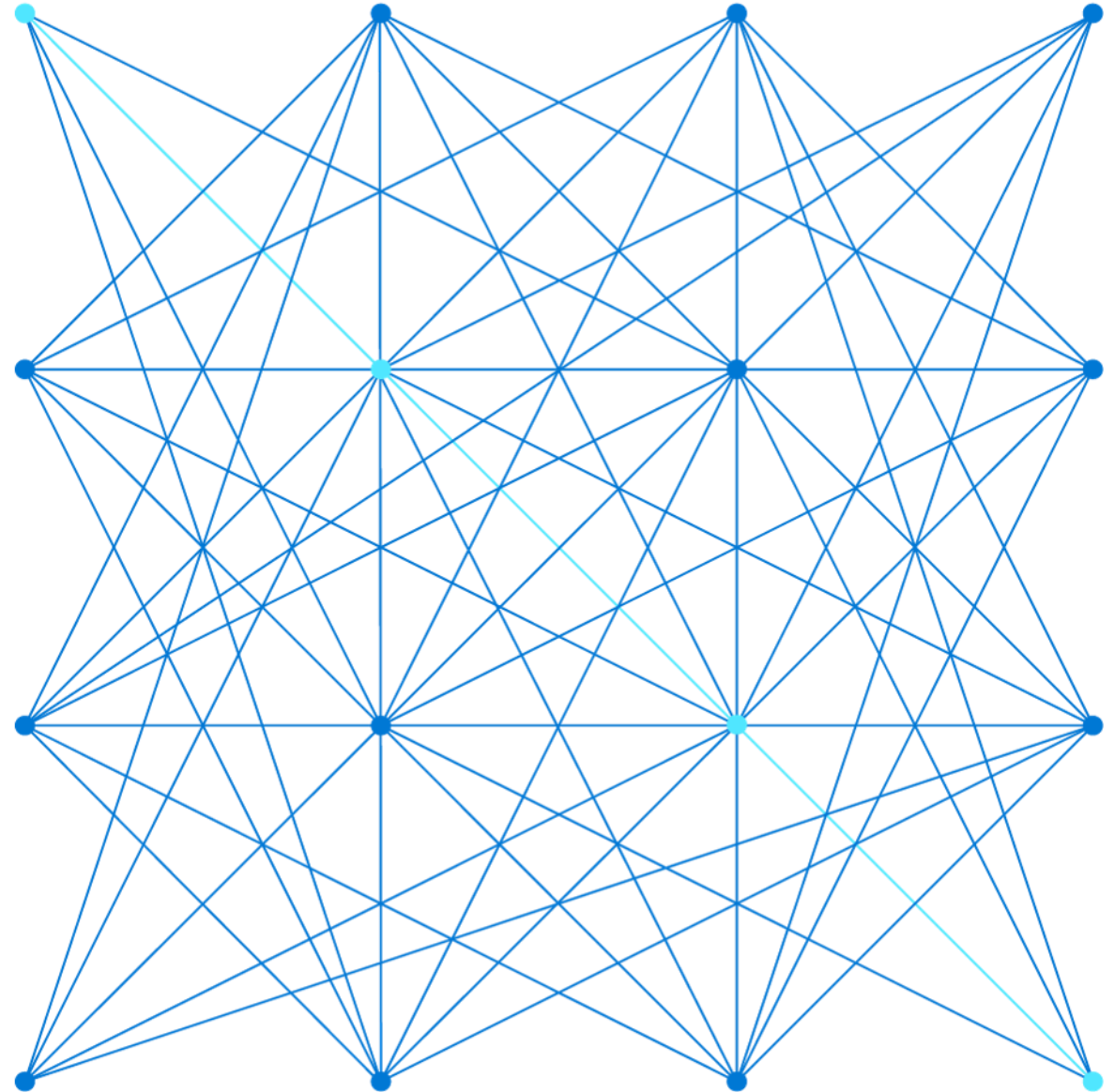
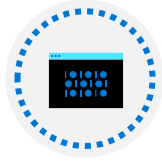


AZ-104T00A

Azure Storage 관리자



Azure Storage 관리 소개



[스토리지 계정 구성](#)



[Blob Storage 구성](#)



[스토리지 보안 구성](#)

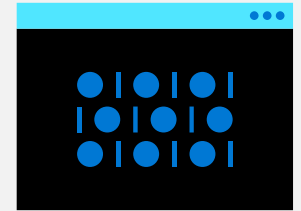


[Azure Files 및 파일 동기화 구성](#)



[랩 07 - Azure Storage 관리](#)

스토리지 계정 구성



스토리지 계정 구성 소개



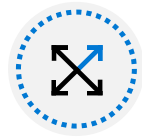
Azure Storage 구현



Azure Storage 서비스 살펴보기



스토리지 계정 유형 확인



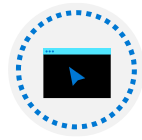
복제 전략 확인



스토리지 액세스



스토리지 엔드포인트 보호



데모 - 스토리지 엔드포인트 보호



요약 및 리소스

Azure Storage 구현

파일, 메시지, 테이블 및 기타 유형의 정보를 저장하는 데 사용할 수 있는 서비스

내구성, 보안, 확장성,
관리형, 액세스 가능성

가상 머신, 비구조적
데이터 및 구조적 데이터용
스토리지

2개 계층: 프리미엄 및
표준

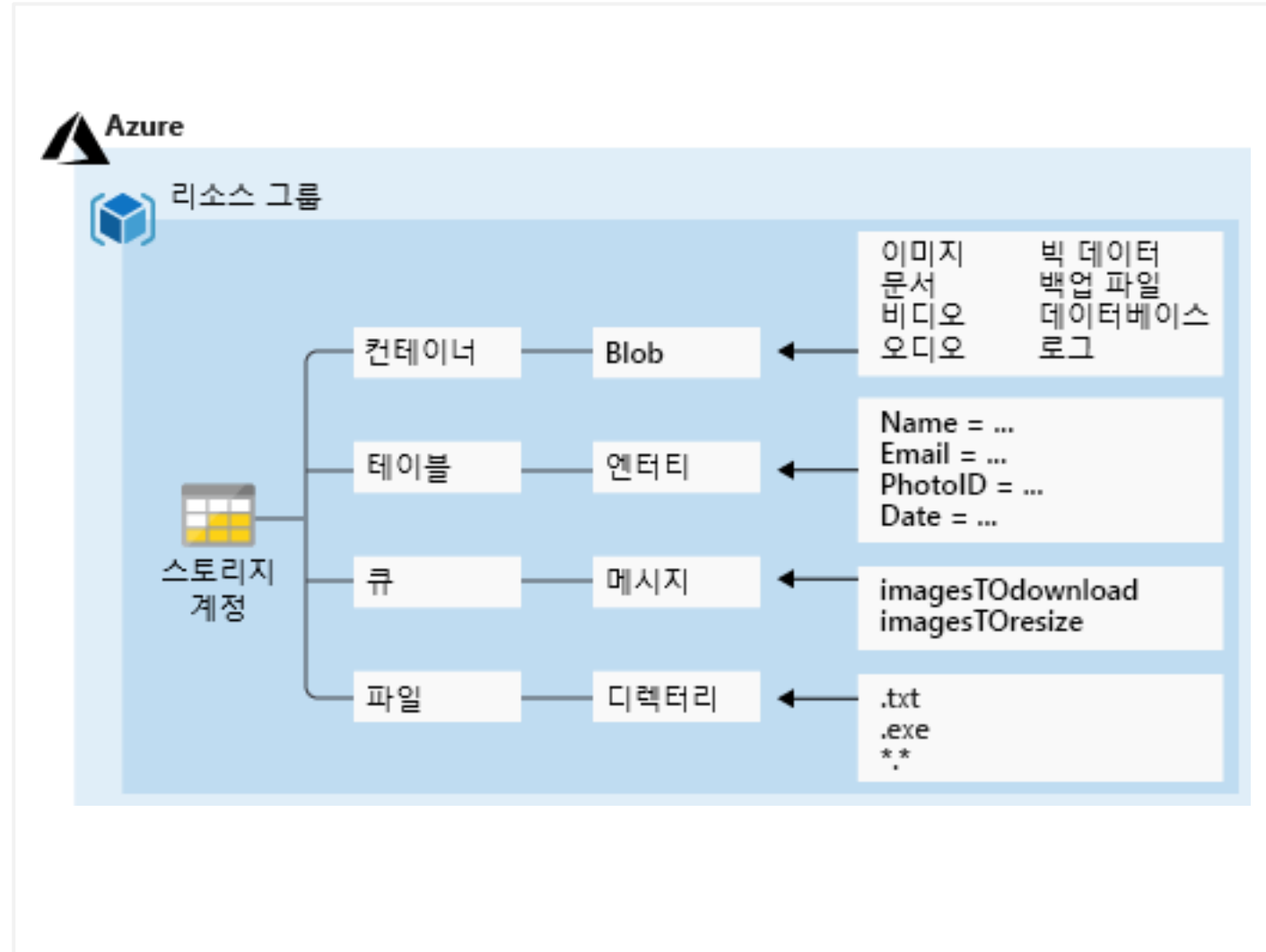
Azure Storage 서비스 살펴보기

Azure 컨테이너: 텍스트 및 이진 데이터를 위한 대규모로 스케일링 가능한 개체 저장소

Azure Tables: 구조화된 비관계형 데이터를 저장하기에 적합합니다.

Azure 큐: 애플리케이션 구성 요소 간에 안정적인 메시징을 위한 메시징 저장소입니다.

Azure Files: 클라우드 또는 온-프레미스 배포에 대한 관리형 파일 공유입니다.



스토리지 계정 유형 확인

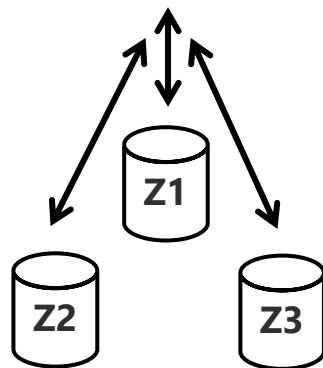
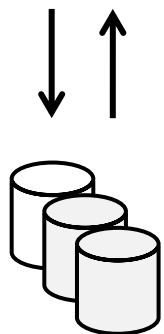
스토리지 계정	권장 사용량
표준 범용 v2	Blob, 파일, 큐, 테이블 및 Data Lake Storage를 비롯한 대부분의 시나리오.
Premium 블록 Blob	트랜잭션 속도가 높은 블록 Blob 시나리오 또는 더 작은 개체를 사용하거나 일관되게 짧은 스토리지 대기 시간이 필요한 시나리오에 추천됩니다.
프리미엄 파일 공유	기업 또는 고성능 파일 공유 애플리케이션.
프리미엄 페이지 Blob	프리미엄 고성능 페이지 Blob 시나리오.



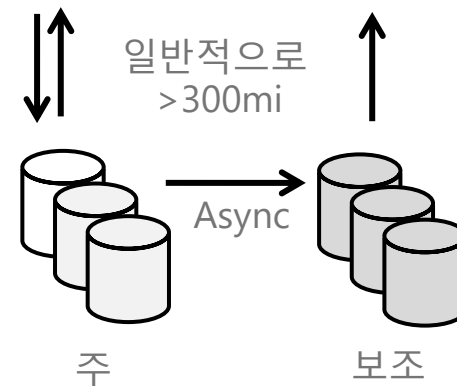
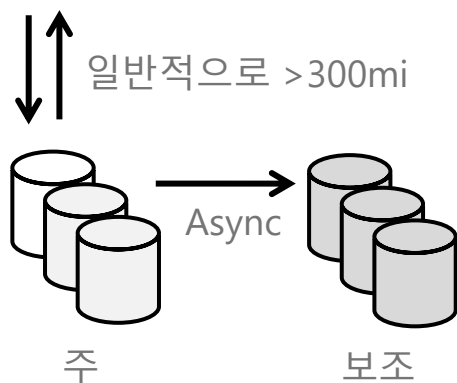
모든 스토리지 계정은 미사용 데이터에 대한 SSE(스토리지 서비스 암호화)를 사용하여 암호화됩니다.

복제 전략 확인 (1/2)

단일 지역



다중 영역



LRS

- 복제본 3개, 지역 1개
- 디스크, 노드, 랙 오류로부터 보호
- 모든 복제본이 커밋될 때 쓰기가 승인됩니다.
- 이중 패리티 RAID보다 우수

ZRS

- 복제본 3개, 영역 3개, 지역 1개
- 디스크, 노드, 랙 및 영역 오류로부터 보호
- 세 영역 모두에 동기 쓰기

GRS

- 복제본 6개, 지역 2개(지역당 3개)
- 주요 지역 재해로부터 보호
- 보조에 대한 비동기 복사본

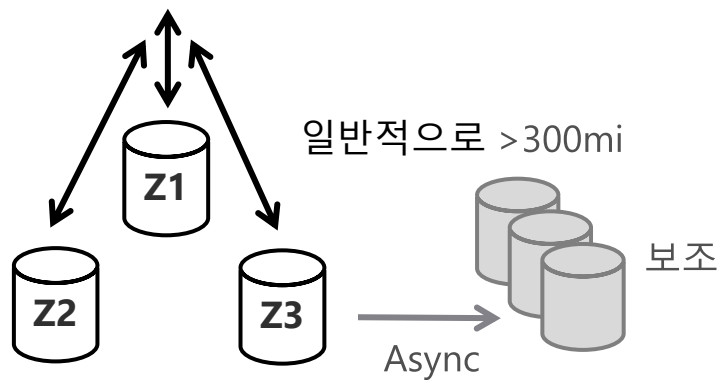
RA-GRS

- 보조에 대한 GRS + 읽기 액세스
- 별도의 보조 엔드포인트
- RPO(복구 지점 목표) 지연을 보조로 쿼리할 수 있음

다음 슬라이드에서 계속됨 ➡

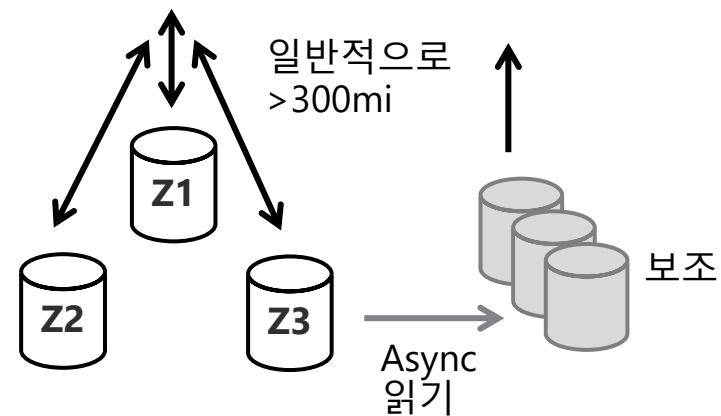
복제 전략 확인(2/2)

다중 영역



GZRS

- 복제본 6개, 영역 3+1개, 지역 2개
- 디스크, 노드, 랙, 영역 및 지역 오류로부터 보호
- 세 개 영역 모두에 동기식 쓰기 그리고 보조에 비동기식 쓰기



RA-GZRS

- GZRS + 보조에 대한 읽기 액세스
- 별도의 보조 엔드포인트
- 보조에 대한 RPO 지연을 쿼리할 수 있습니다.

스토리지 액세스

모든 개체에는 계정 이름 및 스토리지 형식에 따른 고유한 URL 주소가 있습니다.

컨테이너 서비스: `https://mystorageaccount.blob.core.windows.net`

테이블 서비스: `https://mystorageaccount.table.core.windows.net`

큐 서비스: `https://mystorageaccount.queue.core.windows.net`

파일 서비스: `https://mystorageaccount.file.core.windows.net`

원할 경우 사용자 지정 도메인 이름을 구성할 수 있습니다.

CNAME 레코드	대상
blobs.contoso.com	contosoblobs.blob.core.windows.net

스토리지 엔드포인트 보호

storage987123 | 방화벽 및 가상 네트워크

스토리지 계정

검색(Ctrl+/)

개요

활동 로그

액세스 제어(IAM)

태그

문제 진단 및 해결

데이터 전송

이벤트

저장

취소

새로 고침

다음에서 액세스 허용

☐ 모든 네트워크

☒ 선택한 네트워크

스토리지 계정에 대한 네트워크 보안을 구성합니다. [자세한 정보](#)

가상 네트워크

가상 네트워크로 스토리지 계정을 보호합니다. [+ 기존 가상 네트워크 추가](#) [+ 새 가상 네트워크 추가](#)

가상 네트워크	서브넷	주소 범위	엔드포인트 상태	리소스 그룹
▼ vnet01	1			Demo
	subnet01	10.1.0.0/24	✓ 가능하게 하다	Demo

방화벽 및 가상 네트워크를 통해 가상 네트워크의 특정 서브넷이나 공용 IP에서 스토리지 계정에 액세스하는 것을 제한할 수 있습니다.

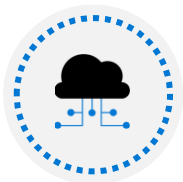
서브넷 및 가상 네트워크는 스토리지 계정과 동일한 Azure 지역 또는 지역 쌍에 있어야 합니다.

© Copyright Microsoft Corporation. All rights reserved.

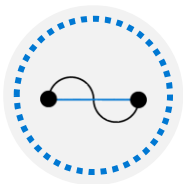
데모 - 스토리지 엔드포인트 보호



스토리지 계정 만들기



스토리지 계정으로 파일 업로드하기



서브넷 서비스 엔드포인트 만들기



서비스 엔드포인트에 스토리지를 고정합니다.



스토리지 엔드포인트 테스트

요약 및 리소스 – 스토리지 계정 구성

지식 점검 문제



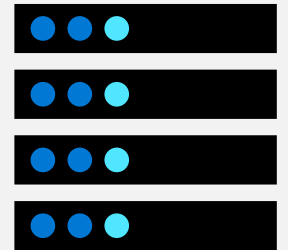
Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

[Azure Storage 계정 만들기\(샌드박스\)](#)

[지역 간에 스토리지 데이터를 복제하고 보조 위치로 장애 조치\(failover\)하여 재해 복구 제공](#)

샌드박스는 실습 연습을 나타냅니다.

Blob Storage 구성



Blob Storage 구성 소개



Blob Storage 구현



Blob 컨테이너 만들기



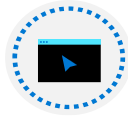
Azure Blob 계층 만들기



Blob 수명 주기 관리 규칙 추가



Blob 개체 복제 확인



데모 - Blob Storage



요약 및 리소스

* Blob 업로드 및 스토리지 가격은 다르지 않습니다.

Blob Storage 구현

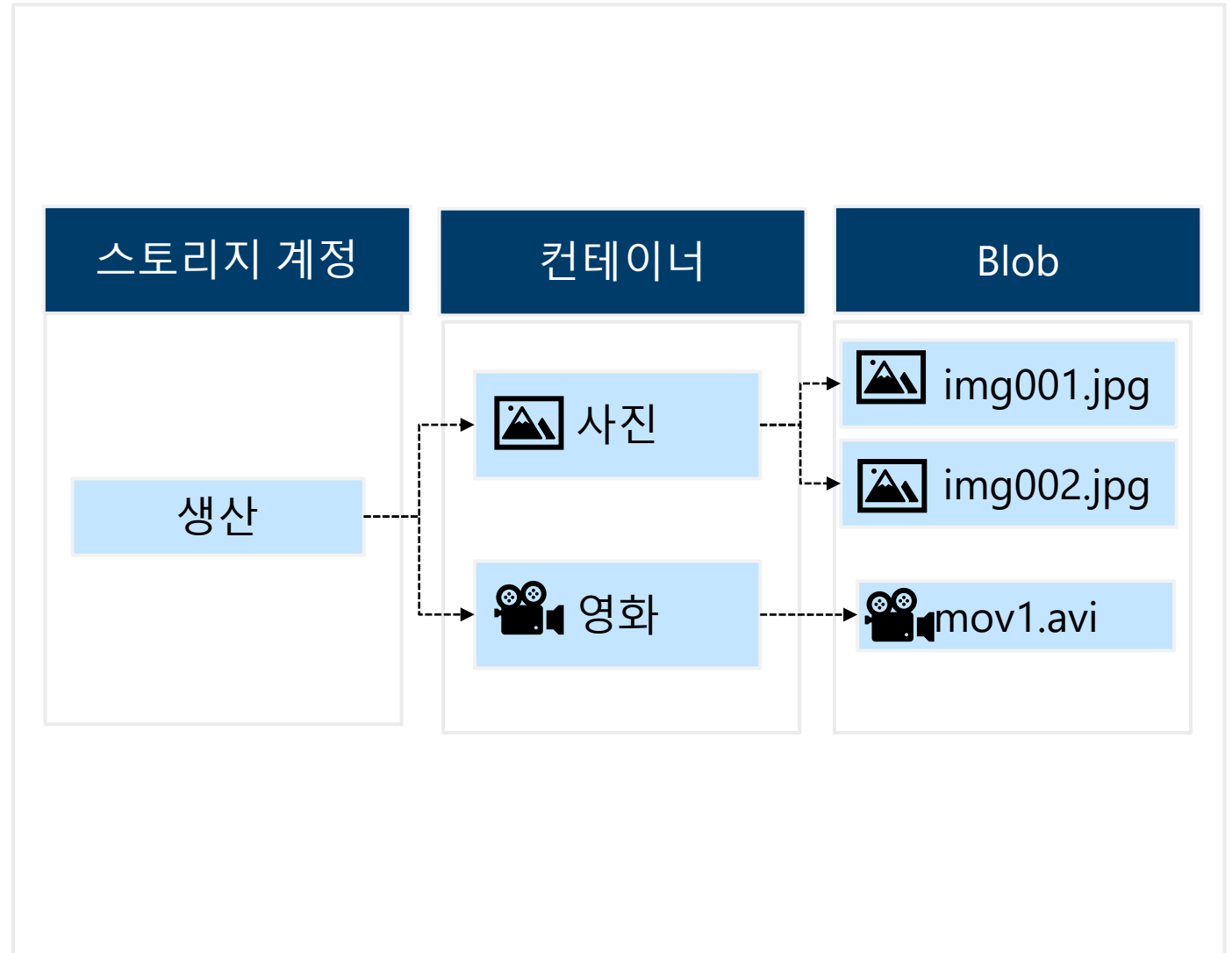
클라우드에 구조화되지 않은 데이터를 저장합니다.

모든 텍스트 또는 이진 데이터 형식을 저장할 수 있습니다.

개체 스토리지라고도 합니다.

일반적인 용도:

- 브라우저에 직접 이미지 또는 문서 제공
- 분산 액세스용 파일 저장.
- 비디오 및 오디오 스트리밍.
- 백업 및 복원, 재해 복구, 보관용으로 데이터 저장
- 온-프레미스 또는 Azure 호스팅 서비스에서 분석하기 위한 데이터 저장.



Blob 컨테이너 만들기

모든 Blob은 컨테이너에 있어야 합니다.

계정에는 무제한의 컨테이너가 있습니다.

컨테이너에는 무제한의 Blob이 있을 수 있습니다.

프라이빗 Blob - 익명 액세스 없음

Blob 액세스 - Blob 전용의 익명 퍼블릭 읽기 권한

컨테이너 액세스 - Blob을 포함하여 전체 컨테이너에 대한 익명의 퍼블릭 읽기 및 리스트 액세스

+ 컨테이너

🔒 액세스 수준 변경

🔄 새로 고침

🗑️ 삭제

새 컨테이너

이름 *

공용 액세스 수준 ⓘ

프라이빗(익명 액세스 없음) ▼

만들기

취소

공용 액세스 수준 ⓘ

개인(익명 액세스 없음) ▲

개인(익명 액세스 없음)

Blob(Blob의 익명 읽기 액세스 전용)

컨테이너(컨테이너 및 Blob에 대한 익명 읽기 액세스)

Azure Blob 계층 만들기

핫 계층 - 스토리지 계정에서 개체에 빈번한 액세스하는 경우에 적합합니다.

쿨 계층 - 자주 액세스하지 않으며 30일 이상 저장되는 대량의 데이터 저장에 적합합니다.

보관 - 검색 대기 시간에 몇 시간이 걸려도 괜찮으며, 180일 이상 보관 계층에 저장할 데이터에 적합합니다.

계층 변경

적합한 액세스 계층에 데이터를 배치하여 스토리지 비용을 최적화하세요. [Azure Blob Storage 액세스 계층에 대한 자세한 정보](#)

액세스 계층

핫(유추)

핫(유추)

쿨

보관



언제든지 이러한 액세스 계층을 전환할 수 있습니다.

Blob 수명 주기 관리 규칙 추가

Blob을 성능과 비용을 최적화하기 위해 더
쿨한 스토리지 계층으로 전환

수명 주기가 끝나면 Blob 삭제

스토리지 계정의 필터링된 경로에 규칙 적용

규칙 추가 ...

✓ 자세히 2 기본 Blob

수명 주기 관리에서는 규칙을 사용하여 Blob을 자동으로 쿨 계층으로 이동하거나 삭제합니다. 규칙을 여러 개 만드는 경우
관련된 작업을 계층 순서대로(핫 스토리지에서 쿨 스토리지로, 다음으로 보관, 그다음으로 삭제)에 구현해야 합니다.

+ if-then 블록 추가

If

기본 Blob이 *

☒ 마지막으로 수정한 날짜

다음 일 수 전 *

값 입력

Then

Blob 삭제

쿨 스토리지로 이동

최소 30일 동안 쿨 스토리지에 보관하려는 자주 액세스하지 않는 데이터용입니다.

보관 스토리지로 이동

온라인 액세스가 필요하지 않고 개체를 180일 이상 동안 보관하려는 경우 사용합니다.

Blob 삭제

지정된 조건에 따라 개체를 삭제합니다.

Blob 개체 복제 확인

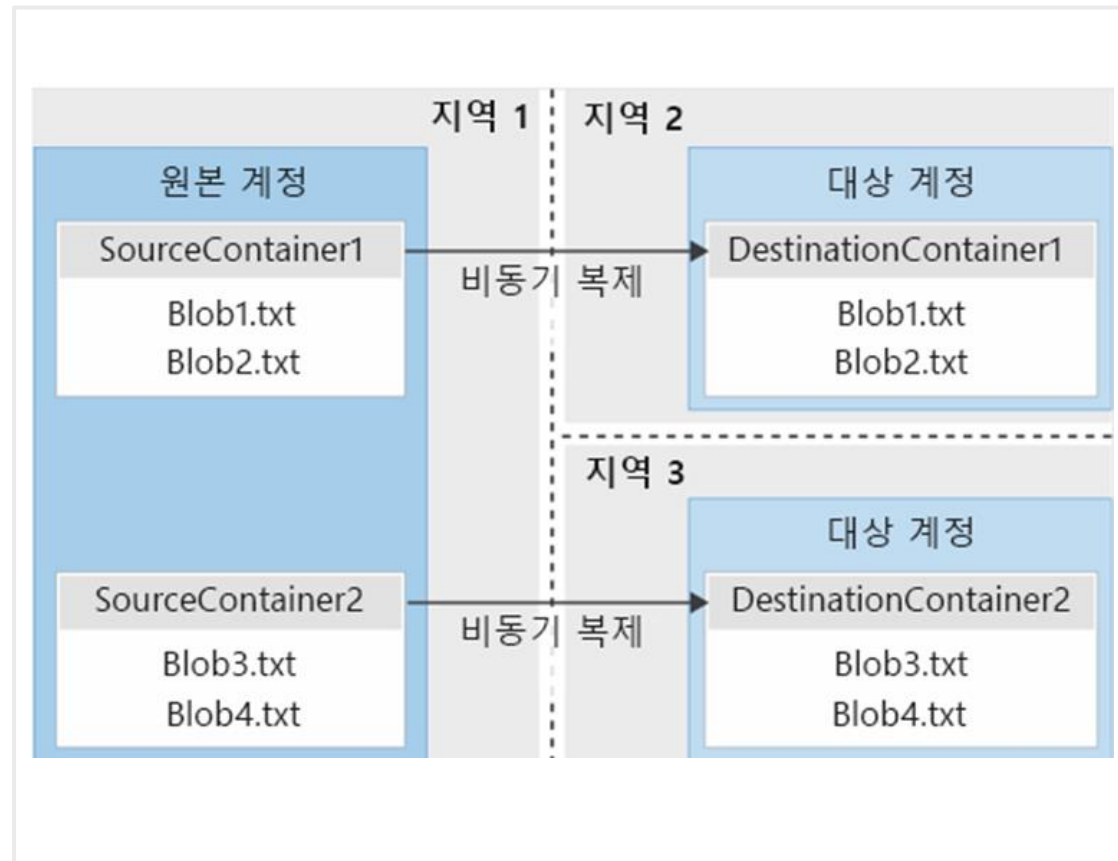
다른 지역과 비동기식

읽기 요청의 대기 시간 최소화

컴퓨팅 작업의 효율성 향상

데이터 배포 최적화

비용 최적화



데모 - Blob Storage



컨테이너
만들기

블록 Blob
업로드

블록 Blob
다운로드

요약 및 리소스- Blob Storage 구성

지식 점검 문제



Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

[Azure Blob 스토리지 계층을 사용하여 스토리지 성능 및 비용 최적화\(샌드박스\)](#)

[Azure Blob Storage 컨테이너에서 메트릭 수집\(샌드박스\)](#)

샌드박스는 실습 연습을 나타냅니다.

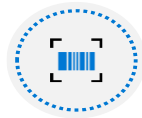
스토리지 보안 구성



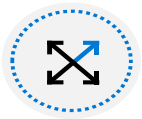
스토리지 보안 구성 소개



스토리지 보안 전략 검토



공유 액세스 서명 만들기



URI 및 SAS 매개 변수 식별



데모 – SAS(포털)



스토리지 서비스 암호화 확인



고객 관리형 키 만들기

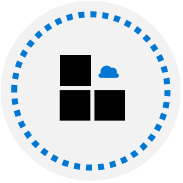


스토리지 보안 모범 사례 적용



요약 및 리소스

스토리지 보안 전략 검토



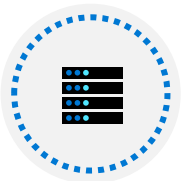
스토리지 서비스 암호화



Azure AD 및 RBAC를 통해 인증



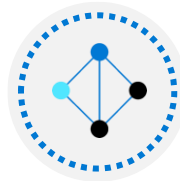
전송 중인 데이터에 대한
클라이언트 측 암호화,
HTTPS 및 SMB 3.0



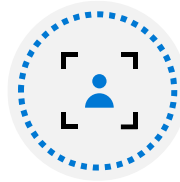
Azure Disk Encryption



공유 액세스 서명 - 위임된 액세스



공유 키 - 암호화된 서명 문자열



컨테이너 및 Blob에 대한 익명
액세스

공유 액세스 서명 만들기

위임된 액세스를 리소스에 제공

스토리지 계정 키를 공유하지 않고도 클라이언트에게 액세스 권한 부여 가능

계정 SAS는 스토리지 서비스 하나 이상의 리소스에 대한 액세스를 위임합니다.

서비스 SAS는 스토리지 서비스 중 하나의 리소스에 대한 액세스 권한을 위임합니다.

허용되는 서비스 ①

☒ Blob ☒ 파일 ☒ 큐 ☒ 테이블

허용되는 리소스 종류 ①

☐ 서비스 ☒ 컨테이너 ☐ 개체

허용되는 권한 ①

☒ 읽기 ☒ 쓰기 ☒ 삭제 ☒ 목록 ☒ 추가 ☒ 만들기 ☒ 업데이트 ☒ 프로세스

Blob 버전 관리 권한 ①

☒ 버전 삭제 사용

허용되는 Blob 인덱스 권한 ①

☒ 읽기/쓰기 ☒ 필터

시작 및 만료 날짜/시간 ①

시작 2021. 06. 26. 오후 5:05:09

종료 2021. 06. 27. 오전 1:05:09

(UTC+07:00) 방콕, 하노이, 자카르타

허용되는 IP 주소 ①

예: 168.1.5.65 또는 168.1.5.65-168.1.5.70

허용되는 프로토콜 ①

☒ HTTPS만 사용 ☐ HTTPS 및 HTTP

기본 설정 라우팅 계층 ①

☒ 기본(기본값) ☐ Microsoft 네트워크 라우팅 ☐ 인터넷 라우팅

① 엔드포인트가 게시되지 않았기 때문에 일부 라우팅 옵션을 사용할 수 없습니다.

서명 키 ①

key1

SAS 및 연결 문자열 생성

URI 및 SAS 매개 변수 식별

- SAS는 하나 이상의 스토리지 리소스를 가리키는 서명된 URI입니다.
- 스토리지 리소스 URI 및 SAS 토큰으로 구성됩니다.



<https://myaccount.blob.core.windows.net/?sp=r&st=2020-05-11T18:31:43Z&se=2020-05-12T02:31:43Z&spr=https&sv=2019-10-10&sr=b&sig=j0qABJZHfUVEBQ3yVn7kWiCKl00sxCiK1rzEchfAz8U%3D>

리소스 URI, 스토리지 서비스 버전, 서비스, 리소스 유형, 시작 시간, 만료 시간, 리소스, 권한, IP 범위, 프로토콜, 서명에 대한 매개 변수를 포함합니다.

데모 – SAS(포털)



서비스 수준에서
SAS 만들기

계정 수준에서
SAS 만들기

스토리지 서비스 암호화 확인

데이터를 보호하여 보안 및 규정 준수 상태 개선

자동으로 데이터를 암호화하고 해독

256비트 AES 암호화를 통해 암호화됨

모든 새 스토리지 계정과 기존 스토리지 계정에 대해 사용 가능하며 비활성화할 수 없습니다.

사용자에게 투명합니다.



자신만의 키를 사용할 수 있습니다(다음 토픽).

암호화

 저장  취소

스토리지 서비스 암호화는 미사용 데이터를 보호합니다. Azure Storage는 데이터 센터에서 작성되는 데이터를 암호화하고 사용자가 데이터에 액세스할 때 자동으로 데이터를 암호 해독합니다.

기본적으로 스토리지 계정의 데이터는 Microsoft 관리 키를 사용하여 암호화됩니다. 고유한 키를 가져올 수 있습니다.

스토리지 서비스 암호화를 사용하도록 설정하면 새 데이터만 암호화되고 이 스토리지 계정의 배경 암호화 프로세스를 통해 소급해서 암호화됩니다.

[Azure Storage 암호화에 대한 자세한 정보](#)

암호화 형식

☒ Microsoft 관리 키

☐ 고객 관리 키

고객 관리형 키 만들기

Azure Key Vault를 사용하여 암호화 키를 관리합니다.

자신의 암호화 키를 만들어
키 자격 증명 모음에 저장

Azure Key Vault의 API를 사용하여 암호화
키를 생성합니다.

사용자 지정 키를 통해 유연성과 제어를
더 많이 제공

암호화 형식

☐ Microsoft 관리 키

☒ 고객 관리 키

i 스토리지 계정 'wallock'은(는) 선택한 키 자격 증명 모음에 대한 액세스 권한을 받습니다. 일시 삭제와 보호 제거 모두 키 자격 증명 모음에 사용하도록 설정되며 사용하지 않도록 설정할 수 없습니다.

[고객 관리 키에 대한 자세한 정보](#)

암호화 키

☐ 키 URI 입력

☒ Key Vault에서 선택

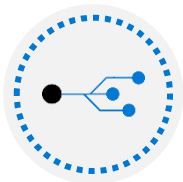
주요 자격 증명 모음 및 키 *

Key Vault: keyvaul987da

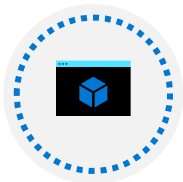
키: Storagekey

[Key Vault 및 키 선택](#)

스토리지 보안 모범 사례 적용



항상 HTTPS를 사용하여 SAS를 만들거나 배포합니다.



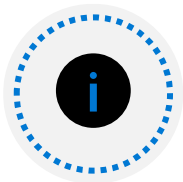
가능한 경우 저장된 액세스 정책을 참조합니다.



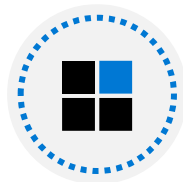
임시 SAS에 단기 만료 시간 사용



스토리지 분석을 사용하여 애플리케이션을 모니터링합니다.



적절한 SAS 시작 시간 선택



액세스할 리소스를 구체적으로 선택



사용량에 따라 계정에 요금이 청구됩니다.



SAS를 사용하여 작성된 데이터의 유효성을 검사합니다.



SAS가 언제나 올바른 선택인 것은 아닙니다.

요약 및 리소스- 스토리지 보안 구성

지식 점검 문제

Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)



[Azure Storage 계정 보안](#)

[공유 액세스 서명을 사용하여 Azure Storage에 대한 액세스 제어\(샌드박스\)](#)

[스토리지 보안 구현](#)

샌드박스는 실습 연습을 나타냅니다.

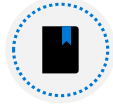
Azure Files 및 파일 동기화 구성



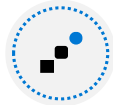
Azure Files 및 파일 동기화 구성 소개



Files와 Blob 비교



파일 공유 관리



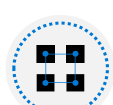
파일 공유 스냅샷 만들기



데모 - 파일 공유



Azure 파일 동기화 구현



Azure 파일 동기화 구성 요소 식별



파일 동기화 배포



도구를 사용하여 스토리지 구성(요약에만 해당)



요약 및 리소스

Files와 Blob 비교

기능	Description	사용 시기
Azure 파일	SMB 인터페이스, 클라이언트 라이브러리, 어디서나 저장된 파일에 액세스할 수 있는 REST 인터페이스	<ul style="list-style-type: none">• 애플리케이션을 클라우드로 리프트 앤 시프트하는 경우• 여러 가상 머신에 공유 데이터를 저장하는 경우• 여러 가상 머신에서 액세스해야 하는 개발 및 디버깅 도구 저장
Azure Blob	클라이언트 라이브러리와 비구조화 데이터(단일 구조 네임스페이스)를 대규모로 블록 Blob에 저장하고 액세스할 수 있게 해주는 REST 인터페이스	<ul style="list-style-type: none">• 스트리밍 및 임의 액세스 시나리오를 지원하는 경우• 어디서나 애플리케이션 데이터에 액세스하는 경우

파일 공유 관리

파일 공유 할당량

Windows – 포트 445가 열려 있는지 확인

Linux – 드라이브 탑재

MacOS – 드라이브 탑재

보안 전송 필요 - SMB 3.0 암호화

연결

Windows Linux macOS

Windows에서 이 Azure 파일 공유에 연결하려면 다음 인증 방법 중 하나를 선택하고 일반 (관리자 권한 아님) PowerShell 터미널에서 다음 PowerShell 명령을 실행하세요.

드라이브 문자

Z

인증 방법

☐ Active Directory

☒ 스토리지 계정 키

i 스토리지 계정 키를 사용하여 공유에 연결하는 것은 관리자 액세스에만 적합합니다. 사용자의 Active Directory ID를 사용하여 Azure 파일 공유 기능을 탑재하는 것이 좋습니다. [자세히 알아보기](#)

```
$connectTestResult = Test-NetConnection -ComputerName  
exampleaccountnametest.file.core.windows.net -Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # 다시 부팅할 때 드라이브가 유지되도록 암호를 저장합니다.  
    cmd.exe /C "cmdkey /add:"exampleaccountnametest.file.core.windows.net"  
/user:"Azure\exampleaccountnametest"  
/pass:""
```

파일 공유 스냅샷 만들기

+ 스냅샷 추가 ↺ 새로 고침 🗑 삭제

이름

만든 날짜

시작자



2020-04-06T03:48:10.0000000Z

2020. 4. 6. 오전 10:48:10

-

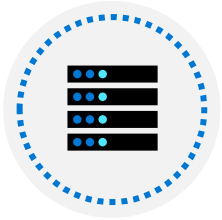
특정 시점의 공유 상태를 캡처하는 증분 스냅샷입니다.

데이터의 읽기 전용복사본입니다.

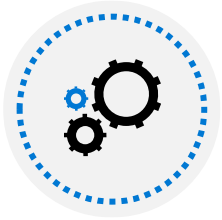
파일 공유 수준의 스냅샷 및 파일 수준에서 복원

- 애플리케이션 오류 및 데이터 손상으로부터 보호
- 실수로 삭제 또는 의도하지 않은 변경 방지
- 일반 백업 목적

데모 - 파일 공유



파일 공유 생성 및 파일 업로드



스냅샷 관리



파일 공유 만들기(PowerShell - 선택 사항)



파일 공유 탑재(PowerShell - 선택 사항)

Azure 파일 동기화 구현

Azure Files에서 조직의 파일 공유를 중앙 집중화하면서 온-프레미스 파일 서버의 유연성과 성능, 호환성은 그대로 유지합니다.

1. 리프트 앤 시프트
2. 지사 백업
3. Backup 및 재해 복구
4. 파일 보관



파일 동기화 구성 요소 식별

스토리지 동기화 서비스는 최상위 리소스입니다.

등록된 서버개체는 서버(또는 클러스터)와 스토리지 동기화 서비스 간의 신뢰 관계를 나타냅니다.

Azure 파일 동기화 에이전트는 다운로드 가능한 패키지로, Windows 서버를 Azure 파일 공유와 동기화할 수 있게 해줍니다.

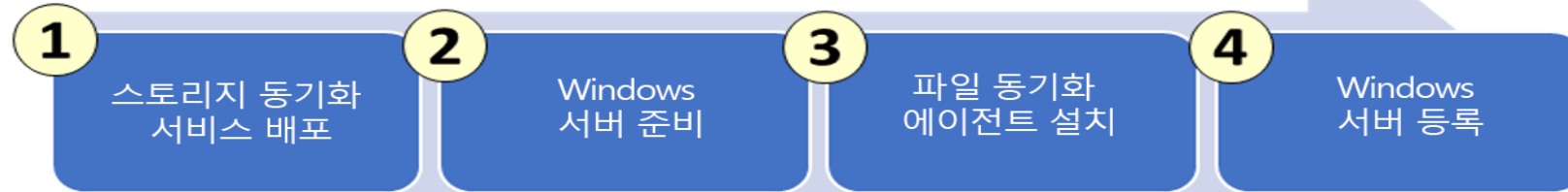
서버 엔드포인트는 등록된 서버의 특정 위치를 나타냅니다 (예: 폴더).

클라우드 엔드포인트는 Azure 파일 공유입니다.

동기화 그룹은 동기화하는 파일을 정의합니다.



파일 동기화 설정



홈 > Azure 파일 동기화 배포

Azure 파일 동기화 배포

* 구독
Visual Studio Enterprise

* 리소스 그룹
ASH

새로 만들기

* 스토리지 동기화 서비스 이름
StorageSync1

* 지역
미국 중남부

리뷰 + 만들기 이전 다음: 태그 >

Microsoft Azure File Sync - Server Registration

Choose a Storage Sync Service

Azure Subscription

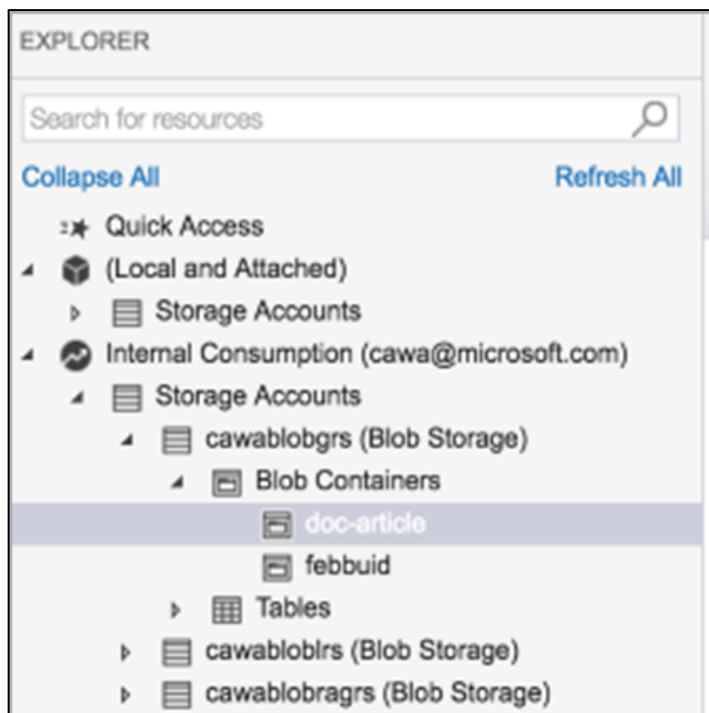
Resource Group

Storage Sync Service

Register

도구를 사용하여 스토리지 구성

Azure Storage Explorer



가져오기 및 내보내기 서비스

가져오기/내보내기 작업 만들기 ...

가져오기/내보내기 작업 만들기

기본 사항 작업 세부 정보 배송 태그 검토 + 만들기

프로젝트 정보

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

구독 * ASC DEMO

리소스 그룹 * 새로 만들기

이름 *

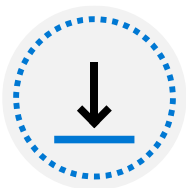
형식 ☒ Azure로 가져오기 ☐ Azure에서 내보내기

대상 Azure 지역 *

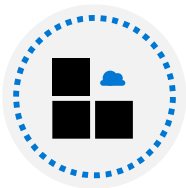
AzCopy

```
azcopy copy [source]
[destination] [flags]
```

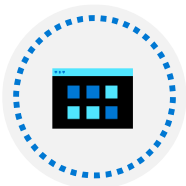
데모 - Storage Explorer(선택 사항)



Storage Explorer 다운로드 및 설치



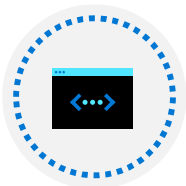
Azure 구독에 연결



Azure Storage 계정 연결

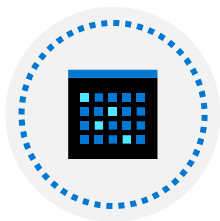


공유하려는 계정에 대한 SAS 연결 문자열 생성



SAS 연결 문자열을 사용하여 스토리지 계정에 연결

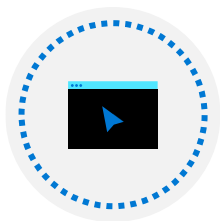
데모 – AzCopy(선택 사항)



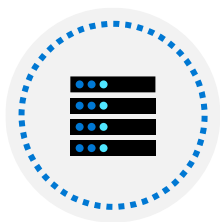
AzCopy 도구 설치



도움말 살펴보기



Blob Storage에서 파일 시스템으로 Blob 다운로드



Azure Blob Storage에 파일 업로드

요약 및 리소스 - Azure Files 및 파일 동기화 구성

지식 점검 문제



Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

[Azure 파일 동기화를 사용하여 온-프레미스 파일 공유 용량 확장](#)

[하이브리드 파일 서버 인프라 구현](#)

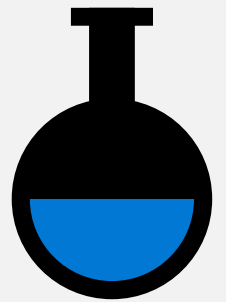
[Azure Storage Explorer를 사용하여 데이터 업로드, 다운로드, 관리\(샌드박스\)](#)

[Azure Import/Export를 사용하여 Azure에서 대량 데이터 내보내기](#)

[명령줄 및 코드로 하나의 컨테이너 또는 스토리지 계정에서 또 다른 컨테이너 또는 스토리지 계정으로 Blob 복사 및 이동\(샌드박스\)](#)

샌드박스는 실습 연습을 나타냅니다.

랩 - Azure 스토리지 관리



랩 07 - Azure Storage 관리

랩 시나리오

현재 온-프레미스 데이터 저장소에 있는 파일을 저장하는 데 Azure Storage를 사용하는 것에 대해 평가해야 합니다. 대부분의 파일에는 자주 액세스하지 않지만 몇 가지 예외가 있습니다. 사용자는 자주 액세스하지 않는 파일을 저렴한 스토리지 계층에 배치하여 스토리지 비용을 최소화하려고 합니다. 또한 네트워크 액세스, 인증, 권한 부여 및 복제를 포함하여 Azure Storage가 제공하는 다양한 보호 메커니즘을 알아볼 계획입니다. 마지막으로 Azure Files 서비스가 온-프레미스 파일 공유를 호스팅하는 데 얼마나 적합한지 확인하고자 합니다.

목표

작업 1:

랩 환경 프로비저닝

작업 2:

Azure 스토리지 계정 만들기 및 구성

작업 3:

Blob 스토리지 관리

작업 4:

Azure 스토리지에 대한 인증 및 권한 부여 관리

작업 5:

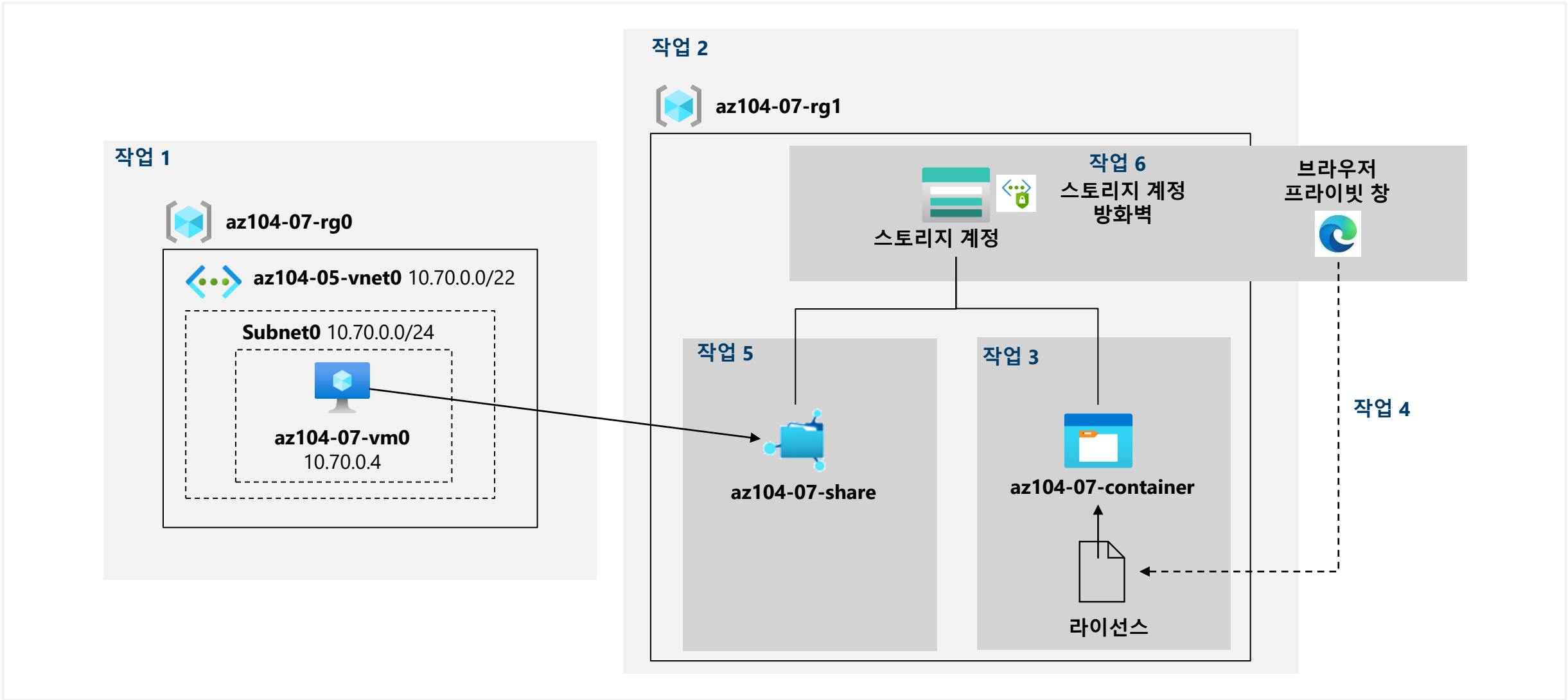
Azure Files 공유 만들기 및 구성

작업 6:

Azure Storage의 네트워크 액세스 관리

다음 슬라이드에서 아키텍처 다이어그램을 확인할 수 있습니다. ➔

랩 07 - 아키텍처 다이어그램



프레젠테이션 종료

