Active Directory 도메인에서 SMB 서버를 설정합니다

ONTAP 9

NetApp
March 04, 2026

목차

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

수행할 작업...	이 명령 사용...
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 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 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.