



# 클라우드 스토리지 풀 생성

## StorageGRID 11.5

NetApp  
April 11, 2024

# 목차

클라우드 스토리지 풀 생성 .....	1
S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정 .....	2
C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정 .....	5
Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정 .....	8

# 클라우드 스토리지 풀 생성

클라우드 스토리지 풀을 생성할 때 StorageGRID에서 오브젝트를 저장할 외부 버킷 또는 컨테이너의 이름과 위치, 클라우드 공급자 유형(Amazon S3 또는 Azure Blob Storage) 및 StorageGRID이 외부 버킷 또는 컨테이너에 액세스하는 데 필요한 정보를 지정합니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 클라우드 스토리지 풀 구성에 대한 지침을 검토해야 합니다.
- 클라우드 스토리지 풀에서 참조하는 외부 버킷 또는 컨테이너가 있어야 합니다.
- 버킷이나 컨테이너에 액세스하는 데 필요한 모든 인증 정보가 있어야 합니다.

## 이 작업에 대해

Cloud Storage Pool은 단일 외부 S3 버킷 또는 Azure Blob 스토리지 컨테이너를 지정합니다. StorageGRID는 저장하는 즉시 클라우드 스토리지 풀을 검증하므로, 클라우드 스토리지 풀에 지정된 버킷이나 컨테이너가 존재하고 연결 가능한지 확인해야 합니다.

## 단계

1. ILM \* > \* 스토리지 풀 \* 을 선택합니다.

스토리지 풀 페이지가 나타납니다. 이 페이지에는 스토리지 풀과 클라우드 스토리지 풀의 두 섹션이 있습니다.

Storage Pools

**Storage Pools**

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

**Cloud Storage Pools**

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

No Cloud Storage Pools found.


2. 페이지의 클라우드 스토리지 풀 섹션에서 \* 생성 \* 을 클릭합니다.

Create Cloud Storage Pool 대화상자가 나타납니다.

### Create Cloud Storage Pool

Display Name 

Provider Type 

Bucket or Container 

3. 다음 정보를 입력합니다.

필드에 입력합니다	설명
표시 이름	Cloud Storage Pool과 그 용도를 간략하게 설명하는 이름입니다. ILM 규칙을 구성할 때 쉽게 식별할 수 있는 이름을 사용합니다.
공급자 유형	이 클라우드 스토리지 풀에 사용할 클라우드 공급자: <ul style="list-style-type: none"> <li>• Amazon S3(S3 또는 C2S S3 클라우드 스토리지 풀에 대해 이 옵션 선택)</li> <li>• Azure Blob 저장소               <ul style="list-style-type: none"> <li>◦ 참고: * 공급자 유형을 선택하면 서비스 끝점, 인증 및 서버 검증 섹션이 페이지 하단에 나타납니다.</li> </ul> </li> </ul>
버킷 또는 컨테이너	Cloud Storage Pool용으로 생성한 외부 S3 버킷 또는 Azure 컨테이너의 이름입니다. 여기서 지정하는 이름은 버킷 또는 컨테이너의 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

4. 선택한 공급자 유형에 따라 페이지의 서비스 엔드포인트, 인증 및 서버 검증 섹션을 완료합니다.

- ["S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"](#)
- ["C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"](#)
- ["Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"](#)

## S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정

S3용 Cloud Storage Pool을 생성할 때 Cloud Storage Pool 엔드포인트를 위해 필요한 인증 유형을 선택해야 합니다. 익명 을 지정하거나 액세스 키 ID 및 비밀 액세스 키를 입력할 수 있습니다.

필요한 것

- 클라우드 스토리지 풀에 대한 기본 정보를 입력하고 공급자 유형으로 \* Amazon S3 \* 를 지정해야 합니다.

### Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

#### Service Endpoint

Protocol ⓘ  HTTP  HTTPS

Hostname ⓘ example.com or 0.0.0.0

Port (optional) ⓘ 443

#### Authentication

Authentication Type ⓘ ▼

#### Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel Save

- 액세스 키 인증을 사용하는 경우 외부 S3 버킷의 액세스 키 ID 및 비밀 액세스 키를 알아야 합니다.

단계

1. 서비스 끝점 \* 섹션에서 다음 정보를 제공합니다.
  - a. 클라우드 스토리지 풀에 연결할 때 사용할 프로토콜을 선택합니다.  
기본 프로토콜은 HTTPS입니다.
  - b. 클라우드 스토리지 풀의 서버 호스트 이름 또는 IP 주소를 입력합니다.

예를 들면 다음과 같습니다.

s3-aws-region.amazonaws.com



이 필드에 버킷 이름을 포함하지 마십시오. 버킷 이름은 \* 버킷 또는 컨테이너 \* 필드에 포함합니다.

a. 필요에 따라 클라우드 스토리지 풀에 연결할 때 사용할 포트를 지정합니다.

기본 포트(HTTPS의 경우 포트 443, HTTP의 경우 포트 80)를 사용하려면 이 필드를 비워 둡니다.

2. Authentication \* 섹션에서 Cloud Storage Pool 엔드포인트에 필요한 인증 유형을 선택합니다.

옵션을 선택합니다	설명
액세스 키	클라우드 스토리지 풀 버킷을 액세스하려면 액세스 키 ID와 비밀 액세스 키가 필요합니다.
익명	모든 사용자가 Cloud Storage Pool 버킷에 액세스할 수 있습니다. 액세스 키 ID와 비밀 액세스 키는 필요하지 않습니다.
CAP(C2S 액세스 포털)	C2S S3에만 사용됩니다. 로 이동합니다 <a href="#">"C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"</a> .

3. Access Key를 선택한 경우 다음 정보를 입력합니다.

옵션을 선택합니다	설명
액세스 키 ID	외부 버킷을 소유하는 계정의 액세스 키 ID입니다.
비밀 액세스 키	연결된 비밀 액세스 키.

4. 서버 확인 섹션에서 클라우드 스토리지 풀에 대한 TLS 연결에 대한 인증서 유효성을 검사하는 데 사용할 방법을 선택합니다.

옵션을 선택합니다	설명
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. Select New * 를 클릭하고 PEM 인코딩된 CA 인증서를 업로드합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다.

5. 저장 \* 을 클릭합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 버킷과 서비스 끝점이 있는지, 그리고 지정한 자격 증명을 사용하여 도달할 수 있는지 검증합니다.
- 버킷에 마커 파일을 쓰면 버킷이 클라우드 스토리지 풀임을 식별할 수 있습니다. 이름이 인 이 파일은 제거하지 마십시오 x-ntap-sgws-cloud-pool-uuid.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 버킷이 이미 없는 경우 오류가 보고될 수 있습니다.

## ! Error

### 422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

클라우드 스토리지 풀 문제 해결 지침을 참조하여 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

관련 정보

["클라우드 스토리지 풀 문제 해결"](#)

## C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정

C2S(Commercial Cloud Services) S3 서비스를 클라우드 스토리지 풀로 사용하려면 C2S 액세스 포털(CAP)을 인증 유형으로 구성해야 합니다. 그러면 StorageGRID가 C2S 계정의 S3 버킷을 액세스하기 위한 임시 자격 증명을 요청할 수 있습니다.

필요한 것

- 서비스 엔드포인트를 포함하여 Amazon S3 Cloud Storage Pool에 대한 기본 정보를 입력해야 합니다.
- C2S 계정에 할당된 모든 필수 및 선택적 API 매개 변수를 포함하여 StorageGRID가 CAP 서버에서 임시 자격 증명을 얻는 데 사용할 전체 URL을 알고 있어야 합니다.
- 적절한 정부 인증 기관(CA)에서 발급한 서버 CA 인증서가 있어야 합니다. StorageGRID는 이 인증서를 사용하여 CAP 서버의 ID를 확인합니다. 서버 CA 인증서는 PEM 인코딩을 사용해야 합니다.
- 적절한 정부 인증 기관(CA)에서 발급한 클라이언트 인증서가 있어야 합니다. StorageGRID는 이 인증서를 사용하여 CAP 서버에 대한 자체 ID를 만듭니다. 클라이언트 인증서는 PEM 인코딩을 사용해야 하며 C2S 계정에 대한 액세스 권한이 부여되어야 합니다.
- 클라이언트 인증서에 대해 PEM 인코딩된 개인 키가 있어야 합니다.
- 클라이언트 인증서의 개인 키가 암호화된 경우 암호를 해독하기 위한 암호가 있어야 합니다.

단계

1. 인증 \* 섹션의 \* 인증 유형 \* 드롭다운에서 \* CAP(C2S 액세스 포털) \* 를 선택합니다.

CAP C2S 인증 필드가 나타납니다.

## Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

### Service Endpoint

Protocol ⓘ  HTTP  HTTPS

Hostname ⓘ s3-aws-region.amazonaws.com

Port (optional) ⓘ 443

### Authentication

Authentication Type ⓘ CAP (C2S Access Portal) ▼

Temporary Credentials URL ⓘ https://example.com/CAP/api/v1/credentials?agency=my

Server CA Certificate ⓘ Select New

Client Certificate ⓘ Select New

Client Private Key ⓘ Select New

Client Private Key Passphrase (optional) ⓘ

### Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save



2. 다음 정보를 제공합니다.

- a. 임시 자격 증명 URL \* 의 경우 StorageGRID가 C2S 계정에 할당된 모든 필수 및 선택적 API 매개 변수를 포함하여 CAP 서버에서 임시 자격 증명을 얻는 데 사용할 전체 URL을 입력합니다.
- b. 서버 CA 인증서 \* 의 경우 \* 새로 선택 \* 을 클릭하고 StorageGRID가 CAP 서버를 확인하는 데 사용할 PEM 인코딩된 CA 인증서를 업로드합니다.
- c. 클라이언트 인증서 \* 의 경우 \* 새 항목 선택 \* 을 클릭하고 StorageGRID가 CAP 서버에 자신을 식별하는 데 사용할 PEM 인코딩된 인증서를 업로드합니다.
- d. 클라이언트 개인 키 \* 의 경우 \* 새 항목 선택 \* 을 클릭하고 클라이언트 인증서에 대한 PEM 인코딩 개인 키를 업로드합니다.

개인 키가 암호화된 경우 기존 형식을 사용해야 합니다. (PKCS #8 암호화된 형식은 지원되지 않습니다.)

- e. 클라이언트 개인 키가 암호화된 경우 클라이언트 개인 키의 암호를 해독하기 위한 암호를 입력합니다. 그렇지 않으면 \* Client Private Key Passphrase \* 필드를 비워 둡니다.

3. 서버 확인 섹션에서 다음 정보를 제공합니다.

- a. 인증서 유효성 검사 \* 의 경우 \* 사용자 지정 CA 인증서 사용 \* 을 선택합니다.
- b. Select New \* 를 클릭하고 PEM 인코딩된 CA 인증서를 업로드합니다.

4. 저장 \* 을 클릭합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 버킷과 서비스 끝점이 있는지, 그리고 지정한 자격 증명을 사용하여 도달할 수 있는지 검증합니다.
- 버킷에 마커 파일을 쓰면 버킷이 클라우드 스토리지 풀임을 식별할 수 있습니다. 이름이 인 이 파일은 제거하지 마십시오 x-ntap-sgws-cloud-pool-uuid.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 버킷이 이미 없는 경우 오류가 보고될 수 있습니다.

**! Error**

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

클라우드 스토리지 풀 문제 해결 지침을 참조하여 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

관련 정보

["클라우드 스토리지 풀 문제 해결"](#)

# Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정

Azure Blob 스토리지용 Cloud Storage Pool을 생성할 때 StorageGRID에서 개체를 저장하는 데 사용할 외부 컨테이너의 계정 이름 및 계정 키를 지정해야 합니다.

## 필요한 것

- 클라우드 스토리지 풀에 대한 기본 정보를 입력하고 공급자 유형으로 \* Azure Blob Storage \* 를 지정해야 합니다. \* 공유 키 \* 가 \* 인증 유형 \* 필드에 나타납니다.

### Create Cloud Storage Pool

Display Name

Provider Type

Bucket or Container

---

### Service Endpoint

URI

---

### Authentication

Authentication Type

Account Name

Account Key

---

### Server Verification

Certificate Validation

- 클라우드 스토리지 풀에 사용되는 Blob 스토리지 컨테이너에 액세스하는 데 사용되는 URI(Uniform Resource Identifier)를 알아야 합니다.
- 스토리지 계정의 이름과 암호 키를 알고 있어야 합니다. Azure 포털을 사용하여 이러한 값을 찾을 수 있습니다.

## 단계

1. Service Endpoint \* 섹션에서 Cloud Storage Pool에 사용되는 Blob 저장소 컨테이너에 액세스하는 데 사용되는 URI(Uniform Resource Identifier)를 입력합니다.

다음 형식 중 하나로 URI를 지정합니다.

- `https://host:port`
- `http://host:port`

포트를 지정하지 않으면 기본적으로 포트 443이 HTTPS URI에 사용되고 포트 80은 HTTP URI에 사용됩니다. Azure Blob 저장소 컨테이너용 + \* 예제 URI \*: `https://myaccount.blob.core.windows.net`

2. 인증 \* 섹션에서 다음 정보를 제공합니다.

- a. 계정 이름 \* 에 대해 외부 서비스 컨테이너를 소유한 Blob 저장소 계정의 이름을 입력합니다.
- b. 계정 키 \* 의 경우 Blob 저장소 계정의 암호 키를 입력합니다.



Azure 끝점의 경우 공유 키 인증을 사용해야 합니다.

3. 서버 검증 \* 섹션에서 클라우드 스토리지 풀에 대한 TLS 연결에 대한 인증서 유효성을 검사하는 데 사용할 방법을 선택합니다.

옵션을 선택합니다	설명
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. Select New * 를 클릭하고 PEM 인코딩된 인증서를 업로드합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다.

4. 저장 \* 을 클릭합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 컨테이너와 URI가 있는지, 지정한 자격 증명을 사용하여 해당 컨테이너에 연결할 수 있는지 확인합니다.
- 컨테이너에 마커 파일을 기록하여 클라우드 스토리지 풀로 식별합니다. 이름이 인 이 파일은 제거하지 마십시오 `x-ntap-sgws-cloud-pool-uuid`.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 컨테이너가 이미 없는 경우 오류가 보고될 수 있습니다.

클라우드 스토리지 풀 문제 해결 지침을 참조하여 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

## 관련 정보

["클라우드 스토리지 풀 문제 해결"](#)

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 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.