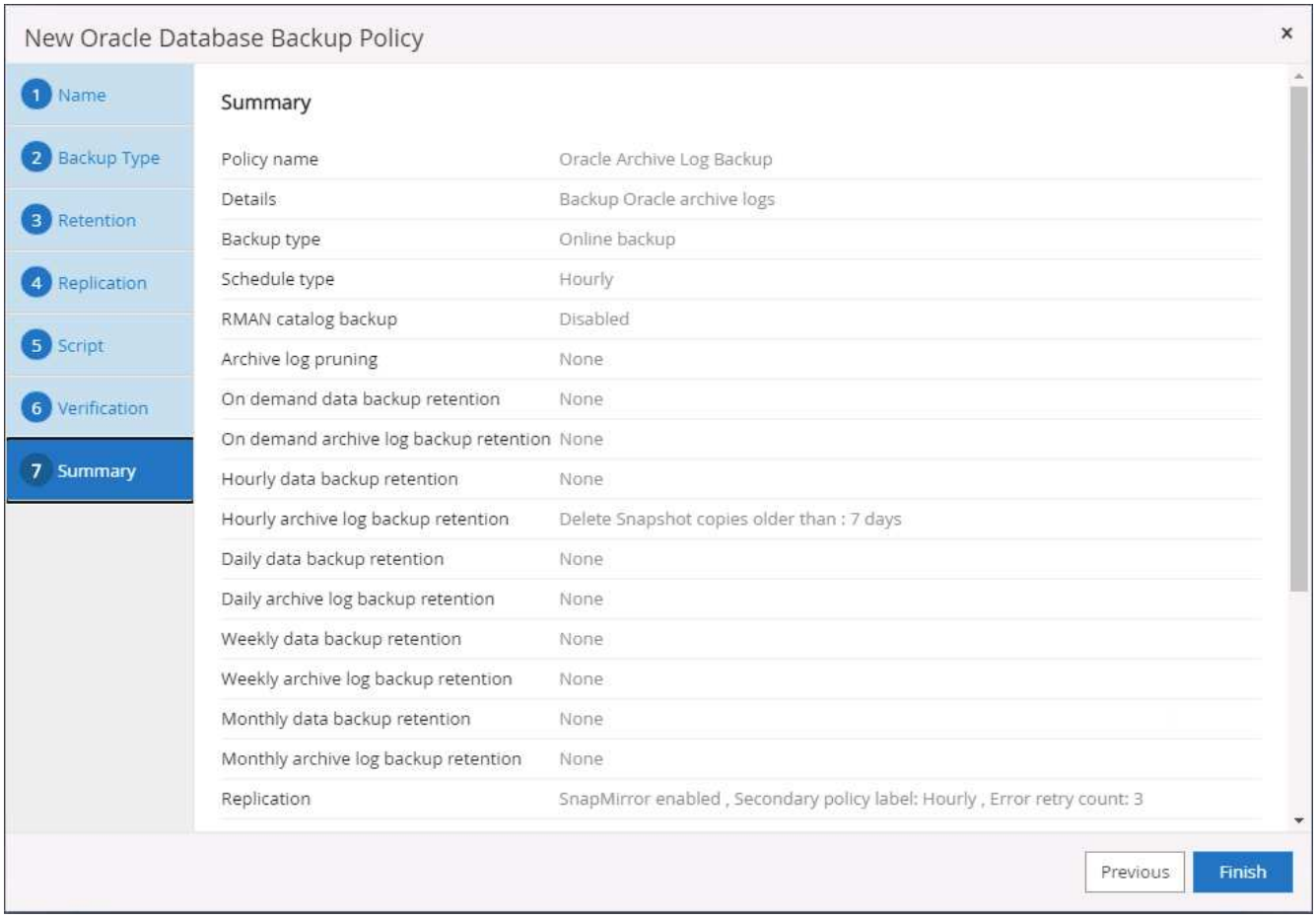
6. 로그 백업 전후에 실행할 선택적 스크립트를 지정합니다.



7. 백업 검증 스크립트를 지정합니다.

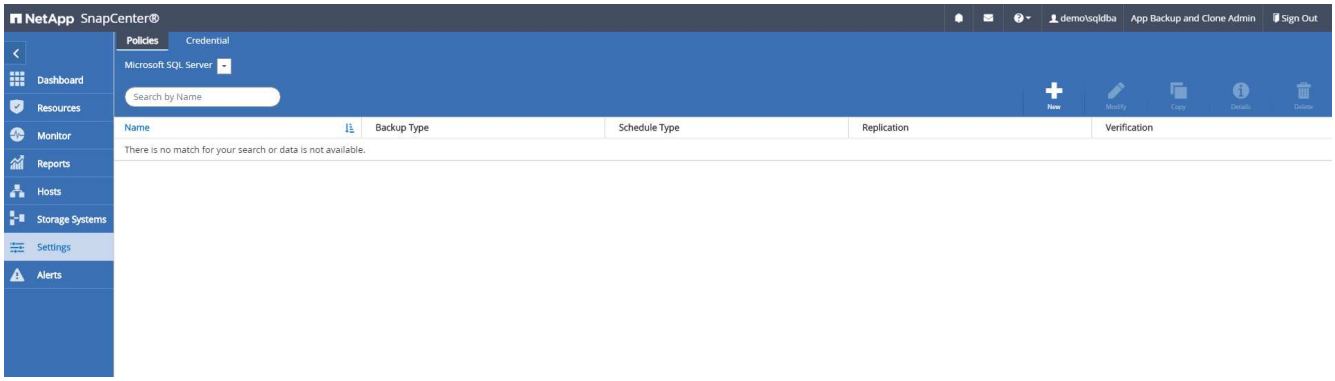

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. 요약.

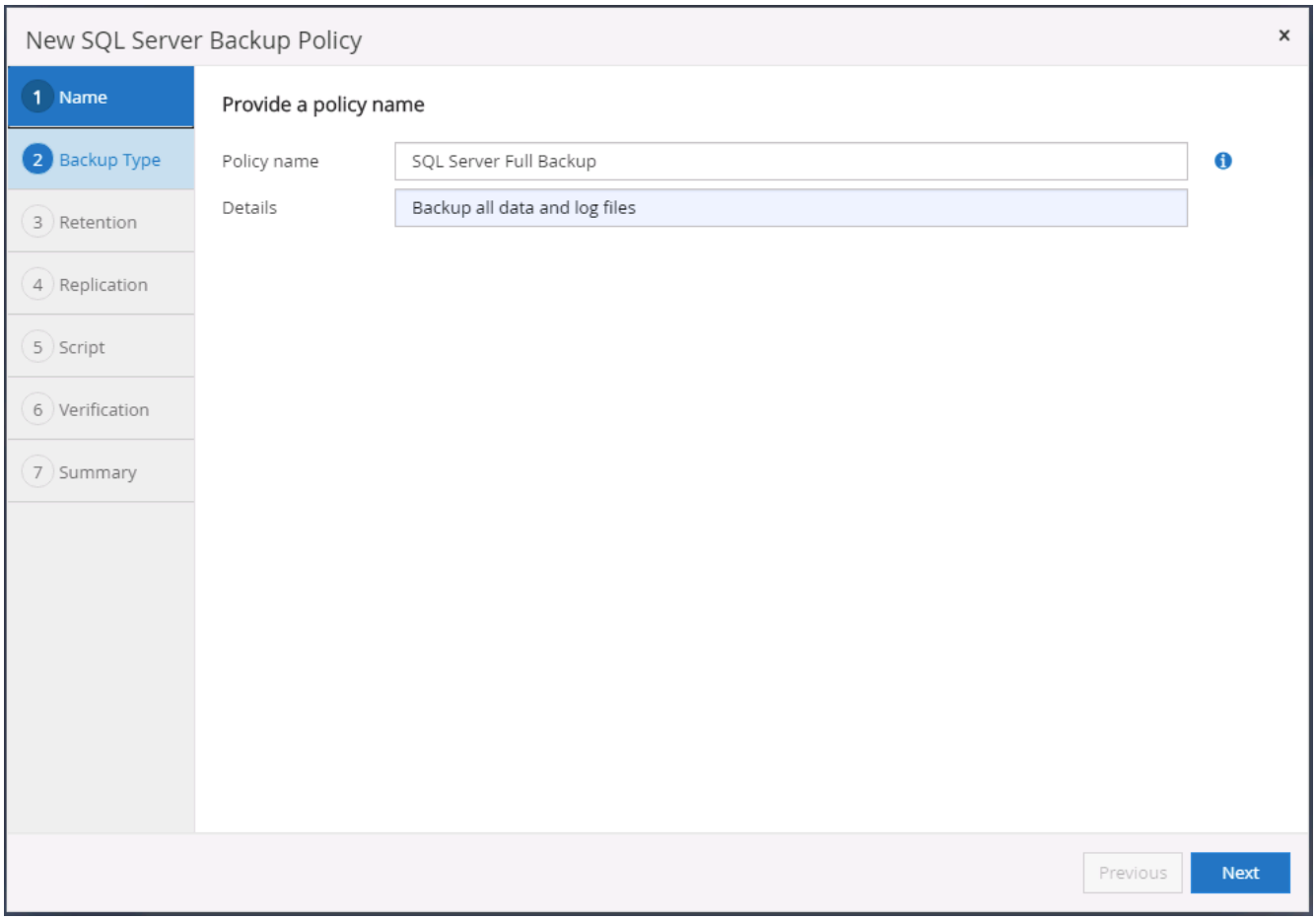


SQL에 대한 전체 데이터베이스 백업 정책을 생성합니다

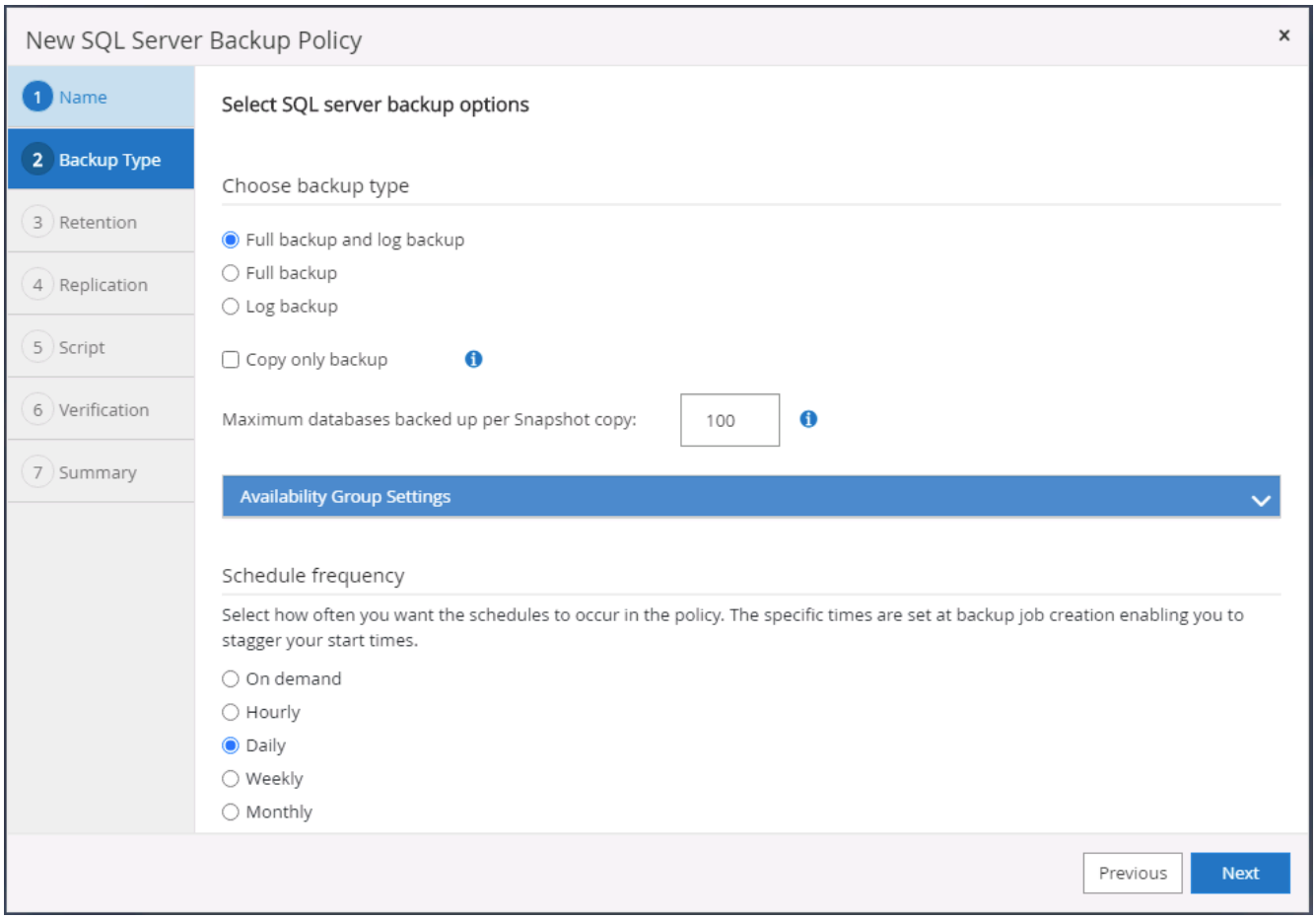
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 설정을 클릭한 다음 정책을 클릭합니다.



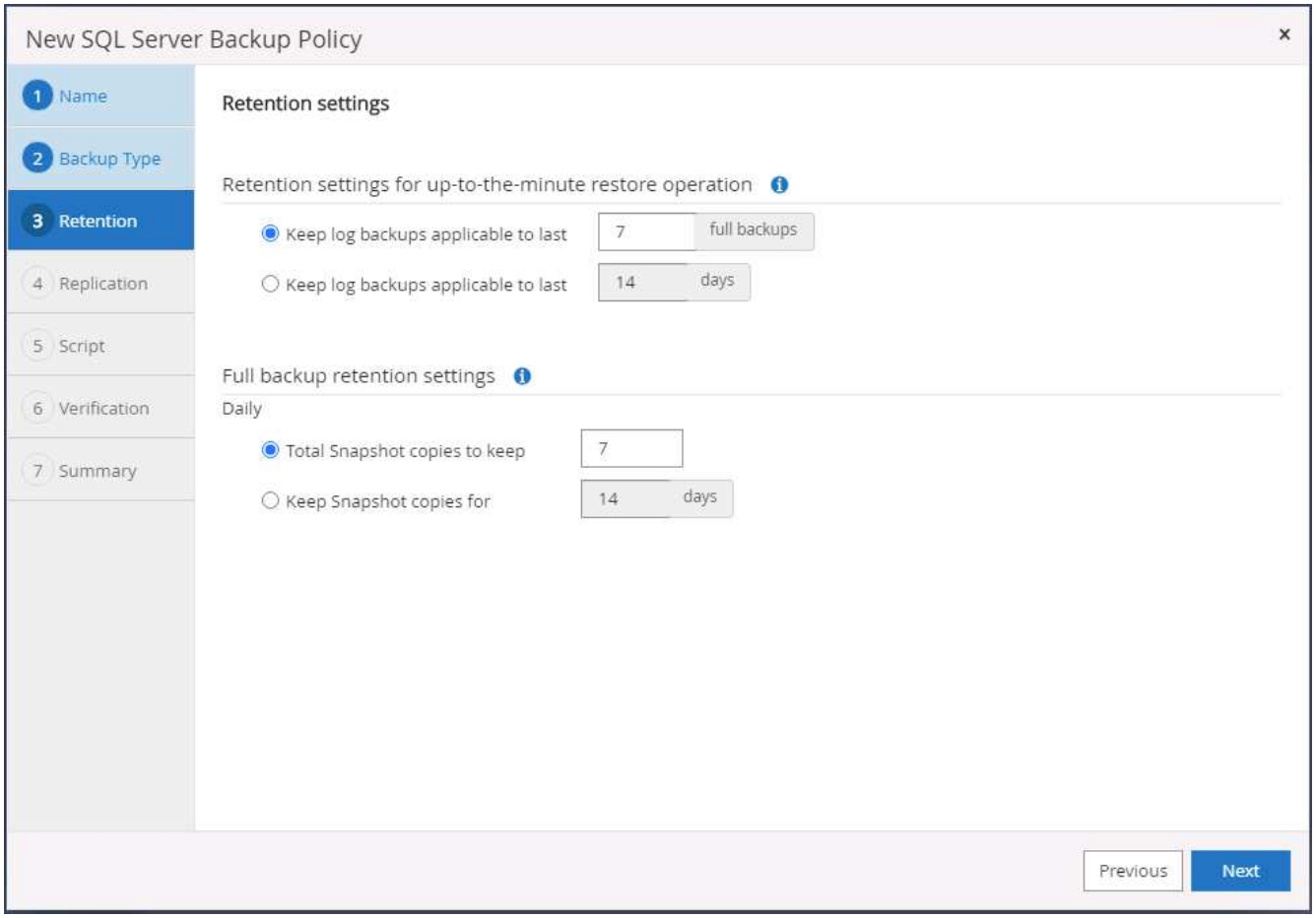
2. 새로 만들기 를 클릭하여 새 백업 정책 생성 워크플로우를 시작하거나 수정할 기존 정책을 선택합니다.



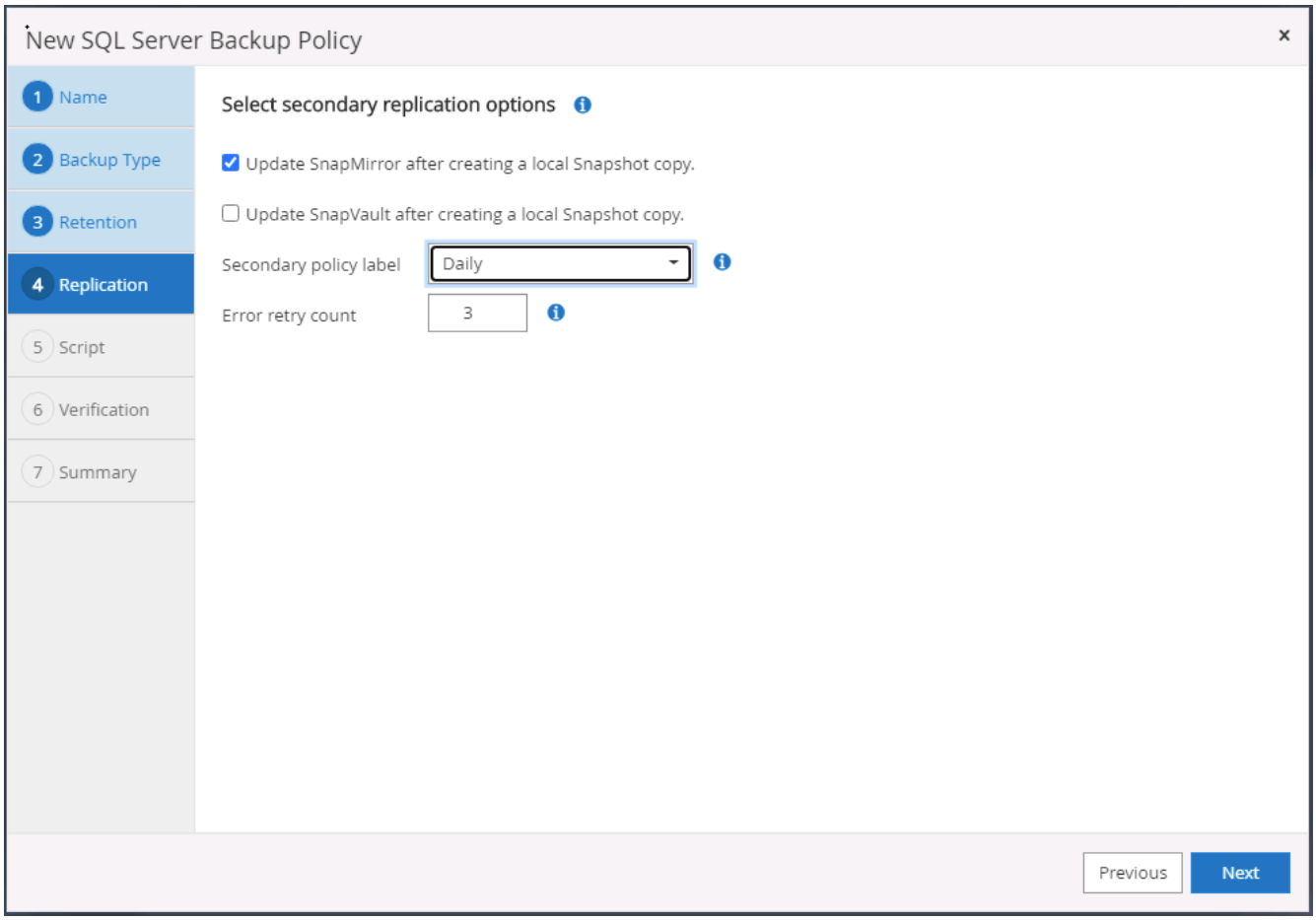
3. 백업 옵션 및 예약 빈도를 정의합니다. 가용성 그룹으로 구성된 SQL Server의 경우 기본 백업 복제본을 설정할 수 있습니다.



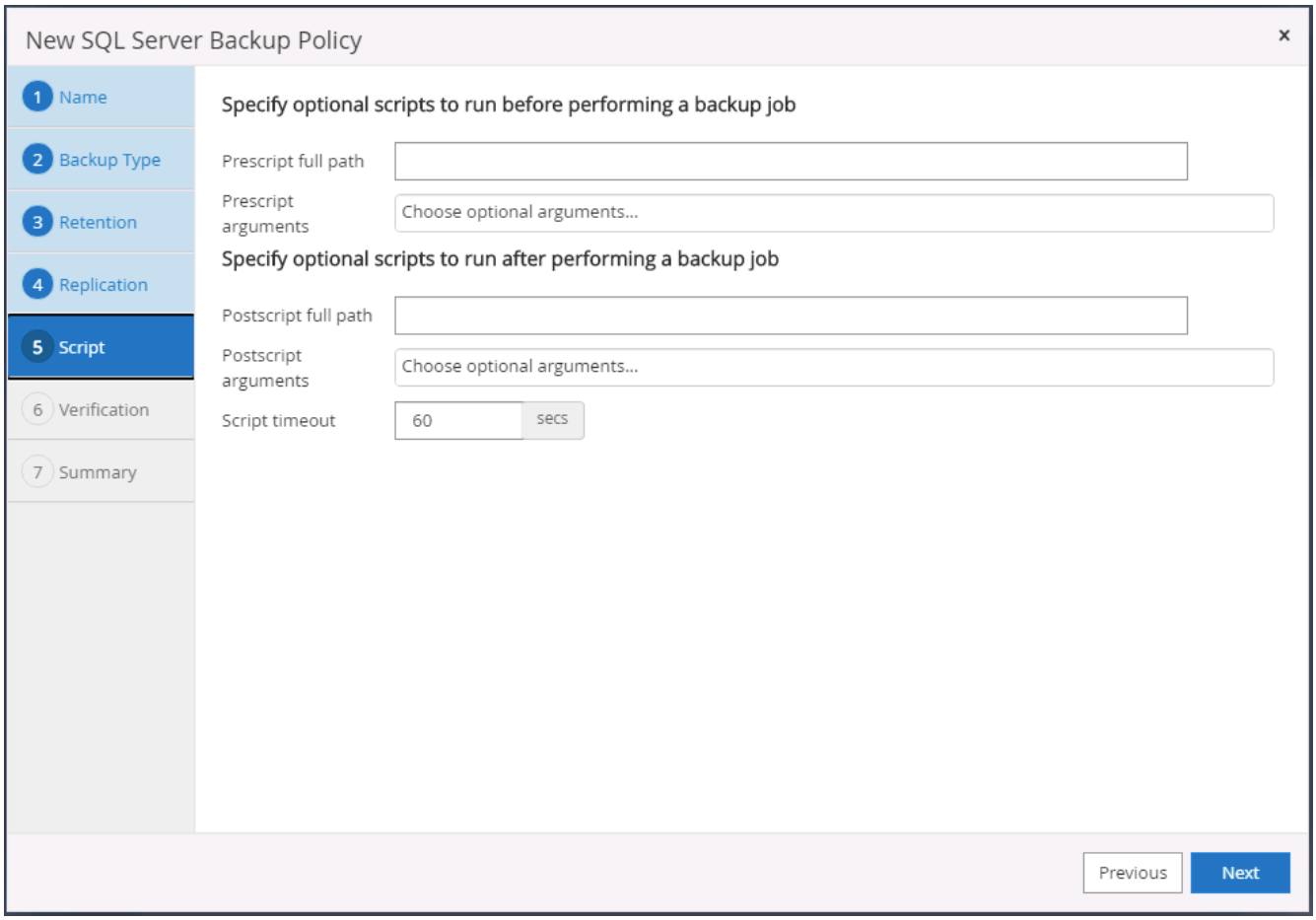
4. 백업 보존 기간을 설정합니다.



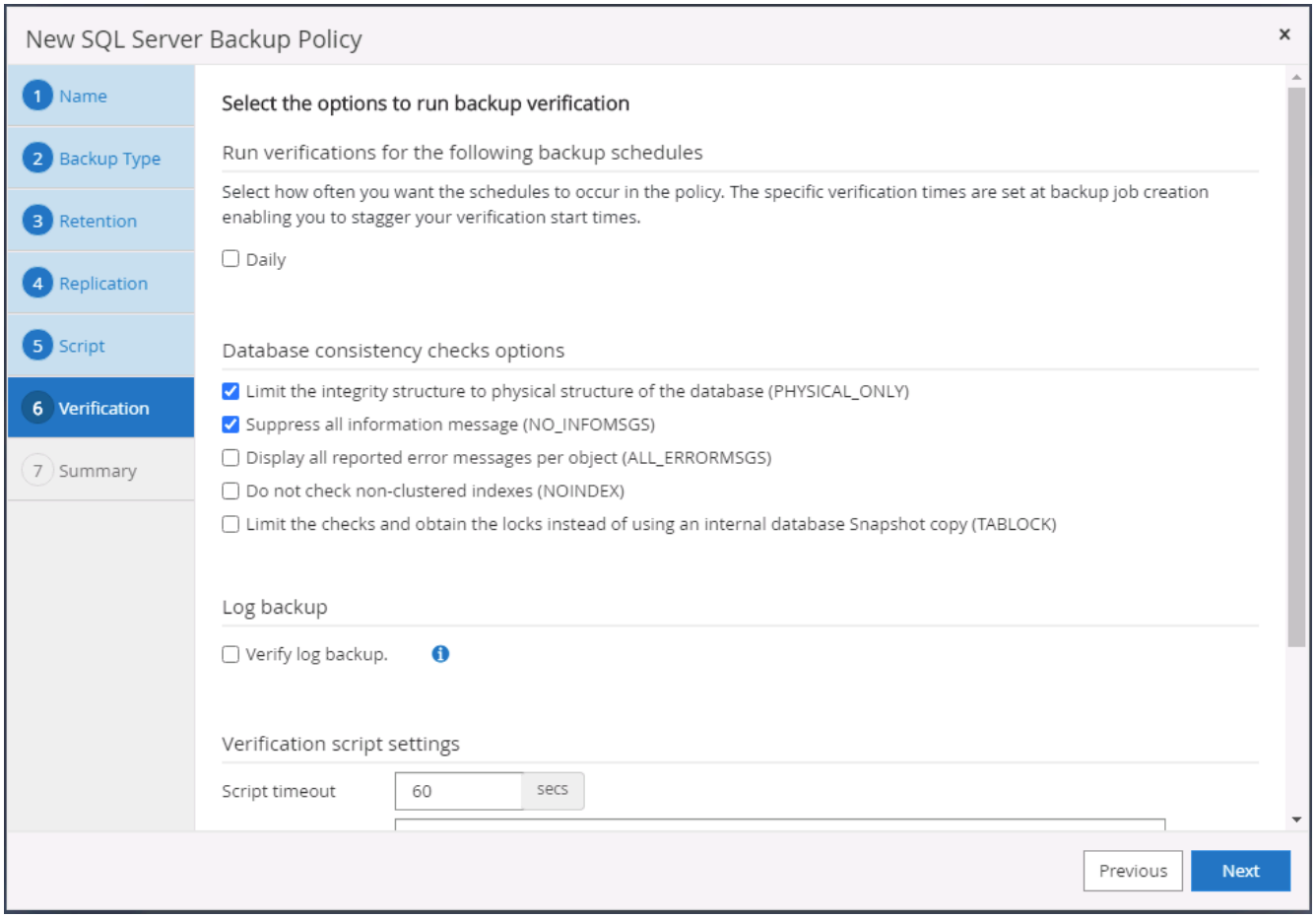
5. 클라우드의 2차 위치에 백업 복사본을 복제할 수 있습니다.



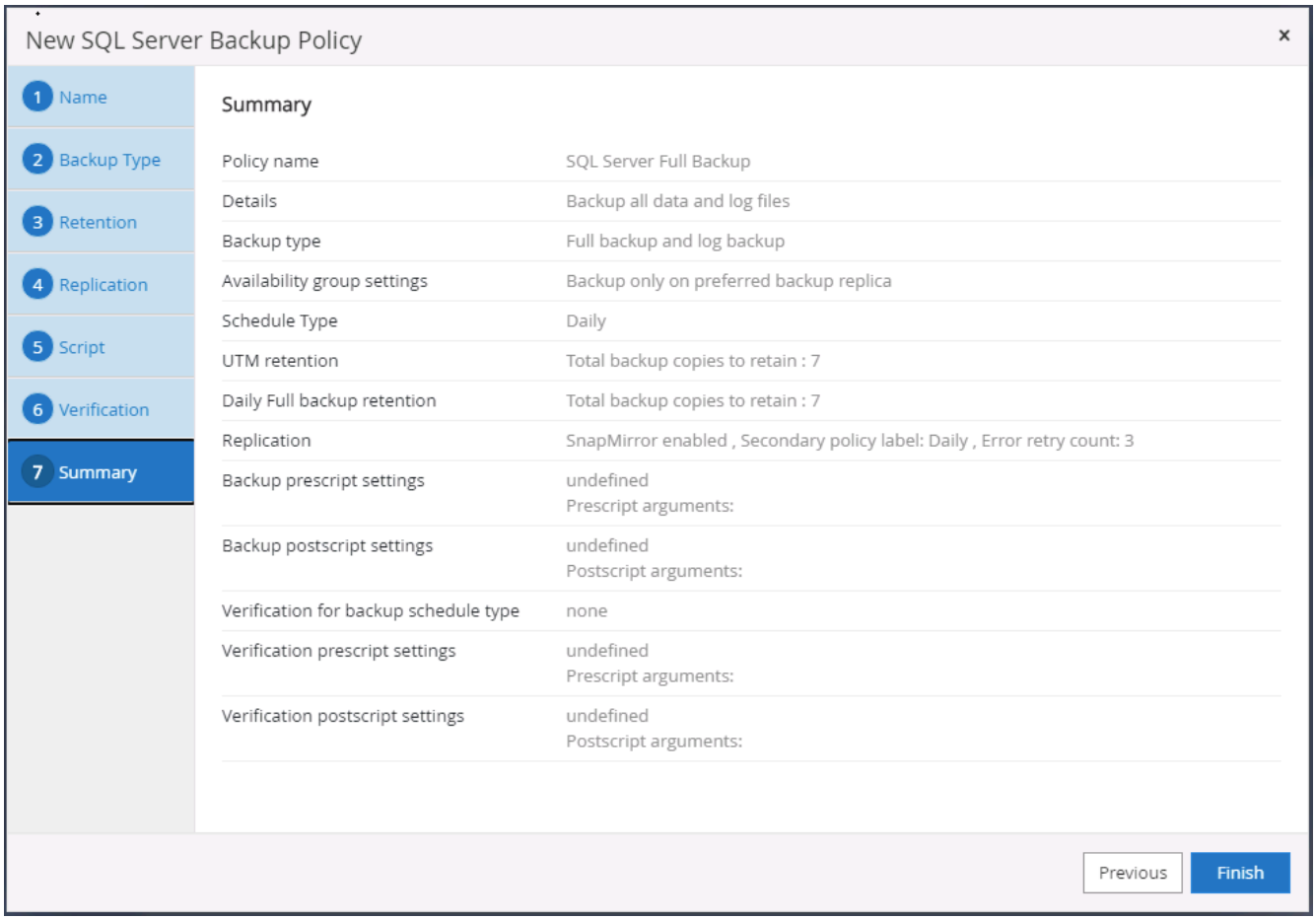
6. 백업 작업 전후에 실행할 선택적 스크립트를 지정합니다.



7. 백업 확인을 실행할 옵션을 지정합니다.

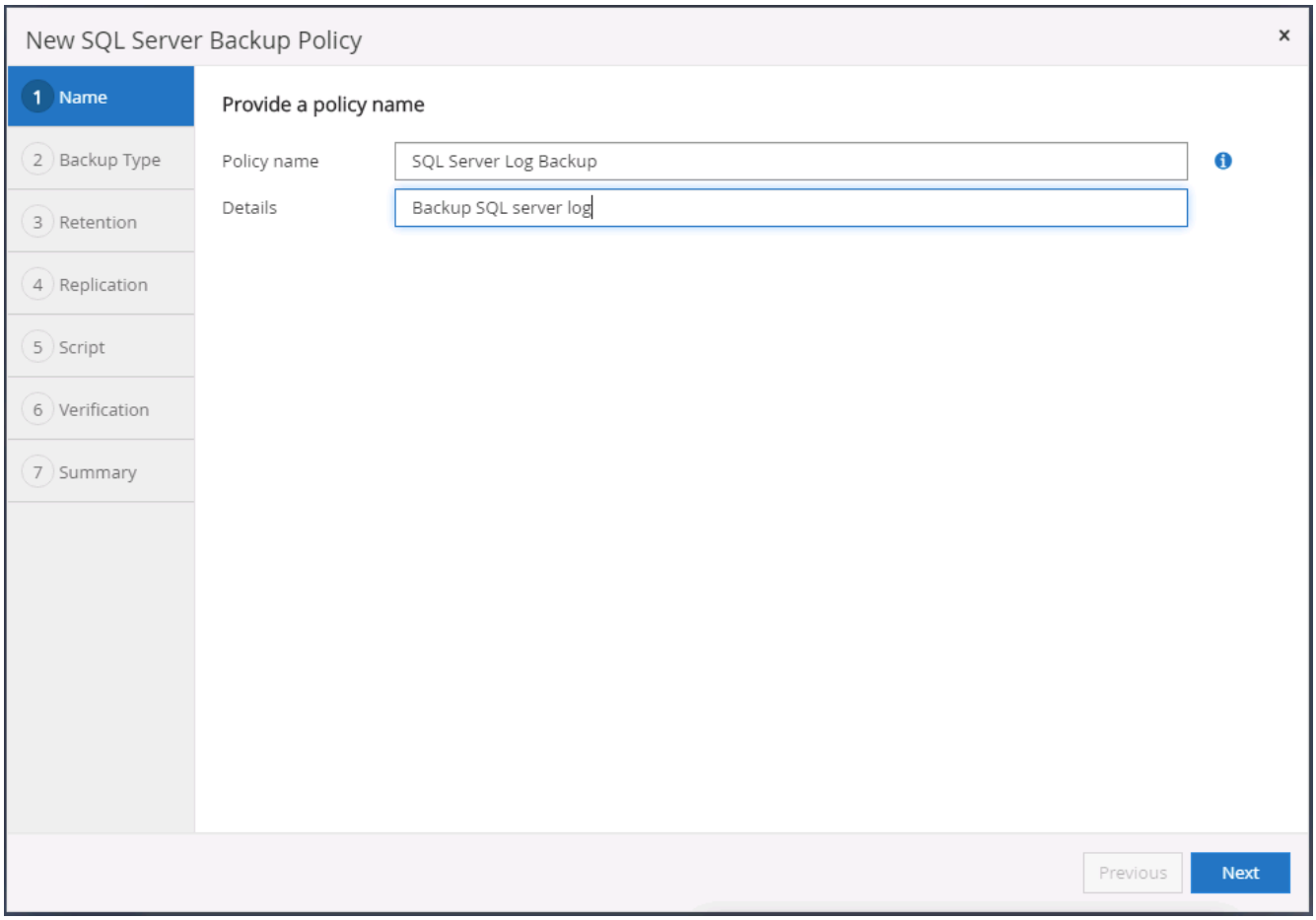

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Database consistency checks options
Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
Suppress all information message (NO_INFOMSGS)
Display all reported error messages per object (ALL_ERRORMSGS)
Do not check non-clustered indexes (NOINDEX)
Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)
Log backup
Verify log backup.
Verification script settings
Script timeout
60
secs
Previous
Next

8. 요약.

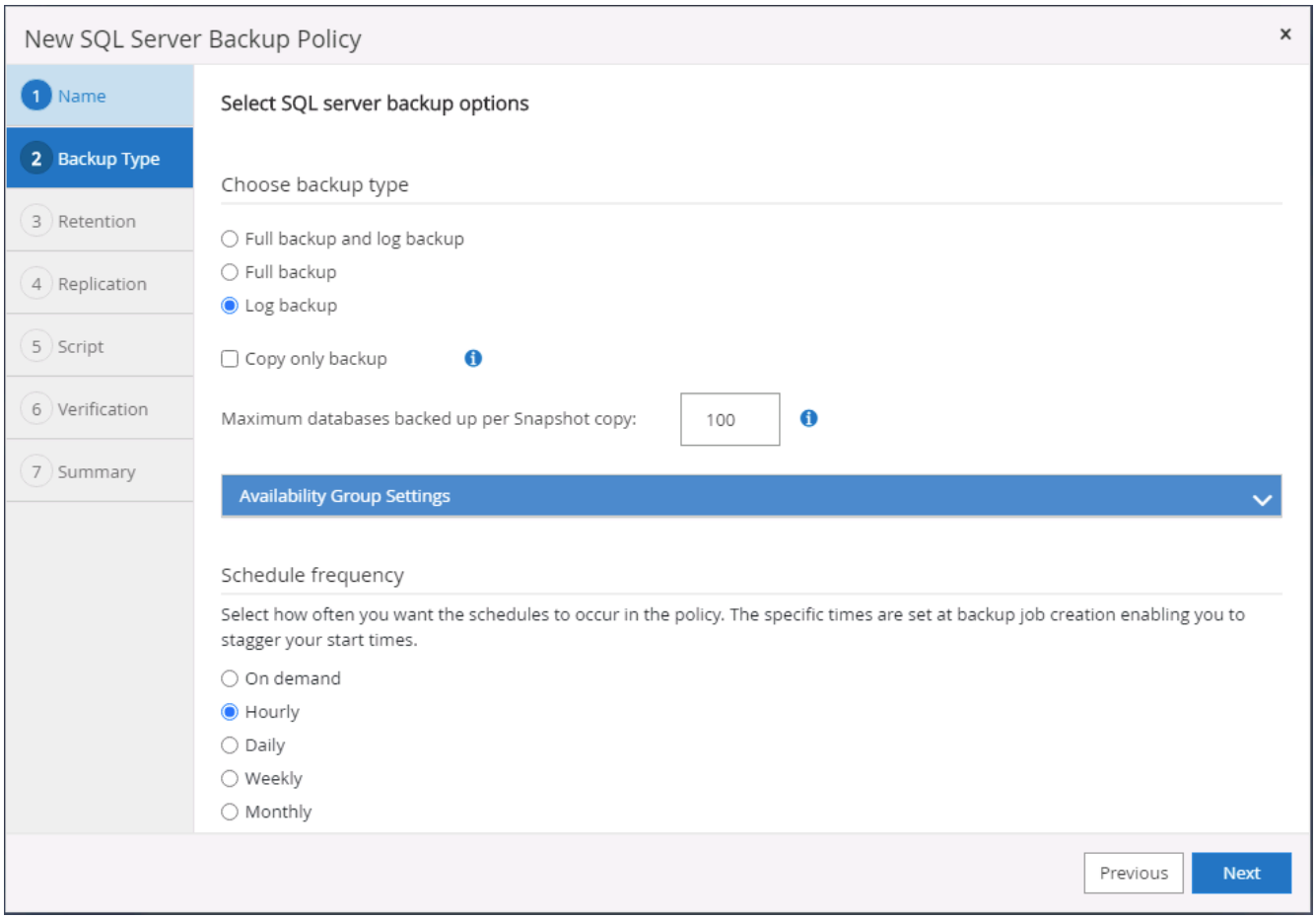


SQL에 대한 데이터베이스 로그 백업 정책을 생성합니다.

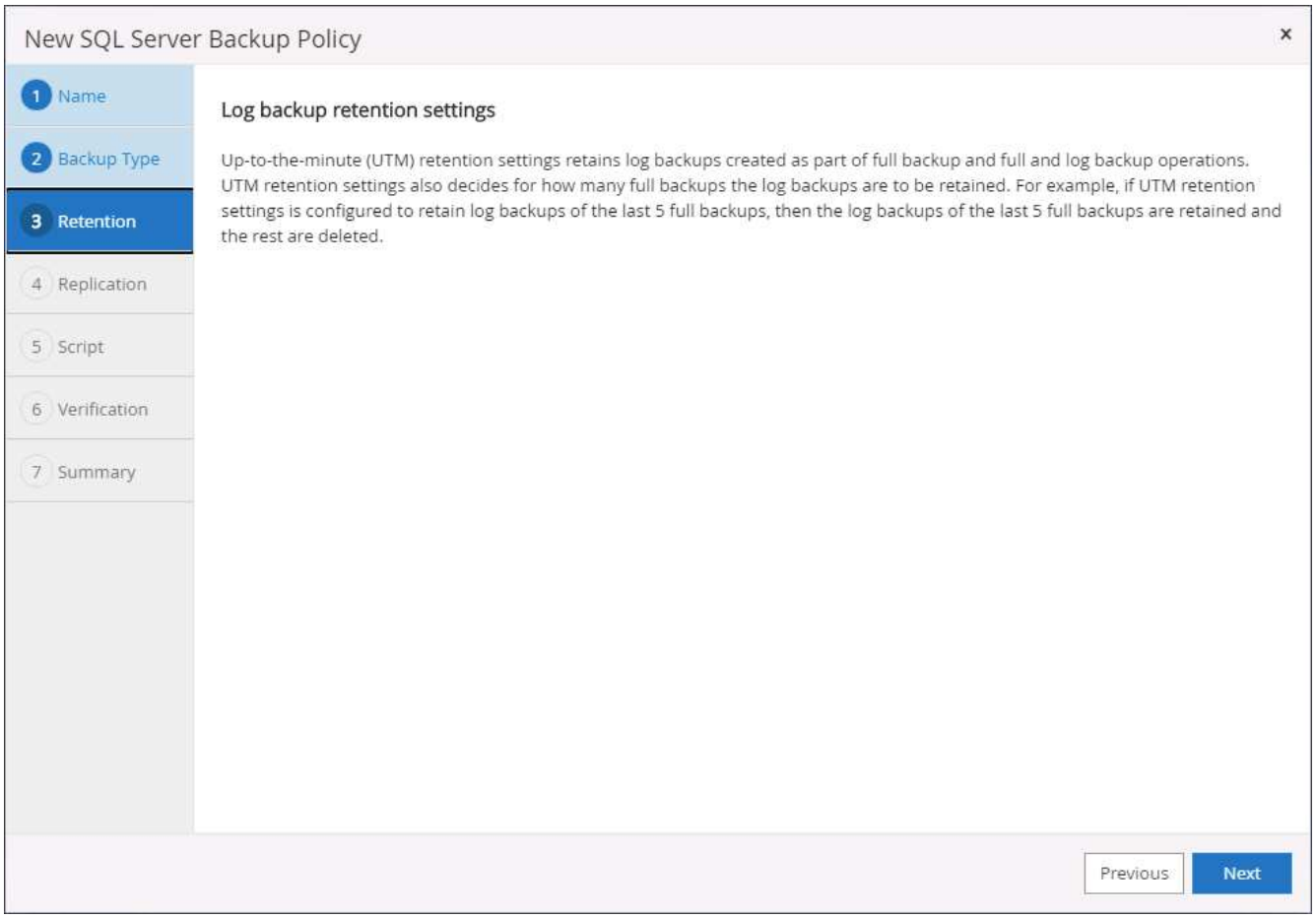
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 설정 > 정책 을 클릭한 다음 새로 만들기 를 클릭하여 새 정책 생성 워크플로를 시작합니다.



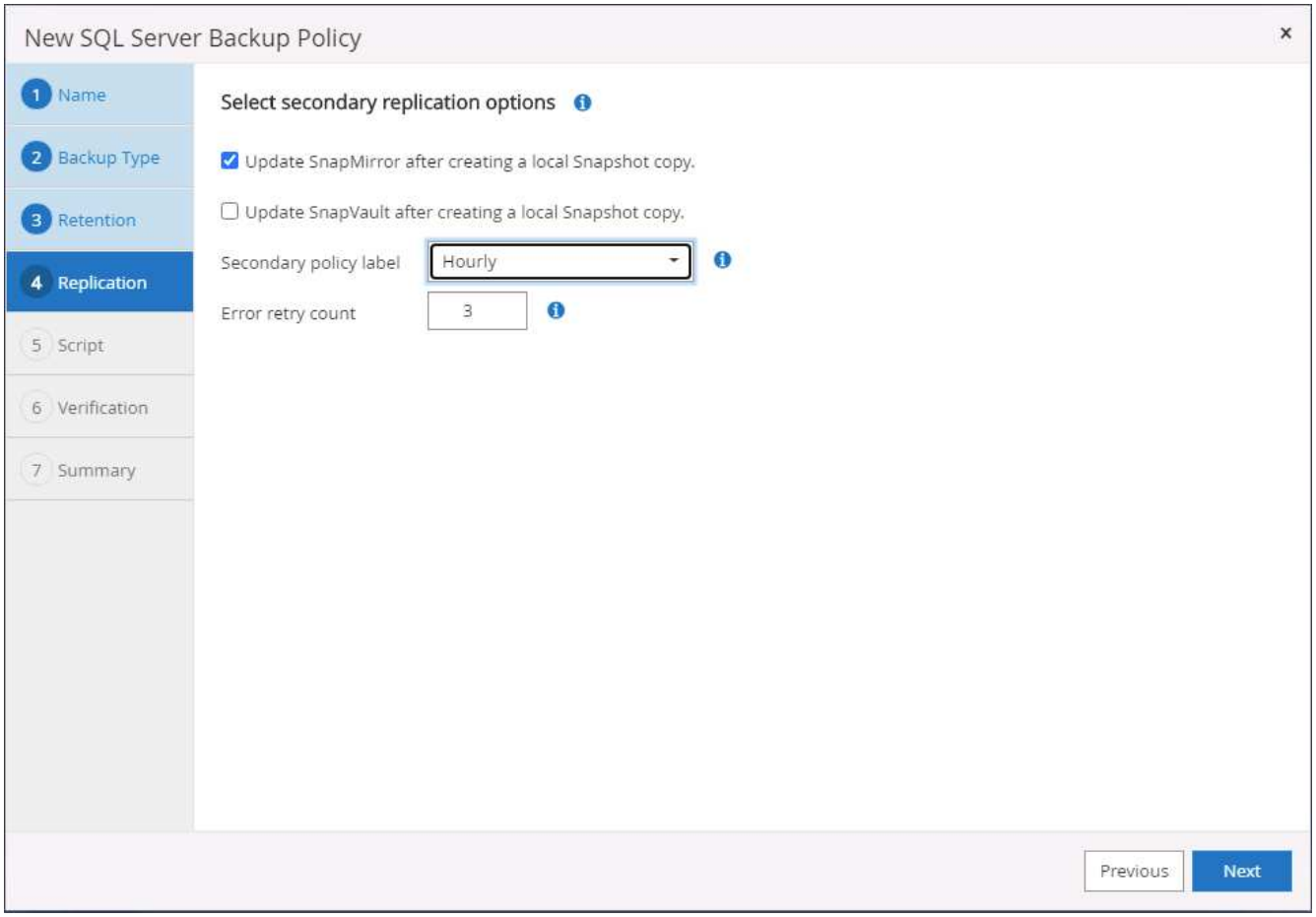
2. 로그 백업 옵션 및 스케줄 빈도를 정의합니다. 가용성 그룹으로 구성된 SQL Server의 경우 기본 백업 복제본을 설정할 수 있습니다.



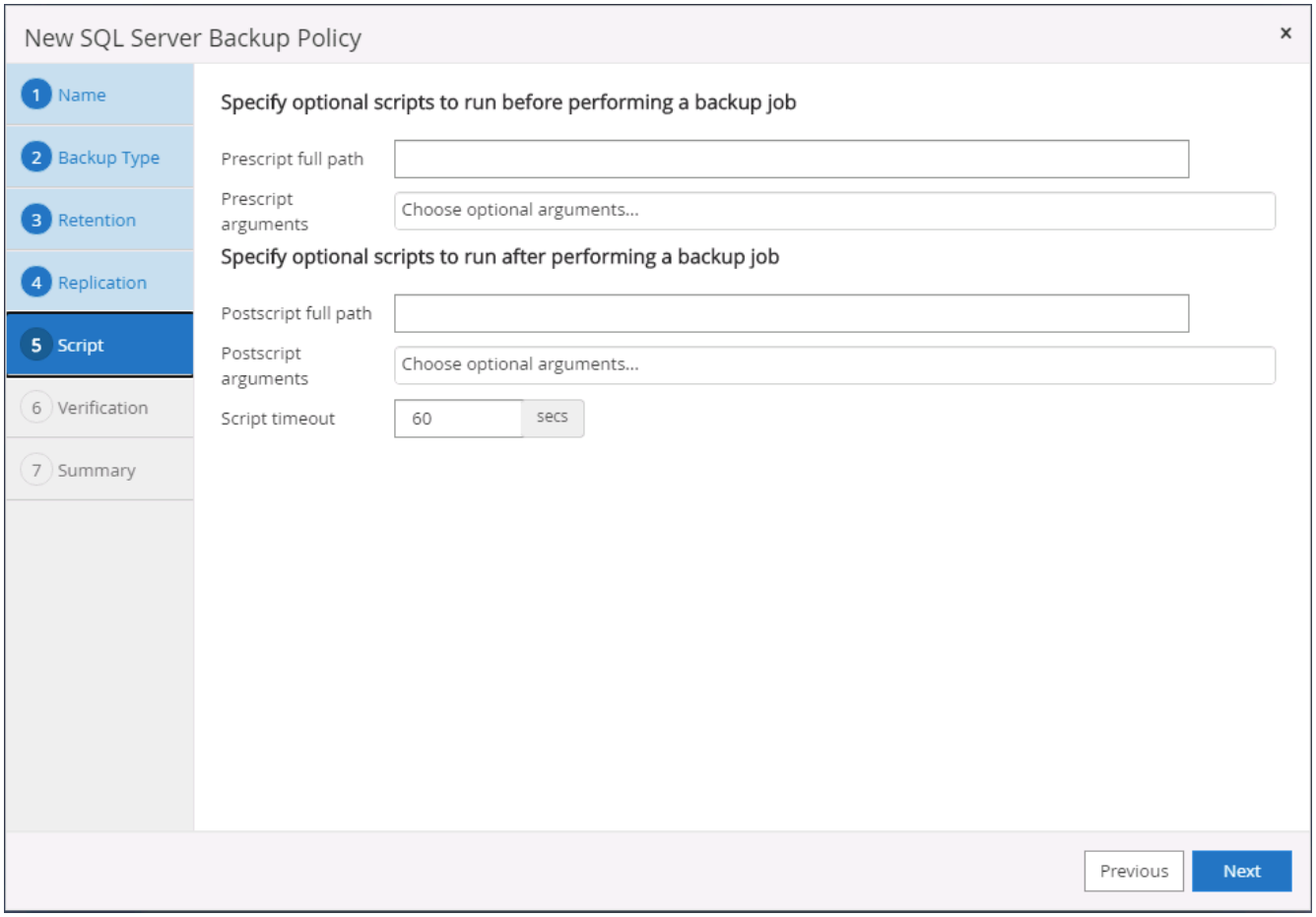
3. SQL Server 데이터 백업 정책은 로그 백업 보존을 정의합니다. 여기서 기본값을 사용합니다.



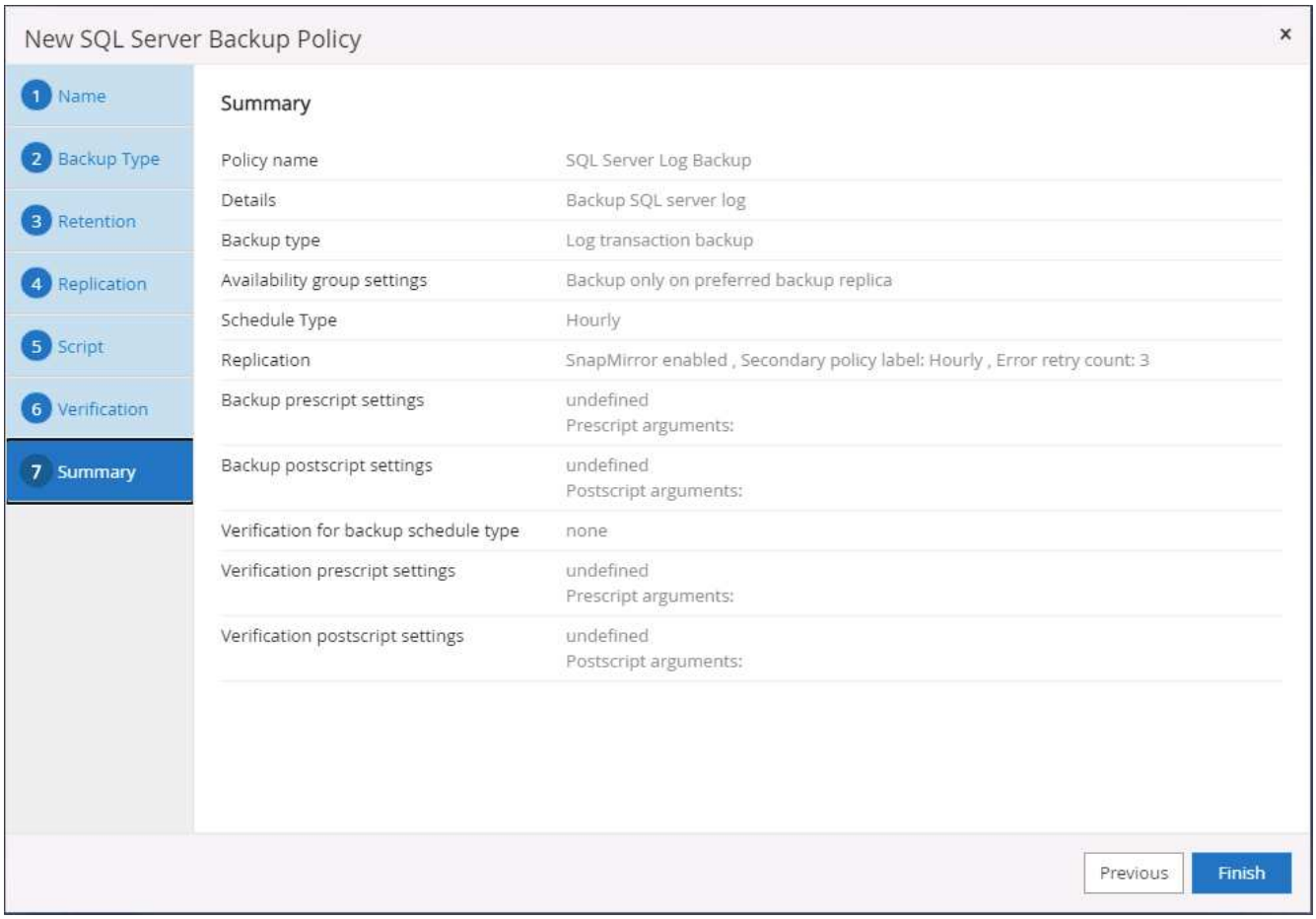
4. 클라우드의 2차 사이트에 로그 백업 복제를 설정합니다.



5. 백업 작업 전후에 실행할 선택적 스크립트를 지정합니다.


New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Specify optional scripts to run before performing a backup job
Prescript full path
Prescript arguments
Choose optional arguments...
Specify optional scripts to run after performing a backup job
Postscript full path
Postscript arguments
Choose optional arguments...
Script timeout
60
secs
Previous
Next

6. 요약.

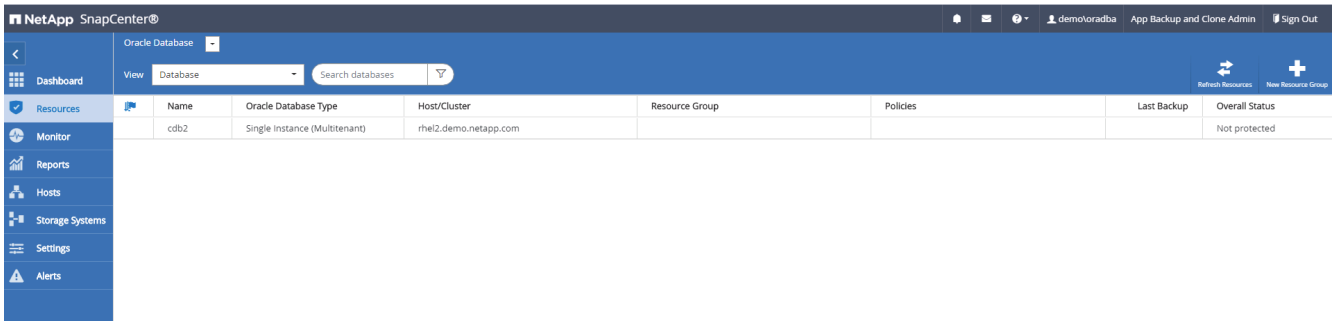


데이터베이스를 보호하기 위해 백업 정책을 구현합니다

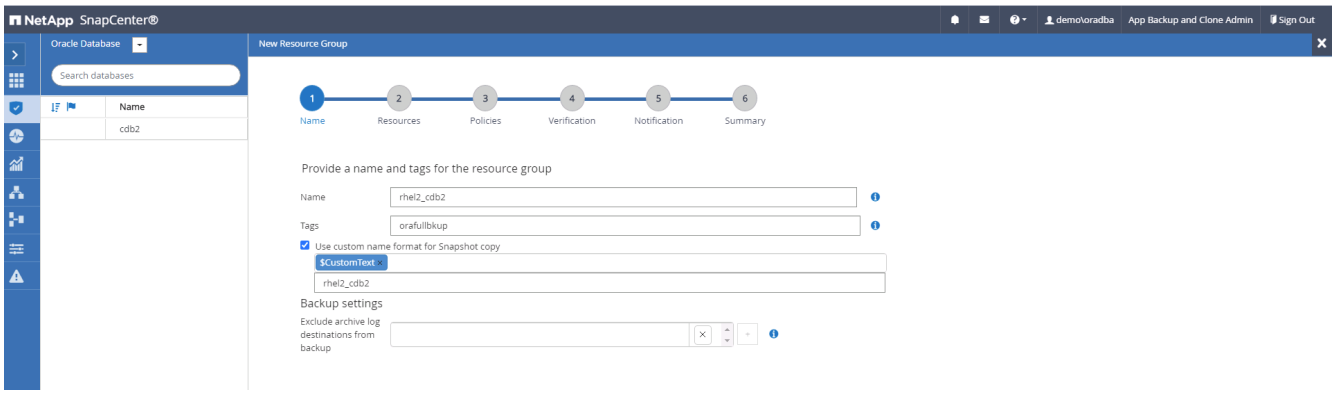
SnapCenter는 리소스 그룹을 사용하여 서버에서 호스팅되는 여러 데이터베이스, 동일한 스토리지 볼륨을 공유하는 데이터베이스, 비즈니스 애플리케이션을 지원하는 여러 데이터베이스 등 데이터베이스 리소스의 논리적 그룹으로 데이터베이스를 백업합니다. 단일 데이터베이스를 보호하면 고유한 리소스 그룹이 만들어집니다. 다음 절차에서는 Oracle 및 SQL Server 데이터베이스를 보호하기 위해 섹션 7에서 만든 백업 정책을 구현하는 방법을 보여 줍니다.

Oracle의 전체 백업을 위한 리소스 그룹을 생성합니다

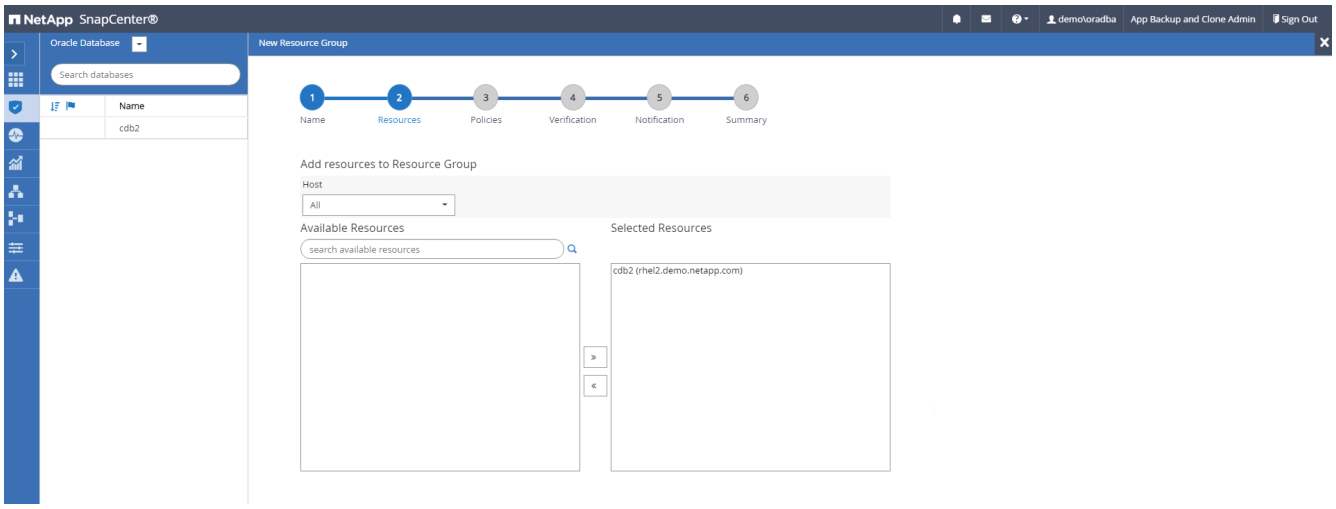
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 리소스 탭으로 이동합니다. 보기 드롭다운 목록에서 데이터베이스 또는 리소스 그룹을 선택하여 리소스 그룹 만들기 워크플로를 시작합니다.



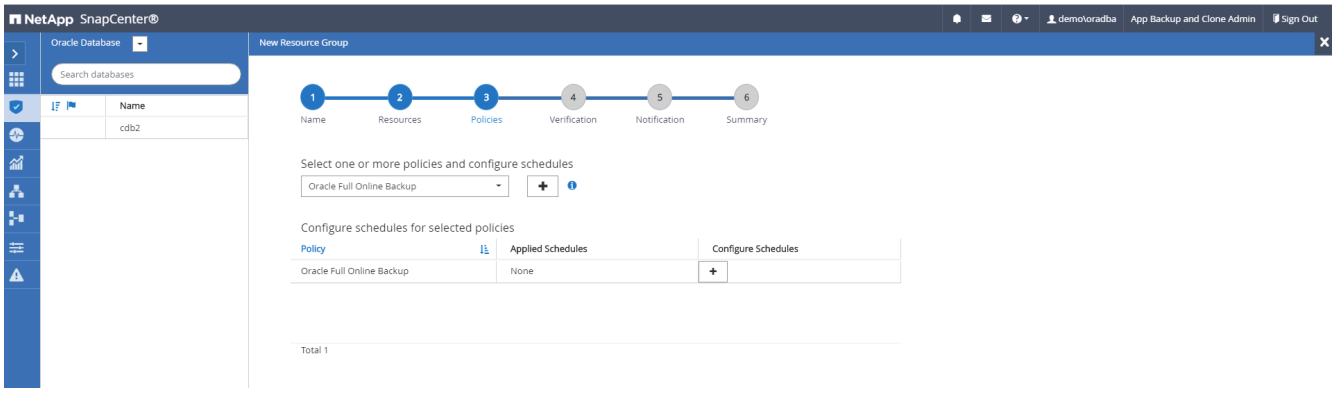
2. 리소스 그룹의 이름과 태그를 입력합니다. 스냅샷 복사본의 명명 형식을 정의하고 구성된 경우 중복 아카이브 로그 대상을 건너뛸 수 있습니다.



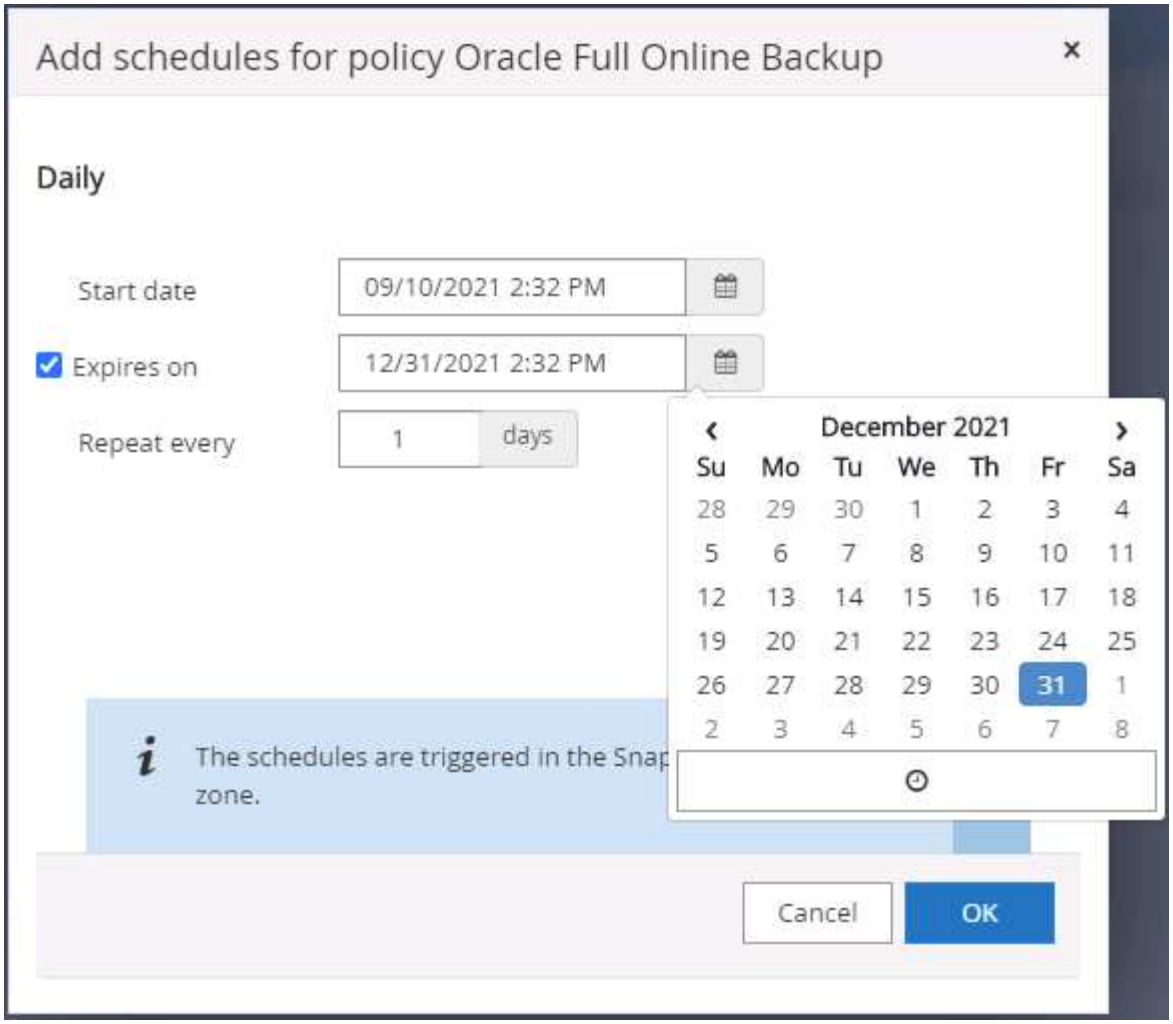
3. 리소스 그룹에 데이터베이스 리소스를 추가합니다.



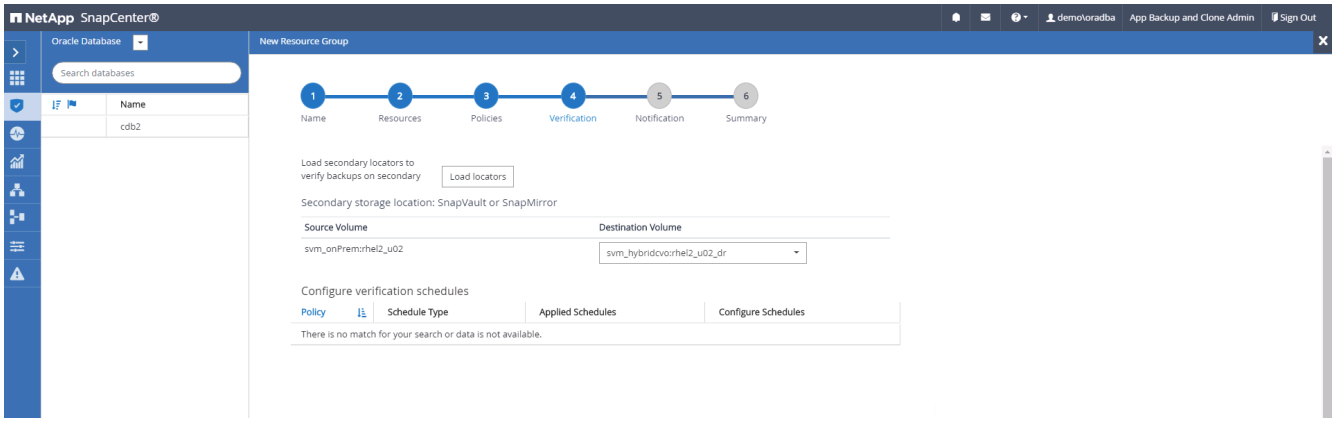
4. 드롭다운 목록에서 섹션 7에 생성된 전체 백업 정책을 선택합니다.



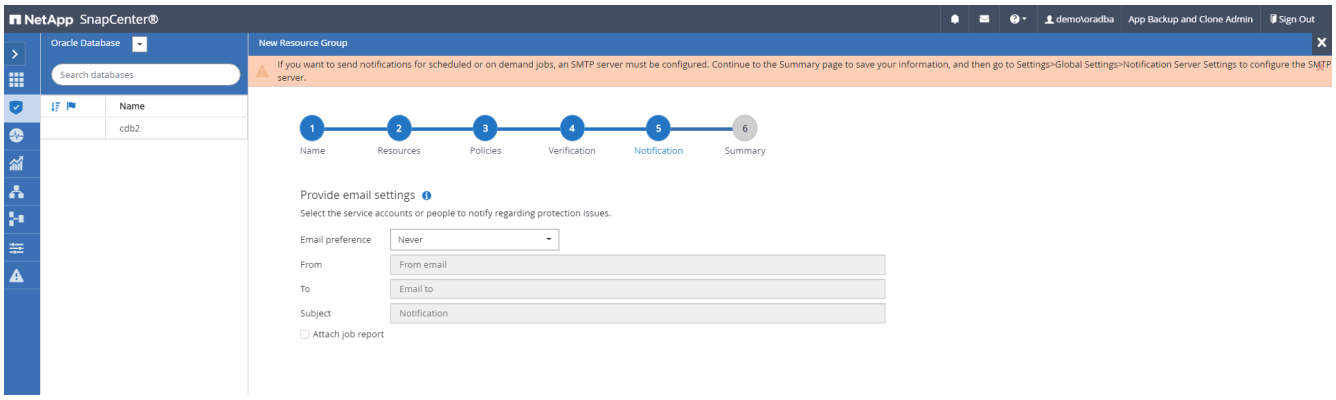
5. (+) 기호를 클릭하여 원하는 백업 일정을 구성합니다.



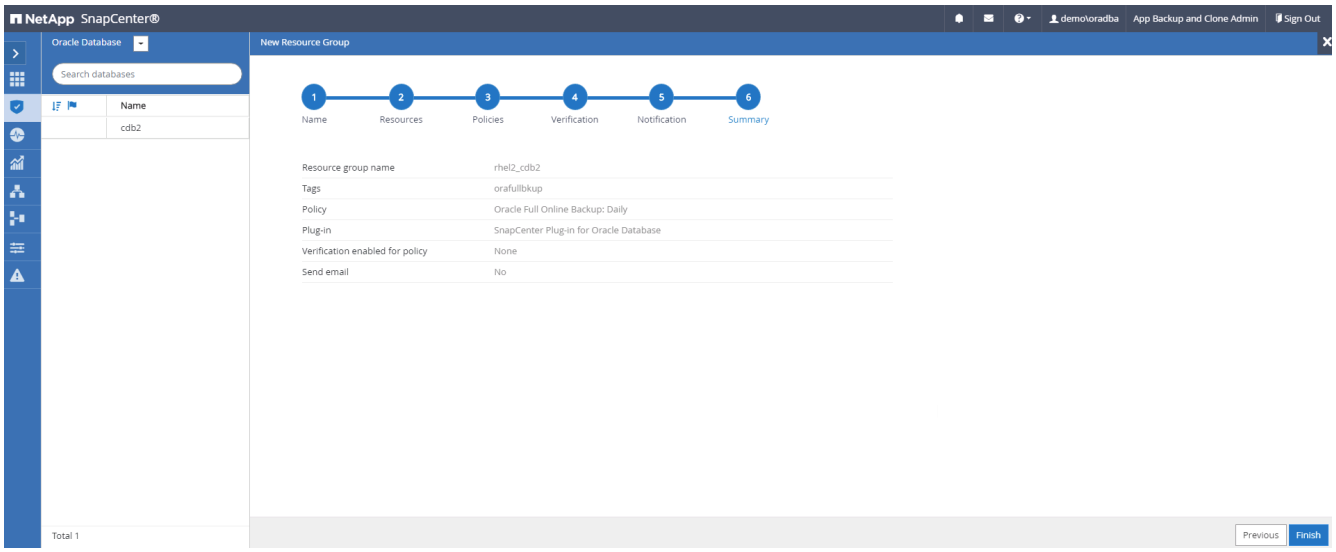
6. Load Locators(로케이터 로드) 를 클릭하여 소스 및 대상 볼륨을 로드합니다.



7. 필요한 경우 이메일 알림에 사용할 SMTP 서버를 구성합니다.

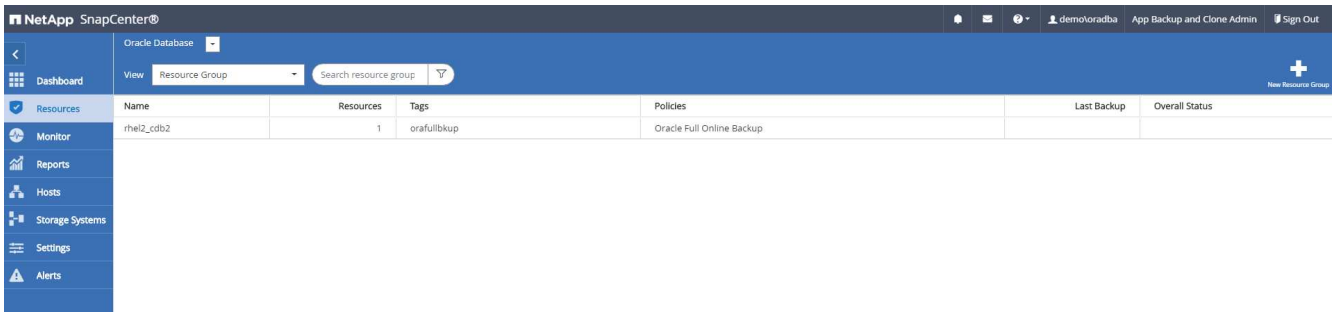


8. 요약.

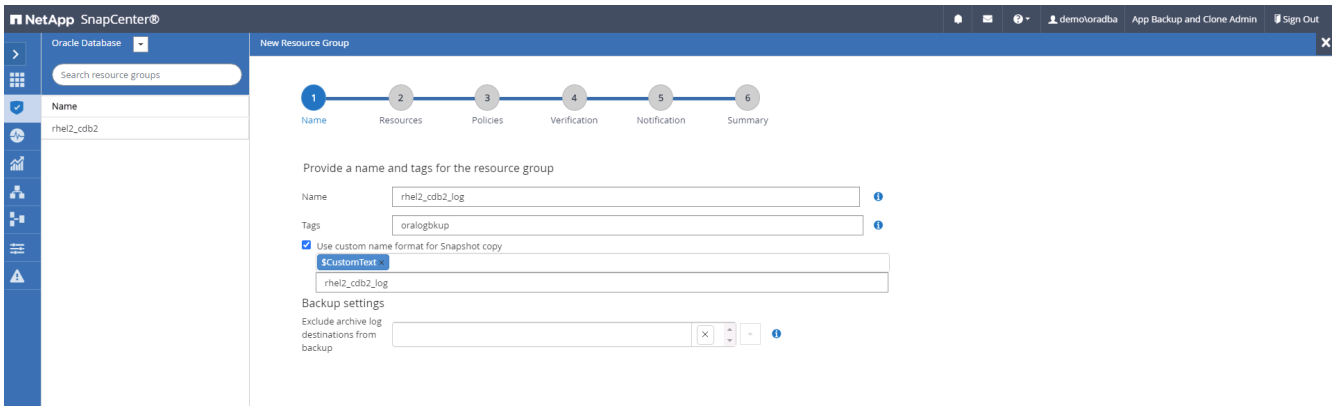


Oracle의 로그 백업을 위한 리소스 그룹을 생성합니다

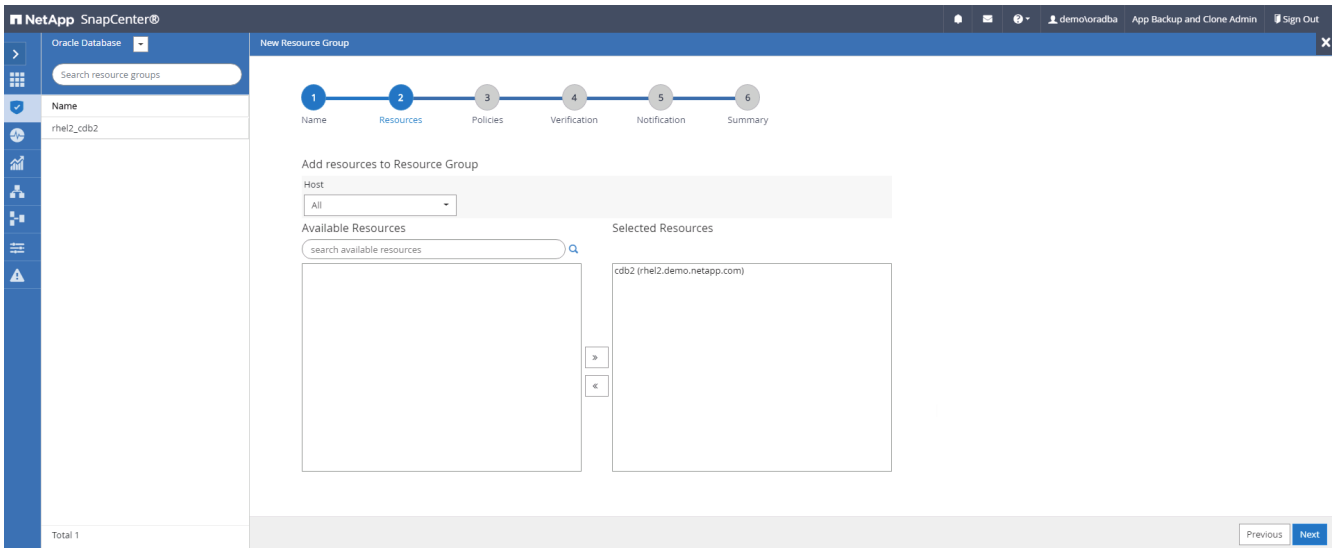
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 리소스 탭으로 이동합니다. 보기 드롭다운 목록에서 데이터베이스 또는 리소스 그룹을 선택하여 리소스 그룹 만들기 워크플로를 시작합니다.



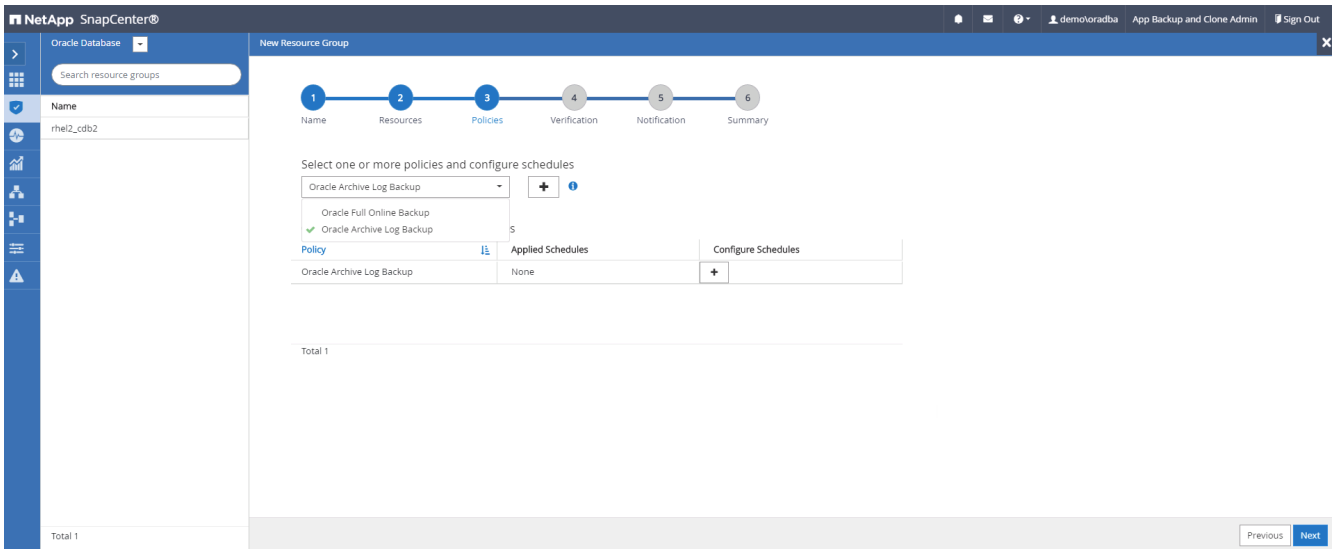
2. 리소스 그룹의 이름과 태그를 입력합니다. 스냅샷 복사본의 명명 형식을 정의하고 구성된 경우 중복 아카이브 로그 대상을 건너뛸 수 있습니다.



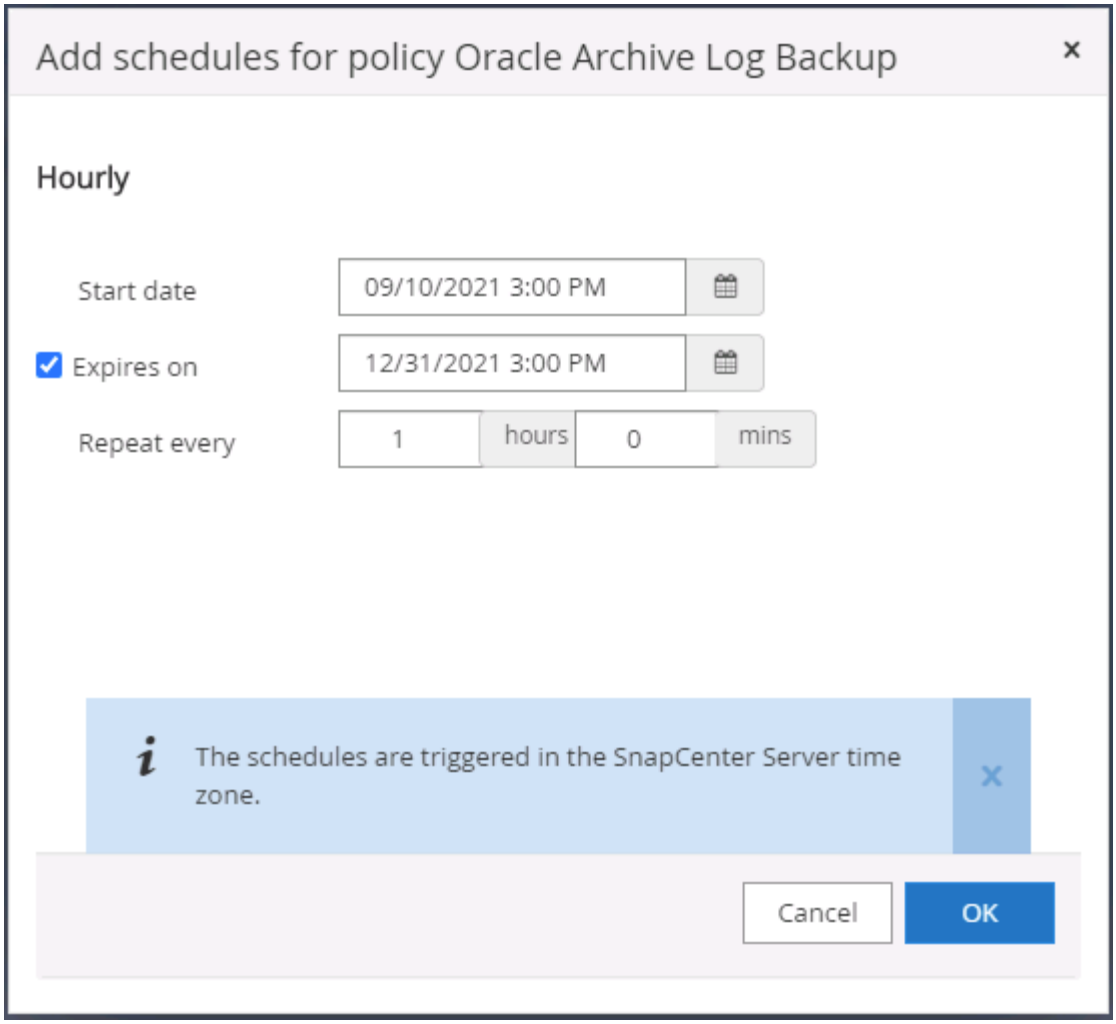
3. 리소스 그룹에 데이터베이스 리소스를 추가합니다.



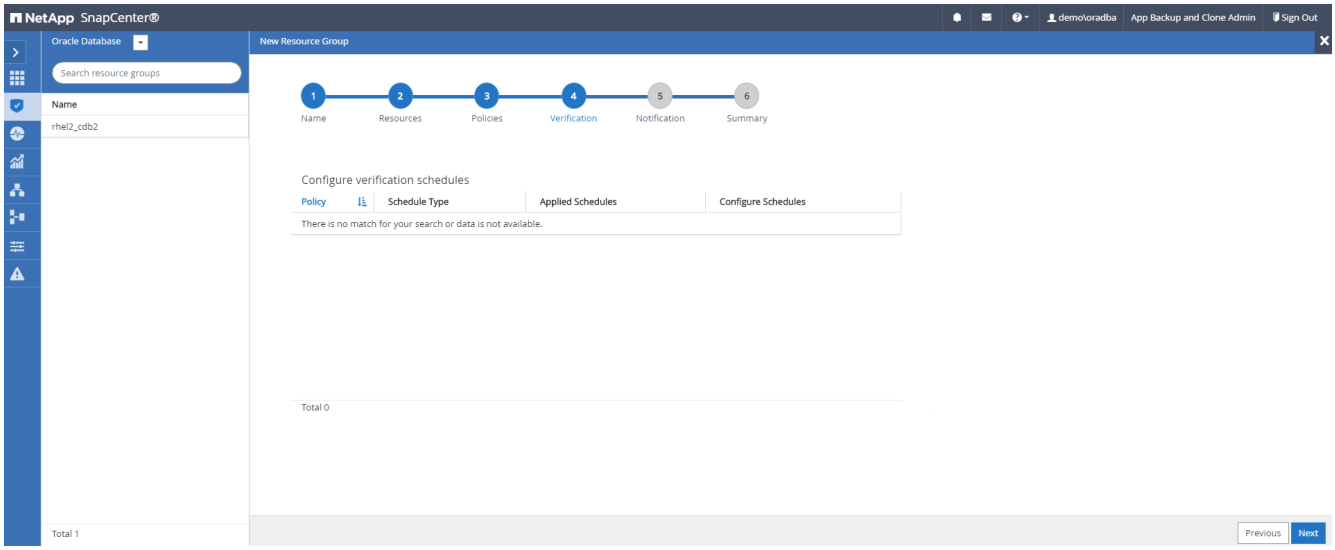
4. 드롭다운 목록에서 섹션 7에 생성된 로그 백업 정책을 선택합니다.



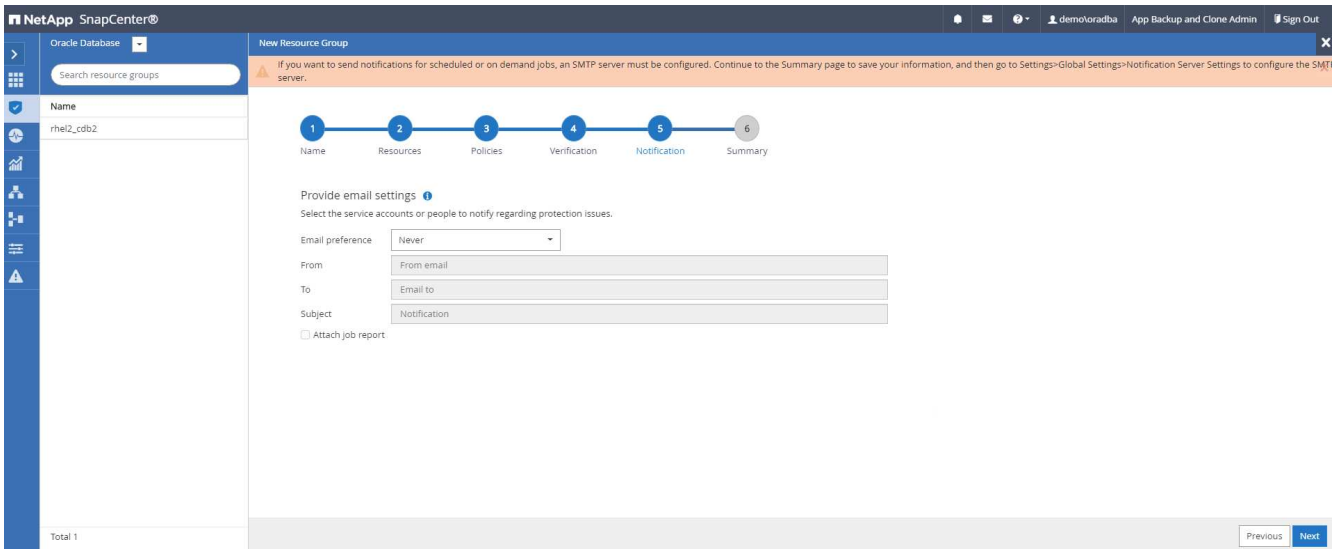
5. (+) 기호를 클릭하여 원하는 백업 일정을 구성합니다.



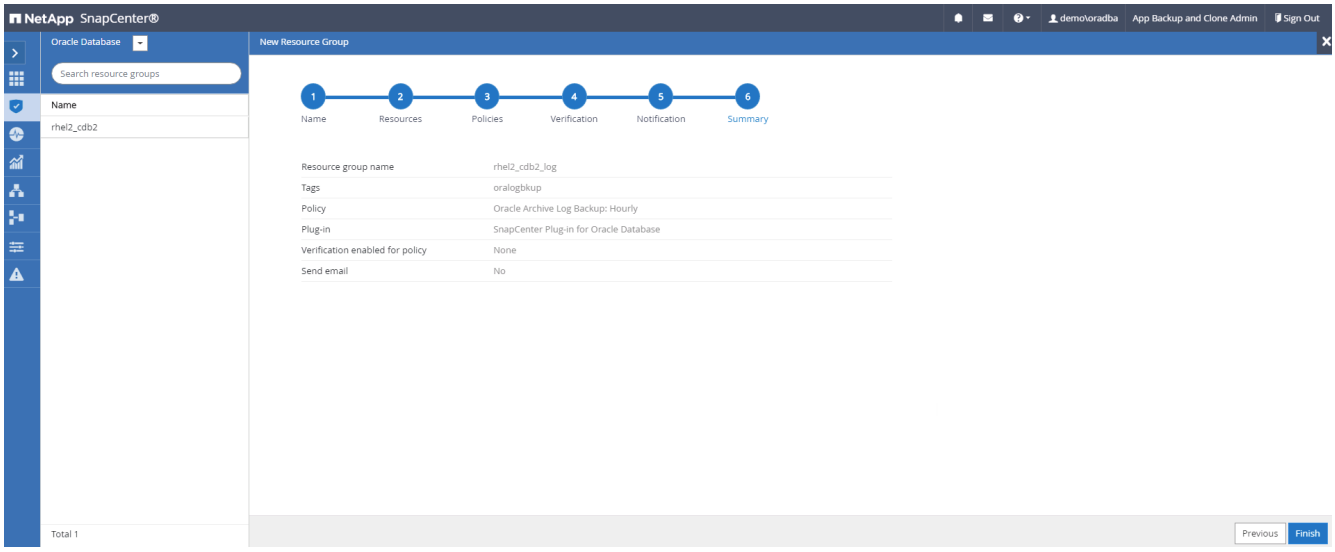
6. 백업 검증이 구성된 경우 여기에 표시됩니다.



7. 필요한 경우 e-메일 알림을 위한 SMTP 서버를 구성합니다.

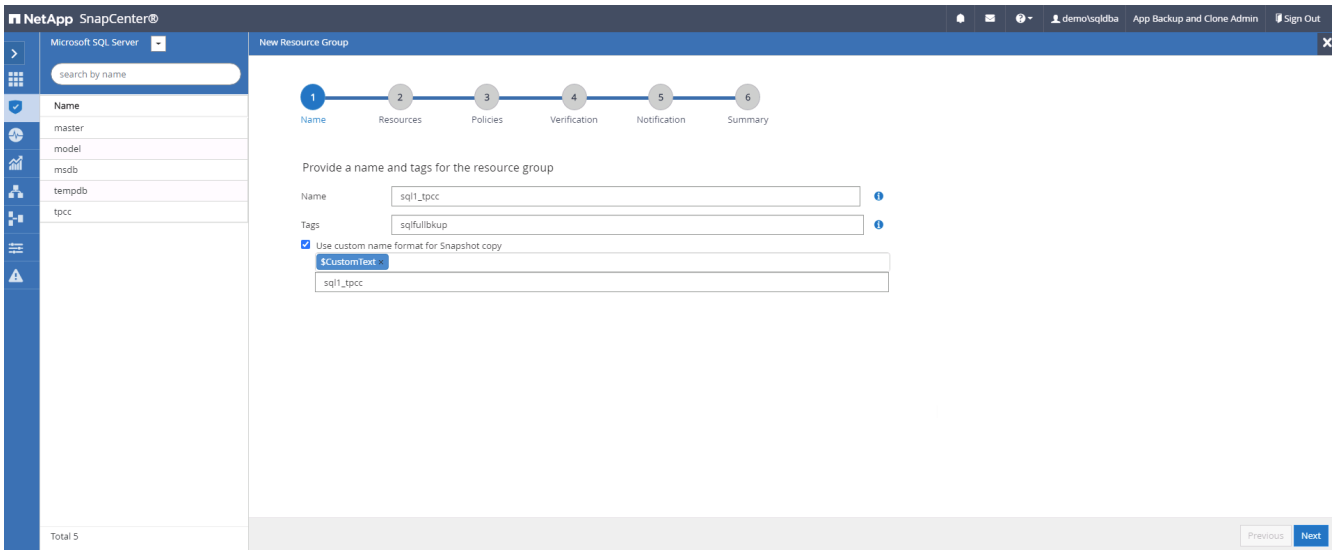


8. 요약.

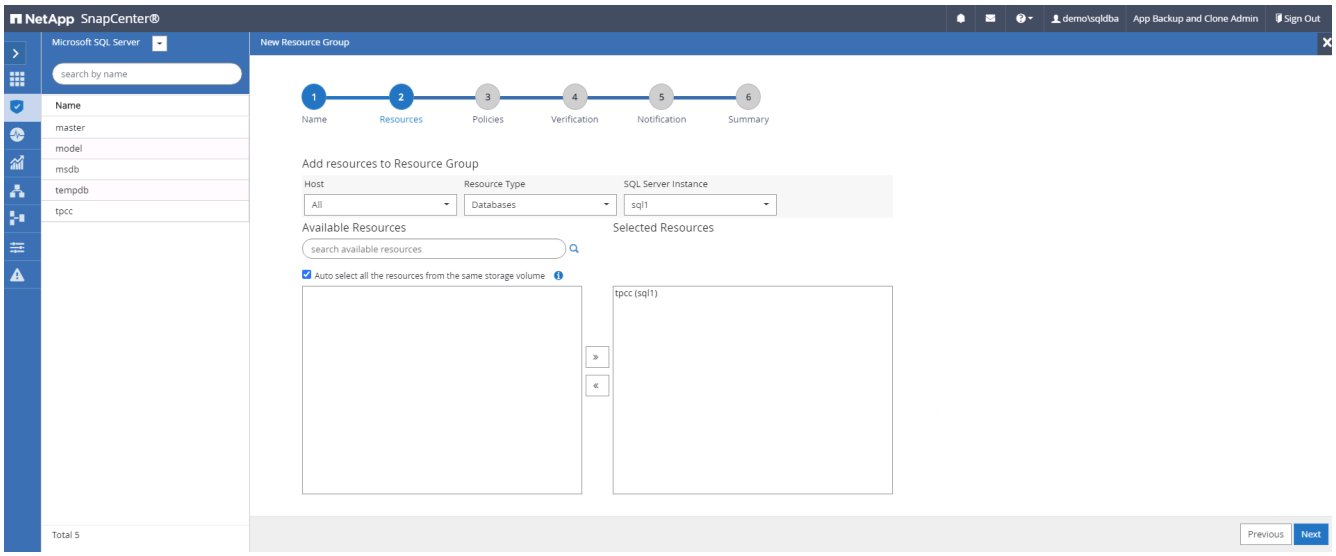


SQL Server의 전체 백업을 위한 리소스 그룹을 생성합니다

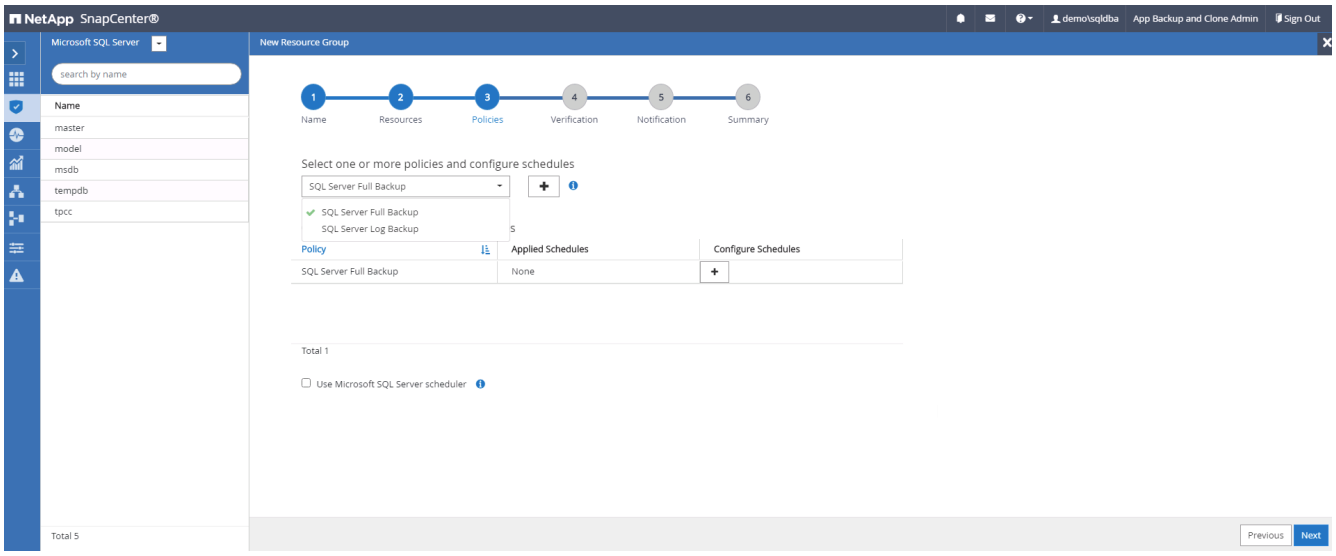
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 리소스 탭으로 이동합니다. 보기 드롭다운 목록에서 데이터베이스 또는 리소스 그룹을 선택하여 리소스 그룹 만들기 워크플로를 시작합니다. 리소스 그룹의 이름과 태그를 입력합니다. 스냅샷 복사본의 명명 형식을 정의할 수 있습니다.



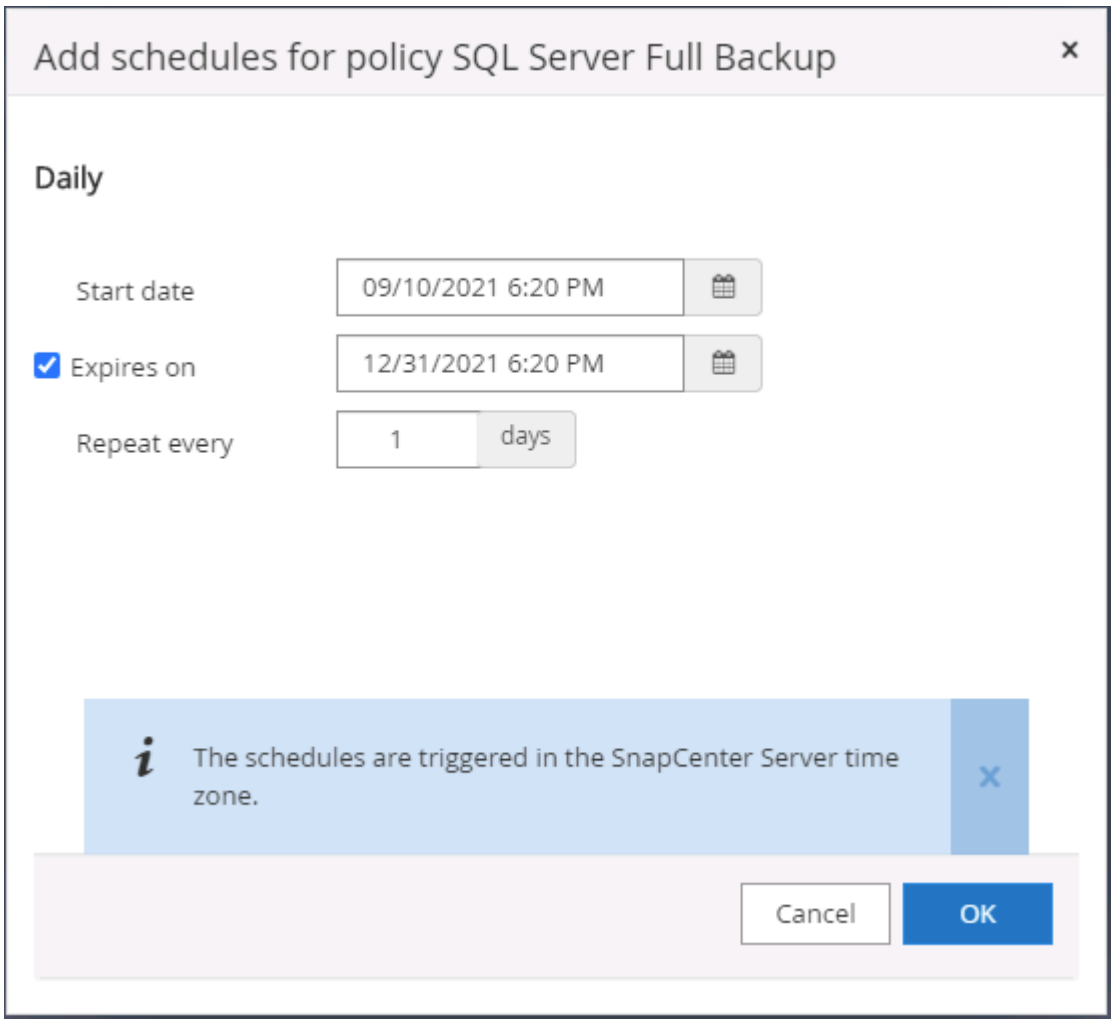
2. 백업할 데이터베이스 리소스를 선택합니다.



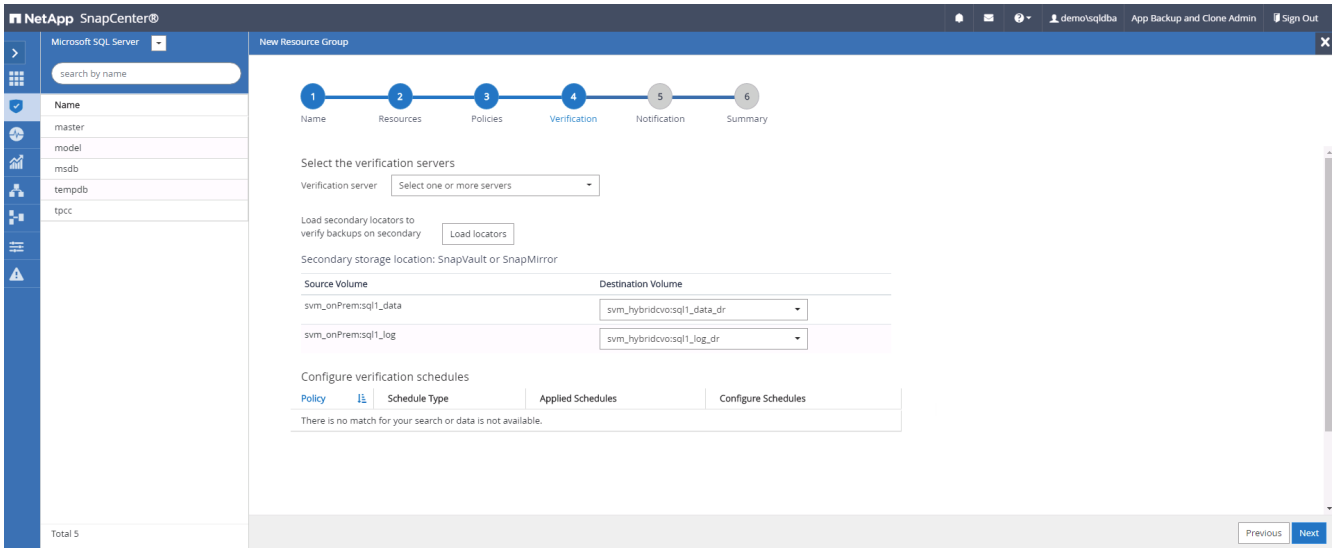
3. 섹션 7에서 생성한 전체 SQL 백업 정책을 선택합니다.



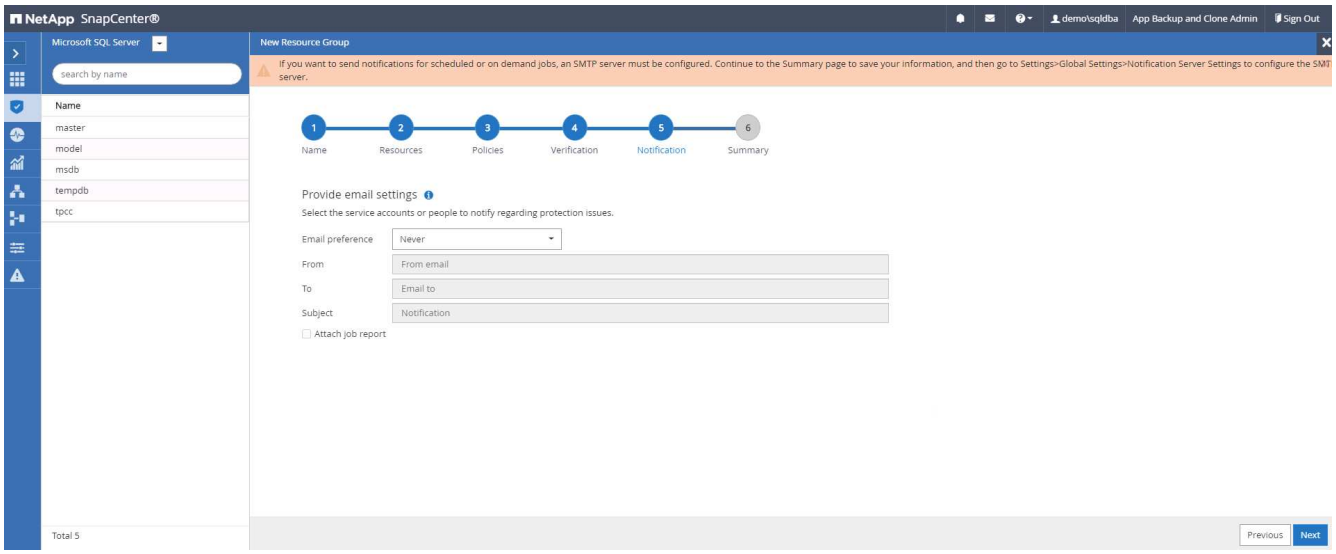
4. 백업 빈도와 정확한 백업 시간을 추가합니다.



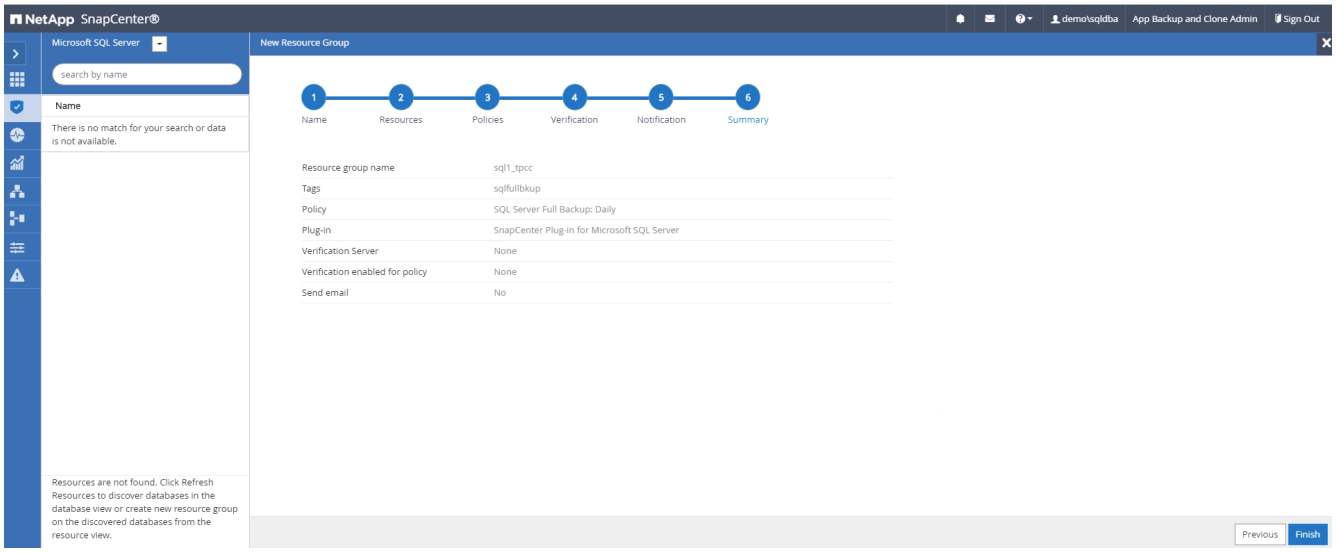
5. 백업 확인을 수행할 경우 보조 백업에 대한 검증 서버를 선택합니다. Load Locator를 클릭하여 보조 스토리지 위치를 채웁니다.



6. 필요한 경우 이메일 알림에 사용할 SMTP 서버를 구성합니다.

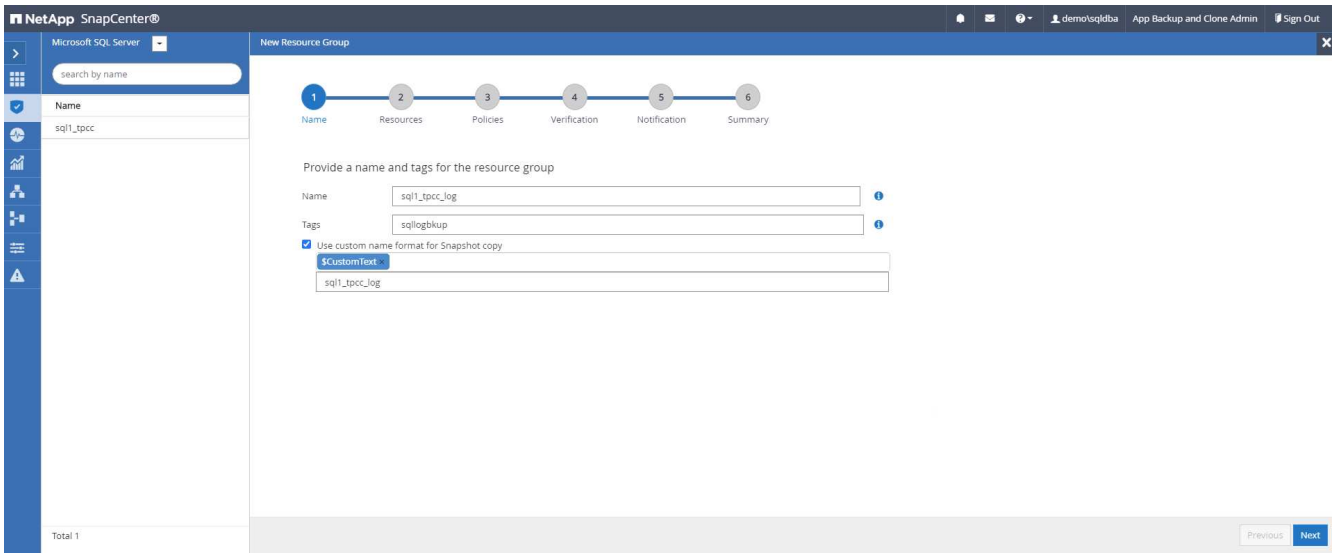


7. 요약.

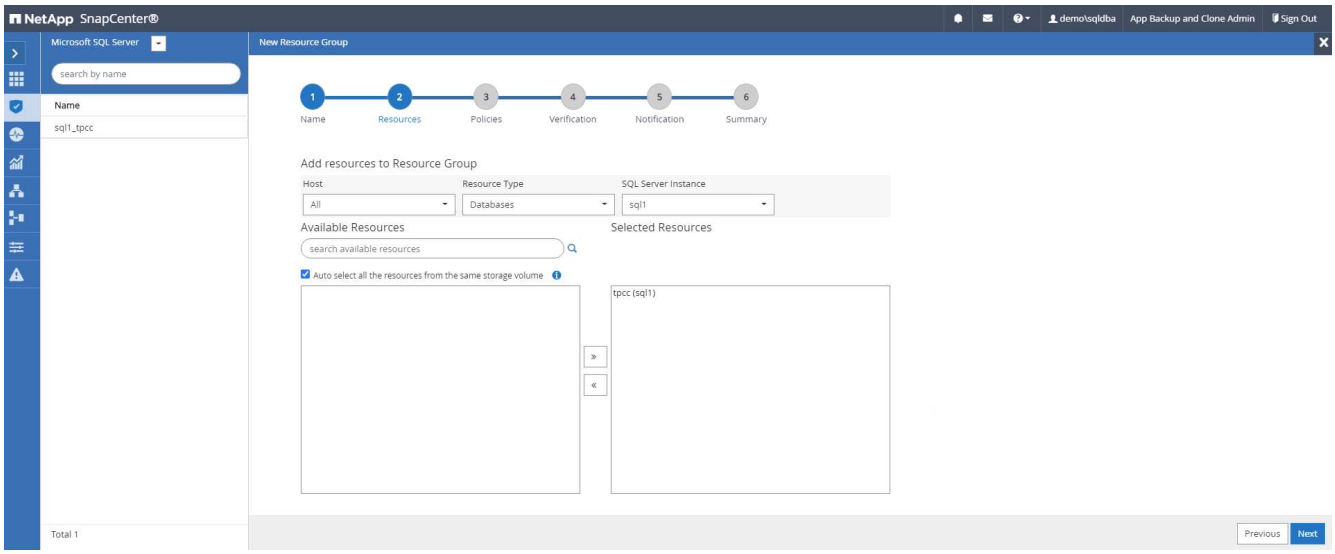


SQL Server의 로그 백업을 위한 리소스 그룹을 생성합니다

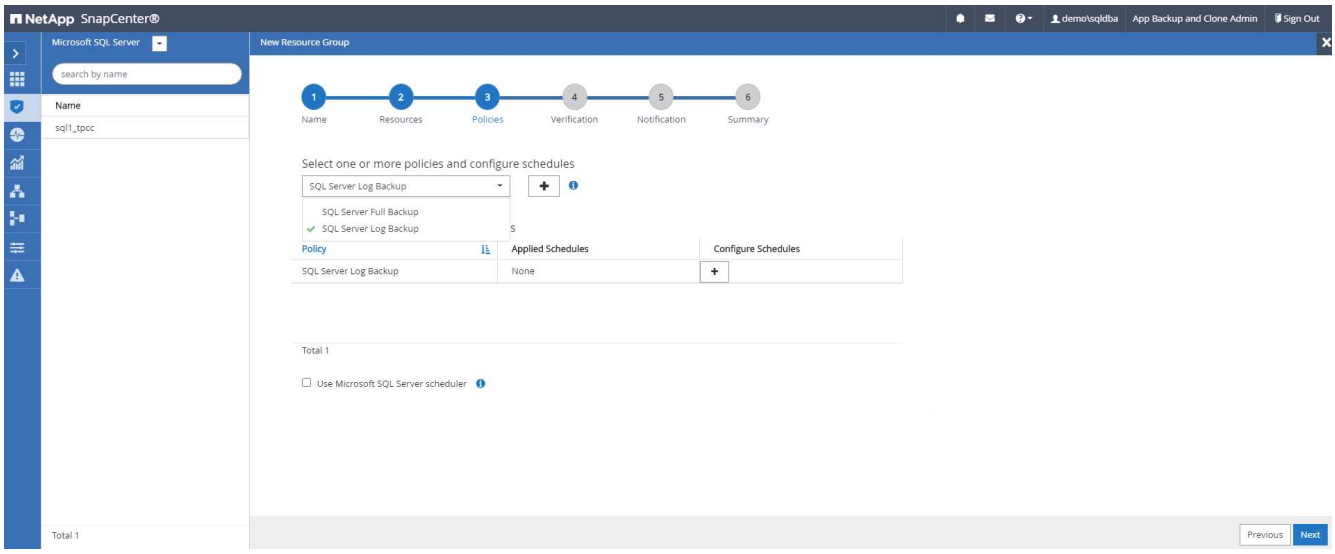
1. 데이터베이스 관리 사용자 ID를 사용하여 SnapCenter에 로그인하고 리소스 탭으로 이동합니다. 보기 드롭다운 목록에서 데이터베이스 또는 리소스 그룹을 선택하여 리소스 그룹 만들기 워크플로를 시작합니다. 리소스 그룹의 이름과 태그를 입력합니다. 스냅샷 복사본의 명명 형식을 정의할 수 있습니다.



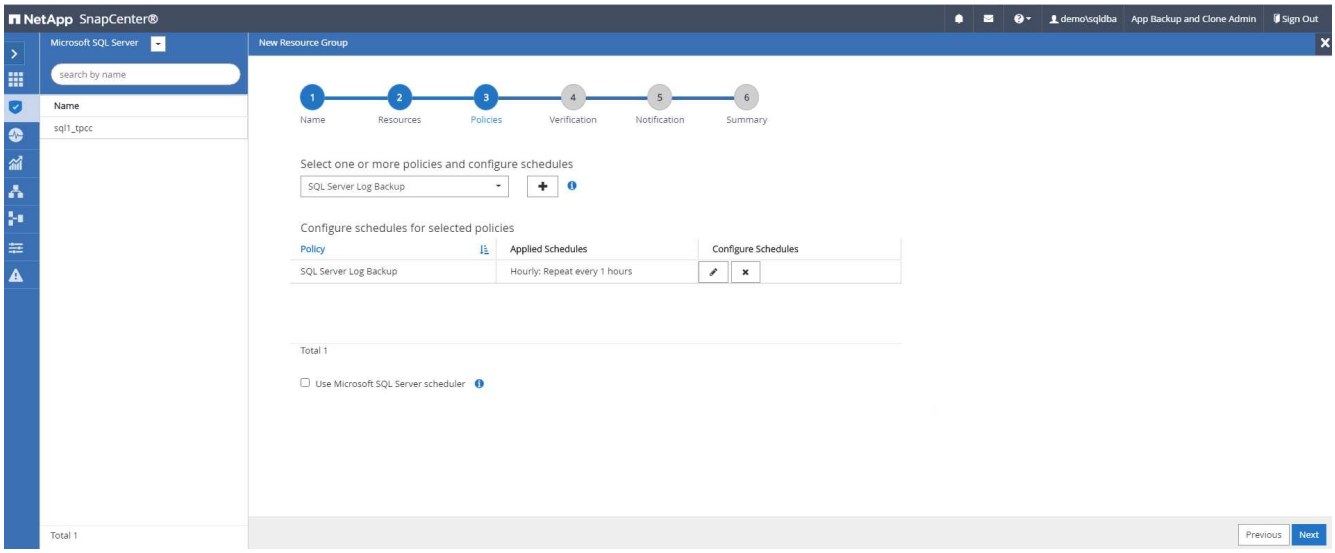
2. 백업할 데이터베이스 리소스를 선택합니다.



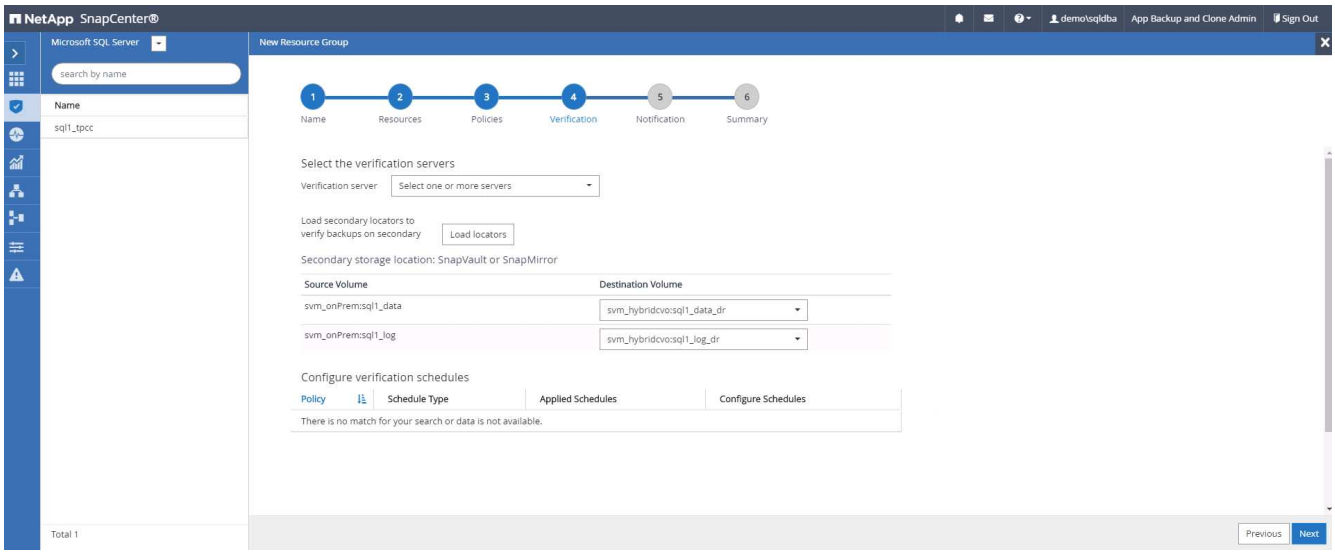
3. 섹션 7에서 생성한 SQL 로그 백업 정책을 선택합니다.



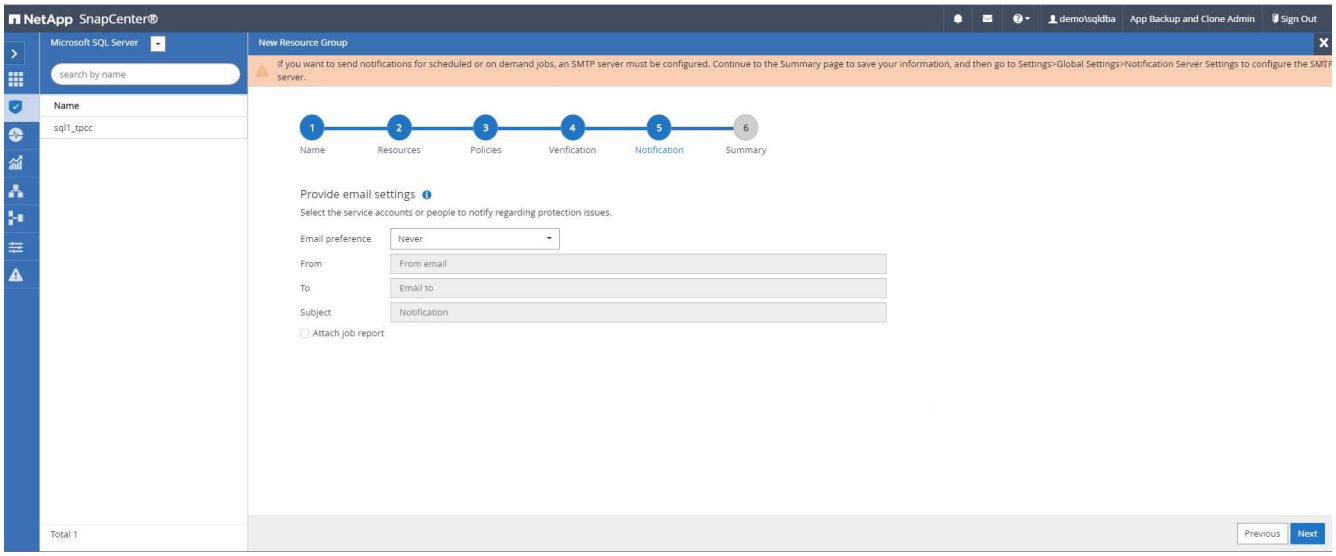
4. 백업 빈도와 정확한 백업 시간을 추가합니다.



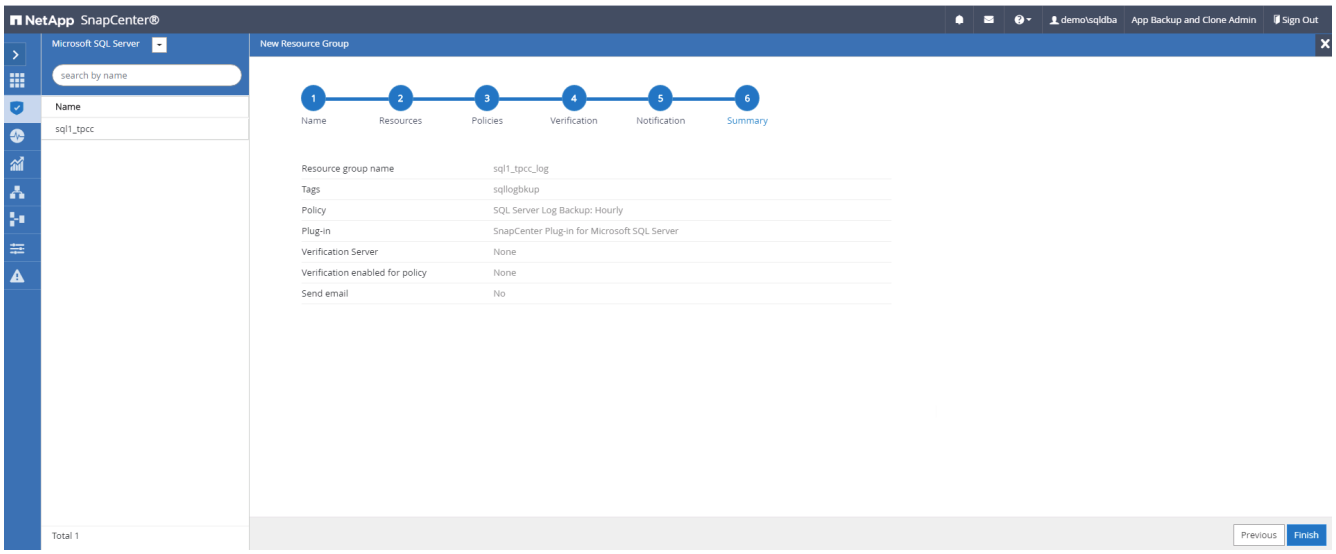
5. 백업 확인을 수행할 경우 보조 백업에 대한 검증 서버를 선택합니다. Load Locator를 클릭하여 보조 스토리지 위치를 채웁니다.



6. 필요한 경우 이메일 알림에 사용할 SMTP 서버를 구성합니다.



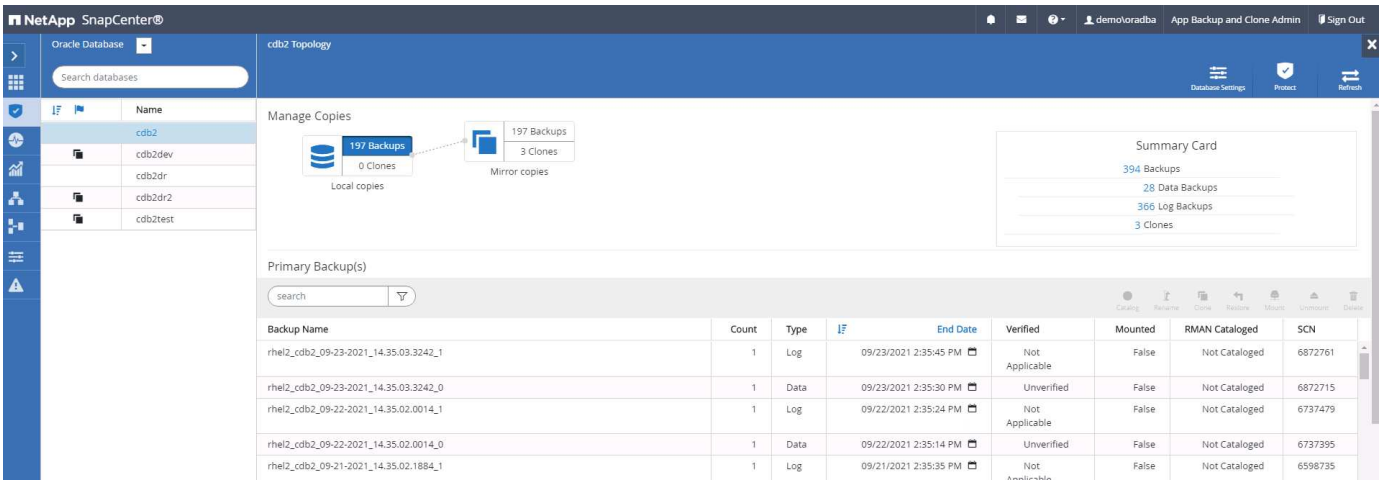
7. 요약.



9.백업 검증

데이터베이스 리소스 보호를 위해 데이터베이스 백업 리소스 그룹을 생성한 후에는 미리 정의된 일정에 따라 백업 작업이 실행됩니다. Monitor 탭에서 작업 실행 상태를 확인합니다.

리소스 탭으로 이동하고 데이터베이스 이름을 클릭하여 데이터베이스 백업에 대한 세부 정보를 확인하고, 로컬 복사본과 미러 복사본 간에 전환하여 스냅샷 백업이 퍼블릭 클라우드의 2차 위치에 복제되었는지 확인합니다.



이때 운영 장애가 발생할 경우 클라우드의 데이터베이스 백업 복사본을 클론 복제하여 개발/테스트 프로세스를 실행하거나 재해 복구를 수행할 수 있습니다.

AWS 퍼블릭 클라우드 시작하기

이 섹션에서는 AWS에서 Cloud Manager 및 Cloud Volumes ONTAP를 구축하는 프로세스에 대해 설명합니다.

설치하고

> ⓘ 그 결과를 더욱 쉽게 확인할 수 있도록 AWS에 구축된 이 문서를 토대로 마련했습니다. 그러나 프로세스는 Azure 및 GCP와 매우 유사합니다.

비행 전 점검

배포 전에 다음 단계에서 배포할 수 있도록 인프라가 마련되어 있는지 확인합니다. 여기에는 다음이 포함됩니다.

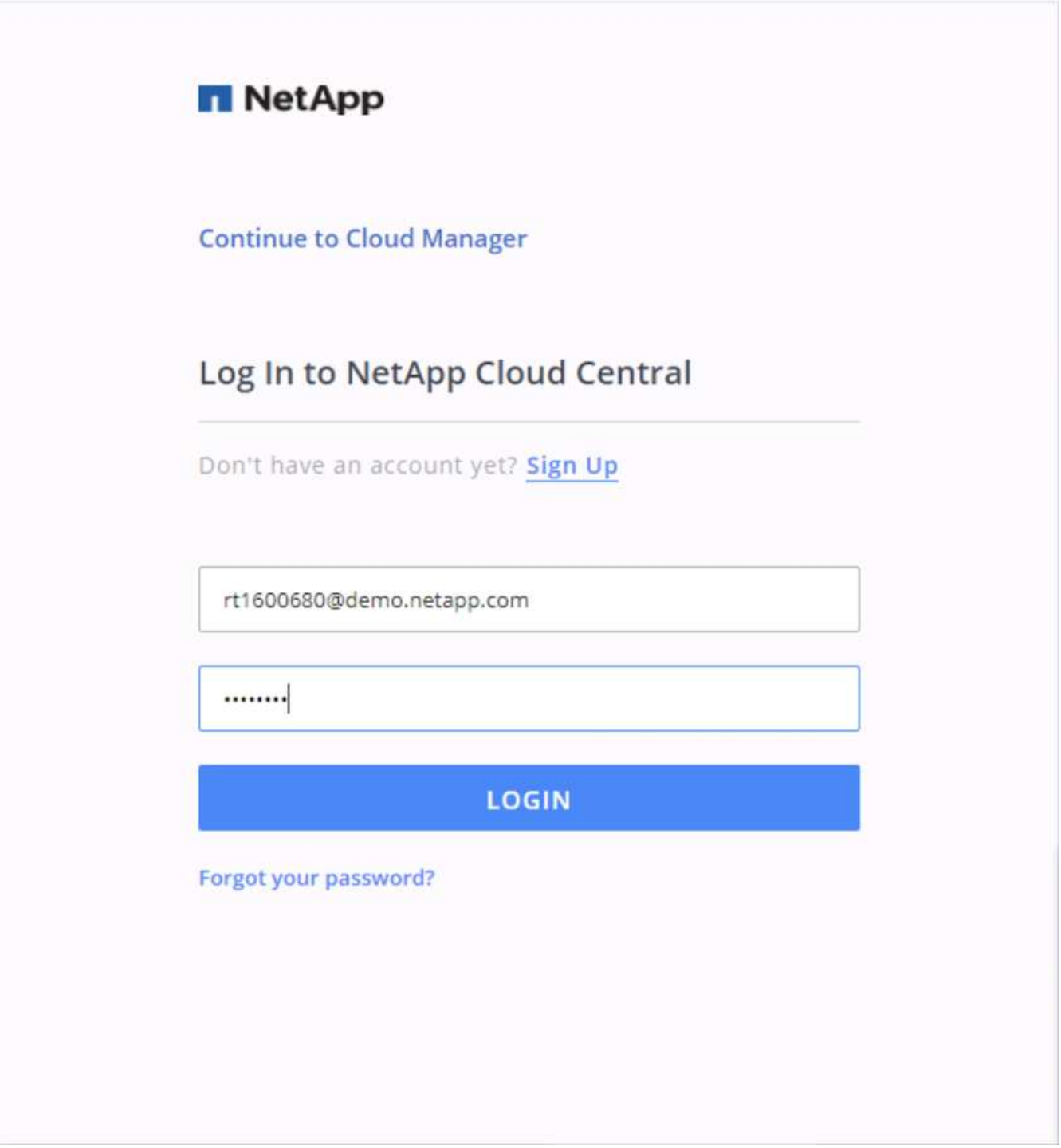
- 설치하 고 있습니다
- 선택한 지역에서 VPC를 사용할 수 있습니다
- 공용 인터넷에 액세스할 수 있는 서브넷입니다
- AWS 계정에 IAM 역할을 추가할 수 있는 권한
- AWS 사용자를 위한 비밀 키 및 액세스 키입니다

2.AWS에서 Cloud Manager 및 Cloud Volumes ONTAP를 구축하는 단계

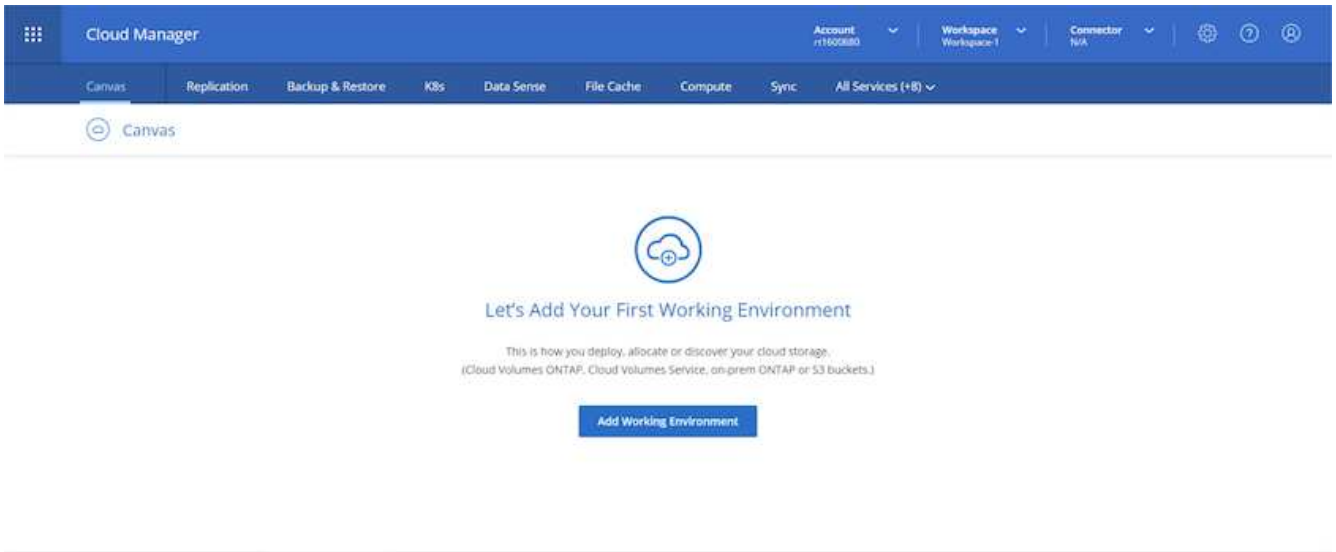
> ⓘ Cloud Manager와 Cloud Volumes ONTAP를 구축하는 방법은 매우 간단합니다. 이 방법은 가장 간단하지만 가장 많은 권한이 필요합니다. 이 방법이 AWS 환경에 적합하지 않은 경우 을 참조하십시오 "NetApp 클라우드 문서".

Cloud Manager 커넥터를 배포합니다

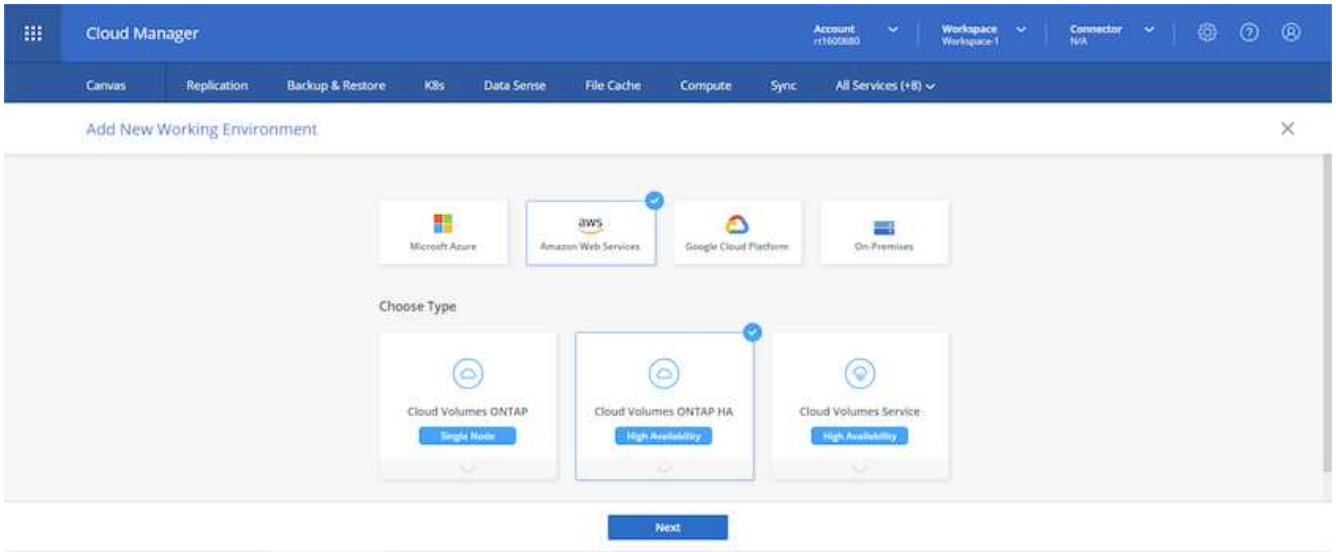
1. 로 이동합니다 "NetApp Cloud Central에서" 로그인 또는 가입



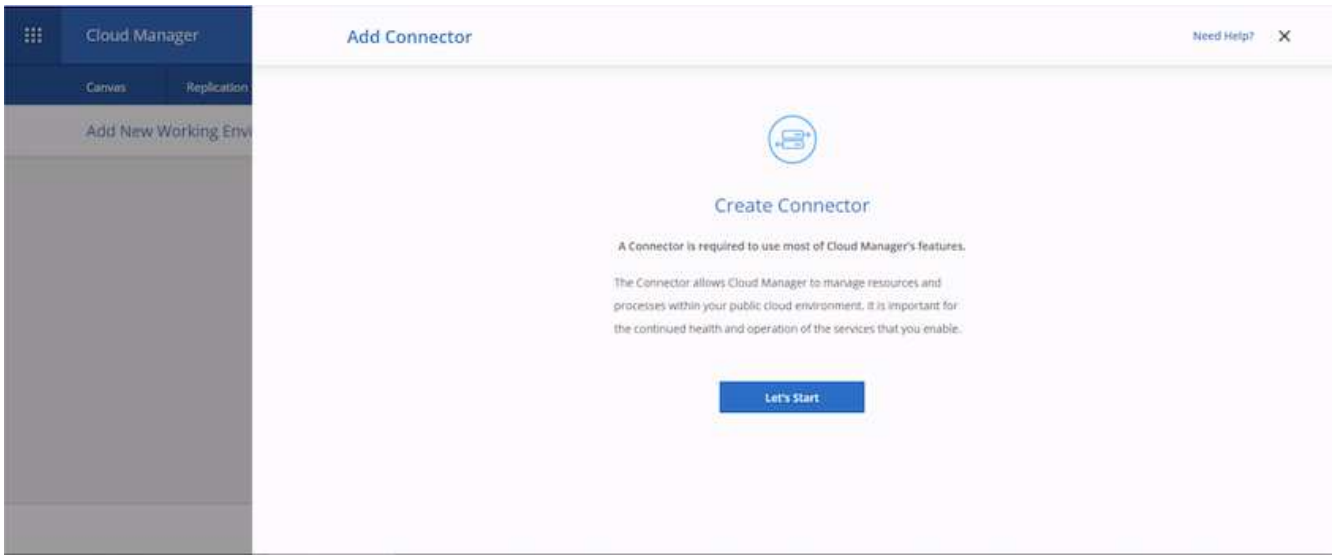
2. 로그인한 후 Canvas로 옮겨야 합니다.



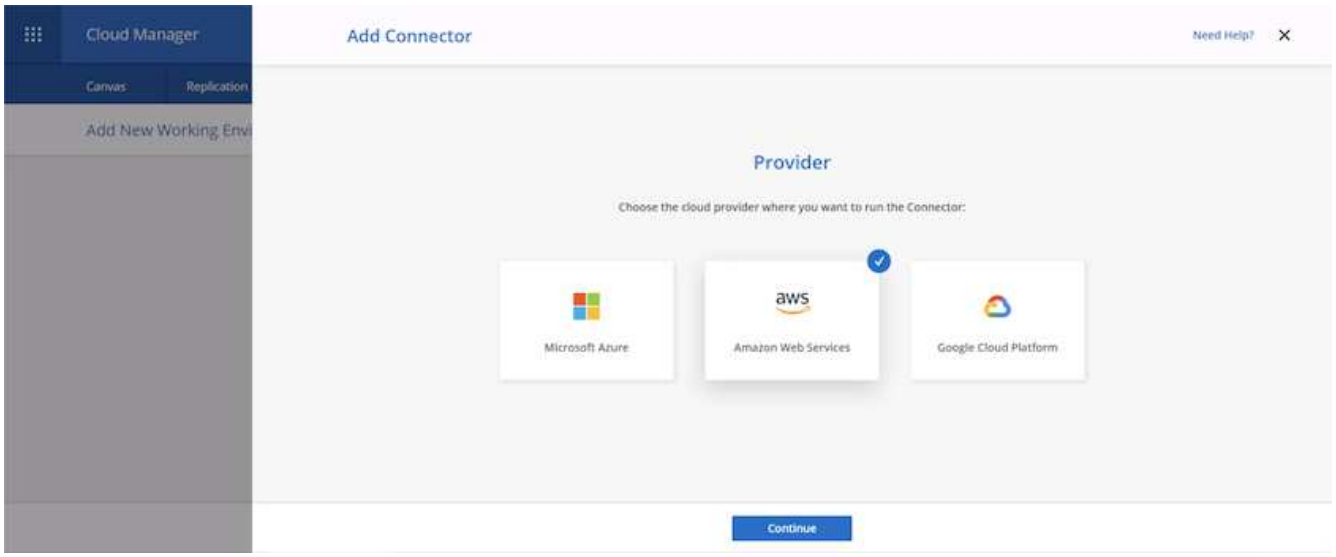
3. "작업 환경 추가"를 클릭하고 AWS에서 Cloud Volumes ONTAP를 선택합니다. 단일 노드 시스템을 배포할지 고가용성 쌍을 구축할지를 선택할 수도 있습니다. 고가용성 쌍을 구축하기로 선택했습니다.



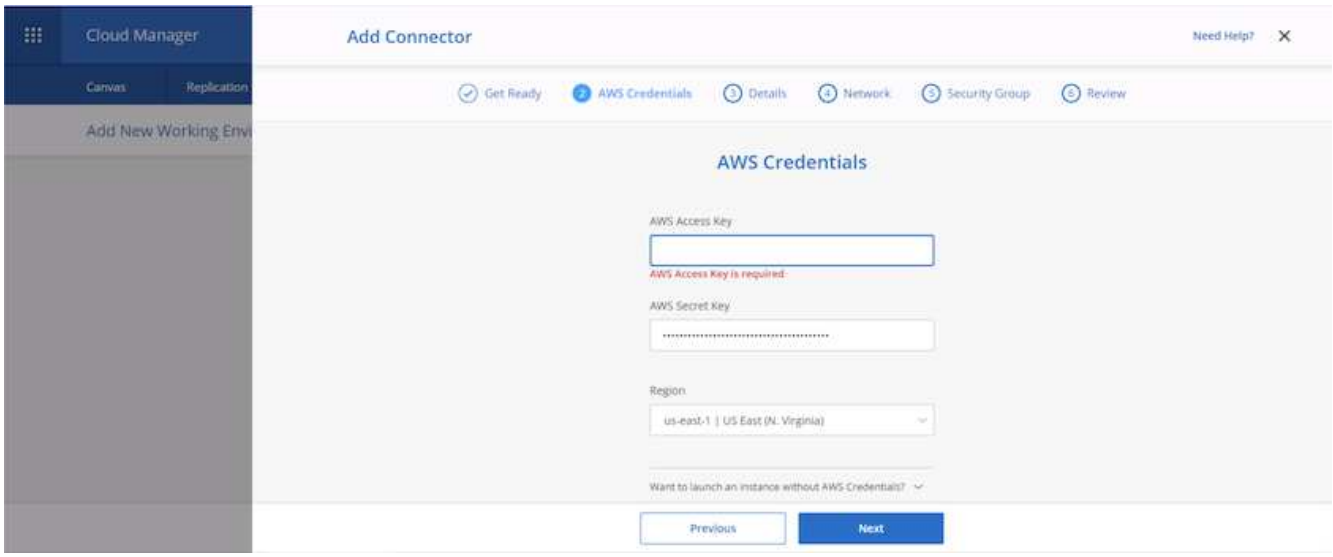
4. 커넥터가 작성되지 않은 경우 커넥터를 작성하라는 팝업 메시지가 나타납니다.



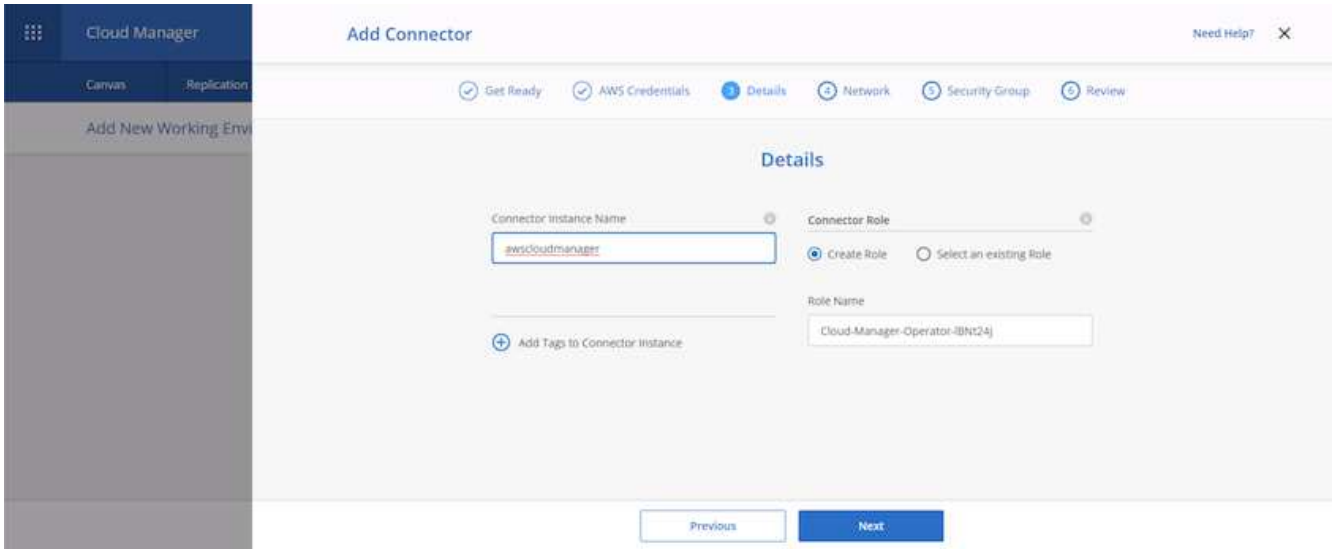
5. 시작 을 클릭한 다음 AWS 를 선택합니다.



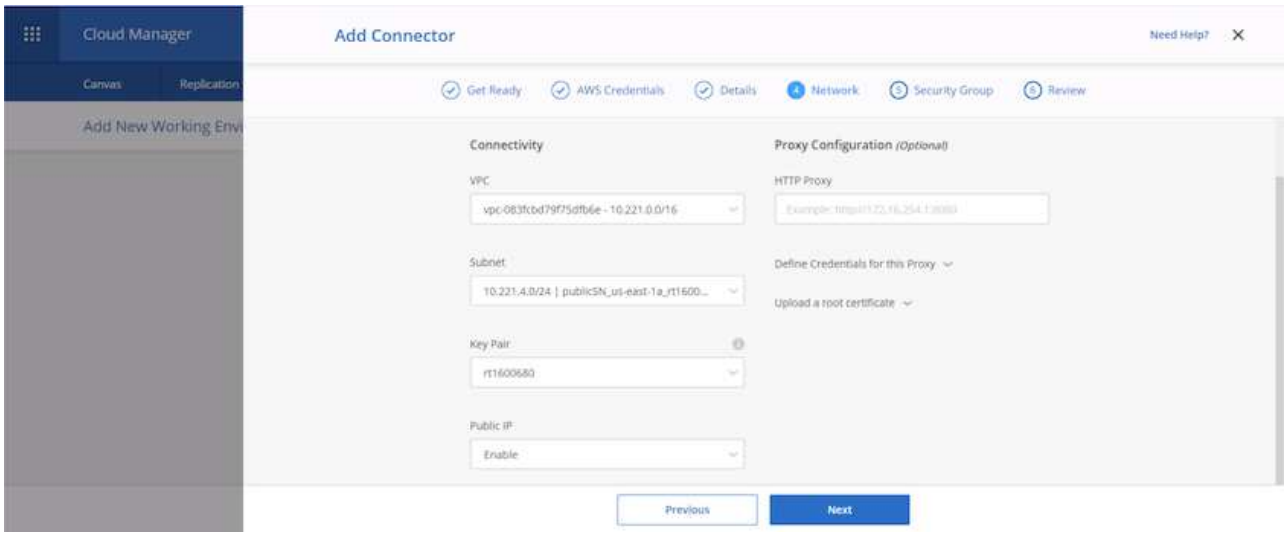
6. 암호 키와 액세스 키를 입력합니다. 사용자에게 에 설명된 올바른 권한이 있는지 확인합니다 "NetApp 정책 페이지를 참조하십시오".



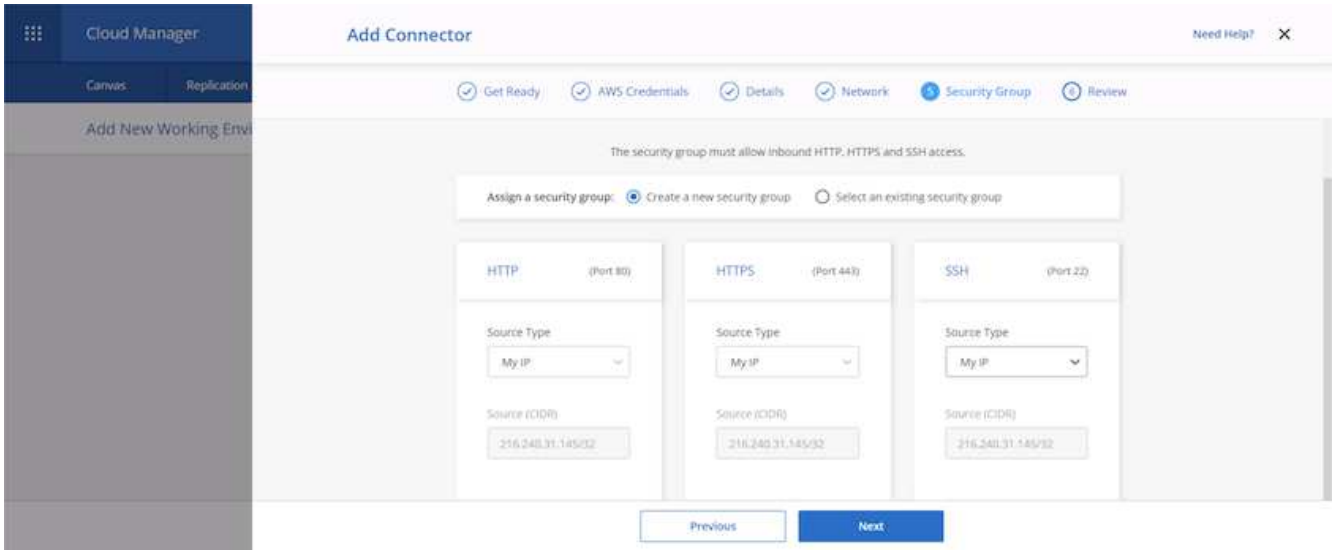
7. 커넥터에 이름을 지정하고 에 설명된 대로 미리 정의된 역할을 사용합니다 "NetApp 정책 페이지를 참조하십시오" 또는 Cloud Manager에게 역할을 맡도록 요청하십시오.



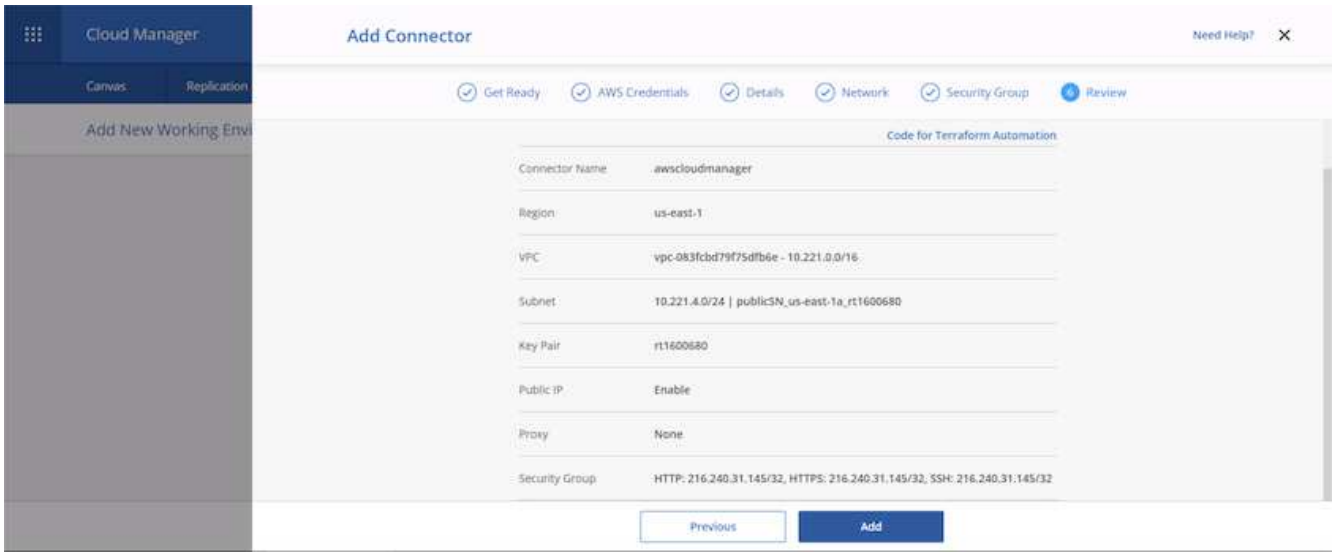
8. 커넥터를 배포하는 데 필요한 네트워킹 정보를 제공합니다. 다음과 같은 방법으로 아웃바운드 인터넷 액세스가 활성화되었는지 확인합니다.
   a. 커넥터에 공용 IP 주소를 제공합니다
   b. 커넥터를 통해 작업할 프록시를 제공합니다
   c. 인터넷 게이트웨이를 통해 공용 인터넷에 연결되는 경로를 커넥터에 제공합니다



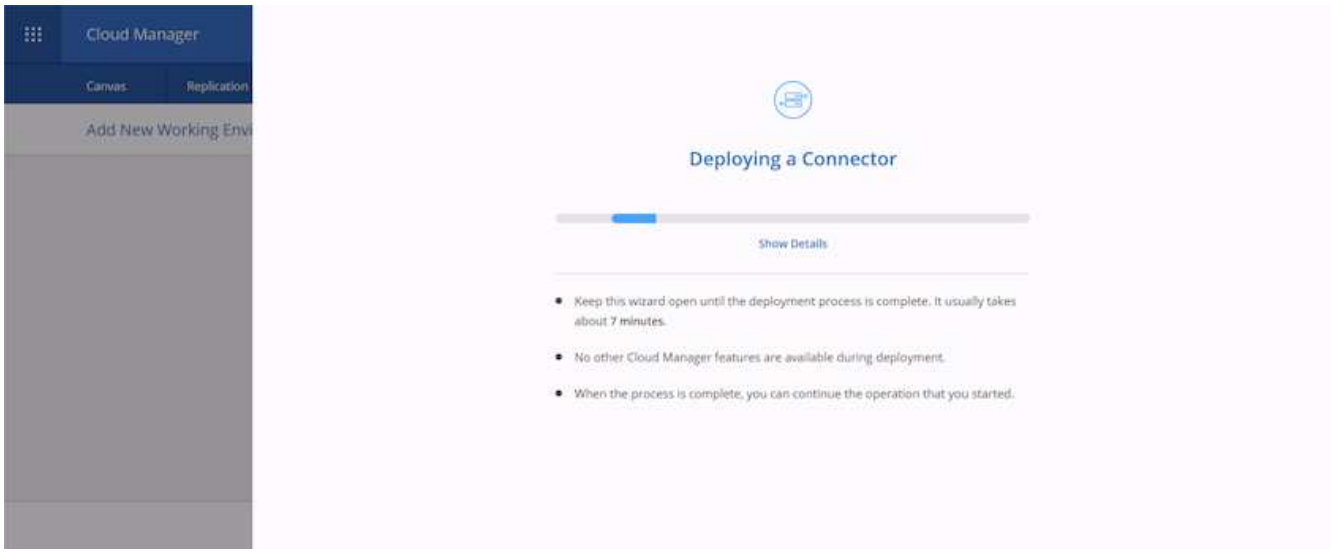
9. 보안 그룹을 제공하거나 새 보안 그룹을 생성하여 SSH, HTTP 및 HTTPS를 통해 커넥터와 통신할 수 있습니다. IP 주소에서만 커넥터에 대한 액세스를 활성화했습니다.



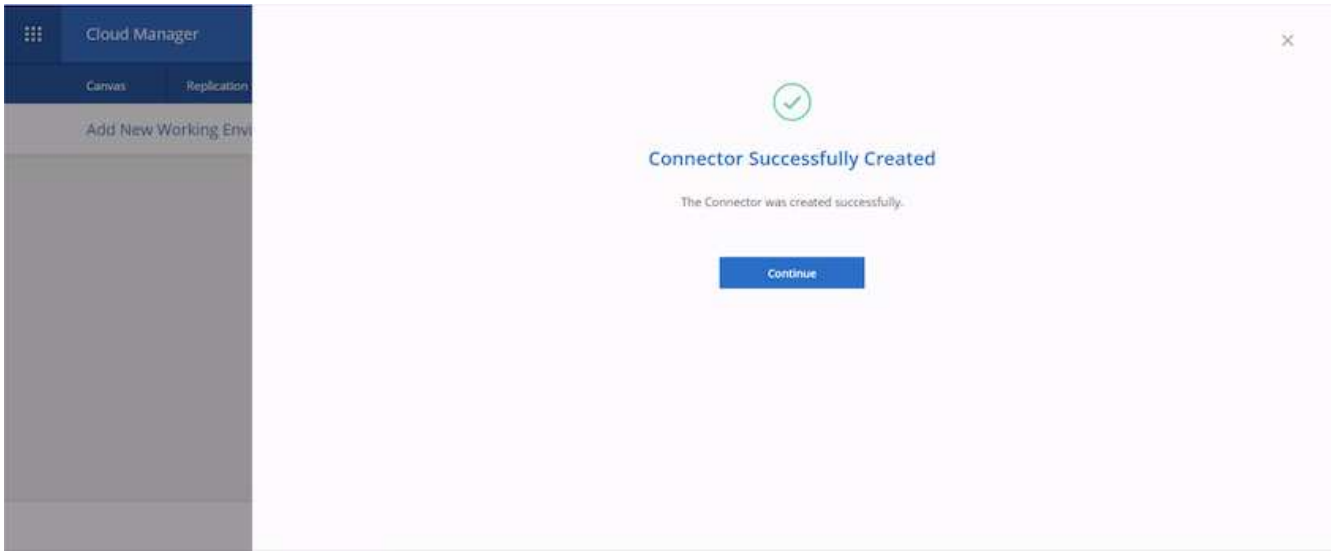
10. 요약 페이지의 정보를 검토하고 추가 를 클릭하여 커넥터를 배포합니다.



11. 이제 커넥터는 클라우드 형성 스택을 사용하여 전개됩니다. Cloud Manager에서 또는 AWS를 통해 진행률을 모니터링할 수 있습니다.

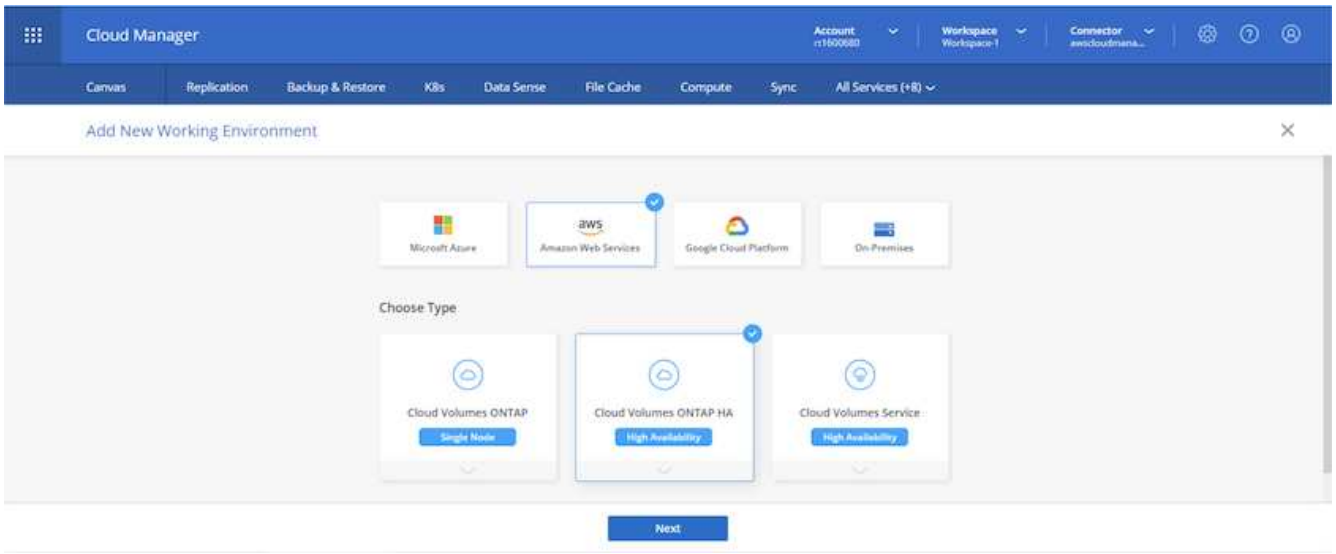


12. 배포가 완료되면 성공 페이지가 나타납니다.

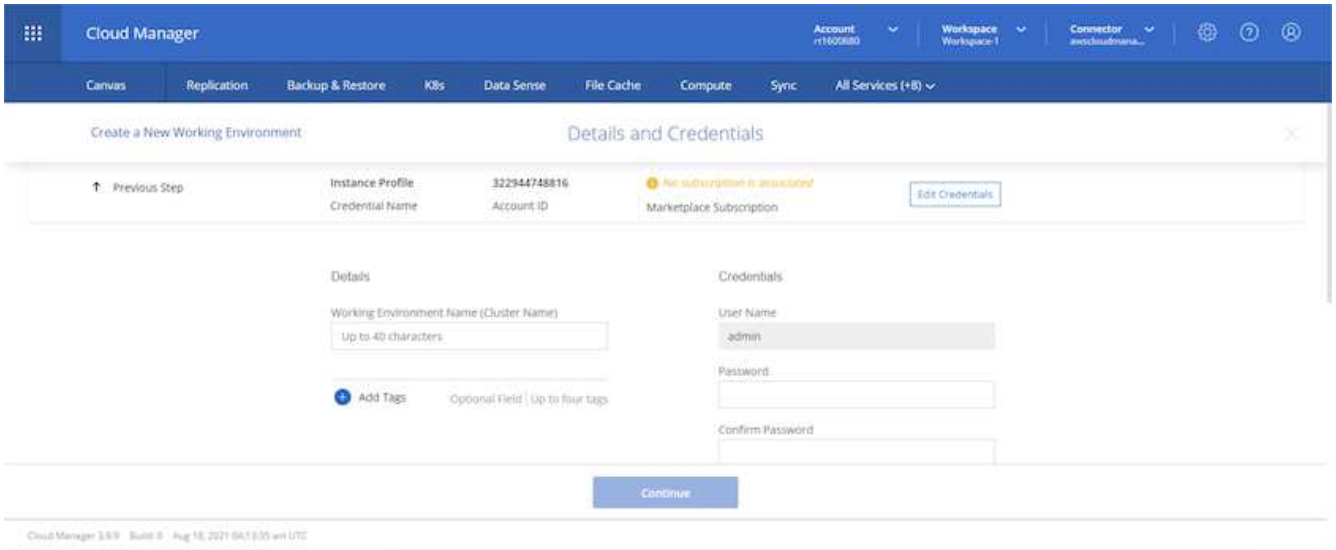


Cloud Volumes ONTAP 구축

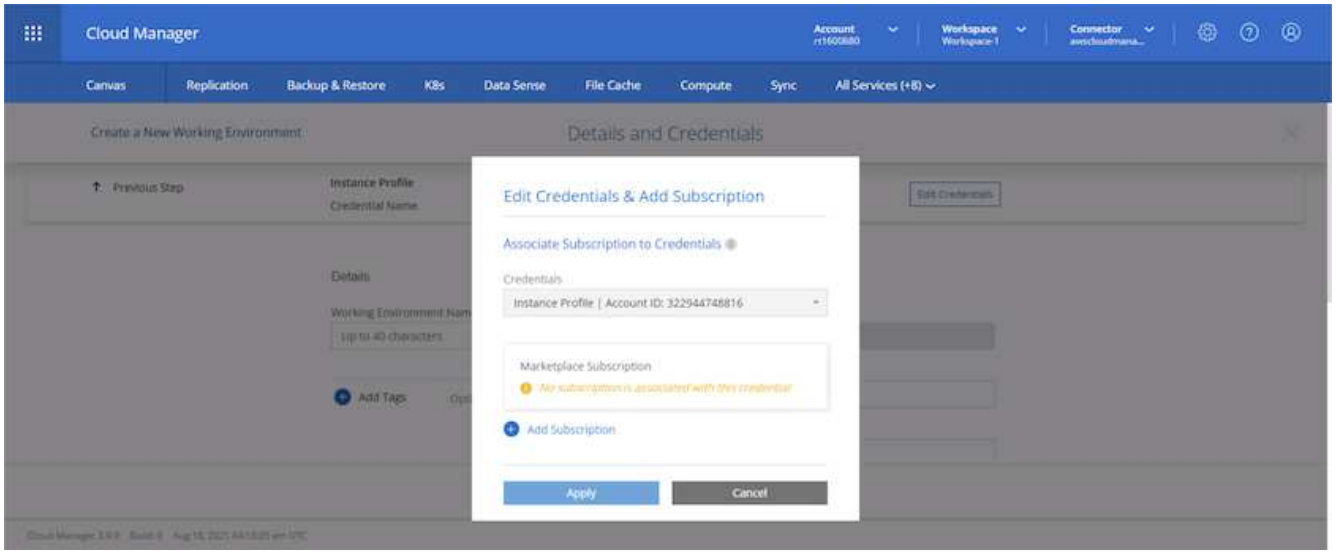
1. 요구사항에 따라 AWS 및 구축 유형을 선택하십시오.



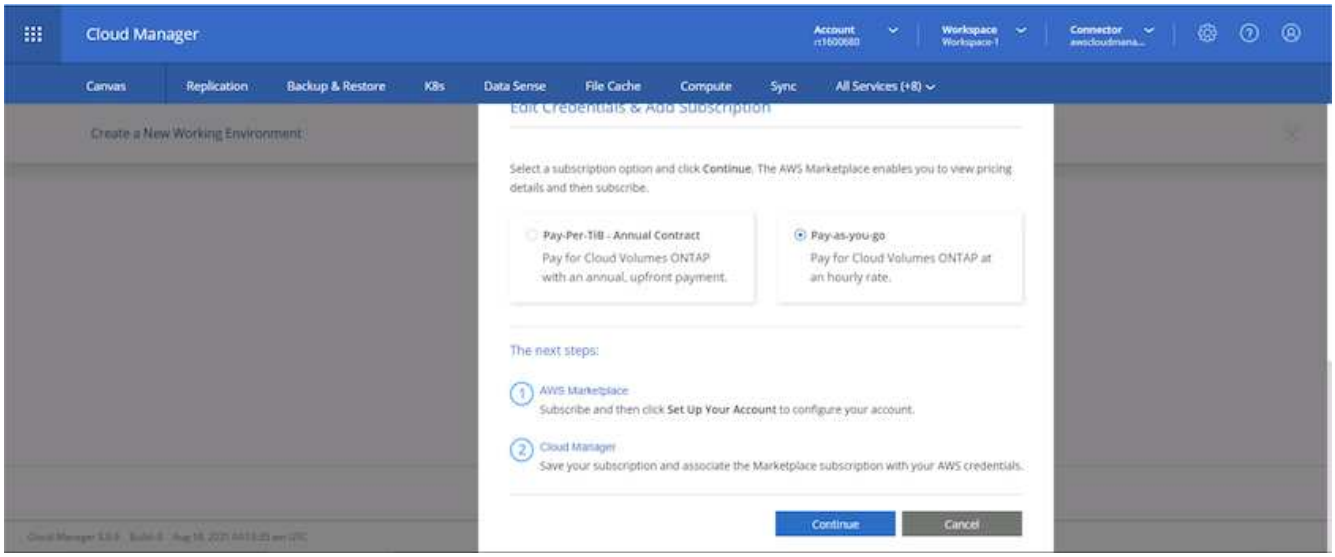
2. 구독이 할당되지 않은 상태에서 PAYGO를 사용하여 구매하려는 경우 자격 증명 편집 을 선택합니다.



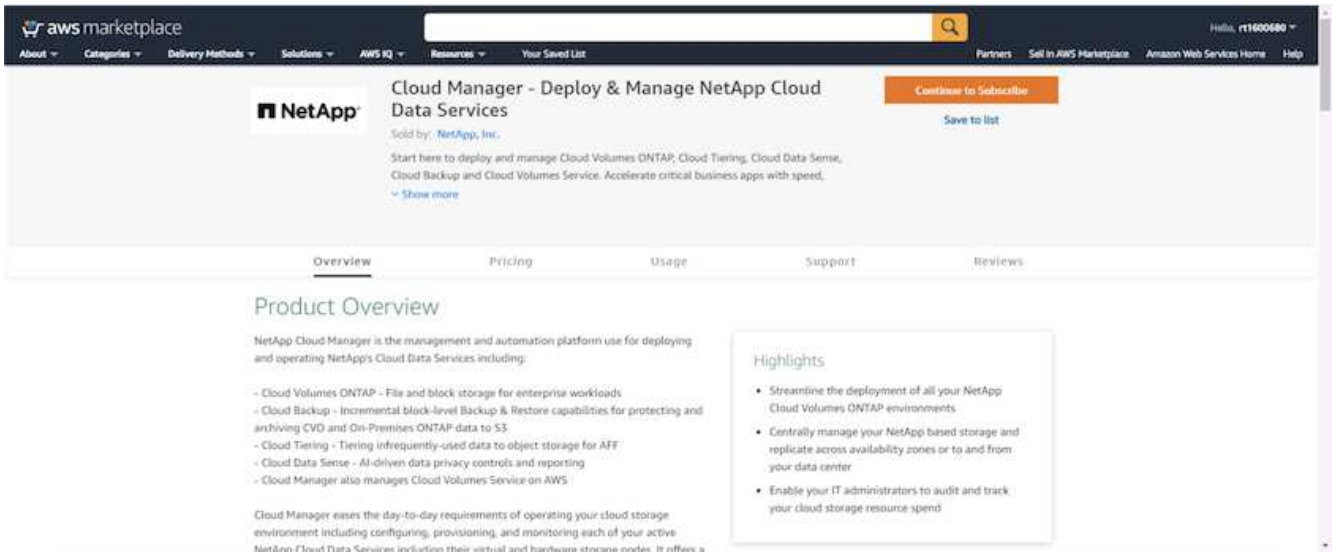
3. 구독 추가 를 선택합니다.



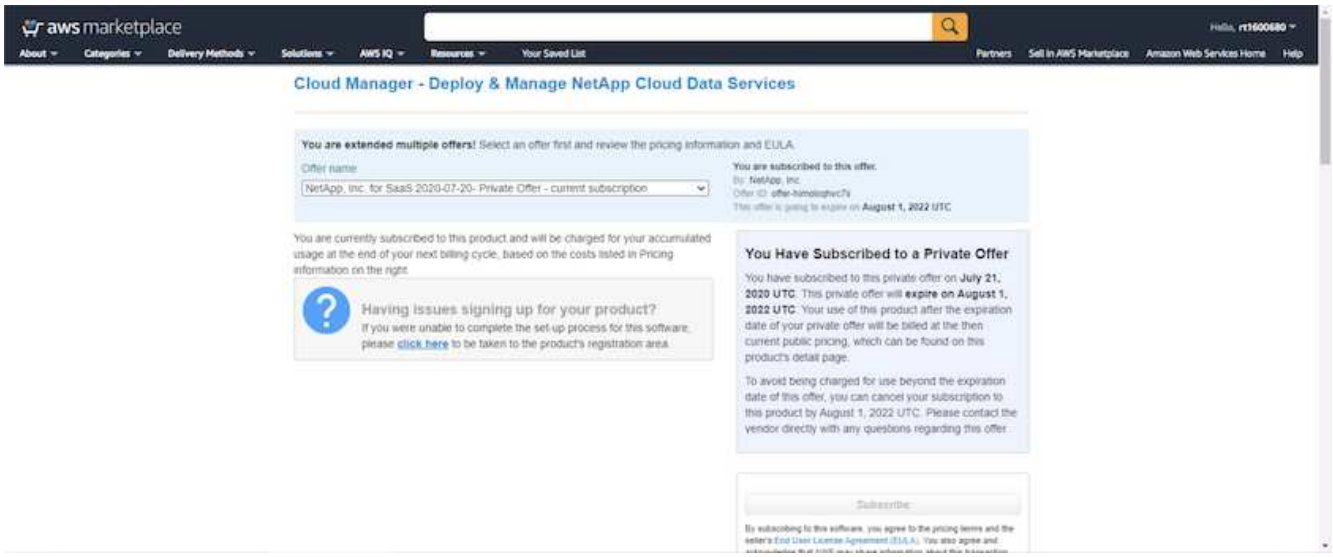
4. 가입하려는 계약 유형을 선택합니다. 나는 선불 종량제 를 선택했습니다.



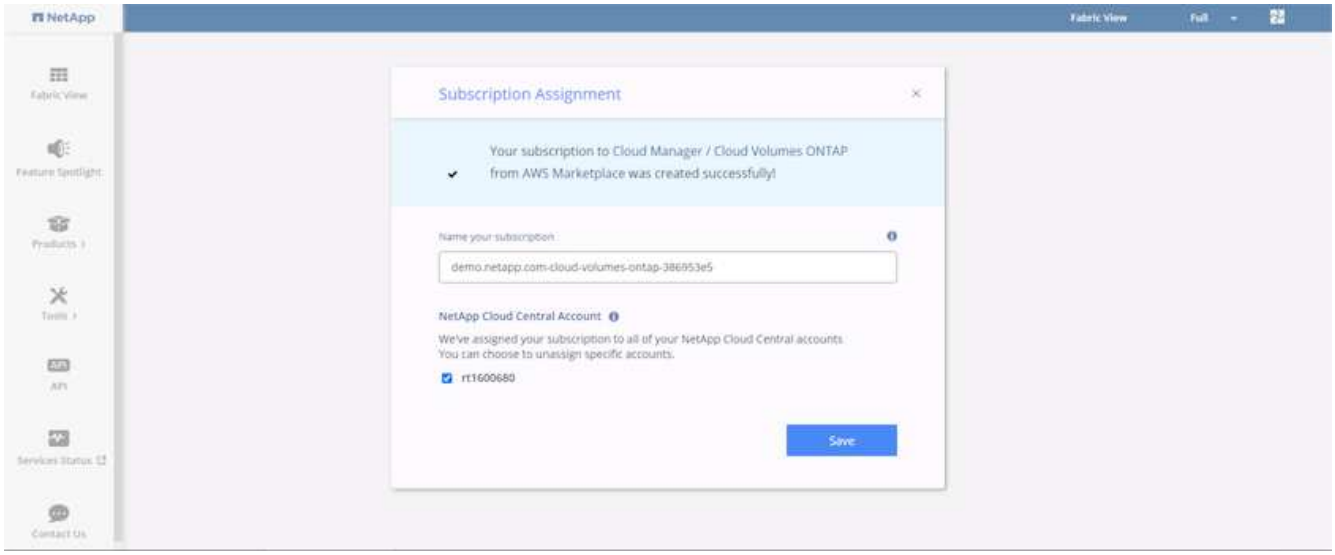
5. AWS로 리디렉션됩니다. 구독으로 계속 을 선택합니다.



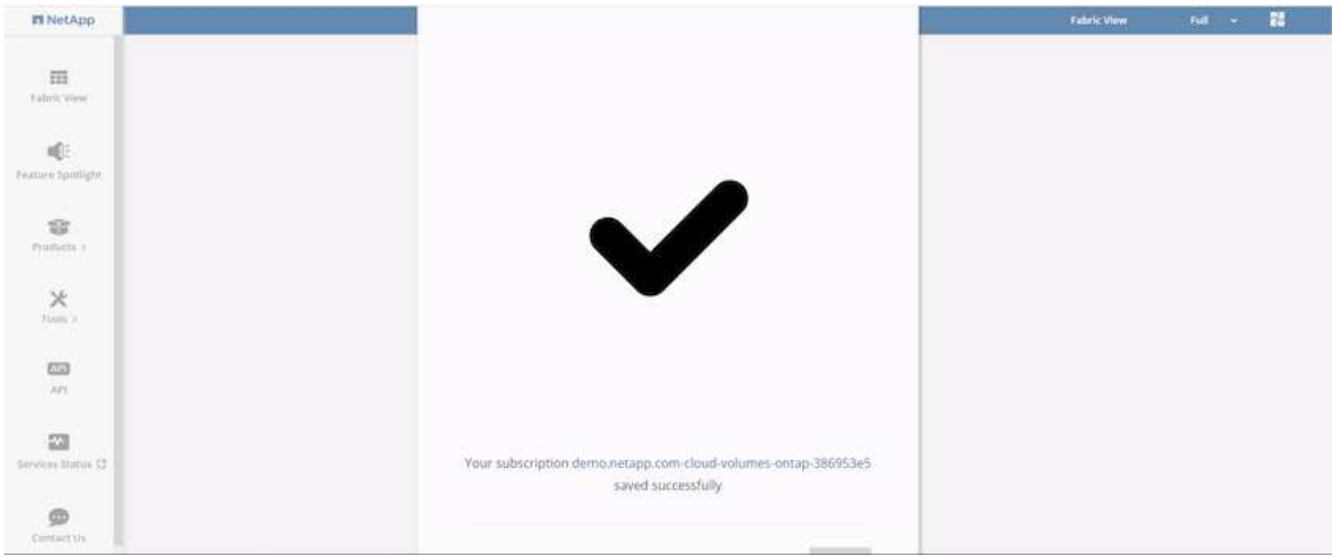
6. 구독하면 NetApp Cloud Central로 리디렉션됩니다. 이미 가입되어 있고 리디렉션되지 않는 경우 "여기를 클릭" 링크를 선택하십시오.



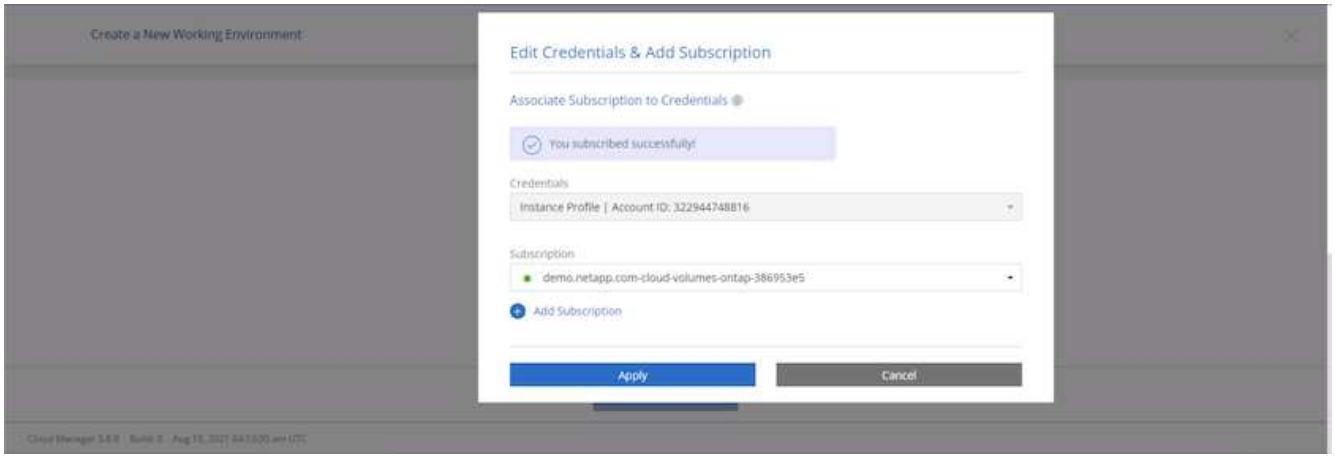
7. 구독의 이름을 지정하고 Cloud Central 계정에 할당해야 하는 Cloud Central로 리디렉션됩니다.



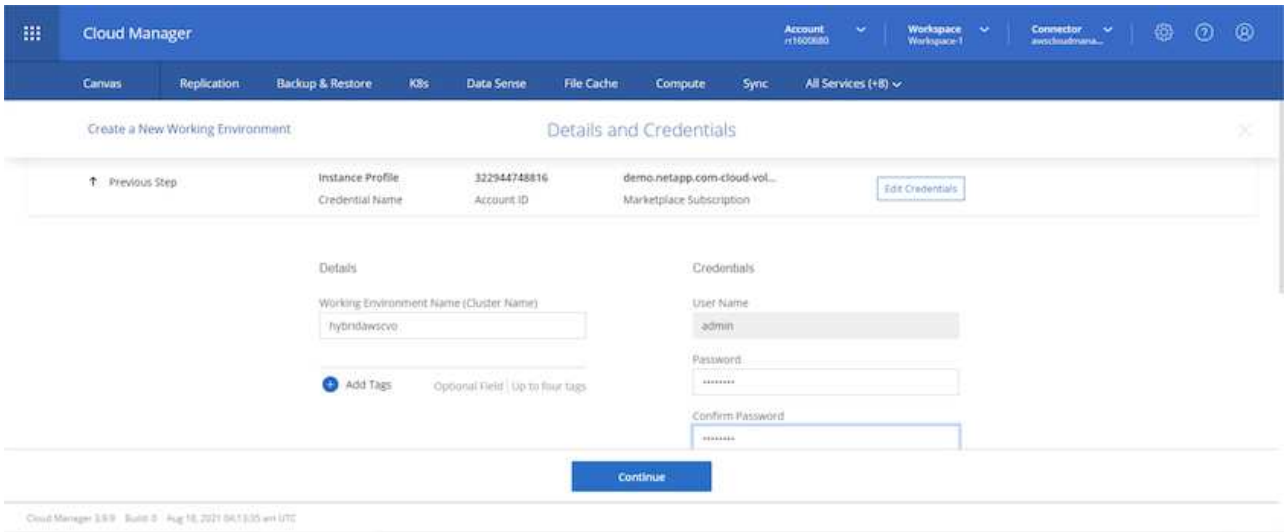
8. 성공하면 확인 표시 페이지가 나타납니다. Cloud Manager 탭으로 다시 이동합니다.



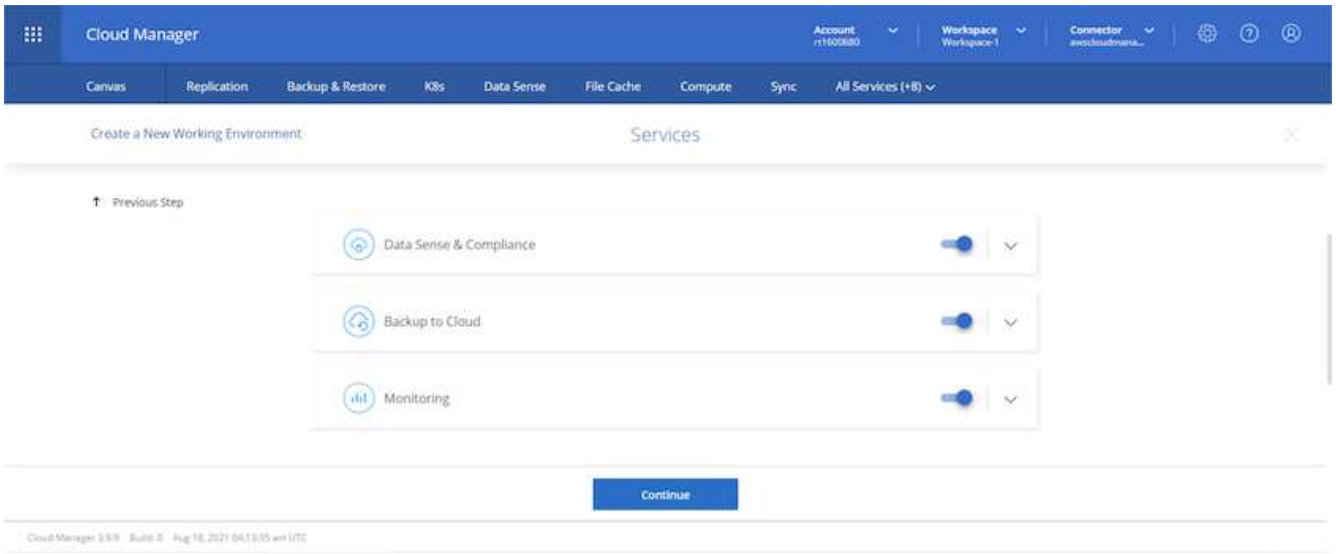
9. 이제 Cloud Central에 구독이 나타납니다. 계속하려면 적용을 클릭하십시오.



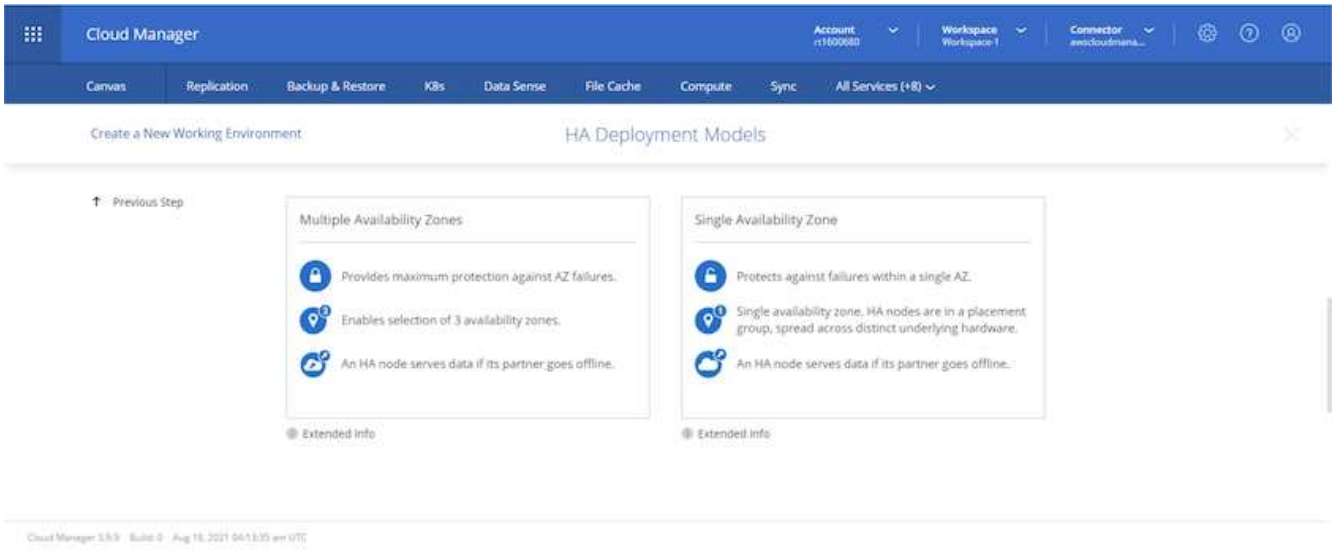
10. 다음과 같은 작업 환경 세부 정보를 입력합니다.
    a. 클러스터 이름입니다
    b. 클러스터 암호입니다
    c. AWS 태그(선택 사항)



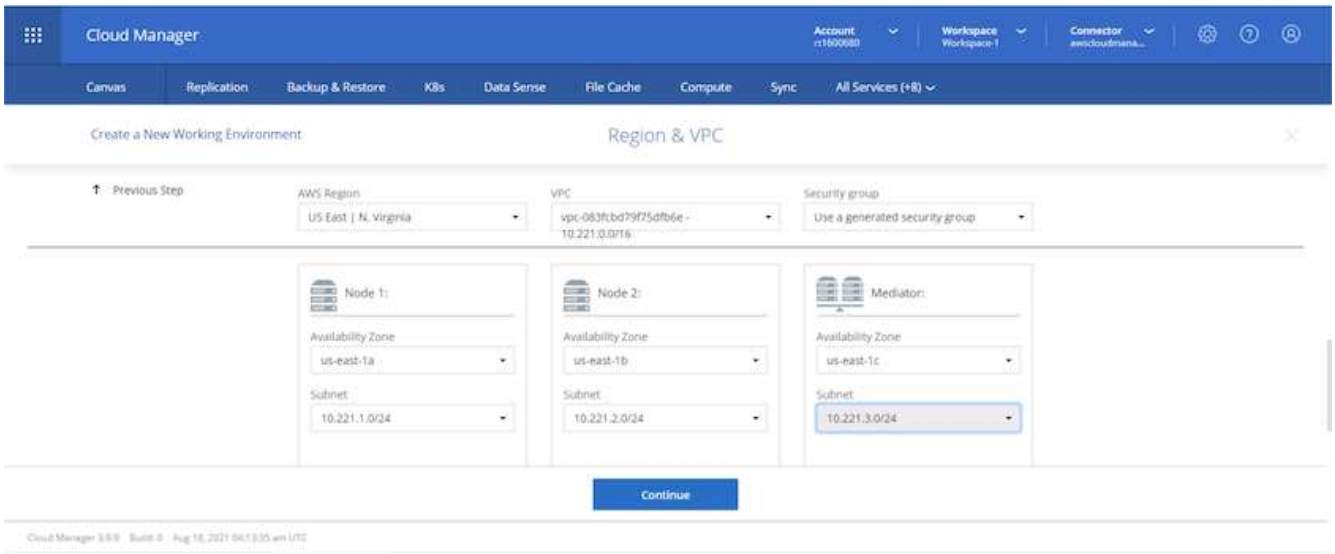
11. 구축할 추가 서비스를 선택하십시오. 이러한 서비스에 대한 자세한 내용은 를 참조하십시오 "NetApp Cloud 홈 페이지".



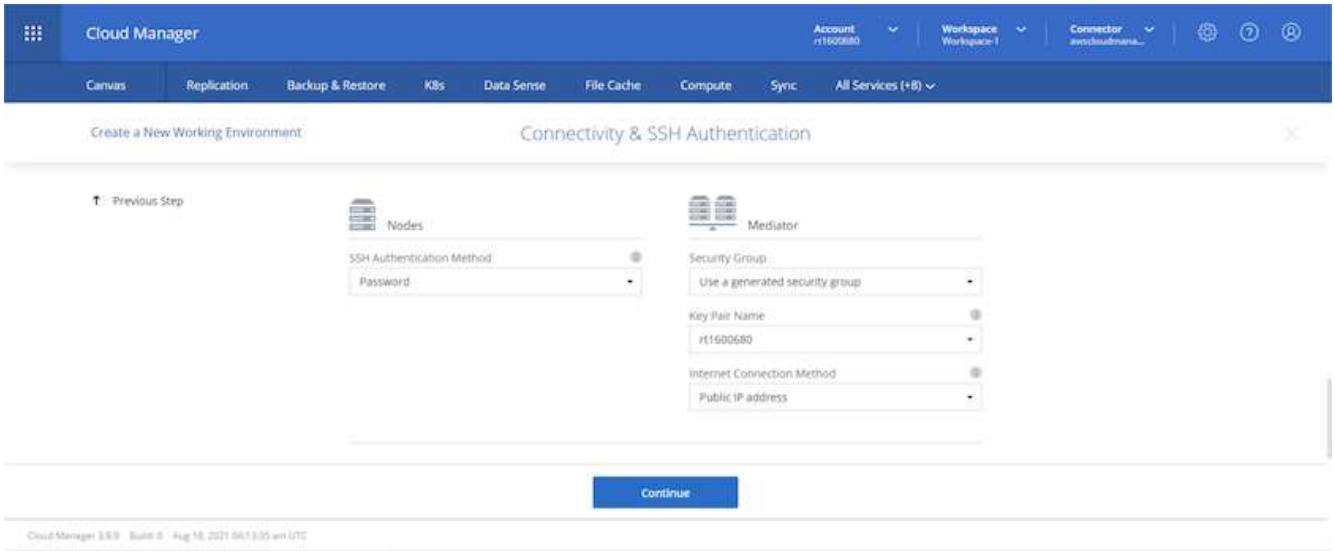
12. 여러 가용성 영역(각각 다른 AZ에 있는 3개의 서브넷이 필요함) 또는 단일 가용성 영역에 구축할지 선택합니다. 여러 개의 AZs를 선택했습니다.



13. 구축할 클러스터의 지역, VPC 및 보안 그룹을 선택합니다. 이 섹션에서는 노드별(및 중재자) 가용성 영역과 해당 영역이 차지하는 서브넷도 할당합니다.

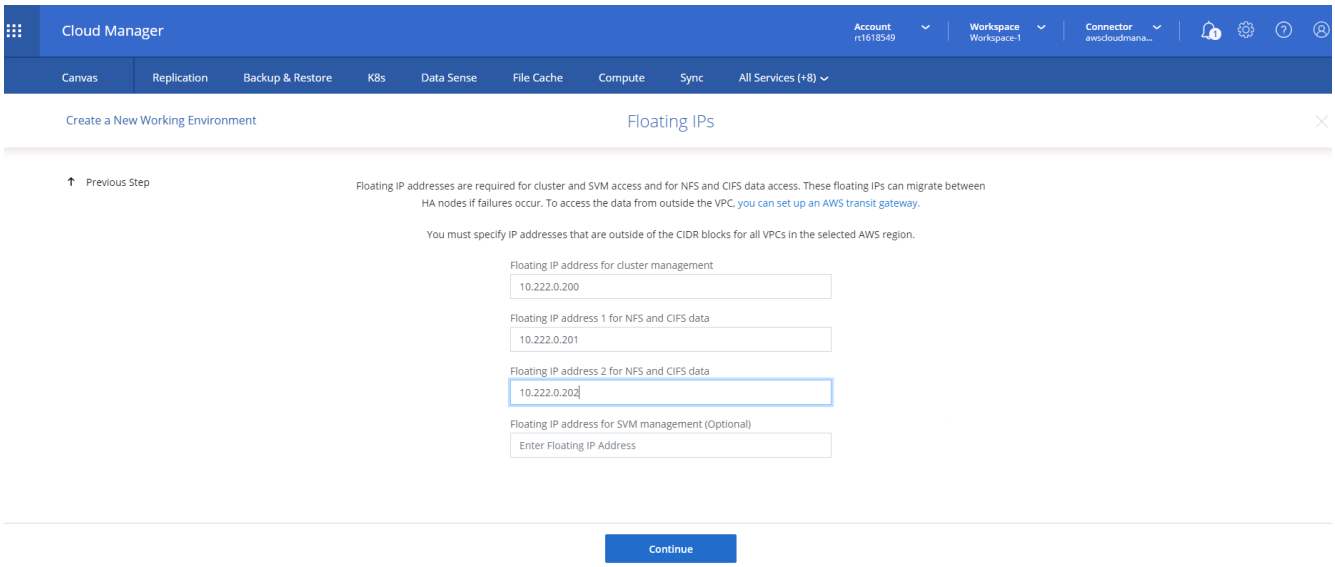


14. 노드 및 중재자의 연결 방법을 선택합니다.

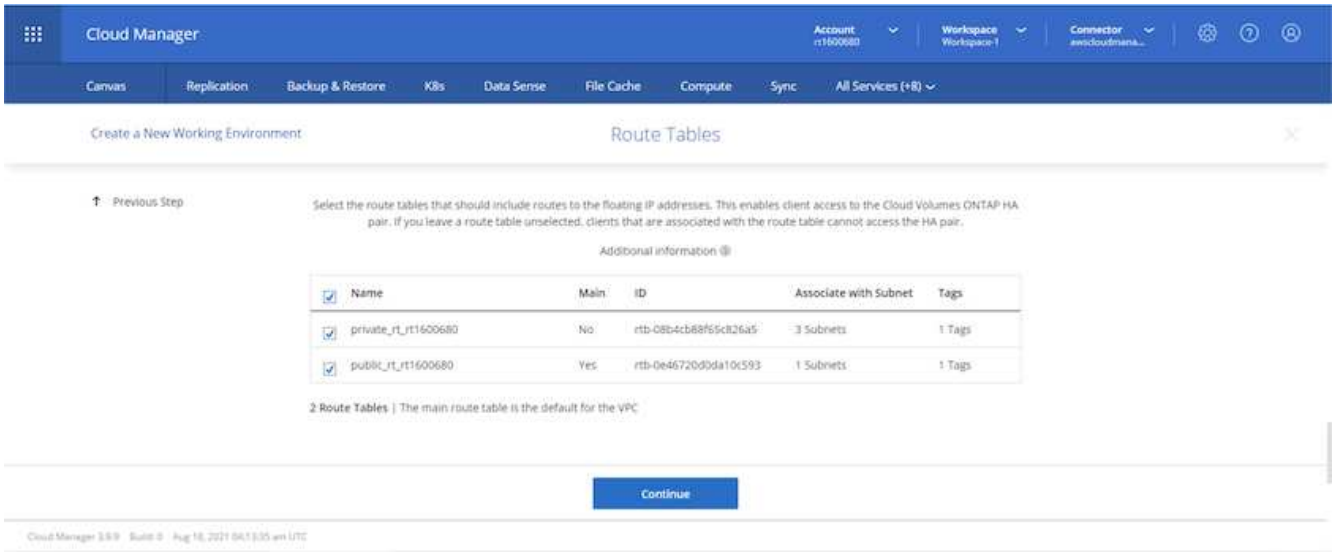


중재자가 AWS API와 통신해야 합니다. 중재자 EC2 인스턴스를 구축한 후 API에 연결할 수 있으면 공용 IP 주소가 필요하지 않습니다.

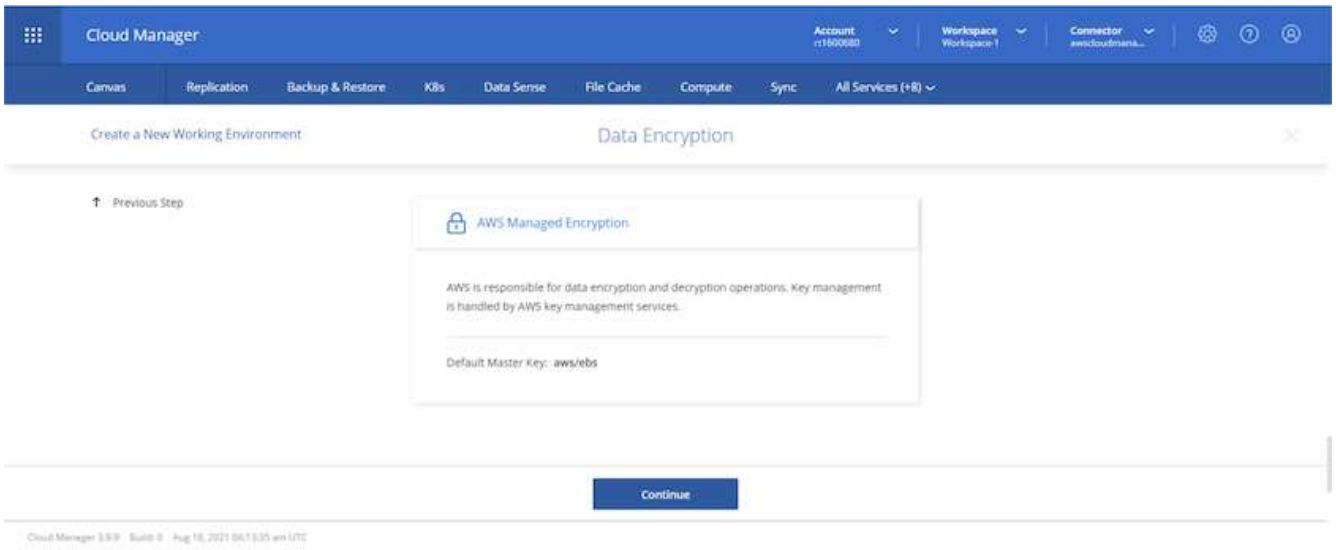
1. 부동 IP 주소는 클러스터 관리 및 데이터 서비스 IP를 포함하여 Cloud Volumes ONTAP가 사용하는 다양한 IP 주소에 대한 액세스를 허용하는 데 사용됩니다. 이러한 주소는 네트워크 내에서 아직 라우팅할 수 없는 주소여야 하며 AWS 환경의 라우팅 테이블에 추가됩니다. 이러한 주소는 페일오버 중에 HA 쌍의 일관된 IP 주소를 지원하는 데 필요합니다. 부동 IP 주소에 대한 자세한 내용은 에서 찾을 수 있습니다 "NetApp 클라우드 문서화".



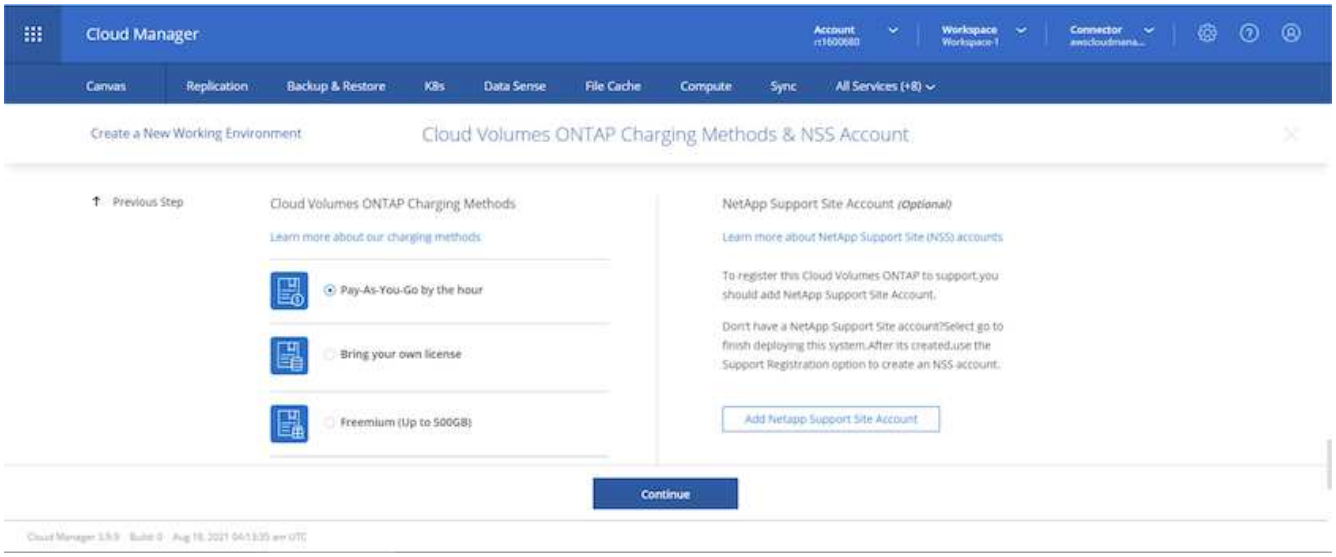
2. 부동 IP 주소를 추가할 라우팅 테이블을 선택합니다. 이러한 라우팅 테이블은 클라이언트가 Cloud Volumes ONTAP와 통신하는 데 사용됩니다.



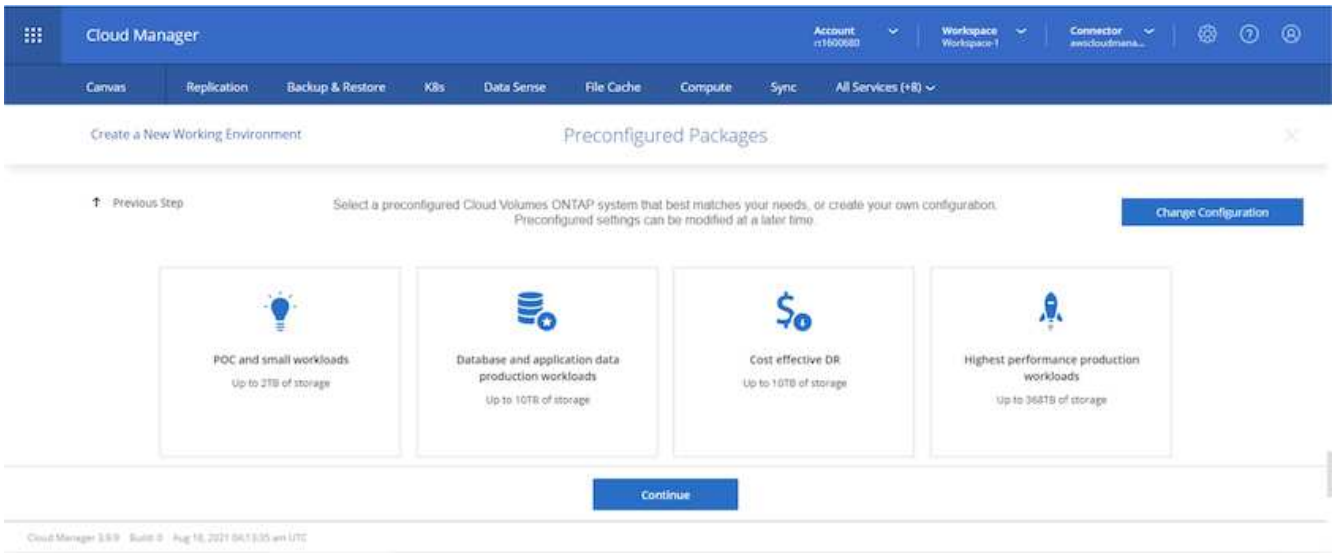
3. ONTAP 루트, 부팅 및 데이터 디스크를 암호화하기 위해 AWS 관리 암호화를 사용할지 AWS KMS를 사용할지 여부를 선택합니다.



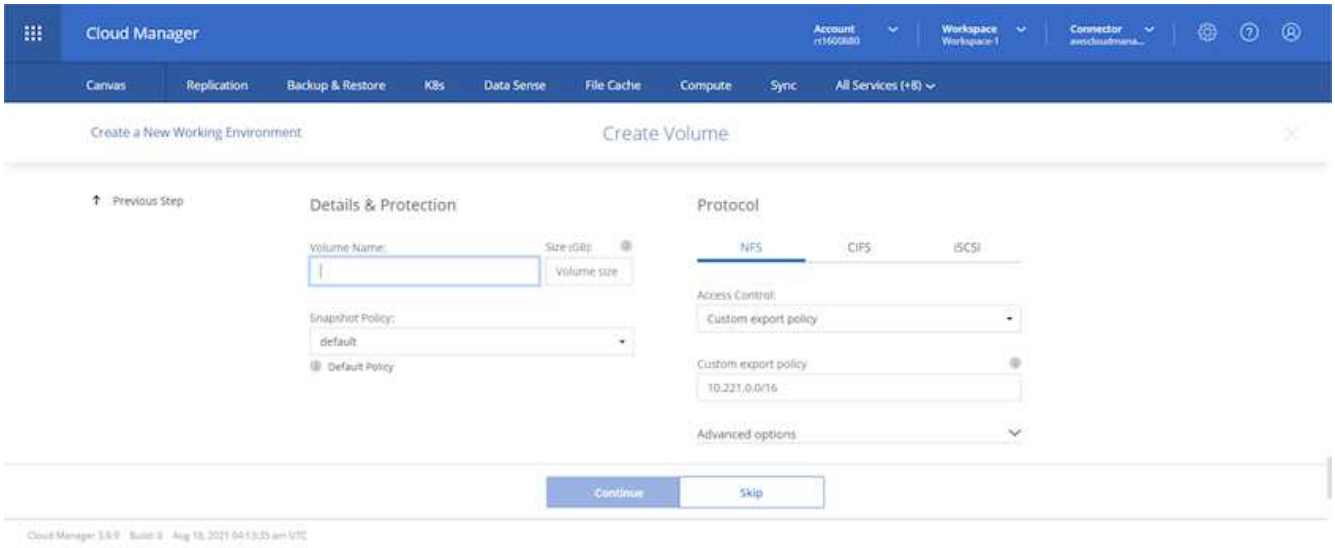
4. 라이센스 모델을 선택합니다. 선택할 항목을 모르는 경우 NetApp 담당자에게 문의하십시오.



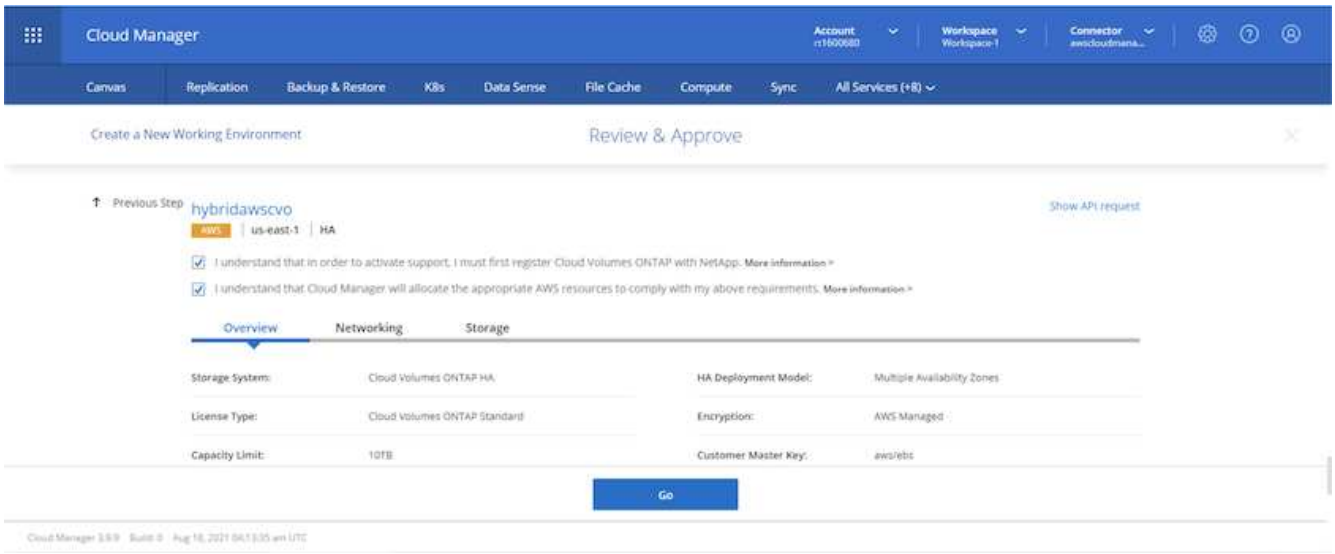
5. 사용 사례에 가장 적합한 구성을 선택하십시오. 이는 사전 요구 사항 페이지에서 다룬 크기 조정 고려 사항과 관련이 있습니다.



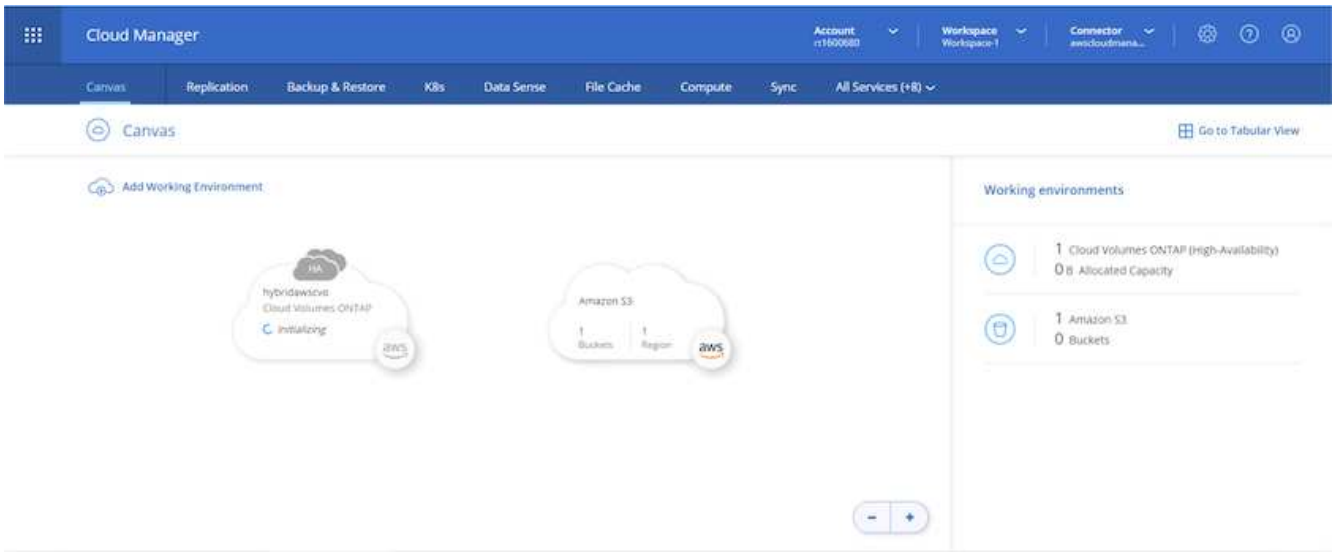
6. 필요에 따라 볼륨을 생성합니다. 다음 단계에서는 SnapMirror를 사용하고, 이로 인해 볼륨이 생성되므로 필요하지 않습니다.



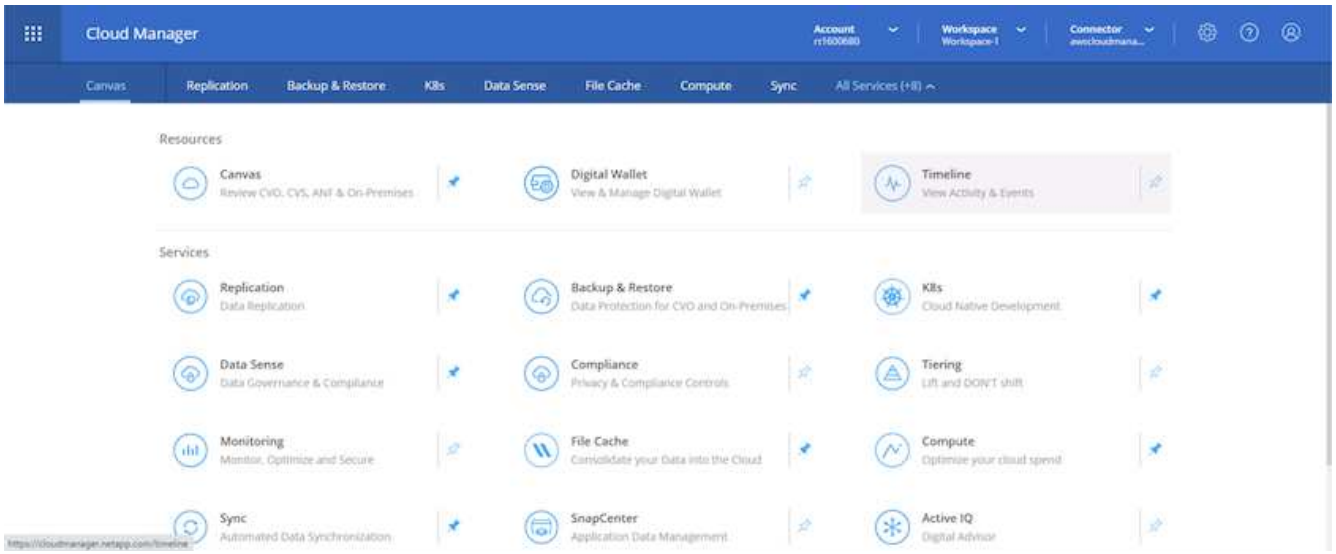
7. 선택 사항을 검토하고 상자를 선택하여 Cloud Manager가 AWS 환경에 리소스를 구축함을 이해했는지 확인합니다. 준비가 되면 이동 을 클릭합니다.



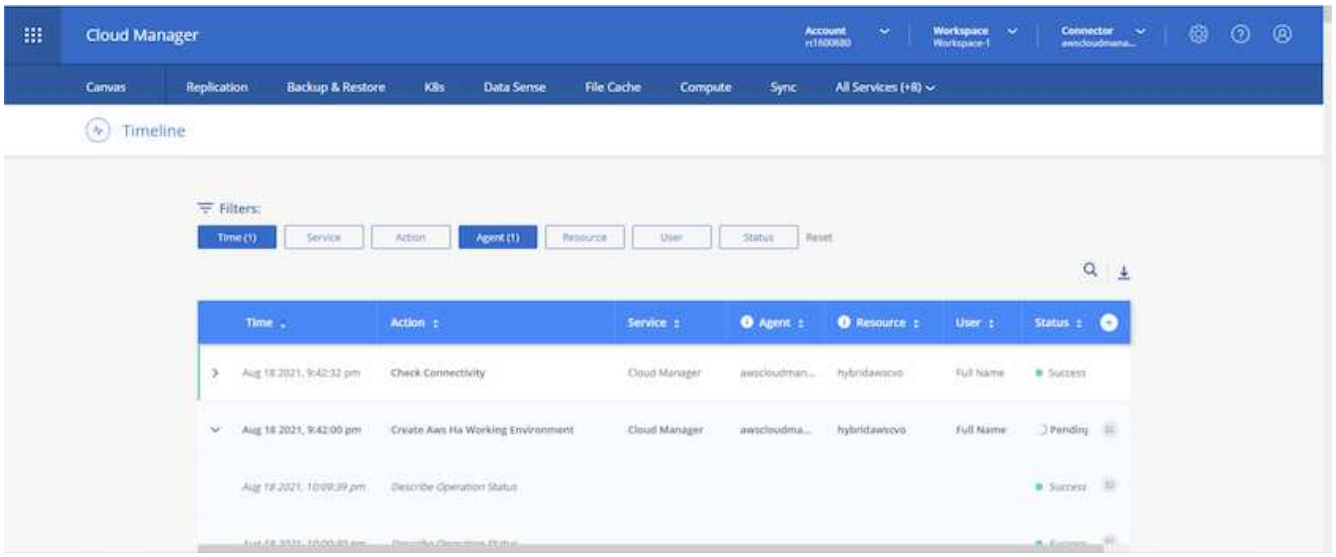
8. 이제 Cloud Volumes ONTAP가 배포 프로세스를 시작합니다. Cloud Manager는 AWS API 및 클라우드 형성 스택을 사용하여 Cloud Volumes ONTAP를 구축합니다. 그런 다음 시스템을 사양에 맞게 구성하여 즉시 활용할 수 있는 즉시 사용 가능한 시스템을 제공합니다. 이 프로세스의 타이밍은 선택한 항목에 따라 달라집니다.



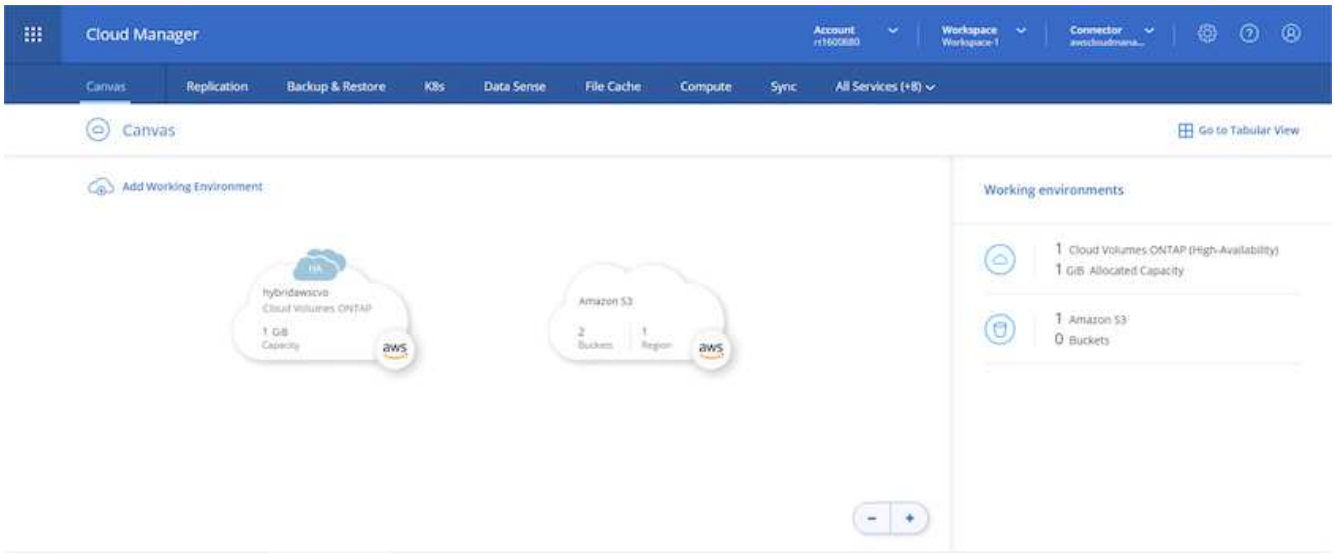
9. 타임라인으로 이동하여 진행 상황을 모니터링할 수 있습니다.



10. 타임라인은 Cloud Manager에서 수행된 모든 작업에 대한 감사 역할을 합니다. AWS와 ONTAP 클러스터 모두에 설정하는 동안 Cloud Manager에서 수행하는 모든 API 호출을 볼 수 있습니다. 또한 이 기능을 사용하면 발생하는 모든 문제를 효과적으로 해결할 수 있습니다.



11. 구축이 완료되면 CVO 클러스터가 현재 용량인 Canvas에 표시됩니다. 현재 상태의 ONTAP 클러스터는 즉시 사용 가능한 진정한 환경을 제공할 수 있도록 완전히 구성되어 있습니다.

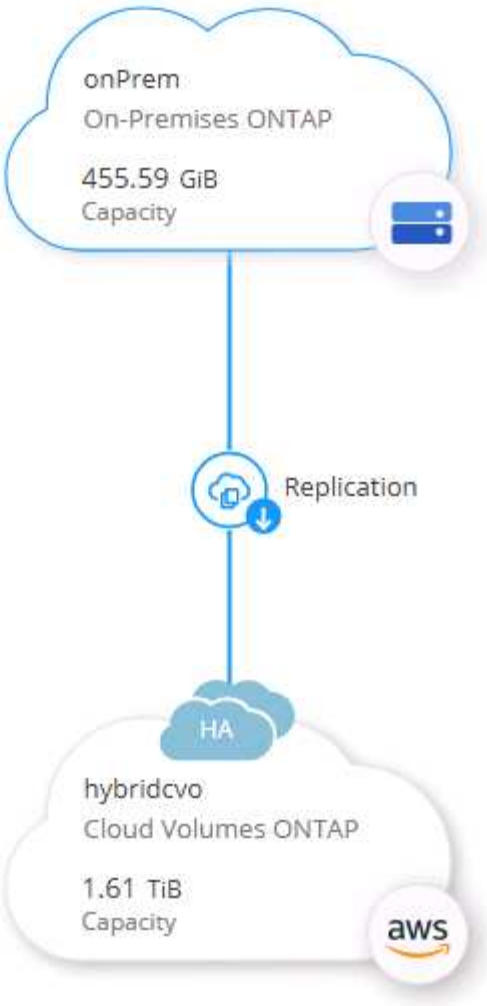


사내에서 클라우드까지 **SnapMirror**를 구성합니다

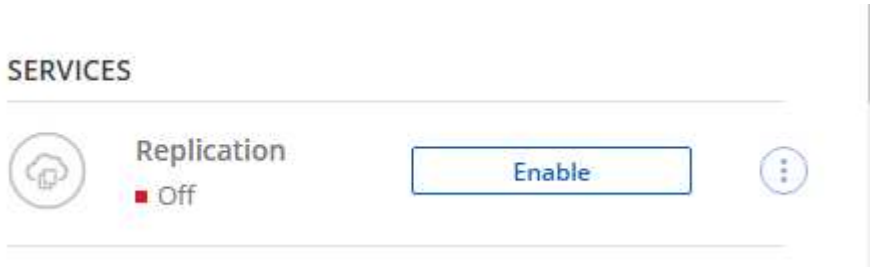
소스 ONTAP 시스템과 타겟 ONTAP 시스템을 구축했으므로 이제 데이터베이스 데이터가 포함된 볼륨을 클라우드에 복제할 수 있습니다.

SnapMirror용 호환 ONTAP 버전에 대한 지침은 를 참조하십시오 "SnapMirror 호환성 매트릭스".

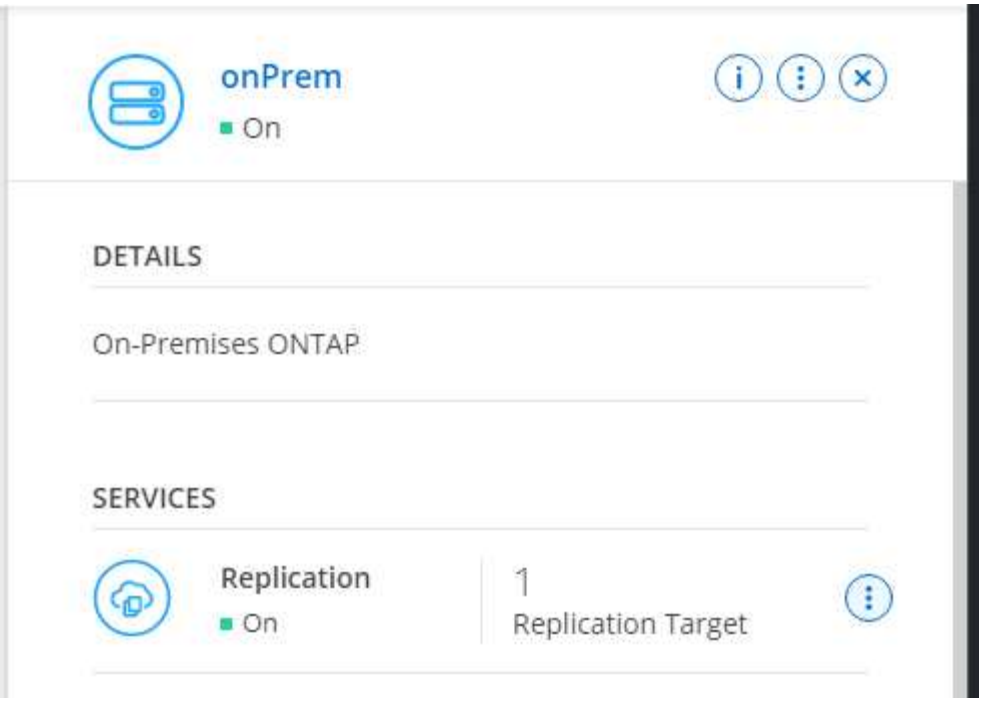
1. 소스 ONTAP 시스템(온-프레미스)을 클릭하고 대상을 끌어다 놓고 복제 > 활성화 를 선택하거나 복제 > 메뉴 > 복제 를 선택합니다.



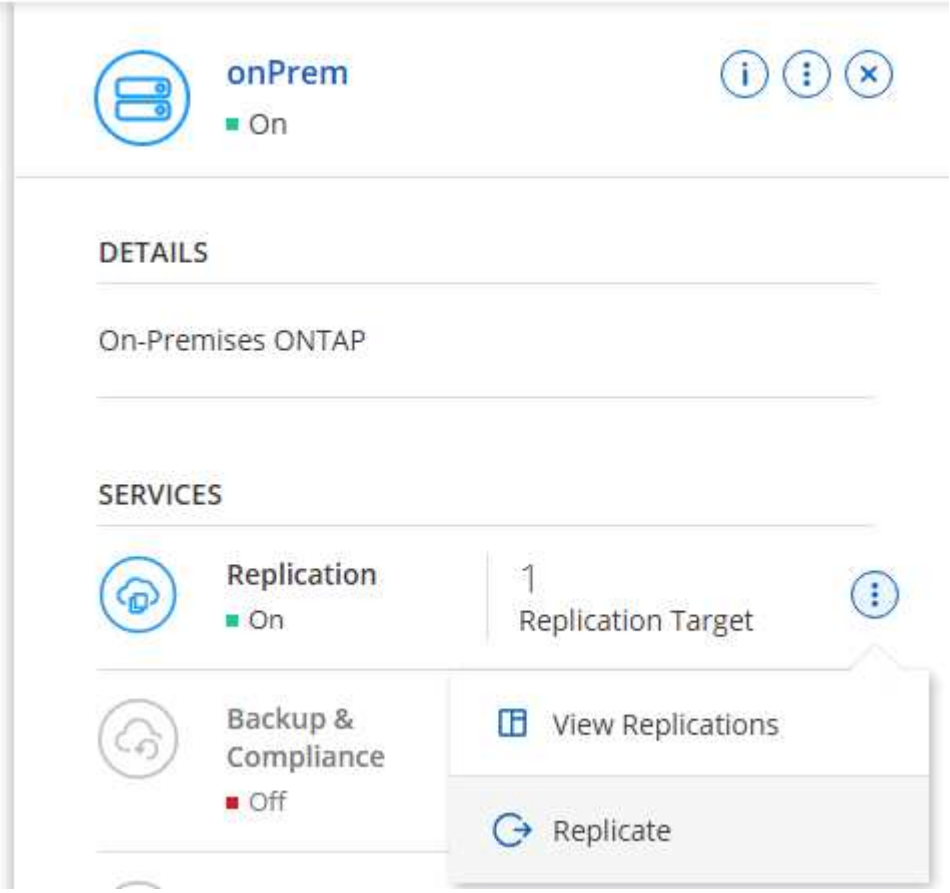
사용을 선택합니다.



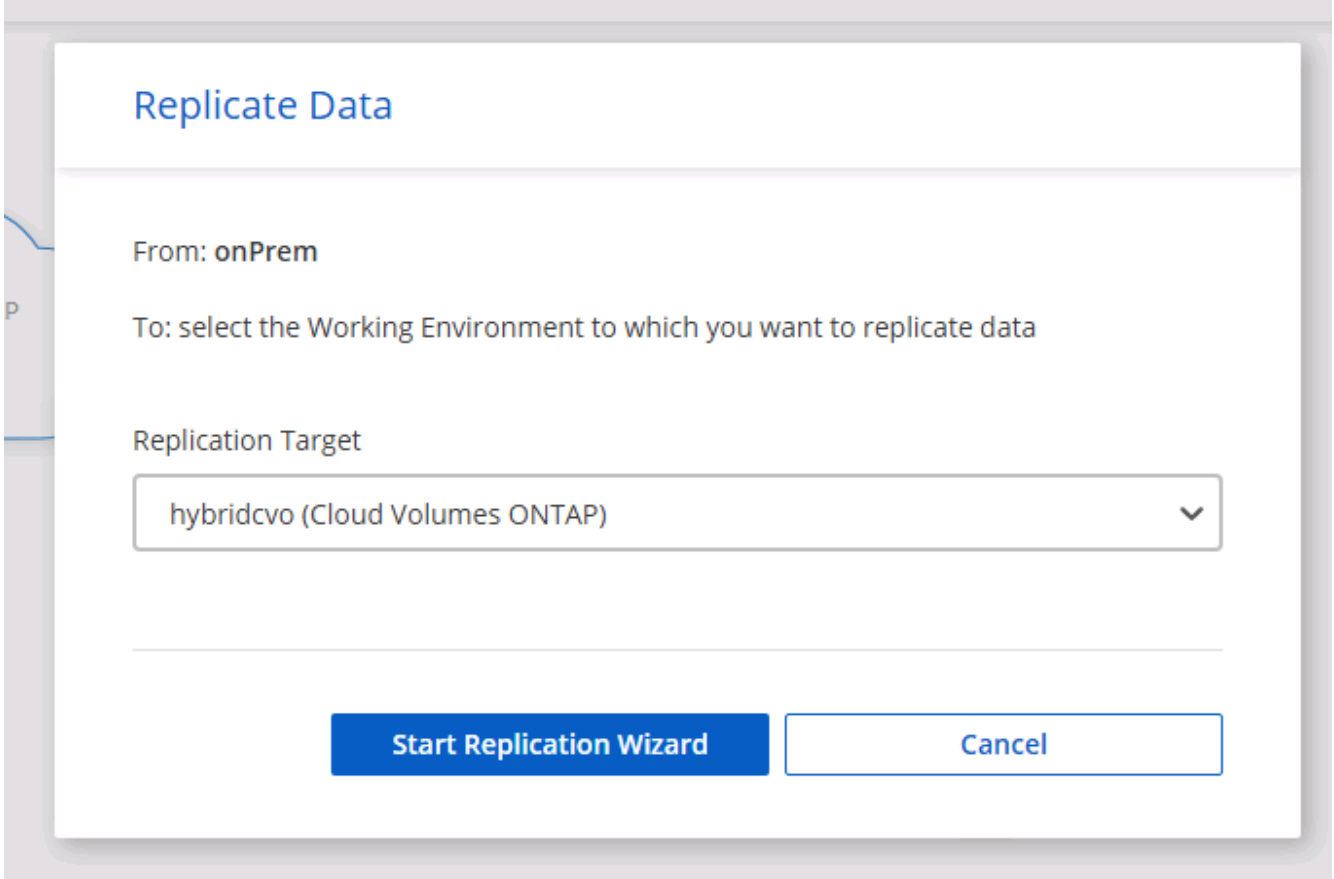
또는 옵션 을 선택합니다.



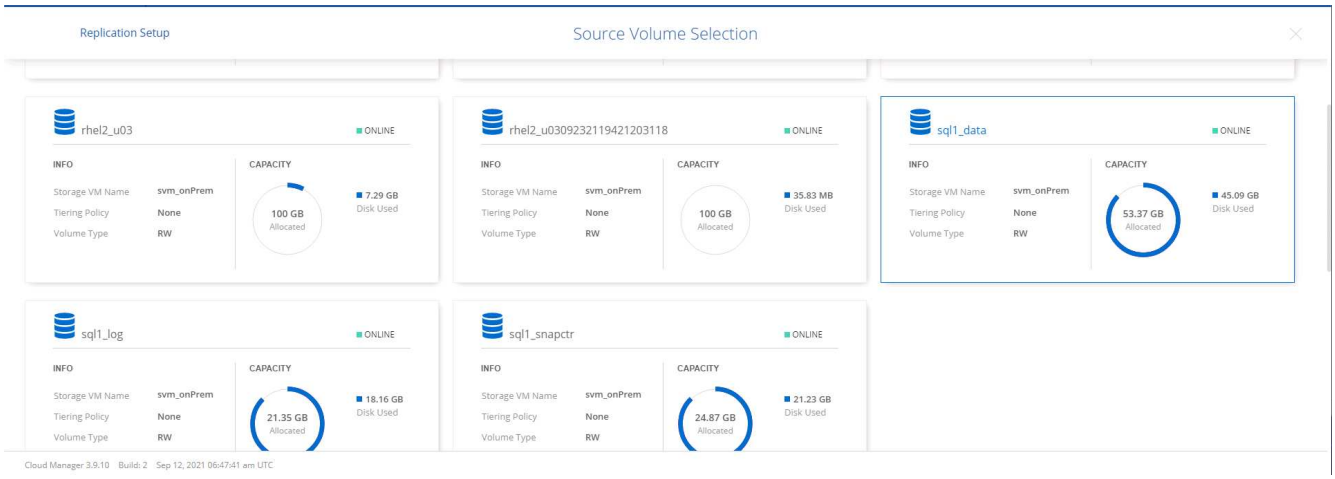
복제.



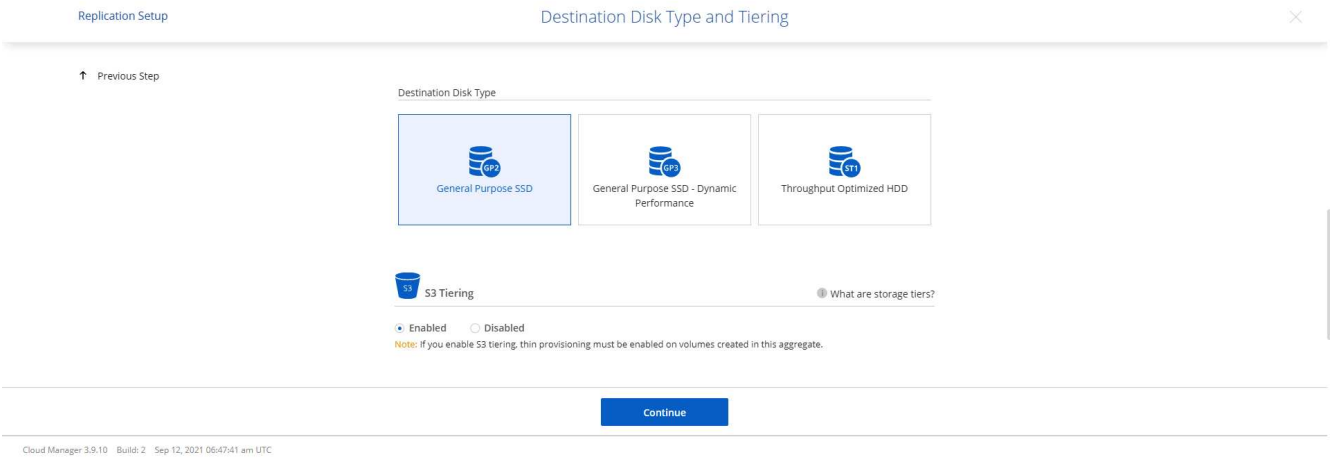
2. 끌어서 놓기를 하지 않은 경우 복제할 대상 클러스터를 선택합니다.



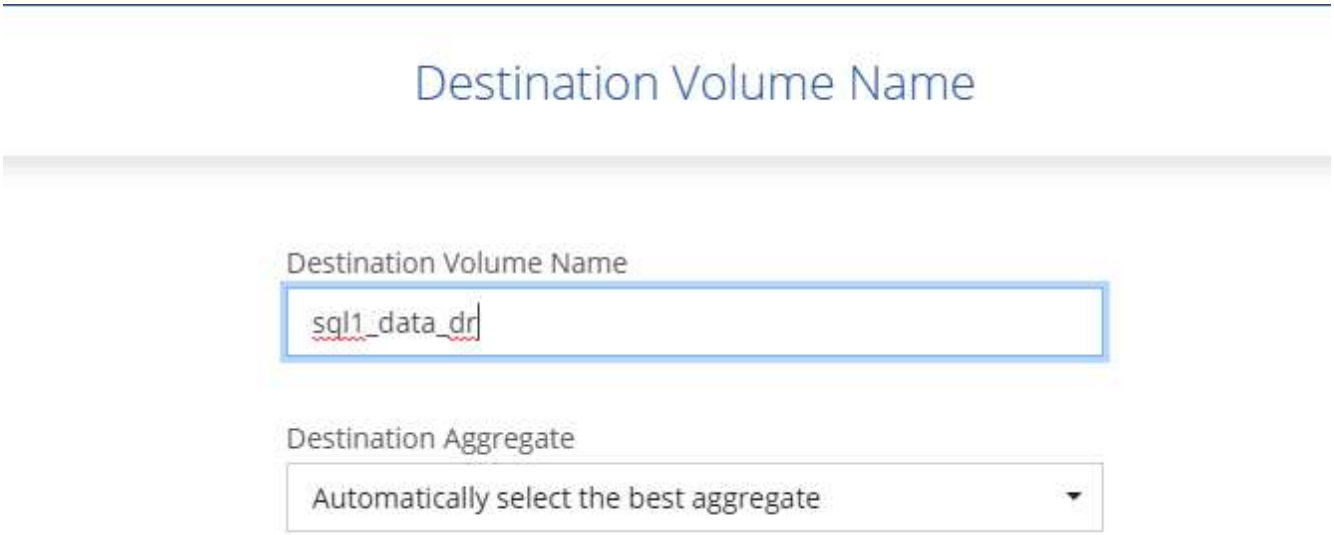
3. 복제할 볼륨을 선택합니다. 데이터와 모든 로그 볼륨을 복제했습니다.



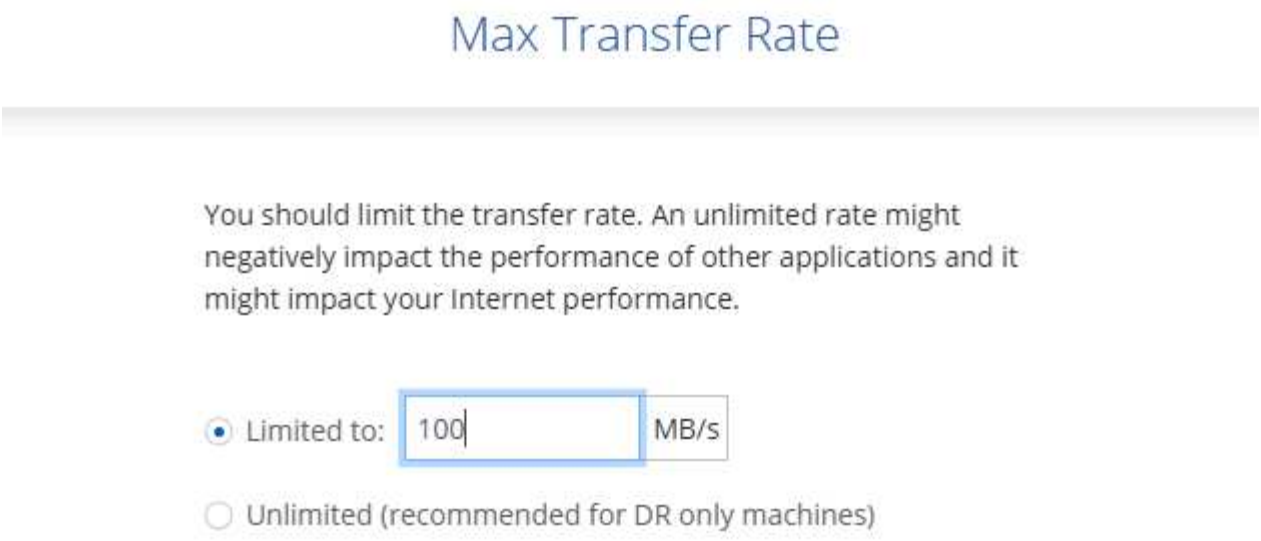
4. 대상 디스크 유형 및 계층화 정책을 선택합니다. 재해 복구를 위해 디스크 유형으로 SSD를 사용하고 데이터 계층화를 유지하는 것이 좋습니다. 데이터 계층화는 미러링된 데이터를 저비용 오브젝트 스토리지로 계층화하여 로컬 디스크의 비용을 절감합니다. 관계를 끊거나 볼륨을 클론하면 데이터에 빠른 로컬 스토리지가 사용됩니다.



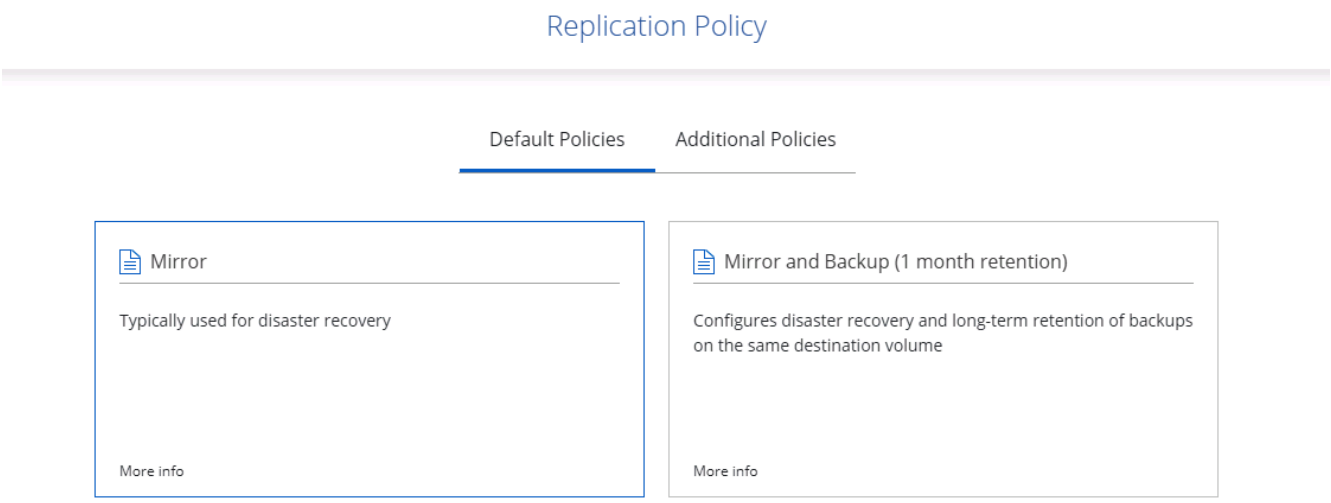
5. 대상 볼륨 이름 선택: '[source_volume_name]_dr'을 선택했습니다.



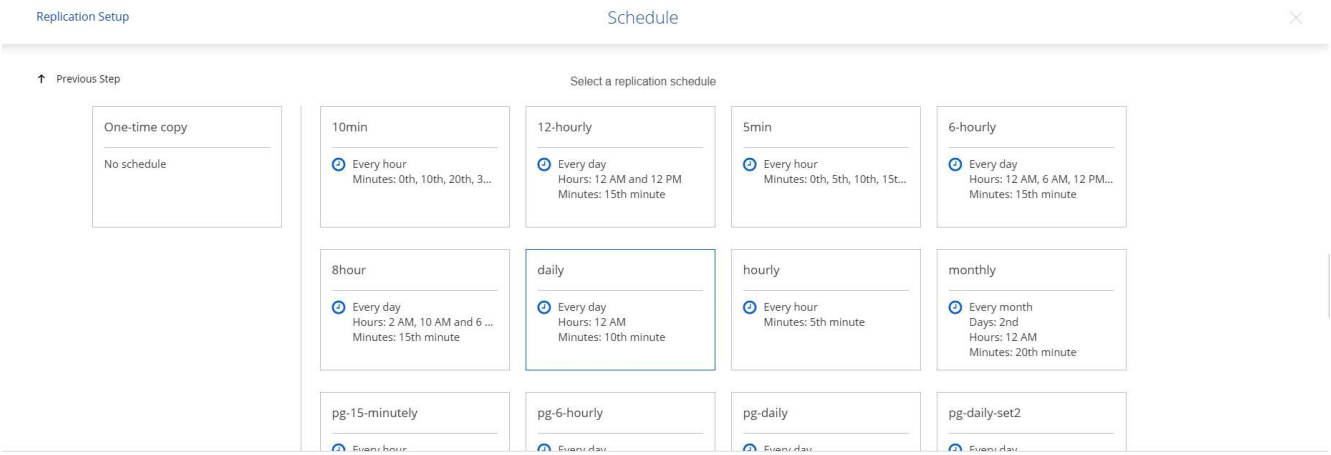
6. 복제에 대한 최대 전송 속도를 선택합니다. 따라서 VPN과 같이 클라우드에 대역폭이 낮은 경우 대역폭을 절약할 수 있습니다.



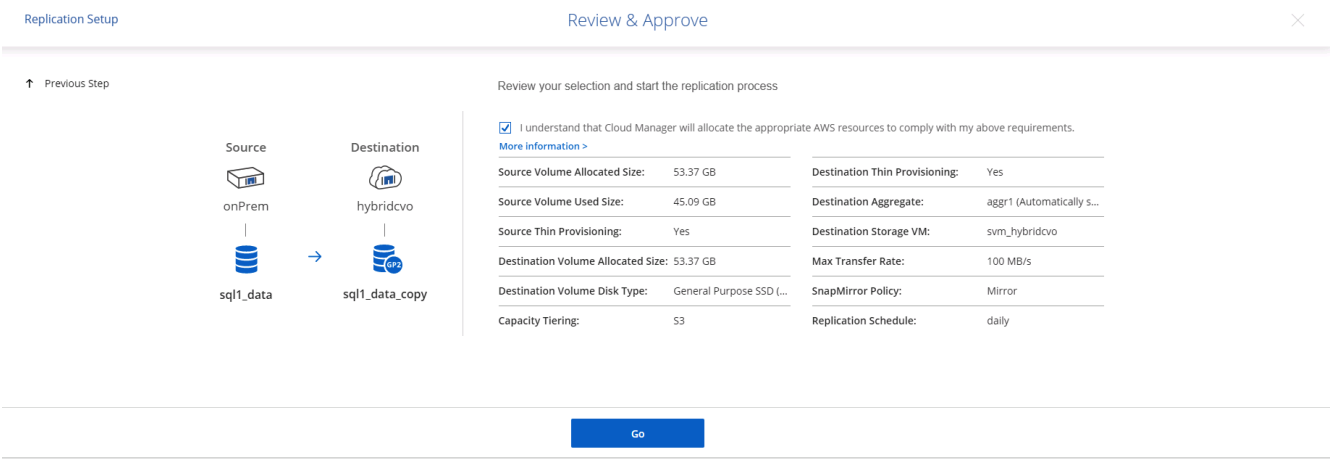
7. 복제 정책을 정의합니다. 우리는 미러를 선택했습니다. 이 미러는 최신 데이터 세트를 가져와 타겟 볼륨에 복제합니다. 요구 사항에 따라 다른 정책을 선택할 수도 있습니다.



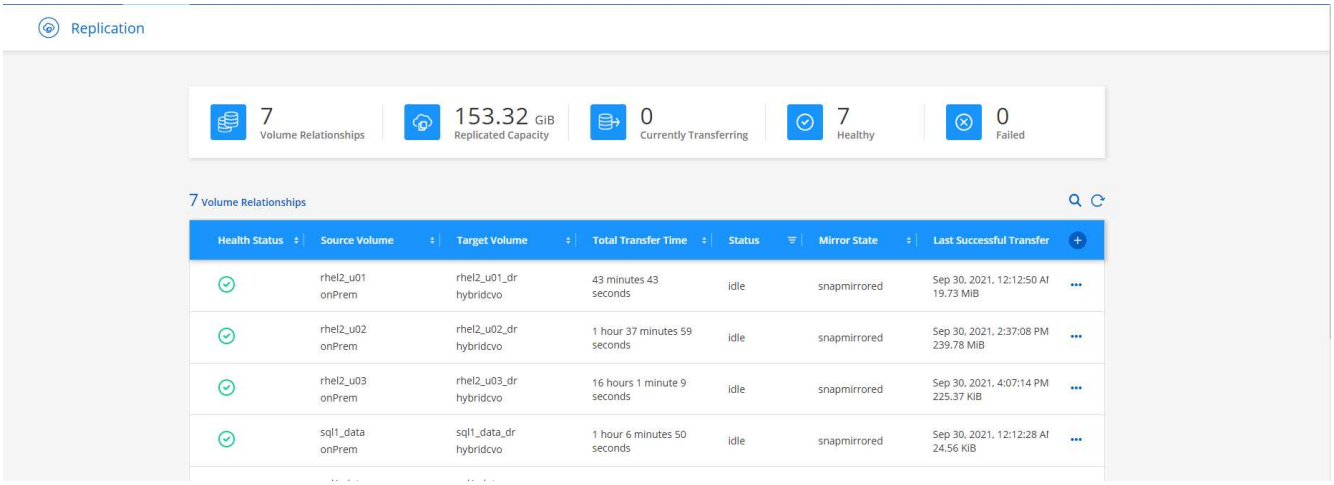
8. 복제를 트리거할 스케줄을 선택합니다. 요구사항에 따라 변경할 수 있지만 데이터 볼륨에 대한 "일별" 스케줄과 로그 볼륨에 대한 "시간별" 스케줄을 설정하는 것이 좋습니다.



9. 입력한 정보를 검토하고 이동을 클릭하여 클러스터 피어와 SVM 피어를 트리거한 다음(두 클러스터 간에 처음 복제하는 경우) SnapMirror 관계를 구축하고 초기화합니다.



10. 데이터 볼륨 및 로그 볼륨에 대해 이 프로세스를 계속합니다.
11. 모든 관계를 확인하려면 Cloud Manager 내의 Replication 탭으로 이동합니다. 여기에서 관계를 관리하고 상태를 확인할 수 있습니다.



12. 모든 볼륨이 복제된 후에는 안정적 상태가 되며 재해 복구 및 개발/테스트 워크플로우로 이동할 준비가 된 것입니다.

데이터베이스 워크로드에 **EC2** 컴퓨팅 인스턴스를 구축합니다

AWS는 다양한 워크로드를 위해 EC2 컴퓨팅 인스턴스를 사전 구성되어 있습니다. 인스턴스 유형 선택에 따라 CPU 코어 수, 메모리 용량, 스토리지 유형 및 용량, 네트워크 성능이 결정됩니다. 사용 사례의 경우, OS 파티션을 제외하고 데이터베이스 워크로드를 실행할 기본 스토리지가 CVO 또는 FSx ONTAP 스토리지 엔진에서 할당됩니다. 따라서 고려해야 할 주요 요소는 CPU 코어, 메모리 및 네트워크 성능 수준을 선택하는 것입니다. 일반적인 AWS EC2 인스턴스 유형은 여기에서 찾을 수 있습니다. "EC2 인스턴스 유형".

컴퓨팅 인스턴스 사이징

1. 필요한 워크로드를 기준으로 적합한 인스턴스 유형을 선택합니다. 고려해야 할 요소에는 지원할 비즈니스 트랜잭션 수, 동시 사용자 수, 데이터 세트 사이징 등이 포함됩니다.
2. EC2 대시보드에서 EC2 인스턴스 구축을 시작할 수 있습니다. 정확한 배포 절차는 이 솔루션의 범위를 벗어납니다. 을 참조하십시오 "Amazon EC2" 를 참조하십시오.

Oracle 워크로드를 위한 **Linux** 인스턴스 구성

이 섹션에는 EC2 Linux 인스턴스를 배포한 이후의 추가 구성 단계가 포함되어 있습니다.

1. SnapCenter 관리 도메인 내에서 이름 확인을 위해 DNS 서버에 Oracle 대기 인스턴스를 추가합니다.
2. 암호 없이 sudo 권한을 가진 SnapCenter OS 자격 증명으로 Linux 관리 사용자 ID를 추가합니다. EC2 인스턴스에서 SSH 암호 인증을 사용하여 ID를 활성화합니다. (기본적으로 EC2 인스턴스에서는 SSH 암호 인증 및 암호 없는 sudo가 해제되어 있습니다.)
3. OS 패치, Oracle 버전 및 패치 등과 같은 온프레미스 Oracle 설치와 일치하도록 Oracle 설치를 구성합니다.
4. NetApp Ansible DB 자동화 역할을 활용하여 데이터베이스 개발/테스트 및 재해 복구 사용 사례에 맞게 EC2 인스턴스를 구성할 수 있습니다. 자동화 코드는 NetApp 퍼블릭 GitHub 사이트에서 다운로드할 수 있습니다. "Oracle 19c 자동화된 구축". 목표는 사내 OS 및 데이터베이스 구성과 일치하도록 EC2 인스턴스에 데이터베이스 소프트웨어 스택을 설치 및 구성하는 것입니다.

SQL Server 작업 부하에 대한 **Windows** 인스턴스 구성

이 섹션에는 EC2 Windows 인스턴스를 처음 구축한 이후의 추가 구성 단계가 나와 있습니다.

1. RDP를 통해 인스턴스에 로그인하려면 Windows 관리자 암호를 검색합니다.
2. Windows 방화벽을 비활성화하고, 호스트를 Windows SnapCenter 도메인에 연결하고, DNS 서버에 인스턴스를 추가하여 이름을 확인합니다.
3. SnapCenter 로그 볼륨을 프로비저닝하여 SQL Server 로그 파일을 저장합니다.
4. Windows 호스트에서 iSCSI를 구성하여 볼륨을 마운트하고 디스크 드라이브를 포맷합니다.
5. SQL Server용 NetApp 자동화 솔루션을 사용하면 이전 작업 중 많은 작업을 자동화할 수 있습니다. 새로 게시된 역할 및 솔루션은 NetApp 자동화 퍼블릭 GitHub 사이트 에서 확인할 수 있습니다. "NetApp 자동화".

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.