

한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

Microsoft Azure

Azure Storage Account – 보존 및 보안

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

저작권에 관련된 법률을 준수하는 것은 고객의 역할이며, 이 문서를 마이크로소프트의 사전 동의 없이 어떤 형태(전자 문서, 물리적인 형태 막론하고) 어떠한 목적으로 재 생산, 저장 및 다시 전달하는 것은 허용되지 않습니다.

마이크로소프트는 이 문서에 들어있는 특허권, 상표, 저작권, 지적 재산권을 가집니다. 문서를 통해 명시적으로 허가된 경우가 아니면, 어떠한 경우에도 특허권, 상표, 저작권 및 지적 재산권은 다른 사용자에게 허여되지 않습니다.

© 2022 Microsoft Corporation All right reserved.

Microsoft®는 미합중국 및 여러 나라에 등록된 상표입니다.

이 문서에 기재된 실제 회사 이름 및 제품 이름은 각 소유자의 상표일 수 있습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2022.03.23	0.5.0	우진환	TASK 01 ~ TASK 03 작성
2022.03.25	1.0.0	우진환	TASK 04 ~ TASK 06 작성

목차

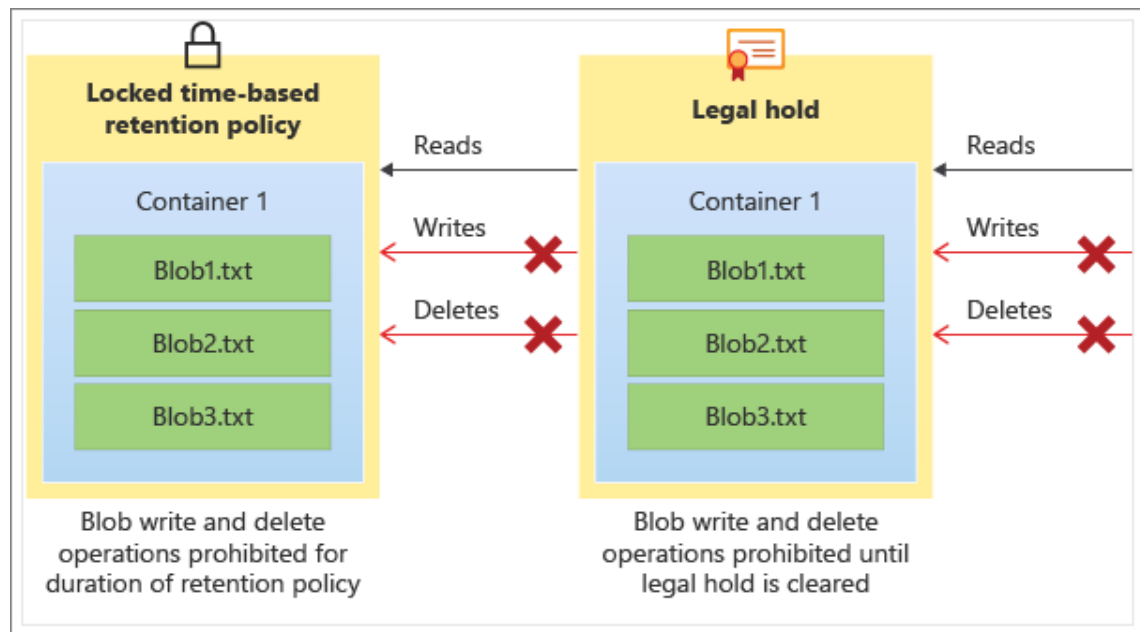
TASK 01. 스토리지 계정 만들기	5
TASK 02. 버전 수준의 불변성.....	10
TASK 03. 시간 기반 보존 정책과 법적 보존	17
TASK 04. PRIVATE ENDPOINT 구성을 위한 가상 머신 준비	23
TASK 05. 스토리지 계정에 대한 PRIVATE ENDPOINT 구성	28
TASK 06. 리소스 정리.....	35

TASK 01. 스토리지 계정 만들기

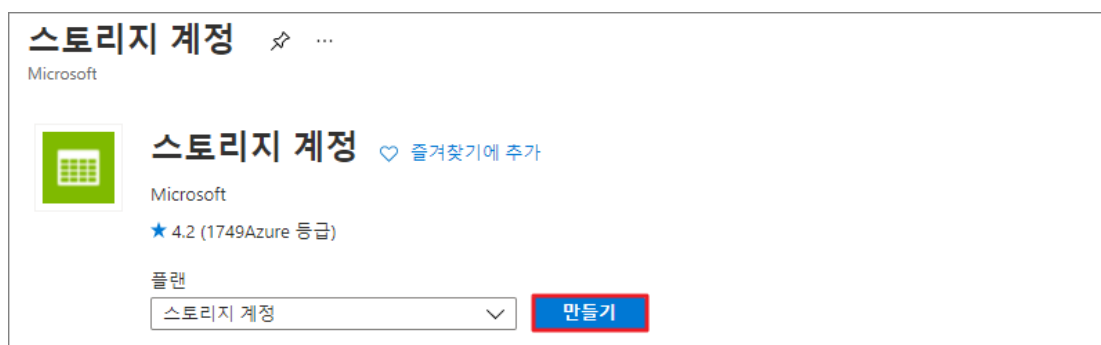
변경이 불가능한 스토리지(immutable storage)는 보존 기간 동안 blob 개체의 업데이트나 삭제를 방지하고 읽기만 가능하도록 하는 기능입니다. immutable storage 정책을 활성화하면 blob 개체의 상태는 WORM (Write Once, Read Many)으로 변경됩니다.

이 기능은 모든 Azure 지역의 일반 목적 V2 (General-purpose V2), 일반 목적 v1, Blob Storage, Block Blob Storage에서 사용할 수 있습니다. immutable storage 기능은 컨테이너 수준에서 사용할 수 있으며 다음과 같은 두 가지 정책을 지원합니다.

- 시간 기반 보존 정책(Time-based retention policy): 이 정책은 보존 기간 동안 blob 개체를 읽고 만들 수 있지만 업데이트와 삭제는 허용되지 않습니다. 보존 기간이 만료되면 blob을 삭제할 수 있지만 덮어쓸 수는 없습니다.
- 법적 보존 정책(Legal hold policy): 이 옵션은 보존 기간을 알 수 없는 경우 사용할 수 있습니다. 법적 보존 정책은 태그 기반 정책이기 때문에 정책을 활성화하려면 하나 이상의 태그를 생성해야 합니다. 이 정책이 활성화되면 blob 개체의 읽기 및 생성은 허용되지만 업데이트와 삭제는 허용되지 않습니다.



1. Azure 포털에서 [리소스 만들기]를 클릭하고 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드에서 [만들기]를 클릭합니다.



2. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.
 - [프로젝트 정보 - 리소스 그룹]: "새로 만들기"를 선택한 후 "03_storageRg"를 입력합니다.
 - [인스턴스 정보 - 스토리지 계정 이름]: 중복되지 않는 고유한 이름을 입력합니다.
 - [인스턴스 정보 - 지역]: (US) East US
 - [인스턴스 정보 - 성능]: 표준
 - [인스턴스 정보 - 중복]: LRS(로컬 중복 스토리지)

저장소 계정 만들기 ...

기본 고급 네트워킹 데이터 보호 암호화 태그 검토 + 만들기

Azure Storage는 가용성, 보안, 내구성, 확장성 및 중복성이 뛰어난 클라우드 스토리지를 제공하는 Microsoft 관리 서비스입니다. Azure Storage는 Azure Blob(개체), Azure Data Lake Storage Gen2, Azure Files, Azure 큐 및 Azure 테이블을 포함합니다. 스토리지 계정의 비용은 사용량 및 아래에서 선택한 옵션에 따라 다릅니다. [Azure Storage 계정에 대한 자세한 정보](#)

프로젝트 정보
새 스토리지 계정을 만들 구독을 선택합니다. 다른 리소스와 함께 스토리지 계정을 구성하고 관리할 새 리소스 그룹 또는 기존 리소스 그룹을 선택합니다.

구독 * Azure Pass - 스폰서십

리소스 그룹 * (신규) 03_storageRg
[새로 만들기](#)

인스턴스 정보
레거시 스토리지 계정 유형을 만들어야 하는 경우 다음을 클릭하세요. [여기](#).

스토리지 계정 이름 ① * kormtt0314stor

지역 ① * (US) East US

성능 ① * ☒ 표준: 대부분 시나리오에 권장됨(범용 v2 계정)
☐ 프리미엄: 짧은 대기 시간이 필요한 경우에 권장됩니다.

중복 ① * LRS(로컬 중복 스토리지)

3. [고급] 탭에서 기본 설정을 유지하고 [다음]을 클릭합니다.
4. [네트워킹] 탭에서 "공용 엔드포인트(모든 네트워크)"를 선택하고 [다음]을 클릭합니다.

저장소 계정 만들기 ...

기본 고급 네트워킹 데이터 보호 암호화 태그 검토 + 만들기

네트워크 연결

공용 IP 주소 또는 서비스 엔드포인트를 통해 공개적으로 또는 프라이빗 엔드포인트를 사용하여 비공개로 스토리지 계정에 연결할 수 있습니다.

연결 방법 *

☒ 공용 엔드포인트(모든 네트워크)
☐ 공용 엔드포인트(선택한 네트워크)
☐ 프라이빗 엔드포인트

i 모든 네트워크에서 이 스토리지 계정에 액세스할 수 있게 됩니다. 네트워크에서 이 리소스에 비공개로 액세스하려면 프라이빗 엔드포인트를 사용하는 것이 좋습니다.
[자세한 정보](#)

네트워크 라우팅

트래픽이 원본에서 Azure 엔드포인트로 이동하는 과정에서 트래픽을 라우팅할 방법을 결정하세요. 대부분의 고객의 경우 Microsoft 네트워크 라우팅이 권장됩니다.

라우팅 기본 설정 ⓘ *

☒ Microsoft 네트워크 라우팅
☐ 인터넷 라우팅

5. [데이터 보호] 탭의 페이지에서 "추적 - Blob에 버전 관리 사용" 옵션을 체크하고 [검토 + 만들기]를 클릭합니다. 이 옵션을 스토리지 계정 생성 후에도 설정할 수 있습니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

저장소 계정 만들기 ...

기본 고급 네트워킹 **데이터 보호** 암호화 태그 검토 + 만들기

복구

실수로 인한 또는 잘못된 삭제나 수정으로부터 데이터를 보호합니다.

☐ 컨테이너에 특정 시점 복원 사용
특정 시점 복원을 사용하여 하나 이상의 컨테이너를 이전 상태로 복원합니다. 특정 시점 복원을 사용하도록 설정한 경우 버전 관리, 변경 피드 및 Blob 일시 삭제도 사용하도록 설정됩니다. [자세한 정보](#)

☒ Blob에 일시 삭제 사용
일시 삭제를 사용하면 덮어쓴 Blob을 포함하여 이전에 삭제로 표시되었던 Blob을 복구할 수 있습니다. [자세한 정보](#)

삭제된 Blob 보존 기간(일) ①

☒ 컨테이너에 일시 삭제 사용
일시 삭제를 사용하면 이전에 삭제로 표시된 컨테이너를 복구할 수 있습니다. [자세한 정보](#)

삭제된 컨테이너 보존 기간(일) ①

☒ 파일 공유에 일시 삭제 사용
일시 삭제를 사용하면 이전에 삭제로 표시된 파일 공유를 복구할 수 있습니다. [자세한 정보](#)

삭제된 파일 공유 보존 기간(일) ①

추적

버전을 관리하고 Blob 데이터에 대해 수행된 변경 내용을 추적합니다.

☒ Blob에 버전 관리 사용
버전 관리를 사용하여 복구 및 복원에 대해 Blob의 이전 버전을 자동으로 유지합니다. [자세한 정보](#)

☐ Blob 변경 피드 사용
계정의 Blob에 대한 만들기, 수정 및 삭제 변경 내용을 추적합니다. [자세한 정보](#)

액세스 제어

☐ 버전 수준 불변성 지원 사용
모든 Blob 버전에 적용할 계정 수준에서 시간 기반 보존 정책을 설정할 수 있습니다. 계정 수준에서 기본 정책을 설정하려면 이 기능을 사용하도록 설정합니다. 이 기능을 사용하지 않고도 컨테이너 수준에서 기본 정책을 설정하거나 특정 Blob 버전에 대한 정책을 설정할 수 있습니다. 이 속성을 사용하려면 버전 관리가 필요합니다. [자세한 정보](#)

6. 동일한 방법으로 스토리지 계정을 하나 더 생성합니다. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 스토리지 계정 이름 접미사에 "version"을 추가합니다.

저장소 계정 만들기 ...

기본 고급 네트워킹 데이터 보호 암호화 태그 검토 + 만들기

Azure Storage는 가용성, 보안, 내구성, 확장성 및 중복성이 뛰어난 클라우드 스토리지를 제공하는 Microsoft 관리 서비스입니다. Azure Storage는 Azure Blob(개체), Azure Data Lake Storage Gen2, Azure Files, Azure 큐 및 Azure 테이블을 포함합니다. 스토리지 계정의 비용은 사용량 및 아래에서 선택한 옵션에 따라 다릅니다. [Azure Storage 계정에 대한 자세한 정보](#)

프로젝트 정보

새 스토리지 계정을 만들 구독을 선택합니다. 다른 리소스와 함께 스토리지 계정을 구성하고 관리할 새 리소스 그룹 또는 기존 리소스 그룹을 선택합니다.

구독 * Azure Pass - 스폰서쉽

리소스 그룹 * 03_storageRg

[새로 만들기](#)

인스턴스 정보

레거시 스토리지 계정 유형을 만들어야 하는 경우 다음을 클릭하세요. [여기](#).

스토리지 계정 이름 ① * kormtt0314version

지역 ① * (US) East US

성능 ① * ☒ 표준: 대부분 시나리오에 권장됨(범용 v2 계정)

☐ 프리미엄: 짧은 대기 시간이 필요한 경우에 권장됩니다.

중복 ① * LRS(로컬 중복 스토리지)

7. [고급] 탭과 [네트워킹] 탭을 기본 옵션을 선택하고 [데이터 보호] 탭에서 "액세스 제어 - 버전 수준 불변성 지원 사용" 옵션을 체크합니다. 이 옵션을 선택하면 "Blob에 버전 관리 사용" 옵션이 자동으로 선택됩니다. 스토리지 계정에서 버전 수준 불변성을 사용하려면 스토리지 계정을 생성할 때 이 옵션을 설정해야 합니다. [검토 + 만들기]를 클릭한 후 [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

저장소 계정 만들기 ...

기본 고급 네트워크 데이터 보호 암호화 태그 검토 + 만들기

복구

실수로 인한 또는 잘못된 삭제나 수정으로부터 데이터를 보호합니다.

☐ 컨테이너에 특정 시점 복원 사용
특정 시점 복원을 사용하여 하나 이상의 컨테이너를 이전 상태로 복원합니다. 특정 시점 복원을 사용하도록 설정한 경우 버전 관리, 변경 피드 및 Blob 일시 삭제도 사용하도록 설정됩니다. [자세한 정보](#)

☒ Blob에 일시 삭제 사용
일시 삭제를 사용하면 덮어쓰 Blob을 포함하여 이전에 삭제로 표시되었던 Blob을 복구할 수 있습니다. [자세한 정보](#)

삭제된 Blob 보존 기간(일) ①

☒ 컨테이너에 일시 삭제 사용
일시 삭제를 사용하면 이전에 삭제로 표시된 컨테이너를 복구할 수 있습니다. [자세한 정보](#)

삭제된 컨테이너 보존 기간(일) ①

☒ 파일 공유에 일시 삭제 사용
일시 삭제를 사용하면 이전에 삭제로 표시된 파일 공유를 복구할 수 있습니다. [자세한 정보](#)

삭제된 파일 공유 보존 기간(일) ①

추적

버전을 관리하고 Blob 데이터에 대해 수행된 변경 내용을 추적합니다.

☒ Blob에 버전 관리 사용
버전 관리를 사용하여 복구 및 복원에 대해 Blob의 이전 버전을 자동으로 유지합니다. [자세한 정보](#)

☐ Blob 변경 피드 사용
계정의 Blob에 대한 만들기, 수정 및 삭제 변경 내용을 추적합니다. [자세한 정보](#)

액세스 제어

☒ 버전 수준 불변성 지원 사용
모든 Blob 버전에 적용할 계정 수준에서 시간 기반 보존 정책을 설정할 수 있습니다. 계정 수준에서 기본 정책을 설정하려면 이 기능을 사용하도록 설정합니다. 이 기능을 사용하지 않고도 컨테이너 수준에서 기본 정책을 설정하거나 특정 Blob 버전에 대한 정책을 설정할 수 있습니다. 이 속성을 사용하려면 버전 관리가 필요합니다. [자세한 정보](#)

TASK 02. 버전 수준의 불변성

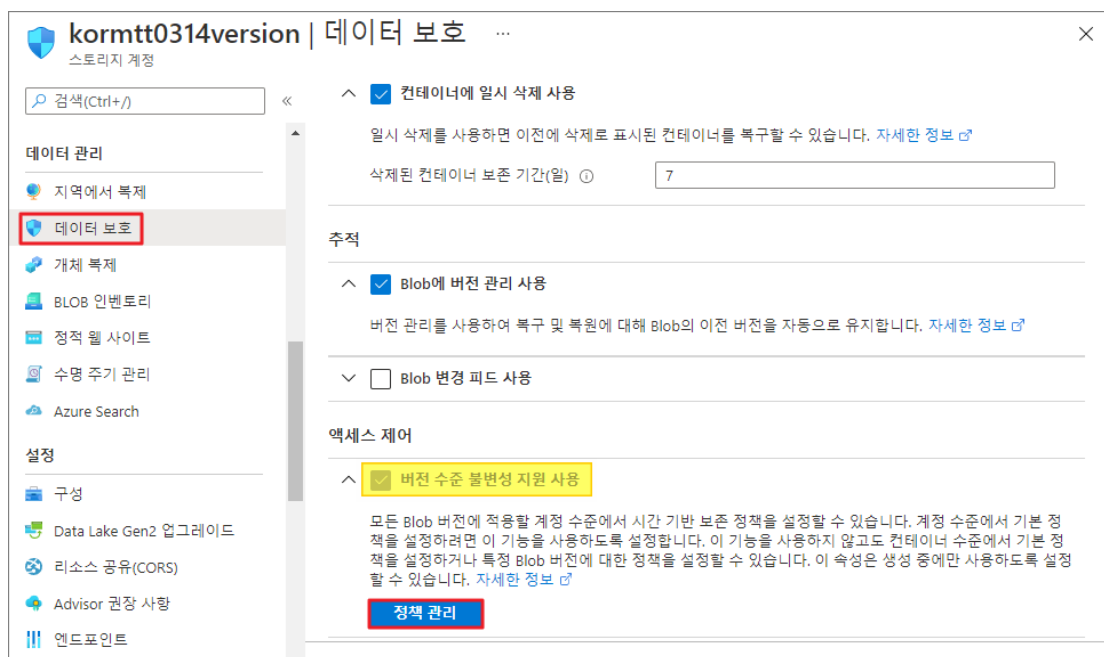
Blob 버전으로 범위가 지정된 불변성 정책을 구성하려면 스토리지 계정 또는 컨테이너에서 버전 수준 불변성에 대한 지원을 사용하도록 설정해야 합니다. 스토리지 계정에서 버전 수준 불변성에 대한 지원을 사용하도록 설정한 후 스토리지 계정에서 이후에 만들어지는 모든 개체에 적용되는 기본 정책을 계정 수준에서 구성할 수 있습니다. 개별 컨테이너에서 버전 수준 불변성에 대한 지원을 사용하도록 설정하면 이후에 컨테이너에서 만들어지는 모든 개체에 적용되는 해당 컨테이너에 대한 기본 정책을 구성할 수 있습니다. 다음 표에는 각 리소스 범위에 대해 지원되는 불변성 정책이 요약되어 있습니다.

리소스	버전 수준 불변성 정책 사용	정책 지원
계정	예, 계정을 만들 때만 가능합니다.	하나의 기본 버전 수준 불변성 정책을 지원합니다. 기본 정책은 정책이 구성된 후 계정에서 만든 모든 새 Blob 버전에 적용됩니다. 법적 보존을 지원하지 않습니다.
컨테이너	예, 컨테이너를 만들 때 가능합니다. 버전 수준의 불변성 정책을 지원하려면 기존 컨테이너를 마이그레이션해야 합니다.	하나의 기본 버전 수준 불변성 정책을 지원합니다. 기본 정책은 정책이 구성된 후 컨테이너에 만들어진 모든 새 Blob 버전에 적용됩니다.

		법적 보존을 지원하지 않습니다.
Blob 버전	해당 없음	하나의 버전 수준 불변성 정책과 하나의 법적 보존을 지원합니다. Blob 버전에 대한 정책은 계정 또는 컨테이너에 지정된 기본 정책을 재정의할 수 있습니다.

즉 버전 수준의 불변성 옵션을 사용하면 컨테이너 수준뿐 아니라 blob 개체와 버전 수준에서도 액세스 정책을 구성할 수 있습니다.

1. 앞서 만들었던 **version** 접미사가 추가된 [스토리지 계정] 블레이드로 이동합니다.
2. [스토리지 계정] 블레이드의 [데이터 관리 - 데이터 보호]로 이동한 후 "액세스 제어" 영역에 "버전 수준의 불변성 지원 사용" 옵션이 이미 선택되어 있고 설정을 변경할 수 없게 표시되어 있는 것을 확인한 후 [정책 관리]를 클릭합니다.



3. [버전 수준 불변성 정책 관리]에서 [정책 추가]를 클릭합니다. [불변성 정책 추가]에서 보존 기간을 10일로 설정하고 [확인]을 클릭합니다. "보호된 쓰기를 허용하여 BLOB 추가" 옵션은 Append blob에 적용할 수 있는 옵션입니다.

버전 수준 불변성 정책 관리

여기에서 만든 정책은 컨테이너 또는 Blob 버전 수준에서 정책으로 덮어쓰지 않는 한 모든 새 Blob 버전에 적용됩니다. [자세한 정보](#)

식별자	보존 간격	상태
불변성 정책 없음		
<div>+ 정책 추가</div>		

불변성 정책 추가

보존 기간(일) *

10

☐ 보호된 쓰기를 허용하여 BLOB 추가

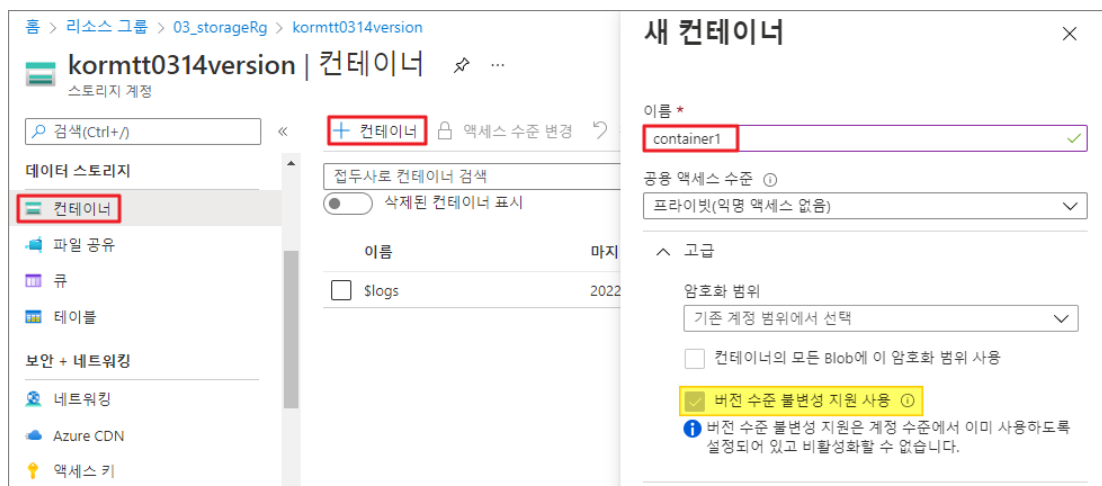
확인

취소

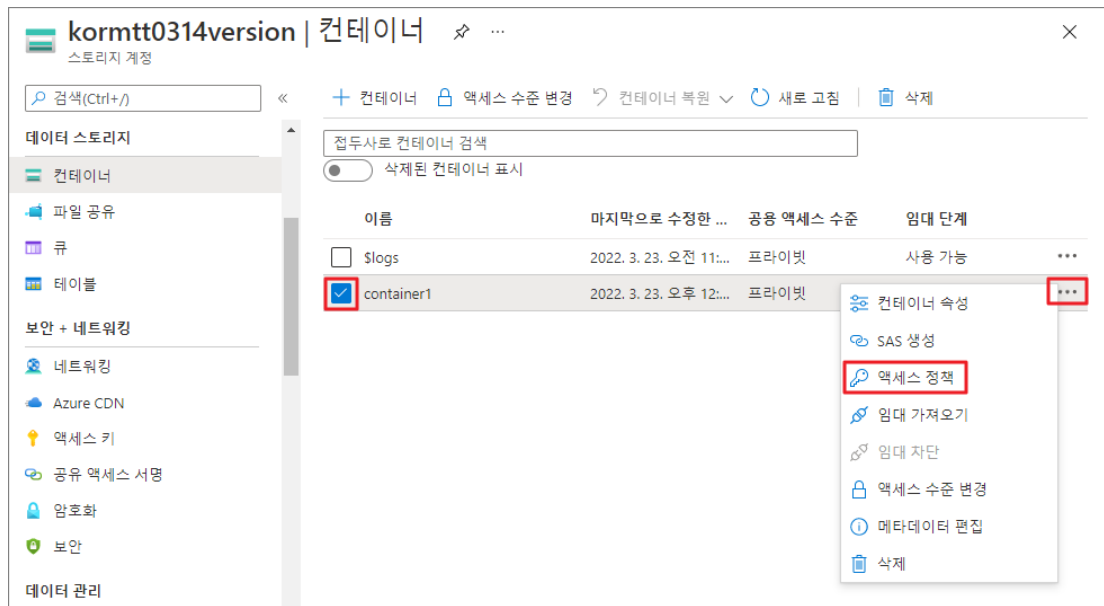
- 정책을 생성한 후 다시 [정책 관리]를 클릭합니다. 추가한 정책이 표시되고 [...]을 클릭하면 다음과 같은 메뉴가 표시되는 것을 확인할 수 있습니다. [...] - 잠금]을 클릭하면 이 정책이 되돌릴 수 없는 상태로 적용됩니다. 즉 정책을 잠그면 지정한 보존 기간이 끝날 때까지 스토리지 계정을 삭제할 수 없습니다. 또한 변경 사항이 적용될 때까지 시간이 걸릴 수 있습니다. 이 실습에서는 테스트를 위해 정책을 잠그지 않습니다.



5. [스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 메뉴에서 [컨테이너]를 클릭합니다. [새 컨테이너] 창의 이름에 "container1"을 입력하고 [고급] 메뉴를 확장합니다. 아래와 같이 "버전 수준 불변성 지원 사용" 옵션이 체크되어 있는 것을 확인할 수 있습니다. [만들기]를 클릭합니다.



6. 새로 만든 컨테이너의 [... - 액세스 정책]을 클릭합니다.



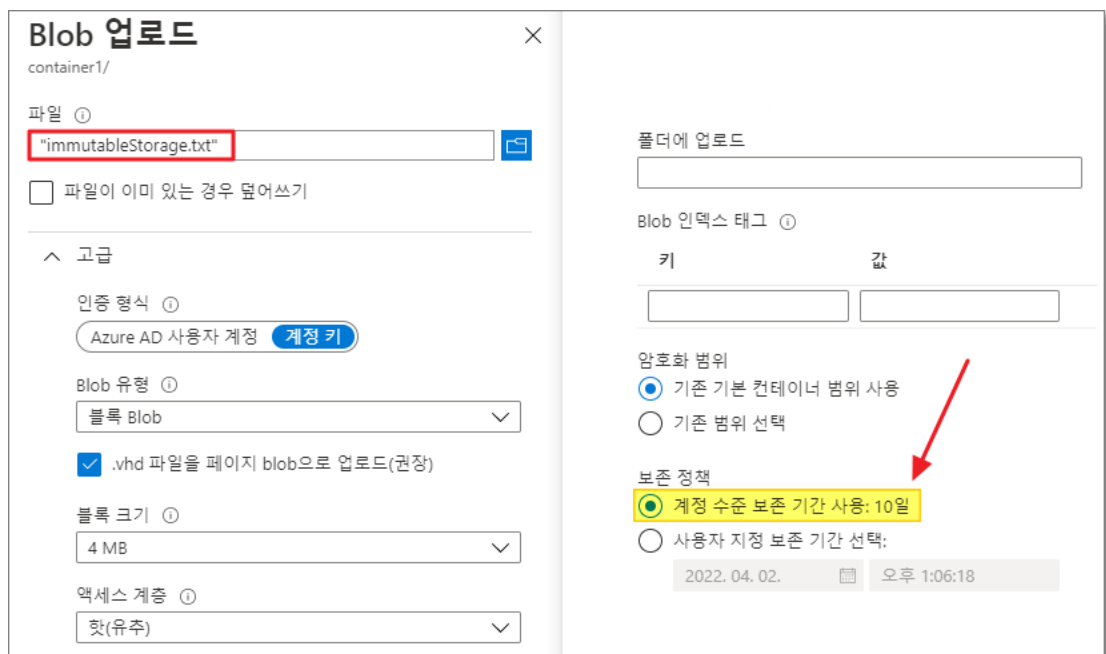
7. [액세스 정책]에서 액세스 정책과 변경이 불가능한 Blob 스토리지 정책이 아무것도 없는 것을 확인하고 창을 닫습니다. 컨테이너에 특별한 보존 정책이 설정되어 있지 않지만 스토리지 계정 수준에서 버전 수준 불변성 지원이 사용되고 있기 때문에 컨테이너는 삭제할 수 없습니다.



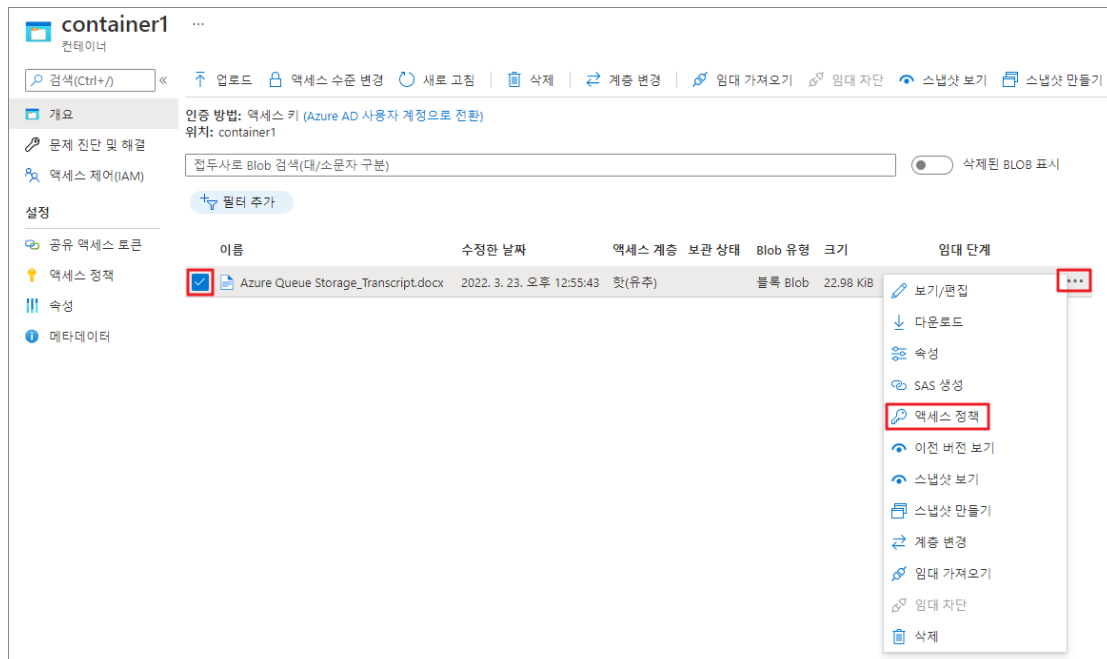
8. `container1` 컨테이너로 이동합니다. [`container1` 컨테이너] 블레이드의 메뉴에서 [업로드]를 클릭합니다.



9. [Blob 업로드]에서 임의의 TXT 파일을 선택하고 [고급]을 확장합니다. 아래와 같이 "보존 정책"에 버전 수준 불변성 지원에서 설정한 스토리지 계정 수준의 정책이 기본적으로 선택되어 있는 것을 확인할 수 있습니다. 필요한 경우 별도의 보존 기간을 설정할 수도 있습니다. [업로드]를 클릭합니다.



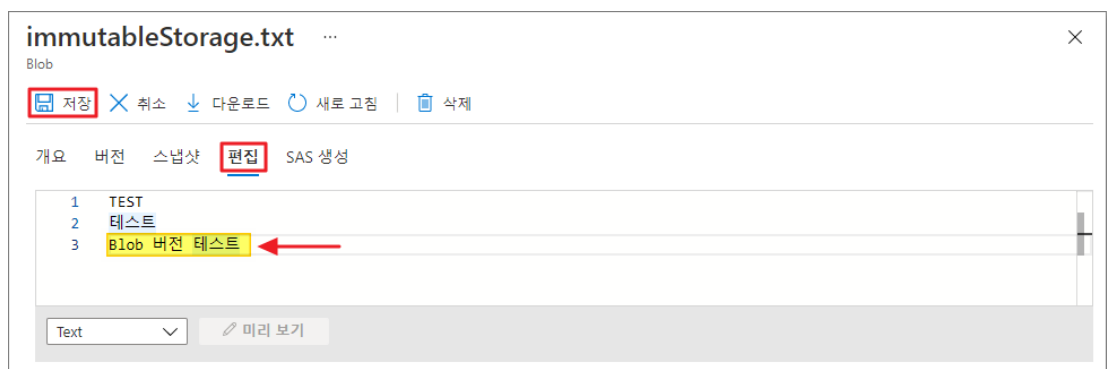
10. 업로드한 파일을 선택하고 [⋯ - 액세스 정책]을 클릭합니다. "버전 수준의 불변성 지원 사용"을 활성화했기 때문에 컨테이너 수준뿐 아니라 Blob 수준에서도 정책을 설정할 수 있습니다.



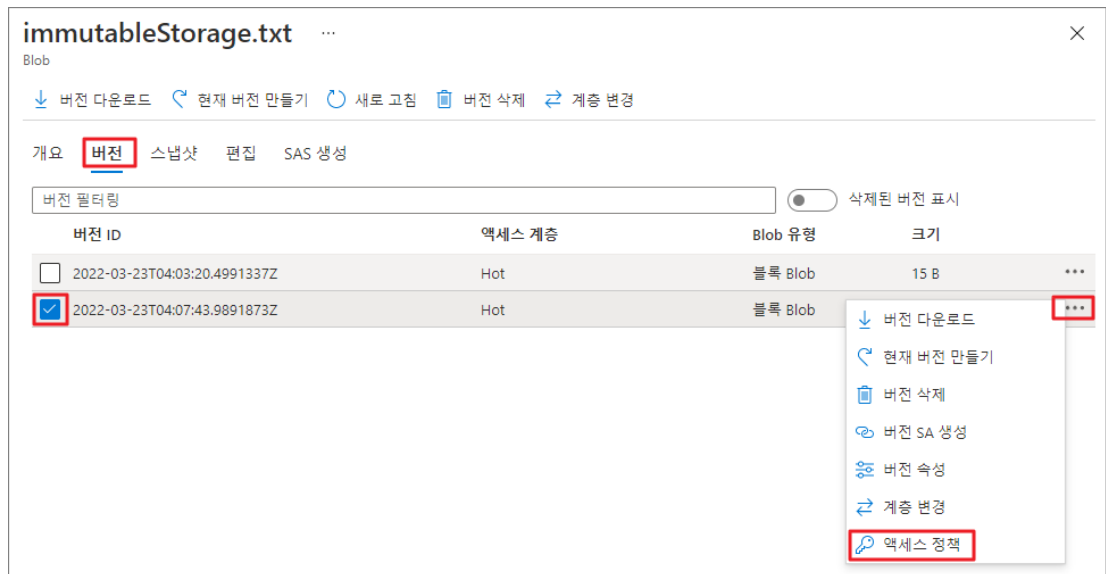
11. [액세스 정책]에서 스토리지 계정 수준에서 설정한 버전 수준 불변성 정책이 자동으로 적용되어 있는 것을 확인할 수 있습니다.



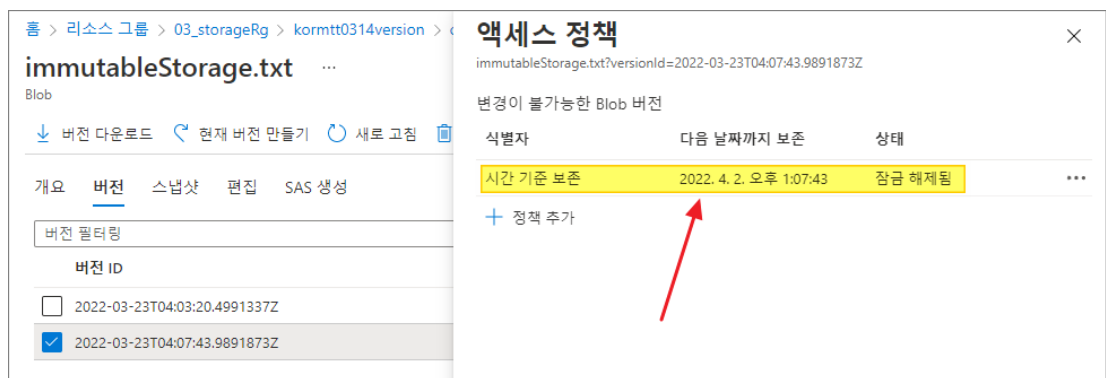
12. 업로드한 파일을 클릭합니다. [편집] 탭으로 이동한 후 파일 내용을 변경하고 [저장]을 클릭합니다.



13. [Blob] 블레이드의 [버전] 탭으로 이동한 후 새로 생성된 Blob 버전을 선택하고 [액세스 정책]을 클릭합니다.



14. [액세스 정책]에서 버전 수준 불변성 지원에서 설정한 정책이 Blob 버전에도 동일하게 설정되어 있는 것을 확인할 수 있습니다.



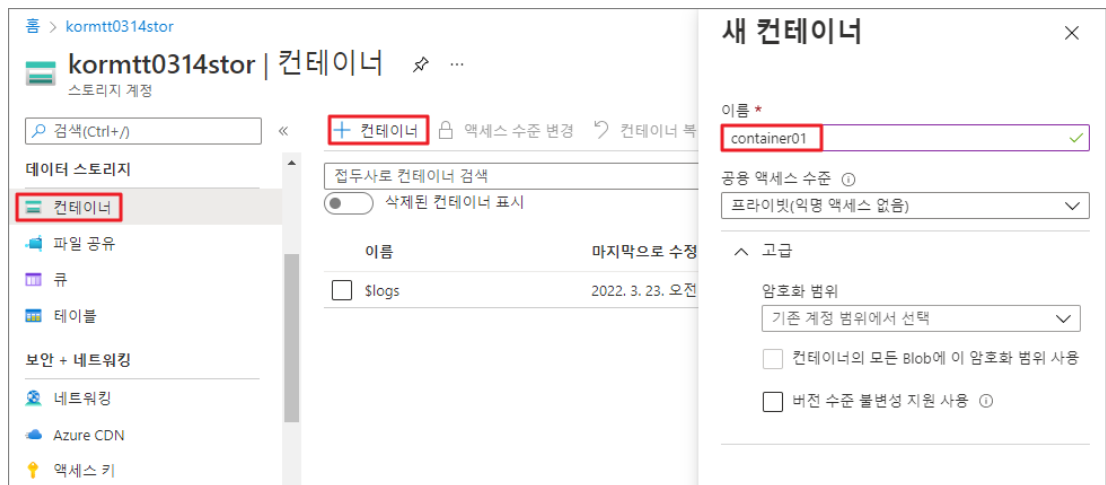
15. 다음 작업을 진행하여 스토리지 계정을 삭제합니다.

- 업로드한 Blob 파일의 [액세스 정책]을 열고 추가되어 있는 보존 정책을 삭제합니다.
- 업로드한 Blob 파일을 삭제합니다.
- version** 접두사가 추가되어 있는 스토리지 계정을 삭제합니다.

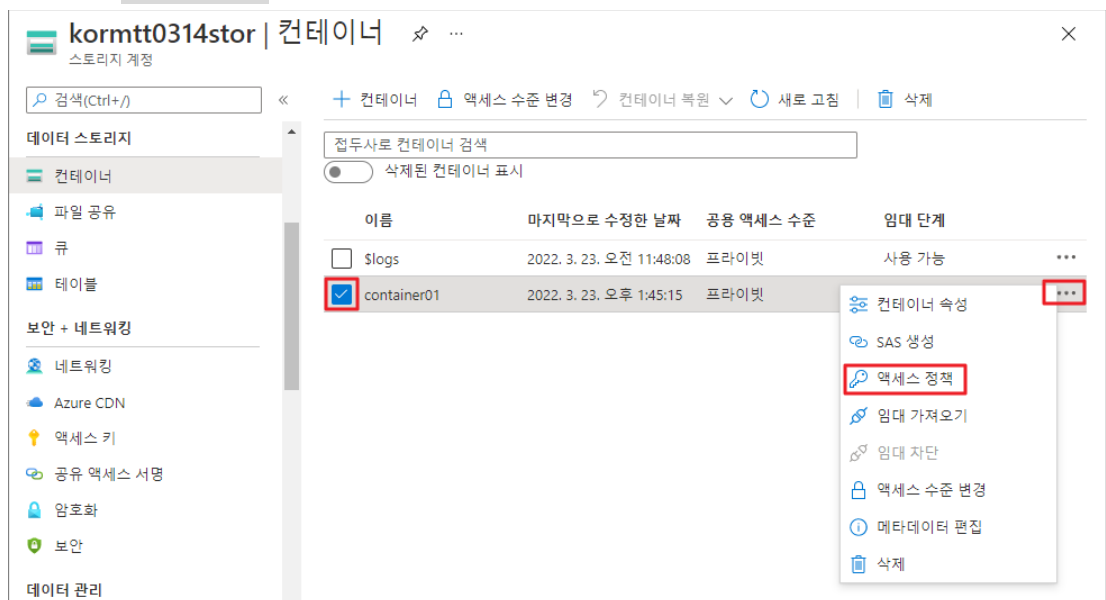
TASK 03. 시간 기반 보존 정책과 법적 보존

- [03_storageRg 리소스 그룹]으로 이동한 후 stor 접미사를 가진 스토리지 계정을 클릭합니다. [스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 메뉴에서 [컨테이너]를 클릭합니다. [새 컨테이너]에서 컨테이너 이름에 "container01"을 입력하고 [만들기]를 클릭합니다.
 - [고급]을 확장하면 앞서 확인했던 버전 수준 불변성과 마찬가지로 컨테이너 수준에서 버전 수준 불변성을 설정할 수 있는 것을 확인할 수 있습니다.
 - [고급]에서 "버전 수준 불변성 지원 사용" 옵션을 선택하지 않는 경우 보존 정책은 컨테이너 수준에서 적용되며 Blob이나 버전 수준에서 설정할 수 없습니다.
 - 버전 수준 불변성을 사용할 계획이라면 컨테이너를 생성할 때 이 옵션을 선택하는 것이 좋습니다. 추후

컨테이너가 버전 수준 불변성을 지원하도록 설정하면 마이그레이션 시간이 필요합니다.



2. 새로 만든 **container01** 컨테이너를 선택하고 [... - 액세스 정책]을 클릭합니다.



3. [액세스 정책]의 "변경이 불가능한 Blob 스토리지" 영역의 [정책 추가]를 클릭합니다.

4. [불변 저장소 정책]에서 다음과 같이 구성하고 [저장]을 클릭합니다.

- 정책 유형: 시간 기준 보존
- 다음에 대한 보존 기간 설정: 1일

5. [액세스 정책]에서 시간 기준 보존이 설정되어 있고 범위가 "컨테이너"로 설정되어 있는 것을 확인합니다.

버전 수준 불변성을 사용하면 적용 범위가 "버전"으로 표시됩니다.

- 시간 기반 보존 정책이 설정되면 상태가 "잠금 해제됨"으로 표시됩니다. 이 상태에서는 해당 정책을

삭제할 수 있기 때문에 개발 및 테스트 단계에서 유용하게 사용할 수 있습니다.

- [...] - 잠금 정책]을 선택하면 정책을 더 이상 삭제할 수 없으며 보존 기간 연장만 허용되며 Blob 업데이트 및 삭제를 수행할 수 없습니다.

액세스 정책 container01

저장

액세스 정책을 저장했습니다.

+ 정책 추가

식별자	시작 시간	만료 시간	권한
결과 없음			

변경이 불가능한 Blob 스토리지 ⓘ

+ 정책 추가

식별자	범위	보존 간격	상태
시간 기준 보존	컨테이너	1일	잠금 해제됨

편집
정책 감사
잠금 정책
삭제

6. [액세스 정책]에서 변경이 불가능한 Blob 스토리지의 [정책 추가]를 다시 클릭합니다.

액세스 정책

container01

저장

액세스 정책을 저장했습니다.

+

 정책 추가

식별자	시작 시간	만료 시간	권한
결과 없음			

변경이 불가능한 Blob 스토리지

+

 정책 추가

식별자	범위	보존 간격	상태
시간 기준 보존	컨테이너	1일	잠금 해제됨

7. [불변 저장소 정책]에서 아래와 같이 구성하고 [저장]을 클릭합니다.

- 정책 유형: 법적 보존
- 태그: NoDelete

불변 저장소 정책

정책 유형

법적 보존

각 법적 보존 정책은 하나 이상의 태그와 연결되어야 합니다. 태그는 레코드를 분류하고 보기 위해 사례 ID 같은 이를 식별자로 사용됩니다. 보존 정책 변경 내용이 적용되는 데 시간이 걸릴 수 있습니다. [변경이 불가능한 Blob Storage에 대한 자세한 정보](#)


태그

NoDelete

태그 추가

8. 다음과 같이 시간 기준 보존과 함께 법적 보존이 함께 설정되어 있는 것을 확인합니다.

21 / 37

 Microsoft



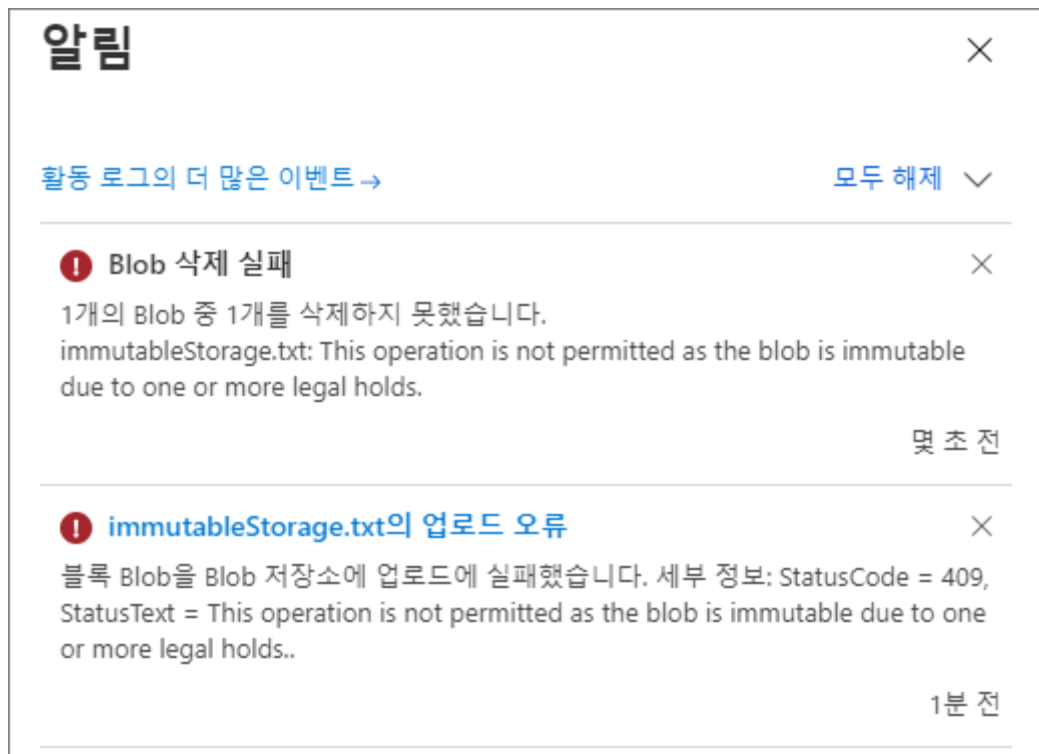
9. [container01 컨테이너] 블레이드로 이동한 후 [업로드]를 클릭합니다. [Blob 업로드]에서 임의의 파일을 선택하고 [업로드]를 클릭합니다.



10. 다음과 같은 테스트를 진행합니다.

- 동일한 이름의 Blob 파일을 업로드합니다. "파일이 이미 있는 경우 덮어쓰기" 옵션을 선택하고 파일을 업로드하면 보존 정책으로 인해 파일 업로드를 할 수 없다는 메시지가 표시됩니다.
- 업로드한 파일을 삭제하면 마찬가지로 보존 정책으로 인해 파일을 삭제할 수 없다는 메시지가 표시됩니다.
- 버전 수준 불변성 지원을 사용하도록 컨테이너를 만든 경우 법적 보존 정책을 설정할 수 없습니다. 버전 수준의 불변성을 설정하기 때문에 동일한 파일을 업로드할 수 있으며 동일한 파일이 덮어쓰기 될

때마다 새로운 버전을 생성하게 됩니다.



TASK 04. Private Endpoint 구성을 위한 가상 머신 준비

Private Link를 사용하면 가상 네트워크의 Private Endpoint를 통해 Azure PaaS 서비스(예, 스토리지 및 SQL Database) 및 Azure 호스팅 고객/파트너 서비스에 액세스할 수 있습니다. 가상 네트워크와 서비스 간의 트래픽은 Microsoft 백본 네트워크를 통하게 되며 공용 인터넷 상에 노출되지 않습니다. 또한 가상 네트워크 내에 자체 Private Link를 만들어 고객에게 프라이빗하게 제공할 수도 있습니다. Azure Private Link는 다음과 같은 장점을 제공합니다.

- Azure 플랫폼의 서비스에 프라이빗 액세스: 원본 및 대상에서 공용 IP 주소 없이 프라이빗으로 Azure에서 실행되는 서비스에 가상 네트워크를 연결할 수 있습니다. 서비스 공급자는 자체 가상 네트워크에서 프라이빗으로 서비스를 제공할 수 있고 소비자는 로컬 가상 네트워크에서 프라이빗하게 해당 서비스에 액세스할 수 있습니다. Private Link 플랫폼은 Azure 백본 네트워크를 통해 소비자 및 서비스 간의 연결을 처리합니다.
- 온-프레미스 및 피어링된 네트워크: 온-프레미스에서는 ExpressRoute의 private peering, VPN 터널을 통해 Azure에서 실행 중인 서비스에 액세스할 수 있고 피어링된 가상 네트워크에서는 Private Endpoint를 사용하여 Azure에서 실행 중인 서비스에 액세스할 수 있습니다. 서비스에 연결하기 위해 public peering을 설정하거나 인터넷을 통과할 필요가 없습니다. 이 기능을 통해 워크로드를 Azure로 안전하게 마이그레이션할 수 있습니다.
- 데이터 유출 방지: Private Link를 사용하면 가상 네트워크의 Private Endpoint가 전체 서비스가 아니라 고객 PaaS 리소스의 특정 인스턴스에 매핑됩니다. Private Endpoint를 사용하는 소비자는 특정 리소스에만

연결할 수 있고 서비스의 다른 리소스에는 연결할 수 없습니다. 이를 통해 데이터 유출 위험으로 부터 리소스를 보호할 수 있습니다.

- 글로벌 도달(Global reach): 다른 지역에서 실행 중인 서비스에 프라이빗하게 연결할 수 있습니다. 예를 들어 Azure 지역 A에 있는 가상 네트워크가 지역 B의 Private Link 뒤에 있는 서비스에 연결할 수 있습니다.
- 자체 서비스의 확장: 서비스를 표준 부하 분산 장치 뒤에 배치하고 Private Link를 활성화할 수 있습니다. 그런 다음 소비자는 자체 가상 네트워크의 Private Endpoint를 사용하여 서비스에 직접 연결할 수 있습니다. 이러한 연결은 간단한 승인 요청 흐름을 사용하여 관리할 수 있습니다.

1. Azure 포털에서 [리소스 만들기]를 클릭한 후 "Windows Server"를 검색하고 클릭합니다. [Windows Server] 블레이드에서 "[smalldisk] Windows Server 2022 Datacenter: Azure Edition"을 선택하고 [만들기]를 클릭합니다.



2. [가상 머신 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성하고 [다음]을 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: 03_storageRg
- [인스턴스 정보 - 가상 머신 이름]: storageVM
- [인스턴스 정보 - 지역]: (US) East US
- [인스턴스 정보 - 가용성 옵션]: 인프라 중복이 필요하지 않습니다.
- [인스턴스 정보 - 보안 유형]: 표준
- [인스턴스 정보 - 크기]: Standard_D2s_v3
- [관리자 계정 - 사용자 이름]: labAdmin
- [관리자 계정 - 암호]: 복잡성을 만족하는 암호 입력
- [인바운드 포트 규칙 - 공용 인바운드 포트]: 선택한 포트 허용
- [인바운드 포트 규칙 - 인바운드 포트 선택]: RDP (3389)

가상 머신 만들기 ...

기본 사항 디스크 네트워킹 관리 고급 태그 검토 + 만들기

Linux 또는 Windows를 실행하는 가상 머신을 만듭니다. Azure Marketplace에서 이미지를 선택하거나 고유한 사용자 지정 이미지를 사용합니다. [기본] 탭을 완료하고 [검토 + 만들기]하여 기본 매개 변수로 가상 머신을 프로비전하거나, 전체 사용자 지정에 대해 각 탭을 검토합니다. [자세한 정보](#)

프로젝트 정보
배포된 리소스와 비용을 관리할 구독을 선택합니다. 풀더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 * ① Azure Pass - 스폰서십

리소스 그룹 * ① 03_storageRg
[새로 만들기](#)

인스턴스 정보

가상 머신 이름 * ① storageVM ✓

지역 * ① (US) East US

가용성 옵션 ① 인프라 중복이 필요하지 않습니다.

보안 유형 ① 표준

이미지 * ① [smalldisk] Windows Server 2022 Datacenter: Azure Edition - Gen2
[모든 이미지 보기](#) | VM 생성 구성

Azure 스폷 인스턴스 ① ☐

크기 * ① Standard_D2s_v3 - 2 vcpu, 8 GiB 메모리 (₩154,347/월)
[모든 크기 보기](#)

관리자 계정

사용자 이름 * ① labAdmin ✓

암호 * ① ✓

암호 확인 * ① ✓

인바운드 포트 규칙
공용 인터넷에서 액세스할 수 있는 가상 머신 네트워크 포트를 선택하세요. [네트워킹] 탭에서 더 제한되거나 세분화된 네트워크 액세스를 지정할 수 있습니다.

공용 인바운드 포트 * ① ☐ 없음 ☒ 선택한 포트 허용

인바운드 포트 선택 * RDP (3389)

3. [디스크] 탭에서 [다음]을 클릭합니다. [네트워킹] 탭에서 "가상 네트워크" 영역의 "새로 만들기"를 클릭합니다.

가상 머신 만들기 ...

기본 사항 디스크 **네트워킹** 관리 고급 태그 검토 + 만들기

NIC(네트워크 인터페이스 카드) 설정을 구성하여 가상 머신에 대한 네트워크 연결을 정의합니다. 보안 그룹 규칙을 사용하여 포트, 인바운드 및 아웃바운드 연결을 제어하거나 기존 부하 분산 솔루션 뒤에 배치할 수 있습니다. [자세한 정보](#)

네트워크 인터페이스
가상 머신을 만들면 네트워크 인터페이스가 만들어집니다.

가상 네트워크 * ① (새로 만드는 중) 03_storageRg-vnet
[새로 만들기](#)

서브넷 * ① (새로 만드는 중) default(10.1.0.0/24)

공용 IP ① (새로 만드는 중) storageVM-ip
[새로 만들기](#)

4. [가상 네트워크 만들기]에서 다음과 같이 구성하고 [확인]을 클릭합니다.
- 주소 범위: 10.30.0.0/16
 - 서브넷: vmSubnet (10.30.0.0/24), endpointSubnet (10.30.1.0/24)

가상 네트워크 만들기

Microsoft Azure Virtual Network 서비스를 통해 Azure 리소스는 구독 전용인 Azure 클라우드의 논리적 격리인 가상 네트워크에서 서로 안전하게 통신할 수 있습니다. 가상 네트워크를 다른 가상 네트워크나 온-프레미스 네트워크에 연결할 수 있습니다. [자세한 정보](#)

이름 * 03_storageRg-vnet

주소 공간

CIDR 표기법으로 된 하나 이상의 주소 접두사로 지정된 가상 네트워크의 주소 공간입니다(예: 192.168.1.0/24).

<input type="checkbox"/> 주소 범위	주소	검침
<input checked="" type="checkbox"/> 10.30.0.0/16 ✓	10.30.0.0 - 10.30.255.255(65536개 주소)	없음
<input type="checkbox"/>	(0개 주소)	없음

서브넷

서브넷의 주소 범위가 CIDR 표기법으로 되어 있습니다. 이 주소 범위는 가상 네트워크의 주소 공간에 포함되어야 합니다.

<input type="checkbox"/> 서브넷 이름	주소 범위	주소
<input type="checkbox"/> vmSubnet	10.30.0.0/24	10.30.0.0 - 10.30.0.255(256개 주소)
<input checked="" type="checkbox"/> endpointSubnet ✓	10.30.1.0/24 ✓	10.30.1.0 - 10.30.1.255(256개 주소)
<input type="checkbox"/>		(0개 주소)

5. [네트워킹] 탭에서 아래와 같이 구성하고 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
- 가상 네트워크: 03_storageRg-vnet
 - 서브넷: vmSubnet(10.30.0.0/24)
 - 다른 옵션은 모두 기본값을 사용합니다.

가상 머신 만들기 ...

기본 사항 디스크 **네트워킹** 관리 고급 태그 검토 + 만들기

NIC(네트워크 인터페이스 카드) 설정을 구성하여 가상 머신에 대한 네트워크 연결을 정의합니다. 보안 그룹 규칙을 사용하여 포트, 인바운드 및 아웃바운드 연결을 제어하거나 기존 부하 분산 솔루션 뒤에 배치할 수 있습니다. [자세한 정보](#)

네트워크 인터페이스

가상 머신을 만들면 네트워크 인터페이스가 만들어집니다.

가상 네트워크 * ① (새로 만드는 중) 03_storageRg-vnet
[새로 만들기](#)

서브넷 * ① (새로 만드는 중) vmSubnet(10.30.0.0/24)
[새로 만들기](#)

공용 IP ① (새로 만드는 중) storageVM-ip
[새로 만들기](#)

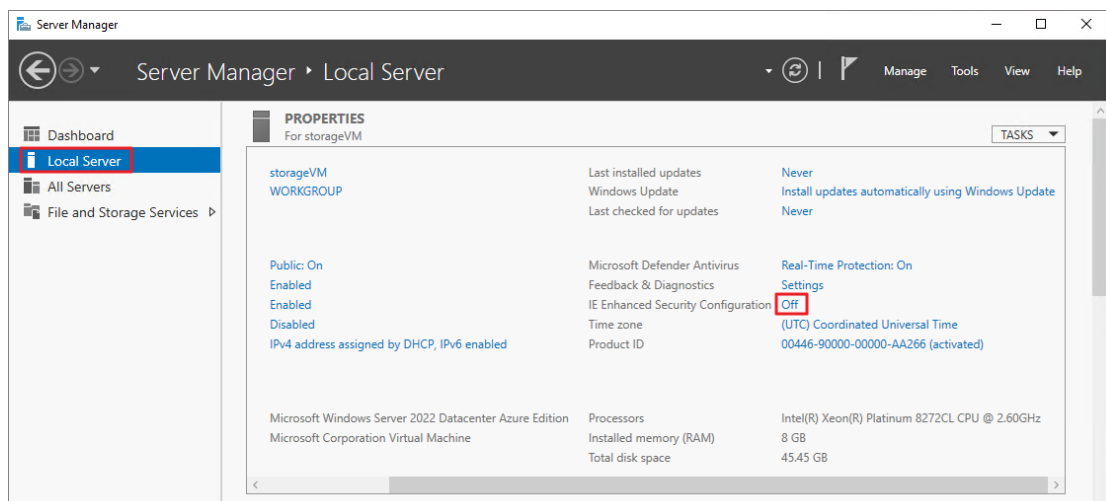
NIC 네트워크 보안 그룹 ①
☐ 없음
☒ 기본
☐ 고급

공용 인바운드 포트 * ①
☐ 없음
☒ 선택한 포트 허용

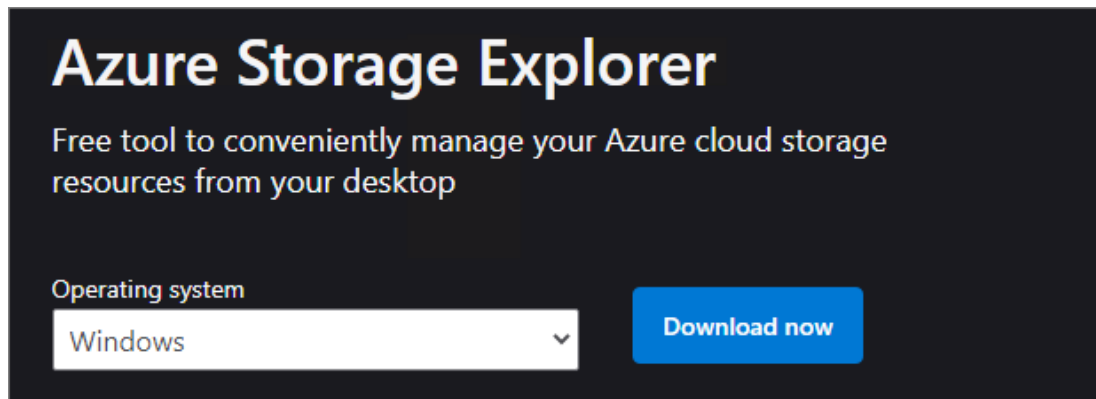
인바운드 포트 선택 * RDP (3389)

⚠ 이렇게 하면 모든 IP 주소가 가상 머신에 액세스할 수 있습니다. 이는 테스트용으로만 권장됩니다. [네트워킹] 탭의 [고급] 컨트롤을 사용하여 인바운드 트래픽을 알려진 IP 주소로 제한하는 규칙을 만듭니다.

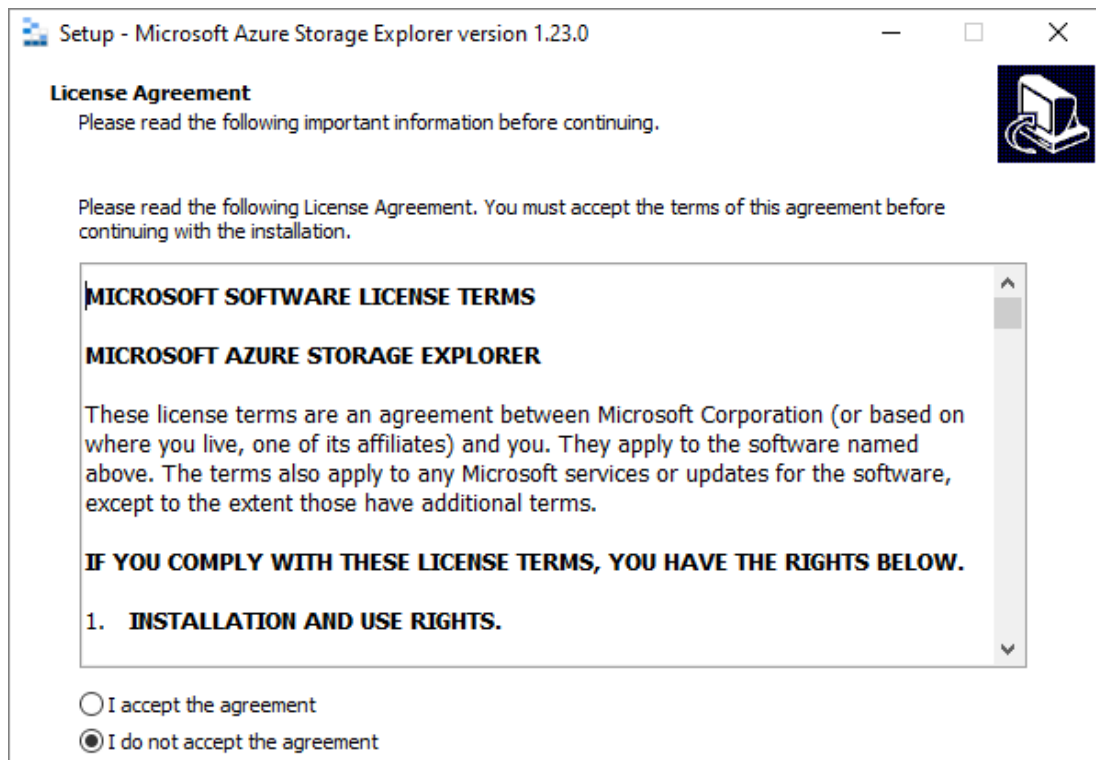
6. 새로 만든 가상 머신에 RDP를 통해 연결합니다. [Server Manager] 콘솔의 [Local Server]로 이동한 후 "IE Enhanced Security Configuration" 설정을 모두 "Off"로 변경합니다.



7. 브라우저를 열고 <https://azure.microsoft.com/en-us/features/storage-explorer/?msclkid=71f22d90aa7c11ecb4373a4f783243b3> 경로에서 Azure Storage Explorer를 다운로드합니다.



8. 다운로드한 파일을 실행하고 기본 옵션으로 Azure Storage Explorer를 설치합니다.



TASK 05. 스토리지 계정에 대한 Private Endpoint 구성

1. **stor** 접미사를 가진 [스토리지 계정] 블레이드로 이동합니다. [보안 + 네트워킹 - 네트워킹]에서 [프라이빗 엔드포인트 연결] 탭으로 이동한 후 [프라이빗 엔드포인트]를 클릭합니다.



2. [프라이빗 엔드포인트 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [다음]을 클릭합니다.

- [프로젝트 정보 - 리소스 그룹]: 03_storageRg
- [인스턴스 정보 - 이름]: storEndpoint
- [인스턴스 정보 - 지역]: East US

3. [리소스] 탭에서 대상 하위 리소스 드롭다운 메뉴를 확장한 후 "blob"을 선택하고 [다음]을 클릭합니다. 이 탭에서 확인할 수 있는 것처럼 스토리지의 각 하위 리소스에 대해 개별적으로 프라이빗 엔드포인트를 설정할 수 있습니다.

4. [가상 네트워크] 탭에서 아래와 같이 구성하고 [다음]을 클릭합니다.

- [네트워킹 - 가상 네트워크]: 03_storageRg-vnet
- [네트워킹 - 서브넷]: 03_storageRg-vnet/endpointSubnet(10.30.1.0/24)
- [프라이빗 DNS 통합 - 프라이빗 DNS 영역과 통합]: 예
- [프라이빗 DNS 통합 - 리소스 그룹]: 03_storageRg

5. [태그] 탭에서 [다음]을 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

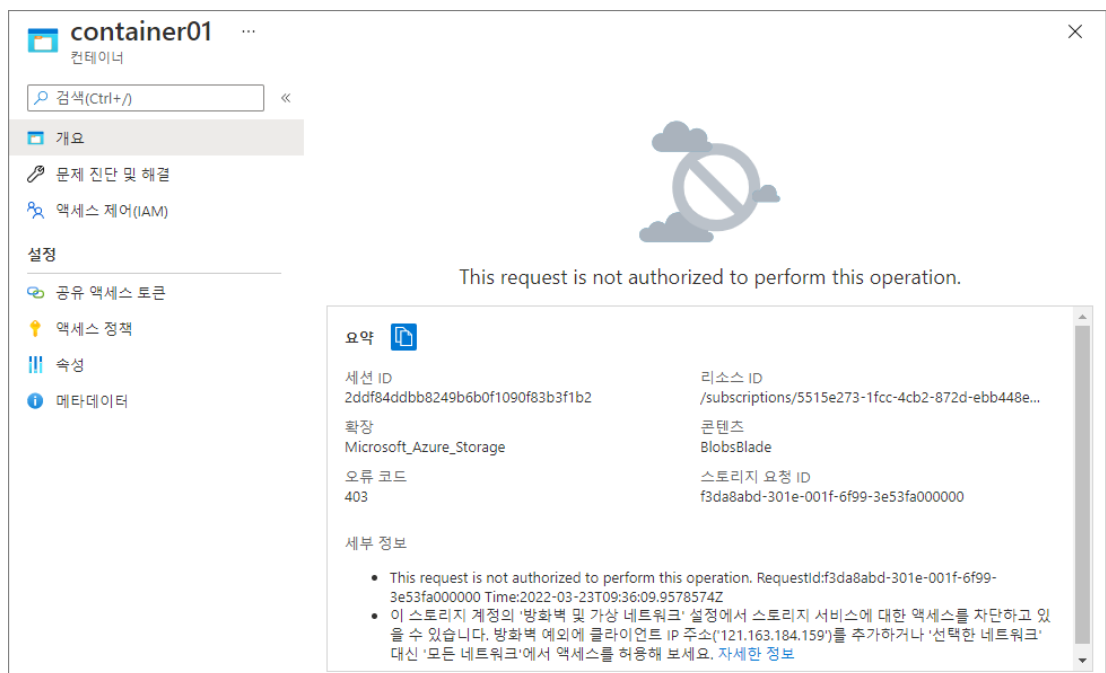
6. [스토리지 계정] 블레이드의 [보안 + 네트워킹 - 네트워킹]으로 이동합니다. [프라이빗 엔드포인트 연결] 탭을 클릭한 후 아래와 같이 새로 생성된 프라이빗 엔드포인트가 표시되는지 확인합니다.

7. [스토리지 계정] 블레이드의 [방화벽 및 가상 네트워크] 탭으로 이동합니다. 현재 상태는 "모든 네트워크"에서 스토리지 계정에 대한 액세스가 허용되도록 설정되어 있습니다. 프라이빗 링크를 통해 Blob 스토리지에 액세스할 것이기 때문에 다음에서 액세스 허용을 "선택한 네트워크"로 선택하고 [저장]을 클릭합니다.

- 모든 네트워크에서 액세스하지 않도록 설정했기 때문에 인터넷을 통해 스토리지 계정의 모든 유형(컨테이너, 파일 공유, 큐, 테이블)에 액세스할 수 없습니다.
- Azure 포털에서는 컨테이너, 파일 공유, 큐를 열면 컨테이너, 파일 공유, 큐는 표시되지만 이를 클릭하여 실제 내용을 확인하려고 하면 액세스가 차단되었다는 메시지가 표시됩니다.



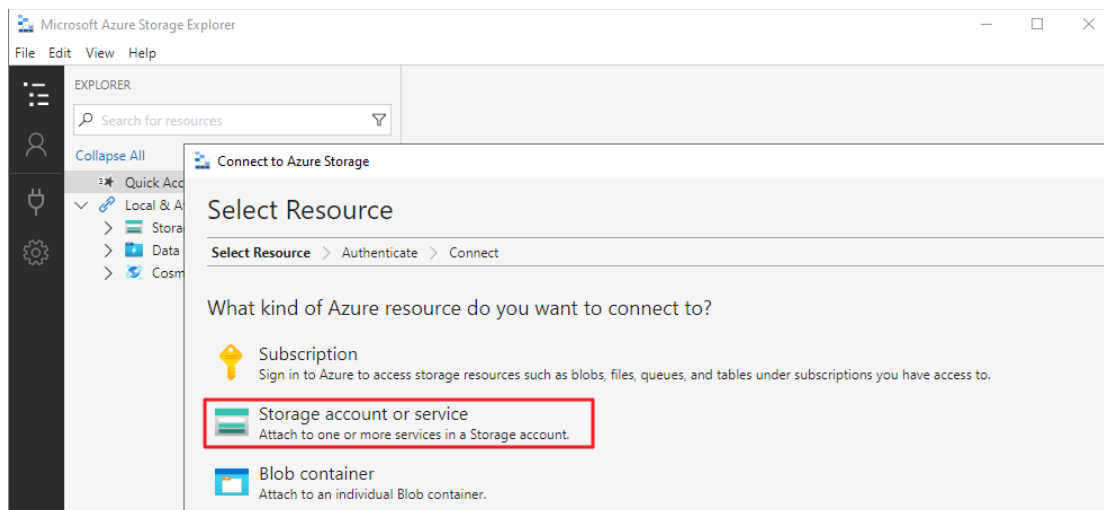
8. [스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 **container01** 컨테이너를 클릭합니다. 아래와 같이 컨테이너의 내용이 표시되지 않는 것을 확인합니다.



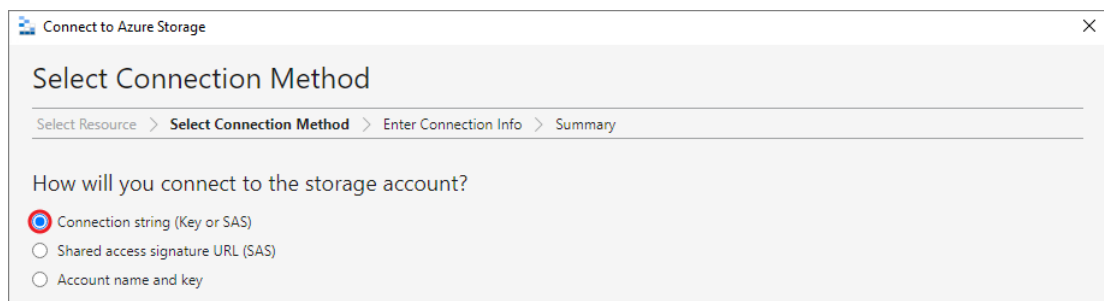
9. [스토리지 계정] 블레이드의 [보안 + 네트워킹 - 액세스 키]로 이동한 후 메뉴에서 [키 표시]를 클릭합니다. **key1**의 연결 문자열을 클립보드에 복사합니다.



10. 이전 작업에서 배포했던 가상 머신에 RDP로 연결합니다. [Microsoft Azure Storage Explorer]를 실행하고 [Connect to Azure Storage] 창에서 [Storage account or service]를 클릭합니다.



11. [Connect to Azure Storage] 창의 [Select Connection Method] 페이지에서 "Connection string (Key or SAS)"를 선택하고 [Next]를 클릭합니다.



12. [Enter Connection Info] 페이지에서 아래와 같이 구성하고 [Next]를 클릭합니다. [Summary] 페이지에서 [Connect]를 클릭합니다.

- Display name: 03_storageRg

- Connection string: 클립보드에 복사했던 값을 붙여 넣습니다.

Connect to Azure Storage

Enter Connection Info

Select Resource > Select Connection Method > Enter Connection Info > Summary

Display name:

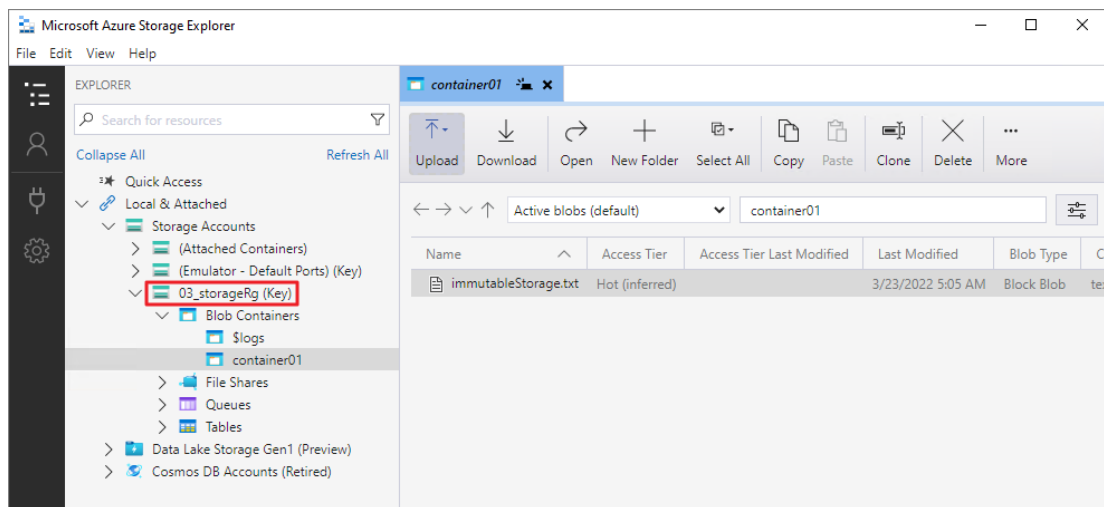
03_storageRg

Connection string:

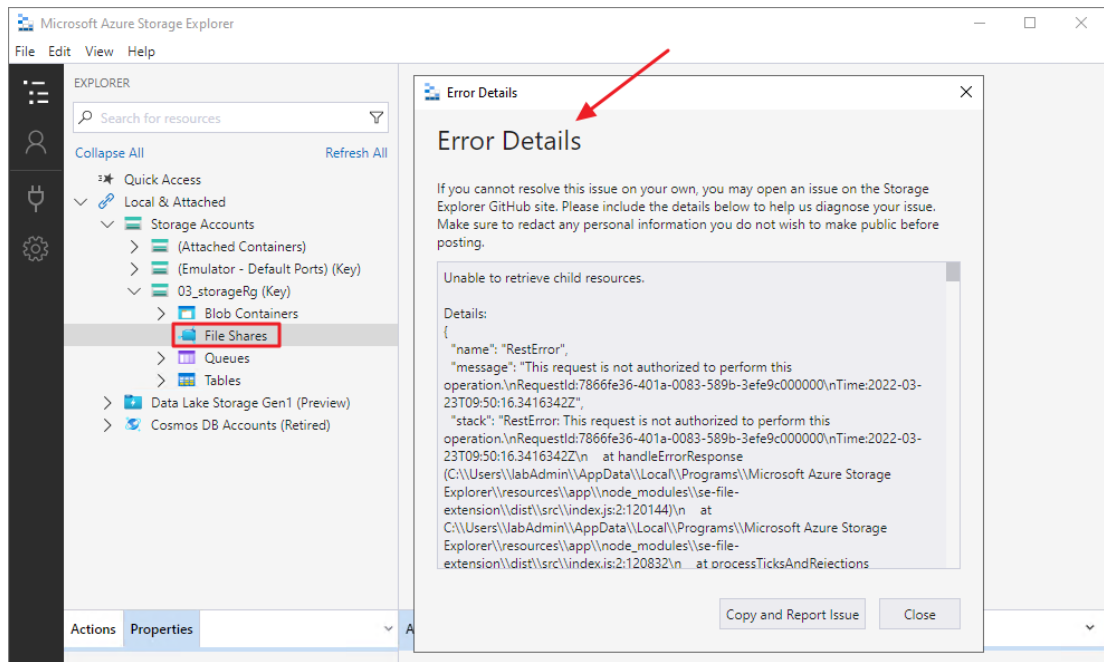
DefaultEndpointsProtocol=https;AccountName=kormtt0314stor;AccountKey=htol4wQICD8LH5Jg+BaOVRyU0F1fAC6b8yw8YM0mb+7yiqIsq2BR5yuV4CVtWtNngsXMR68z7wP+AStNVEIew=:EndpointSuffix=core.windows.net

13. [Microsoft Azure Storage Explorer]의 [Local & Attached - Storage Accounts - 03_storageRg - Blob Containers]를 확장한 후 **container01** 컨테이너를 클릭합니다. 아래와 같이 컨테이너의 내용이 표시되는 것을 확인합니다. 다음과 같은 작업을 진행하여 프라이빗 엔드포인트를 통해 Blob 스토리지 작업을 진행할 수 있는지 확인합니다.

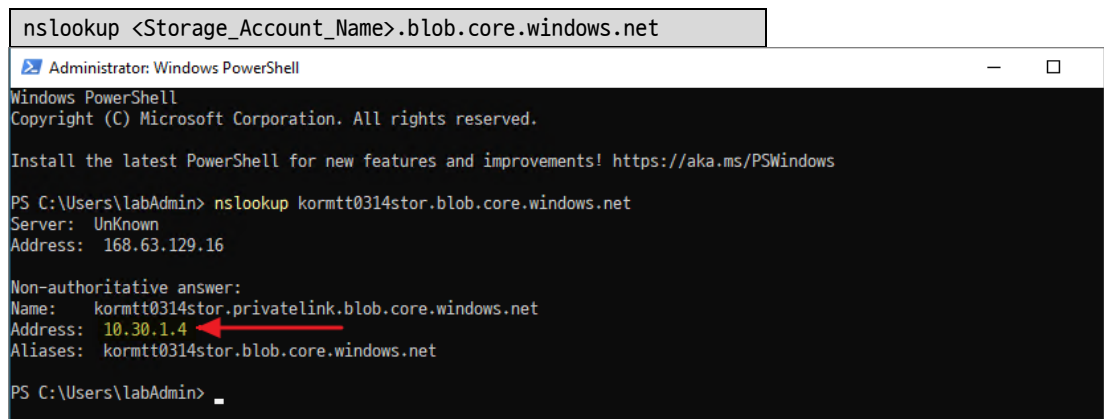
- **container02** 이름의 컨테이너를 만들고 이 컨테이너에 파일을 업로드합니다.
- **container01** 컨테이너에서 보존 설정이 되어 있는 Blob 파일을 삭제하고 Azure 포털과 마찬가지로 삭제 실패가 표시되는 것을 확인합니다.



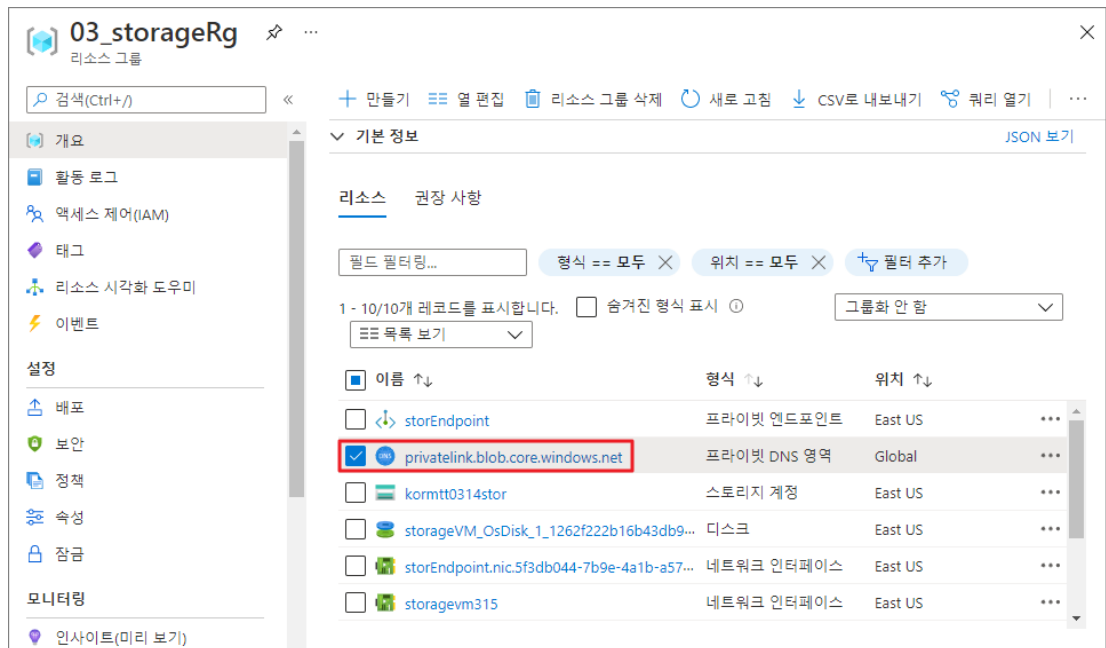
14. [Microsoft Azure Storage Explorer]에서 [Local & Attached - Storage Accounts - 03_storageRg - File Shares]를 확장한 후 아래와 같이 액세스 오류가 발생하는 것을 확인합니다. 프라이빗 엔드포인트가 설정되어 있지 않은 큐와 테이블 또한 동일하게 오류가 발생하는 것을 확인합니다.



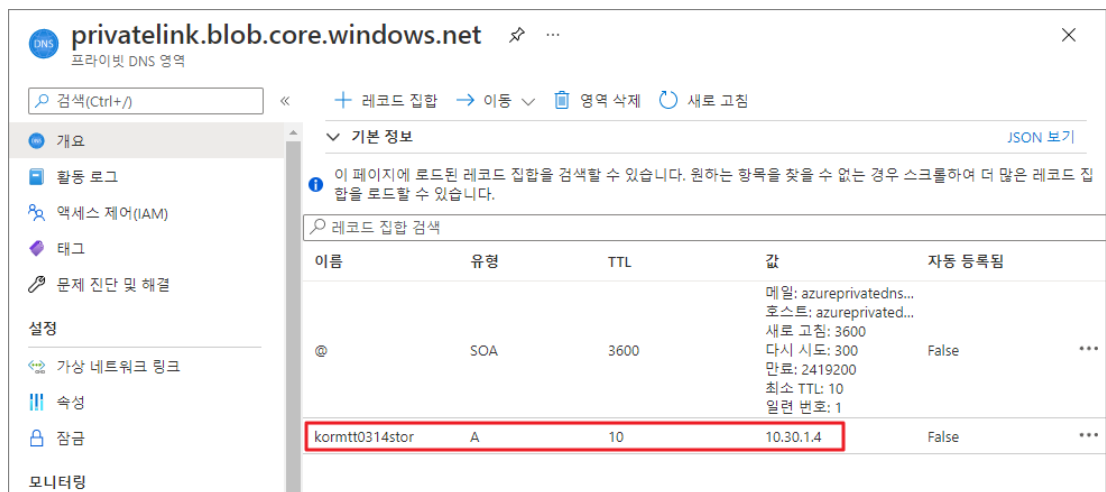
15. 가상 머신에서 PowerShell을 열고 다음 명령을 실행하여 프라이빗 엔드포인트로 등록된 Blob 엔드포인트의 IP 주소가 프라이빗 IP 주소로 반환되는 것을 확인합니다.



16. [03_storageRg 리소스 그룹] 블레이드로 이동한 후 프라이빗 DNS 영역 리소스를 클릭합니다.



17. [privatelink.blob.core.windows.net 프라이빗 DNS 영역] 블레이드의 [개요]에서 아래와 같이 등록된 스토리지 계정 이름과 프라이빗 IP 주소를 확인할 수 있습니다.

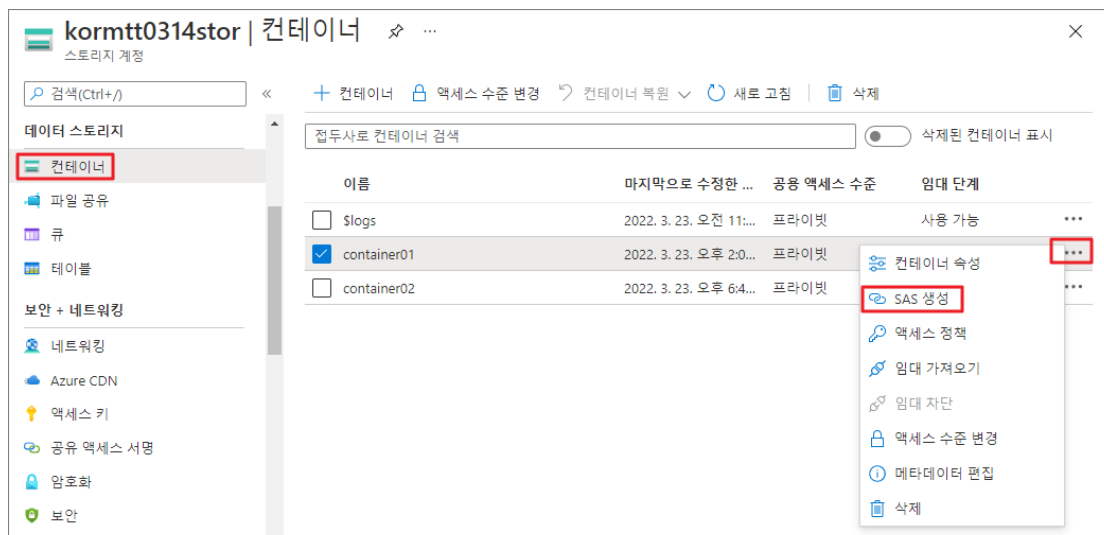


TASK 06. 리소스 정리

1. [스토리지 계정] 블레이드의 [보안 + 네트워킹 - 네트워킹]으로 이동한 후 [방화벽 및 가상 네트워크] 탭을 클릭합니다. "방화벽" 영역에서 "클라이언트 IP 주소 추가" 옵션을 선택하고 [저장]을 클릭합니다.



2. [스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 **container01** 컨테이너를 선택하고 [... - 액세스 정책]을 클릭합니다.



3. [액세스 정책]에서 변경이 불가능한 Blob 스토리지의 모든 정책을 삭제하고 [저장]을 클릭합니다.

액세스 정책

container01

 저장

액세스 정책을 저장했습니다.

[+ 정책 추가](#)

식별자	시작 시간	만료 시간	권한
결과 없음			

변경이 불가능한 Blob 스토리지 ⓘ

[+ 정책 추가](#)

식별자	범위	보존 간격	상태	
시간 기준 보존	컨테이너	1일	잠금 해제됨	...
법적 보존	컨테이너	무한	사용	...

4. `03_storageRg` 리소스 그룹을 삭제합니다.