



S3 액세스 키를 관리합니다 StorageGRID 11.7

NetApp
April 12, 2024

목차

S3 액세스 키를 관리합니다.....	1
S3 액세스 키 관리: 개요.....	1
자체 S3 액세스 키를 생성합니다.....	1
S3 액세스 키를 봅니다.....	2
자체 S3 액세스 키를 삭제합니다.....	3
다른 사용자의 S3 액세스 키를 생성합니다.....	3
다른 사용자의 S3 액세스 키를 봅니다.....	4
다른 사용자의 S3 액세스 키를 삭제합니다.....	5

S3 액세스 키를 관리합니다

S3 액세스 키 관리: 개요

S3 테넌트 계정의 각 사용자는 StorageGRID 시스템에 오브젝트를 저장하고 검색하기 위한 액세스 키가 있어야 합니다. 액세스 키는 액세스 키 ID와 비밀 액세스 키로 구성됩니다.

S3 액세스 키는 다음과 같이 관리할 수 있습니다.

- 자신의 S3 자격 증명 관리 * 권한이 있는 사용자는 자신의 S3 액세스 키를 생성하거나 제거할 수 있습니다.
- 루트 액세스 * 권한이 있는 사용자는 S3 루트 계정 및 다른 모든 사용자의 액세스 키를 관리할 수 있습니다. 루트 액세스 키는 버킷 정책에 의해 명시적으로 비활성화되지 않는 한 테넌트의 모든 버킷과 객체에 대한 전체 액세스를 제공합니다.

StorageGRID는 서명 버전 2 및 서명 버전 4 인증을 지원합니다. 버킷 정책에 의해 명시적으로 활성화되지 않은 경우 교차 계정 액세스가 허용되지 않습니다.

자체 S3 액세스 키를 생성합니다

S3 테넌트를 사용 중이며 적절한 권한이 있는 경우 자체 S3 액세스 키를 생성할 수 있습니다. 버킷과 오브젝트에 액세스하려면 액세스 키가 있어야 합니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 이 있는 사용자 그룹에 속해 있습니다 ["자신의 S3 자격 증명 또는 루트 액세스 권한을 관리합니다"](#).

이 작업에 대해

하나 이상의 S3 액세스 키를 생성하여 테넌트 계정의 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해 필요한 것보다 더 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료하려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 특정 기간에 대한 액세스를 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출되었을 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.
- 환경의 보안 위험이 낮으며 정기적으로 새 키를 만들 필요가 없는 경우 키에 대한 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.



계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

2. Create key * 를 선택합니다.
3. 다음 중 하나를 수행합니다.
 - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
 - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.



만료 날짜는 현재 날짜로부터 최대 5년일 수 있습니다. 만료 시간은 현재 시간에서 최소 1분이 될 수 있습니다.

4. Create access key * 를 선택합니다.

액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

5. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.



이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.

6. 마침 * 을 선택합니다.

새 키가 내 액세스 키 페이지에 나열됩니다.

7. 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우, 필요에 따라 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제합니다. 을 참조하십시오 ["API를 사용하여 S3 액세스 키의 클론을 생성합니다"](#).

S3 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 S3 액세스 키 목록을 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬할 수 있으므로 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 할 수 있습니다 ["새 키를 만듭니다"](#) 또는 ["키를 삭제합니다"](#) 더 이상 을(를) 사용하지 않습니다.



계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 사용자는 자신의 S3 자격 증명 관리 가 있는 사용자 그룹에 속해 있습니다 ["권한"](#).

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.
2. 내 액세스 키 페이지에서 * 만료 시간 * 또는 * 액세스 키 ID * 를 기준으로 기존 액세스 키를 정렬합니다.
3. 필요에 따라 새 키를 만들거나 더 이상 사용하지 않는 키를 삭제합니다.

기존 키가 만료되기 전에 새 키를 만들면 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

만료된 키는 자동으로 제거됩니다.

자체 S3 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 자신의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 자신의 S3 자격 증명 관리 권한이 있습니다. 을 참조하십시오 "[테넌트 관리 권한](#)".



계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.
2. 내 액세스 키 페이지에서 제거할 각 액세스 키에 대한 확인란을 선택합니다.
3. Delete key * 를 선택합니다.
4. 확인 대화 상자에서 * 키 삭제 * 를 선택합니다.

페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

다른 사용자의 S3 액세스 키를 생성합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 버킷 및 오브젝트에 액세스해야 하는 애플리케이션 같은 다른 사용자를 위한 S3 액세스 키를 생성할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 "[지원되는 웹 브라우저](#)".
- 이 있는 사용자 그룹에 속해 있습니다 "[루트 액세스 권한](#)".

이 작업에 대해

하나 이상의 다른 사용자를 위한 S3 액세스 키를 생성하여 해당 테넌트 계정에 대한 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해 사용자 요구 사항보다 더 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료되려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 사용자의 액세스를 특정 기간으로 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출될 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.

- 환경의 보안 위험이 낮으며 정기적으로 새 키를 만들 필요가 없는 경우 키에 대한 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.



사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에게 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. S3 액세스 키를 관리할 사용자를 선택합니다.

사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택한 다음 * 키 만들기 * 를 선택합니다.
4. 다음 중 하나를 수행합니다.
 - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
 - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.



만료 날짜는 현재 날짜로부터 최대 5년일 수 있습니다. 만료 시간은 현재 시간에서 최소 1분이 될 수 있습니다.

5. Create access key * 를 선택합니다.

액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

6. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.



이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.

7. 마침 * 을 선택합니다.

새 키가 사용자 세부 정보 페이지의 액세스 키 탭에 나열됩니다.

8. 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우, 필요에 따라 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제합니다. 을 참조하십시오 "[API를 사용하여 S3 액세스 키의 클론을 생성합니다](#)".

다른 사용자의 S3 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬하면 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 새 키를 생성하고 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 루트 액세스 권한이 있습니다.



사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에게 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 사용자 페이지에서 S3 액세스 키를 보려는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 * 액세스 키 * 를 선택합니다.
4. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.
5. 필요에 따라 새 키를 생성하고 에서 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

기존 키가 만료되기 전에 새 키를 만들면 사용자는 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

만료된 키는 자동으로 제거됩니다.

관련 정보

["다른 사용자의 S3 액세스 키를 생성합니다"](#)

["다른 사용자의 S3 액세스 키를 삭제합니다"](#)

다른 사용자의 S3 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 루트 액세스 권한이 있습니다. 을 참조하십시오 ["테넌트 관리 권한"](#).



사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에게 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 사용자 페이지에서 관리할 S3 액세스 키가 있는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 * 액세스 키 * 를 선택한 다음 삭제할 각 액세스 키에 대한 확인란을 선택합니다.

4. Actions * > * Delete Selected key * 를 선택합니다.

5. 확인 대화 상자에서 * 키 삭제 * 를 선택합니다.

페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

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.