S3 오브젝트 스토리지 관리

ONTAP 9

NetApp
February 14, 2026

목차

S3 오브젝트 스토리지 관리

ONTAP 9의 S3 지원에 대해 알아보십시오

ONTAP S3 구성에 대해 자세히 알아보십시오

ONTAP 9.8부터는 ONTAP System Manager와 같은 친숙한 관리 효율성 툴을 사용하여 ONTAP 클러스터에서 ONTAP S3(Simple Storage Service) 오브젝트 스토리지 서버를 사용하여 ONTAP에서 개발 및 운영을 위한 고성능 오브젝트 스토리지를 신속하게 프로비저닝하고 ONTAP의 스토리지 효율성 및 보안을 활용할 수 있습니다.

2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 설명서와 통합되었습니다. 이제 ONTAP S3 문서에 ONTAP 모범 사례 _ TR-4814:S3의 콘텐츠가 포함되어 있습니다.

System Manager 및 ONTAP CLI를 사용하는 S3 구성

System Manager 및 ONTAP CLI를 사용하여 ONTAP S3를 구성 및 관리할 수 있습니다. System Manager를 사용하여 S3를 활성화하고 버킷을 생성할 때 ONTAP은 단순한 구성을 위한 모범 사례 기본값을 선택합니다. 구성 매개 변수를 지정해야 하는 경우 ONTAP CLI를 사용할 수도 있습니다. CLI에서 S3 서버 및 버킷을 구성할 경우에도 원하는 경우 System Manager로 관리하거나 그 반대로 구성할 수 있습니다.

System Manager를 사용하여 S3 버킷을 생성하는 경우, ONTAP은 시스템에서 가장 가용성이 높은 기본 성능 서비스 수준을 구성합니다. 예를 들어, AFF 시스템에서 기본 설정은 * Extreme * 입니다. 성능 서비스 수준은 사전 정의된 QoS(Quality of Service) 정책 그룹입니다. 기본 서비스 수준 대신 사용자 지정 QoS 정책 그룹 또는 정책 그룹을 지정할 수 있습니다.

사전 정의된 적응형 QoS 정책 그룹은 다음과 같습니다.

- * Extreme *: 가장 낮은 지연 시간과 최고의 성능을 기대하는 애플리케이션에 사용됩니다.
- * 성능 *: 성능 요구사항 및 지연 시간이 중간 정도인 애플리케이션에 사용됩니다.
- * 가치 *: 처리량과 용량이 지연 시간보다 더 중요한 애플리케이션에 사용됩니다.
- * 사용자 정의 *: 사용자 정의 QoS 정책을 지정하거나 QoS 정책을 지정하지 않습니다.

계층화에 * 사용을 선택하면 성능 서비스 수준이 선택되지 않으며 시스템은 계층형 데이터에 대해 최적의 성능을 갖춘 저비용 미디어를 선택합니다.

참고 항목: "적응형 QoS 정책 그룹을 사용합니다".

ONTAP는 가장 적합한 디스크가 있는 로컬 계층에서 이 버킷을 프로비저닝하려고 시도하여 선택한 서비스 수준을 충족시킵니다. 그러나 버킷에 포함할 디스크를 지정해야 하는 경우 로컬 계층(애그리게이트)을 지정하여 CLI에서 S3 오브젝트 스토리지를 구성하는 것이 좋습니다. CLI에서 S3 서버를 구성할 경우에도 원할 경우 System Manager로 관리할 수 있습니다.

버킷에 사용할 애그리게이트를 지정할 수 있는 기능은 CLI를 통해서만 지정할 수 있습니다.

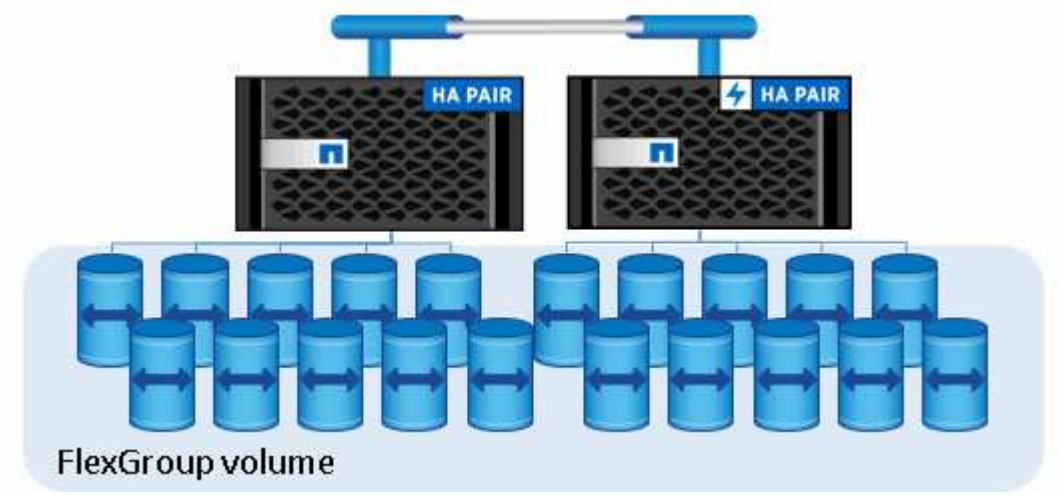
Cloud Volumes ONTAP에서 **S3** 버킷 구성

Cloud Volumes ONTAP에서 버킷 서비스를 제공하려면 기본 애그리게이트를 수동으로 선택하여 해당 애그리게이트가 하나의 노드만 사용하는지 확인하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다. 따라서 Cloud Volumes ONTAP 환경에서는 이 작업을 수행해야 합니다 CLI에서 S3 버킷을 구성합니다.

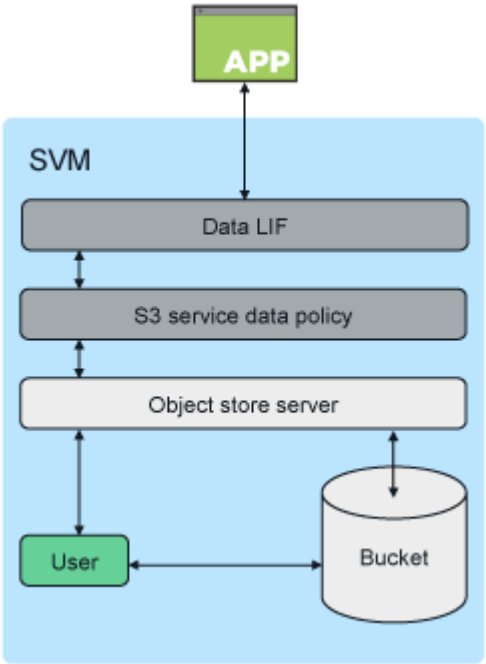
그렇지 않으면 Cloud Volumes ONTAP의 S3 서버가 사내 환경과 Cloud Volumes ONTAP에서 동일하게 구성 및 관리됩니다.

FlexGroup 볼륨을 사용하는 ONTAP S3 아키텍처

ONTAP에서 버킷의 기본 아키텍처는 여러 개의 구성 멤버 볼륨으로 구성되지만 단일 볼륨으로 관리되는 단일 네임스페이스인 A "FlexGroup 볼륨"입니다.



버킷에 대한 액세스는 승인된 사용자 및 클라이언트 애플리케이션을 통해 제공됩니다.



버킷을 FabricPool 엔드포인트로 사용하는 것을 포함하여 S3 애플리케이션에만 사용할 경우 기본 FlexGroup 볼륨은 S3 프로토콜만 지원합니다.

ONTAP 9.12.1부터 NAS 프로토콜을 사용하도록 미리 구성된 에서도 S3 프로토콜을 활성화할 수 "멀티프로토콜 NAS 볼륨"있습니다. 멀티프로토콜 NAS 볼륨에서 S3 프로토콜이 활성화된 경우 클라이언트 애플리케이션은 NFS, SMB 및 S3를 사용하여 데이터를 읽고 쓸 수 있습니다.

버킷 제한

최소 용량

최소 버킷 용량은 ONTAP 플랫폼에 의해 결정됩니다.

- 온프레미스 플랫폼의 경우 95GB입니다.
- Lab on Demand 이용 시 1.6GB의 용량이 필요합니다.
- ONTAP Select 의 경우 200MB가 필요합니다.

최대 크기

최대 버킷 용량은 FlexGroup 의 최대 크기인 60PB로 제한됩니다.

최대 버킷 수

FlexGroup 볼륨당 최대 버킷 수는 1,000개이며, 클러스터당 최대 12,000개(FlexGroup 볼륨 12개 사용 시)입니다.

ONTAP 9.14.1 이상을 사용한 자동 **FlexGroup** 사이징

ONTAP 9.14.1부터 기본 FlexGroup 크기는 포함된 버킷 크기를 기반으로 합니다. 버킷을 추가하거나 제거하면 FlexGroup 볼륨이 자동으로 증가 또는 감소합니다.

예를 들어 초기 Bucket_A가 100GB로 프로비저닝되면 FlexGroup는 100GB로 씬 프로비저닝됩니다. 300GB의 Bucket_B, 500GB의 Bucket_C라는 두 개의 추가 버킷을 생성하면 FlexGroup 볼륨이 900GB로 증가합니다.

(100GB의 Bucket_A + 300GB의 Bucket_B + 500GB의 Bucket_C = 900GB)

Bucket_A를 삭제하면 기본 FlexGroup 볼륨이 800GB로 줄어듭니다.

ONTAP 9.13.1 이하 버전에서 기본 **FlexGroup** 크기가 수정되었습니다

버킷 확장을 위한 용량을 제공하려면 FlexGroup 볼륨에 있는 모든 버킷의 총 사용 용량이 클러스터의 사용 가능한 스토리지 애그리게이트 기준 최대 FlexGroup 볼륨 용량의 33% 미만이어야 합니다. 이 조건을 충족할 수 없으면 새로 생성되는 자동으로 생성된 FlexGroup 볼륨에 새 버킷이 프로비저닝됩니다.

ONTAP 9.14.1 이전 버전에서는 FlexGroup 크기가 환경에 따라 기본 크기로 고정되어 있습니다.

- 1.6PB(ONTAP
- ONTAP Select은 100TB

클러스터의 용량이 기본 크기로 FlexGroup 볼륨을 프로비저닝할 수 없을 경우 ONTAP는 기존 환경에서 프로비저닝할 수 있을 때까지 기본 크기를 절반으로 줄입니다.

예를 들어, 300TB 환경에서 FlexGroup 볼륨은 200TB(1.6PB, 800TB, 400TB FlexGroup 볼륨 크기가 너무 커서 환경에 맞지 않는 경우)로 자동으로 프로비저닝됩니다.

ONTAP S3 주요 사용 사례

다음은 ONTAP S3 서비스에 대한 클라이언트 액세스의 주요 사용 사례입니다.

- FabricPool을 사용하여 비활성 데이터를 ONTAP의 버킷에 계층화하여 ONTAP to ONTAP 계층화를 지원합니다. 내의 버킷으로 계층화하거나 "로컬 클러스터"의 버킷으로의 계층화가 "원격 클러스터"모두 지원됩니다. ONTAP S3에 계층화하면 추가 FabricPool 라이센스나 새로운 기술을 관리할 필요 없이 비활성 데이터에 저렴한 ONTAP 시스템을 사용하고 새로운 플래시 용량에 대한 비용을 절감할 수 있습니다.
- ONTAP 9.12.1부터 NAS 프로토콜을 사용하도록 미리 구성된 에서도 S3 프로토콜을 활성화할 수 "멀티프로토콜 NAS 볼륨"있습니다. 멀티프로토콜 NAS 볼륨에서 S3 프로토콜이 사용되면 클라이언트 애플리케이션은 S3, NFS, SMB를 사용하여 데이터를 읽고 쓸 수 있으므로 다양한 추가 사용 사례가 열립니다. 가장 일반적인 사용 사례 중 하나는 볼륨에 데이터를 쓰는 NAS 클라이언트와 S3 클라이언트가 동일한 데이터를 읽고 분석, 비즈니스 인텔리전스, 머신 러닝, 광학 문자 인식 등과 같은 특수 작업을 수행하는 것입니다.

> ONTAP S3는 추가 하드웨어 및 관리 없이 기존 ONTAP 클러스터에서 S3 기능을 사용하려는 경우에 적합합니다. NetApp StorageGRID은 오브젝트 스토리지에 대한 NetApp의 대표적인 솔루션입니다. StorageGRID는 광범위한 S3 작업, 고급 ILM 기능 또는 ONTAP 기반 시스템에서 얻을 수 없는 용량을 활용해야 하는 네이티브 S3 애플리케이션에 권장됩니다. 자세한 내용은 를 "StorageGRID 설명서 "참조하십시오.

관련 정보

"FlexGroup 볼륨 관리"

계획

S3 오브젝트 스토리지를 위한 ONTAP 버전 및 플랫폼 지원

S3 오브젝트 스토리지는 ONTAP 9.8 이상을 사용하는 모든 AFF, FAS 및 ONTAP Select 플랫폼에서 지원됩니다.

FC, iSCSI, NFS, NVMe_oF 및 SMB 등의 다른 프로토콜과 마찬가지로, S3을 사용하려면 먼저 라이센스를 설치해야 ONTAP에서 사용할 수 있습니다. S3 라이센스는 비용이 들지 않는 라이센스이지만 ONTAP 9.8로 업그레이드하는 시스템에 설치해야 합니다. S3 라이센스는 NetApp 지원 사이트의 에서 다운로드할 수 "마스터 라이센스 키 페이지" 있습니다.

새로운 ONTAP 9.8 이상 시스템에는 S3 라이센스가 사전 설치되어 있습니다.

Cloud Volumes ONTAP

ONTAP S3는 Cloud Volumes ONTAP에서 사내 환경과 동일하게 구성 및 작동합니다. 단 한 가지 예외가 있습니다.

- Cloud Volumes ONTAP에서 버킷을 생성할 때는 CLI 절차를 사용하여 기본 FlexGroup 볼륨이 단일 노드의 애그리게이트만 사용하도록 해야 합니다. 노드가 지리적으로 서로 분리되어 있는 가용성 영역에 있고 지연 시간 문제가 발생하기 쉽기 때문에 여러 노드에서 애그리게이트를 사용하는 것은 성능에 영향을 미칩니다.

클라우드 공급자	**ONTAP** 버전
Google 클라우드	ONTAP 9.12.1 이상
설치하고	ONTAP 9.11.0 이상
Azure를 지원합니다	ONTAP 9.9.1 이상

NetApp ONTAP용 **Amazon FSx**

S3 오브젝트 스토리지는 ONTAP 9.11 이상을 사용하는 Amazon FSx for NetApp 서비스에서 지원됩니다.

MetroCluster를 통해 **S3** 지원

ONTAP 9.14.1부터 MetroCluster IP 및 FC 구성의 미러링된 애그리게이트에서 SVM에 S3 오브젝트 스토리지 서버를 사용하도록 설정할 수 있습니다.

ONTAP 9.12.1부터 MetroCluster IP 구성의 미러링되지 않은 Aggregate에서 SVM에서 S3 오브젝트 스토리지 서버를 활성화할 수 있습니다. MetroCluster IP 구성에서 미러링되지 않은 애그리게이트의 제한에 대한 자세한 내용은 를 참조하십시오. "미러링되지 않은 애그리게이트의 고려 사항"

SnapMirror S3는 MetroCluster 구성에서 지원되지 않습니다.

S3 ONTAP 9.7의 공용 미리 보기

ONTAP 9.7에서는 S3 오브젝트 스토리지가 공용 미리 보기로 도입되었습니다. 이 버전은 프로덕션 환경을 위해 제작되지 않았으며 ONTAP 9.8부터 더 이상 업데이트되지 않습니다. ONTAP 9.8 이상 릴리즈에서만 운영 환경에서 S3 오브젝트 스토리지를 지원합니다.

9.7 공용 미리 보기로 생성된 S3 버킷은 ONTAP 9.8 이상에서 사용할 수 있지만 향상된 기능을 활용할 수는 없습니다. 9.7 공용 미리 보기로 만든 버킷이 있는 경우 이러한 버킷의 내용을 9.8 버킷으로 마이그레이션하여 기능 지원, 보안 및 성능 향상을 지원해야 합니다.

ONTAP S3가 지원되는 작업

ONTAP S3 작업은 아래 명시된 경우를 제외하고 표준 S3 REST API에서 지원됩니다. 자세한 내용은 를 참조하십시오 "Amazon S3 API 참조".

> 이러한 S3 작업은 ONTAP에서 네이티브 S3 버킷을 사용할 때 특히 지원됩니다. 버전 관리, 개체 잠금 및 기타 기능과 관련된 작업과 같은 이러한 작업 중 일부는 을 사용할 때 지원되지 "S3 NAS 버킷(멀티프로토콜 NAS 볼륨의 S3)"않습니다.

특정 작업에 대해 별도로 언급하지 않는 한, ONTAP 9.8부터 다음과 같은 일반적인 요청 헤더가 지원됩니다.

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`

- `Date`
- `Expect`
- `Host`
- `x-amz-date`

버킷 작업

ONTAP에서 AWS S3 API를 사용하여 다음 작업이 지원됩니다.

버킷 작동	로 시작하는 **ONTAP** 지원
CreateBucket ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1
삭제 버킷 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
DeleteBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
DeleteBucketLifecycle ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
DeleteBuckketPolicy를 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1
GetBucketAcl ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetBuckLifecycleConfiguration 을 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.13.1 *만료 작업만 지원됩니다.
GetBucketLocation ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.10.1
GetBucketPolicy ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1

버킷 작동	로 시작하는 **ONTAP** 지원
GetBucketVersioning ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
HeadBucket ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListAllMyBuckets ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListBuckets ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListBucketVersions ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
퍼트버킷	• ONTAP 9.11.1 • ONTAP 9.8 - ONTAP REST API에서만 지원됩니다
PutBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
PutBucketLifecycleConfiguration ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.13.1 * 만료 작업만 지원됩니다.
PutBucketPolicy ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1
PutBucketVersioning ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1

오브젝트 작업

ONTAP 9.9.1부터 ONTAP S3는 오브젝트 메타데이터 및 태그 지정을 지원합니다.

- PutObject 및 CreateMultipartUpload 를 사용하여 키-값 쌍을 포함합니다 `x-amz-meta-<key>.`

  예: ' x-amz-meta-project: ONTAP_S3'.

- GetObject 및 HeadObject 는 사용자 정의 메타데이터를 반환합니다.
- 메타데이터와 달리 태그는 다음을 사용하여 오브젝트와 독립적으로 읽을 수 있습니다.
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging 을 선택합니다

ONTAP 9.11.1부터 ONTAP S3는 다음과 같은 ONTAP API와 함께 개체 버전 관리 및 관련 작업을 지원합니다.

- GetBuckketVersioning 을 참조하십시오
- 목록 BuckketVersions
- PutBucketVersioning을 참조하십시오

특정 작업에 대해 별도로 언급하지 않는 한 다음 URI 쿼리 매개변수가 지원됩니다.

- `versionId`(ONTAP 9.12.1부터 시작되는 개체 작업에 필요함)

개체 작업입니다	로 시작하는 **ONTAP** 지원
AbortMultipartUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. `uploadId`	ONTAP 9.8
CompleteMultipartUpload를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. `uploadId`	ONTAP 9.8
CopyObject 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9.12.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
CreateMultptUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
DeleteObject 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bypass-governance-retention`	ONTAP 9.8
DeleteObjects ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다.* `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging 을 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
GetObject 를 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` 그리고 이 추가 요청 헤더는 다음과 같습니다. • 범위	ONTAP 9.8
GetObjectAcl ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetObjectAttributes ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.14.1
GetObjectTagging ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1
HeadObject ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8

개체 작업입니다	로 시작하는 **ONTAP** 지원
ListMultipartUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8
ListObjects 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8
ListObjectsV2 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8

개체 작업입니다	로 시작하는 **ONTAP** 지원
ListObjectVersions 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1
목록 파트 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8
PutObject 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
PutObjectLockConfiguration ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.14.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
PutObjectRetention ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1
업로드 파트	ONTAP 9.8
업로드파트 복사 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `partNumber` • `uploadId` 그리고 다음과 같은 추가 요청 헤더가 있습니다. • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

그룹 정책

이러한 작업은 S3에 한정되지 않으며 일반적으로 IAM(Identity and Management) 프로세스와 연결됩니다. ONTAP는 이러한 명령을 지원하지만 IAM REST API는 사용하지 않습니다.

- 정책을 생성합니다
- AttachGroup 정책

사용자 관리

이러한 작업은 S3에 한정되지 않으며 일반적으로 IAM 프로세스와 연관됩니다.

- CreateUser 를 선택합니다
- DeleteUser 를 클릭합니다
- 그룹 생성

- 삭제 그룹

릴리즈별 **S3** 작업

ONTAP 9.14.1

ONTAP 9.14.1에는 S3 오브젝트 잠금 지원이 추가되었습니다.

> 법적 증거 자료 보관 작업(정의된 보존 시간이 없는 잠금)은 지원되지 않습니다.

- GetObjectLockConfiguration 을 참조하십시오
- GetObjectRetention을 참조하십시오
- PutObjectLockConfiguration 을 참조하십시오
- PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1에는 버킷 라이프사이클 관리 지원이 추가되었습니다.

- DeleteBucketLifecycleConfiguration을 참조하십시오
- GetBuckLifecycleConfiguration 을 참조하십시오
- PutBucketLifecycleConfiguration을 참조하십시오

ONTAP 9.12.1

ONTAP 9.12.1에는 버킷 정책 및 오브젝트 복사 기능이 추가되었습니다.

- DeleteBuckketPolicy를 참조하십시오
- GetBuckketPolicy를 참조하십시오
- BucketPolicy를 참조하십시오
- CopyObject 를 선택합니다
- 업로드파트 복사

ONTAP 9.11.1

ONTAP 9.11.1에는 버전 관리, 미리 지정된 URL, 청크 업로드 지원, S3 API를 사용한 버킷 생성 및 삭제와 같은 일반적인 S3 작업 지원이 추가되었습니다.

- ONTAP S3는 이제 청크 업로드 서명 요청을 지원합니다. `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3는 이제 미리 설정된 URL을 사용하여 개체를 공유하거나 다른 사용자가 사용자 자격 증명 없이도 개체를 업로드할 수 있도록 클라이언트 응용 프로그램을 지원합니다.
- CreateBucket
- 삭제 버킷
- GetBuckketVersioning 을 참조하십시오
- 목록 BuckketVersions
- 퍼트버킷

- PutBucketVersioning을 참조하십시오
- DeleteObjects 를 클릭합니다
- ListObjectVersions 를 선택합니다

첫 번째 버킷이 될 때까지 기본 FlexGroup이 생성되지 않으므로 외부 클라이언트가 CreateBucket을 사용하여 버킷을 생성하려면 먼저 ONTAP에서 버킷을 생성해야 합니다.

ONTAP 9.10.1

ONTAP 9.10.1에는 SnapMirror S3 및 GetBucketLocation에 대한 지원이 추가되었습니다.

- GetBucketLocation 을 참조하십시오

ONTAP 9.9.1

ONTAP 9.9.1에서는 ONTAP S3에 개체 메타데이터 및 태그 지정 지원에 대한 지원을 추가합니다.

- PutObject 및 CreateMultipartUpload 는 이제 를 사용하여 키-값 쌍을 `x-amz-meta-<key>` 포함합니다. 예를 들면 다음과 `x-amz-meta-project: ontap_s3`같습니다.
- GetObject 및 HeadObject 는 이제 사용자 정의 메타데이터를 반환합니다.

태그는 버킷과 함께 사용할 수도 있습니다. 메타데이터와 달리 태그는 다음을 사용하여 오브젝트와 독립적으로 읽을 수 있습니다.

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging 을 선택합니다

ONTAP S3 상호 운용성

ONTAP S3 서버는 일반적으로 이 표에 명시된 경우를 제외하고 다른 ONTAP 기능과 상호 작용합니다.

피처 영역	지원	지원되지 않습니다
Cloud Volumes ONTAP	• ONTAP 9.9.1 이상 릴리즈의 Azure 클라이언트 • ONTAP 9.11.0 이상 릴리즈의 AWS 클라이언트 • ONTAP 9.12.1 이상 릴리스의 Google Cloud 클라이언트	• ONTAP 9.8 및 이전 릴리스의 모든 클라이언트용 Cloud Volumes ONTAP

피처 영역	지원	지원되지 않습니다
데이터 보호	• Cloud Sync • 오브젝트 잠금, 거버넌스 및 규정 준수(ONTAP 9.14.1부터) • "개체 버전 관리" (ONTAP 9.11.1부터) • 미러링되지 않은 MetroCluster 애그리게이트(ONTAP 9.12.1부터) • 미러링된 MetroCluster 애그리게이트(ONTAP 9.14.1부터) • "SnapMirror S3" (ONTAP 9.10.1부터) • SnapMirror(NAS 볼륨만 해당, ONTAP 9.12.1부터) • SnapLock(NAS 볼륨 전용, ONTAP 9.14.1부터)	• 삭제 코딩 • NDMP • SMTape • SnapMirror (동기 및 비동기) • SnapMirror 클라우드 • SVM 재해 복구 • SyncMirror (SyncMirror 미러링된 집계는 ONTAP 9.14.1부터 MetroCluster 구성에서 지원됩니다. SyncMirror MetroCluster 구성 외부에서는 지원되지 않습니다.)
암호화	• NetApp 애그리게이트 암호화(NAE) • NetApp 볼륨 암호화(NVE) • NSE(NetApp 스토리지 암호화) • TLS/SSL	• 슬래그
MetroCluster 환경	-	SnapMirror S3
스토리지 효율성	• 중복 제거 • 압축 • 컴팩션	• 집계 수준 효율성(동일한 집계에 있는 멤버는 교차 볼륨 중복 제거를 활용할 수 있지만 다른 집계에 있는 멤버는 활용할 수 없음) • ONTAP S3 버킷을 포함하는 FlexGroup 볼륨의 볼륨 클론 • FlexClone 기술(볼륨, 파일 및 LUN)
서비스 품질(QoS)	• QoS 최대(천장) • 최소 QoS(층)	-

피처 영역	지원	지원되지 않습니다
추가 기능	• "S3 이벤트를 감사합니다" (ONTAP 9.10.1부터) • "버킷 수명 주기 관리" (ONTAP 9.13.1부터) • FabricPool 클라우드 계층(네이티브 S3만 해당) • FabricPool 로컬 계층(NAS 볼륨만 해당) • FlexCache 볼륨(ONTAP 9.18.1부터 지원)	• FPolicy를 참조하십시오 • Qtree • 할당량 • FabricPool 클라우드 계층(NAS 볼륨만 해당) • FabricPool 로컬 계층(네이티브 S3 전용)

ONTAP에서 S3를 사용한 검증된 타사 솔루션

S3는 보편적인 표준이며, 이는 지원되는 애플리케이션의 포괄적인 목록이 아닙니다. 단지 해당 파트너와 협력하여 검증된 솔루션 목록일 뿐입니다. 찾고 있는 솔루션이 목록에 없으면 NetApp 계정 담당자에게 문의하십시오.

네이티브 **S3** 버킷을 사용하여 검증된 타사 솔루션

- 아마존 SageMaker
- Apache Hadoop S3A 클라이언트
- 아파치 카프카
- 아파치 스파크
- Commvault(V11)
- Confluent Kafka
- NetBackup을 선택합니다
- 레드햇 키
- Rubrik으로 이동합니다
- 스노우플레이크
- 트리노
- Veeam(V12)

이러한 솔루션은 ONTAP에서 네이티브 S3 버킷을 사용할 때 특별히 검증됩니다. 버전 관리, 객체 잠금 및 기타 기능과 관련된 솔루션 등 일부 솔루션은 ONTAP을 사용할 때 지원되지 않습니다. "S3 NAS 버킷(멀티프로토콜 NAS 볼륨의 S3)" .

구성

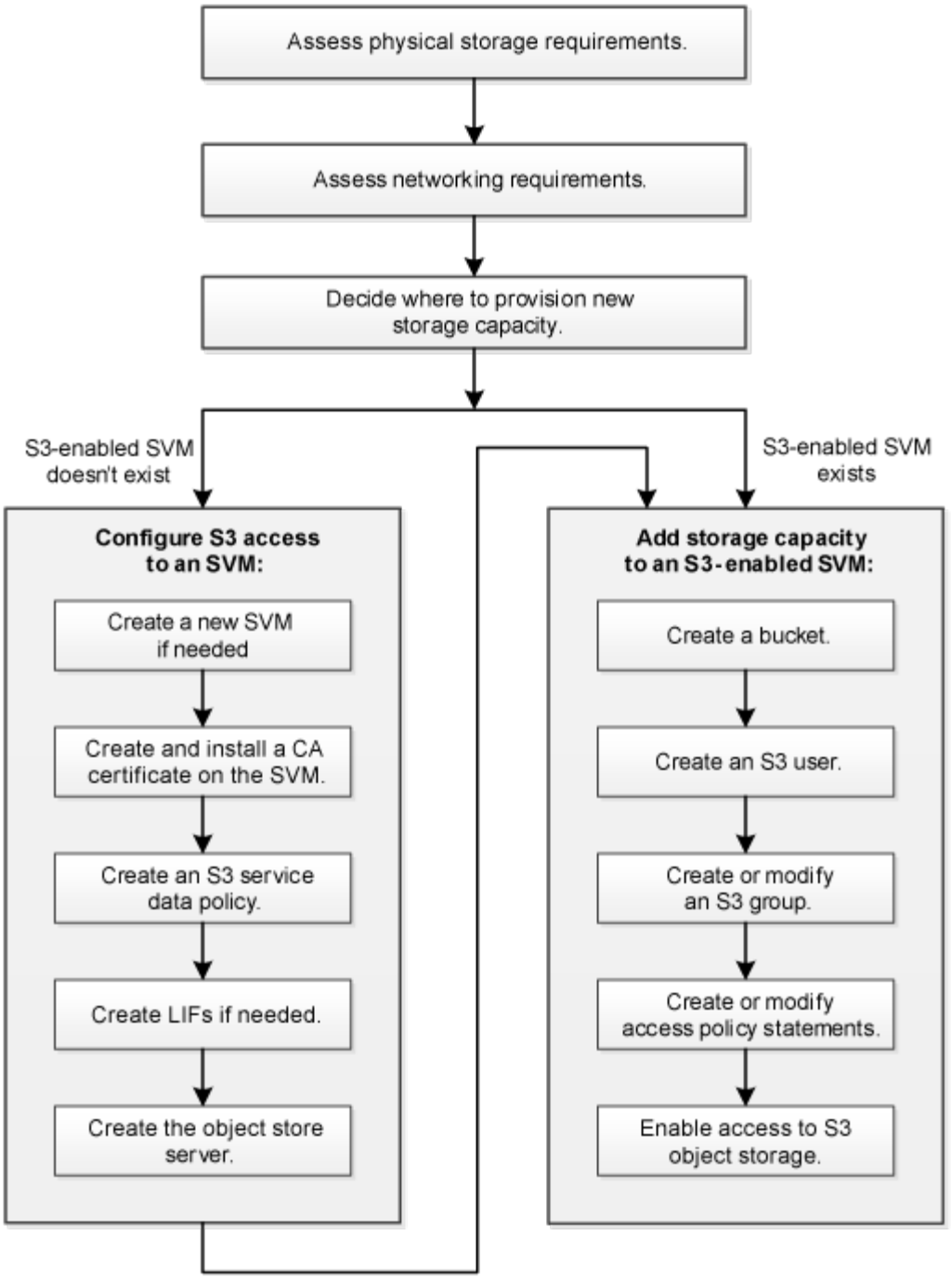
S3 구성 프로세스 정보

ONTAP S3 구성 워크플로우

S3 구성에는 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음, 특정 목적에 맞는 워크플로우 선택, 즉 새 SVM 또는 기존 SVM에 대한 S3 액세스 구성, 또는 이미 S3 액세스용으로 완전히 구성된 기존 SVM에 버킷 및 사용자 추가 등이 포함됩니다.

클러스터와 클라이언트 간의 시간을 동기화하려면 NTP(네트워크 시간 프로토콜) 구성이 필요합니다. 클라이언트 액세스를 위해서는 ONTAP S3 객체 저장소와 클라이언트 간에 최소 15분 이상의 유효한 타임스탬프가 필요합니다. "NTP 구성 방법에 대해 알아보세요" .

System Manager를 사용하여 새 스토리지 VM에 대한 S3 액세스를 구성하면 인증서 및 네트워킹 정보를 입력하라는 메시지가 표시되고 스토리지 VM 및 S3 오브젝트 스토리지 서버가 단일 작업으로 생성됩니다.



ONTAP S3의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 S3 스토리지를 프로비저닝하기 전에 새 오브젝트 저장소를 위한 기존 Aggregate의 공간이 충분한지 확인해야 합니다. 존재하지 않는 경우, 디스크를 기존 Aggregate에 추가하거나 원하는 유형 및 위치의 새 Aggregate를 생성할 수 있습니다.

이 작업에 대해

S3 지원 SVM에서 S3 버킷을 생성하면 FlexGroup 볼륨이 "자동으로 생성됩니다" 해당 버킷을 지원합니다. ONTAP Select에서 기본 애그리게이트와 FlexGroup 구성요소를 자동으로(기본값) 선택할 수도 있고, 기본 애그리게이트와 FlexGroup 구성요소를 직접 선택할 수도 있습니다.

Aggregate 및 FlexGroup 구성 요소(예: 기본 디스크에 특정한 성능 요구 사항이 있는 경우)를 지정하려는 경우, 애그리게이트 구성이 FlexGroup 볼륨 프로비저닝을 위한 모범 사례 지침을 준수해야 합니다. 자세한 내용:

- "FlexGroup 볼륨 관리"
- "NetApp 기술 보고서 4571-A: NetApp ONTAP FlexGroup 볼륨 모범 사례"

Cloud Volumes ONTAP에서 버킷을 제공하는 경우 기본 애그리게이트를 수동으로 선택하여 하나의 노드만 사용하도록 하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다. 에 대해 자세히 알아보십시오 "Cloud Volumes ONTAP용 버킷 생성".

ONTAP S3 서버를 사용하여 성능 계층과 동일한 클러스터에 로컬 FabricPool 용량 계층을 생성할 수 있습니다. 예를 들어, SSD 디스크가 한 HA 쌍에 연결되어 있고 _cold_data를 다른 HA 쌍의 HDD 디스크에 계층화하려는 경우 이 방법이 유용할 수 있습니다. 이 사용 사례에서 로컬 용량 계층이 포함된 S3 서버와 버킷은 성능 계층과 다른 HA 쌍이어야 합니다. 1노드 및 2노드 클러스터에서는 로컬 계층화가 지원되지 않습니다.

단계

1. 기존 애그리게이트에서 사용 가능한 공간 표시:

   '스토리지 집계 쇼'

   충분한 공간 또는 필수 노드 위치가 있는 Aggregate가 있는 경우 S3 구성의 이름을 기록합니다.

```
cluster-1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. 충분한 공간 또는 필수 노드 위치가 있는 애그리게이트가 없는 경우 'storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'storage aggregate create' 명령을 사용하여 새 애그리게이트를 생성합니다.

관련 정보

- "스토리지 집계 추가 디스크"
- "저장소 집계 생성"

ONTAP S3 네트워킹 요구사항을 평가합니다

S3 스토리지를 클라이언트에 제공하기 전에 네트워킹이 S3 프로비저닝 요구사항을 충족하도록 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

이 작업에 대해

원격 FabricPool 용량(클라우드) 계층 및 원격 S3 클라이언트의 경우 데이터 SVM을 사용하고 데이터 LIF를 구성해야 합니다. FabricPool 클라우드 계층의 경우 클러스터 피어링이 필요하지 않으므로 인터클러스터 LIF도 구성해야 합니다.

로컬 FabricPool 용량 계층의 경우 시스템 SVM("클러스터")을 사용해야 하지만 LIF 구성을 위한 두 가지 옵션이 있습니다.

- 클러스터 LIF를 사용할 수 있습니다.

  이 옵션을 선택하면 더 이상 LIF 구성이 필요하지 않지만 클러스터 LIF의 트래픽이 증가합니다. 또한 로컬 계층은 다른 클러스터에서 액세스할 수 없습니다.

- 데이터 및 인터클러스터 LIF를 사용할 수 있습니다.

  이 옵션을 사용하려면 S3 프로토콜에 LIF를 설정하는 등 추가 구성이 필요합니다. 하지만 로컬 계층도 다른 클러스터에 대한 원격 FabricPool 클라우드 계층으로 액세스할 수 있습니다.

단계

1. 사용 가능한 물리적 포트 및 가상 포트를 표시합니다.

   네트워크 포트 쇼

   - 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
   - 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.

2. 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하고 사용 가능한 충분한 주소가 있는지 확인합니다.

   네트워크 서브넷 쇼

   서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 network subnet create 명령을 사용하여 생성된다.

에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 사용 가능한 IPspace 표시:

   네트워크 IPspace 쇼

   기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6이 활성화되어 있는지 확인합니다.

   네트워크 옵션 IPv6 쇼

   필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

관련 정보

- "네트워크 포트가 표시됩니다"
- "네트워크 옵션 IPv6"
- "네트워크 IPspace가 표시됩니다"
- "네트워크 서브넷 생성"

새로운 **ONTAP S3** 스토리지 용량을 프로비저닝할 위치를 결정합니다

새 S3 버킷을 생성하기 전에 새 SVM이나 기존 SVM에 배치할 것인지 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- S3에 대해 활성화되지 않은 새 SVM 또는 SVM에서 버킷을 프로비저닝하려면 다음 항목의 단계를 완료하십시오.

  "S3를 위해 SVM을 생성합니다"

  "S3에 대한 버킷을 생성합니다"

  S3는 NFS 및 SMB와 SVM에서 공존할 수 있지만, 다음 중 하나가 참인 경우 새 SVM을 생성하도록 선택할 수 있습니다.

  - 클러스터에서 S3를 처음으로 사용하도록 설정하고 있습니다.
  - S3 지원을 활성화하지 않으려는 클러스터에 기존 SVM이 있습니다.
  - 클러스터에 하나 이상의 S3 기반 SVM이 있고 성능 특성이 다른 또 다른 S3 서버를 원합니다. SVM에서 S3를 활성화한 후 버킷 프로비저닝을 진행합니다.

- 기존 S3 기반 SVM에서 초기 버킷 또는 추가 버킷을 프로비저닝하려면 다음 항목의 단계를 완료하십시오.

  "S3에 대한 버킷을 생성합니다"

SVM에 대한 S3 액세스를 구성합니다

ONTAP S3용 **SVM**을 생성합니다

S3는 SVM의 다른 프로토콜과 공존할 수 있지만, 네임스페이스와 워크로드를 격리하기 위해 새 SVM을 생성할 수 있습니다.

이 작업에 대해

SVM에서 S3 오브젝트 스토리지만 제공하는 경우 S3 서버는 DNS 구성이 필요하지 않습니다. 그러나 다른 프로토콜을 사용하는 경우 SVM에서 DNS를 구성할 수 있습니다.

System Manager를 사용하여 새 스토리지 VM에 대한 S3 액세스를 구성하면 인증서 및 네트워킹 정보를 입력하라는 메시지가 표시되고 스토리지 VM 및 S3 오브젝트 스토리지 서버가 단일 작업으로 생성됩니다.

예 **1.** 단계

시스템 관리자

S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비가 되어 있어야 합니다. S3 서버 FQDN은 버킷 이름으로 시작하지 않아야 합니다.

인터페이스 역할 데이터에 대한 IP 주소를 입력할 준비가 되어 있어야 합니다.

외부 CA 서명 인증서를 사용하는 경우 이 절차를 수행하는 동안 해당 인증서를 입력하라는 메시지가 표시됩니다. 또한 시스템에서 생성한 인증서를 사용할 수도 있습니다.

1. 스토리지 VM에서 S3를 설정합니다.

   a. 새 스토리지 VM 추가: * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다.

      기존 스토리지 VM이 없는 새 시스템인 경우 * 대시보드 > 프로토콜 구성 * 을 클릭합니다.

   S3 서버를 기존 스토리지 VM에 추가하려면 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * S3 * 아래를 클릭합니다.

   a. S3 * 활성화 를 클릭한 다음 S3 서버 이름 을 입력합니다.

   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. S3 라이센스가 클러스터에서 라이센스되었는지 확인합니다.

```
system license show -package s3
```

   그렇지 않은 경우 영업 담당자에게 문의하십시오.

2. SVM 생성:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- '-rootvolume-security-style' 옵션에 UNIX 설정을 사용합니다.
- 기본 C. UTF-8 '-language' 옵션을 사용합니다.
- IPSpace 설정은 선택 사항입니다.

3. 새로 생성한 SVM의 구성 및 상태 확인:

```
vserver show -vserver <svm_name>
```

'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다. spaceba:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 엑스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다. 기본적으로 vsadmin 사용자 계정은 생성되고 '잠김' 상태입니다. vsadmin 역할이 기본 vsadmin 사용자 계정에 할당됩니다.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                  List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

ONTAP S3 지원 **SVM**에 **CA** 인증서를 생성하고 설치합니다

S3 클라이언트는 S3 지원 SVM에 HTTPS 트래픽을 전송하기 위해 인증 기관(CA) 인증서가 필요합니다. CA 인증서는 클라이언트 애플리케이션과 ONTAP 개체 저장소 서버 간에 신뢰 관계를 만듭니다. 원격 클라이언트가 액세스할 수 있는 개체 저장소로 사용하기 전에 ONTAP 에 CA 인증서를 설치해야 합니다.

이 작업에 대해

S3 서버가 HTTP만 사용하도록 구성할 수 있고 CA 인증서 요구 사항 없이 클라이언트를 구성할 수는 있지만 HTTPS 트래픽을 CA 인증서가 있는 ONTAP S3 서버로 보호하는 것이 가장 좋습니다.

IP 트래픽이 클러스터 LIF만 통과하는 로컬 계층화 사용 사례에는 CA 인증서가 필요하지 않습니다.

이 절차의 지침은 ONTAP 자체 서명 인증서를 만들고 설치합니다. ONTAP에서 자체 서명된 인증서를 생성할 수 있지만 타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다. 자세한 내용은 관리자 인증 설명서를 참조하십시오.

"관리자 인증 및 RBAC"

및 추가 구성 옵션에 대한 자세한 `security certificate` 내용은 "ONTAP 명령 참조입니다"를 참조하십시오.

단계

1. 자체 서명된 디지털 인증서 생성:

   'Security certificate create - vserver_svm_name _ -type root-ca-common-name_ca_cert_name _'

   '-type root-ca' 옵션은 자체 서명된 디지털 인증서를 만들어 설치하여 CA(인증 기관)를 사용하여 다른 인증서에 서명합니다.

   '-common-name' 옵션은 SVM의 CA(인증 기관) 이름을 생성하며 인증서의 전체 이름을 생성할 때 사용됩니다.

   기본 인증서 크기는 2048비트입니다.

   예

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   인증서의 생성된 이름이 표시되면 이 절차의 이후 단계를 위해 저장해야 합니다.

   에 대한 자세한 내용은 `security certificate create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 인증서 서명 요청 생성:

   'Security certificate generate - csr-common-name_s3_server_name_[additional_options]'

   서명 요청의 '-common-name' 매개변수는 S3 서버 이름(FQDN)이어야 합니다.

   필요한 경우 SVM에 대한 위치 및 기타 세부 정보를 제공할 수 있습니다.

   그만큼 `-dns-name` 매개변수는 클라이언트가 DNS 이름 목록을 제공하는 주체 대체 이름 확장을 지정하기 위해 종종 필요합니다.

   그만큼 `-ipaddr` 클라이언트는 IP 주소 목록을 제공하는 주체 대체 이름 확장을 지정하기 위해 종종 매개변수가 필요합니다.

   나중에 참조할 수 있도록 인증서 요청과 개인 키의 복사본을 보관하라는 메시지가 표시됩니다.

   에 대한 자세한 내용은 `security certificate generate-csr` "ONTAP 명령 참조입니다"을 참조하십시오.

3. SVM_CA를 사용하여 CSR에 서명하여 S3 서버의 인증서를 생성합니다.

   '보안 인증서 서명 - vserver_svm_name_-ca_ca_cert_name_-ca-serial_ca_cert_serial_number_[additional_options]'

   이전 단계에서 사용한 명령 옵션을 입력합니다.

- '-ca' — 1단계에서 입력한 CA의 공통 이름입니다.
- '-ca-serial' — 1단계의 CA 일련 번호입니다. 예를 들어 CA 인증서 이름이 svm1_ca_159D1587CE21E9D4_svm1_ca인 경우 일련 번호는 159D1587CE21E9D4입니다.

  기본적으로 서명된 인증서는 365일 후에 만료됩니다. 다른 값을 선택하고 다른 서명 세부 정보를 지정할 수 있습니다.

  메시지가 표시되면 2단계에서 저장한 인증서 요청 문자열을 복사하여 입력합니다.

서명된 인증서가 표시되면 나중에 사용할 수 있도록 저장합니다.

4. S3 기반 SVM에 서명된 인증서 설치:

   'Security certificate install-type server-vserver_svm_name_'

   메시지가 표시되면 인증서와 개인 키를 입력합니다.

   인증서 체인이 필요한 경우 중간 인증서를 입력할 수 있습니다.

   개인 키와 CA 서명 디지털 인증서가 표시되면 나중에 참조할 수 있도록 저장합니다.

5. 공개 키 인증서 받기:

   'Security certificate show -vserver_svm_name_-common-name_ca_cert_name_-type root-ca-instance'

   나중에 클라이언트 측 구성을 위해 공개 키 인증서를 저장합니다.

   예

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                        Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
               Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
           Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                           Country Name: US
                State or Province Name:
                           Locality Name:
                      Organization Name:
                      Organization Unit:
Contact Administrator's Email Address:
                               Protocol: SSL
                        Hashing Function: SHA256
                Self-Signed Certificate: true
       Is System Internal Certificate: false
```

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "보안 인증서 서명"

ONTAP S3 서비스 데이터 정책을 생성합니다

S3 데이터 및 관리 서비스에 대한 서비스 정책을 생성할 수 있습니다. LIF에서 S3 데이터 트래픽을 활성화하려면 S3 서비스 데이터 정책이 필요합니다.

이 작업에 대해

데이터 LIF 및 인터클러스터 LIF를 사용하는 경우 S3 서비스 데이터 정책이 필요합니다. 로컬 계층화 사용 사례에서 클러스터 LIF를 사용하는 경우에는 필요하지 않습니다.

LIF에 서비스 정책을 지정한 경우, 이 정책을 사용하여 LIF에 대한 기본 역할, 페일오버 정책 및 데이터 프로토콜 목록을 구성합니다.

SVM 및 LIF에 여러 프로토콜을 구성할 수 있지만 오브젝트 데이터를 제공할 때 S3가 유일한 프로토콜이 되도록 하는

것이 좋습니다.

단계

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. 서비스 데이터 정책 생성:

   'network interface service-policy create-vserver_svm_name_-policy_policy_name_-services data-core, data-s3-server'

   ONTAP S3을 활성화하는 데 필요한 서비스는 데이터 코어(Data-Core) 및 데이터-S3-서버(Data-S3-Server) 서비스뿐입니다. 단, 다른 서비스는 필요에 따라 포함할 수 있습니다.

   에 대한 자세한 내용은 `network interface service-policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP S3에 대한 데이터 LIF를 생성합니다

새 SVM을 생성한 경우 S3 액세스를 위해 생성하는 전용 LIF는 데이터 LIF가 되어야 합니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF 서비스 정책이 이미 존재해야 합니다.
- 모범 사례로서, 데이터 액세스에 사용되는 LIF(Data-S3-서버)와 관리 작업(관리-https)에 사용되는 LIF는 별도로 두어야 합니다. 두 서비스 모두 같은 LIF에서 활성화해서는 안 됩니다.
- DNS 레코드에는 Data-S3-서버가 연결된 LIF의 IP 주소만 있어야 합니다. 다른 LIF의 IP 주소가 DNS 레코드에 지정된 경우 다른 서버에서 ONTAP S3 요청을 처리할 수 있으므로 예기치 않은 응답이나 데이터 손실이 발생할 수 있습니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

  및 `network interface capacity details show` 에 대한 자세한 `network interface capacity show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

- 원격 FabricPool 용량(클라우드) 계층화를 사용하는 경우 인터클러스터 LIF도 구성해야 합니다.

단계

1. LIF 생성:

   'network interface create-vserver_svm_name_-lif_lif_name_-service-policy_service_policy_names_-home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_|-subnet-name_subnet_subnet_name_} - firewall-policy data-auto-revert_revert_revert_false

   - 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

     에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

     또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

   - '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
   - IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
   - 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
   - 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
   - '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

     필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.

     ⓘ ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

   - '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.
   - '-service-policy' 옵션은 사용자가 만든 데이터 및 관리 서비스 정책과 필요한 기타 정책을 지정합니다.

2. '-address' 옵션에서 IPv6 주소를 할당하려면 다음과 같이 하십시오.

   a. network NDP prefix show 명령을 사용하여 다양한 인터페이스에서 습득한 RA prefix 목록을 볼 수 있다.

      고급 권한 수준에서 network NDP prefix show 명령을 사용할 수 있다.

   b. IPv6 주소를 수동으로 구성하려면 접두사:id 형식을 사용합니다.

      접두사는 다양한 인터페이스에서 습득한 접두사입니다.

   ID를 도출하려면 임의의 64비트 16진수 숫자를 선택합니다.

3. 'network interface show' 명령을 사용하여 LIF가 성공적으로 생성되었는지 확인합니다.
4. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면...	사용...
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

예

다음 명령을 실행하면 'y-s3-policy' 서비스 정책에 할당된 S3 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"
- "네트워크 NDP 접두사가 표시됩니다"

ONTAP S3를 사용하여 원격 **FabricPool** 계층화를 위한 인터클러스터 **LIF**를 생성합니다

ONTAP S3를 사용하여 원격 FabricPool 용량(클라우드) 계층화를 활성화하는 경우 인터클러스터 LIF를 구성해야 합니다. 데이터 네트워크와 공유하는 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 인터클러스터 네트워킹에 필요한 포트 수가 줄어듭니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- LIF 서비스 정책이 이미 존재해야 합니다.

이 작업에 대해

인터클러스터 LIF는 로컬 Fabric 풀 계층화나 외부 S3 애플리케이션을 제공하기 위해 필요하지 않습니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 시스템 SVM에 대한 인터클러스터 LIF 생성:

   'network interface create-vserver cluster-lif_LIF_name_-service-policy default-인터클러스터-home -node_node_-home-port_port_-address_port_ip_-netmask_mask_'

   다음 예에서는 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 인터클러스터 LIF가 생성되었는지 확인합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. 인터클러스터 LIF가 중복되는지 확인합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다

   다음 예에서는 e0c 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0d 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP S3 오브젝트 저장소 서버를 생성합니다

ONTAP 오브젝트 저장소 서버는 ONTAP NAS 및 SAN 서버에서 제공하는 파일 또는 블록 스토리지가 아니라 데이터를 S3 오브젝트로 관리합니다.

시작하기 전에

S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비가 되어 있어야 합니다. FQDN은 버킷 이름으로 시작할 수 없습니다. 가상 호스팅 스타일을 사용하여 버킷에 액세스하는 경우 서버 이름이 로 `mydomain.com`사용됩니다. `bucketname.mydomain.com`예를 들어,

자체 서명된 CA 인증서(이전 단계에서 만든 인증서) 또는 외부 CA 공급업체에서 서명한 인증서가 있어야 합니다. IP 트래픽이 클러스터 LIF만 통과하는 로컬 계층화 사용 사례에는 CA 인증서가 필요하지 않습니다.

이 작업에 대해

오브젝트 저장소 서버가 생성되면 UID 0의 루트 사용자가 생성됩니다. 이 루트 사용자에 대해 액세스 키 또는 암호 키가 생성되지 않았습니다. ONTAP 관리자는 'object-store-server users Regenerate-keys' 명령을 실행하여 이 사용자의 액세스 키와 비밀 키를 설정해야 합니다.

> NetApp 모범 사례로서 이 루트 사용자를 사용하지 마십시오. 루트 사용자의 액세스 키 또는 암호 키를 사용하는 모든 클라이언트 애플리케이션은 오브젝트 저장소의 모든 버킷과 개체에 대한 모든 액세스 권한을 가집니다.

에 대한 자세한 내용은 `vserver object-store-server` "ONTAP 명령 참조입니다"을 참조하십시오.

예 **2.** 단계

시스템 관리자

기존 스토리지 VM에 S3 서버를 추가하는 경우 이 절차를 사용합니다. S3 서버를 새 스토리지 VM에 추가하려면 을 참조하십시오 "S3를 위한 스토리지 SVM 생성".

인터페이스 역할 데이터에 대한 IP 주소를 입력할 준비가 되어 있어야 합니다.

1. 기존 스토리지 VM에서 S3를 설정합니다.
   a. 스토리지 VM을 선택합니다. * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * S3 * 아래를 클릭합니다.
   b. S3 * 활성화 를 클릭한 다음 S3 서버 이름 을 입력합니다.
   c. 인증서 유형을 선택합니다.

      시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.

   d. 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. S3 서버 생성:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

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

   - 로컬 계층화를 구성하는 경우 SVM 이름은 데이터 SVM 또는 시스템 SVM(클러스터) 이름일 수 있습니다.
   - 인증서 이름은 서버 CA 인증서(중간 또는 루트 CA 인증서)가 아니라 서버 인증서(최종 사용자 또는 리프 인증서)의 이름이어야 합니다.
   - HTTPS는 기본적으로 포트 443에서 활성화됩니다. '-secure-listener-port' 옵션을 사용하여 포트 번호를 변경할 수 있습니다.

     HTTPS가 활성화된 경우 SSL/TLS와의 올바른 통합을 위해 CA 인증서가 필요합니다. ONTAP 9.15.1부터 TLS 1.3은 S3 오브젝트 스토리지에서 지원됩니다.

   - HTTP는 기본적으로 해제되어 있습니다. 활성화되면 서버는 포트 80에서 수신 대기합니다. 를 사용하여 활성화할 수 있습니다 `-is-http-enabled` 옵션을 선택하거나 를 사용하여 포트 번호를 변경합니다 `-listener-port` 옵션을 선택합니다.

     HTTP가 활성화되면 요청과 응답이 네트워크를 통해 일반 텍스트로 전송됩니다.

2. S3이 구성되었는지 확인:

   'vserver object-store-server show'를 선택합니다

예

이 명령은 모든 객체 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 지원 SVM에 스토리지 용량 추가

ONTAP S3 버킷을 생성합니다

S3 오브젝트는 _ bucket _ 에 유지됩니다. 다른 디렉터리 내의 디렉터리 안에 파일로 중첩되지 않습니다.

시작하기 전에

S3 서버가 포함된 스토리지 VM이 이미 존재해야 합니다.

이 작업에 대해

- ONTAP 9.14.1부터는 S3 FlexGroup 볼륨에 버킷이 생성되면 자동 크기 조정이 활성화되었습니다. 따라서 기존 및 새 FlexGroup 볼륨에서 버킷 생성 중에 과도한 용량 할당이 필요 없습니다. FlexGroup 볼륨의 크기는 다음 지침에 따라 최소 필요한 크기로 조정됩니다. 필요한 최소 크기는 FlexGroup 볼륨에 있는 모든 S3 버킷의 총 크기입니다.
  - ONTAP 9.14.1부터 새 버킷 생성 시 S3 FlexGroup 볼륨이 생성되는 경우 필요한 최소 크기로 FlexGroup 볼륨이 생성됩니다.
  - ONTAP 9.14.1 전에 S3 FlexGroup 볼륨을 생성한 경우, ONTAP 9.14.1 이후 생성되거나 삭제된 첫 번째 버킷이 FlexGroup 볼륨의 크기를 필요한 최소 크기로 조정합니다.
  - ONTAP 9.14.1 전에 S3 FlexGroup 볼륨이 생성되었고 이미 필요한 최소 크기가 있는 경우, ONTAP 9.14.1 이후 버킷 생성 또는 삭제에 의해 S3 FlexGroup 볼륨의 크기가 유지됩니다.
- 스토리지 서비스 수준은 *value*, *performance* 및 _extreme_default 수준으로 사전 정의된 QoS(Adaptive Quality of Service) 정책 그룹입니다. 기본 스토리지 서비스 수준 대신 맞춤형 QoS 정책 그룹을 정의하여 버킷에 적용할 수도 있습니다. 스토리지 서비스 정의에 대한 자세한 내용은 을 "스토리지 서비스 정의"참조하십시오. 성능 관리에 대한 자세한 내용은 을 "성능 관리"참조하십시오. ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로

사용하도록 설정됩니다. 프로비저닝 프로세스 도중 또는 나중에 QoS를 사용하지 않도록 설정하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

- 로컬 용량 계층화를 구성하는 경우, S3 서버가 있는 시스템 스토리지 VM이 아닌 데이터 스토리지 VM에 버킷 및 사용자를 생성합니다.
- 원격 클라이언트 액세스의 경우 S3 지원 스토리지 VM에서 버킷을 구성해야 합니다. S3이 활성화되지 않은 스토리지 VM에서 버킷을 생성하는 경우 로컬 계층화에만 사용할 수 있습니다.
- ONTAP 9.14.1부터 가능합니다 "MetroCluster 구성의 경우 미러링된 또는 미러링되지 않은 애그리게이트에 버킷을 생성합니다".
- CLI의 경우 버킷을 생성할 때 두 가지 프로비저닝 옵션이 있습니다.
  - ONTAP Select에서 기본 애그리게이트와 FlexGroup 구성 요소 사용(기본값)
    - ONTAP는 애그리게이트를 자동으로 선택하여 첫 번째 버킷에 대한 FlexGroup 볼륨을 생성 및 구성합니다. 플랫폼에 사용할 수 있는 가장 높은 서비스 수준이 자동으로 선택되거나 스토리지 서비스 수준을 지정할 수 있습니다. 스토리지 VM에서 나중에 추가하는 모든 추가 버킷은 동일한 기본 FlexGroup 볼륨을 갖게 됩니다.
    - 또는 버킷이 계층화에 사용되는지 여부를 지정할 수 있습니다. 이 경우 ONTAP는 계층형 데이터에 대해 최적의 성능을 제공하는 경제적인 미디어를 선택하려고 합니다.
  - 기본 애그리게이트 및 FlexGroup 구성요소 선택(고급 권한 명령 옵션 필요): 버킷과 FlexGroup 볼륨을 생성해야 하는 애그리게이트를 수동으로 선택한 다음, 각 애그리게이트에서 구성요소 수를 지정할 수 있습니다. 추가 버킷 추가 시:
    - 새 버킷에 대해 Aggregate 및 구성요소를 지정하는 경우 새 FlexGroup가 새 버킷에 대해 생성됩니다.
    - 새 버킷의 Aggregate 및 구성요소를 지정하지 않을 경우 새 버킷이 기존 FlexGroup에 추가됩니다. 을 참조하십시오 FlexGroup 볼륨 관리 를 참조하십시오.

      버킷을 생성할 때 Aggregate 및 구성요소를 지정하면 QoS 정책 그룹, 기본값 또는 사용자 지정이 적용되지 않습니다. 나중에 'vserver object-store-server bucket modify' 명령을 사용하여 이 작업을 수행할 수 있습니다.

    에 대한 자세한 내용은 `vserver object-store-server bucket modify` "ONTAP 명령 참조입니다 "을 참조하십시오.
- 참고: * Cloud Volumes ONTAP에서 버킷을 제공하는 경우 CLI 절차를 사용해야 합니다. 기본 애그리게이트는 한 노드만 사용하는지 확인하기 위해 수동으로 선택하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다.

ONTAP CLI로 **S3** 버킷을 생성합니다

1. Aggregate 및 FlexGroup 구성 요소를 직접 선택하려면 권한 수준을 Advanced(고급)로 설정하십시오. 그렇지 않으면 admin 권한 수준이 Advanced(고급)로 설정됩니다
2. 버킷 생성:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -size [integer{KB|MB|GB|TB|PB}] [-comment text]
   [additional_options]
   ```

   스토리지 VM 이름은 데이터 스토리지 VM 또는 일 수 있습니다 `Cluster` 로컬 계층화를 구성하는 경우 (시스템 스토리지 VM 이름)

ONTAP에서 성능 또는 사용량을 기준으로 버킷을 생성하려면 다음 옵션 중 하나를 사용하십시오.

- 서비스 레벨

  가치, 성능, 익스트림 등의 가치 중 하나로 스토리지 서비스 수준 옵션을 포함시키십시오.

- 계층화

  사용된 용량 계층 TRUE 옵션을 포함합니다.

  기본 FlexGroup 볼륨을 생성할 애그리게이트를 지정하려면 다음 옵션을 사용하십시오.

- '-aggr-list' 매개 변수는 FlexGroup 볼륨 구성요소에 사용할 애그리게이트 목록을 지정합니다.

  목록의 각 항목은 지정된 애그리게이트에 구성요소를 생성합니다. Aggregate를 여러 번 지정하여 Aggregate에 여러 구성요소를 생성할 수 있습니다.

FlexGroup 볼륨 전체에서 일관된 성능을 위해서는 모든 애그리게이트에서 동일한 디스크 유형과 RAID 그룹 구성을 사용해야 합니다.

- '-aggr-list-multiplier' 매개 변수는 FlexGroup 볼륨을 생성할 때 '-aggr-list' 매개 변수로 나열된 애그리게이트를 반복하는 횟수를 지정합니다.

  '-aggr-list-multiplier' 파라미터의 기본값은 4이다.

3. 필요한 경우 QoS 정책 그룹을 추가합니다.

   'vserver object-store-server bucket modify -bucket_bucket_name_-qos-policy-group_qos_policy_group_'

4. 버킷 생성 확인:

   'vserver object-store-server bucket show[-instance]'

예

다음 예에서는 스토리지 VM용 버킷을 생성합니다 `vs1` 있습니다 `1TB` 집계 지정:

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

System Manager로 **S3** 버킷을 생성합니다

1. S3 지원 스토리지 VM에 새 버킷을 추가합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.
      - 이 지점에서 * Save * (저장 *)를 클릭하면 다음 기본 설정으로 버킷이 생성됩니다.
        - 그룹 정책이 이미 적용되어 있지 않으면 버킷에 대한 액세스 권한이 사용자에게 부여되지 않습니다.

오브젝트 저장소에 대한 무제한 액세스 권한이 있으므로 S3 루트 사용자를 사용하여 ONTAP 오브젝트 스토리지를 관리하고 권한을 공유해서는 안 됩니다. 대신 할당한 관리 권한이 있는 사용자 또는 그룹을 만듭니다.

- 시스템에서 가장 높은 수준의 서비스 품질(성능) 수준입니다.
- 이 기본값으로 버킷을 만들려면 * 저장 * 을 클릭합니다.

추가 권한 및 제한 사항을 구성합니다

버킷을 구성할 때 * 추가 옵션 * 을 클릭하여 오브젝트 잠금, 사용자 권한 및 성능 수준에 대한 설정을 구성하거나 나중에 이 설정을 수정할 수 있습니다.

FabricPool 계층화에 S3 오브젝트 저장소를 사용하려는 경우 성능 서비스 수준이 아닌 * 계층화에 사용 * (계층 데이터에 최적의 성능을 제공하는 저비용 미디어 사용)을 선택하는 것이 좋습니다.

버킷에서 버전 관리를 사용하도록 설정한 경우, S3 클라이언트를 사용하여 오브젝트의 특정 버전에 오브젝트 잠금 보존 시간을 배치할 수 있습니다. 개체의 특정 버전을 잠그더라도 개체의 다른 버전이 삭제되는 것을 막을 수는 없습니다. 나중에 복구할 수 있도록 개체의 버전 관리를 활성화하려면 * 버전 관리 활성화 * 를 선택합니다. 버킷에서 오브젝트 잠금을 사용하도록 설정하는 경우 버전 관리가 기본적으로 활성화됩니다. 개체 버전 관리에 대한 자세한 내용은 를 "Amazon용 S3 버킷에서 버전 관리 사용"참조하십시오.

9.14.1부터 S3 버킷에서 오브젝트 잠금이 지원됩니다. 버킷이 생성될 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에서는 오브젝트 잠금을 활성화할 수 없습니다. 오브젝트 잠금은 네이티브 S3 사용 사례에서만 사용할 수 있습니다. S3 프로토콜을 사용하도록 구성된 멀티프로토콜 NAS 볼륨은 SnapLock를 사용하여 WORM 스토리지에 데이터를 커밋해야 합니다. S3 오브젝트 잠금에는 표준 SnapLock 라이센스가 필요합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

ONTAP One 이전에는 SnapLock 라이센스가 보안 및 규정 준수 번들에 포함되어 있었습니다. 보안 및 규정 준수 번들은 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다. . "설치합니다" 객체 잠금을 활성화하기 전에 먼저 이 작업을 수행해야 합니다.

SnapLock 라이센스가 설치되어 있음을 확인한 후 버킷의 객체가 삭제되거나 덮어쓰지 않도록 보호하려면 * 개체 잠금 활성화 * 를 선택합니다. 잠금은 모든 오브젝트 또는 특정 버전에서 활성화될 수 있으며 클러스터 노드에 대해 SnapLock 컴플라이언스 클록이 초기화된 경우에만 활성화됩니다. 다음 단계를 수행하십시오.

1. 클러스터의 어떤 노드에서도 SnapLock 컴플라이언스 클록이 초기화되지 않으면 * SnapLock 규정 준수 클록 초기화 * 버튼이 나타납니다. Initialize SnapLock Compliance Clock * 을 클릭하여 클러스터 노드에서 SnapLock 컴플라이언스 클록을 초기화합니다.
2. 오브젝트에 대해 *WORM(Write Once, Read Many)* 권한을 허용하는 시간 기반 잠금을 활성화하려면 * Governance * mode를 선택하십시오. _Governance_mode에서도 특정 권한을 가진 관리자 사용자가 객체를 삭제할 수 있습니다.
3. 객체에 대해 보다 엄격한 삭제 규칙을 지정하고 업데이트하려면 * 규정 준수 * 모드를 선택하십시오. 이 오브젝트 잠금 모드에서는 지정된 보존 기간이 완료된 후에만 오브젝트를 만료시킬 수 있습니다. 보존 기간을 지정하지 않으면 객체는 무기한으로 잠긴 상태로 유지됩니다.
4. 특정 기간 동안 잠금을 적용하려면 잠금 보존 기간을 일 또는 년 단위로 지정합니다.

잠금은 버전 및 비버전 S3 버킷에 적용할 수 있습니다. NAS 객체에는 객체 잠금을 적용할 수 없습니다.

버킷에 대한 보호 및 권한 설정 및 성능 서비스 수준을 구성할 수 있습니다.

사용 권한을 구성하기 전에 사용자 및 그룹을 이미 만들어야 합니다.

자세한 내용은 을 "새 버킷을 위한 거울을 작성합니다"참조하십시오.

버킷에 대한 접근을 확인합니다

S3 클라이언트 애플리케이션(ONTAP S3 또는 외부 타사 애플리케이션)에서 다음을 입력하여 새로 생성된 버킷에 대한 액세스를 확인할 수 있습니다.

- S3 서버 CA 인증서입니다.
- 사용자의 액세스 키와 비밀 키입니다.
- S3 서버 FQDN 이름 및 버킷 이름입니다.

ONTAP S3 버킷 크기를 늘리거나 줄입니다

필요한 경우 기존 버킷의 크기를 늘리거나 줄일 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 버킷 크기를 관리할 수 있습니다.

시스템 관리자

1. 스토리지 > 버킷 * 을 선택하고 수정할 버킷을 찾습니다.
2. 버킷 이름 옆에 있는 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
3. Edit bucket * 창에서 버킷 용량을 변경합니다.
4. * 저장 *.

CLI를 참조하십시오

1. 버킷 용량 변경:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

MetroCluster 구성의 경우 미러링된 또는 미러링되지 않은 애그리게이트에 **ONTAP S3** 버킷을 생성합니다

ONTAP 9.14.1부터 MetroCluster FC 및 IP 구성의 미러링 또는 미러링되지 않은 애그리게이트에 버킷을 프로비저닝할 수 있습니다.

이 작업에 대해

- 기본적으로 버킷은 미러링된 애그리게이트에서 프로비저닝됩니다.
- 에 설명된 것과 동일한 프로비저닝 지침을 따릅니다 "버킷을 만듭니다" MetroCluster 환경에서 버킷 생성에 적용됩니다.

- 다음 S3 오브젝트 스토리지 기능은 MetroCluster 환경에서 * 지원되지 않음 *.
  - SnapMirror S3
  - S3 버킷 라이프사이클 관리
  - Compliance * 모드에서 S3 오브젝트 잠금

    거버넌스 * 모드에서 S3 오브젝트 잠금이 지원됩니다.

  - 로컬 FabricPool 계층화

시작하기 전에

S3 서버를 포함하는 SVM이 이미 존재해야 합니다.

버킷을 생성하는 프로세스

CLI를 참조하십시오

1. Aggregate 및 FlexGroup 구성 요소를 직접 선택하려면 권한 수준을 Advanced(고급)로 설정하십시오. 그렇지 않으면 admin 권한 수준이 Advanced(고급)로 설정됩니다
2. 버킷 생성:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   를 설정합니다 `-use-mirrored-aggregates` 옵션을 로 설정합니다 `true` 또는 `false` 미러링된 애그리게이트를 사용할지, 아니면 미러링되지 않은 애그리게이트를 사용할지에 따라 다릅니다.

   > 기본적으로 은(는) 입니다 `-use-mirrored-aggregates` 옵션이 로 설정되어 있습니다 `true`.

   - SVM 이름은 데이터 SVM이어야 합니다.
   - 옵션을 지정하지 않을 경우 ONTAP는 800GB 버킷을 생성하고 서비스 레벨이 시스템에서 사용 가능한 최대 레벨로 설정합니다.
   - ONTAP에서 성능 또는 사용량을 기준으로 버킷을 생성하려면 다음 옵션 중 하나를 사용하십시오.
     - 서비스 레벨

       가치, 성능, 익스트림 등의 가치 중 하나로 스토리지 서비스 수준 옵션을 포함시키십시오.

     - 계층화

       사용된 용량 계층 TRUE 옵션을 포함합니다.

   - 기본 FlexGroup 볼륨을 생성할 애그리게이트를 지정하려면 다음 옵션을 사용하십시오.
     - '-aggr-list' 매개 변수는 FlexGroup 볼륨 구성요소에 사용할 애그리게이트 목록을 지정합니다.

       목록의 각 항목은 지정된 애그리게이트에 구성요소를 생성합니다. Aggregate를 여러 번 지정하여 Aggregate에 여러 구성요소를 생성할 수 있습니다.

   FlexGroup 볼륨 전체에서 일관된 성능을 위해서는 모든 애그리게이트에서 동일한 디스크 유형과 RAID 그룹 구성을 사용해야 합니다.

   - '-aggr-list-multiplier' 매개 변수는 FlexGroup 볼륨을 생성할 때 '-aggr-list' 매개 변수로 나열된 애그리게이트를 반복하는 횟수를 지정합니다.

     '-aggr-list-multiplier' 파라미터의 기본값은 4이다.

3. 필요한 경우 QoS 정책 그룹을 추가합니다.

   'vserver object-store-server bucket modify -bucket_bucket_name_-qos-policy -group_qos_policy_group_'

4. 버킷 생성 확인:

   'vserver object-store-server bucket show[-instance]'

예

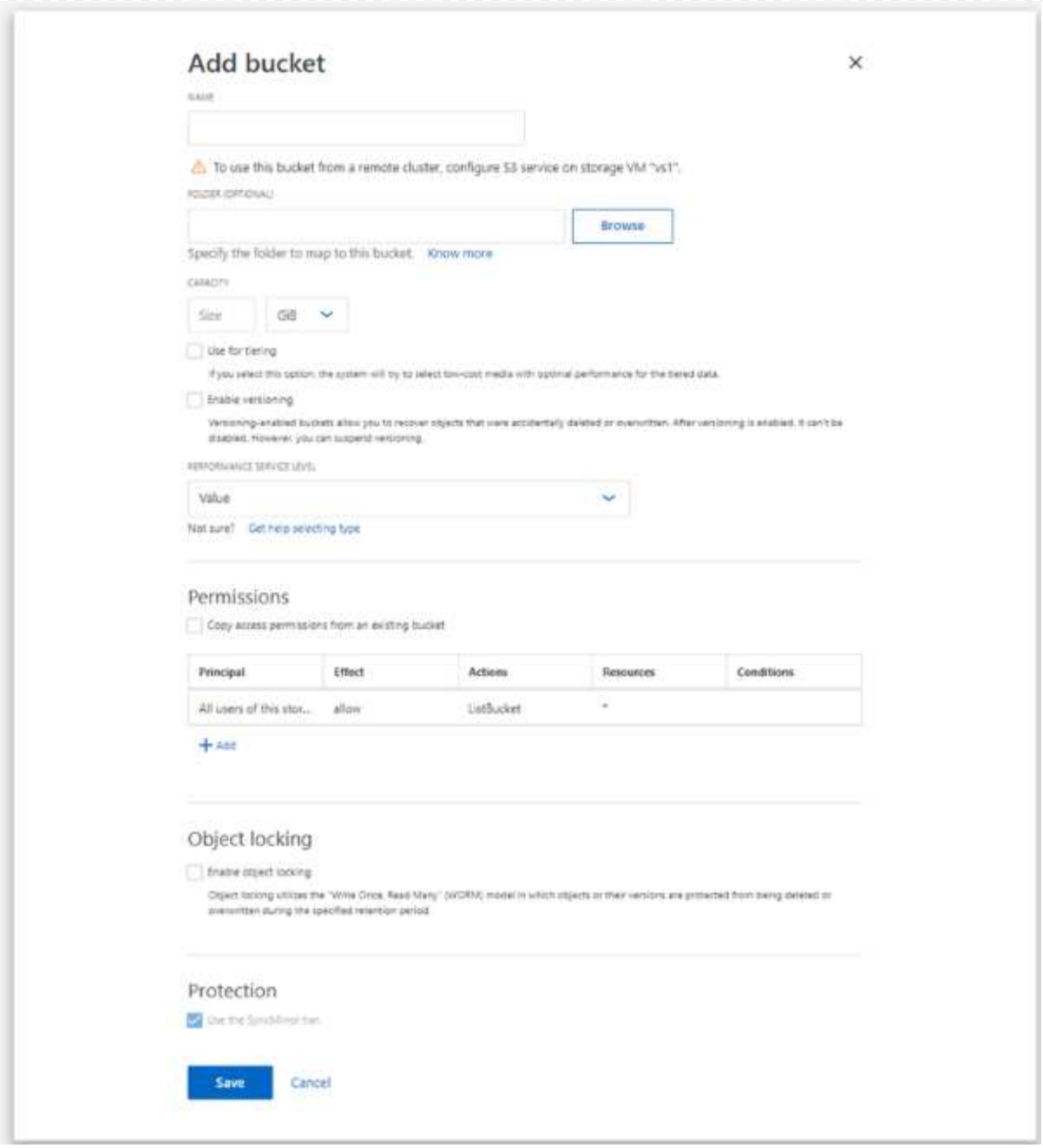
다음 예에서는 미러링된 애그리게이트에 1TB 크기의 SVM VS1에 대한 버킷을 생성합니다.

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

시스템 관리자

1. S3 지원 스토리지 VM에 새 버킷을 추가합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      기본적으로 버킷은 미러링된 애그리게이트에서 프로비저닝됩니다. 미러링되지 않은 Aggregate에 버킷을 생성하려면 * More Options * 를 선택하고 다음 이미지와 같이 * Protection * 아래에서 * Use the SyncMirror tier * 확인란의 선택을 취소합니다.



- 이 지점에서 * Save * (저장 *)를 클릭하면 다음 기본 설정으로 버킷이 생성됩니다.
  - 그룹 정책이 이미 적용되어 있지 않으면 버킷에 대한 액세스 권한이 사용자에게 부여되지 않습니다.

> 오브젝트 저장소에 대한 무제한 액세스 권한이 있으므로 S3 루트 사용자를 사용하여 ONTAP 오브젝트 스토리지를 관리하고 권한을 공유해서는 안 됩니다. 대신 할당한 관리 권한이 있는 사용자 또는 그룹을 만듭니다.

  - 시스템에서 가장 높은 수준의 서비스 품질(성능) 수준입니다.
- bucket을 구성할 때 * 추가 옵션 * 을 클릭하여 사용자 권한 및 성능 수준을 구성하거나 나중에 이러한 설정을 수정할 수 있습니다.
  - 권한을 구성하려면 * 추가 옵션 * 을 사용하기 전에 사용자 및 그룹을 이미 만들어야 합니다.

- FabricPool 계층화에 S3 오브젝트 저장소를 사용하려는 경우 성능 서비스 수준이 아닌 * 계층화에 사용 * (계층 데이터에 최적의 성능을 제공하는 저비용 미디어 사용)을 선택하는 것이 좋습니다.

2. S3 클라이언트 앱(다른 ONTAP 시스템 또는 외부 타사 앱)에서 다음을 입력하여 새 버킷에 대한 액세스를 확인합니다.
   - S3 서버 CA 인증서입니다.
   - 사용자의 액세스 키와 비밀 키입니다.
   - S3 서버 FQDN 이름 및 버킷 이름입니다.

ONTAP S3 버킷 라이프사이클 관리 규칙을 생성합니다

ONTAP 9.13.1부터 S3 버킷에서 오브젝트 라이프사이클을 관리하는 라이프사이클 관리 규칙을 생성할 수 있습니다. 버킷의 특정 오브젝트에 대한 삭제 규칙을 정의하고 이 규칙을 통해 버킷 오브젝트를 만료시킬 수 있습니다. 따라서 보존 요구사항을 충족하고 전체 S3 오브젝트 스토리지를 효율적으로 관리할 수 있습니다.

버킷 오브젝트에 대해 오브젝트 잠금이 설정되어 있으면 잠긴 오브젝트에 오브젝트 만료에 대한 라이프사이클 관리 규칙이 적용되지 않습니다. 개체 잠금에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

시작하기 전에

- S3 서버와 버킷을 포함하는 S3 기반 SVM이 이미 존재해야 합니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다" 를 참조하십시오.
- 멀티프로토콜 NAS 볼륨에서 S3를 사용하거나 MetroCluster 구성에서 S3를 사용하는 경우에는 버킷 라이프사이클 관리 규칙이 지원되지 않습니다.

이 작업에 대해

수명 주기 관리 규칙을 생성할 때 버킷 객체에 다음 삭제 작업을 적용할 수 있습니다.

- 현재 버전 삭제 - 이 작업은 규칙에 의해 식별된 개체를 만료시킵니다. 버킷에 버전 관리가 활성화되어 있는 경우 S3는 만료된 개체를 모두 사용할 수 없게 합니다. 버전 관리를 사용하지 않으면 이 규칙은 개체를 영구적으로 삭제합니다. CLI 작업은 입니다 `Expiration`.
- 현재 버전이 아닌 버전 삭제 - 이 작업은 S3에서 현재 개체가 아닌 개체를 영구적으로 제거할 수 있는 시기를 지정합니다. CLI 작업은 입니다 `NoncurrentVersionExpiration`.

현재 버전이 아닌 버전은 현재 버전의 생성 또는 수정 시간을 기반으로 합니다. 현재 개체가 아닌 개체의 지연된 제거는 실수로 개체를 삭제하거나 덮어쓸 때 유용할 수 있습니다. 예를 들어, 최신 버전이 아닌 버전이 5일 후에 삭제되도록 만료 규칙을 구성할 수 있습니다. 예를 들어 2014년 1월 1일 오전 10시 30분 UTC에 (버전 ID `111111`)라는 개체를 만든다고 가정해 `photo.gif` 보겠습니다. 2014년 1월 2일 오전 11시 30분에 실수로 (버전 ID)를 삭제했는데 `photo.gif`, 이 경우 새 버전 ID(예: 버전 ID `111111`)가 포함된 삭제 마커가 `4857693` 만들어집니다. 삭제가 영구화되기 전에 원래 버전(버전 ID `111111`)을 복구할 수 있는 기간이 5 `photo.gif`일입니다. `2014년 1월 8일 00:00 UTC`에 만료에 대한 수명 주기 규칙은 최신 버전이 아닌 `5`일 후에 실행되고 영구적으로 삭제됩니다 `photo.gif`(버전 ID `111111`).

- 만료된 삭제 표식 삭제 - 이 작업은 만료된 개체 삭제 표식을 삭제합니다.

버전 관리를 사용하는 버킷에서 삭제 표식이 있는 오브젝트는 개체의 현재 버전이 됩니다. 객체는 삭제되지 않으며, 객체에 대해 작업을 수행할 수 없습니다. 이러한 개체는 연결된 현재 버전이 없으면 만료됩니다. CLI 작업은 입니다 `Expiration`.

- 불완전한 다중 파트 업로드 삭제 - 이 작업은 다중 파트 업로드가 계속 진행되도록 허용할 최대 시간(일)을 설정합니다. 다음 중 삭제됩니다. CLI 작업은 입니다 `AbortIncompleteMultipartUpload`.

수행하는 절차는 사용하는 인터페이스에 따라 다릅니다. ONTAP 9.13,1에서는 CLI를 사용해야 합니다. ONTAP 9.14.1부터 System Manager를 사용할 수도 있습니다.

CLI를 사용하여 수명 주기 관리 규칙을 관리합니다

ONTAP 9.13.1부터는 ONTAP CLI를 사용하여 라이프사이클 관리 규칙을 생성하여 S3 버킷에서 오브젝트를 만료할 수 있습니다.

시작하기 전에

CLI의 경우 버킷 수명 주기 관리 규칙을 생성할 때 각 만료 작업 유형에 대한 필수 필드를 정의해야 합니다. 이러한 필드는 초기 생성 후 수정할 수 있습니다. 다음 표에는 각 작업 유형에 대한 고유 필드가 표시됩니다.

작업 유형	고유 필드
NonCurrentVersionExpiration 을 참조하십시오	• `-non-curr-days` - 현재 버전이 아닌 버전이 삭제될 때까지 남은 일 수입니다 • `-new-non-curr-versions` - 유지할 최신 버전이 아닌 버전 수입니다
만료	• `-obj-age-days` - 생성 후 현재 버전의 오브젝트를 삭제할 수 있는 일 수입니다 • `-obj-exp-date` 객체가 만료되는 특정 날짜입니다 • `-expired-obj-del-markers` - 객체를 정리해 마커를 삭제합니다
AbortIncompleteMultipartUpload를 중단합니다	• `-after-initiation-days` - 시작 일수입니다. 이후 업로드가 중단될 수 있습니다

버킷 수명주기 관리 규칙을 특정 객체 하위 집합에만 적용하려면 관리자는 규칙을 생성할 때 각 필터를 설정해야 합니다. 규칙을 생성할 때 이러한 필터를 설정하지 않으면 버킷 내의 모든 오브젝트에 규칙이 적용됩니다.

다음을 제외한 _ 을(를) 처음 생성한 후 모든 필터를 수정할 수 있습니다. +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

단계

1. 를 사용합니다 `vserver object-store-server bucket lifecycle-management-rule create` 버킷 수명 주기 관리 규칙을 생성하기 위해 만료 작업 유형에 필요한 필드가 있는 명령입니다.

예

다음 명령을 실행하면 NonCurrentVersionExpiration 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

예

다음 명령을 실행하면 만료 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

예

다음 명령을 실행하면 AbortIncompleteMultipartUpload 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

System Manager를 사용하여 라이프사이클 관리 규칙을 관리합니다

ONTAP 9.14.1부터 System Manager를 사용하여 S3 오브젝트를 만료할 수 있습니다. S3 오브젝트에 대한 라이프사이클 관리 규칙을 추가, 편집, 삭제할 수 있습니다. 또한 한 버킷에 대해 생성된 수명주기 규칙을 가져와 다른 버킷의 오브젝트에 사용할 수 있습니다. 활성 규칙을 사용하지 않도록 설정하고 나중에 활성화할 수 있습니다.

문서 수정 상태 관리 규칙을 추가합니다

1. 스토리지 > Bucket * 을 클릭합니다.
2. 만료 규칙을 지정할 버킷을 선택합니다.
3. ⋮아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 추가 > 라이프사이클 규칙 * 을 클릭합니다.

5. 문서 수정 상태 규칙 추가 페이지에서 규칙 이름을 추가합니다.
6. 규칙의 범위를 정의하여 버킷의 모든 오브젝트에 적용할지 또는 특정 오브젝트에 적용할지 여부를 지정합니다. 오브젝트를 지정하려면 다음 필터 조건 중 하나 이상을 추가합니다.
   a. 접두사: 규칙을 적용할 개체 키 이름의 접두사를 지정합니다. 일반적으로 개체의 경로 또는 폴더입니다. 규칙마다 접두사를 하나씩 입력할 수 있습니다. 유효한 접두사가 제공되지 않는 한 규칙은 버킷의 모든 오브젝트에 적용됩니다.
   b. 태그: 규칙을 적용할 개체에 대해 최대 3개의 키 및 값 쌍(태그)을 지정합니다. 필터링에는 유효한 키만 사용됩니다. 값은 선택 사항입니다. 그러나 값을 추가하는 경우에는 해당 키에 대해 유효한 값만 추가해야 합니다.
   c. 크기: 오브젝트의 최소 크기와 최대 크기 사이에서 범위를 제한할 수 있습니다. 두 값 중 하나 또는 모두를 입력할 수 있습니다. 기본 단위는 MiB입니다.
7. 작업을 지정합니다.
   a. * 객체의 현재 버전 만료 *: 생성 후 특정 일 수 또는 특정 날짜에 모든 현재 객체를 영구적으로 사용할 수 없도록 규칙을 설정합니다. 만료된 개체 삭제 표식 삭제 * 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.
   b. * 현재 버전이 아닌 버전을 영구적으로 삭제 *: 현재 버전이 아닌 버전을 삭제할 일 수와 보관할 버전 수를 지정합니다.
   c. 만료된 개체 삭제 표식 삭제: 만료된 삭제 표식이 있는 개체를 삭제하려면 이 작업을 선택합니다. 만료된 삭제 표식은 연결된 현재 개체가 없는 삭제 표식입니다.

      이 옵션은 보존 기간 이후 모든 오브젝트를 자동으로 삭제하는 * 현재 버전의 오브젝트 만료 * 옵션을 선택하면 사용할 수 없습니다. 이 옵션은 개체 태그가 필터링에 사용되는 경우에도 사용할 수 없습니다.

   d. * 불완전한 다중 파트 업로드 삭제 *: 불완전한 다중 파트 업로드가 삭제되는 일 수를 설정합니다. 진행 중인 다중 파트 업로드가 지정된 보존 기간 내에 실패할 경우 불완전한 다중 파트 업로드를 삭제할 수 있습니다. 이 옵션은 개체 태그가 필터링에 사용되는 경우 사용할 수 없습니다.
   e. 저장 * 을 클릭합니다.

문서 수정 상태 규칙 불러오기

1. 스토리지 > Bucket * 을 클릭합니다.
2. 만료 규칙을 가져올 버킷을 선택합니다.
3. ⋮ 아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 추가 > 규칙 가져오기 * 를 클릭합니다.
5. 규칙을 가져올 버킷을 선택합니다. 선택한 버킷에 대해 정의된 수명 주기 관리 규칙이 나타납니다.
6. 가져올 규칙을 선택합니다. 한 번에 하나의 규칙을 선택할 수 있으며 기본 선택 항목이 첫 번째 규칙입니다.
7. 가져오기 * 를 클릭합니다.

규칙을 편집, 삭제 또는 비활성화합니다

규칙과 연결된 문서 수정 상태 관리 작업만 편집할 수 있습니다. 규칙이 객체 태그로 필터링된 경우 * 만료된 객체 삭제 마커 삭제 * 및 * 불완전한 다중 파트 업로드 삭제 * 옵션을 사용할 수 없습니다.

규칙을 삭제하면 해당 규칙이 이전에 연결된 개체에 더 이상 적용되지 않습니다.

1. 스토리지 > Bucket * 을 클릭합니다.
2. 수명주기 관리 규칙을 편집, 삭제 또는 비활성화할 버킷을 선택합니다.
3. ⋮ 아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 필요한 규칙을 선택합니다. 한 번에 하나의 규칙을 편집하고 사용하지 않도록 설정할 수 있습니다. 한 번에 여러 규칙을 삭제할 수 있습니다.
5. 편집 *, * 삭제 * 또는 * 비활성화 * 를 선택하고 절차를 완료합니다.

ONTAP S3 사용자를 생성합니다

특정 권한을 가진 S3 사용자를 생성합니다. 모든 ONTAP 개체 저장소에서 인증된 클라이언트로의 연결을 제한하려면 사용자 인증이 필요합니다.

시작하기 전에.

S3 지원 스토리지 VM이 이미 존재해야 합니다.

이 작업에 대해

S3 사용자에게 스토리지 VM의 모든 버킷에 대한 액세스 권한을 부여할 수 있습니다. S3 사용자를 생성할 때 사용자에 대한 액세스 키와 비밀 키도 생성됩니다. 객체 저장소 및 버킷 이름의 FQDN과 함께 사용자와 공유해야 합니다.

보안 강화를 위해 ONTAP 9.15.1부터 S3 사용자가 생성된 시점에만 액세스 키와 비밀 키가 표시되며 다시 표시할 수 없습니다. 키를 분실한 경우"새 키를 다시 생성해야 합니다".

버킷 정책 또는 오브젝트 서버 정책에서 S3 사용자에게 특정 액세스 권한을 부여할 수 있습니다.

ⓘ 새 오브젝트 저장소 서버를 만들면 ONTAP에서 루트 사용자(UID 0)를 생성합니다. 이 사용자는 모든 버킷에 액세스할 수 있는 권한이 있는 사용자입니다. NetApp에서는 ONTAP S3를 루트 사용자로 관리하는 대신 특정 권한으로 관리자 역할을 생성하는 것이 좋습니다.

CLI를 참조하십시오

1. S3 사용자 생성:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - 코멘트 추가는 선택 사항입니다.
   - ONTAP 9.14.1부터 에서 키가 유효한 기간을 정의할 수 있습니다 `-key-time-to-live` 매개 변수. 이 형식으로 보존 기간을 추가하여 액세스 키가 만료되는 기간을 표시할 수 있습니다.
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     예를 들어 1일, 2시간, 3분, 4초의 보존 기간을 입력하려면 값을 로 입력합니다 `P1DT2H3M4S`. 지정하지 않으면 이 키는 무기한 동안 유효합니다.

     아래 예는 이름을 가진 사용자를 생성합니다 `sm_user1` 있습니다 `vs0`키 보존 기간이 1주일로 설정되어 있습니다.

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. 액세스 키와 비밀 키를 저장해야 합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 클릭합니다. 사용자를 추가해야 하는 스토리지 VM을 선택하고 * Settings * 를 선택한 다음 S3 아래에서 를 클릭합니다 .
2. 사용자를 추가하려면 * 사용자 > 추가 * 를 클릭합니다.
3. 사용자의 이름을 입력합니다.
4. ONTAP 9.14.1부터 사용자에 대해 생성된 액세스 키의 보존 기간을 지정할 수 있습니다. 키가 자동으로 만료되는 일, 시간, 분 또는 초 단위로 보존 기간을 지정할 수 있습니다. 기본적으로 이 값은 로 설정됩니다 `0` 이는 키가 무기한 유효함을 나타냅니다.
5. 저장 * 을 클릭합니다. 사용자가 만들어지고 해당 사용자에 대한 액세스 키와 비밀 키가 생성됩니다.
6. 액세스 키와 비밀 키를 다운로드하거나 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

다음 단계

- S3 그룹을 생성하거나 수정합니다

ONTAP S3 사용자 그룹을 생성하거나 수정하여 버킷에 대한 액세스를 제어합니다

적절한 액세스 권한을 가진 사용자 그룹을 생성하여 버킷 액세스를 간소화할 수 있습니다.

시작하기 전에

S3 지원 SVM의 S3 사용자가 이미 존재해야 합니다.

이 작업에 대해

S3 그룹의 사용자는 SVM의 모든 버킷에 대한 액세스 권한을 부여할 수 있지만 여러 SVM에는 액세스할 수 없습니다. 그룹 액세스 권한은 다음 두 가지 방법으로 구성할 수 있습니다.

- 버킷 레벨에서

  S3 사용자 그룹을 생성한 후 버킷 정책 문에 그룹 권한을 지정하며 해당 버킷에만 적용됩니다.

- SVM 레벨에서

  S3 사용자 그룹을 생성한 후 그룹 정의에 오브젝트 서버 정책 이름을 지정합니다. 이러한 정책은 그룹 구성원에 대한 버킷 및 액세스를 결정합니다.

시스템 관리자

1. 스토리지 VM 편집: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다 .
2. 그룹 추가: * 그룹 * 을 선택한 다음 * 추가 * 를 선택합니다.
3. 그룹 이름을 입력하고 사용자 목록에서 선택합니다.
4. 기존 그룹 정책을 선택하거나 지금 추가하거나 나중에 정책을 추가할 수 있습니다.

CLI를 참조하십시오

1. S3 그룹 생성: 'vserver object-store-server group create-vserver_svm_name_-name_group_name_-users_user_name\(s\)*[-policies_policy_names*][-comment_text_\]' 객체 저장소에 하나의 버킷만 있는 구성에서는 '-policies' 옵션을 생략할 수 있으며 그룹 이름은 버킷 정책에 추가할 수 있습니다. '-policies' 옵션은 나중에 객체 스토리지 서버 정책을 생성한 후 'vserver object-store-server group modify' 명령을 사용하여 추가할 수 있습니다.

ONTAP S3 키를 재생성하고 보존 기간을 수정합니다

S3 클라이언트 액세스를 사용하도록 사용자를 생성하는 동안 액세스 키와 비밀 키가 자동으로 생성됩니다. 키가 만료되거나 손상된 경우 사용자의 키를 다시 생성할 수 있습니다.

선택키 생성에 대한 자세한 내용은 을 참조하십시오 "S3 사용자를 생성합니다".

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
2. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
3. 사용자 * 탭에서 액세스 키가 없거나 사용자의 키가 만료되었는지 확인합니다.
4. 키를 다시 생성해야 하는 경우 사용자 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다.
5. 기본적으로 생성된 키는 무기한으로 유효합니다. 9.14.1부터 키가 자동으로 만료되는 보존 기간을 수정할 수 있습니다. 보존 기간을 일, 시간, 분 또는 초로 입력합니다.
6. 저장 * 을 클릭합니다. 키가 재생성됩니다. 키 보존 기간의 변경 사항은 즉시 적용됩니다.
7. 액세스 키와 비밀 키를 다운로드하거나 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

CLI를 참조하십시오

1. 를 실행하여 사용자의 액세스 및 비밀 키를 다시 생성합니다 `vserver object-store-server user regenerate-keys` 명령.
2. 기본적으로 생성된 키는 무기한으로 유효합니다. 9.14.1부터 키가 자동으로 만료되는 보존 기간을 수정할 수 있습니다. 다음 형식으로 보존 기간을 추가할 수 있습니다.
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   예를 들어 1일, 2시간, 3분, 4초의 보존 기간을 입력하려면 값을 로 입력합니다 `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. 액세스 키와 비밀 키를 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

액세스 정책 문을 만들거나 수정합니다

ONTAP S3 버킷 및 오브젝트 저장소 서버 정책에 대해 알아보십시오

S3 리소스에 대한 사용자 및 그룹 액세스는 버킷 및 오브젝트 저장소 서버 정책에 의해 제어됩니다. 사용자 또는 그룹이 적은 경우 버킷 수준에서 액세스를 제어하는 것이 충분하지만 사용자 및 그룹이 많은 경우에는 오브젝트 저장소 서버 수준에서 액세스를 제어하는 것이 더 쉽습니다.

기본 **ONTAP S3** 버킷 정책에 액세스 규칙을 추가합니다

기본 버킷 정책에 액세스 규칙을 추가할 수 있습니다. 접근 제어의 범위는 포함된 버킷이므로 하나의 버킷이 있을 때 가장 적합합니다.

시작하기 전에

S3 서버와 버킷이 포함된 S3 지원 스토리지 VM이 이미 존재해야 합니다.

권한을 부여하기 전에 사용자 또는 그룹을 이미 만들어야 합니다.

이 작업에 대해

새 사용자와 그룹에 대한 새 문을 추가하거나 기존 문의 특성을 수정할 수 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket policy` "ONTAP 명령 참조입니다"을 참조하십시오.

사용자 및 그룹 권한은 버킷이 생성될 때 또는 나중에 필요할 때 부여할 수 있습니다. 버킷 용량과 QoS 정책 그룹 할당을 수정할 수도 있습니다.

ONTAP 9.9.1부터 ONTAP S3 서버에서 AWS 클라이언트 개체 태그 지정 기능을 지원하려는 경우 해당 작업이 수행됩니다 `GetObjectTagging`, `PutObjectTagging`, 및 `DeleteObjectTagging` 버킷 또는 그룹 정책을 사용하여 허용되어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

단계

1. 버킷 편집: * 저장소 > 버킷 * 을 클릭하고 원하는 버킷을 클릭한 다음 * 편집 * 을 클릭합니다. 사용 권한을 추가하거나 수정할 때 다음 매개 변수를 지정할 수 있습니다.
   - * Principal *: 액세스 권한이 부여된 사용자 또는 그룹입니다.
   - * 효과 *: 사용자 또는 그룹에 대한 액세스를 허용하거나 거부합니다.
   - * 조치 *: 주어진 사용자 또는 그룹에 대해 버킷에서 허용되는 작업.
   - * 리소스 *: 액세스가 부여되거나 거부되는 버킷 내의 객체 경로 및 이름입니다.

     기본값은 ***bucketname** * 및 ***bucketname/** * * 이며 버킷의 모든 개체에 대한 액세스를 허용합니다**.** 단일 개체에 대한 액세스 권한을 부여할 수도 있습니다**(**예**: ***bucketname/*_readme.txt**).

   - * 조건 * (선택 사항): 액세스를 시도할 때 계산되는 식입니다. 예를 들어, 액세스가 허용되거나 거부될 IP 주소 목록을 지정할 수 있습니다.

> ONTAP 9.14.1부터 * 리소스 * 필드에서 버킷 정책의 변수를 지정할 수 있습니다. 이러한 변수는 정책을 평가할 때 상황별 값으로 대체되는 자리 표시자입니다. 예를 들어, IF를 입력합니다 `${aws:username}` 이 정책에 대한 변수로 지정되면 이 변수가 요청 컨텍스트 사용자 이름으로 대체되고 해당 사용자에 대해 구성된 대로 정책 작업을 수행할 수 있습니다.

CLI를 참조하십시오

단계

1. 버킷 정책에 구문 추가:

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid text][-index integer]'

   다음 매개 변수는 액세스 권한을 정의합니다.

효과	이 문은 액세스를 허용하거나 거부할 수 있습니다
액션	모든 작업을 의미하는 ' * '를 지정하거나, GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl 중 하나 이상의 목록을 지정할 수 있습니다. ListBuckketMultpartUploads, ListMultipartUploadParts를 참조하십시오.

``원자''	하나 이상의 S3 사용자 또는 그룹 목록 • 최대 10명의 사용자 또는 그룹을 지정할 수 있습니다. • S3 Group을 지정한 경우 Group/group_name 형태의 그룹이어야 한다 • '*'는 공개 액세스를 의미하도록 지정할 수 있습니다. 즉, 액세스 키와 비밀 키 없이 액세스할 수 있습니다. • 보안 주체를 지정하지 않으면 스토리지 VM의 모든 S3 사용자에게 액세스 권한이 부여됩니다.
'-resource'	버킷과 버킷에 포함된 모든 물체 와일드카드 문자입니다 `*` 및 `?` 리소스를 지정하기 위한 정규식을 만드는 데 사용할 수 있습니다. 리소스의 경우 정책에 변수를 지정할 수 있습니다. 정책 변수는 정책을 평가할 때 컨텍스트 값으로 대체되는 자리 표시자입니다.

선택적으로 '-sid' 옵션을 사용하여 텍스트 문자열을 주석으로 지정할 수 있습니다.

예

다음 예에서는 객체 저장소 서버 사용자 user1의 readme 폴더에 대한 액세스를 허용하는 스토리지 VM svm1.example.com 및 bucket1에 대한 객체 저장소 서버 버킷 정책 문을 생성합니다.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

다음 예에서는 객체 저장소 서버 그룹 group1의 모든 객체에 대한 액세스를 허용하는 스토리지 VM svm1.example.com 및 bucket1에 대한 객체 저장소 서버 버킷 정책 문을 생성합니다.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

ONTAP 9.14.1부터 버킷 정책에 대한 변수를 지정할 수 있습니다. 다음 예에서는 스토리지 VM에 대한 서버 버킷 정책 설명을 생성합니다 `svm1` 및 `bucket1`, 및 은 지정합니다 `${aws:username}` 정책 리소스에 대한 변수로 사용됩니다. 정책이 평가되면 정책 변수가 요청 컨텍스트 사용자 이름으로 대체되고 해당 사용자에 대해 구성된 대로 정책 작업을 수행할 수 있습니다. 예를 들어, 다음 정책 문을 평가할 때 `${aws:username}` S3 작업을 수행하는 사용자로 대체됩니다. 사용자인 경우 `user1` 사용자에게 액세스 권한이 부여된 작업을 수행합니다 `bucket1` 현재 `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3 오브젝트 저장소 서버 정책을 생성하거나 수정합니다

오브젝트 저장소의 하나 이상의 버킷에 적용할 수 있는 정책을 생성할 수 있습니다. 오브젝트 저장소 서버 정책을 사용자 그룹에 연결할 수 있으므로 여러 버킷에서 리소스 액세스 관리를 간소화할 수 있습니다.

시작하기 전에

S3 서버와 버킷을 포함하는 S3 기반 SVM이 이미 존재해야 합니다.

이 작업에 대해

오브젝트 스토리지 서버 그룹에서 기본 정책 또는 사용자 지정 정책을 지정하여 SVM 레벨에서 액세스 정책을 활성화할 수 있습니다. 정책은 그룹 정의에 지정될 때까지 적용되지 않습니다.

> 개체 스토리지 서버 정책을 사용할 때는 정책 자체가 아니라 그룹 정의에서 보안 주체(사용자 및 그룹)를 지정합니다.

ONTAP S3 리소스에 액세스하기 위한 세 가지 읽기 전용 기본 정책이 있습니다.

- 전체 액세스
- NoS3액세스
- ReadOnlyAccess 를 참조하십시오

또한 새 사용자 지정 정책을 만든 다음 새 사용자 및 그룹에 대한 새 문을 추가하거나 기존 문의 특성을 수정할 수도 있습니다. 에 대한 자세한 내용은 `vserver object-store-server policy` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.9.1부터 ONTAP S3 서버에서 AWS 클라이언트 개체 태그 지정 기능을 지원하려는 경우 해당 작업이 수행됩니다 `GetObjectTagging`, `PutObjectTagging`, 및 `DeleteObjectTagging` 버킷 또는 그룹 정책을 사용하여 허용되어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 오브젝트 저장소 서버 정책을 생성하거나 수정합니다 *

단계

1. 스토리지 VM 편집: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다 .
2. 사용자 추가: * Policies * 를 클릭한 다음 * Add * 를 클릭합니다.
   a. 정책 이름을 입력하고 그룹 목록에서 선택합니다.
   b. 기존 기본 정책을 선택하거나 새 정책을 추가합니다.

      그룹 정책을 추가하거나 수정할 때 다음 매개 변수를 지정할 수 있습니다.

      - Group(그룹): 액세스 권한이 부여된 그룹입니다.
      - 효과: 하나 이상의 그룹에 대한 액세스를 허용하거나 거부합니다.
      - 조치: 주어진 그룹에 대해 하나 이상의 버킷에서 허용되는 조치.
      - 리소스: 액세스가 부여되거나 거부되는 하나 이상의 버킷 내에 있는 오브젝트의 경로 및 이름입니다. 예를 들면 다음과 같습니다.
        - * 스토리지 VM의 모든 버킷에 대한 액세스 권한을 부여합니다.
        - * bucketname * 및 * bucketname/** 특정 버킷의 모든 물체에 대한 액세스 권한을 부여합니다.
        - * bucketname/readme.txt * 특정 버킷의 개체에 대한 액세스 권한을 부여합니다.
   c. 필요한 경우 기존 정책에 구문을 추가합니다.

CLI를 참조하십시오

- CLI를 사용하여 오브젝트 저장소 서버 정책을 생성하거나 수정합니다 *

단계

1. 오브젝트 스토리지 서버 정책 생성:

   'vserver object-store-server policy create-vserver_svm_name_-policy_policy_name_[-comment_text_]'

2. 정책에 대한 문을 생성합니다.

   'vserver object-store-server policy statement create-vserver_svm_name_-policy_policy_name_-effect{allow|deny}-action_object_store_actions_-resource_object_store_resources_[sid text]'입니다

   다음 매개 변수는 액세스 권한을 정의합니다.

효과	이 문은 액세스를 허용하거나 거부할 수 있습니다

액션	모든 작업을 의미하는 ' * '를 지정하거나, GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl 중 하나 이상의 목록을 지정할 수 있습니다. ListAllMyBucket, ListBuckketMultpartUploads, ListMultipartUploadParts를 포함합니다.
'-resource'	버킷과 버킷에 포함된 모든 물체 와일드카드 문자 ' * '와 '?'입니다 리소스를 지정하기 위한 정규식을 구성하는 데 사용할 수 있습니다.

선택적으로 '-sid' 옵션을 사용하여 텍스트 문자열을 주석으로 지정할 수 있습니다.

기본적으로 새 문은 순서대로 처리되는 문 목록의 끝에 추가됩니다. 나중에 문을 추가하거나 수정할 때 문장의 '-index' 설정을 수정하여 처리 순서를 변경할 수 있습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP S3 액세스를 위한 외부 디렉토리 서비스를 구성합니다

ONTAP 9.14.1부터 외부 디렉토리용 서비스가 ONTAP S3 오브젝트 스토리지와 통합되었습니다. 이러한 통합은 외부 디렉터리 서비스를 통한 사용자 및 액세스 관리를 단순화합니다.

ONTAP 오브젝트 스토리지 환경에 대한 액세스 권한을 통해 외부 디렉토리 서비스에 속하는 사용자 그룹을 제공할 수 있습니다. LDAP(Lightweight Directory Access Protocol)는 ID 및 액세스 관리(IAM)를 위한 데이터베이스와 서비스를 제공하는 Active Directory와 같은 디렉터리 서비스와 통신하는 인터페이스입니다. 액세스를 제공하려면 ONTAP S3 환경에서 LDAP 그룹을 구성해야 합니다. 액세스를 구성하면 그룹 구성원에게 ONTAP S3 버킷에 대한 권한이 부여됩니다. LDAP에 대한 자세한 내용은 를 "ONTAP NFS SVM에서 LDAP 이름 서비스 사용에 대해 알아보세요 "참조하십시오.

또한 빠른 바인딩 모드에 맞게 Active Directory 사용자 그룹을 구성하여 사용자 자격 증명을 검증하고 LDAP 연결을 통해 타사 및 오픈 소스 S3 응용 프로그램을 인증할 수 있습니다.

시작하기 전에

LDAP 그룹을 구성하고 그룹 액세스를 위해 빠른 바인딩 모드를 활성화하기 전에 다음 사항을 확인하십시오.

1. S3 서버가 포함된 S3 사용 스토리지 VM이 생성되었습니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다".
2. 해당 스토리지 VM에 버킷이 생성되었습니다. 을 참조하십시오 "버킷을 만듭니다".
3. 스토리지 VM에 DNS가 구성되어 있다. 을 "DNS 서비스를 구성합니다"참조하십시오.
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 "SVM에 자체 서명된 루트 CA 인증서 설치"참조하십시오.
5. LDAP 클라이언트는 SVM에서 TLS를 사용하도록 구성했습니다. "ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성"및 을 "정보를 위해 ONTAP NFS SVM과 LDAP 클라이언트 구성을 연결합니다."참조하십시오.

LDAP에 대한 **S3** 액세스를 구성합니다

1. 그룹에 대한 SVM의 _NAME 서비스 데이터베이스_로 LDAP를 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAP 명령 참조에서 https://docs .NetApp.com/us-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html 명령 링크에 대해 자세히[`vserver services name-service ns-switch modify` 알아보십시오.

2. 를 사용하여 오브젝트 저장소 버킷 정책 문을 생성합니다 `principal` 액세스 권한을 부여할 LDAP 그룹으로 설정합니다.

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

예: 다음 예제에서는 에 대한 버킷 정책 문을 만듭니다 `buck1`. 이 정책은 LDAP 그룹에 대한 액세스를 허용합니다 `group1` 리소스(버킷 및 해당 객체)에 `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. LDAP 그룹의 사용자를 확인합니다 `group1` 는 S3 클라이언트에서 S3 작업을 수행할 수 있습니다.

인증에 **LDAP** 빠른 바인드 모드를 사용합니다

1. 그룹에 대한 SVM의 _NAME 서비스 데이터베이스_로 LDAP를 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAP 명령 참조에서 https://docs .NetApp.com/us-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html 명령 링크에 대해 자세히[`vserver services name-service ns-switch modify`

알아보십시오.

2. S3 버킷에 액세스하는 LDAP 사용자에게 버킷 정책에 정의된 권한이 있는지 확인합니다. 자세한 내용은 을 참조하십시오 "버킷 정책을 수정합니다".
3. LDAP 그룹의 사용자가 다음 작업을 수행할 수 있는지 확인합니다.
   a. S3 클라이언트의 액세스 키를 다음 형식으로 구성합니다 `"NTAPFASTBIND" + base64-encode(user-name:password)`. 예 `"NTAPFASTBIND"`: +base64-encode(ldapuser:password)
   `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      S3 클라이언트에서 비밀 키를 입력하라는 메시지가 표시될 수 있습니다. 비밀 키가 없으면 16자 이상의 암호를 입력할 수 있습니다.

   b. 사용자에게 권한이 있는 S3 클라이언트에서 기본 S3 작업을 수행합니다.

Base64 자격 증명

ONTAP S3의 기본 구성은 HTTP를 제외하며 HTTPS 및 TLS(전송 계층 보안) 연결만 사용합니다. ONTAP는 자체 서명된 인증서를 생성할 수 있지만 타사 CA(인증 기관)의 인증서를 사용하는 것이 좋습니다. CA 인증서를 사용할 때는 클라이언트 응용 프로그램과 ONTAP 개체 저장소 서버 간에 신뢰할 수 있는 관계를 만듭니다.

Base64로 인코딩된 자격 증명은 쉽게 디코딩됩니다. HTTPS를 사용하면 인코딩된 자격 증명이 중간자 패킷 스니퍼에 의해 캡처되지 않습니다.

사전 서명된 URL을 생성할 때 인증에 LDAP Fast-bind 모드를 사용하지 마십시오. 인증은 사전 서명된 URL에 포함된 Base64 액세스 키만을 기반으로 합니다. Base64 액세스 키를 디코딩하는 모든 사용자에게 사용자 이름과 암호가 표시됩니다.

인증 방법은 **nsswitch**이고 **LDAP**가 설정된 예입니다

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다.

Active Directory 또는 **SMB** 서버에 대한 **S3** 액세스 구성

버킷 정책 문에 지정된 nasgroup 또는 nasgroup에 속한 사용자에게 UID 및 GID가 설정되지 않은 경우 이러한 특성을 찾을 수 없으면 조회가 실패합니다. Active Directory는 UID가 아닌 SID를 사용합니다. SID 항목을 UID에 매핑할 수 없는 경우 필요한 데이터를 ONTAP로 가져와야 합니다.

그렇게 하려면 SVM이 Active Directory로 인증되고 필요한 사용자 및 그룹 정보를 가져올 수 있도록 을 "SVM active-directory create 를 참조하십시오"사용하십시오.

또는 를 사용하여 "SVM CIFS 생성"Active Directory 도메인에 SMB 서버를 생성합니다.

네임 서버와 개체 저장소에 서로 다른 도메인 이름을 사용하는 경우 조회 실패가 발생할 수 있습니다. 조회 실패를 방지하기 위해 NetApp UPN 형식의 리소스 권한 부여에 신뢰할 수 있는 도메인을 사용할 것을 권장합니다. `nasgroup/group@trusted_domain.com` 신뢰할 수 있는 도메인은 SMB 서버의 신뢰할 수 있는 도메인 목록에 추가된 도메인입니다. 방법을 알아보세요. "선호하는 신뢰할 수 있는 도메인을 추가, 제거 및 수정합니다." SMB 서버 목록에서.

인증 방법이 도메인이고 신뢰할 수 있는 도메인이 **Active Directory**에 구성된 경우 키를 생성합니다

`s3/services/<svm_uuid>/users`UPN 형식으로 지정된 사용자가 있는 끝점을 사용합니다. 예:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다.

인증 방법이 도메인이고 신뢰할 수 있는 도메인이 없는 경우 키를 생성합니다

이 작업은 LDAP가 비활성화되어 있거나 POSIX 사용자가 UID 및 GID를 구성하지 않은 경우에 가능합니다. 예:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다. 신뢰할 수 있는 도메인이 없는 경우 사용자 이름에 선택적 도메인 값(@FQDN)만 추가하면 됩니다.

LDAP 또는 도메인 사용자가 자신의 **ONTAP S3** 액세스 키를 생성할 수 있습니다

ONTAP 9.14.1부터 ONTAP 관리자는 사용자 지정 역할을 만들고 로컬 또는 도메인 그룹이나 LDAP(Lightweight Directory Access Protocol) 그룹에 부여하여 해당 그룹에 속한 사용자가 S3 클라이언트 액세스에 대한 자체 액세스 및 비밀 키를 생성할 수 있습니다.

액세스 키 생성을 위해 API를 호출하는 사용자에게 사용자 지정 역할을 생성하고 할당할 수 있도록 스토리지 VM에서 몇 가지 구성 단계를 수행해야 합니다.

LDAP가 비활성화된 경우 다음을 수행할 수 있습니다. "ONTAP S3 액세스를 위한 외부 디렉토리 서비스 구성" 사용자가 액세스 키를 생성할 수 있도록 합니다.

시작하기 전에

다음을 확인합니다.

1. S3 서버가 포함된 S3 사용 스토리지 VM이 생성되었습니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다".
2. 해당 스토리지 VM에 버킷이 생성되었습니다. 을 참조하십시오 "버킷을 만듭니다".
3. 스토리지 VM에 DNS가 구성되어 있다. 을 "DNS 서비스를 구성합니다"참조하십시오.
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 "SVM에 자체 서명된 루트 CA 인증서 설치"참조하십시오.
5. LDAP 클라이언트는 스토리지 VM에서 TLS를 사용하도록 구성했습니다. 을 "ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성"참조하십시오.
6. 클라이언트 구성을 SVM에 연결합니다. 을 "ONTAP NFS SVM과 LDAP 클라이언트 구성 연결"참조하십시오. 에 대한 자세한 내용은 `vserver services name-service ldap create` "ONTAP 명령 참조입니다"을 참조하십시오.
7. 데이터 스토리지 VM을 사용하는 경우 관리 네트워크 인터페이스(LIF) 및 VM에 그리고 LIF에 대한 서비스 정책을 생성합니다. 및 `network interface service-policy create` 에 대한 자세한 `network interface create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

액세스 키 생성을 위한 사용자를 구성합니다

예 **3.** 단계

LDAP 사용자

1. LDAP를 스토리지 VM의 _NAME 서비스 데이터베이스_로 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

에 대한 자세한 내용은 `vserver services name-service ns-switch modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. S3 사용자 REST API 끝점에 액세스하여 사용자 지정 역할 생성:
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
이 예에서 는 입니다 `s3-role` 스토리지 VM의 사용자에 대해 역할이 생성됩니다 `svm-1`, 모든 액세스 권한, 읽기, 만들기 및 업데이트가 부여되는 대상.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

에 대한 자세한 내용은 `security login rest-role create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. LDAP 사용자 그룹을 만듭니다. `security login` 명령을 실행하고 S3 사용자 REST API 엔드포인트에 액세스하기 위한 새로운 사용자 지정 역할을 추가합니다. 자세히 알아보세요 `security login create` 에서 "ONTAP 명령 참조입니다" .

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

이 예에서는 LDAP 그룹입니다 `ldap-group-1` 이(가) 에 생성됩니다 `svm-1`및 사용자 지정 역할 `s3role` API 끝점에 액세스할 수 있도록 이 API에 추가되고, 빠른 바인드 모드에서 LDAP 액세스가 활성화됩니다.

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

자세한 내용은 을 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다 ."참조하십시오.

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

LDAP 그룹에 사용자 정의 역할을 추가하면 해당 그룹의 사용자는 ONTAP 에 제한된 액세스 권한을 가질 수 있습니다. `/api/protocols/s3/services/{svm.uuid}/users` 엔드포인트. API를 호출하면 LDAP 그룹 사용자는 S3 클라이언트에 액세스하기 위한 액세스 키와 비밀 키를 직접 생성할 수 있습니다. 키는 본인만 생성할 수 있으며 다른 사용자는 생성할 수 없습니다.

도메인 사용자

1. S3 사용자 REST API 엔드포인트에 액세스할 수 있는 사용자 지정 역할을 만듭니다.

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

이 예에서는 `s3-role` 스토리지 VM의 사용자에 대한 역할이 생성됩니다. `svm-1` 모든 접근 권한(읽기, 만들기, 업데이트)이 부여됩니다.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

에 대한 자세한 내용은 `security login rest-role create` "ONTAP 명령 참조입니다"을 참조하십시오.

1. 도메인 사용자 그룹을 만듭니다. `security login` 명령을 실행하고 S3 사용자 REST API 엔드포인트에 액세스하기 위한 새로운 사용자 지정 역할을 추가합니다. 자세히 알아보세요 `security login create` 에서 "ONTAP 명령 참조입니다" .

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   이 예에서 도메인 그룹은 `domain\group1` 에서 생성됩니다 `svm-1` , 그리고 사용자 정의 역할 `s3role` API 엔드포인트에 액세스하기 위해 추가되었습니다.

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

도메인 그룹에 사용자 정의 역할을 추가하면 해당 그룹의 사용자가 ONTAP 에 제한적으로 액세스할 수 있습니다. `/api/protocols/s3/services/{svm.uuid}/users` 엔드포인트. API를 호출하면 도메인 그룹 사용자는 S3 클라이언트에 액세스하기 위한 액세스 키와 비밀 키를 직접 생성할 수 있습니다. 해당 키는 본인만 생성할 수 있으며 다른 사용자는 생성할 수 없습니다.

S3 또는 LDAP 사용자로 자체 액세스 키를 생성합니다

ONTAP 9.14.1부터 관리자가 사용자 고유의 키를 생성하는 역할을 부여한 경우, S3 클라이언트에 액세스하기 위한 고유한 액세스 및 비밀 키를 생성할 수 있습니다. 다음 ONTAP REST API 끝점을 사용하여 자신에 대해서만 키를 생성할 수 있습니다.

S3 사용자를 생성하고 키를 생성합니다**.**

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다. 이 엔드포인트에 대한 자세한 내용은 참조를 참조하세요. "API 설명서" .

HTTP 메소드	경로
게시	/api/protocols/s3/services/{svm.uuid}/사용자

도메인 사용자의 경우 S3 사용자 이름에 다음 형식을 사용하세요. `user@fqdn` , 어디 `fqdn` 도메인의 정규화된 도메인 이름입니다.

컬의 예

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON 출력 예

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3 사용자에 대한 키 재생성

S3 사용자가 이미 있는 경우 해당 사용자의 액세스 키와 비밀 키를 다시 생성할 수 있습니다. 이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
반점	/api/프로토콜/s3/서비스/{svm.uuid}/사용자/{이름}

컬의 예

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON 출력 예

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3 오브젝트 스토리지에 대한 클라이언트 액세스 지원

원격 **FabricPool** 계층화에 대해 **ONTAP S3** 액세스를 설정합니다

ONTAP S3를 원격 FabricPool 용량(클라우드) 계층으로 사용하려면 ONTAP S3 관리자가 원격 ONTAP 클러스터 관리자에게 S3 서버 구성에 대한 정보를 제공해야 합니다.

이 작업에 대해

FabricPool 클라우드 계층을 구성하려면 다음 S3 서버 정보가 필요합니다.

- 서버 이름(FQDN)
- 버킷 이름
- CA 인증서
- 액세스 키
- 암호(암호 액세스 키)

또한 다음과 같은 네트워킹 구성이 필요합니다.

- DNS 서버에 S3 서버의 FQDN 이름과 LIF의 IP 주소를 포함하여 admin SVM용으로 구성된 원격 ONTAP S3 서버의 호스트 이름에 대한 항목이 있어야 합니다.
- 클러스터 피어링이 필요하지 않더라도 로컬 클러스터에 인터클러스터 LIF를 구성해야 합니다.

ONTAP S3를 클라우드 계층으로 구성하는 방법에 대한 FabricPool 설명서를 참조하십시오.

"FabricPool를 사용하여 스토리지 계층 관리"

로컬 **FabricPool** 계층화에 대해 **ONTAP S3** 액세스를 설정합니다

ONTAP S3를 로컬 FabricPool 용량 계층으로 사용하려면 생성한 버킷을 기반으로 오브젝트 저장소를 정의한 다음 오브젝트 저장소를 성능 계층 애그리게이트에 연결하여 FabricPool를 생성해야 합니다.

시작하기 전에

ONTAP S3 서버 이름과 버킷 이름이 있어야 하며, 클러스터 LIF("-vserver Cluster" 매개 변수)를 사용하여 S3 서버를 생성해야 합니다.

이 작업에 대해

오브젝트 저장소 구성에는 S3 서버, 버킷 이름 및 인증 요구사항을 비롯한 로컬 용량 계층에 대한 정보가 포함됩니다.

생성한 오브젝트 저장소 구성은 다른 오브젝트 저장소 또는 버킷과 다시 연관해서는 안 됩니다. 로컬 계층에 대해 여러 개의 버킷을 생성할 수 있지만, 단일 버킷에 여러 오브젝트 저장소를 생성할 수는 없습니다.

로컬 용량 계층에는 FabricPool 라이센스가 필요하지 않습니다.

단계

1. 로컬 용량 계층에 대한 객체 저장소 생성:

   '스토리지 집계 객체 저장 구성 create-object-store-name_store_name_-IPSpace 클러스터 공급자 유형 ONTAP_S3-server_name_-container-name_bucket_name_-access-key_access-secret-password password"

   - container-name은 사용자가 만든 S3 버킷입니다.
   - '-access-key' 파라미터는 ONTAP S3 서버에 대한 요청을 승인한다.
   - secret-password 매개 변수(secret access key)는 ONTAP S3 서버에 대한 요청을 인증합니다.
   - '-is-certificate-validation-enabled' 매개 변수를 'false'로 설정하여 ONTAP S3에 대한 인증서 확인을 비활성화할 수 있습니다.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. 오브젝트 저장소 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config show'를 선택합니다

3. 선택 사항 "비활성 데이터 보고를 사용하여 볼륨의 비활성 데이터 양을 결정합니다":.

   볼륨의 비활성 데이터 양을 보면 FabricPool 로컬 계층화에 사용할 애그리게이트를 결정할 수 있습니다.

4. 오브젝트 저장소를 Aggregate에 연결합니다.

   'STORAGE 집계 객체-STORE ATTACH-AGGATE_AGGr_NAME_-OBJECT-STORE-NAME_STORE_NAME_'

'allow-flexgroup * true *' 옵션을 사용하면 FlexGroup 볼륨 구성요소를 포함하는 애그리게이트를 연결할 수 있습니다.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. 오브젝트 저장소 정보를 표시하고 첨부된 오브젝트 저장소를 사용할 수 있는지 확인합니다.

'스토리지 골재 오브젝트 저장소 쇼'

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

관련 정보

- "저장소 집계 객체-저장소 연결"
- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체-저장소 구성 표시"
- "저장소 집계 객체-저장소 표시"

S3 클라이언트 애플리케이션이 **ONTAP S3** 서버에 액세스하도록 설정

S3 클라이언트 애플리케이션에서 ONTAP S3 서버에 액세스하려면 ONTAP S3 관리자가 S3 사용자에게 구성 정보를 제공해야 합니다.

시작하기 전에

S3 클라이언트 앱은 다음 AWS 서명 버전을 사용하여 ONTAP S3 서버를 인증할 수 있어야 합니다.

- 서명 버전 4, ONTAP 9.8 이상
- 서명 버전 2, ONTAP 9.11.1 이상

다른 서명 버전은 ONTAP S3에서 지원되지 않습니다.

ONTAP S3 관리자는 버킷 정책 또는 오브젝트 스토리지 서버 정책에서 S3 사용자를 생성하고 개별 사용자 또는 그룹 구성원으로 액세스 권한을 부여해야 합니다.

S3 클라이언트 앱은 ONTAP S3 서버 이름을 확인할 수 있어야 합니다. 이 경우 ONTAP S3 관리자가 S3 서버 LIF의 S3 서버 이름(FQDN) 및 IP 주소를 제공해야 합니다.

이 작업에 대해

ONTAP S3 버킷에 액세스하려면 S3 클라이언트 애플리케이션의 사용자가 ONTAP S3 관리자가 제공하는 정보를 입력합니다.

ONTAP 9.9.1부터 ONTAP S3 서버는 다음 AWS 클라이언트 기능을 지원합니다.

- 사용자 정의 개체 메타데이터

  PUT(또는 POST)를 사용하여 개체를 만들 때 키 값 쌍 집합을 메타데이터로 할당할 수 있습니다. 개체에 대해 가져오기/헤드 작업을 수행하면 사용자 정의 메타데이터가 시스템 메타데이터와 함께 반환됩니다.

- 개체 태그 지정

  객체 분류에 대한 태그로 별도의 키 값 쌍 세트를 할당할 수 있습니다. 메타데이터와 달리 태그는 오브젝트와 독립적으로 REST API를 사용하여 생성되고 읽혀지며, 오브젝트가 만들어지거나 그 이후에 언제든지 구현됩니다.

> ⓘ 클라이언트가 태그 정보를 가져오고 넣을 수 있도록 하려면 버킷 또는 그룹 정책을 사용하여 GetObjectTagging, PutObjectTagging, DeleteObjectTagging 등의 작업을 허용해야 합니다.

자세한 내용은 AWS S3 설명서를 참조하십시오.

단계

1. S3 서버 이름과 CA 인증서를 입력하여 ONTAP S3 서버로 S3 클라이언트 앱을 인증합니다.
2. 다음 정보를 입력하여 S3 클라이언트 앱에서 사용자를 인증합니다.
   - S3 서버 이름(FQDN) 및 버킷 이름입니다
   - 사용자의 액세스 키 및 암호 키입니다

ONTAP S3 스토리지 서비스 레벨

ONTAP에는 해당 최소 성능 요소에 매핑된 사전 정의된 스토리지 서비스가 포함되어 있습니다.

클러스터 또는 SVM에서 사용 가능한 실제 스토리지 서비스 세트는 SVM에서 애그리게이트를 구성하는 스토리지 유형에 따라 결정됩니다.

다음 표에는 최소 성능 요소가 사전 정의된 스토리지 서비스에 매핑되는 방식이 나와 있습니다.

스토리지 서비스	예상 **IOPS(SLA)**	최대 **IOPS(SLO)**	최소 볼륨 **IOPS**	예상 지연 시간	예상 **IOPS**가 적용됩니까**?**
값	TB당 128개	TB당 512개	75를	17ms	AFF: 예 그렇지 않으면 아니오
성능	TB당 2048개	TB당 4096	500입니다	2ms	예
익스트림	TB당 6144	12288/TB	1000입니다	1ms	예

다음 표에는 각 미디어 또는 노드 유형에 대해 사용 가능한 스토리지 서비스 수준이 정의되어 있습니다.

미디어 또는 노드	사용 가능한 스토리지 서비스 수준입니다
디스크	값
가상 머신 디스크	값
하이브리드	값
최적의 용량을 제공하는 플래시	값
솔리드 스테이트 드라이브(SSD) - 비 AFF	값
최적의 성능을 발휘하는 플래시-SSD(AFF)	최고의 성능, 가치

ONTAP S3 버킷을 위한 CORS(Cross-Origin Resource Sharing)를 구성합니다

ONTAP 9.16.1부터 CORS(Cross-Origin Resource Sharing)를 구성하여 다른 도메인의 클라이언트 웹 애플리케이션이 ONTAP 버킷을 액세스할 수 있도록 할 수 있습니다. 이렇게 하면 웹 브라우저를 사용하여 버킷 객체에 안전하게 액세스할 수 있습니다.

CORS는 HTTP를 기반으로 하는 프레임워크로, 한 웹 페이지에 정의된 스크립트가 다른 도메인의 서버에 있는 리소스에 액세스할 수 있도록 합니다. 프레임워크는 웹 보안의 초기 기반인 _same-origin policy_를 안전하게 우회하는 데 사용됩니다. 주요 개념 및 용어에 대한 설명은 아래에 나와 있습니다.

원점

오리진은 리소스의 위치와 ID를 정확하게 정의합니다. 이 값은 다음 값의 조합으로 표시됩니다.

- URI 체계(프로토콜)
- 호스트 이름(도메인 이름 또는 IP 주소)
- 포트 번호입니다

원점의 간단한 예는 다음과 같습니다 `https://www.mycompany.com:8001`. 오리진이 CORS와 함께 사용될 때 요청을 하는 클라이언트를 식별합니다.

동일한 원본 정책입니다

SOP(동일 원본 정책)는 브라우저 기반 스크립트에 적용되는 보안 개념 및 제한 사항입니다. 이 정책은 두 페이지가 동일한 원본에 있는 경우 웹 페이지에서 처음 로드된 스크립트가 다른 페이지의 데이터에 액세스할 수 있도록 합니다. 이 제한 사항은 악성 스크립트가 다른 오리진 페이지의 데이터에 액세스하는 것을 방지합니다.

일반적인 **CORS** 사용 사례

CORS에는 몇 가지 일반적인 사용 사례가 있습니다. 대부분의 경우 도메인 간 인증뿐만 아니라 AJAX 요청, 글꼴 로드, 스타일시트 및 스크립트와 같이 도메인 간 액세스의 잘 정의된 인스턴스가 포함됩니다. CORS는 단일 페이지 애플리케이션(SPA)의 일부로 구현할 수도 있습니다.

HTTP 헤더

CORS는 HTTP 요청 및 응답에 삽입된 헤더를 사용하여 구현됩니다. 예를 들어, 액세스 제어를 구현하고 메서드와 헤더를 포함하여 허용되는 작업을 나타내는 몇 가지 응답 헤더가 있습니다. HTTP 요청에 _Origin_header가 있으면

도메인 간 요청으로 정의됩니다. 오리진 값은 CORS 서버에서 유효한 CORS 구성을 찾는 데 사용됩니다.

HTTP 사전 전송 요청

서버가 특정 메서드 및 헤더를 포함하여 CORS를 지원하는지 여부를 초기에 확인하기 위한 선택적 요청입니다. 응답에 따라 CORS 요청을 완료할 수도 있고 완료할 수도 없습니다.

ONTAP 버킷

버킷은 잘 정의된 네임스페이스를 기반으로 저장 및 액세스하는 오브젝트의 컨테이너입니다. ONTAP 버킷에는 두 가지 유형이 있습니다.

- NAS 및 S3 프로토콜을 통해 액세스할 수 있는 NAS 버킷입니다
- S3 프로토콜을 통해서만 액세스할 수 있는 S3 버킷

ONTAP에서의 **CORS** 구현

CORS는 ONTAP 9.16.1 이상 릴리즈에서 기본적으로 사용됩니다. 활성화할 각 SVM에서 CORS를 구성해야 합니다.

ONTAP 클러스터에 대해 CORS를 사용하지 않도록 설정하는 관리 옵션은 없습니다. 그러나 규칙을 정의하지 않거나 기존 규칙을 모두 삭제하여 이 규칙을 효과적으로 비활성화할 수 있습니다.

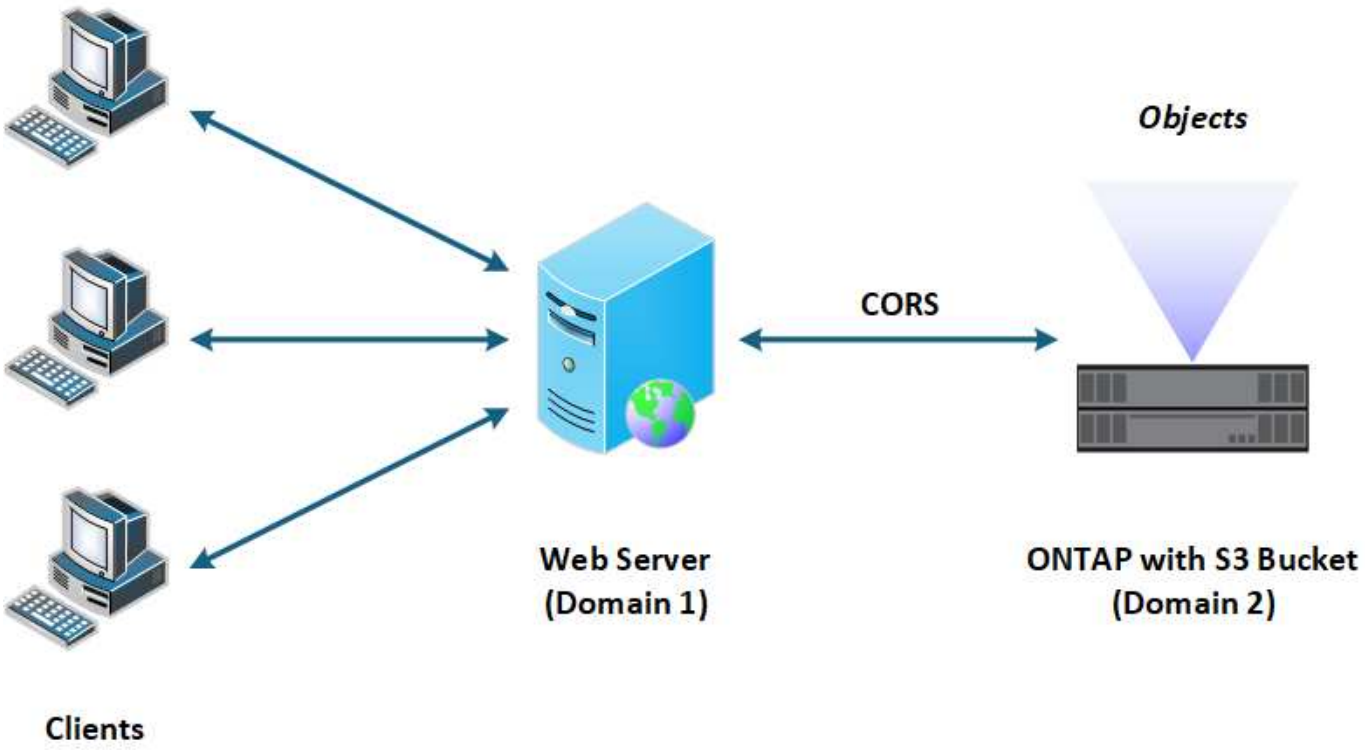
가능한 사용 사례

ONTAP CORS 구현은 도메인 간 리소스 액세스를 위한 다음과 같은 몇 가지 가능한 토폴로지를 지원합니다.

- ONTAP S3 버킷(동일하거나 다른 SVM 또는 클러스터 내부)
- ONTAP NAS 버킷(동일하거나 다른 SVM 또는 클러스터 내)
- ONTAP S3 및 NAS 버킷(동일하거나 다른 SVM 또는 클러스터 내)
- ONTAP 버킷 및 외부 공급업체 버킷
- 다양한 시간대의 버킷

개략적인 보기

다음은 CORS에서 ONTAP S3 버킷에 대한 액세스를 지원하는 방법을 개략적으로 보여 줍니다.



CORS 규칙 정의

이 기능을 활성화하고 사용하려면 ONTAP에서 CORS 규칙을 정의해야 합니다.

구성 작업

ONTAP에서 지원되는 세 가지 기본 구성 규칙 동작은 다음과 같습니다.

- 표시
- 생성
- 삭제

ONTAP에 정의된 CORS 규칙에는 SVM과 버킷은 물론 허용된 오리진, 메서드 및 헤더를 포함한 여러 속성이 있습니다.

관리 옵션

ONTAP 클러스터에서 CORS를 관리할 때 사용할 수 있는 몇 가지 옵션이 있습니다.

ONTAP 명령줄 인터페이스입니다

명령줄 인터페이스를 사용하여 CORS를 구성할 수 있습니다. 자세한 내용은 을 CLI를 사용하여 CORS 관리 참조하십시오.

ONTAP REST API를 참조하십시오

ONTAP REST API를 사용하여 CORS를 구성할 수 있습니다. CORS 기능을 지원하기 위해 추가된 새 끝점이 없습니다. 대신 다음과 같은 기존 끝점을 사용할 수 있습니다.

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

자세한 내용은 을 "ONTAP 자동화 설명서"참조하십시오.

S3 API를 사용합니다

S3 API를 사용하여 ONTAP 버킷에서 CORS 구성을 생성하고 삭제할 수 있습니다. S3 클라이언트 관리자는 다음을 비롯하여 충분한 Privileges가 필요합니다.

- 액세스 또는 비밀 키 자격 증명
- s3api를 통한 액세스를 허용하도록 버킷에 구성된 정책입니다

업그레이드 및 되돌리기

CORS를 사용하여 ONTAP S3 버킷을 액세스하려는 경우 몇 가지 관리 문제를 알고 있어야 합니다.

업그레이드 중

모든 노드가 9.16.1로 업그레이드되면 CORS 기능이 지원됩니다. 혼합 모드 클러스터에서 이 기능은 유효 클러스터 버전(ECV)이 9.16.1 이상일 때만 사용할 수 있습니다.

되돌리기

사용자 관점에서 클러스터 복원을 진행하기 전에 모든 CORS 구성을 제거해야 합니다. 내부적으로 이 작업은 모든 CORS 데이터베이스를 삭제합니다. 이러한 데이터 구조를 지우고 되돌리는 명령을 실행하라는 메시지가 표시됩니다.

CLI를 사용하여 **CORS** 관리

ONTAP CLI를 사용하여 CORS 규칙을 관리할 수 있습니다. 주요 작업은 아래에 설명되어 있습니다. CORS 명령을 실행하려면 ONTAP * admin * 권한 수준이어야 합니다.

생성

명령을 사용하여 CORS 규칙을 정의할 수 `vserver object-store-server bucket cors-rule create` 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket cors-rule create` "ONTAP 명령 참조입니다"을 참조하십시오.

매개 변수

규칙을 만드는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`vserver`	규칙이 생성되는 오브젝트 저장소 서버 버킷을 호스팅하는 SVM(SVM)의 이름을 지정합니다.

매개 변수	설명
bucket	규칙이 생성되는 오브젝트 저장소 서버의 버킷 이름입니다.
index	규칙이 생성되는 개체 저장소 서버 버킷의 인덱스를 나타내는 선택적 매개 변수입니다.
rule id	오브젝트 저장소 서버 버킷 규칙의 고유 식별자입니다.
allowed-origins	오리진 간 요청이 출발할 수 있는 오리진 목록입니다.
allowed-methods	오리진 간 요청에서 허용되는 HTTP 메서드 목록입니다.
allowed-headers	크로스 오리진 요청에서 허용되는 HTTP 헤더 목록입니다.
expose-headers	고객이 애플리케이션에서 액세스할 수 있는 CORS 응답에 보내는 추가 헤더 목록입니다.
max-age-in-seconds	브라우저가 특정 리소스에 대해 비행 전 응답을 캐시해야 하는 시간을 지정하는 선택적 매개 변수입니다.

예

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

표시

명령을 사용하여 현재 규칙 및 해당 내용의 목록을 표시할 수 `vserver object-store-server bucket cors-rule show` 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket cors-rule show` "ONTAP 명령 참조입니다"을 참조하십시오.

매개 변수를 포함하면 `-instance` 각 규칙에 대해 제공되는 데이터가 확장됩니다. 원하는 필드를 지정할 수도 있습니다.

예

```
server object-store-server bucket cors-rule show -instance
```

삭제

delete 명령을 사용하여 CORS 규칙의 인스턴스를 제거할 수 있습니다. `index`규칙 값이 필요하므로 이 작업은 다음 두 단계로 수행됩니다.

1. `show`명령을 실행하여 규칙을 표시하고 해당 인덱스를 검색합니다.

2. 인덱스 값을 사용하여 삭제를 실행합니다.

예

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

수정

기존 CORS 규칙을 수정하는 데 사용할 수 있는 CLI 명령이 없습니다. 규칙을 수정하려면 다음을 수행해야 합니다.

1. 기존 규칙을 삭제합니다.
2. 원하는 옵션을 사용하여 새 규칙을 만듭니다.

SnapMirror S3로 버킷 보호

ONTAP SnapMirror S3에 대해 알아보십시오

ONTAP 9.10.1부터 SnapMirror 미러링 및 백업 기능을 사용하여 ONTAP S3 오브젝트 저장소의 버킷을 보호할 수 있습니다. 표준 SnapMirror와 달리 SnapMirror S3를 통해 AWS S3와 같은 비 NetApp 대상에 대한 미러링 및 백업을 수행할 수 있습니다.

SnapMirror S3는 ONTAP S3 버킷에서 다음 대상에 이르는 액티브 미러 및 백업 계층을 지원합니다.

타겟	액티브 미러 및 테이크오버 지원	백업 및 복원을 지원합니까?
ONTAP S3 • 버킷이 동일한 SVM에 포함됩니다 • 동일한 클러스터에서 서로 다른 SVM의 버킷 • SVM의 다양한 클러스터에서 버킷	예	예
StorageGRID	아니요	예
설치하고	아니요	예
Azure용 Cloud Volumes ONTAP	예	예
AWS 환경을 위한 Cloud Volumes ONTAP	예	예
Google Cloud용 Cloud Volumes ONTAP	예	예

ONTAP S3 서버에서 기존 버킷을 보호하거나 데이터 보호를 즉시 활성화할 수 있는 새로운 버킷을 생성할 수 있습니다.

SnapMirror S3 요구사항

- ONTAP 버전입니다

  소스 및 대상 클러스터에서 ONTAP 9.10.1 이상이 실행되고 있어야 합니다.

SnapMirror S3는 MetroCluster 구성에서 지원되지 않습니다.

- 라이센싱

  에서 사용할 수 있는 라이센스는 다음과 같습니다 "ONTAP 1 을 참조하십시오" ONTAP 소스 및 대상 시스템에서 다음 항목에 대한 액세스를 제공하려면 소프트웨어 제품군이 필요합니다.

  - ONTAP S3 프로토콜 및 스토리지
  - SnapMirror S3에서 다른 NetApp 오브젝트 저장소 타겟(ONTAP S3, StorageGRID, Cloud Volumes ONTAP) 공략
  - SnapMirror S3에서 AWS S3(에서 사용 가능"ONTAP One 호환성 번들")를 비롯한 타사 오브젝트 저장소 공략
  - 클러스터에서 ONTAP 9.10.1을 실행 중인 "FabricPool 라이센스"경우 가 필요합니다.
- ONTAP S3
  - ONTAP S3 서버에서 소스 및 타겟 SVM을 실행해야 합니다.
  - TLS 액세스를 위한 CA 인증서를 S3 서버를 호스팅하는 시스템에 설치하는 것이 좋지만 반드시 필요한 것은 아닙니다.
    - S3 서버의 인증서를 서명하는 데 사용되는 CA 인증서는 S3 서버를 호스팅하는 클러스터의 관리 스토리지 VM에 설치해야 합니다.
    - 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.
    - 소스 또는 대상 스토리지 VM이 HTTPS에서 수신 대기 중이 아닌 경우 CA 인증서를 설치할 필요가 없습니다.
- 피어링(ONTAP S3 타겟용)
  - 인터클러스터 LIF를 구성해야 하며(원격 ONTAP 대상용), 소스 및 대상 클러스터의 인터클러스터 LIF가 소스 및 대상 S3 서버 데이터 LIF에 연결할 수 있습니다.
  - 소스 및 타겟 클러스터를 피어링했습니다(원격 ONTAP 타겟의 경우).
  - 소스 및 타겟 스토리지 VM을 모든 ONTAP 타겟에 대해 피어링했습니다.
- SnapMirror 정책
  - 모든 SnapMirror S3 관계에 S3별 SnapMirror 정책이 필요하지만 여러 관계에 동일한 정책을 사용할 수 있습니다.
  - 사용자 고유의 정책을 만들거나 다음 값을 포함하는 기본 * 연속 * 정책을 사용할 수 있습니다.
    - 스로틀(처리량/대역폭의 상한) - 무제한
    - 복구 지점 목표 시간: 1시간(3600초)

SnapMirror 관계에 있는 두 개의 S3 버킷이 있을 때 개체의 현재 버전이 만료(삭제됨)되도록 라이프사이클 정책이 구성된 경우 동일한 작업이 파트너 버킷에 복제된다는 것을 알아야 합니다. 파트너 버킷이 읽기 전용 또는 패시브 인 경우에도 마찬가지입니다.

- 루트 사용자 키 SnapMirror S3 관계에 필요한 스토리지 VM 루트 사용자 액세스 키는 ONTAP에서 기본적으로 할당하지 않습니다. SnapMirror S3 관계를 처음 생성할 때 소스 및 대상 스토리지 VM에 키가 있는지 확인해야 하며, 키가 없으면 키를 다시 생성해야 합니다. 다시 생성해야 하는 경우 액세스 및 암호 키 쌍을 사용하는 모든 클라이언트 및 모든 SnapMirror 오브젝트 저장소 구성을 새 키로 업데이트해야 합니다.

S3 서버 구성에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "스토리지 VM에서 S3 서버를 활성화합니다"
- "ONTAP S3 구성 프로세스 정보"

클러스터 및 스토리지 VM 피어링에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "미러링 및 보관 준비(System Manager, 1-6단계)"
- "클러스터 및 SVM 피어링(CLI)"

지원되는 **SnapMirror** 관계

SnapMirror S3는 팬아웃 및 캐스케이드 관계를 지원합니다. 개요는 다음을 참조하세요. "팬아웃 및 캐스케이드 데이터 보호 구축" .

SnapMirror S3는 팬인 구축(여러 소스 버킷과 단일 대상 버킷 간의 데이터 보호 관계)을 지원하지 않습니다. SnapMirror S3는 여러 클러스터에서 단일 보조 클러스터로 여러 버킷 미러를 지원할 수 있지만 각 소스 버킷에는 보조 클러스터에 자체 대상 버킷이 있어야 합니다.

SnapMirror S3는 MetroCluster 환경에서 지원되지 않습니다.

S3 버킷에 대한 액세스 제어

새 버킷을 생성할 때 사용자 및 그룹을 생성하여 액세스를 제어할 수 있습니다.

SnapMirror S3는 소스 버킷에서 타겟 버킷으로 오브젝트를 복제하지만 소스 오브젝트 저장소의 사용자, 그룹 및 정책을 타겟 오브젝트 저장소로 복제하지 않습니다.

페일오버 이벤트 중에 클라이언트가 대상 버킷에 액세스할 수 있도록 대상 오브젝트 저장소에서 사용자, 그룹 정책, 권한 및 유사한 구성 요소를 구성해야 합니다.

대상 클러스터에서 사용자가 생성될 때 소스 키를 수동으로 제공하는 경우 소스 및 대상 사용자가 동일한 액세스 및 암호 키를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

자세한 내용은 다음 항목을 참조하십시오.

- "S3 사용자 및 그룹 추가(System Manager)"
- "S3 사용자 생성(CLI)"
- "S3 그룹 생성 또는 수정(CLI)"

SnapMirror S3에서 **S3** 오브젝트 잠금 및 버전 관리를 사용합니다

오브젝트 잠금 및 버전 관리가 활성화된 ONTAP 버킷에서 SnapMirror S3를 사용할 수 있으며 다음과 같은 몇 가지 사항을 고려해야 합니다.

- 오브젝트 잠금이 설정된 상태로 소스 버킷을 복제하려면 대상 버킷에도 오브젝트 잠금이 설정되어 있어야 합니다.

또한 소스와 대상 모두에 버전 관리가 활성화되어 있어야 합니다. 이렇게 하면 두 버킷의 기본 보존 정책이 서로 다른 경우 삭제 내용을 대상 버킷에 미러링할 필요가 없습니다.

- S3 SnapMirror는 오브젝트의 기간별 버전을 복제하지 않습니다. 개체의 현재 버전만 복제됩니다.

Object Locked 객체가 대상 버킷으로 미러링되면 원래 보존 시간이 유지됩니다. 잠금 해제된 객체가 복제되면 대상 버킷의 기본 보존 기간이 적용됩니다. 예를 들면 다음과 같습니다.

- 버킷 A의 기본 보존 기간은 30일이고 버킷 B의 기본 보존 기간은 60일입니다. Bucket A에서 Bucket B로 복제된 객체는 Bucket B의 기본 보존 기간보다 작더라도 30일 보존 기간을 유지합니다
- 버킷 A에는 기본 보존 기간이 없고 버킷 B에는 기본 보존 기간이 60일입니다. 잠금 해제된 객체가 버킷 A에서 버킷 B로 복제되면 60일의 보존 기간이 적용됩니다. 객체가 Bucket A에서 수동으로 잠길 경우 Bucket B로 복제될 때 원래 보존 기간이 유지됩니다
- 버킷 A의 기본 보존 기간은 30일이고 버킷 B의 기본 보존 기간은 없습니다. 버킷 A에서 버킷 B로 복제된 객체는 30일의 보존 기간을 유지합니다.

원격 클러스터의 미러링 및 백업 보호

원격 클러스터에서 새로운 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

새로운 S3 버킷을 생성하면 원격 클러스터의 SnapMirror S3 대상으로 즉시 보호할 수 있습니다.

이 작업에 대해

소스 시스템과 대상 시스템 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 스토리지 VM을 편집하여 사용자를 추가하고 소스 및 대상 스토리지 VM 모두에서 사용자를 그룹에 추가하려면 다음을 수행합니다.

   스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM, * 설정 * 을 차례로 클릭한 다음 S3를 클릭합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값(*bucketname, bucketname/* *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) 활성화 * 를 선택합니다. 그런 다음 다음 다음 값을 입력합니다.

- 목적지
  - * 대상: ONTAP 시스템 *
  - * 클러스터 *: 원격 클러스터를 선택합니다.
  - * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서: * destination_certificate의 내용을 복사하여 붙여 넣습니다.

5. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
6. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
7. 저장 * 을 클릭합니다. 소스 스토리지 VM에 새 버킷이 생성되면 대상 스토리지 VM을 생성한 새 버킷에 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성

   'vserver object-store-server user show'를 선택합니다

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 다음을 입력합니다.

   'vserver object-store-server user reenate-keys-vserver svm_name-user_root_'

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 소스 및 타겟 SVM 모두에 버킷 생성:

   'vserver object-store-server bucket create-vserver svm_name-bucket bucket_name[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 소스 및 타겟 SVM의 기본 버킷 정책에 액세스 규칙을 추가합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-

principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다. `snapmirror policy create -vserver` *`svm_name`* `-policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   매개 변수:

   - 유형 `continuous` - SnapMirror S3 관계에 대한 유일한 정책 유형입니다(필수).
   - `-rpo` - 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - `-throttle` - 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 서버 인증서 설치:

   a. 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_src_admin_svm*-cert-name_dest_server_certificate_'

   b. 대상 클러스터에서 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_dest_admin_svm*-cert-name_src_server_certificate_'

      외부 CA 공급업체에서 서명한 인증서를 사용하는 경우, 소스 및 대상 관리 SVM에 동일한 인증서를 설치합니다.

   에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

   '스냅미러 create-source-path_src_svm_name_:/bucket/*bucket_name*-destination -path_dest_peer_svm_name_:/bucket/*bucket_name*,…} [-policy policy_name]'입니다

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

예

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

원격 클러스터에서 기존 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷을 보호할 수 있습니다.

이 작업에 대해

소스 및 대상 클러스터 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 미러 관계를 생성할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 선택한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 기존 사용자 및 그룹이 존재하고 소스 및 대상 스토리지 VM 모두에서 올바른 액세스 권한이 있는지 확인합니다. * 스토리지 > 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다. 마지막으로 * S3 * 타일을 찾아 를 선택하고 * 사용자 * 탭을 선택한 다음 * 그룹 * 탭을 선택하여 사용자 및 그룹 액세스 설정을 확인합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
   a. 보호 > 개요 * 를 선택한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 을 선택한 다음 * 추가 * 를 클릭합니다.
   c. 정책 이름과 설명을 입력합니다.
   d. 클러스터 또는 SVM에서 정책 범위를 선택합니다.
   e. SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
   f. 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal and Effect *: 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 *: 다음 값이 표시되는지 확인하십시오.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 *: 기본값(*bucketname, bucketname/* *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3 보호로 기존 버킷 보호:
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 보호 * 를 클릭하고 다음 값을 입력합니다.

- 목적지
  - * 대상 *: ONTAP 시스템
  - * 클러스터 *: 원격 클러스터를 선택합니다.
  - * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서 *: _destination_certificate의 내용을 복사하여 붙여 넣습니다.

6. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
7. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
8. 저장 * 을 클릭합니다. 기존 버킷은 대상 스토리지 VM의 새 버킷으로 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우, 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우
   `vserver object-store-server user show` 루트 사용자 키를 다시 생성하십시오. + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 이 없으면 다음을 입력합니다
   `vserver object-store-server user regenerate-keys -vserver` *`svm_name`* `-user` *`root`*. + 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 대상 SVM에서 미러 타겟으로 사용할 버킷을 생성합니다.

   'vserver object-store-server bucket create-vserver_svm_name_-bucket_dest_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 기본 버킷 정책의 액세스 규칙이 소스 및 타겟 SVM에서 모두 올바른지 확인합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다.

   '스냅샷 정책 생성 - vserver svm_name - policy policy_name - type continuous [-RPO_integer_] [-throttle_throttle_type_] [-comment_text_] [*additional_options*]'

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 인증서 설치:

   a. 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_src_admin_svm*-cert-name_dest_server_certificate_'

   b. 대상 클러스터에서 *SOURCE_S3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_dest_admin_svm*-cert-name_src_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 소스 및 대상 SVM 관리자에 동일한 인증서를 설치합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

   '스냅미러 create-source-path_src_svm_name_:/bucket/*bucket_name*-destination-path dest_peer_svm_name:/bucket/*bucket_name*,…} [-policy policy_name]'입니다

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

원격 클러스터의 대상 **ONTAP S3** 버킷에서 테이크오버합니다

소스 버킷의 데이터를 사용할 수 없는 경우 SnapMirror 관계를 중단하여 대상 버킷에 대한 쓰기 가능 및 데이터 제공을 시작할 수 있습니다.

이 작업에 대해

테이크오버 작업이 수행되면 소스 버킷이 읽기 전용으로 전환되고 원래 타겟 버킷은 읽기-쓰기로 변환되어 SnapMirror S3 관계를 반대로 전환합니다.

비활성화된 소스 버킷을 다시 사용할 수 있게 되면 SnapMirror S3는 두 버킷의 컨텐츠를 자동으로 다시 동기화합니다. 볼륨 SnapMirror 구축에 필요한 것처럼 관계를 명시적으로 재동기화할 필요는 없습니다.

테이크오버 작업은 원격 클러스터에서 시작되어야 합니다.

SnapMirror S3는 소스 버킷에서 타겟 버킷으로 오브젝트를 복제하지만 소스 오브젝트 저장소의 사용자, 그룹 및 정책을 타겟 오브젝트 저장소로 복제하지 않습니다.

페일오버 이벤트 중에 클라이언트가 대상 버킷에 액세스할 수 있도록 대상 오브젝트 저장소에서 사용자, 그룹 정책, 권한 및 유사한 구성 요소를 구성해야 합니다.

대상 클러스터에서 사용자가 생성될 때 소스 키를 수동으로 제공하는 경우 소스 및 대상 사용자가 동일한 액세스 및 암호 키를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

시스템 관리자

사용할 수 없는 버킷에서 페일오버 및 데이터 서비스 시작:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 클릭하고 * 페일오버 * 를 선택한 다음 * 페일오버 * 를 클릭합니다.

CLI를 참조하십시오

1. '스냅미러 페일오버 시작-목적지-PATH_svm_name_:/bucket/*bucket_name*' 대상 버킷에 대한 페일오버 작업을 시작합니다
2. 페일오버 작업의 상태 '스냅샷 표시 - 필드 상태'를 확인합니다

   예

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

관련 정보

- "S3 사용자 및 그룹 추가(System Manager)"
- "S3 사용자 생성(CLI)"
- "S3 그룹 생성 또는 수정(CLI)"
- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

원격 클러스터의 타겟 **SVM**에서 **ONTAP S3** 버킷을 복원합니다

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 오브젝트를 복원하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용된 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

복구 작업은 원격 클러스터에서 시작해야 합니다.

시스템 관리자

백업된 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
     - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준.
       을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - destination_s3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

잠긴 버킷을 복원합니다

ONTAP 9.14.1부터 잠긴 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

오브젝트 잠김 버킷은 새 버킷이나 기존 버킷으로 복원할 수 있습니다. 다음과 같은 시나리오에서 오브젝트 잠금 버킷을 대상으로 선택할 수 있습니다.

- * 새 버킷으로 복원 * : 오브젝트 잠금이 활성화된 경우, 버킷을 생성하여 오브젝트 잠금이 활성화된 버킷을 복원할 수 있습니다. 잠긴 버킷을 복원하면 원래 버킷의 오브젝트 잠금 모드와 보존 기간이 복제됩니다. 새 버킷에 대해 다른 잠금 보존 기간을 정의할 수도 있습니다. 이 보존 기간은 다른 소스의 잠기지 않은 개체에 적용됩니다.
- * 기존 버킷으로 복원 *: 기존 버킷에서 버전 관리 및 유사한 오브젝트 잠금 모드가 활성화되어 있는 한 오브젝트 잠금 버킷을 기존 버킷으로 복원할 수 있습니다. 원래 버킷의 보존 기간이 유지됩니다.
- * 비잠금 버킷 복원 * : 버킷에서 오브젝트 잠금이 활성화되지 않은 경우에도 오브젝트 잠금이 활성화되어 있고 소스 클러스터에 있는 버킷으로 복원할 수 있습니다. 버킷을 복원하면 잠기지 않은 모든 객체가 잠기며 대상 버킷의 보존 모드 및 기간을 적용할 수 있습니다.

CLI를 참조하십시오

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 "새 ONTAP S3 버킷에 대한 클라우드 백업 관계를 생성한다"참조하십시오.
2. 대상 버킷에 대한 복원 작업을 시작합니다. '스냅미러 복구 - 소스 - path_svm_name_:/bucket/*bucket_name* - destination-path_svm_name_:/bucket/*bucket_name*'

예

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

로컬 클러스터의 미러링 및 백업 보호

로컬 클러스터에서 새로운 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

새로운 S3 버킷을 생성하면 동일한 클러스터의 SnapMirror S3 대상으로 즉시 보호할 수 있습니다. 다른 스토리지 VM의 버킷이나 소스와 동일한 스토리지 VM의 버킷에 데이터를 미러링할 수 있습니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 및 대상 스토리지 VM 사이에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 S3 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 스토리지 VM을 편집하여 사용자를 추가하고 사용자를 그룹에 추가하려면 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값 '(버켓 이름, 버켓 이름/ *)' 또는 필요한 기타 값을 사용합니다

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
   d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) 활성화 * 를 선택합니다. 그런 다음 다음 다음 값을 입력합니다.
      - 목적지

        - * 대상 *: ONTAP 시스템
        - * 클러스터 *: 로컬 클러스터를 선택합니다.
        - * 스토리지 VM *: 로컬 클러스터에서 스토리지 VM을 선택합니다.
        - * S3 서버 CA 인증서 *: 소스 인증서의 내용을 복사하여 붙여 넣습니다.
    - 출처
        - * S3 서버 CA 인증서 *: 대상 인증서의 내용을 복사하여 붙여 넣습니다.
5. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
6. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
7. 저장 * 을 클릭합니다. 소스 스토리지 VM에 새 버킷이 생성되면 대상 스토리지 VM을 생성한 새 버킷에 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성
   `vserver object-store-server user show`

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 'vserver object-store-server user reenate-keys-vserver_svm_name_-user_root_'를 입력합니다

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 소스 및 타겟 SVM 모두에 버킷 생성:

   'vserver object-store-server bucket create-vserver svm_name-bucket bucket_name[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 소스 및 타겟 SVM의 기본 버킷 정책에 액세스 규칙을 추가합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. 관리 SVM에 CA 서버 인증서 설치:
   a. 관리 SVM에 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_src_server_certificate_'
   b. 관리 SVM에 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_dest_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우에는 관리 SVM에 이 인증서를 설치해야 합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 관계 생성:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
   -policy test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

로컬 클러스터에서 기존 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 동일한 클러스터에서 기존 S3 버킷을 보호할 수 있습니다. 다른 스토리지 VM의 버킷이나 소스와 동일한 스토리지 VM의 버킷에 데이터를 미러링할 수 있습니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 및 대상 스토리지 VM 사이에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오
2. 기존 사용자 및 그룹이 존재하고 소스 및 대상 스토리지 VM 모두에서 올바른 액세스 권한이 있는지 확인합니다. * 스토리지 > 스토리지 VM을 선택하고 * 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다. 마지막으로 * S3 * 타일을 찾아 를 선택하고 * 사용자 * 탭을 선택한 다음 * 그룹 * 탭을 선택하여 사용자 및 그룹 액세스 설정을 확인합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. 기존 버킷의 버킷 접근 정책이 고객의 요구를 지속적으로 충족하는지 확인합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값(버켓 이름, 버켓 이름/ *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3로 기존 버킷 보호:
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 보호 * 를 클릭하고 다음 값을 입력합니다.

- 목적지
  - * 대상 *: ONTAP 시스템
  - * 클러스터 *: 로컬 클러스터를 선택합니다.
  - * 스토리지 VM *: 동일하거나 다른 스토리지 VM을 선택하십시오.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서 *: _destination_certificate의 내용을 복사하여 붙여 넣습니다.

6. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
7. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
8. 저장 * 을 클릭합니다. 기존 버킷은 대상 스토리지 VM의 새 버킷으로 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성
   `vserver object-store-server user show`

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 'vserver object-store-server user reenate-keys-vserver_svm_name_-user_root_'를 입력합니다

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 대상 SVM에서 미러 타겟으로 사용할 버킷을 생성합니다.

   'vserver object-store-server bucket create-vserver_svm_name_-bucket_dest_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 기본 버킷 정책에 대한 액세스 규칙이 소스 및 타겟 SVM에서 모두 올바른지 확인합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.

   '스냅샷 정책 생성 - vserver_svm_name_-policy_policy_name - type continuous [-RPO_integer_] [-throttle_throttle_type_] [-comment text] [*additional_options*]'

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 관리 SVM에 CA 서버 인증서 설치:

   a. 관리 SVM에 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_src_server_certificate_'

   b. 관리 SVM에 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_dest_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우에는 관리 SVM에 이 인증서를 설치해야 합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 관계 생성:
   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

로컬 클러스터의 타겟 **ONTAP S3** 버킷에서 테이크오버합니다

소스 버킷의 데이터를 사용할 수 없는 경우 SnapMirror 관계를 중단하여 대상 버킷에 대한 쓰기 가능 및 데이터 제공을 시작할 수 있습니다.

이 작업에 대해

테이크오버 작업이 수행되면 소스 버킷이 읽기 전용으로 전환되고 원래 타겟 버킷은 읽기-쓰기로 변환되어 SnapMirror S3 관계를 반대로 전환합니다.

비활성화된 소스 버킷을 다시 사용할 수 있게 되면 SnapMirror S3는 두 버킷의 컨텐츠를 자동으로 다시 동기화합니다. 표준 볼륨 SnapMirror 배포에 필요하므로 관계를 명시적으로 다시 동기화할 필요는 없습니다.

대상 버킷이 원격 클러스터에 있는 경우 원격 클러스터에서 테이크오버 작업을 시작해야 합니다.

시스템 관리자

사용할 수 없는 버킷에서 페일오버 및 데이터 서비스 시작:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 클릭하고 * 페일오버 * 를 선택한 다음 * 페일오버 * 를 클릭합니다.

CLI를 참조하십시오

1. '스냅미러 페일오버 시작-목적지-PATH_svm_name_:/bucket/*bucket_name*' 대상 버킷에 대한 페일오버 작업을 시작합니다
2. 페일오버 작업의 상태 '스냅샷 표시 - 필드 상태'를 확인합니다

예

'clusterA:::> SnapMirror 페일오버 start-destination-path vs1:/bucket/test-bucket-mirror'

관련 정보

- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

로컬 클러스터의 타겟 **SVM**에서 **ONTAP S3** 버킷을 복원합니다

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 오브젝트를 복원하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용된 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

복구 작업은 로컬 클러스터에서 시작해야 합니다.

시스템 관리자

백업 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 버킷을 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
4. 대상 S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준.
       을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - 대상 S3 서버 CA 인증서의 내용.
5. 대상 * 에서 소스 S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
6. 보호 * > 관계 를 클릭하여 복원 진행률을 모니터링합니다.

잠긴 버킷을 복원합니다

ONTAP 9.14.1부터 잠긴 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

오브젝트 잠김 버킷은 새 버킷이나 기존 버킷으로 복원할 수 있습니다. 다음과 같은 시나리오에서 오브젝트 잠금 버킷을 대상으로 선택할 수 있습니다.

- * 새 버킷으로 복원 * : 오브젝트 잠금이 활성화된 경우, 버킷을 생성하여 오브젝트 잠금이 활성화된 버킷을 복원할 수 있습니다. 잠긴 버킷을 복원하면 원래 버킷의 오브젝트 잠금 모드와 보존 기간이 복제됩니다. 새 버킷에 대해 다른 잠금 보존 기간을 정의할 수도 있습니다. 이 보존 기간은 다른 소스의 잠기지 않은 개체에 적용됩니다.
- * 기존 버킷으로 복원 *: 기존 버킷에서 버전 관리 및 유사한 오브젝트 잠금 모드가 활성화되어 있는 한 오브젝트 잠금 버킷을 기존 버킷으로 복원할 수 있습니다. 원래 버킷의 보존 기간이 유지됩니다.
- * 비잠금 버킷 복원 * : 버킷에서 오브젝트 잠금이 활성화되지 않은 경우에도 오브젝트 잠금이 활성화되어 있고 소스 클러스터에 있는 버킷으로 복원할 수 있습니다. 버킷을 복원하면 잠기지 않은 모든 객체가 잠기며 대상 버킷의 보존 모드 및 기간을 적용할 수 있습니다.

CLI를 참조하십시오

1. 오브젝트를 새 버킷으로 복원하는 경우 새 버킷을 생성합니다. 자세한 내용은 을 "새 ONTAP S3 버킷에 대한 클라우드 백업 관계를 생성한다"참조하십시오.
2. 대상 버킷에 대한 복원 작업을 시작합니다. '스냅미러 복구 - 소스 - path_svm_name_:/bucket/*bucket_name* - destination-path_svm_name_:/bucket/*bucket_name*'

예

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

클라우드 타겟을 통한 백업 보호

ONTAP SnapMirror S3 클라우드 타겟 관계 요구사항

소스 및 타겟 환경이 클라우드 타겟에 대한 SnapMirror S3 백업 보호 요구사항을 충족하는지 확인하십시오.

데이터 버킷에 액세스하려면 오브젝트 저장소 공급자의 유효한 계정 자격 증명이 있어야 합니다.

클러스터를 클라우드 오브젝트 저장소에 연결하려면 먼저 클러스터에서 인터클러스터 LIF 및 IPspace를 구성해야 합니다. 로컬 스토리지의 데이터를 클라우드 오브젝트 저장소로 원활하게 전송하려면 각 노드에 대한 인터클러스터 LIF를 생성해야 합니다.

StorageGRID 대상의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

또한 StorageGRID 서버 인증서에 서명하는 데 사용되는 CA 인증서는 ONTAP S3 클러스터의 관리 스토리지 VM에 다음을 사용하여 설치해야 합니다. `security certificate install` 명령. 자세한 내용은 "CA 인증서를 설치하는 중입니다"StorageGRID 사용 여부 를 참조하십시오.

AWS S3 타겟의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

ONTAP 클러스터의 관리 스토리지 VM용 DNS 서버는 FQDN(사용되는 경우)을 IP 주소로 확인할 수 있어야 합니다.

관련 정보

- "보안 인증서 설치"

새 **ONTAP S3** 버킷에 대한 클라우드 백업 관계를 생성한다

새로운 S3 버킷을 생성하면 객체 저장소 공급자(StorageGRID 시스템 또는 Amazon S3 배포)의 SnapMirror S3 대상 버킷에 즉시 백업할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- • 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 스토리지 VM을 편집하여 사용자를 추가하고 사용자를 그룹에 추가합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM, * 설정 * 을 차례로 클릭한 다음 * S3 * 아래를 클릭합니다 .

      을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음 * Amazon S3 * 또는 * StorageGRID * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
      - * Principal * and * Effect *: 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 적용합니다.
      - * 조치 *: 다음 값이 표시되는지 확인하십시오.

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- * 리소스 : 필요한 기본값 **_(bucketname, bucketname/)** 또는 기타 값을 사용합니다.

  을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) * 를 선택하고 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 소스 스토리지 VM에 새 버킷이 생성되고 클라우드 오브젝트 저장소에 백업됩니다.

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우
   `vserver object-store-server user show` 루트 사용자 키를 재생성합니다. + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 이 없으면 다음을 입력합니다
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`. + 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 소스 SVM에서 버킷을 생성합니다. 'vserver object-store-server bucket create-vserver_svm_name_-bucket_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'
3. 기본 버킷 정책에 액세스 규칙을 추가합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_][-index_integer_integer

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수: * `type continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수). * `-rpo` – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항). `-throttle`* – 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 서버 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 대상 오브젝트 저장소 정의:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   매개 변수: * `-object-store-name` – 로컬 ONTAP 시스템에 있는 개체 저장소 대상의 이름입니다. `-usage*` – `data` 이 워크플로에 사용합니다. * `-provider-type` – `AWS_S3` 및 `SGWS` (StorageGRID) 타겟이 지원됩니다. `-server*` – 대상 서버의 FQDN 또는 IP 주소입니다. `-is-ssl-enabled*` – SSL 활성화는 선택 사항이지만 권장됩니다. + 에서 에 대해 자세히 `snapmirror object-store config create` "ONTAP 명령 참조입니다"알아보십시오.

   예

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS
   -server sgws.example.com -container-name target-test-bucket -is-ssl
   -enabled true -port 443 -access-key abc123 -secret-password xyz890
   ```

7. SnapMirror S3 관계 생성:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   매개 변수:
   * `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
   를 누릅니다
   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path sgws-store:/objstore -policy test-policy
   ```

8. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

기존 **ONTAP S3** 버킷에 대한 클라우드 백업 관계를 생성한다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷 백업을 시작할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 사용자 및 그룹이 올바르게 정의되었는지 확인합니다. * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3를 클릭합니다 .

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. →보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
   c. 정책 이름과 설명을 입력합니다.
   d. 정책 범위, 클러스터 또는 SVM을 선택합니다
   e. SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
   f. 스로틀 * 및 * 복구 지점 목표 값 * 을 입력합니다.
3. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음, StorageGRID Webscale * 용 * Amazon S3 * 또는 * 기타 * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * Actions * - GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl, ListBuckketMultipartUploads, ListMultiPartUploadParts 등의 값이 표시되는지 확인합니다
      - * 리소스 * - 기본값(*(버켓 이름, 버켓 이름/ *)* 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3를 사용하여 버킷 백업:

a. 스토리지 * > * 버킷 * 을 클릭한 다음 백업할 버킷을 선택합니다.

b. 보호 * 를 클릭하고 * 대상 * 에서 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 기존 버킷이 클라우드 오브젝트 저장소로 백업됩니다.

CLI를 참조하십시오

1. 기본 버킷 정책의 액세스 규칙이 올바른지 확인합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_integer']

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수: * `type continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수). * `-rpo` – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항). `-throttle`* – 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

   에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

4. SnapMirror S3 대상 오브젝트 저장소 정의:
   `snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   매개 변수: * `-object-store-name` – 로컬 ONTAP 시스템에 있는 개체 저장소 대상의 이름입니다. `-usage`* – `data` 이 워크플로에 사용합니다. * `-provider-type` – `AWS_S3` 및 `SGWS` (StorageGRID)

타겟이 지원됩니다. `-server`* – 대상 서버의 FQDN 또는 IP 주소입니다. `-is-ssl-enabled`* – SSL 활성화는 선택 사항이지만 권장됩니다. + 에서 에 대해 자세히 `snapmirror object-store config create` "ONTAP 명령 참조입니다"알아보십시오.

예

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. SnapMirror S3 관계 생성:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

매개 변수:
* `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
를 누릅니다
생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

클라우드 타겟에서 **ONTAP S3** 버킷 복원

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 복구하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

시스템 관리자

백업 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
     - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준. 을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - 대상 S3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

CLI 절차

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 참조하십시오 "버킷에 대한 백업 관계 생성(클라우드 타겟)".
2. 대상 버킷에 대한 복구 작업을 시작합니다.
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   예

   다음 예에서는 대상 버킷을 기존 버킷으로 복원합니다.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror S3 정책을 수정합니다

RPO 및 스로틀 값을 조정하려는 경우 S3 SnapMirror 정책을 수정할 수 있습니다.

시스템 관리자

1. 보호 > 관계 * 를 클릭한 다음 수정할 관계에 대한 보호 정책을 선택합니다.
2. 정책 이름 옆에 있는 을 ⋮ 클릭한 다음 * 편집 * 을 클릭합니다.

CLI를 참조하십시오

SnapMirror S3 정책 수정:

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

매개 변수:

- `-rpo`: 복구 지점 목표의 시간을 초 단위로 지정합니다.
- `-throttle`: 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

관련 정보

- "스냅미러 정책 수정"

스냅샷으로 **S3** 데이터를 보호합니다

ONTAP S3 스냅샷에 대해 자세히 알아보십시오

ONTAP 9.16.1부터 ONTAP 스냅샷 기술을 사용하여 ONTAP S3 버킷의 읽기 전용 시점 이미지를 생성할 수 있습니다.

S3 스냅샷 기능을 사용하면 스냅샷을 수동으로 생성하거나 스냅샷 정책을 통해 스냅샷을 자동으로 생성할 수 있습니다. S3 스냅샷은 S3 클라이언트에 S3 버킷으로 제공됩니다. S3 클라이언트를 통해 스냅샷에서 콘텐츠를 찾아보고 복원할 수 있습니다.

ONTAP 9.16.1에서 S3 스냅샷은 S3 버킷의 현재 버전만 캡처합니다. 최신 버전이 아닌 버킷을 S3 스냅샷에서 캡처하지 않습니다. 또한 스냅샷 생성 후 객체 태그가 수정되면 시점 객체 태그가 스냅샷에 캡처되지 않습니다.

S3 스냅샷은 클러스터 시간을 기준으로 합니다. 시간을 동기화하려면 클러스터에서 NTP 서버를 구성해야 합니다. 자세한 내용은 을 "클러스터 시간을 관리합니다"참조하십시오.

할당량 및 공간 사용량

할당량은 S3 버킷에 사용되는 오브젝트 수와 논리적 크기를 추적합니다. S3 스냅샷이 생성될 때 스냅샷이 파일 시스템에서 삭제될 때까지 S3 스냅샷에서 캡처된 오브젝트는 사용된 버킷 오브젝트 수 및 크기에 계산됩니다.

다중 파트 개체

멀티 파트 객체의 경우 최종 객체만 스냅샷에 캡처됩니다. 다중 부분 객체의 부분 업로드는 스냅샷에 캡처되지 않습니다.

버전 및 비버전 버킷의 스냅샷

버전 및 비버전 버킷 모두에서 스냅샷을 생성할 수 있습니다. 스냅숏은 스냅숏이 캡처될 때 현재 개체 버전만 포함합니다.

버전 관리된 버킷 및 스냅샷

오브젝트 버전 관리가 활성화된 버킷에서 스냅샷은 스냅샷이 생성된 후 가장 최근의 오브젝트 버전의 콘텐츠를 유지합니다. 버킷에서 비최신 버전은 제외됩니다.

이 예에서는 오브젝트 버전 관리가 활성화된 버킷에서 오브젝트에 `obj1` v1, v2, v3, v4, v5가 있습니다. v3(캡처 시점에 가장 최근 버전)에서 `obj1` 스냅샷을 `snap1` 생성했습니다. 브라우징 시 `snap1` `obj1` v3에 생성된 컨텐츠가 있는 객체로 표시됩니다. 이전 버전의 콘텐츠는 반환되지 않습니다.

스냅샷이 삭제될 때까지 현재 버전이 아닌 버전은 파일 시스템에 유지됩니다.

비버전 버킷 및 스냅샷

버전이 지정되지 않은 버킷에서 S3 스냅샷은 스냅샷 생성 전에 최신 커밋의 내용을 유지합니다.

다음 예를 들어 개체 버전 관리를 사용할 수 없는 버킷에서 (T1, T2, T3, T4 및 T5)에서 개체를 `obj1` 여러 번 덮어썼습니다. T3와 T4 사이에 S3 스냅샷을 `snap1` 생성했습니다. 브라우징 시 `snap1` `obj1` T3에서 생성된 컨텐츠와 함께 가 나타납니다.

개체 만료 및 스냅샷

ONTAP S3 오브젝트 만료 및 S3 스냅샷 기능은 서로 독립적으로 작동합니다. ONTAP 오브젝트 만료 기능은 S3 버킷에 정의된 라이프사이클 관리 규칙에 따라 오브젝트 버전을 만료한다. S3 스냅샷은 스냅샷이 생성된 시점의 버킷 객체의 정적 복사본입니다.

버킷에서 오브젝트 버전 관리를 사용하는 경우, 해당 버킷에 정의된 만료 규칙으로 인해 특정 버전의 오브젝트가 삭제되면 만료된 오브젝트 버전의 콘텐츠가 하나 이상의 S3 스냅샷에서 현재 버전으로 캡처된 경우 파일 시스템에 계속 남아 있습니다. 해당 객체 버전은 해당 스냅샷이 삭제될 때만 파일 시스템에 더 이상 존재하지 않습니다.

마찬가지로, 버전 관리가 비활성화된 버킷에서 만료 규칙에 따라 오브젝트가 삭제되지만 일부 기존 S3 스냅샷에서 오브젝트가 캡처된 경우 해당 오브젝트는 파일 시스템에 유지됩니다. 객체를 캡처하는 스냅샷이 삭제되면 객체가 파일 시스템에서 영구적으로 제거됩니다.

S3 오브젝트 만료 및 라이프사이클 관리에 대한 자세한 내용은 을 참조하십시오"버킷 수명 주기 관리 규칙을 생성합니다".

S3 스냅샷의 제한 사항

ONTAP 9.16.1에서 다음 기능 제외 및 시나리오를 참고하십시오.

- S3 버킷에 대해 최대 1023개의 스냅샷을 생성할 수 있습니다.
- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌리려면 먼저 클러스터의 모든 버킷에서 모든 S3 스냅샷과 메타데이터를 삭제해야 합니다.
- 스냅샷이 있는 오브젝트가 포함된 S3 버킷을 삭제해야 하는 경우 해당 버킷에 있는 모든 오브젝트의 해당 스냅샷을 모두 삭제했는지 확인하십시오.
- S3 스냅샷은 다음 구성에서 지원되지 않습니다.

- 완전히 새로운 차원의 제휴가 이루어질 수 있습니다 SnapMirror
- 물체 잠금이 활성화된 버킷
- NetApp 콘솔에서
- On System Manager 를 참조하십시오
- ONTAP MetroCluster 구성에서

- 로컬 또는 원격 FabricPool 용량 계층으로 사용되는 버킷에서는 S3 스냅샷을 사용하지 않는 것이 좋습니다.

ONTAP S3 스냅샷을 생성합니다

S3 스냅샷을 수동으로 생성하거나 스냅샷 정책을 설정하여 S3 스냅샷을 자동으로 생성할 수 있습니다. 스냅샷은 데이터 백업 및 복구에 사용하는 개체의 정적 복사본 역할을 합니다. 스냅샷 보존 기간을 결정하기 위해 지정된 간격으로 자동 스냅샷 생성을 지원하는 스냅샷 정책을 생성할 수 있습니다.

S3 스냅샷은 오브젝트 버전 관리를 사용 또는 사용하지 않고 S3 버킷에서 오브젝트 데이터를 보호하는 데 도움이 됩니다.

스냅샷은 S3 버킷에서 오브젝트 버전 관리를 사용하지 않는 경우, 이전 오브젝트 버전을 사용할 수 없는 경우 복원 작업에 사용할 수 있는 시점 레코드의 역할을 하기 때문에 데이터 보호를 설정하는 데 특히 유용합니다.

이 작업에 대해

- 다음 명명 규칙이 스냅샷에 적용됩니다(수동 및 자동 스냅샷 모두).
  - S3 스냅샷 이름은 최대 30자까지 지정할 수 있습니다
  - S3 스냅샷 이름은 소문자, 숫자, 점(.) 및 하이픈(-)만 구성할 수 있습니다.
  - S3 스냅샷 이름은 문자 또는 숫자로 끝나야 합니다
  - S3 스냅샷 이름에는 하위 문자열이 포함될 수 없습니다 `s3snap`
- S3 프로토콜의 컨텍스트에서 버킷 명명 제한으로 인해 버킷 이름이 63자로 제한됩니다. ONTAP S3 스냅샷은 S3 프로토콜을 통해 버킷으로 표시되므로 스냅샷 버킷 이름에 유사한 제한이 적용됩니다. 기본적으로 원래 버킷 이름이 기본 버킷 이름으로 사용됩니다.
- 어떤 버킷에 속하는 스냅샷을 보다 쉽게 식별할 수 있도록 스냅샷 버킷 이름은 기본 버킷 이름과 스냅샷 이름 앞에 붙는 특수 문자열로 `-s3snap-` 구성됩니다. 스냅샷 버킷 이름의 형식은 로 `<base_bucket_name>-s3snap-<snapshot_name>`지정됩니다.

  예를 들어, 다음 명령을 실행하여 `snap1` 에서 을 `bucket-a` 생성하면 기본 버킷에 액세스 권한이 있는 경우, S3 클라이언트를 통해 액세스할 수 있는 이름으로 스냅샷 버킷이 `bucket-a-s3snap-snap1` 생성됩니다.

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- 63자를 초과하는 스냅샷 버킷 이름을 생성하는 스냅샷을 생성할 수 없습니다.
- 자동 스냅샷 이름에는 기존 볼륨 스냅샷의 명명 규칙과 유사한 정책 일정 이름과 타임스탬프가 포함됩니다. 예를

들어 예약된 스냅샷 이름은 및 `hourly-2024-05-22-1105` 일 수 `daily-2024-01-01-0015` 있습니다.

S3 스냅샷을 수동으로 생성합니다

ONTAP CLI를 사용하여 S3 스냅샷을 수동으로 생성할 수 있습니다. 이 절차는 로컬 클러스터에만 스냅샷을 생성합니다.

단계

1. S3 스냅샷 생성:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

다음 예에서는 `vs0` 스토리지 VM 및 `website-data` 버킷에 이라는 스냅샷을 `pre-update` 생성합니다.

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

버킷에 S3 스냅샷 정책을 할당합니다

S3 버킷 수준에서 스냅샷 정책을 구성하면 ONTAP가 예약된 S3 스냅샷을 자동으로 생성합니다. 기존 스냅샷 정책과 마찬가지로 S3 스냅샷에 대해 최대 5개의 일정을 구성할 수 있습니다.

스냅샷 정책은 일반적으로 스냅샷을 생성할 스케줄, 각 스케줄에 대해 보존할 복제본 수 및 스케줄 접두사를 지정합니다. 예를 들어 정책은 매일 오전 12시 10분에 S3 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하고 이름을 지정할 수 `daily-<timestamp>` 있습니다.

기본 스냅샷 정책은 다음을 보존합니다.

- 시간별 스냅샷 6개
- 일일 스냅샷 2개
- 주간 스냅샷 2개

시작하기 전에

- S3 버킷에 할당하기 전에 스냅샷 정책을 생성해야 합니다.

> S3 스냅샷에 대한 정책은 다른 ONTAP 스냅샷 정책과 동일한 규칙을 따릅니다. 하지만 스냅샷 스케줄에 보존 기간이 구성된 스냅샷 정책은 S3 버킷에 할당할 수 없습니다.

스냅샷 자동 생성을 위한 스냅샷 정책 생성에 대한 자세한 내용은 을 참조하십시오"사용자 지정 스냅샷 정책 구성 개요".

단계

1. 버킷에 스냅샷 정책을 할당합니다.

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

또는

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌려야 하는 경우 모든 버킷의 값이 (또는 -)로 설정되어 `none` 있는지 확인하십시오 `snapshot-policy`.

관련 정보

"ONTAP S3 스냅샷에 대해 자세히 알아보십시오"

ONTAP S3 스냅샷을 보고 복원합니다

ONTAP 9.16.1부터 S3 클라이언트의 버킷에 대한 S3 스냅샷 데이터를 보고 찾아볼 수 있습니다. ONTAP 9.18.1부터 ONTAP CLI를 사용하여 S3 스냅샷 버킷에 기본적으로 액세스할 수 있습니다. 또한 S3 스냅샷에서 S3 클라이언트의 단일 객체, 객체 세트 또는 전체 버킷을 복원할 수 있습니다.

시작하기 전에

- ONTAP CLI에서 버킷 스냅샷 복원 작업을 기본적으로 수행하려면 클러스터의 모든 노드에서 ONTAP 9.18.1 이상이 실행되어야 합니다. ONTAP 9.18.1부터 S3 브라우저는 더 이상 필요하지 않지만 작업은 계속 지원됩니다.
- 주어진 버킷에 대해 한 번에 하나의 스냅샷 복원 작업만 허용됩니다.

이 작업에 대해

ONTAP 9.16.1부터 ONTAP S3 스냅샷 기능은 수동 및 예약된 스냅샷 생성 및 삭제, S3 버킷에 대한 스냅샷 정책, S3 클라이언트 기반 스냅샷 검색을 포함하여 ONTAP S3 버킷에 대한 기본 스냅샷 기능을 제공합니다.

ONTAP 9.18.1부터 네이티브 ONTAP 스냅샷 복원에 대한 지원이 추가되어 ONTAP 관리자가 S3 브라우저를 사용하지 않고도 특정 시점 복원 기능을 사용할 수 있습니다. 스냅샷에는 현재 버킷 버전만 캡처됩니다. 버전 기록은 캡처되지 않으며 S3 스냅샷 복원 작업으로 복원되지 않습니다.

S3 스냅샷 나열 및 보기

S3 스냅샷 세부 정보를 보고, 비교하고, 오류를 식별할 수 있습니다. ONTAP CLI를 사용하면 S3 버킷에서 생성된 모든 스냅샷을 나열할 수 있습니다.

단계

1. S3 스냅샷 목록:

```
vserver object-store-server bucket snapshot show
```

클러스터의 모든 버킷에 대해 생성된 S3 스냅샷의 스냅샷 이름, 스토리지 VM, 버킷, 생성 시간 및 인스턴스 UUID를 볼 수 있습니다.

2. 버킷 이름을 지정하여 해당 버킷에 대해 생성된 모든 S3 스냅샷의 이름, 생성 시간, 인스턴스 UUID를 볼 수도 있습니다.

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

S3 스냅샷 콘텐츠를 찾아봅니다

환경에서 장애나 문제가 발견되면 S3 버킷 스냅샷의 콘텐츠를 탐색하여 오류를 식별할 수 있습니다. 또한 S3 스냅샷을 탐색하여 오류 없는 콘텐츠를 복원할 수도 있습니다.

S3 스냅샷은 S3 클라이언트에 스냅샷 버킷으로 제공됩니다. 스냅샷 버킷 이름은 다음과 같이 형식화됩니다. `<base_bucket_name>-s3snap-<snapshot_name>` . 다음을 사용하여 스토리지 VM의 모든 스냅샷 버킷을 볼 수 있습니다. `ListBuckets` S3 API 작업.

S3 스냅샷 버킷은 기본 버킷의 액세스 정책을 상속받으며 읽기 전용 작업만 지원합니다. 삭제 및 쓰기 기반 작업은 금지됩니다. 기본 버킷에 액세스할 수 있는 권한이 있는 경우 S3 스냅샷 버킷에서 다음과 같은 읽기 전용 S3 API 작업을 수행할 수도 있습니다. `HeadObject` , `GetObject` , `GetObjectTagging` , `ListObjects` , `ListObjectVersions` , `GetObjectAcl` , 그리고 `CopyObject` .

> 이 `CopyObject` 작업은 S3 스냅샷 버킷이 소스 버킷의 스냅샷인 경우에만 지원되며, 스냅샷의 스토리지 타겟인 경우에는 지원되지 않습니다.

이러한 작업에 대한 자세한 내용은 을 "ONTAP S3가 지원되는 작업"참조하십시오.

ONTAP 사용하여 **S3** 스냅샷에서 버킷 복원

ONTAP 9.18.1부터 ONTAP CLI를 사용하여 ONTAP S3 스냅샷을 사용하여 전체 버킷을 복원할 수 있습니다. 선택한 스냅샷이 생성된 시점에 존재했던 버킷 버전만 복원할 수 있습니다.

단계

1. 버킷을 복원하는 데 사용할 스냅샷을 식별하세요.

```
vserver object-store-server bucket snapshot show
```

2. 버킷을 복원합니다.

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

S3 클라이언트를 사용하여 S3 버킷 스냅샷에서 데이터 복원

ONTAP 에서 전체 버킷을 복원하는 것 외에도 S3cmd나 S3 Browser와 같은 S3 클라이언트를 사용하여 S3 스냅샷에서 단일 개체, 개체 세트 또는 전체 버킷을 복원할 수도 있습니다.

"버전이 지정된 스냅샷과 버전이 지정되지 않은 스냅샷에 대해 자세히 알아보세요."

다음을 사용하여 전체 버킷, 특정 접두사가 있는 개체 또는 단일 개체를 복원할 수 있습니다. `aws s3 cp` 명령.

단계

1. 기본 S3 버킷의 스냅샷을 생성합니다.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. 스냅샷을 사용하여 기본 버킷을 복원합니다.
   - 전체 버킷을 복원합니다. 스냅샷 버킷 이름을 형식으로 `<base_bucket_name>-s3snap-<snapshot_name>` 사용합니다.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

   - 다음 접두사를 사용하여 디렉터리의 개체를 `dir1` 복원합니다.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

   - 이름이 인 단일 개체 복원 `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

ONTAP S3 스냅샷을 삭제합니다

더 이상 필요하지 않은 S3 스냅샷을 삭제하고 버킷의 스토리지 공간을 확보할 수 있습니다. S3 스냅샷을 수동으로 제거하거나 S3 버킷에 연결된 스냅샷 정책을 수정하여 일정에 대해 보존할 스냅샷 수를 변경할 수 있습니다.

S3 버킷에 대한 스냅샷 정책은 기존 ONTAP 스냅샷 정책과 동일한 삭제 규칙을 따릅니다. 스냅샷 정책 생성에 대한 자세한 내용은 을 "스냅샷 정책을 생성합니다"참조하십시오.

이 작업에 대해

- 여러 스냅숏에서 객체 버전(버전 버킷의 경우) 또는 객체(버전이 지정되지 않은 버킷의 경우)가 캡처된 경우 마지막으로 보호된 스냅샷이 삭제된 후에만 파일 시스템에서 객체가 제거됩니다.
- 스냅샷이 있는 오브젝트가 포함된 S3 버킷을 삭제해야 하는 경우 해당 버킷에 있는 모든 오브젝트의 모든 스냅샷을 삭제했는지 확인하십시오.
- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌려야 하는 경우 모든 버킷에 대해 모든 S3 스냅샷을 삭제했는지 확인하십시오. S3 버킷의 스냅샷 메타데이터를 제거하기 위해 명령을 실행해야 할 수도 `vserver object-store-server bucket clear-snapshot-metadata` 있습니다. 자세한 내용은 을 "S3 스냅샷 메타데이터를 지웁니다"참조하십시오.
- 스냅샷을 일괄적으로 삭제할 때 여러 스냅샷에 캡처된 많은 수의 개체를 제거하여 개별 스냅샷을 삭제할 때보다 더 많은 공간을 효율적으로 확보할 수 있습니다. 따라서 스토리지 오브젝트를 위해 더 많은 공간을 재확보할 수 있습니다.

단계

1. 특정 S3 스냅샷을 삭제하려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. 버킷에서 모든 S3 스냅샷을 제거하려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

S3 스냅샷 메타데이터를 지웁니다

S3 스냅샷을 사용하면 스냅샷 메타데이터도 버킷에서 생성됩니다. 스냅샷 메타데이터는 모든 스냅샷이 해당 스냅샷에서 제거되더라도 계속해서 버킷에 있게 됩니다. 스냅샷 메타데이터가 있으면 다음 작업이 차단됩니다.

- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌립니다
- 버킷에 SnapMirror S3 구성

이러한 작업을 수행하기 전에 버킷에서 모든 스냅샷 메타데이터를 지워야 합니다.

시작하기 전에

메타데이터 지우기를 시작하기 전에 버킷에서 모든 S3 스냅샷을 제거했는지 확인합니다.

단계

1. 버킷에서 스냅샷 메타데이터를 지우려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

S3 이벤트를 감사합니다

ONTAP S3 이벤트 감사에 대해 자세히 알아보십시오

ONTAP 9.10.1부터 ONTAP S3 환경에서 데이터 및 관리 이벤트를 감사할 수 있습니다. S3 감사 기능은 기존의 NAS 감사 기능과 유사하며, S3 및 NAS 감사가 클러스터에 공존할 수 있습니다.

SVM에서 S3 감사 구성을 생성하고 활성화하면 S3 이벤트가 로그 파일에 기록됩니다. 기록할 다음 이벤트를 지정할 수 있습니다.

릴리즈별 오브젝트 액세스(데이터) 이벤트

9.11.1:

- 목록 BuckketVersions
- ListBucket(ListObjects 9.10.1의 이름이 이것으로 변경됨)
- ListAllMyBucket(9.10.1의 ListBucket 이름이 이것으로 변경됨)

9.10.1:

- HeadObject 를 선택합니다
- GetObject 를 참조하십시오
- PutObject 를 선택합니다
- DeleteObject 를 클릭합니다
- ListBucket
- ListObjects 를 선택합니다
- MPUpload 를 클릭합니다
- MPUploadPart 를 참조하십시오
- MPComplete(MPComplete)
- MPAbort(MP중단)
- GetObjectTagging
- DeleteObjectTagging 을 선택합니다
- PutObjectTagging
- 업로드 목록
- 목록 파트

릴리스별 관리 이벤트

9.15.1:

- GetBucketCORS 를 참조하십시오

- PutBucketCORS/퍼트버케토르스
- DeleteBucketCORS를 클릭합니다

9.14.1:

- GetObjectRetention을 참조하십시오
- PutObjectRetention
- PutBucketObjectLockConfiguration 을 참조하십시오
- GetBucketObjectLockConfiguration 을 참조하십시오

9.13.1:

- PutBucketLifecycle 을 참조하십시오
- DeleteBucketLifecycle
- GetBucketLifecycle 을 참조하십시오

9.12.1:

- GetBuckketPolicy를 참조하십시오
- CopyObject 를 선택합니다
- 업로드파트 복사
- BucketPolicy를 참조하십시오
- DeleteBuckketPolicy를 참조하십시오

9.11.1:

- GetBuckketVersioning 을 참조하십시오
- PutBucketVersioning을 참조하십시오

9.10.1:

- 머리버킷
- GetBuckketAcl
- GetObjectAcl
- 퍼트버킷
- 삭제 버킷
- ModifyObject태그 지정
- GetBucketLocation 을 참조하십시오

로그 형식은 JSON(JavaScript Object Notation)입니다.

S3 및 NFS 감사 구성의 경우 결합된 제한은 클러스터당 400개의 SVM입니다.

다음 라이센스가 필요합니다.

- ONTAP S3 프로토콜 및 스토리지를 위한 ONTAP One, 이전의 코어 번들에 포함됨

자세한 내용은 을 참조하십시오 "ONTAP 감사 프로세스의 작동 방식".

감사 보장

기본적으로 S3 및 NAS 감사가 보장됩니다. ONTAP는 노드를 사용할 수 없는 경우에도 감사 가능한 모든 버킷 액세스 이벤트를 기록할 수 있도록 보장합니다. 해당 작업에 대한 감사 레코드가 영구 스토리지의 스테이징 볼륨에 저장될 때까지 요청된 버킷 작업을 완료할 수 없습니다. 공간이 부족하거나 다른 문제로 인해 스테이징 파일에 감사 레코드를 커밋할 수 없는 경우 클라이언트 작업이 거부됩니다.

감사를 위한 공간 요구 사항

ONTAP 감사 시스템에서는 감사 레코드가 처음에는 개별 노드의 이진 스테이징 파일에 저장됩니다. 주기적으로 이러한 로그는 통합되어 사용자가 읽을 수 있는 이벤트 로그로 변환되며, SVM의 감사 이벤트 로그 디렉토리에 저장됩니다.

스테이징 파일은 감사 구성이 생성될 때 ONTAP에서 생성하는 전용 스테이징 볼륨에 저장됩니다. 애그리게이트당 하나의 스테이징 볼륨이 있습니다.

감사 구성에서 사용 가능한 충분한 공간을 계획해야 합니다.

- 감사된 버킷을 포함하는 애그리게이트에서 스테이징 볼륨의 경우
- 변환된 이벤트 로그가 저장되는 디렉토리가 포함된 볼륨입니다.

S3 감사 구성을 생성할 때 다음 두 가지 방법 중 하나를 사용하여 이벤트 로그 수와 볼륨의 사용 가능한 공간을 제어할 수 있습니다.

- 숫자 제한, '-rotate-limit' 매개변수는 보존되어야 하는 최소 감사 파일 수를 제어합니다.
- 시간 제한: '-retention-duration' 매개변수는 파일을 보존할 수 있는 최대 기간을 제어합니다.

두 매개 변수 모두에서 구성된 값을 초과하면 오래된 감사 파일을 삭제하여 새 감사 파일을 저장할 공간을 만들 수 있습니다. 두 매개 변수 모두 값이 0이면 모든 파일이 유지되어야 함을 나타냅니다. 따라서 충분한 공간을 확보하기 위해 매개 변수 중 하나를 0이 아닌 값으로 설정하는 것이 좋습니다.

감사 보장 때문에 감사 데이터에 사용할 수 있는 공간이 회전 제한 전에 초과되면 최신 감사 데이터를 생성할 수 없으므로 클라이언트가 데이터에 액세스하지 못합니다. 따라서 이 값과 감사에 할당된 공간을 신중하게 선택해야 하며 감사 시스템의 사용 가능한 공간에 대한 경고에 응답해야 합니다.

자세한 내용은 을 참조하십시오 "기본 감사 개념".

ONTAP S3 감사 구성 계획

S3 감사 구성에 대해 여러 매개 변수를 지정하거나 기본값을 그대로 사용해야 합니다. 특히 적절한 여유 공간을 확보하는 데 도움이 되는 로그 회전 매개 변수를 고려해야 합니다.

에 대한 자세한 내용은 `vserver object-store-server audit create` "ONTAP 명령 참조입니다"을 참조하십시오.

일반 매개변수

감사 구성을 만들 때 지정해야 하는 필수 매개 변수는 두 가지입니다. 지정할 수 있는 세 가지 선택적 매개 변수도 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_SVM 이름 _ 감사 구성을 생성할 SVM의 이름입니다. S3에 대해 SVM이 이미 존재하고 사용하도록 설정해야 합니다.	`-vserver svm_name`	예
_로그 대상 경로 _ 변환된 감사 로그를 저장할 위치를 지정합니다. SVM에 경로가 이미 있어야 합니다. 경로는 최대 864자까지 가능하며 읽기-쓰기 권한이 있어야 합니다. 경로가 유효하지 않으면 감사 구성 명령이 실패합니다.	'-destination_text_'	예
_ 감사할 이벤트의 범주 _ 다음 이벤트 범주를 감사할 수 있습니다. • Data GetObject , PutObject 및 DeleteObject 이벤트 • 관리 PutBucket 및 DeleteBucket 이벤트 기본값은 데이터 이벤트만 감사하는 것입니다.	'-events{data|management},…'	아니요

다음 매개 변수 중 하나를 입력하여 감사 로그 파일 수를 제어할 수 있습니다. 값을 입력하지 않으면 모든 로그 파일이 유지됩니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_ 로그 파일 회전 제한 _ 가장 오래된 로그 파일을 회전하기 전에 유지할 감사 로그 파일 수를 결정합니다. 예를 들어 값을 5로 입력하면 마지막 5개의 로그 파일이 유지됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-rotate-limit_integer _'	아니요

_로그 파일 지속 시간 제한 _ 로그 파일을 삭제하기 전에 보존할 수 있는 기간을 결정합니다. 예를 들어 5d0h0m 값을 입력하면 5일 이상 지난 로그가 삭제됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-retention duration_integer_time_'	아니요

감사 로그 회전을 위한 매개 변수입니다

크기 또는 일정에 따라 감사 로그를 회전할 수 있습니다. 기본값은 크기에 따라 감사 로그를 회전하는 것입니다.

로그 크기에 따라 로그를 회전합니다

기본 로그 회전 방법과 기본 로그 크기를 사용하려면 로그 회전을 위한 특정 매개 변수를 구성할 필요가 없습니다. 기본 로그 크기는 100MB입니다.

기본 로그 크기를 사용하지 않으려면 '-rotate-size' 매개변수를 구성하여 사용자 정의 로그 크기를 지정할 수 있습니다.

로그 크기만을 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-schedule-minute' 매개 변수를 설정 해제합니다.

'vserver audit modify -vserver_svm_name_-destination/-rotate-schedule-minute -'

일정에 따라 로그를 회전합니다

일정에 따라 감사 로그를 회전하도록 선택한 경우 시간 기반 회전 매개 변수를 조합하여 로그 회전을 예약할 수 있습니다.

- 시간 기반 회전을 사용하는 경우 '-rotate-schedule-minute' 매개변수는 필수입니다.
- 다른 모든 시간 기반 회전 매개변수는 옵션입니다.
  - '-rotate-schedule-month’입니다
  - '-rotate-schedule-DayOfWeek'
  - '-rotate-schedule-day'
  - '-rotate-schedule-hour'
- 회전 일정은 모든 시간 관련 값을 사용하여 계산됩니다. 예를 들어, '-rotate-schedule-minute' 매개 변수만 지정하면 감사 로그 파일은 모든 연도의 모든 월에 지정된 모든 요일에 지정된 분을 기준으로 회전합니다.
- 시간 기반 회전 매개 변수(예: '-rotate-schedule-month' 및 '-rotate-schedule-minutes')를 하나 또는 두 개만 지정하는 경우 모든 시간 동안 모든 요일에 지정한 분 값을 기준으로 로그 파일이 회전되며 지정된 개월 동안에만 회전됩니다.

  예를 들어 월요일, 수요일 및 토요일은 오전 10시 30분에 월, 3월, 8월 중 감사 로그를 회전하도록 지정할 수 있습니다

- '-rotate-schedule-dayOfWeek' 및 '-rotate-schedule-day' 값을 모두 지정하면 독립적으로 간주됩니다.

  예를 들어, `-rotate-schedule-dayOfWeek’를 금요일로 지정하고 '-rotate-schedule-day’를 13일로 지정하면 13일에 금요일이 아니라 지정한 달의 13일에 감사 로그가 회전합니다.

- 일정만 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-size 매개 변수'를 해제합니다.

  'vserver audit modify -vserver_svm_name_-destination/-rotate-size-'

로그 크기 및 일정에 따라 로그를 회전합니다

모든 조합의 -rotate-size 매개 변수와 시간 기반 회전 매개 변수를 모두 설정하여 로그 크기와 일정에 따라 로그 파일을 회전하도록 선택할 수 있습니다. 예를 들어, '-rotate-size'를 10MB로 설정하고 '-rotate-schedule-minute'를 15로 설정하면 로그 파일 크기가 10MB에 도달하거나 매 시간 15분(둘 중 먼저 발생하는 이벤트)에 도달할 때 로그 파일이 회전합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP S3 감사 구성을 생성하고 사용합니다

S3 감사를 구현하려면 먼저 S3 기반 SVM에서 영구 오브젝트 저장소 감사 구성을 생성한 다음 구성을 활성화합니다.

시작하기 전에

- S3 지원 SVM이 있습니다.
- 로컬 계층에 볼륨을 스테이징할 공간이 충분한지 확인합니다.

이 작업에 대해

감사 구성은 감사하려는 S3 버킷을 포함하는 각 SVM에 필요합니다. 신규 또는 기존 S3 서버에서 S3 감사를 활성화할 수 있습니다. 감사 구성은 * vserver object-store-server audit delete * 명령을 통해 제거될 때까지 S3 환경에서 지속됩니다.

S3 감사 구성은 감사를 위해 선택한 SVM의 모든 버킷에 적용됩니다. 감사 가능 SVM에는 감사되고 감사되지 않은 버킷이 포함될 수 있습니다.

로그 크기 또는 일정에 따라 자동 로그 회전에 대해 S3 감사를 구성하는 것이 좋습니다. 자동 로그 회전을 구성하지 않으면 기본적으로 모든 로그 파일이 유지됩니다. vserver object-store-server audit rotate -log * 명령을 사용하여 S3 로그 파일을 수동으로 회전할 수도 있습니다.

SVM이 SVM 재해 복구 소스인 경우 타겟 경로가 루트 볼륨에 있을 수 없습니다.

단계

1. 감사 구성을 생성하여 로그 크기 또는 일정에 따라 감사 로그를 회전합니다.

감사 로그를 회전하려면...	입력...
로그 크기	'vserver object-store-server audit create-vserver_svm_name_-destination_path_[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integer_d][_integer_h][_integer_m]]}[-rotate-size{_integer*[KB|MB|GB|TB|PB]}]']

감사 로그를 회전하려면...	입력...
일정	'vserver object-store-server audit create-vserver_svm_name_-destination path[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integerd*][*integerh*][*integerm*]}[-rotate-schedule -month_chron_month_][-rotate_schedule -DayOfWeek_chron_dayOfWeek_] [-rotate_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_month 시간 기반 감사 로그 회전을 구성하려면 '-rotate-schedule-minute' 매개 변수가 필요합니다.

2. S3 감사 활성화:

   'vserver object-store-server audit enable-vserver_svm_name_'

예

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그는 /audit_log 디렉토리에 저장됩니다. 로그 파일 크기 제한은 200MB입니다. 로그 크기가 200MB에 도달하면 로그가 회전합니다.

'cluster1::> vserver audit create - vserver vs1-destination/audit_log-rotate-size 200MB'

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 파일 크기 제한은 100MB(기본값)이며, 로그 삭제 전 5일 동안 보존됩니다.

'cluster1::> vserver audit create - vserver vs1-destination/audit_log-retention-duration 5d0h0m'

다음 예제에서는 시간 기반 회전을 사용하여 S3 관리 이벤트와 중앙 액세스 정책 스테이징 이벤트를 감사하는 감사 구성을 만듭니다. 감사 로그는 매월 오후 12시 30분에 순환됩니다 일주일 내내. 로그 회전 제한은 5입니다.

'cluster1:> vserver audit create - vserver vs1-destination/audit_log-events management-rotate-schedule -month all-rotate-schedule -dayOfWeek all-rotate-schedule-hour 12-rotate-schedule-minute 30-rotate-limit 5'

ONTAP S3 감사를 위한 버킷 선택

감사 가능 SVM에서 감사할 버킷은 지정해야 합니다.

시작하기 전에

- S3 감사를 위해 SVM을 사용하도록 설정했습니다.

이 작업에 대해

S3 감사 구성은 SVM별로 활성화되지만 감사를 위해 SVM에서 버킷을 선택해야 합니다. SVM에 버킷을 추가하고 새 버킷을 감사하려면 이 절차를 사용하여 해당 버킷을 선택해야 합니다. S3 감사를 위해 SVM에서 감사하지 않은 버킷을 포함할 수도 있습니다.

감사 구성은 명령에 의해 제거될 때까지 버킷에 대해 `vserver object-store-server audit event-selector delete` 유지됩니다.

단계

1. S3 감사에 사용할 버킷 선택:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`: 감사할 이벤트 액세스 형식을 지정합니다 `read-only`. , `write-only` 또는 `all` (기본값은 입니다. `all`)
   - `-permission`: 감사할 이벤트 권한의 유형을 지정합니다 `allow-only`. , `deny-only` 또는 `all` (기본값은 입니다. `all`)

예

다음 예제에서는 읽기 전용 액세스로 허용된 이벤트만 기록하는 버킷 감사 구성을 만듭니다.

'cluster1::> vserver object-store-server audit event-selector create-vserver vs1-bucket test-bucket-access read-only-permission allow-only'

ONTAP S3 감사 구성을 수정합니다

개별 버킷의 감사 매개 변수 또는 SVM에서 감사를 위해 선택한 모든 버킷의 감사 구성을 수정할 수 있습니다.

에 대한 감사 구성을 수정하려면...	입력...
개별 버킷	'vserver object-store-server audit event-selector modify -vserver_svm_name_[-bucket_bucket_name_][_parameters to modify _]'
SVM의 모든 버킷	'vserver object-store-server audit modify -vserver_svm_name_[_parameters to modify _]'

예

다음 예에서는 쓰기 전용 액세스 이벤트만 감사하도록 개별 버킷 감사 구성을 수정합니다.

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

다음 예에서는 SVM의 모든 버킷에 대한 감사 구성을 수정하여 로그 크기 제한을 10MB로 변경하고 회전 전에 로그 파일 3개를 보존합니다.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3 감사 구성을 표시합니다

감사 구성을 완료한 후 감사가 올바르게 구성되어 있고 활성화되어 있는지 확인할 수 있습니다. 또한 클러스터의 모든 오브젝트 저장소 감사 구성에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

버킷 및 SVM 감사 구성에 대한 정보를 표시할 수 있습니다.

- 버킷: `vserver object-store-server audit event-selector show` 명령을 사용합니다

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 있는 버킷에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 버킷 이름
  - 액세스 및 권한 값
- SVM: 명령을 사용합니다 `vserver object-store-server audit show`

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 감사 상태
  - 대상 디렉토리

'-fields' 파라미터를 지정하여 표시할 감사 구성 정보를 지정할 수 있습니다.

단계

S3 감사 구성에 대한 정보 표시:

에 대한 구성을 수정하려면...	입력...
버킷	'vserver object-store-server audit event-selector show[-vserver_svm_name_][*parameters*]'
SVM	'vserver object-store-server audit show[-vserver_svm_name_][*parameters*]'

예

다음 예는 단일 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

다음 예는 SVM의 모든 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver            :vs1
     Bucket             :test-bucket
     Access             :all
     Permission         :all
```

다음 예에서는 모든 SVM에 대한 이름, 감사 상태, 이벤트 유형, 로그 형식, 타겟 디렉토리를 표시합니다.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

다음 예에서는 SVM 이름과 모든 SVM의 감사 로그에 대한 세부 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit show -log-save-details

                 Rotation                            Rotation
      Vserver    File Size Rotation Schedule         Limit
      ---------- --------- ------------------------- --------
      vs1        100MB     -                         0
```

다음 예제는 모든 SVM에 대한 모든 감사 구성 정보를 목록 형식으로 표시합니다.

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                          Log Format: json
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

저작권 정보

상표 정보