액세스 정책 문을 만들거나 수정합니다

ONTAP 9

NetApp
February 12, 2026

목차

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 **1.** 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"
}
```

저작권 정보

상표 정보