



セキュアなLDAPセッション通信

ONTAP 9

NetApp
December 20, 2024

目次

セキュアなLDAPセッション通信	1
LDAPの署名と封印の概念	1
CIFSサーバでLDAPの署名と封印を有効にする	1
LDAP over TLSの設定	1

セキュアなLDAPセッション通信

LDAPの署名と封印の概念

ONTAP 9以降では、署名と封印を設定して、Active Directory (AD) サーバへのクエリに対してLDAPセッションセキュリティを有効にすることができます。Storage Virtual Machine (SVM) のCIFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーテクノロジーを使用してLDAPペイロードデータの整合性を確認します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。LDAPトラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、*ldap Security Level* オプションで指定します。デフォルトは `none`。

CIFSトラフィックに対するLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`` 使用してSVMで有効にします ``-session-security-for-ad-ldap`。

CIFSサーバでLDAPの署名と封印を有効にする

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

開始する前に

AD サーバ管理者に問い合わせ、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver vserver_name -session-security -for-ad-ldap {none|sign|seal}`

署名(`sign`、データ整合性)、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、`none``署名と封印のどちらも有効にしないことも可能です。デフォルト値は `none``。

2. LDAPの署名と封印のセキュリティ設定が正しく設定されていることを確認します。 `vserver cifs security show -vserver vserver_name`



SVMがネーム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）の照会と同じLDAPサーバを使用する場合は、コマンドのオプション `vserver services name-service ldap client modify`` に対応する設定を有効にする必要があります。 ``-session-security`

LDAP over TLSの設定

自己署名ルートCA証明書のコピーをエクスポートする

LDAP over SSL/TLSを使用してActive Directory通信を保護するには、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、ASCIIテキストファイルに変換する必要があります。ONTAPでは、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

CIFSサーバが属しているドメイン用にActive Directory証明書サービスがインストールされ、設定されている必要があります。Active Director証明書サービスのインストールと設定については、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"

ステップ

1. ドメインコントローラのルートCA証明書をテキスト形式で取得します .pem。

"Microsoft TechNetライブラリ : technet.microsoft.com"

終了後

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"

自己署名ルートCA証明書をSVMにインストールする

LDAPサーバへのバインド時にTLSを使用したLDAP認証が必要な場合は、最初に自己署名ルートCA証明書をSVMにインストールする必要があります。

タスクの内容

LDAP over TLSが有効な場合、SVM上のONTAP LDAPクライアントでは、ONTAP 9 .0および9.1の破棄された証明書はサポートされません。

ONTAP 9 .2以降では、TLS通信を使用するONTAP内のすべてのアプリケーションで、オンライン証明書ステータスプロトコル (OCSP) を使用してデジタル証明書ステータスを確認できます。OCSPがLDAP over TLSに対して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 vserver_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. 証明書ファイルをテキストエディタで開き .pem、で始まる行とで終わる -----END

CERTIFICATE-----`行を含めて証明書をコピーし `-----BEGIN CERTIFICATE-----、コマンドプロンプトのあとに証明書を貼り付けます。

- 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たことを確認します。 `security certificate show -vserver vserver_name`

サーバで **LDAP over TLS** を有効にします

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。

10.1以降では、**ONTAP 9**チャンネルバインドが**Active Directory (AD)** 接続とネームサービス**LDAP**接続の両方で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封印のいずれか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または再度有効にするには、コマンドでパラメータを `vserver cifs security modify`使用し`-try-channel-binding-for-ad-ldap`ます。`

詳細については、以下を参照してください。

- "LDAPの概要"
- "2020年のWindows向けLDAPチャンネルバインドおよびLDAP署名の要件"です。

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行います。 `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. LDAP over TLSのセキュリティ設定がに設定されていることを確認し `true`ます。 `vserver cifs security show -vserver vserver_name`



SVMがネーム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、コマンドを使用してオプションを `vserver services name-service ldap client modify`変更する必要もあります。 `-use-start-tls`

著作権に関する情報

Copyright © 2024 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。