



IBM Db2 보호 SnapCenter software

NetApp
November 06, 2025

목차

IBM Db2 보호	1
IBM Db2용 SnapCenter 플러그인	1
IBM Db2용 SnapCenter 플러그인 개요	1
IBM Db2용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업	1
IBM Db2용 SnapCenter 플러그인 기능	2
IBM Db2용 SnapCenter 플러그인에서 지원하는 스토리지 유형	2
IBM Db2 플러그인에 필요한 최소 ONTAP 권한	3
IBM Db2용 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	6
IBM Db2에 대한 백업 전략	6
IBM Db2에 대한 복원 및 복구 전략	8
IBM Db2용 SnapCenter 플러그인 설치를 준비하세요	10
IBM Db2용 SnapCenter 플러그인 설치 워크플로	10
Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	10
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	15
Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	16
IBM Db2용 SnapCenter 플러그인에 대한 자격 증명 설정	17
Windows Server 2016 이상에서 gMSA 구성	19
IBM Db2용 SnapCenter 플러그인 설치	20
CA 인증서 구성	25
데이터 보호를 준비하세요	33
IBM Db2용 SnapCenter 플러그인을 사용하기 위한 전제 조건	33
IBM Db2를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	33
IBM Db2 리소스 백업	34
IBM Db2 리소스 백업	34
데이터베이스를 자동으로 검색합니다	36
플러그인 호스트에 수동으로 리소스 추가	36
IBM Db2에 대한 백업 정책 만들기	37
리소스 그룹을 만들고 정책을 첨부합니다	40
ASA r2 시스템에서 IBM Db2 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다	43
PowerShell cmdlet을 사용하여 IBM Db2용 스토리지 시스템 연결 및 자격 증명 만들기	45
Db2 데이터베이스 백업	47
리소스 그룹 백업	52
IBM Db2 백업 작업 모니터링	53
IBM Db2에 대한 백업 작업 취소	54
토폴로지 페이지에서 IBM Db2 백업 및 복제본 보기	55
IBM Db2 복원	56
워크플로 복원	56
수동으로 추가된 리소스 백업 복원	57
자동 검색된 데이터베이스 백업을 복원하고 복구합니다	61

IBM Db2 복원 작업 모니터링	62
IBM Db2 리소스 백업 복제	63
복제 워크플로	63
IBM Db2 백업 복제	64
IBM Db2 복제 작업 모니터링	71
클론 분할	72
SnapCenter 업그레이드 후 IBM Db2 데이터베이스 복제본 삭제 또는 분할	73

IBM Db2 보호

IBM Db2용 SnapCenter 플러그인

IBM Db2용 SnapCenter 플러그인 개요

IBM Db2 데이터베이스용 SnapCenter 플러그인은 IBM Db2 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter software 의 호스트 측 구성 요소입니다. IBM Db2 데이터베이스용 플러그인은 SnapCenter 환경에서 IBM Db2 데이터베이스의 백업, 복원 및 복제를 자동화합니다.

- SnapCenter 6.0은 IBM Db2 10.5 이상을 지원합니다.
- SnapCenter 6.0.1은 IBM Db2 9.7.x 이상을 지원합니다. 또한 SnapCenter 6.0.1부터 AIX에서 IBM Db2가 지원됩니다.

SnapCenter 단일 인스턴스 및 다중 인스턴스 Db2 설정을 지원합니다. Linux와 Windows 환경 모두에서 IBM Db2 데이터베이스 플러그인을 사용할 수 있습니다. Windows 환경에서는 Db2가 수동 리소스로 지원됩니다.



Db2 pureScale 환경 및 Db2 다중 노드(DPF) 시스템은 지원되지 않습니다.

IBM Db2 데이터베이스용 플러그인이 설치되면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들 수 있습니다. NetApp SnapVault 기술과 함께 플러그인을 사용하면 표준을 준수하기 위해 디스크 간 백업 복제를 수행할 수도 있습니다.

Db2용 SnapCenter 플러그인은 ONTAP 및 Azure NetApp 파일 스토리지 레이아웃에서 NFS와 SAN을 지원합니다.

VMDK, vVol 및 RDM 가상 스토리지 레이아웃이 지원됩니다.

IBM Db2용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업

사용자 환경에 IBM Db2 데이터베이스용 플러그인을 설치하면 SnapCenter 사용하여 IBM Db2 데이터베이스와 해당 리소스를 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 데이터베이스를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

IBM Db2용 SnapCenter 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. IBM Db2 데이터베이스용 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 비중단 **NetApp** 스냅샷 복사 기술

SnapCenter IBM Db2 Database용 플러그인과 함께 NetApp 스냅샷 기술을 사용하여 리소스를 백업합니다.

IBM Db2 플러그인을 사용하면 다음과 같은 이점도 얻을 수 있습니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP 의 일관성 그룹(CG) 스냅샷 기능에 대한 지원.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- XFS 파일 시스템에서 Linux LVM을 지원합니다.

IBM Db2용 SnapCenter 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. IBM Db2용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
물리적 서버	<ul style="list-style-type: none"> • FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨
VMware ESXi	<ul style="list-style-type: none"> • FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. _opt/ NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • VMFS에 VMDK가 생성됨 • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

IBM Db2 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 생성
 - lun 생성
 - lun 삭제

- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-is-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지

- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시

- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

IBM Db2용 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미리 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되므로 별도의 ONTAP 일정을 만들지 마세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

IBM Db2에 대한 백업 전략

IBM Db2에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.
4. 데이터베이스의 애플리케이션 일관성 스냅샷을 백업하기 위해 스냅샷 복사 기반 정책을 생성할지 여부를 결정합니다.
5. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
6. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
7. 백업 작업 전이나 후에 명령을 실행할지 여부를 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 IBM Db2 데이터베이스와 인스턴스입니다. IBM Db2용 SnapCenter 플러그인을 설치하면 해당 Linux 호스트의 모든 인스턴스에 있는 IBM Db2 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter IBM Db2 데이터베이스에 대한 스냅샷 복사 기반 백업 유형을 지원합니다.

스냅샷 복사 기반 백업

스냅샷 복사 기반 백업은 NetApp 스냅샷 기술을 활용하여 IBM Db2 데이터베이스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만듭니다.

IBM Db2용 SnapCenter 플러그인이 일관성 그룹 스냅샷을 사용하는 방법

플러그인을 사용하면 리소스 그룹에 대한 일관성 그룹 스냅샷을 만들 수 있습니다. 일관성 그룹은 여러 볼륨을 수용하여 하나의 엔티티로 관리할 수 있는 컨테이너입니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷으로, 볼륨 그룹의 일관된 복사본을 제공합니다.

또한 스토리지 컨트롤러가 스냅샷을 일관되게 그룹화하는 데 걸리는 대기 시간을 지정할 수도 있습니다. 이용 가능한 대기 시간 옵션은 긴급, 보통, *느긋함*입니다. 일관된 그룹 스냅샷 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화하거나 비활성화할 수도 있습니다. WAFL 동기화는 일관성 그룹 스냅샷의 성능을 향상시킵니다.

SnapCenter 데이터 백업의 정리 작업을 관리하는 방법

SnapCenter 스토리지 시스템 및 파일 시스템 수준에서 데이터 백업의 정리 작업을 관리합니다.

기본 또는 보조 스토리지의 스냅샷과 IBM Db2 카탈로그의 해당 항목은 보존 설정에 따라 삭제됩니다.

IBM Db2 백업 일정을 결정하기 위한 고려 사항

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타

요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업을 수행할 빈도)

일부 플러그인의 경우 일정 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기)

백업 일정은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업을 위해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다.

IBM Db2에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

IBM Db2 데이터베이스용 플러그인에 대한 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `_dts1_`은 리소스 그룹 이름입니다.
- `_mach1x88_`은 호스트 이름입니다.
- `_03-12-2015_23.17.26_`은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, `customtext_resourcegroup_policy_hostname` 또는 `resourcegroup_hostname`입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

IBM Db2에 대한 복원 및 복구 전략

IBM Db2 리소스에 대한 복원 및 복구 전략 정의

데이터베이스를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.



데이터베이스의 수동 복구만 지원됩니다.

단계

1. 수동으로 추가된 IBM Db2 리소스에 대해 지원되는 복원 전략을 확인합니다.
2. 자동 검색된 IBM Db2 데이터베이스에 지원되는 복원 전략을 확인합니다.

수동으로 추가된 **IBM Db2** 리소스에 대해 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 IBM Db2 리소스에 대한 복원 전략에는 두 가지 유형이 있습니다.



수동으로 추가한 IBM Db2 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 촬영된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

자동으로 검색된 **IBM Db2**에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다.

전체 리소스 복원은 자동으로 검색된 IBM Db2 데이터베이스에 지원되는 복원 전략입니다. 이렇게 하면 리소스의 모든 볼륨, Q트리, LUN이 복원됩니다.

자동 검색된 **IBM Db2**에 대한 복원 작업 유형

IBM Db2용 SnapCenter 플러그인은 단일 파일 SnapRestore 및 자동으로 검색된 IBM Db2 데이터베이스에 대한 연결 및 복사 복원 유형을 지원합니다.

단일 파일 **SnapRestore** 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- 선택한 백업이 SnapMirror 또는 SnapVault 보조 위치에서 시작되고 전체 리소스 옵션이 선택된 경우

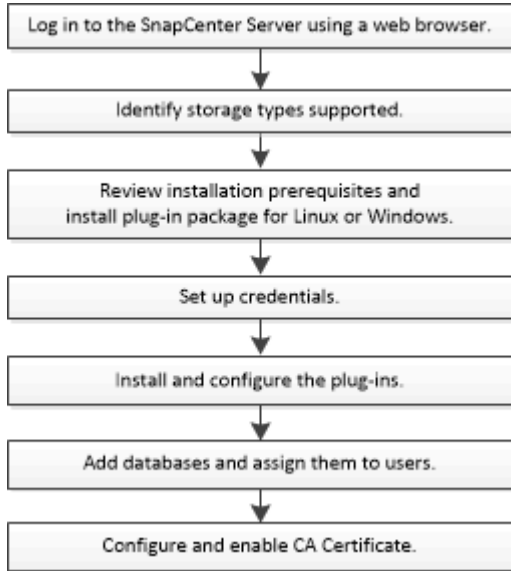
단일 파일 **SnapRestore** 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 전체 리소스 옵션을 선택한 경우

IBM Db2용 SnapCenter 플러그인 설치를 준비하세요

IBM Db2용 SnapCenter 플러그인 설치 워크플로

IBM Db2 데이터베이스를 보호하려면 IBM Db2용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. Windows, Linux 및 AIX 환경에서 지원되는 IBM Db2용 SnapCenter 플러그인입니다.

- 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows의 경우 플러그인 생성 서비스는 “LocalSystem” Windows 사용자를 사용하여 실행해야 합니다. 이는 IBM Db2용 플러그인이 도메인 관리자로 설치된 경우의 기본 동작입니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트의 IBM Db2 플러그인과 함께 배포됩니다.
- SnapCenter 서버는 IBM Db2 호스트용 플러그인의 8145 또는 사용자 정의 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- Windows 호스트에 IBM Db2용 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치했어야 합니다.

"Windows용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

Linux 및 AIX 호스트

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

"Linux용 JAVA 다운로드"

"AIX용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

- Linux 호스트에서 실행되는 IBM Db2 데이터베이스의 경우 IBM Db2용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위해 기본 셸로 `*bash*`를 사용해야 합니다.

보충 명령

IBM Db2용 SnapCenter 플러그인에서 보충 명령을 실행하려면 `allowed_commands.config` 파일에 해당 명령을 포함해야 합니다.

- Windows 호스트의 기본 위치: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 호스트의 기본 위치: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 편집기에서 `allowed_commands.config` 파일을 엽니다. 각 명령을 별도의 줄에 입력하세요. 명령은 대소문자를 구분하지 않습니다. 완전히 정규화된 경로 이름을 지정하고, 경로 이름에 공백이 포함된 경우 따옴표(")로 묶으세요.

예를 들어:

명령어: `mount`

명령어: `umount`

명령: `"C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe"`

명령어: `myscript.bat`

`allowed_commands.config` 파일이 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

`"/mnt/mount -a]` 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."

`_allowed_commands.config`에 명령이나 스크립트가 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

`"/mnt/mount -a]` 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."



모든 명령을 허용하려면 와일드카드 항목(*)을 사용해서는 안 됩니다.

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 사용하면 루트가 아닌 사용자도 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- `/etc/ssh/sshd_config` 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 `/etc/sudoers` 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `_etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_LINUX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

AIX 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 4.4 이상에서는 루트가 아닌 사용자도 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 `sudo` 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.

- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- /etc/ssh/sshd_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. AIX용 SnapCenter 플러그인 패키지를 설치하려는 AIX 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `/etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_AIX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	<p>마이크로소프트 윈도우</p> <p>지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .</p>
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	<p>5GB</p> <div>  <p>충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.</p> </div>
필수 소프트웨어 패키지	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK <p>지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .</p>

Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	<ul style="list-style-type: none"> • 레드햇 엔터프라이즈 리눅스 • SUSE Linux Enterprise Server(SLES) <p>지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .</p>
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB

목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB <div>  <p>충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.</p> </div>
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK <p>JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.</p> <p>지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".</p>

IBM Db2용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

- 리눅스 호스트

Linux 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	<p>인증에 사용할 사용자 이름과 비밀번호를 입력하세요.</p> <ul style="list-style-type: none"> • 도메인 관리자 또는 관리자 그룹의 모든 구성원 <p>SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다.</p> <ul style="list-style-type: none"> ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) <p>작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다.</p> <p><i>UserName</i></p> <p>비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.</p>
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	사용할 인증 모드를 선택하세요.
sudo 권한을 사용하세요	<p>루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.</p> <div>  Linux 사용자에게만 적용됩니다. </div>

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.
이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

IBM Db2용 SnapCenter 플러그인 설치

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 관리 문서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"IBM Db2에 대해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	<p>호스트 유형을 선택하세요:</p> <ul style="list-style-type: none"> • Windows • 리눅스 <div>  <p>IBM Db2용 플러그인은 IBM Db2 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다.</p> </div>
호스트 이름	<p>통신 호스트 이름을 입력하세요. 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.</p>
신임장	<p>생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요.</p> <p>제공한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.</p> <div>  <p>자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.</p> </div>

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

REST API를 사용하여 Db2용 플러그인을 설치하는 경우 버전을 3.0으로 전달해야 합니다. 예를 들어, Db2:3.0

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	<p>기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트에 표시됩니다.</p> <div>  <p>플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.</p> </div>
설치 경로	<p>IBM Db2용 플러그인은 IBM Db2 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다.</p> <ul style="list-style-type: none"> • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/ NetApp/snapcenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
사전 설치 확인 건너뛰기	<p>플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.</p>
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	<p>Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.</p> <div>  <p>다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.</p> </div> <div>  <p>gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.</p> </div>

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트의 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 11(Windows 및 Linux 플러그인 모두)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을

충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\ NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

- Windows 플러그인의 경우 설치 및 업그레이드 로그는 다음 위치에 있습니다. C:\Windows\ SnapCenter plugin\Install<JOBID>\
- Linux 플러그인의 경우 설치 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log에 있고 업그레이드 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Upgrade<JOBID>.log에 있습니다.

당신이 완료한 후

SnapCenter 6.0 이상으로 업그레이드하려는 경우 기존 PERL 기반 Db2 플러그인이 원격 플러그인 서버에서 제거됩니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows**용 **SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 -skiprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **IBM Db2용 SnapCenter** 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 IBM Db2 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 IBM Db2 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- IBM Db2 클라이언트가 있는 각 Linux 호스트에 IBM Db2 데이터베이스용 플러그인을 설치해야 합니다.
- IBM Db2 데이터베이스용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 구성에 대한 최신 정보가 포함되어 있습니다.

"NetApp 상호 운용성 매트릭스 도구"

- IBM Db2 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter 이미 설치되어 있어야 합니다.

이 작업에 관하여

매개변수가 언급되지 않으면 SnapCenter 기본값으로 설치됩니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 C:\ProgramData\NetApp\ SnapCenter\Package Repository에서 IBM Db2용 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: path_to_installation_bin_file/snapcenter_linux_host_plugin.bin
-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address
-DSERVER_HTTPS_PORT=port_number_for_server
 - -DPORT는 SMCORE HTTPS 통신 포트를 지정합니다.
 - -DSERVER_IP는 SnapCenter 서버 IP 주소를 지정합니다.
 - -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
 - -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
 - DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<설치 디렉토리>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음

PLUGINS_ENABLED = DB2:3.0 매개변수를 추가합니다.

5. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.






명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

IBM Db2 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCORE 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 SnapCenter IBM Db2 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `_opt/ NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된
비밀번호와 동일하게 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.


```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **SnapCenter IBM Db2** 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **CA** 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 KEYSTORE_PASS 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

```
C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키tool -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. keystore.jks 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

키툴 `-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -대상키스토어 keystore.jks -대상키스토어 유형 JKS`

5. 키스토어에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 `agent.properties` 파일의 `KEYSTORE_PASS` 키 값입니다.

키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks

8. `agent.properties` 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 `SCC_CERTIFICATE_ALIAS` 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 `'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'`입니다.

단계

1. `agent.properties` 파일에서 기본 디렉토리를 `CRL_PATH` 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.





cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비하세요

IBM Db2용 SnapCenter 플러그인을 사용하기 위한 전제 조건

IBM Db2용 SnapCenter 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 11을 설치합니다.

호스트 머신의 환경 경로 변수에 Java 경로를 설정해야 합니다.

- 백업 복제가 필요한 경우 SnapMirror 와 SnapVault 설정하세요.

IBM Db2를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 로 백업하거나 복제하는 IBM Db2 데이터베이스입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당

작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 데이터 보호 작업의 백업 빈도, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

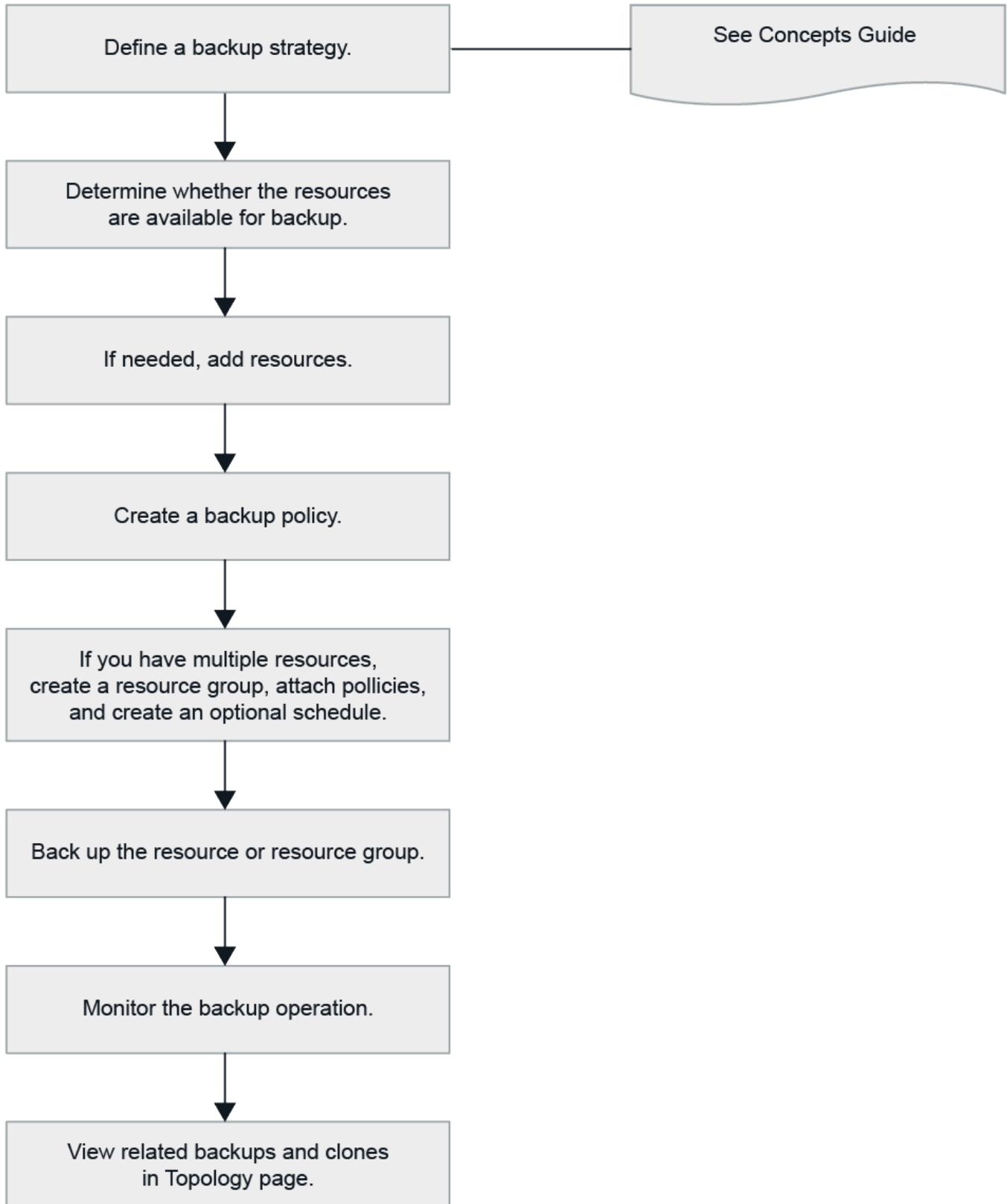
리소스 그룹은 무엇을 보호하고 싶은지, 언제 보호하고 싶은지 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹이 매일 전체 백업을 수행하도록 구성할 수 있습니다.

IBM Db2 리소스 백업

IBM Db2 리소스 백업

리소스(데이터베이스) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 워크플로에는 계획, 백업할 데이터베이스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

데이터베이스를 자동으로 검색합니다

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 IBM Db2 데이터베이스입니다. 사용 가능한 IBM Db2 데이터베이스를 발견한 후 리소스 그룹에 리소스를 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에


- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 이미 완료했어야 합니다.
- IBM Db2용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 있는 리소스의 자동 검색을 지원하지 않습니다. 데이터베이스를 수동으로 추가하는 동안 가상 환경에 대한 저장소 정보를 제공해야 합니다.

이 작업에 관하여

- 플러그인을 설치하면 해당 Linux 호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.
- 데이터베이스만 자동으로 검색됩니다.

자동으로 검색된 리소스는 수정하거나 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 IBM Db2용 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) *를 클릭하세요  *를 선택한 다음 호스트 이름을 선택합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 호스트에서 사용 가능한 리소스를 알아보려면 *리소스 새로 고침*을 클릭하세요.

리소스는 리소스 유형, 호스트 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우 전체 상태 열에 보호되지 않음이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되며 백업 작업이 수행되지 않은 경우, 전체 상태 열에 백업이 실행되지 않았습니라는 메시지가 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공으로 변경됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

플러그인 호스트에 수동으로 리소스 추가

Windows 호스트에서는 자동 검색이 지원되지 않습니다. Db2 인스턴스와 데이터베이스 리소스를 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 완료했어야 합니다.

이 작업에 관하여

다음 구성에서는 수동 검색이 지원되지 않습니다.


- RDM 및 VMDK 레이아웃

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 드롭다운 목록에서 IBM Db2용 SnapCenter 플러그인을 선택합니다.
2. 리소스 페이지에서 *IBM DB2 리소스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	데이터베이스 이름을 지정하세요.
호스트 이름	호스트 이름을 입력하세요.
유형	데이터베이스 또는 인스턴스를 선택하세요.
사례	데이터베이스의 부모인 인스턴스의 이름을 지정합니다.
신임장	자격 증명을 선택하거나 자격 증명에 대한 정보를 추가하세요. 이는 선택 사항입니다.

4. 스토리지 공간 제공 페이지에서 스토리지 유형을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 클릭합니다.

선택 사항: *를 클릭할 수 있습니다.  * 아이콘을 클릭하면 다른 스토리지 시스템에서 볼륨, LUN, Q트리를 추가할 수 있습니다.

5. 선택 사항: 리소스 설정 페이지에서 Windows 호스트의 리소스에 대해 IBM Db2 플러그인에 대한 사용자 정의 키-값 쌍을 입력합니다.
6. 요약 검토한 후 *마침*을 클릭하세요.

호스트 이름, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 데이터베이스가 표시됩니다.

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

"사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다."

데이터베이스를 추가한 후 IBM Db2 데이터베이스 세부 정보를 수정할 수 있습니다.

IBM Db2에 대한 백업 정책 만들기

SnapCenter 사용하여 IBM Db2 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 IBM Db2 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스 그룹에 대한 정책을 재사용할 때 시간을 절약할 수 있습니다.

이 작업에 관하여

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이로 인해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보관하게 될 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

- 왼쪽 탐색 창에서 *설정*을 클릭합니다.
- 설정 페이지에서 *정책*을 클릭합니다.
- *새로 만들기*를 클릭합니다.
- 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
- 정책 유형 페이지에서 다음을 수행합니다.
 - 저장 유형을 선택하세요.
 - 사용자 정의 백업 설정 섹션에서 플러그인에 키-값 형식으로 전달해야 하는 특정 백업 설정을 제공합니다.

플러그인에 전달할 여러 개의 키-값을 제공할 수 있습니다.

- 스냅샷 및 복제 페이지에서 다음 작업을 수행합니다.

- 주문형, 매시간, 매일, 매주, 매월 중에서 선택하여 일정 빈도를 지정하세요.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있을 뿐만 아니라 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

- 스냅샷 설정 섹션에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. 스냅샷 보관 기간은 100년 미만이어야 합니다.



스냅샷 복사 기반 백업의 경우 SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이기 때문에 보존 작업이 실패할 수 있습니다.

b. 정책 라벨을 지정합니다.

원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

7. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다.
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요.
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

8. 요약 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.


리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

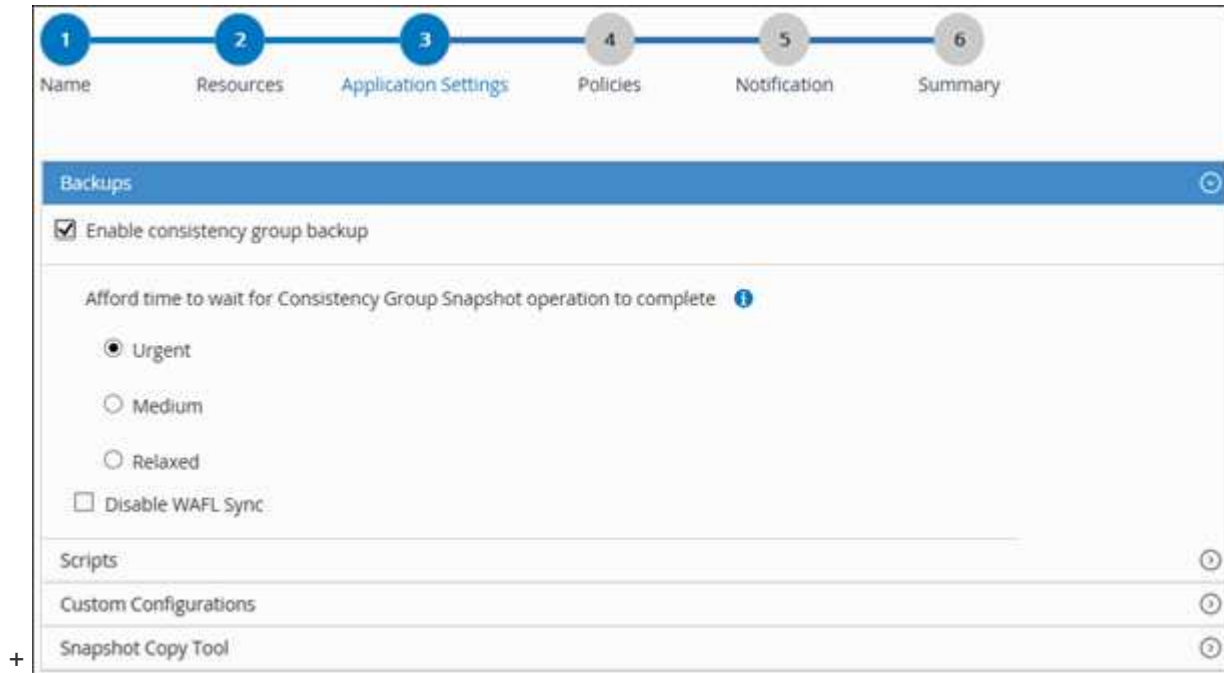
4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 다음을 수행합니다.
 - a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.



- 스크립트 화살표를 클릭하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 사용자 정의 구성 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.

매개변수	환경	설명
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.



사용자 정의 키-값 쌍은 IBM Db2 Linux 플러그인 시스템에서는 지원되지만 중앙화된 Windows 플러그인으로 등록된 IBM Db2 데이터베이스에서는 지원되지 않습니다.

- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 생성하기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷 복사본을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.


- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다.  *.

정책은 '선택한 정책에 대한 일정 구성' 섹션에 나열되어 있습니다.

- b.

일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.

- c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `policy_name`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 IBM Db2 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.


5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.


7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책_policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.




SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*을 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 IBM Db2용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 IBM Db2 데이터베이스를 백업, 복원 또는 복제하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter 에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. *SnapCenterPS*를 클릭하여 PowerShell Core를 시작합니다.
2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만드는 방법을 보여줍니다.

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$true
```

4. SnapCenter Server에 IBM Db2 통신 호스트를 추가합니다.

Linux의 경우:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'  
-CredentialName 'defaultcreds'
```

Windows의 경우:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'  
-CredentialName 'defaultcreds'
```

5. 호스트에 패키지와 IBM Db2용 SnapCenter 플러그인을 설치합니다.

Linux의 경우:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes  
DB2
```

Windows의 경우:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes DB2,SCW
```

6. SQLLIB의 경로를 설정합니다.

Windows의 경우 Db2 플러그인은 SQLLIB 폴더의 기본 경로인 "C:\Program Files\IBM\SQLLIB\BIN"을 사용합니다.

기본 경로를 재정의하려면 다음 명령을 사용하세요.

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

Db2 데이터베이스 백업

데이터베이스 백업에는 SnapCenter 서버와의 연결 설정, 리소스 추가, 정책 추가, 백업 리소스 그룹 생성 및 백업이 포함됩니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 스냅샷 복사 기반 백업 작업의 경우 모든 테넌트 데이터베이스가 유효하고 활성화되어 있는지 확인하세요.
- 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

선택하다 그런 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 선택할 수 있습니다. 필터 창을 닫으려면.

3. 백업할 리소스를 선택하세요.
4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
"일관성 그룹 스냅샷" 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

- 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.

백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 생성합니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.

원하신다면...	그 다음에...
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 선택하다 * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

_policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약 검토한 후 *마침*을 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 선택하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 - b. *백업*을 선택하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.
 - MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."](#)

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 수동 리소스를 추가합니다.

이 예제에서는 IBM Db2 인스턴스를 추가하는 방법을 보여줍니다.

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

Db2 데이터베이스의 경우:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.
4. Add-SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter 에 새 리소스 그룹을 추가합니다.

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

이 예제에서는 리소스 그룹을 백업하는 방법을 보여줍니다.

```
C:\PS> New-SMBackup -ResourceGroupName  
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

이 예제에서는 Db2 인스턴스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy  
db2_policy
```

이 예제에서는 Db2 데이터베이스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"  
} -Policy db2_policy
```

6. Get-smJobSummaryReport cmdlet을 사용하여 작업 상태(실행 중, 완료 또는 실패)를 모니터링합니다.

```
PS C:\> Get-SmJobSummaryReport -JobId 467  
  
SmJobId           : 467  
JobCreatedDateTime :  
JobStartDateTime  : 27-Jun-24 01:40:09  
JobEndDateTime     : 27-Jun-24 01:41:15  
JobDuration        : 00:01:06.7013330  
JobName            : Backup of Resource Group  
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy  
'snapshot-based-db2'  
JobDescription     :  
Status             : Completed  
IsScheduled        : False  
JobError           :  
JobType            : Backup  
PolicyName         : db2_policy  
JobResultData      :
```

7. Get-SmBackupReport cmdlet을 사용하여 복원 또는 복제 작업을 수행하기 위한 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링합니다.

```
PS C:\> Get-SmBackupReport -JobId 467
```

```
BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 84
SmJobId              : 467
StartDateTime        : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration             : 00:01:06.7013330
CreatedDateTime      : 27-Jun-24 18:39:45
Status               : Completed
ProtectionGroupName  : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId  : 23
PolicyName           : db2_policy
SmPolicyId           : 13
BackupName           : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DB2
PluginDisplayName     : IBM DB2
JobTypeId            :
JobHost              : HOSTFQDN
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은



필요하지 않습니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.







5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

IBM Db2 백업 작업 모니터링


SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.

- b. 시작일과 종료일을 지정하세요.
- c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
- d. 상태 드롭다운에서 백업 상태를 선택합니다.
- e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **IBM Db2** 데이터베이스의 데이터 보호 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리 활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

IBM Db2에 대한 백업 작업 취소


대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.




작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 IBM Db2 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.



표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.

3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. *요약 카드*를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약を確認하세요.

요약 카드 섹션에는 스냅샷 복사 기반 백업과 복제본의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

주문형 백업 후, 새로 고침 버튼을 클릭하면 백업이나 복제의 세부 정보가 새로 고침됩니다.


5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.


백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

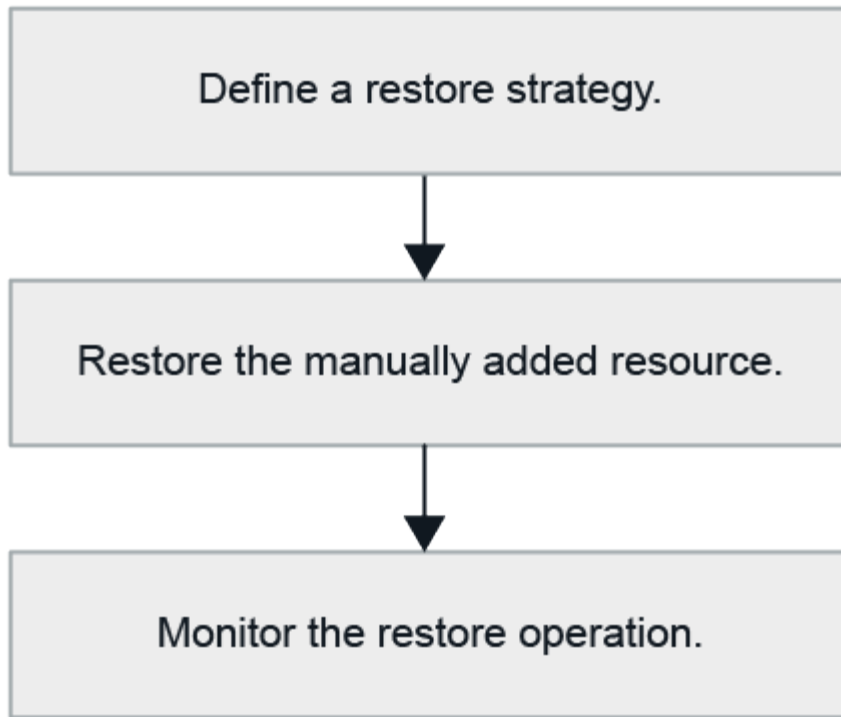
8. 복제본을 분할하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

IBM Db2 복원

워크플로 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#) .

수동으로 추가된 리소스 백업 복원

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.




백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01:35:06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *리소스 완료*를 선택합니다.

- a. *전체 리소스*를 선택하면 IBM Db2 데이터베이스의 구성된 모든 데이터 볼륨이 복원됩니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.

여러 개의 LUN을 선택할 수 있습니다.



*모두*를 선택하면 볼륨, Q트리 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.
8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.
9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

롤포워드 상태가 "DB 보류" 상태인 경우에만 복구가 가능합니다. 이 상태는 아카이브 로깅이 활성화된 Db2 데이터베이스에 적용됩니다.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 백업을 식별합니다.

이 예에서는 복원에 사용할 수 있는 백업이 두 개 있음을 보여줍니다.

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library

      BackupId      BackupName      BackupTime
-----
BackupType
-----
1      Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM Full Backup
2      Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.



AppObjectId는 "Host\Plugin\UID"이고, 여기서 UID = <instance_name>은 수동으로 검색된 DB2 인스턴스 리소스를 나타내고 UID = <instance_name>\<database_name>은 IBM Db2 데이터베이스 리소스를 나타냅니다. Get-smResources cmdlet에서 ResourceID를 가져올 수 있습니다.

```
Get-smResources -HostName cn24.sccore.test.com -PluginCode DB2
```

이 예제에서는 기본 저장소에서 데이터베이스를 복원하는 방법을 보여줍니다.

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

이 예제에서는 보조 저장소에서 데이터베이스를 복원하는 방법을 보여줍니다.

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

자동 검색된 데이터베이스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 자동 검색된 리소스의 경우 SFSR을 통해 복원이 지원됩니다.
- 자동 복구가 지원되지 않습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.




백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 옆에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.

5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *전체 리소스*를 선택하여 IBM Db2 데이터베이스의 구성된 데이터 볼륨을 복원합니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령이 필요하지 않습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령이 필요하지 않습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

롤포워드 상태가 "DB 보류" 상태인 경우에만 복구가 가능합니다. 이 상태는 아카이브 로깅이 활성화된 Db2 데이터베이스에 적용됩니다.







IBM Db2 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.


이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

IBM Db2 리소스 백업 복제

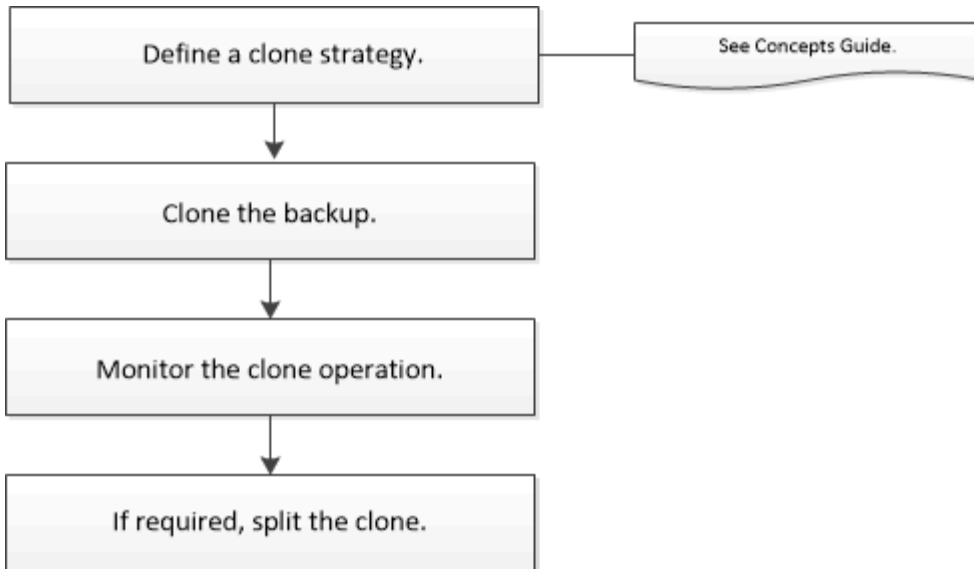
복제 워크플로

복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

- 소스 IBM Db2 서버에서 복제할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
 - 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
 - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
 - 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

당신이 완료한 후

자동으로 검색된 Db2 리소스를 복제한 후 복제된 리소스는 수동 리소스로 표시됩니다. 복제된 Db2 리소스를 복구하려면 *리소스 새로 고침*을 클릭하세요. 복제본을 삭제하면 저장소와 호스트도 정리됩니다.

복제 작업 후 리소스를 새로 고치지 않고 복제본을 삭제하려고 하면 스토리지와 호스트가 정리되지 않습니다. fstab에서 항목을 수동으로 삭제해야 합니다.

IBM Db2 백업 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 대체 호스트에서 Db2에 대한 복제본을 생성하는 동안 다른 호스트의 원래 마운트 경로와 동일한 복제본 마운트 경로에 대한 n-1 디렉토리 구조를 생성해야 합니다. 마운트 경로에는 755 실행 권한이 있어야 합니다.
- 복제 전 또는 복제 후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["FlexClone 볼륨을 부모 볼륨에서 분할합니다."].

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계


1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
대상 복제 인스턴스	<p>기존 백업에서 복제할 대상 Db2 복제 인스턴스 ID를 입력합니다.</p> <p>이는 ANF 스토리지 유형 리소스에만 적용됩니다.</p>
대상 클론 이름	<p>복제본의 이름을 입력하세요.</p> <p>이는 Db2 데이터베이스 리소스에만 적용됩니다.</p>
NFS 내보내기 IP 주소	<p>복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다.</p> <p>이는 NFS 저장 유형 리소스에만 적용됩니다.</p>
용량 풀 최대 처리량(MiB/s)	용량 풀의 최대 처리량을 입력하세요.

7. 스크립트 페이지에서 다음 단계를 수행합니다.



스크립트는 플러그인 호스트에서 실행됩니다.

- a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.
 - 사전 복제 명령: 동일한 이름을 가진 기존 데이터베이스 삭제
 - 복제 후 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

Linux 머신에서 볼륨이나 qtree에 대한 마운트 명령:

NFS의 예: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

자동으로 검색된 Db2 리소스를 복제한 후 복제된 리소스는 수동 리소스로 표시됩니다. 복제된 Db2 리소스를 복구하려면 *리소스 새로 고침*을 클릭하세요. 복제본을 삭제하면 저장소와 호스트도 정리됩니다.

복제 작업 후 리소스를 새로 고치지 않고 복제본을 삭제하려고 하면 스토리지와 호스트가 정리되지 않습니다. fstab에서 항목을 수동으로 삭제해야 합니다.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 복제할 수 있는 백업을 나열합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예제에서는 지정된 리소스 그룹, 해당 리소스 및 관련 정책에 대한 정보를 표시합니다.

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

Description :

CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :

```
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. New-SmClone cmdlet을 사용하여 기존 백업에서 복제 작업을 시작합니다.

이 예제에서는 모든 로그를 포함하는 지정된 백업에서 복제본을 만듭니다.

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

이 예제에서는 지정된 Microsoft SQL Server 인스턴스에 대한 복제본을 만듭니다.

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업의 상태를 확인합니다.

이 예제에서는 지정된 작업 ID에 대한 복제 보고서를 표시합니다.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```







cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

IBM Db2 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.


이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.

2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.


단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 **.

5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.

6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계가 존재하지 않아 실패합니다."

SnapCenter 업그레이드 후 IBM Db2 데이터베이스 복제본 삭제 또는 분할

SnapCenter 4.3으로 업그레이드한 후에는 더 이상 복제본이 표시되지 않습니다. 복제본이 생성된 리소스의 토폴로지 페이지에서 복제본을 삭제하거나 분할할 수 있습니다.



이 작업에 관하여

숨겨진 복제본의 저장 공간을 찾으려면 다음 명령을 실행하세요. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbbackup cmdlet을 사용하여 복제된 리소스의 백업을 삭제합니다.
2. remove-smresourcegroup cmdlet을 사용하여 복제된 리소스의 리소스 그룹을 삭제합니다.
3. remove-smprotectresource cmdlet을 사용하여 복제된 리소스의 보호를 제거합니다.
4. 리소스 페이지에서 상위 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 복제본을 선택합니다.
6. 복제본을 선택한 다음 클릭하세요.  클론을 삭제하거나 클릭하세요.  클론을 분할합니다.
7. *확인*을 클릭합니다.

저작권 정보

Copyright © 2025 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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