

한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 07

LAB 05. Blob 스토리지의 공용 액세스

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 허용되지 않습니다.

© 2023 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
2023.08.28	1.0.0	우진환	LAB 05 내용 작성

목차

도전 과제.....	5
STEP 01. BLOB 컨테이너를 가지고 있는 스토리지 계정 만들기.....	5
STEP 02. 스토리지 계정에 파일 업로드.....	5
STEP 03. 익명 액세스 확인.....	5
TASK 01. BLOB 컨테이너를 가지고 있는 스토리지 계정 만들기	6
TASK 02. 스토리지 계정에 파일 업로드	8
TASK 03. 익명 액세스 확인	9

도전 과제

이 실습에서는 퍼블릭 컨테이너를 가지고 있는 Azure 스토리지 계정을 만들고 파일을 업로드한 다음 퍼블릭 액세스를 테스트합니다.

STEP 01. Blob 컨테이너를 가지고 있는 스토리지 계정 만들기

1. 다음 속성을 사용하여 스토리지 계정을 만듭니다.

속성	값
리소스 그룹	CSSClod<xxxxxxxx>
스토리지 계정 이름	sa<xxxxxxxx>
지역	(US) East US
성능	표준
중복	LRS(로컬 중복 스토리지)

2. 새로 만든 스토리지 계정의 익명 액세스를 허용하도록 설정합니다.
3. "public" 이름의 컨테이너를 만들고 Blob에 대한 익명 읽기 전용 액세스를 허용합니다.

STEP 02. 스토리지 계정에 파일 업로드

1. public 컨테이너에 임의의 이미지 파일을 업로드합니다.
2. 업로드한 이미지 파일의 Blob 인덱스 태그에 키(source)와 값(Portal)을 추가합니다.

STEP 03. 익명 액세스 확인

1. public 컨테이너에 두 번째 이미지 파일을 업로드합니다. 이 이미지는 "쿨" 티어로 업로드합니다.
2. 두 번째 이미지 파일의 Blob 인덱스 태그에 키(source)와 값(Archive)을 추가합니다.
3. 브라우저에서 업로드한 이미지 파일을 볼 수 있는지 확인합니다.

TASK 01. Blob 컨테이너를 가지고 있는 스토리지 계정 만들기

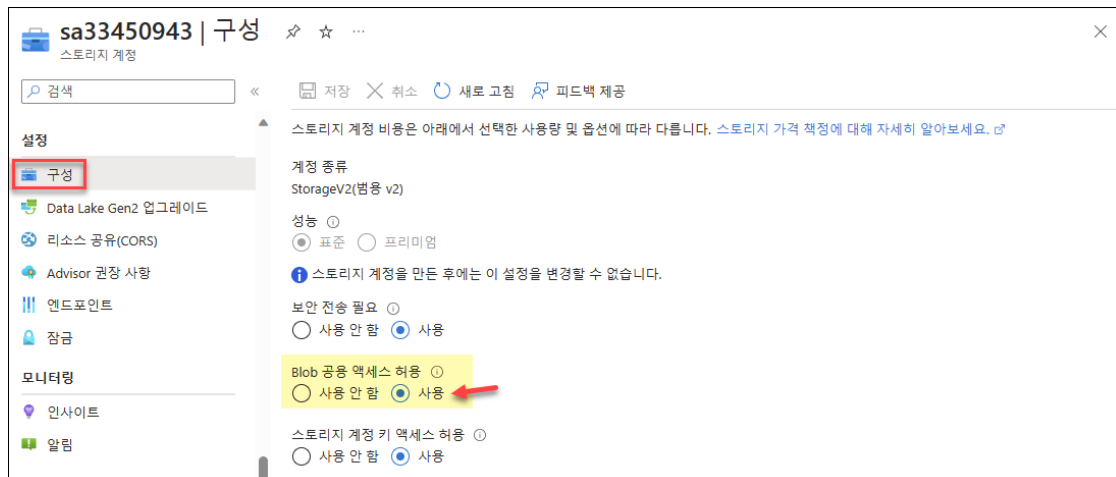
1. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드에서 [만들기]를 클릭합니다.



2. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토]를 클릭합니다. [검토] 탭에서 [만들기]를 클릭합니다.

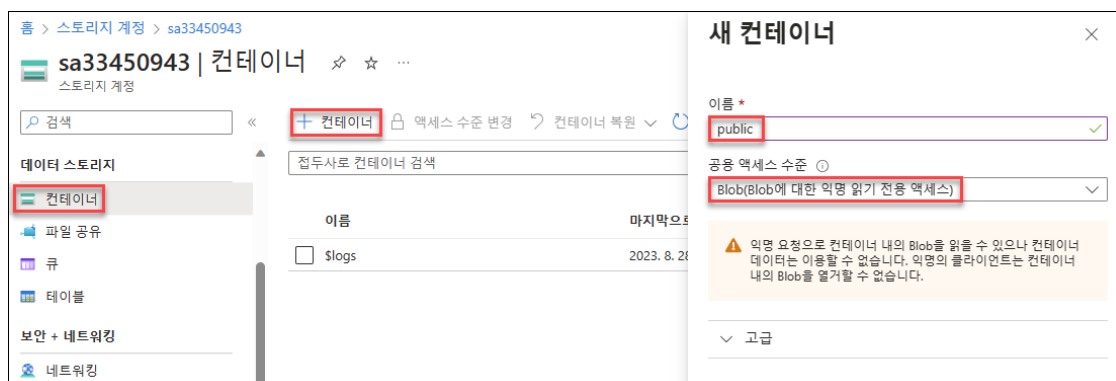
- [프로젝트 정보 - 리소스 그룹]: CSSClod<xxxxxxxx>
- [인스턴스 정보 - 스토리지 계정 이름]: sa<xxxxxxxx>
- [인스턴스 정보 - 지역]: (US) East US
- [인스턴스 정보 - 성능]: 표준
- [인스턴스 정보 - 중복]: LRS(로컬 중복 스토리지)

3. 새로 만든 [sa<xxxxxxxx>] 스토리지 계정 블레이드의 [설정 - 구성]으로 이동합니다. "Blob 공용 액세스 허용" 설정이 "사용"으로 설정되어 있는지 확인합니다.

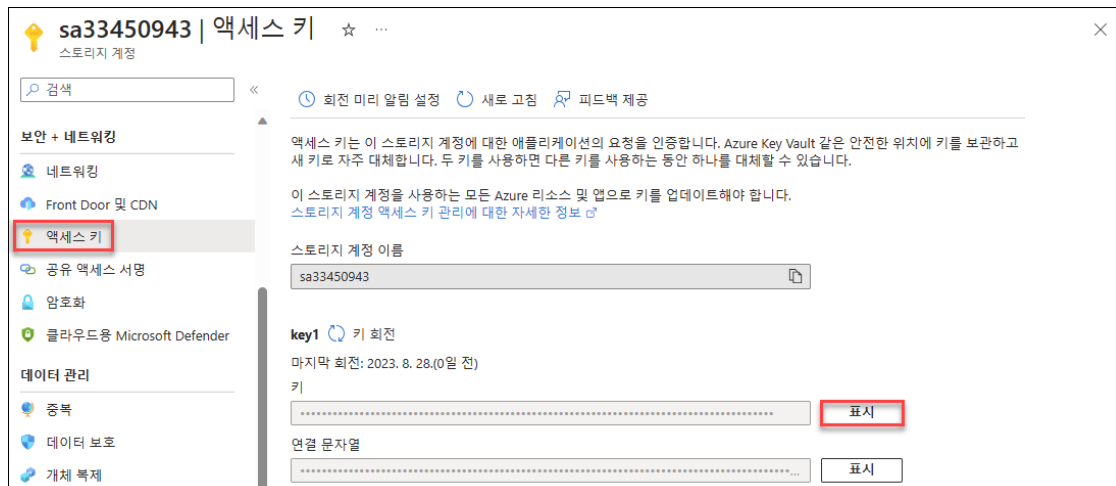


4. [sa<xxxxxxxx> 스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 메뉴에서 [컨테이너]를 클릭합니다. [새 컨테이너]에서 아래와 같이 구성한 후 [만들기]를 클릭합니다.

- 이름: public
- 공용 액세스 수준: Blob(Blob에 대한 익명 읽기 전용 액세스)

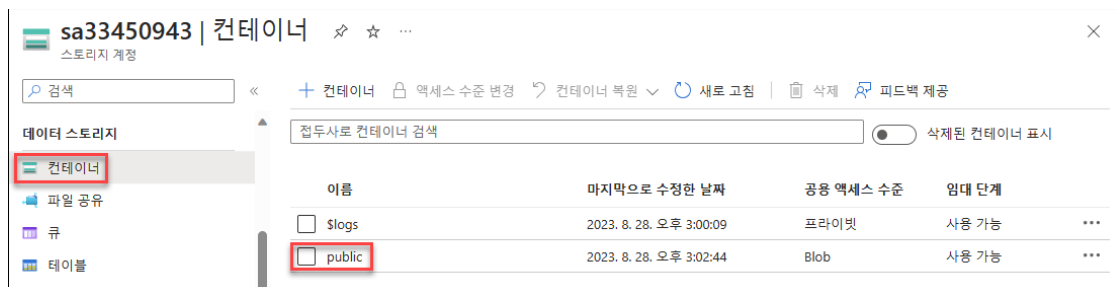


5. Blob 퍼블릭 액세스 수준은 익명 요청으로 컨테이너 내의 Blob을 읽을 수 있지만 컨테이너 데이터는 사용할 수 없습니다. 익명 클라이언트는 컨테이너 내의 Blob을 나열할 수 없지만 Blob을 개별적으로 읽을 수 있습니다.
6. [sa<xxxxxxxx> 스토리지 계정] 블레이드의 [보안 + 네트워킹 - 액세스 키]로 이동한 후 "key1"의 값을 확인합니다. 스토리지 계정에는 두 개의 액세스 키가 있으며 두 키 모두 스토리지 계정에 대한 전체 액세스를 제공합니다. 두 개의 키를 사용하면 해당 키를 사용할 수 있는 웹 앱과 같은 애플리케이션의 동작을 방해하지 않고 예약된 키의 재활용이 가능합니다.



TASK 02. 스토리지 계정에 파일 업로드

1. [sa<xxxxxxxx> 스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동합니다. **public** 컨테이너를 클릭합니다.



2. [public 컨테이너] 블레이드의 메뉴에서 [업로드]를 클릭합니다. [Blob 업로드] 창에서 아래와 같이 구성한 후 [업로드]를 클릭합니다.
 - 임의의 이미지 파일을 선택하여 업로드합니다.
 - [고급]을 확장합니다.
 - 블록 크기: 64 KiB
 - 액세스 계층: 핫(유추)
 - Blob 인덱스 태그: 키(source)와 값(Portal)을 입력합니다.



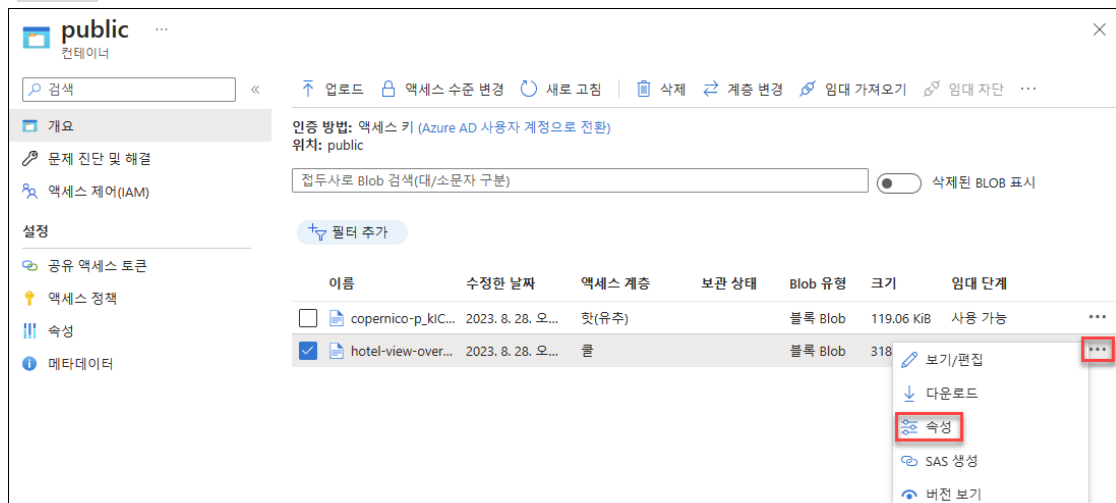
3. Blob 인덱스 태그는 파일이 업로드될 때 또는 업로드한 후에 설정할 수 있습니다. 태그는 간단한 키/값 쌍으로 구성되며 애플리케이션이나 Azure Cloud Shell을 사용하여 검색할 수 있습니다.

TASK 03. 익명 액세스 확인

1. [sa<xxxxxxxx> 스토리지 계정] 블레이드의 [데이터 스토리지 - 컨테이너]로 이동한 후 public 컨테이너를 클릭합니다. [public 컨테이너] 블레이드의 메뉴에서 [업로드]를 클릭합니다. [Blob 업로드] 창에서 아래와 같이 구성한 후 [업로드]를 클릭합니다.
 - 두 번째 임의의 이미지 파일을 업로드합니다.
 - 블록 크기: 64 KiB
 - 액세스 계층: 쿨
 - Blob 인덱스 태그: 키(source)와 값(Archive)을 입력합니다.



2. [public 컨테이너] 블레이드에서 두 번째로 업로드한 파일을 선택한 후 [... - 속성]을 클릭합니다.



3. Blob 파일 속성의 [개요]에서 URL 값을 복사합니다.



4. 다른 브라우저를 열고 복사한 URL에 액세스합니다. 아래와 같이 별도의 인증 없이 이미지 파일이 표시되는 것을 확인합니다.

