NAS 데이터에 S3 클라이언트 액세스 제공

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/s3-multiprotocol/index.html on April 24, 2024. Always check docs.netapp.com for the latest.

목차

NAS 데이터에 S3 클라이언트 액세스 제공

S3 멀티 프로토콜 개요

ONTAP 9.12.1부터는 S3 프로토콜을 실행하는 클라이언트가 다시 포맷하지 않고 NFS 및 SMB 프로토콜을 사용하는 클라이언트에 제공되는 동일한 데이터에 액세스할 수 있도록 설정할 수 있습니다. 이 기능을 사용하면 NAS 클라이언트에서 NAS 데이터를 계속 처리하는 동시에 S3 애플리케이션(예: 데이터 마이닝 및 인공 지능)을 실행하는 S3 클라이언트에 오브젝트 데이터를 제공할 수 있습니다.

S3 멀티 프로토콜 기능은 다음과 같은 두 가지 사용 사례를 해결합니다.

1. S3 클라이언트를 사용하여 기존 NAS 데이터에 액세스

   기존 데이터가 기존 NAS 클라이언트(NFS 또는 SMB)를 사용하여 생성되었고 NAS 볼륨(FlexVol 또는 FlexGroup 볼륨)에 있는 경우, 이제 S3 클라이언트에서 분석 툴을 사용하여 이 데이터에 액세스할 수 있습니다.

2. NAS 및 S3 프로토콜을 모두 사용하여 I/O를 수행할 수 있는 최신 클라이언트를 위한 백엔드 스토리지

   이제 NAS 및 S3 프로토콜을 모두 사용하여 동일한 데이터를 읽고 쓸 수 있는 Spark 및 Kafka와 같은 애플리케이션에 통합 액세스를 제공할 수 있습니다.

S3 멀티 프로토콜의 작동 방식

ONTAP 멀티 프로토콜을 사용하면 동일한 데이터 세트를 파일 계층으로 또는 버킷의 객체로 제공할 수 있습니다. 이를 위해 ONTAP는 S3 클라이언트가 S3 오브젝트 요청을 사용하여 NAS 스토리지에 파일을 생성, 읽기, 삭제 및 열거할 수 있도록 "S3 NAS 버킷"을 생성합니다. 이 매핑은 NAS 보안 구성, 파일 및 디렉터리 액세스 권한 감시 및 필요에 따라 보안 감사 추적에 대한 쓰기 작업을 따릅니다.

이 매핑은 지정된 NAS 디렉토리 계층을 S3 버킷으로 제공하여 수행됩니다. 디렉토리 계층의 각 파일은 이름이 매핑된 디렉토리에서 상대적으로 아래로 내려가는 S3 오브젝트로 표시되며 디렉토리 경계는 슬래시 문자('/')로 표시됩니다.

일반 ONTAP 정의 S3 사용자는 NAS 디렉토리에 매핑되는 버킷에 정의된 버킷 정책에 따라 이 스토리지에 액세스할 수 있습니다. 이를 위해서는 S3 사용자와 SMB/NFS 사용자 간에 매핑을 정의해야 합니다. SMB/NFS 사용자의 자격 증명은 NAS 권한 확인에 사용되며 이러한 액세스로 인해 발생하는 모든 감사 레코드에 포함됩니다.

SMB 또는 NFS 클라이언트가 파일을 생성하면 파일이 디렉토리에 즉시 배치되므로 데이터가 쓰기 전에 클라이언트에 표시됩니다. S3 클라이언트는 모든 데이터가 기록될 때까지 새 오브젝트가 네임스페이스에 표시되지 않는 다른 의미를 기대합니다. S3를 NAS 스토리지에 매핑하는 방식은 S3 의미를 사용하여 파일을 생성하므로 S3 생성 명령이 완료될 때까지 파일을 외부적으로 볼 수 없습니다.

S3 NAS 버킷 용 데이터 보호

S3 NAS “버킷”은 S3 클라이언트용 NAS 데이터의 단순한 매핑이며 표준 S3 버킷이 아닙니다. 따라서 NetApp S3 SnapMirror 기능을 사용하여 S3 NAS 버킷을 보호할 필요가 없습니다. 대신 비동기식 SnapMirror 볼륨 복제를 사용하여 S3 NAS 버킷을 포함하는 볼륨을 보호할 수 있습니다. SnapMirror Synchronous 및 SVM 재해 복구는 지원되지 않습니다.

ONTAP 9.14.1부터, MetroCluster IP 및 FC 구성을 위한 미러링된 애그리게이트 및 미러링되지 않은

애그리게이트에서 S3 NAS 버킷이 지원됩니다.

에 대해 자세히 알아보십시오 "비동기식 SnapMirror입니다".

S3 NAS 버킷에 대한 감사

S3 NAS 버킷은 기존의 S3 버킷이 아니므로 액세스 감사를 위해 S3 감사를 구성할 수 없습니다. 에 대해 자세히 알아보십시오 "S3 감사".

그럼에도 불구하고 S3 NAS 버킷에 매핑된 NAS 파일 및 디렉토리는 기존의 ONTAP 감사 절차를 사용하여 액세스 이벤트에 대한 감사를 수행할 수 있습니다. 따라서 S3 작업은 다음과 같은 예외를 제외하고 NAS 감사 이벤트를 트리거할 수 있습니다.

- S3 정책 구성(그룹 또는 버킷 정책)에 의해 S3 클라이언트 액세스가 거부되면 이벤트에 대한 NAS 감사가 시작되지 않습니다. 이는 SVM 감사 점검을 수행하기 전에 S3 권한을 확인하기 때문입니다.
- S3 GET 요청의 타겟 파일이 0 크기인 경우 0개의 콘텐츠가 GET 요청으로 반환되고 읽기 액세스가 기록되지 않습니다.
- S3 GET 요청의 타겟 파일이 사용자에게 통과 권한이 없는 폴더에 있는 경우 액세스 시도가 실패하고 이벤트가 기록되지 않습니다.

에 대해 자세히 알아보십시오 "SVM에서 NAS 이벤트 감사".

S3 및 NAS 상호 운용성

ONTAP S3 NAS 버킷은 여기에 나열된 기능을 제외한 표준 NAS 및 S3 기능을 지원합니다.

NAS 기능은 현재 **S3 NAS** 버킷에서 지원되지 않습니다

FabricPool 용량 계층입니다

S3 NAS 버킷은 FabricPool의 용량 계층으로 구성할 수 없습니다.

S3 기능은 현재 **S3 NAS** 버킷에서 지원되지 않습니다

AWS 사용자 메타데이터

- S3 사용자 메타데이터의 일부로 수신된 키 값 쌍은 현재 릴리즈의 오브젝트 데이터와 함께 디스크에 저장되지 않습니다.
- 접두사 "x-amz-meta"가 있는 요청 헤더는 무시됩니다.

AWS 태그

- Put 객체와 Multitpart initiate 요청에서 접두사 "x-amz-tagging"이 있는 헤더는 무시됩니다.
- 기존 파일의 태그 업데이트 요청(예: "tagging query-string"으로 PUT, GET 및 Delete 요청)은 오류로 거부됩니다.

버전 관리

버킷 매핑 구성에서는 버전 관리를 지정할 수 없습니다.

- null이 아닌 버전 사양(versionId=xyz 쿼리 문자열)이 포함된 요청은 오류 응답을 받습니다.
- 버킷의 버전 관리 상태에 영향을 주는 요청은 오류와 함께 거부됩니다.

다중 파트 작업

다음 작업은 지원되지 않습니다.

- AbortMultipartUpload 를 클릭합니다
- CompleteMultipartUpload를 클릭합니다
- CreateMultptUpload 를 클릭합니다
- ListMultipartUpload 를 클릭합니다

S3 클라이언트 액세스를 위한 NAS 데이터 요구사항

S3 액세스를 위해 NAS 파일 및 디렉토리를 매핑할 때 몇 가지 고유한 비호환성이 있다는 것을 이해하는 것이 중요합니다. S3 NAS 버킷을 사용하여 NAS 파일 계층을 서비스하기 전에 NAS 파일 계층을 조정해야 할 수 있습니다.

S3 NAS 버킷은 S3 버킷 구문을 사용하여 해당 디렉토리를 매핑함으로써 NAS 디렉토리에 대한 S3 액세스를 제공하며 디렉토리 트리의 파일은 오브젝트로 표시됩니다. 오브젝트 이름은 S3 버킷 구성에 지정된 디렉토리를 기준으로 파일의 슬래시로 구분된 경로 이름입니다.

이 매핑에서는 S3 NAS 버킷을 사용하여 파일 및 디렉토리를 제공할 경우 다음과 같은 몇 가지 요구사항이 발생합니다.

- S3 이름은 1024바이트로 제한되므로 S3를 사용하면 경로 이름이 더 긴 파일에 액세스할 수 없습니다.
- 파일 및 디렉터리 이름은 255자로 제한되므로 개체 이름은 255자 이하의 연속된 비슬래시('/') 문자를 사용할 수 없습니다
- 백슬래시('\') 문자로 구분된 SMB 경로 이름은 S3에 슬래시('/') 문자를 포함하는 객체 이름으로 표시됩니다.
- 매핑된 NAS 디렉토리 트리에는 일부 합법적인 S3 오브젝트 이름 쌍이 공존할 수 없습니다. 예를 들어, "part1/Part2"와 "part1/Part2/Part3"이라는 합법적인 S3 개체 이름은 NAS 디렉터리 트리에 동시에 존재할 수 없는 파일에 매핑됩니다. "part1/Part2"는 이름의 파일과 다른 디렉토리에 있습니다.
  - "part1/Part2"가 기존 파일인 경우 "part1/Part2/Part3"의 S3 생성이 실패합니다.
  - "part1/Part2/Part3"이 기존 파일인 경우 "part1/Part2"의 S3 생성 또는 삭제가 실패합니다.
  - 기존 오브젝트의 이름과 일치하는 S3 오브젝트 생성은 NAS에 있지만 정확히 일치해야 하는 기존 오브젝트(버전이 지정되지 않은 버킷)를 대체합니다. 위의 예제에서는 이름이 충돌하는 동안 이름이 일치하지 않으므로 기존 개체를 제거하지 않습니다.

오브젝트 저장소는 매우 많은 임의 이름을 지원하도록 설계되었지만 하나의 디렉토리에 많은 수의 이름을 배치하면 NAS 디렉토리 구조에 성능 문제가 발생할 수 있습니다. 특히 슬래시('/') 문자가 없는 이름은 모두 NAS 매핑의 루트 디렉토리에 배치됩니다. "NAS에 적합하지 않은" 이름을 광범위하게 사용하는 응용 프로그램은 NAS 매핑이 아닌 실제 오브젝트 저장소 버킷에서 호스팅하는 것이 좋습니다.

NAS 데이터에 대한 S3 프로토콜 액세스를 설정합니다

S3 프로토콜 액세스를 활성화하려면 NAS 지원 SVM이 오브젝트 저장소 서버 추가, 네트워킹 및 인증 요구사항 확인을 포함하여 S3 지원 서버와 동일한 요구사항을 충족하는지 확인해야 합니다.

새로운 ONTAP 설치의 경우 NAS 데이터를 클라이언트에 제공하도록 구성한 후 SVM에 대한 S3 프로토콜 액세스를 지원하는 것이 좋습니다. NAS 프로토콜 구성에 대한 자세한 내용은 다음을 참조하십시오.

- "NFS 구성"
- "SMB 구성"

시작하기 전에

S3 프로토콜을 활성화하기 전에 다음을 구성해야 합니다.

- S3 프로토콜 및 NFS, SMB 프로토콜 또는 둘 다 라이센스가 부여됩니다.
- SVM은 원하는 NAS 프로토콜을 위해 구성됩니다.
- NFS 및/또는 SMB 서버가 존재합니다.
- DNS 및 기타 필요한 서비스가 구성됩니다.
- NAS 데이터를 클라이언트 시스템으로 내보내거나 공유 중입니다.

이 작업에 대해

S3 클라이언트에서 S3 기반 SVM으로 HTTPS 트래픽을 활성화하려면 CA(인증 기관) 인증서가 필요합니다. 다음 세 소스의 CA 인증서를 사용할 수 있습니다.

- SVM에서 자체 서명된 새로운 ONTAP 인증서
- SVM에 자체 서명된 기존 ONTAP 인증서
- 타사 인증서입니다.

NAS 데이터 제공에 사용하는 S3/NAS 버킷에 동일한 데이터 LIF를 사용할 수 있습니다. 특정 IP 주소가 필요한 경우 를 참조하십시오 "데이터 LIF 생성". LIF에서 S3 데이터 트래픽을 활성화하려면 S3 서비스 데이터 정책이 필요합니다. S3를 포함하도록 SVM의 기존 서비스 정책을 수정할 수 있습니다.

S3 오브젝트 서버를 생성할 때 S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비를 해야 합니다. S3 서버 FQDN은 버킷 이름으로 시작하지 않아야 합니다.

시스템 관리자

1. NAS 프로토콜이 구성된 스토리지 VM에서 S3를 설정합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 NAS 지원 스토리지 VM을 선택한 다음 설정 을 클릭하고 을 클릭합니다 ⚙ S3 아래.
   b. 인증서 유형을 선택합니다. 시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.
   c. 네트워크 인터페이스를 입력합니다.
2. 시스템에서 생성한 인증서를 선택한 경우 새 스토리지 VM 생성이 확인되면 인증서 정보가 표시됩니다. 다운로드 * 를 클릭하고 클라이언트 액세스를 위해 저장합니다.
   - 비밀 키는 다시 표시되지 않습니다.
   - 인증서 정보가 다시 필요한 경우 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

CLI를 참조하십시오

1. SVM에서 S3 프로토콜이 허용되는지 확인합니다.
   `vserver show -fields allowed-protocols`
2. 이 SVM에 대한 공개 키 인증서를 기록합니다. + 새로운 ONTAP 자체 서명 인증서가 필요한 경우 를 참조하십시오 "SVM에서 CA 인증서를 생성하고 설치합니다".
3. 서비스 데이터 정책을 업데이트합니다
   a. SVM+에 대한 서비스 데이터 정책을 표시합니다 `network interface service-policy show -vserver svm_name`
   b. 를 추가합니다 `data-core` 및 `data-s3-server services` 없을 경우 를 누릅니다 `network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. SVM에 있는 데이터 LIF가 귀사의 요구사항을 충족하는지 확인하십시오.
   `network interface show -vserver svm_name`
5. S3 서버 생성:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

S3 서버를 생성할 때 또는 나중에 언제든지 추가 옵션을 지정할 수 있습니다.

- HTTPS는 기본적으로 포트 443에서 활성화됩니다. secure-listener-port 옵션을 사용하여 포트 번호를 변경할 수 있습니다. +HTTPS가 활성화되면 SSL/TLS와의 올바른 통합을 위해 CA 인증서가 필요합니다.
- HTTP는 기본적으로 사용되지 않으며, 이 옵션을 설정하면 서버가 포트 80에서 수신 대기합니다. is-http-enabled 옵션을 사용하여 설정하거나 -listener-port 옵션을 사용하여 포트 번호를 변경할 수 있습니다. + HTTP가 활성화되면 모든 요청과 응답이 일반 텍스트로 네트워크를 통해 전송됩니다.
  1. S3이 원하는 대로 구성되었는지 확인합니다 `vserver object-store-server show`
- example * + 다음 명령은 모든 오브젝트 스토리지 서버의 구성 값을 확인합니다.
  `cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

S3 NAS 버킷을 생성합니다

S3 NAS 버킷은 S3 버킷 이름과 NAS 경로 사이의 매핑입니다. S3 NAS 버킷을 사용하면 기존 볼륨 및 디렉토리 구조가 있는 SVM 네임스페이스의 모든 부분에 S3 액세스를 제공할 수 있습니다.

시작하기 전에

- S3 오브젝트 서버는 NAS 데이터를 포함하는 SVM으로 구성됩니다.
- NAS 데이터는 에 부합합니다 "S3 클라이언트 액세스에 대한 요구 사항".

이 작업에 대해

SVM의 루트 디렉토리 내에 모든 파일 및 디렉토리 세트를 지정하도록 S3 NAS 버킷을 구성할 수 있습니다.

다음 매개 변수의 조합을 기반으로 NAS 데이터에 대한 액세스를 허용하거나 허용하지 않는 버킷 정책을 설정할 수도 있습니다.

- 파일 및 디렉터리
- 사용자 및 그룹 권한
- S3 작업

예를 들어, 대규모 사용자 그룹에 읽기 전용 데이터 액세스 권한을 부여하는 별도의 버킷 정책과 제한된 그룹이 해당 데이터의 하위 집합에 대한 작업을 수행할 수 있도록 하는 다른 버킷 정책이 필요할 수 있습니다.

S3 NAS “버킷”은 맵핑이며 S3 버킷이 아니기 때문에 표준 S3 버킷의 다음 속성은 S3 NAS 버킷에 적용되지 않습니다.

- * aggr-list\aggr-list-multiplier\storage-service-level\volume\size\exclude-aggr-list\QoS-policy-group * + S3 NAS 버킷을 구성할 때 볼륨 또는 qtree가 생성되지 않습니다.
- 역할 * 이 보호됨\is-protected-on-ONTAP\is-protected-on-cloud * + S3 NAS 버킷은 S3 SnapMirror를 사용하여 보호되거나 미러링되지 않지만 볼륨 단위로 제공되는 일반 SnapMirror 보호를 사용합니다.
- * 버전 관리 상태 * + NAS 볼륨에는 일반적으로 서로 다른 버전을 저장할 수 있는 스냅샷 기술이 있습니다. 그러나 버전 관리는 현재 S3 NAS 버킷에서 사용할 수 없습니다.
- 볼륨 명령을 통해 NAS 볼륨에 대해 * logical-used\object-count * + 등가 통계를 사용할 수 있습니다.

시스템 관리자

NAS 지원 스토리지 VM에 새 S3 NAS 버킷을 추가합니다.

1. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
2. S3 NAS 버킷의 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력하지 말고 * More Options * 를 클릭합니다.
3. 유효한 경로 이름을 입력하거나 찾아보기를 클릭하여 유효한 경로 이름 목록에서 선택합니다. + 올바른 경로 이름을 입력하면 S3 NAS 구성과 관련이 없는 옵션이 숨겨집니다.
4. S3 사용자를 NAS 사용자 및 생성된 그룹에 이미 매핑한 경우 해당 사용 권한을 구성한 다음 * 저장 * 을 클릭합니다. +이 단계에서 사용 권한을 구성하기 전에 S3 사용자를 NAS 사용자에게 이미 매핑해야 합니다.

그렇지 않으면 * 저장 * 을 클릭하여 S3 NAS 버킷 구성을 완료합니다.

CLI를 참조하십시오

NAS 파일 시스템이 포함된 SVM에서 S3 NAS 버킷 생성 를 누릅니다 `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-type nas -nas-path` *`junction_path`* `[-comment` *`text`*`]`

예:
```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

S3 클라이언트 사용자를 활성화합니다

S3 클라이언트 사용자가 NAS 데이터에 액세스할 수 있도록 하려면 S3 사용자 이름을 해당 NAS 사용자에게 매핑한 다음 버킷 서비스 정책을 사용하여 NAS 데이터에 액세스할 수 있는 권한을 부여해야 합니다.

시작하기 전에

클라이언트 액세스의 사용자 이름(Linux/UNIX, Windows 및 S3 클라이언트 사용자)이 이미 있어야 합니다.

이 작업에 대해

S3 사용자 이름을 해당 Linux/UNIX 또는 Windows 사용자에게 매핑하면 S3 클라이언트가 NAS 파일에 액세스할 때 NAS 파일에 대한 권한 부여 검사를 수행할 수 있습니다. S3-NAS 매핑은 단일 이름 또는 POSIX 정규식으로 표현될 수 있는 S3 사용자 이름_Pattern_과 Linux/UNIX 또는 Windows 사용자 이름_Replacement_를 제공하여 지정합니다.

이름 매핑이 없는 경우 기본 이름 매핑이 사용됩니다. 여기서 S3 사용자 이름 자체는 UNIX 사용자 이름 및 Windows 사용자 이름으로 사용됩니다. 를 사용하여 UNIX 및 Windows 기본 사용자 이름 매핑을 수정할 수 있습니다 `vserver object-store-server modify` 명령.

로컬 이름 매핑 구성만 지원되며 LDAP는 지원되지 않습니다.

S3 사용자를 NAS 사용자에게 매핑한 후에는 액세스 권한이 있는 리소스(디렉토리 및 파일)와 해당 사용자가 액세스할 수 있거나 수행할 수 없는 작업을 지정하는 권한을 사용자에게 부여할 수 있습니다.

시스템 관리자

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 S3/NAS 지원 스토리지 VM을 선택합니다.
   b. 설정 * 을 선택한 다음 을 클릭합니다 → 이름 매핑 * (* 호스트 사용자 및 그룹 * 아래).
   c. S3 to Windows * 또는 * S3 to UNIX * 타일(또는 둘 다)에서 * 추가 * 를 클릭한 다음 원하는 * 패턴 * (S3) 및 * 교체 * (NAS) 사용자 이름을 입력합니다.
2. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다.
   a. 스토리지 > 버킷 * 을 클릭하고 을 클릭합니다 ⋮ 원하는 S3 버킷 옆에 있는 * 편집 * 을 클릭합니다.
   b. 추가 * 를 클릭하고 원하는 값을 입력합니다.
      - * Principal * - S3 사용자 이름을 제공하거나 기본값(모든 사용자)을 사용합니다.
      - * 효과 * - * 허용 * 또는 * 거부 * 를 선택합니다.
      - * 조치 * - 이러한 사용자 및 리소스에 대한 조치를 입력합니다. 현재 오브젝트 저장소 서버가 S3 NAS 버킷에 대해 지원하는 리소스 작업 집합은 GetObject , PutObject , DeleteObject , ListBucket , GetBuckketAcl 입니다. GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBuckketVersioning, PutBucketVersioning 및 ListBuckketVersions. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
      - * 리소스 * - 작업이 허용 또는 거부된 폴더나 파일 경로를 입력하거나 기본(버킷의 루트 디렉터리)을 사용합니다.

CLI를 참조하십시오

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다. 를 누릅니다 `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` 매핑 평가의 우선 순위 번호입니다. 1 또는 2를 입력합니다.
   - `-pattern` - S3 사용자 이름 또는 정규식입니다
   - `-replacement` - Windows 또는 UNIX 사용자 이름입니다

예

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1 vserver name-mapping create -direction s3-unix
-position 2 -pattern s3_user_1 -replacement unix_user_1
```

1. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다. 를 누릅니다 `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - 사용자가 작업을 요청할 때 액세스를 허용할지 또는 거부할지 여부를 지정합니다.
   - `-action <Action>, …` - 허용 또는 거부된 리소스 작업을 지정합니다. 현재 오브젝트 저장소 서버가 S3 NAS 버킷에 대해 지원하는 리소스 작업 집합은 GetObject , PutObject , DeleteObject , ListBucket , GetBuckketAcl 입니다. GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBuckketVersioning, PutBucketVersioning 및 ListBuckketVersions. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.

- `-principal <Objectstore Principal>, …` - 이 매개 변수에 지정된 개체 저장소 서버 사용자 또는 그룹에 대해 액세스를 요청하는 사용자의 유효성을 검사합니다.
  - 개체 저장소 서버 그룹은 그룹 이름에 접두사 그룹 / 을 추가하여 지정합니다.
  - `-principal` -(하이픈 문자)는 모든 사용자에게 액세스 권한을 부여합니다.
- `-resource <text>, …` - 허용/거부 권한이 설정된 버킷, 폴더 또는 개체를 지정합니다. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
- `[-sid <SID>]` - 오브젝트 저장소 서버 버킷 정책 문에 대한 선택적 텍스트 설명을 지정합니다.

예

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.