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

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。デフォルトはです `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て、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。デフォルト値はです `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）の照会に同じ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`で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**接続でチャネルバインディングを試行します。**AD**サーバとの**LDAP**チャ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

商標に関する情報