# SVM에 대한 SMB 액세스를 구성합니다

ONTAP 9

NetApp
March 04, 2026

# 목차

# SVM에 대한 SMB 액세스를 구성합니다

## ONTAP SVM에 대한 SMB 액세스를 구성합니다

SMB 클라이언트 액세스를 위해 SVM이 아직 구성되지 않은 경우 새 SVM을 생성 및 구성하거나 기존 SVM을 구성해야 합니다. SMB를 구성하려면 SVM 루트 볼륨 액세스를 열고, SMB 서버를 생성하고, LIF를 생성하고, 호스트 이름 확인을 지원하고, 이름 서비스를 구성하고, 필요한 경우 Kerberos 보안 활성화.

## ONTAP SVM을 생성하여 SMB 데이터 액세스를 제공합니다

SMB 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM을 하나 이상 가지고 있지 않은 경우 하나 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

단계

1. SVM 생성: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - '-rootvolume-security-style' 옵션에 NTFS 설정을 사용합니다.
   - 기본 C. UTF-8 '-language' 옵션을 사용합니다.
   - IPSpace 설정은 선택 사항입니다.
2. 새로 생성한 SVM의 구성 및 상태 확인: `vserver show -vserver vserver_name`

   허용되는 프로토콜 필드에는 CIFS가 포함되어야 합니다. 나중에 이 목록을 편집할 수 있습니다.

   '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 `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -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.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                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, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

# ONTAP SVM에서 SMB 프로토콜이 활성화되었는지 확인합니다

## SVM에서 SMB를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.

프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. SVM에 대해 현재 활성화 및 비활성화된 프로토콜은 'vserver show -vserver vserver_name -protocols'(vserver show -vserver vserver vserver_name -protocol)를 확인하십시오

   "vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.
   - SMB 프로토콜을 활성화하려면: 'vserver add-protocols-vserver vserver_name-protocols cifs'
   - 프로토콜을 작동 불가능하게 하려면: "vserver remove-protocols-vserver vserver_name-protocols protocol_name[,protocol_name,...]"
3. 활성화된 프로토콜과 비활성화된 프로토콜이 'vserver show -vserver vserver_name -protocols'(vserver show -vserver vserver_name -protocol)로 올바르게 업데이트되었는지 확인합니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

다음 명령을 실행하면 VS1 이라는 SVM의 활성화된 프로토콜 목록에 "CIFS"를 추가하여 SMB를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

# ONTAP SVM 루트 볼륨의 SMB 엑스포트 정책을 엽니다

## SVM 루트 볼륨의 기본 엑스포트 정책에는 SMB를 통한 모든 클라이언트의 개방형 액세스를 지원하는 규칙이 포함되어야 합니다. 이러한 규칙이 없으면 모든 SMB 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 엑스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

모든 SMB 액세스가 기본 엑스포트 정책에서 열려 있는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 엑스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 엑스포트 정책('vserver export-policy rule show')을 확인하십시오

   명령 출력은 다음과 같아야 합니다.

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 엑스포트 규칙을 생성합니다. 'vserver export-policy rule create-vserver vserver_name-policyname default-ruleindex 1-protocol cifs-clientmatch 0.0.0.0/0 -rorule any-rwrule any-superuser any'입니다
3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 SMB 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

# ONTAP SMB LIF를 생성합니다

## LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

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.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

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).

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

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

단계

1. LIF 생성:

   'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-node_node_name_-home-port_port_name_{-address_ip_address_-netmask ip_address|-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true|false}'

| * ONTAP 9.5 이하 * |
| --- |
| 'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-node_node_name_-home-port_port_name_{-address_name_- netmask_ip_address_ |
| - subnet-name_subnet_name_} -firewall-policy data-auto-revert{true |
| false} |

| * ONTAP 9.6 이상 * |
| --- |
| 'network interface create-vserver_vserver_name_-lif_lif_name_-service-policy_service_policy_name_-home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_ |
| -subnet_name_subnet_name_} -firewall-policy data-auto-revert_revert_false |

   - 서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
   - 를 클릭합니다 `-data-protocol` ONTAP 9.6부터 서비스 정책을 사용하여 LIF를 생성할 때 매개 변수가 필요하지 않습니다. ONTAP 9.5 이하 버전을 사용하는 경우 `-data-protocol` LIF를 생성할 때 매개 변수를 지정해야 하며 나중에 데이터 LIF를 폐기 및 재생성하지 않고 수정할 수 없습니다.
   - 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. 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.

2. LIF가 성공적으로 생성되었는지 확인합니다.

네트워크 인터페이스 쇼

3. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

| 다음을 확인하려면… | 사용… |
| --- | --- |
| IPv4 주소입니다 | 네트워크 핑 |
| IPv6 주소입니다 | 네트워크 핑6 |

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

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

```
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.
```

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스 복원"

# ONTAP SMB 호스트 이름 확인을 위해 DNS를 활성화합니다

명령을 사용하여 SVM에서 DNS를 사용하도록 설정하고, 호스트 이름 확인에 DNS를 사용하도록 구성할 수 `vserver services name-service dns` 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다. 에 대한 자세한 내용은 `vserver services name-service dns` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. `vserver services name-service dns create`DNS 서버 이름을 하나만 입력하면 명령이 경고를 표시합니다. 에 대한 자세한 내용은 `vserver services name-service dns create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

에 대해 자세히 "SVM에서 동적 DNS 구성"알아보십시오.

단계

1. SVM에서 DNS를 활성화합니다. 'vserver services name-service dns create-vserver vserver_name-domain domain_name-name-servers ip_address-state enabled'

   다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 표시합니다.

   다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

# Active Directory 도메인에서 SMB 서버를 설정합니다

## SMB 서버에 대한 ONTAP 시간 서비스를 구성합니다

Active Domain 컨트롤러에서 SMB 서버를 생성하기 전에 SMB 서버가 속할 도메인의 도메인 컨트롤러에 대한 클러스터 시간 및 시간이 5분 이내에 일치하는지 확인해야 합니다.

이 작업에 대해

Active Directory 도메인에서 사용하는 것과 동일한 NTP 서버를 동기화에 사용하도록 클러스터 NTP 서비스를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 설정할 수 있습니다.

단계

1. cluster time-service NTP server create 명령을 사용하여 시간 서비스를 구성합니다.
   - 대칭 인증 없이 시간 서비스를 구성하려면 'cluster time-service ntp server create-server_ip_address' 명령을 입력합니다
   - 대칭적 인증으로 시간 서비스를 구성하려면 'cluster time-service ntp server create-server_ip_address-key-id key-id key_id"cluster time-service ntp server create-server 10.10.10.1"cluster time-service ntp server create-server 10.10.10.10.10.10.2' 명령을 입력한다
2. cluster time-service ntp server show 명령을 사용하여 시간 서비스가 올바르게 설정되었는지 확인합니다.

   클러스터 시간 서비스 NTP 서버가 표시됩니다

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

관련 정보

- "클러스터 시간 - 서비스 NTP"

## NTP 서버에서 대칭 인증을 관리하기 위한 ONTAP 명령

ONTAP 9.5부터 NTP(네트워크 시간 프로토콜) 버전 3이 지원됩니다. NTPv3에는 SHA-1 키를 사용한 대칭 인증이 포함되어 있어 네트워크 보안을 강화합니다.

| 수행할 작업... | 이 명령 사용... |
| --- | --- |
| 대칭 인증 없이 NTP 서버를 구성합니다 | 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 서버 이름(server_name)을 만듭니다 |
| 대칭 인증을 사용하여 NTP 서버를 구성합니다 | 클러스터 시간 서비스 NTP 서버는 '-server"server_ip_address"-key-id"key_id'를 생성합니다 |
| 기존 NTP 서버에 대칭 인증 사용 기존 NTP 서버는 필요한 키 ID를 추가하여 인증을 사용하도록 수정할 수 있습니다 | 클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 서버 이름 키 ID 키 ID |
| 공유 NTP 키를 구성합니다 | 클러스터 시간 서비스 NTP 키는 ``id"sshared_key_id' -type'sshared_key_type' -value'sshared_key_value'를 만듭니다<br>공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다 |
| 알 수 없는 키 ID로 NTP 서버를 구성합니다 | 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다 |
| NTP 서버에 키 ID가 구성되지 않은 서버를 구성합니다. | 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다<br>키 ID, 유형 및 값은 NTP 서버에 구성된 키 ID, 유형 및 값과 동일해야 합니다. |
| 대칭 인증을 사용하지 않도록 설정합니다 | 클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 서버 이름 인증 비활성화 |

관련 정보

- "클러스터 시간 - 서비스 NTP"

## ONTAP Active Directory 도메인에 SMB 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 AD(Active Directory) 도메인을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버와 SMB 서버에 연결할 도메인의 AD 도메인 컨트롤러에 연결할 수 있어야 합니다.

SMB 서버에 연결할 AD 도메인에서 시스템 계정을 만들 수 있는 권한이 있는 모든 사용자는 SVM에 SMB 서버를 생성할 수 있습니다. 여기에는 다른 도메인의 사용자가 포함될 수 있습니다.

SMB 서버를 생성하려면 조직 단위(OU)에 대해 다음과 같은 최소 권한이 필요합니다.

- 컴퓨터 객체 생성
- 컴퓨터 개체 삭제
- 비밀번호 재설정
- 읽기 및 쓰기 계정 제한 사항
- DNS 호스트 이름에 대한 쓰기 검증됨
- 서비스 주체 이름에 대한 쓰기 유효성 검사
- msDS-SupportedEncryptedTypes 읽기
- msDS-SupportedEncryptedTypes 쓰기

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-Uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

이 작업에 대해

Activity Directory 도메인에서 SMB 서버를 생성하는 경우:

- 도메인을 지정할 때는 FQDN(정규화된 도메인 이름)을 사용해야 합니다.
- 기본 설정은 Active Directory CN=Computer 개체에 SMB 서버 컴퓨터 계정을 추가하는 것입니다.
- `-ou` 옵션을 사용하여 SMB 서버를 다른 OU에 추가하도록 선택할 수 있습니다.
- SMB 서버에 대해 쉼표로 구분된 하나 이상의 NetBIOS 별칭 목록(최대 200)을 추가하도록 선택할 수도 있습니다.

  SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 서버의 이름에 응답하도록 할 때 유용합니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다. ONTAP는 `-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러 통신을 암호화해야 하며 기본값은 false입니다.

SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다. .

"SMB 관리" SMB 서버 구성 옵션에 대한 자세한 내용은 에 나와 있습니다.

단계

1. smb 라이센스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

   SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

   SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이센스가 필요하지 않습니다.

2. AD 도메인에서 SMB 서버를 생성합니다.(+ vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou 조직_unit] [-NetBIOS-별칭 netbios_name,…] [-keytab -Uri {(ftp | http)://hostname | ip_address}] [-comment text]+'

   도메인에 참가할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

   다음 명령을 실행하면 도메인 " example.com`": 에 SMB 서버 "'smb_server01'"이 생성됩니다

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   다음 명령을 실행하면 도메인 "mydomain.com`" 에 SMB 서버 "sMB_server02"가 생성되고 keytab 파일을 사용하여 ONTAP 관리자를 인증합니다.

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

   이 예제에서 명령 출력은 "'sMB_SERVER01'"이라는 SMB 서버가 SVM vs1.example.com 에서 생성되어 "'example.com`" 도메인에 가입된 것을 보여 줍니다.

   ```
   cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                               Authentication Style: domain
                  CIFS Server Administrative Status: up
                            CIFS Server Description: -
                            List of NetBIOS Aliases: -
   ```

4. 필요한 경우 도메인 컨트롤러(ONTAP 9.8 이상)와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true'

예

다음 명령을 실행하면 ""example.com`"" 도메인의 SVM vs2.example.com 에 "sMB_server02" 이름의 SMB 서버가 생성됩니다. 컴퓨터 계정은 ""OU=ENG,OU=Corp,DC=example,DC=com" 컨테이너에 생성됩니다. SMB 서버에는 NetBIOS 별칭이 할당됩니다.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

다음 명령을 사용하면 다른 도메인의 사용자(이 경우 신뢰할 수 있는 도메인 관리자)가 SVM vs3.example.com 에 "'smb_server03" 이름의 SMB 서버를 생성할 수 있습니다. '-domain' 옵션은 SMB 서버를 생성하려는 홈 도메인(DNS 구성에 지정됨)의 이름을 지정합니다. 사용자 이름 옵션은 신뢰할 수 있는 도메인의 관리자를 지정합니다.

- 홈 도메인: example.com
- 신뢰할 수 있는 도메인: trust.lab.com
- 신뢰할 수 있는 도메인의 사용자 이름: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

## ONTAP SMB 인증을 위한 keytab 파일을 생성합니다

ONTAP 9.7부터 ONTAP는 keytab 파일을 사용하여 AD(Active Directory) 서버에서 SVM 인증을 지원합니다. AD 관리자는 keytab 파일을 생성하여 ONTAP 관리자가 이를 URI(Uniform Resource Identifier)로 사용할 수 있도록 합니다. 이 URI는 'vserver cifs' 명령에 AD 도메인과의 Kerberos 인증이 필요한 경우에 제공됩니다.

AD 관리자는 표준 Windows Server "ktpass" 명령을 사용하여 keytab 파일을 만들 수 있습니다. 이 명령은 인증이 필요한 기본 도메인에서 실행해야 합니다. "ktpass" 명령은 기본 도메인 사용자에 대해서만 keytab 파일을 생성하는 데 사용할 수 있으며, trusted-domain 사용자를 사용하여 생성된 키는 지원되지 않습니다.

Keytab 파일은 특정 ONTAP 관리자 사용자를 위해 생성됩니다. admin 사용자의 암호가 변경되지 않는 한, 특정 암호화 유형 및 도메인에 대해 생성된 키는 변경되지 않습니다. 따라서 admin 사용자의 암호를 변경할 때마다 새 keytab 파일이 필요합니다.

지원되는 암호화 유형은 다음과 같습니다.

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP는 DES-CBC-CRC 암호화 유형을 지원하지 않습니다.

- RC4-HMAC

AES256은 가장 높은 암호화 유형으로, ONTAP 시스템에서 활성화된 경우 사용해야 합니다.

keytab 파일은 admin 암호를 지정하거나 임의로 생성된 암호를 사용하여 생성할 수 있습니다. 그러나 언제든지 한 개의 암호 옵션만 사용할 수 있습니다. AD 서버에서는 키 탭 파일 내의 키를 해독하기 위해 관리자 사용자 고유의 개인 키가 필요하기 때문입니다. 특정 관리자에 대한 개인 키를 변경하면 keytab 파일이 무효화됩니다.

# 워크그룹에서 **SMB** 서버를 설정합니다

## **ONTAP** 워크그룹의 **SMB** 서버 구성에 대해 알아보십시오

## 작업 그룹에서 SMB 서버를 구성원으로 설정하는 작업은 SMB 서버를 생성한 다음 로컬 사용자 및 그룹을 만드는 작업으로 구성됩니다.

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 작업 그룹에서 SMB 서버를 구성할 수 있습니다.

작업 그룹 모드의 SMB 서버는 NTLM 인증만 지원하며 Kerberos 인증을 지원하지 않습니다.

## 지정된 작업 그룹을 사용하여 **ONTAP SVM**에 **SMB** 서버를 생성합니다

## "vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 작업 그룹을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버에 연결할 수 있어야 합니다.

이 작업에 대해

워크그룹 모드의 SMB 서버는 다음 SMB 기능을 지원하지 않습니다.

- SMB3 Witness 프로토콜
- SMB3 CA 공유

- SMB를 통한 SQL
- 폴더 리디렉션
- 로밍 프로필
- GPO(그룹 정책 개체)
- VSS(볼륨 스냅샷 서비스)

및 선택적 구성 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

단계

1. smb 라이센스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

   SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

   SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이센스가 필요하지 않습니다.

2. 워크그룹에서 SMB 서버를 생성합니다. 'vserver cifs create-vserver vserver_name-cifs-server cifs_server_name-workgroup workgroup_name[-comment text]'

   다음 명령을 실행하면 워크그룹 workgroup01에 SMB 서버 "smb_server01"이 생성됩니다.

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

   다음 예제에서 명령 출력은 "'workgroup01'" 워크그룹의 SVM vs1.example.com 에서 "'smb_server01'" 이름의 SMB 서버가 생성되었음을 보여 줍니다.

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                    Workgroup Name: workgroup01
                               Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

작업을 마친 후

작업 그룹의 CIFS 서버의 경우 SVM에서 로컬 사용자와 로컬 그룹을 생성해야 합니다(선택 사항).

관련 정보

"SMB 관리"

## 로컬 ONTAP SMB 사용자 계정을 생성합니다

SMB 연결을 통해 SVM에 포함된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. SMB 세션을 생성할 때 인증에 로컬 사용자 계정을 사용할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 사용자 기능이 기본적으로 활성화됩니다.

로컬 사용자 계정을 생성할 때 사용자 이름을 지정해야 하며 계정을 연결할 SVM을 지정해야 합니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs users-and-groups local-user` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 로컬 사용자:'vserver cifs users-and-groups local-user create-vserver_vserver_name_-user-name_user_name__optional_parameters_'를 생성합니다

   다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

   - 이름

     사용자의 전체 이름입니다.

   - ``설명''

     로컬 사용자에 대한 설명입니다.

   - '-is-account-disabled{true|false}'

     사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.

   명령을 실행하면 로컬 사용자 암호를 묻는 메시지가 표시됩니다.

2. 로컬 사용자의 암호를 입력한 다음 암호를 확인합니다.
3. 사용자가 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'

예

다음 예에서는 SVM vs1.example.com 과 관련된 "sUE Chang"이라는 전체 이름으로 로컬 사용자 "sMB_SERVER01\sue"를 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

## 로컬 ONTAP SMB 그룹을 생성합니다

SMB 연결을 통해 SVM과 관련된 데이터에 대한 액세스 권한을 부여하는 데 사용할 수 있는 로컬 그룹을 생성할 수 있습니다. 그룹의 구성원이 보유한 사용자 권한 또는 기능을 정의하는 권한을 할당할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 그룹 기능이 기본적으로 활성화됩니다.

로컬 그룹을 생성할 때 그룹 이름을 지정해야 하며 그룹을 연결할 SVM을 지정해야 합니다. 로컬 도메인 이름을 사용하거나 사용하지 않고 그룹 이름을 지정할 수 있으며, 선택적으로 로컬 그룹에 대한 설명을 지정할 수 있습니다. 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs users-and-groups local-group` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 로컬 그룹 'vserver cifs users-and-groups local-group create-vserver vserver_name-group-name group_name'을 생성합니다

   다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

   - ``설명''

     로컬 그룹에 대한 설명입니다.

2. 그룹이 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-group show-vserver vserver_name'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 "sMB_SERVER01\engineering"을 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

작업을 마친 후

새 그룹에 구성원을 추가해야 합니다.

## 로컬 **ONTAP SMB** 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자가 해당 그룹에 연결된 권한을 가지도록 하려는 경우에 유용합니다.

이 작업에 대해

더 이상 로컬 사용자, 도메인 사용자 또는 도메인 그룹이 그룹의 구성원 자격에 따라 액세스 권한이나 권한을 가지도록 하지 않으려면 그룹에서 해당 구성원을 제거할 수 있습니다.

로컬 그룹에 구성원을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- special_everyone_group에 사용자를 추가할 수 없습니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- special_everyone_group에서 구성원을 제거할 수 없습니다.
- 로컬 그룹에서 구성원을 제거하려면 ONTAP에서 해당 이름을 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에 구성원을 추가하거나 그룹에서 구성원을 제거합니다.
    - 멤버(+ vserver cifs users-and-groups local-group add-member -vserver_name -group-name group_name -member-name name[,…]+')를 추가합니다

로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정하여 지정된 로컬 그룹에 추가할 수 있습니다.

- 멤버(+ vserver cifs users-and-groups local-group remove-member-vserver vserver_name -group-name group_name -member-name[,…]+')를 제거합니다

  로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정하여 지정된 로컬 그룹에서 제거할 수 있습니다.

예

다음 예에서는 SVM vs1.example.com 에서 로컬 사용자 "sMB_SERVER01\SUB""를 로컬 그룹 "sMB_SERVER01\engineering""에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

다음 예에서는 SVM vs1.example.com 에서 로컬 그룹 "sMB_SERVER01\engineering"에서 로컬 사용자 "sMB_SERVER01\SUB" 및 "sMB_SERVER01\James"를 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

# 활성화된 ONTAP SMB 버전을 확인합니다

## ONTAP 9 릴리즈에서는 클라이언트 및 도메인 컨트롤러와의 연결에 대해 기본적으로 설정되는 SMB 버전을 결정합니다. SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

이 작업에 대해

클라이언트 및 도메인 컨트롤러 모두에 연결하는 경우 가능하면 SMB 2.0 이상을 활성화해야 합니다. 보안상의 이유로 SMB 1.0은 사용하지 않는 것이 좋습니다. 사용자 환경에서 필요하지 않은 것으로 확인된 경우에는 사용하지 않도록 설정해야 합니다.

ONTAP 9.3부터는 새 SVM에서 기본적으로 비활성화되어 있습니다.

SMB1-enabled-for-dc-connections가 false로 설정되어 있고 -SMB1-enabled가 true로 설정되어 있으면 ONTAP는 SMB 1.0 연결을 클라이언트로 거부하지만 인바운드 SMB 1.0 연결을 서버로 계속 허용합니다.

"SMB 관리" 지원되는 SMB 버전 및 기능에 대한 자세한 내용은 에 나와 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 활성화된 SMB 버전을 확인합니다.

```
vserver cifs options show
```

목록을 아래로 스크롤하여 클라이언트 연결에 대해 설정된 SMB 버전을 볼 수 있으며 AD 도메인 연결에 대해 AD 도메인에서 SMB 서버를 구성하는 경우

3. 필요에 따라 클라이언트 연결에 대해 SMB 프로토콜을 설정하거나 해제합니다.
   - SMB 버전 활성화하기:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

에 사용할 수 있는 값 `smb_version`:

- '-SMB1-활성화됨'
- '-SMB2-ENABLED'입니다
- '-SMB3-enabled'입니다
- `-smb31-enabled`

다음 명령을 실행하면 SVM vs1.example.com 에서 SMB 3.1이 활성화됩니다. `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true`

   - SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. SMB 서버가 Active Directory 도메인에 있는 경우 필요에 따라 DC 연결에 대한 SMB 프로토콜을 설정하거나 해제합니다.
   - SMB 버전 활성화하기:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

# ONTAP SMB 서버를 DNS 서버에 매핑합니다

## Windows 사용자가 SMB 서버 이름에 드라이브를 매핑할 수 있도록 사이트의 DNS 서버에는 SMB 서버 이름 및 모든 NetBIOS 별칭을 가리키는 항목이 데이터 LIF의 IP 주소에 있어야 합니다.

시작하기 전에

사이트의 DNS 서버에 대한 관리 액세스 권한이 있어야 합니다. 관리 액세스 권한이 없는 경우 DNS 관리자에게 이 작업을 수행하도록 요청해야 합니다.

이 작업에 대해

SMB 서버 이름에 NetBIOS 별칭을 사용하는 경우 각 별칭에 대해 DNS 서버 진입점을 만드는 것이 좋습니다.

단계

1. DNS 서버에 로그인합니다.
2. 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 LIF의 IP 주소에 매핑합니다.
3. NetBIOS 별칭을 사용하는 경우 별칭 정규 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버 데이터 LIF의 IP 주소에 매핑합니다.

결과

매핑이 네트워크를 통해 전파되면 Windows 사용자는 드라이브를 SMB 서버 이름 또는 NetBIOS 별칭에 매핑할 수 있습니다.