클라우드 스토리지 풀 생성

StorageGRID 11.5

NetApp
April 11, 2024

목차

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.

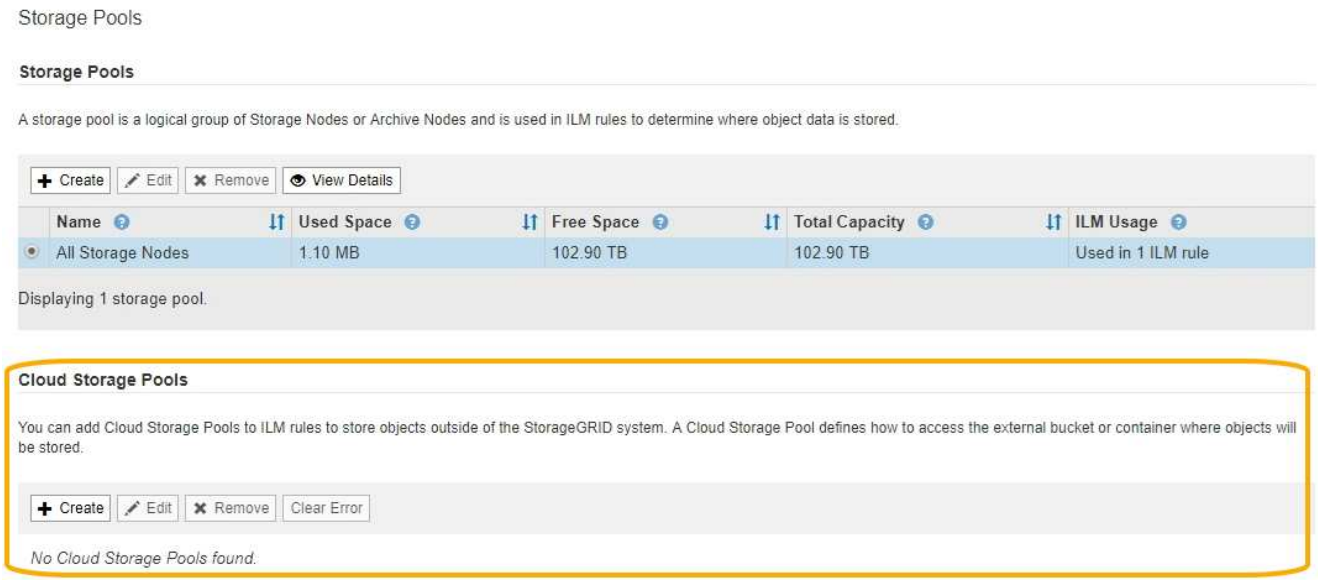
이 작업에 대해

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.



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

   Create Cloud Storage Pool 대화상자가 나타납니다.

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: • Amazon S3(S3 또는 C2S S3 클라우드 스토리지 풀에 대해 이 옵션 선택) • Azure Blob 저장소 ◦ 참고: * 공급자 유형을 선택하면 서비스 끝점, 인증 및 서버 검증 섹션이 페이지 하단에 나타납니다.
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.

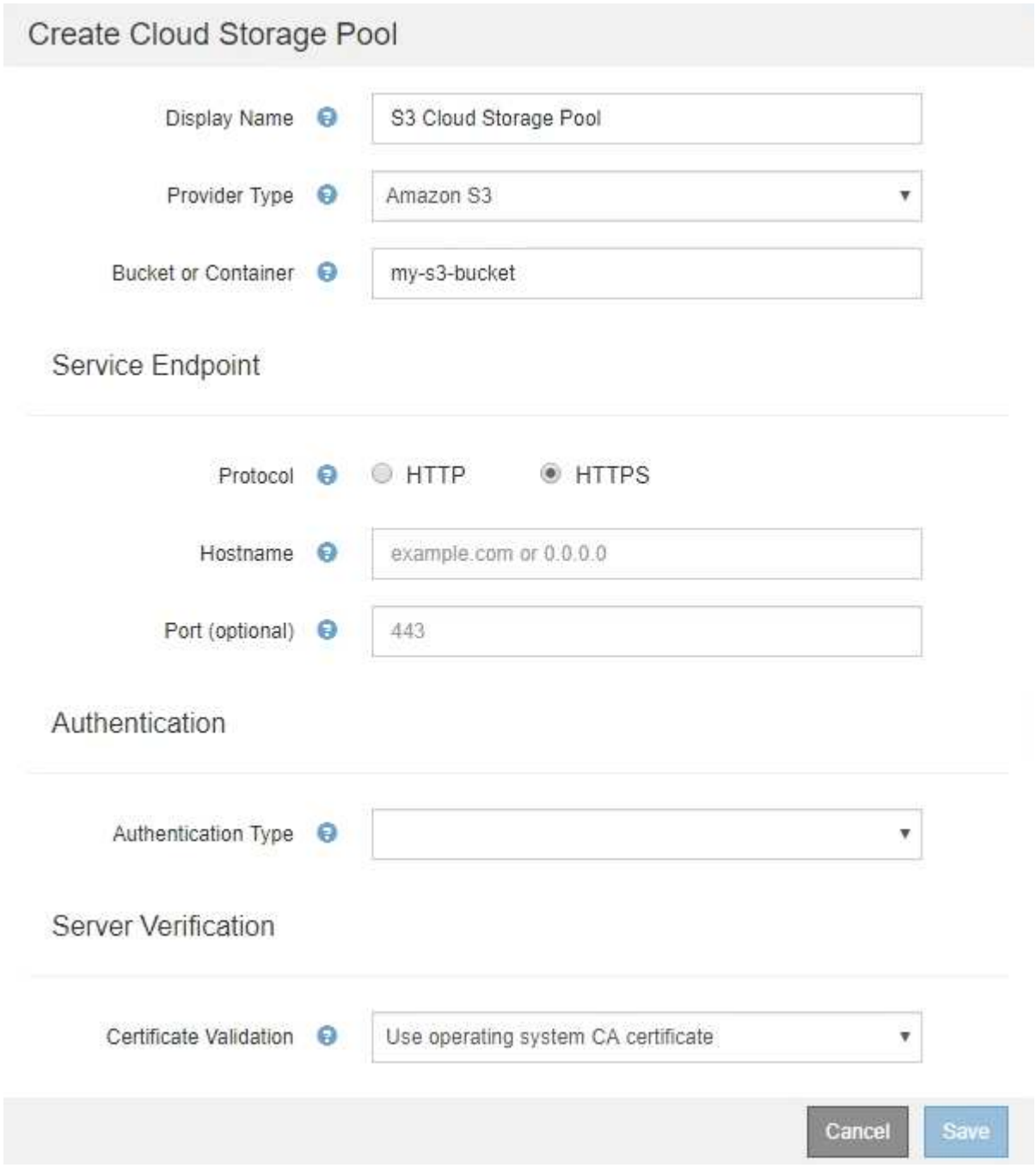
4. 선택한 공급자 유형에 따라 페이지의 서비스 엔드포인트, 인증 및 서버 검증 섹션을 완료합니다.
   - "S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"
   - "C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"
   - "Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정"

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.



- 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 "C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정".

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.

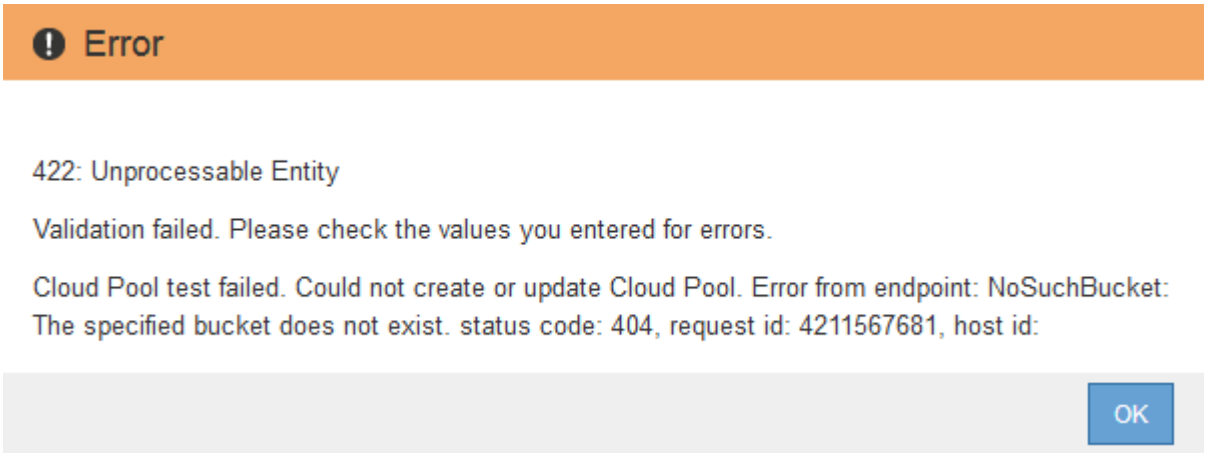
옵션을 선택합니다	설명
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. Select New * 를 클릭하고 PEM 인코딩된 CA 인증서를 업로드합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다.

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.



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.

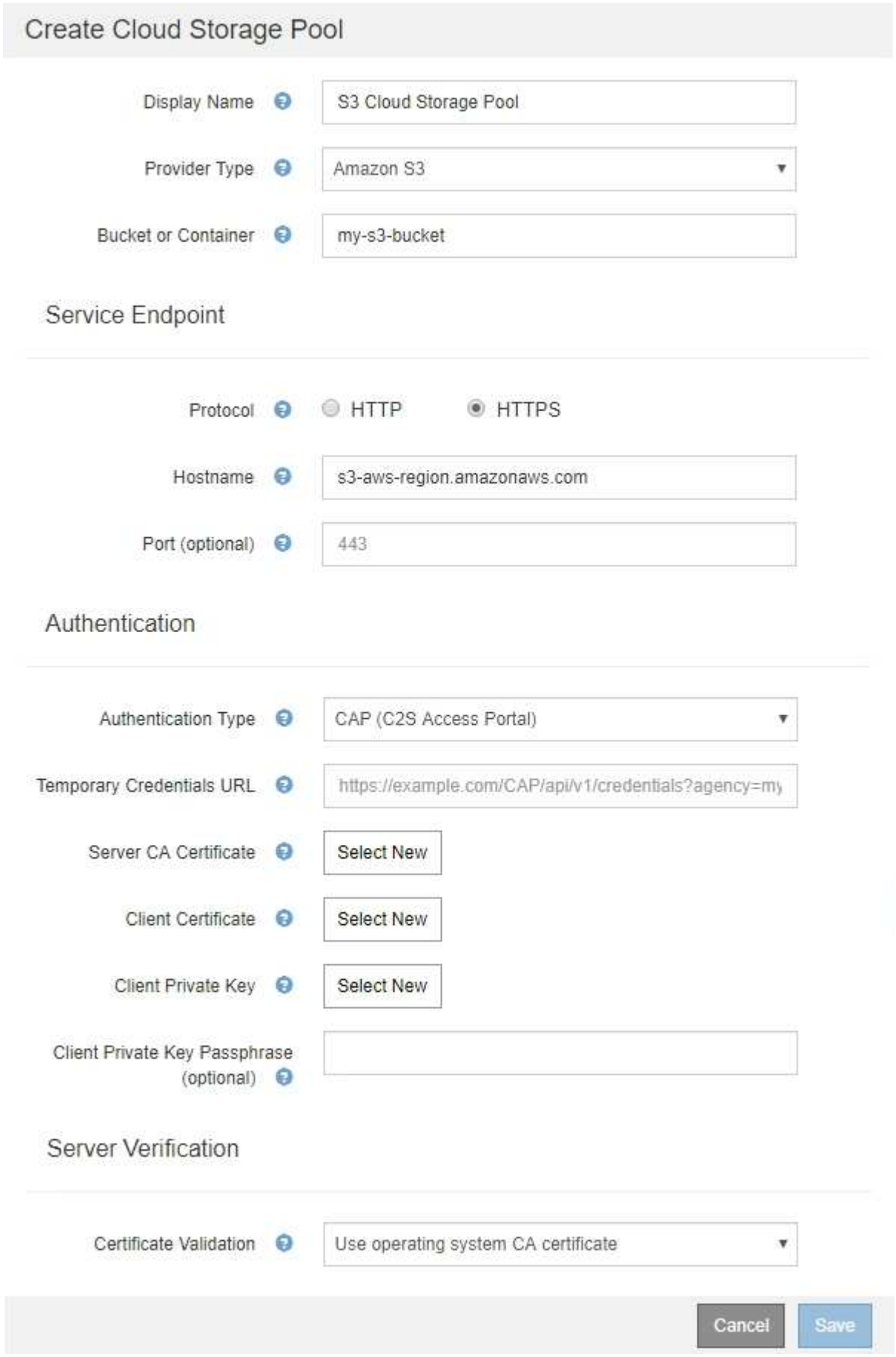
필요한 것

- 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.



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.

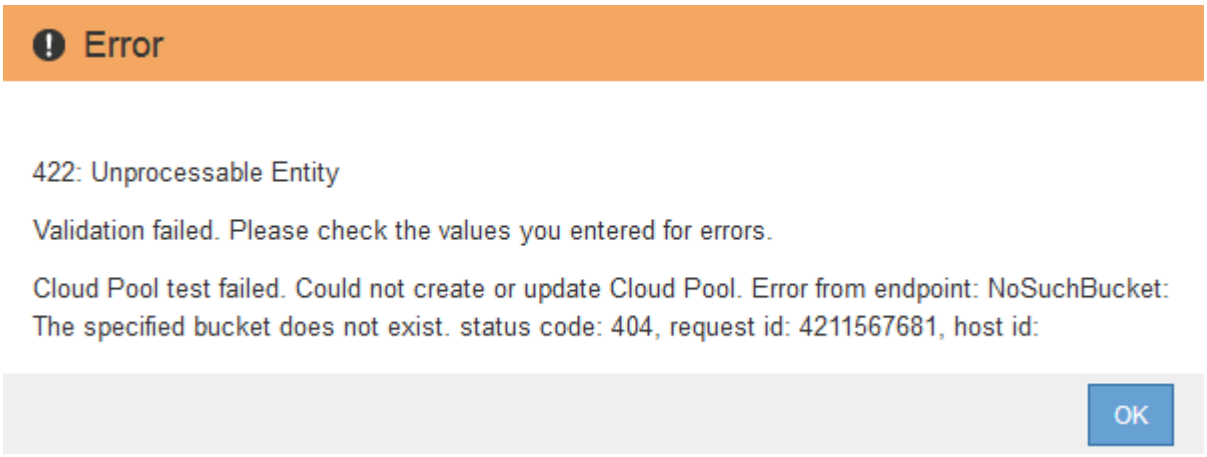
   b. Select New * 를 클릭하고 PEM 인코딩된 CA 인증서를 업로드합니다.

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.



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

관련 정보

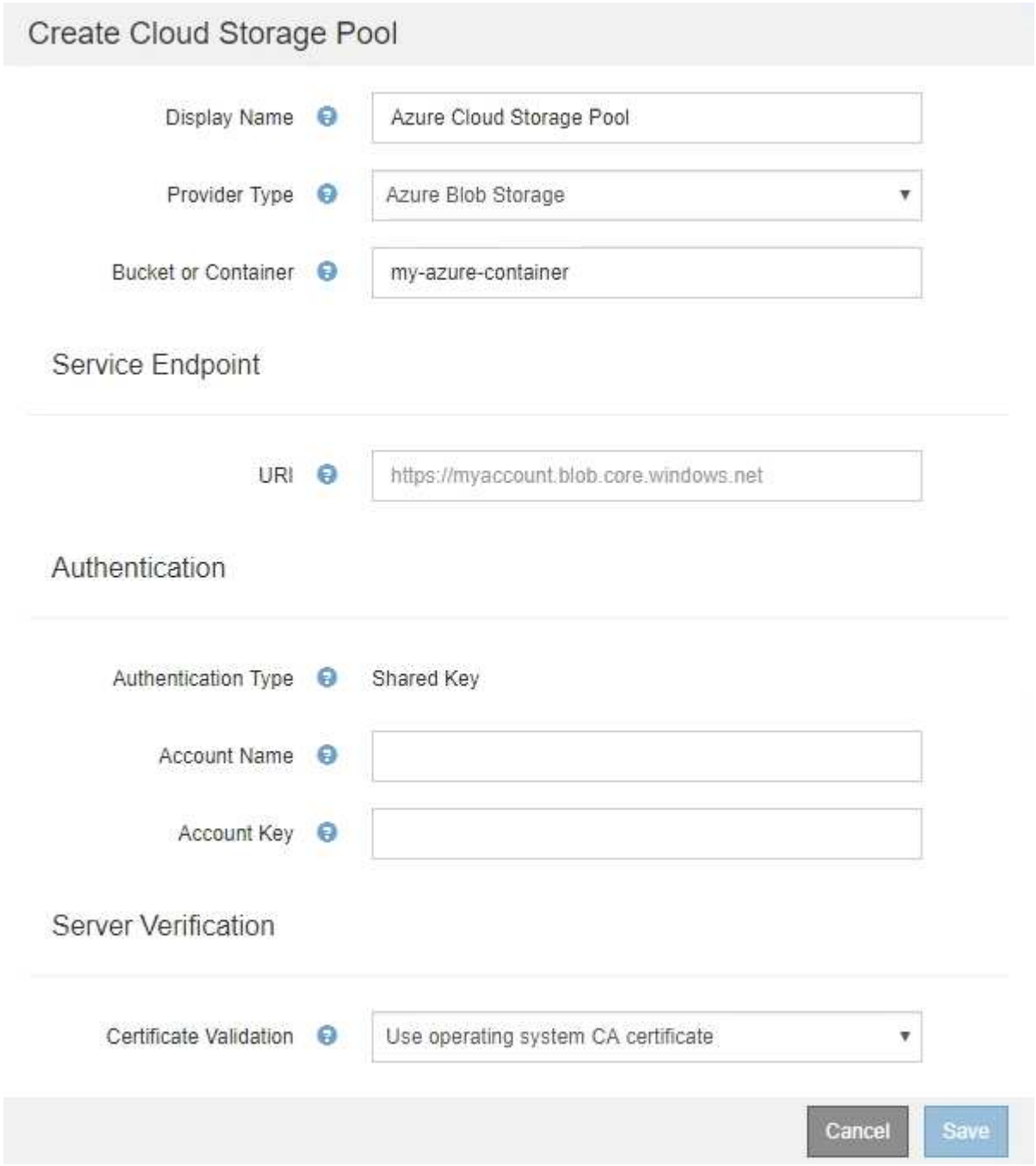
"클라우드 스토리지 풀 문제 해결"

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.



- 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"