



# LDAP over TLSの設定

## ONTAP 9

NetApp  
January 23, 2026

# 目次

LDAP over TLSの設定 .....	1
ONTAP SMB SVMの自己署名ルートCA証明書をエクスポートする .....	1
ONTAP SMB SVMに自己署名ルートCA証明書をインストールする .....	1
ONTAP SMBサーバでLDAP over TLSを有効にする .....	2

# LDAP over TLSの設定

## ONTAP SMB SVMの自己署名ルートCA証明書をエクスポートする

Active Directory通信の保護にLDAP over SSL/TLSを使用するには、まずActive Directory証明書サービスの自己署名ルートCA証明書のコピーを証明書ファイルにエクスポートし、それをASCIIテキスト ファイルに変換する必要があります。ONTAPは、このテキスト ファイルを使用して証明書をStorage Virtual Machine (SVM) にインストールします。

開始する前に

Active Directory証明書サービスがすでにインストールされ、CIFSサーバが属するドメイン用に設定されている必要があります。Active Directory証明書サービスのインストールと設定の詳細については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ : [technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)"

手順

1. .pem`テキスト形式のドメイン コントローラのルート CA 証明書を取得します。

"Microsoft TechNetライブラリ : [technet.microsoft.com/ja-jp/library/](https://technet.microsoft.com/ja-jp/library/)"

終了後の操作

SVMに証明書をインストールします。

関連情報

"Microsoft TechNetライブラリ"

## ONTAP SMB SVMに自己署名ルートCA証明書をインストールする

LDAPサーバにバインドするときにTLSを使用したLDAP認証が必要な場合は、まず自己署名されたルートCA証明書をSVMにインストールする必要があります。

タスク概要

TLS通信を使用するONTAP内のすべてのアプリケーションは、Online Certificate Status Protocol (OCSP) を使用してデジタル証明書のステータスを確認できます。LDAP over TLSでOCSPが有効になっている場合、失効した証明書は拒否され、接続は失敗します。

手順

1. 自己署名ルートCA証明書をインストールします。
  - a. 証明書のインストールを開始します : `security certificate install -vserver vservice_name -type server-ca`

コンソール出力に次のメッセージが表示されます： Please enter Certificate: Press  
<Enter> when done

- b. 証明書 `.pem` ファイルをテキスト エディターで開き、`-----BEGIN CERTIFICATE-----` で始まり `-----END CERTIFICATE-----` で終わる行を含む証明書をコピーして、コマンド プロンプトの後に貼り付けます。
  - c. 証明書が正しく表示されることを確認します。
  - d. Enterキーを押して、インストールを完了します。
2. 証明書がインストールされていることを確認します： `security certificate show -vserver vserver_name`

#### 関連情報

- ["security certificate install"](#)
- ["セキュリティ証明書の表示"](#)

## ONTAP SMBサーバでLDAP over TLSを有効にする

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するためには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

ONTAP 9.10.1以降、Active Directory (AD) とネームサービスのLDAP接続の両方で、LDAPチャンネルバインディングがデフォルトでサポートされます。ONTAPは、Start-TLSまたはLDAPSが有効で、セッションセキュリティが署名またはシールに設定されている場合にのみ、LDAP接続でチャンネルバインディングを試行します。ADサーバとのLDAPチャンネルバインディングを無効化または再有効化するには、``vserver cifs security modify`` コマンドで ``-try-channel-binding-for-ad-ldap`` パラメータを使用します。

詳細については、以下を参照してください。

- ["ONTAP NFS SVMのLDAPについて学ぶ"](#)
- ["Windows の 2020 年 LDAP チャンネル バインディングおよび LDAP 署名要件"](#)。

#### 手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を許可するSMBサーバのセキュリティ設定を構成します： `vserver cifs security modify -vserver vserver_name -use-start-tls-for -ad-ldap true`
2. LDAP over TLS セキュリティ設定が次のように設定されていることを確認します： `true vserver cifs security show -vserver vserver_name`



SVMが名前マッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、``vserver services name-service ldap client modify`` コマンドを使用して ``-use-start-tls`` オプションも変更する必要があります。

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。