보안 **LDAP** 세션 통신

ONTAP 9

NetApp
February 12, 2026

목차

보안 LDAP 세션 통신 . . . 1
ONTAP SMB LDAP 서명 및 봉인에 대해 자세히 알아보십시오 . . . 1
ONTAP SMB 서버에서 LDAP 서명 및 봉인을 활성화합니다 . . . 1
TLS를 통해 LDAP를 구성합니다 . . . 1
ONTAP SMB SVM에 대한 자체 서명 루트 CA 인증서를 내보냅니다 . . . 1
ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다 . . . 2
ONTAP SMB 서버에서 TLS를 통한 LDAP를 활성화합니다 . . . 3

보안 LDAP 세션 통신

ONTAP SMB LDAP 서명 및 봉인에 대해 자세히 알아보십시오

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록 서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

ONTAP SMB 서버에서 LDAP 서명 및 봉인을 활성화합니다

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-session-security-for-ad-ldap{none|sign|seal}'

   서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

> SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

TLS를 통해 LDAP를 구성합니다

ONTAP SMB SVM에 대한 자체 서명 루트 CA 인증서를 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: technet.microsoft.com"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

   "Microsoft TechNet 라이브러리: technet.microsoft.com"

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"Microsoft TechNet 라이브러리"

ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:
   a. 인증서 설치를 시작합니다. 'Security certificate install - vserver vserver_name -type server -ca'

      콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

   b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 ---- '----'로 끝나는 종료 인증서 ---- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.
   c. 인증서가 올바르게 표시되는지 확인합니다.
   d. Enter 키를 눌러 설치를 완료합니다.
2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserver_vserver_name_'

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"

ONTAP SMB 서버에서 TLS를 통한 LDAP를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(Active Directory) 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 ' vserver cifs security modify ' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- "ONTAP NFS SVM용 LDAP에 대해 알아보세요"
- "Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver_vserver_name_

> SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.

저작권 정보

상표 정보