구성
ONTAP 9

NetApp
April 29, 2024

목차

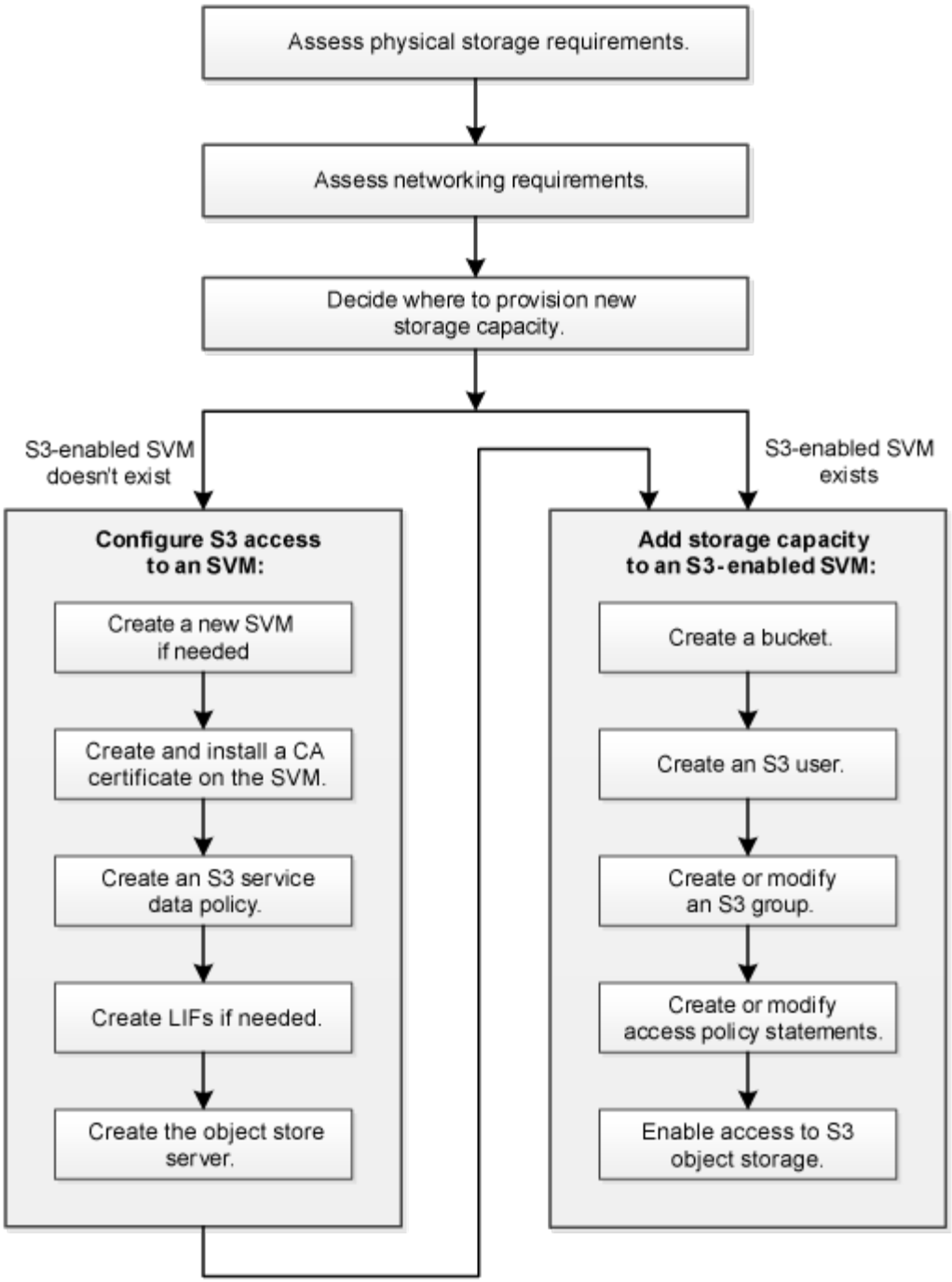
구성

S3 구성 프로세스 정보

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.

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.



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 기반 SVM에서 S3 버킷을 생성할 때 FlexGroup 볼륨이 자동으로 생성되어 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.

네트워킹 요구 사항을 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.

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.

새 **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

S3를 위해 **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.

   기존 스토리지 VM에 S3 서버를 추가하는 경우 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 을 클릭합니다 ⚙ S3 * 아래.

   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
```

SVM에서 CA 인증서를 생성하고 설치합니다

S3 클라이언트에서 S3 기반 SVM으로 HTTPS 트래픽을 활성화하려면 CA(인증 기관) 인증서가 필요합니다.

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. 타사 공급업체의 CA 인증서도 지원됩니다. 자세한 내용은 관리자 인증 설명서를 참조하십시오.

"관리자 인증 및 RBAC"

추가 구성 옵션은 보안 인증서 man 페이지를 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.

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.

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

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
```

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.

데이터 **LIF** 생성

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 구성되어 있어야 합니다.
- 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.

- LIF 서비스 정책이 이미 존재해야 합니다.

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).
- 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.

  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. '네트워크 라우트 생성' man 페이지에는 SVM 내에서 정적 라우트를 생성하는 정보가 포함되어 있습니다.
- '-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.
```

원격 **FabricPool** 계층화에 대한 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 구성되어 있어야 합니다.
- 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
   ```

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
```

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.

   'network interface show – service-policy default-인터클러스터-failover'

   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
```

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.

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.

추가 구성 및 표시 옵션은 'vserver object-store-server' man 페이지를 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 을 클릭합니다 ⚙ S3 * 아래.
   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.

   - 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

버킷을 만듭니다

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 참조하십시오 "스토리지 서비스 정의". 성능 관리에 대한 자세한 내용은 을 참조하십시오 "성능 관리". ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 중에 또는 나중에 QoS를 비활성화하거나 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.

  을 참조하십시오 "SVM 객체 저장소 서버 버킷 수정" 를 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)

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

```
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.

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 참조하십시오 "Amazon용 S3 버킷에서 버전 관리 사용".

9.14.1부터 S3 버킷에서 오브젝트 잠금이 지원됩니다. S3 오브젝트 잠금에는 표준 SnapLock 라이센스가 필요합니다. 이 라이센스는 에 포함되어 있습니다 "ONTAP 1 을 참조하십시오". 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 있습니다 "ONTAP One으로 업그레이드하십시오". 버킷에서 물체 잠금을 사용하도록 설정하는 경우 다음을 수행해야 합니다 "SnapLock 라이센스가 설치되어 있는지 확인합니다". SnapLock 라이센스가 설치되어 있지 않으면 를 수행해야 합니다 "설치합니다" 개체 잠금을 활성화하기 전에 이 옵션을 선택합니다. 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 참조하십시오 "새 버킷을 위한 거울을 작성합니다".

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.

MetroCluster 구성의 경우 미러링된 또는 미러링되지 않은 애그리게이트에 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 *.
  - S3 SnapMirror
  - 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

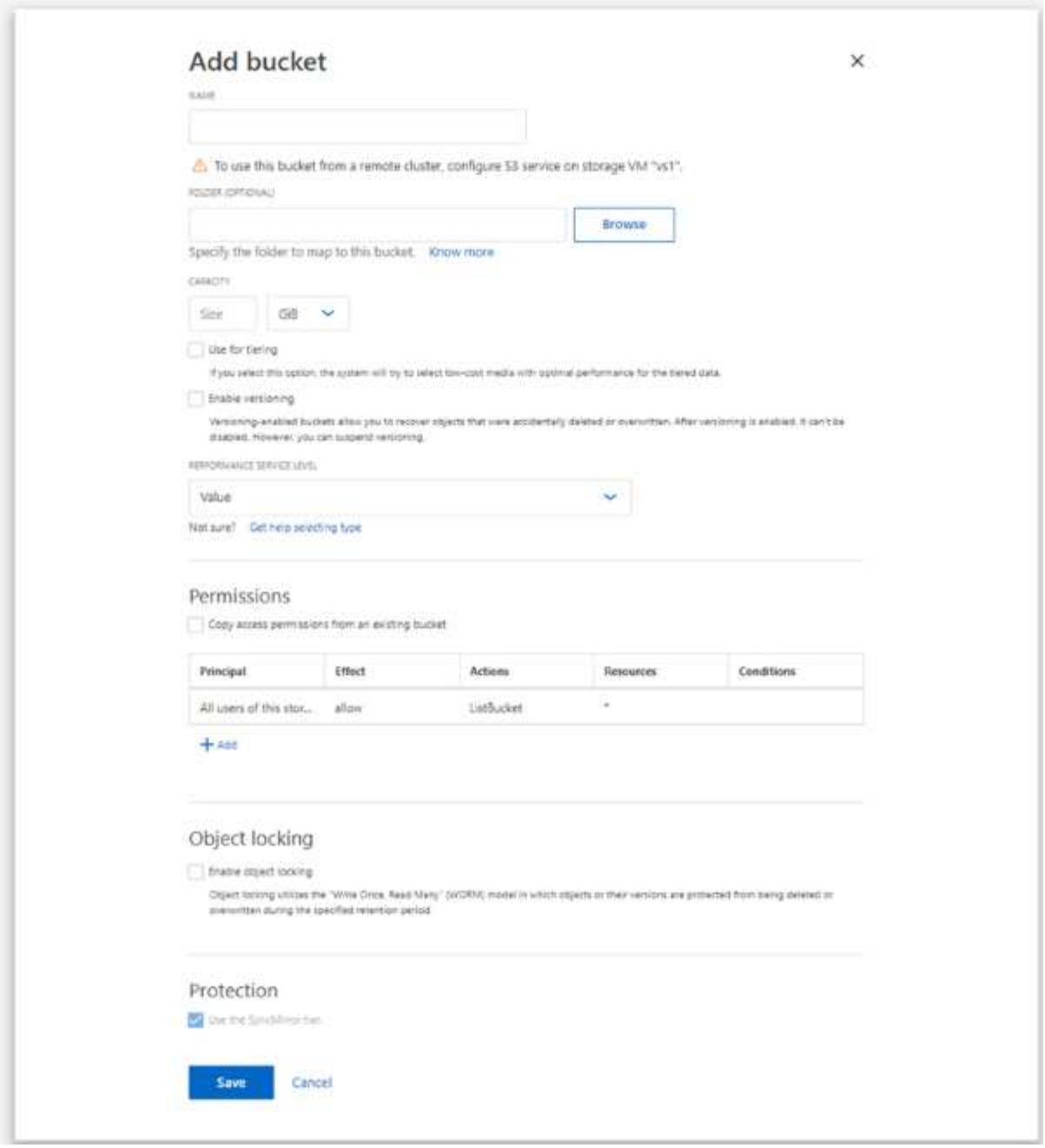
다음 예에서는 미러링된 애그리게이트에 1TB 크기의 SVM VS1에 대한 버킷을 생성합니다.

```
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 애플리케이션 – 다른 ONTAP 시스템 또는 외부 타사 애플리케이션 – 다음을 입력하여 새 버킷에 대한 액세스를 확인합니다.
   - S3 서버 CA 인증서입니다.
   - 사용자의 액세스 키 및 암호 키입니다.
   - S3 서버 FQDN 이름 및 버킷 이름입니다.

버킷 수명 주기 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.

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`.
- 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 활용할 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. 를 클릭합니다 ⋮ 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 버전 영구 삭제 *: 버전이 최신 버전이 아닌 날짜 후 삭제될 수 있는 날짜 수 및 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. 를 클릭합니다 ⋮ 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. 를 클릭합니다 ⋮ 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.

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. S3 사용자의 키는 에서 볼 수 있습니다 `vserver object-store-server user show` 명령.

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 을 클릭합니다 S3 아래.
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

S3 그룹을 생성하거나 수정합니다

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 을 클릭합니다 S3 아래.
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.

키를 다시 생성하고 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".

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.

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
2. 설정 * 탭에서 을 클릭합니다 S3 * 타일에서.
3. 사용자 * 탭에서 액세스 키가 없거나 사용자의 키가 만료되었는지 확인합니다.
4. 키를 다시 생성해야 하는 경우 을 클릭합니다 사용자 옆에 있는 * 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.

액세스 정책 문을 만들거나 수정합니다

버킷 및 오브젝트 저장소 서버 정책에 대해 설명합니다

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.

버킷 정책을 수정합니다

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. 더 많은 옵션은 'vserver object-store-server bucket policy' man 페이지를 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}/*##
```

오브젝트 저장소 서버 정책을 만들거나 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. 자세한 옵션은 을 참조하십시오 `vserver object-store-server policy` "명령 참조".

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 을 클릭합니다 S3 아래.
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.

외부 디렉토리 서비스에 대한 **S3** 액세스를 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 참조하십시오 "LDAP 사용 개요".

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 참조하십시오 "DNS 서비스를 구성합니다".
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 참조하십시오 "SVM에 자체 서명된 루트 CA 인증서를 설치합니다".
5. LDAP 클라이언트는 SVM에서 TLS를 사용하도록 구성했습니다. 을 참조하십시오 "LDAP 클라이언트 구성을 생성합니다" 및 "정보를 위해 LDAP 클라이언트 구성을 SVM에 연결합니다".

외부 디렉토리 서비스에 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
```

이 명령에 대한 자세한 내용은 를 참조하십시오 "SVM 서비스 이름 - 서비스 ns - 스위치 수정" 명령.

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
```

이 명령에 대한 자세한 내용은 를 참조하십시오 "SVM 서비스 이름 - 서비스 ns - 스위치 수정" 명령.

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.

LDAP 또는 도메인 사용자가 자신의 S3 액세스 키를 생성할 수 있도록 합니다

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.

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

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 참조하십시오 "DNS 서비스를 구성합니다".
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 참조하십시오 "SVM에 자체 서명된 루트 CA 인증서를 설치합니다".
5. LDAP 클라이언트는 스토리지 VM에서 TLS를 사용하도록 구성했습니다. 을 참조하십시오 "LDAP 클라이언트 구성을 생성합니다" 및.
6. 클라이언트 구성을 SVM에 연결합니다. 을 참조하십시오 "LDAP 클라이언트 구성을 SVM과 연결합니다" 및 "SVM 서비스 이름 - 서비스 LDAP 생성".
7. 데이터 스토리지 VM을 사용하는 경우 관리 네트워크 인터페이스(LIF) 및 VM에 그리고 LIF에 대한 서비스 정책을 생성합니다. 를 참조하십시오 "네트워크 인터페이스 생성" 및 "네트워크 인터페이스 서비스 - 정책 생성" 명령.

액세스 키 생성을 위한 사용자를 구성합니다

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
```

   이 명령에 대한 자세한 내용은 를 참조하십시오 "SVM 서비스 이름 - 서비스 ns - 스위치 수정" 명령.

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
```

이 명령에 대한 자세한 내용은 를 참조하십시오 "보안 로그인 REST-ROLE 생성" 명령.

3. security login 명령으로 LDAP 사용자 그룹을 생성하고 S3 사용자 REST API 끝점에 액세스하기 위한 새 사용자 지정 역할을 추가합니다. 이 명령에 대한 자세한 내용은 를 참조하십시오 "보안 로그인 생성" 명령.

```
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 참조하십시오 "nsswitch 인증에 LDAP 고속 바인딩을 사용합니다".

도메인 또는 LDAP 그룹에 사용자 지정 역할을 추가하면 해당 그룹의 사용자가 ONTAP에 대한 제한된 액세스를 허용할 수 있습니다 /api/protocols/s3/services/{svm.uuid}/users 엔드포인트. 도메인 또는 LDAP 그룹 사용자는 API를 호출하여 자신의 액세스 및 비밀 키를 생성하여 S3 클라이언트에 액세스할 수 있습니다. 사용자는 자신의 키를 생성할 수 있고 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.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다. 이 끝점의 다른 메서드에 대한 자세한 내용은 참조를 참조하십시오 "API 설명서".

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

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":"_name_"}'
```

JSON 출력 예


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "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: 볼륨의 비활성 데이터 양을 확인하려면 의 단계를 따릅니다 "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
```

S3 애플리케이션에서 클라이언트 액세스 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

스토리지 서비스 정의

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
FlexArray LUN을 나타냅니다	값
하이브리드	값
최적의 용량을 제공하는 플래시	값
솔리드 스테이트 드라이브(SSD) - 비 AFF	값
최적의 성능을 발휘하는 플래시-SSD(AFF)	최고의 성능, 가치