SVM에 대한 S3 액세스를 구성합니다

ONTAP 9

NetApp
February 12, 2026

목차

SVM에 대한 S3 액세스를 구성합니다

ONTAP S3용 SVM을 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 SVM에 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 LIF를 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
```