ASA リモート アクセス VPN IKE/SSL - パスワード期限切れと RADIUS、TACACS、LDAP 変更の設定例

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[ローカル認証を使用する ASA](#)
[ACS ユーザとローカル ユーザ](#)
[ACS ユーザと Active Directory ユーザ](#)
[RADIUS 経由で ACS を使用する ASA](#)
[TACACS+ 経由で ACS を使用する ASA](#)
[LDAP 搭載の ASA](#)
[SSL の Microsoft LDAP](#)
[有効期限が切れる前の LDAP と警告](#)
[ASA と L2TP](#)
[ASA SSL VPN Client](#)
[ASA SSL Web ポータル](#)
[ACS ユーザのパスワード変更](#)
[確認](#)
[トラブルシューティング](#)
[関連情報](#)

概要

このドキュメントでは、終端に Cisco 適応型セキュリティ アプライアンス（ASA）を使用したリモート アクセス VPN トンネルの有効期限およびパスワード変更機能について説明します。 このドキュメントでは、次を対象としています。

- クライアントの種類： Cisco VPN Client および Cisco AnyConnect セキュア モビリティ
- 異なるプロトコル： TACACS、RADIUS、Lightweight Directory Access Protocol（LDAP）
- Cisco Secure Access Control System（ACS）の異なるストア： ローカルおよび Active Directory（AD）

前提条件

要件

次の項目に関する知識があることが推奨されます。

- コマンドライン インターフェイス（CLI）を使用した ASA 設定に関する知識
- ASA での VPN 設定に関する基本的な知識
- Cisco Secure ACS の基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス、バージョン 8.4 以降
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System、バージョン 5.4 以降
- Cisco AnyConnect セキュア モビリティ、バージョン 3.1
- Cisco VPN Client、リリース 5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

> **注**：
>
> このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。
>
> debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

ローカル認証を使用する ASA

ローカルに定義されたユーザの ASA では、パスワードの有効期限またはパスワードの変更機能は使用できません。 RADIUS、TACACS、LDAP、または Windows NT などの外部サーバが必要になります。

ACS ユーザとローカル ユーザ

ACS では、ローカルに定義されたユーザに対するパスワードの有効期限とパスワードの変更機能の両方をサポートしています。 たとえば、新しく作成されたユーザが次回ログインする際にパスワードを変更するよう強制したり、指定した日付にアカウントを無効にしたりすることができます。

すべてのユーザのパスワード ポリシーを設定できます。 たとえば、パスワードの有効期限が切れ

るとユーザ アカウントを無効にしたり（ログイン機能なしでブロック）、パスワードを変更するオプションを提示したりすることができます。

ユーザ固有の設定はグローバル設定よりも優先されます。

ACS-RESERVED-Never-Expired はユーザ ID の内部属性です。

この属性はユーザによって有効にされ、グローバル アカウントの有効期限の設定を無効にするために使用できます。 グローバル ポリシーによって無効にされる予定でも、この設定を使用するとそのアカウントは無効になりません。

ACS ユーザと Active Directory ユーザ

ACS は、AD データベースでユーザを確認するように設定できます。 Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAPv2）を使用する場合、パスワードの有効期限とパスワードの変更がサポートされます。 詳細については、『Cisco Secure Access Control System 5.4 ユーザ ガイド』の「ACS 5.4 での認証」にある「認証プロトコルと ID ストアの互換性」を参照してください。

次の項で説明するように、ASA では、パスワード管理機能を使用して MSCHAPv2 が強制的に使われるように ASA を設定できます。

ACS はドメイン コントローラ（DC）のディレクトリに接続してパスワードを変更する際に、Common Internet File System（CIFS）分散コンピューティング環境およびリモート プロシージャ コール（DCE/RPC）のコールを使用します。

ASA は AD パスワードを変更するために RADIUS と TACACS+ 両方のプロトコルを使用して ACS に接続できます。

RADIUS 経由で ACS を使用する ASA

RADIUS プロトコルはパスワードの有効期限またはパスワードの変更をネイティブでサポートしていません。 通常、Password Authentication Protocol（PAP）は RADIUS で使用されます。 ASA はユーザ名とパスワードをプレーン テキストで送信し、パスワードは RADIUS 共有秘密を使用して暗号化されます。

一般的なシナリオでは、ユーザのパスワードが期限切れになると、ACS は ASA に Radius-Reject メッセージを返します。 ACS には次のように表示されます。

ASA では、これは単純な Radius-Reject メッセージであり、認証に失敗します。

この問題を解決するために、ASA では、tunnel-group 設定で **password-management** コマンドを使用できます。

```
tunnel-group RA general-attributes
 authentication-server-group ACS
 password-management
```

password-management コマンドは、PAP ではなく MSCHAPv2 が強制的に ASA で使用されるように Radius-Request で動作を変更します。

MSCHAPv2 プロトコルはパスワードの期限切れおよびパスワードの変更をサポートしています

。 そのため、Xauth フェーズ中に VPN ユーザが特定の tunnel-group にアクセスすると、ASA による Radius-Request に MS-CHAP-Challenge が含まれるようになります。

パスワードを変更する必要があることが ACS で認識されると、MSCHAPv2 エラー 648 の Radius-Reject メッセージが返されます。

ASA はそのメッセージを認識し、Cisco VPN Client から新しいパスワードを要求するために MODE_CFG を使用します。

```
Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received Password Expiration from Auth server!
```

Cisco VPN Client に、新しいパスワードの入力を求めるダイアログボックスが表示されます。

ASA は MS-CHAP-CPW および MS-CHAP-NT-Enc-PW ペイロード（新しいパスワード）とともに別の Radius-Request を送信します。

ACS は要求を確認し、MS-CHAP2-Success とともに Radius-Accept を返します。

ACS で「24204 Password changed successfully」がレポートされ、この動作を確認できます。

ASA は認証が正常に行われたことをレポートし、クイック モード（QM）プロセスを続行します。

```
Oct 02 06:22:28 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

TACACS+ 経由で ACS を使用する ASA

同様に、TACACS+ をパスワードの有効期限とパスワードの変更に使用できます。 ASA では MSCHAPv2 ではなく ASCII の認証タイプで TACACS+ を使用するため、password-management 機能は必要ありません。

複数のパケットが交換され、ACS は新しいパスワードを要求します。

Cisco VPN Client に、新しいパスワードの入力を求めるダイアログボックス（RADIUS が使用するダイアログとは異なります）が表示されます。

ACS は新規パスワードの確認を要求します。

Cisco VPN Client に確認ボックスが表示されます。

確認が正しい場合、ACS は正常に認証が行われたことをレポートします。

ACS は次に、パスワードが正常に変更されたイベントをログに記録します。

ASA のデバッグに、交換プロセス全体と認証が正常に行われたことが表示されます。

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
```

```
   Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

このパスワードの変更は ASA に対して完全に透過的に行われます。 要求パケットと応答パケットがより多く使用されるため TACACS+ セッションは少し長くなります。これは VPN クライアントで解析され、パスワードを変更するユーザに表示されます。

LDAP 搭載の ASA

パスワードの有効期限とパスワードの変更は Microsoft AD と Sun LDAP サーバのスキーマで完全にサポートされます。

パスワードを変更する場合、サーバは「bindresponse = invalidCredentials」を「error = 773」とともに返します。 このエラーは、パスワードをリセットする必要があることを示します。 一般的なエラー コードには次のようなものがあります。

エラー コード	Error
525	User not found
52e	証明書が無効です
530	Not permitted to logon at this time
531	Not permitted to logon at this workstation
532	Password expired
533	Account disabled
701	Account expired
773	User must reset password
775	ユーザ アカウントのロック

LDAP サーバを設定します。

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
   Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

tunnel-group および password-management 機能でこの設定を使用します。

```
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
 password-management
```

パスワード変更が必要になる AD ユーザを設定します。

ユーザが Cisco VPN Client を使用しようとすると、ASA は無効なパスワードをレポートします。

```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[111] Session Start
[111] New request Session, context 0xbd835c10, reqType = Authentication
[111] Fiber started
[111] Creating LDAP context with uri=ldap://10.48.66.128:389
[111] Connect to LDAP server: ldap://10.48.66.128:389, status = Successful
[111] supportedLDAPVersion: value = 3
[111] supportedLDAPVersion: value = 2
[111] Binding as Administrator
[111] Performing Simple authentication for Administrator to 10.48.66.128
[111] LDAP Search:
       Base DN = [CN=USers,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[111] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[111] Talking to Active Directory server 10.48.66.128
[111] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[111] Read bad password count 2
[111] Binding as cisco-test
[111] Performing Simple authentication for cisco-test to 10.48.66.128
[111] Simple authentication for cisco-test returned code (49) Invalid
credentials
[111] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 773, vece
[111] Invalid password for cisco-test
```

資格情報が無効な場合、52e エラーが表示されます。

```
[110] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 52e, vece
```

次に、Cisco VPN Client はパスワードの変更を要求します。

このダイアログボックスにはポリシーが表示されるため、TACACS または RADIUS が使用するダイアログとは異なります。 この例のポリシーでは、パスワードの最小長は 7 文字です。

ユーザがパスワードを変更すると、このエラー メッセージが LDAP サーバから ASA に表示される可能性があります。

```
[113] Modify Password for cisco-test successfully converted password to unicode
[113] modify failed, no SSL enabled on connection
```

Microsoft ポリシーではパスワードの変更にセキュア ソケット レイヤ（SSL）を使用する必要があります。 設定を変更します。

```
aaa-server LDAP (outside) host 10.48.66.128
 ldap-over-ssl enable
```

SSL の Microsoft LDAP

デフォルトで、SSL 経由の Microsoft LDAP は機能しません。 この機能を有効にするには、正しいキーの拡張を使用してコンピュータのアカウントの証明書をインストールする必要があります。 詳細については、『How to enable LDAP over SSL with a third-party certification authority（サードパーティの証明機関が SSL 経由の LDAP を有効にする方法）』を参照してください。

ASA は LDAP 証明書を検証しないため、証明書は自己署名証明書です。 関連する機能拡張の要

求の詳細については、Cisco Bug ID CSCui40212 の『Allow ASA to validate certificate from LDAPS server（ASA で LDAPS サーバからの証明書の検証を許可する）』を参照してください。

注: ACS はバージョン 5.5 以降で LDAP 証明書を検証します。

証明書をインストールするには、mmc コンソールを開いて、[Add/Remove Snap-in] を選択し、証明書を追加したら、[Computer Account] を選択します。

[Local computer] を選択し、個人ストアに証明書をインポートして、関連する認証局（CA）を信頼済みストアに移動します。 証明書が信頼されていることを検証します。

ASA バージョン 8.4.2 にはバグがあり、SSL 経由で LDAP を使用しようとするとこのエラーが返される可能性があります。

```
ASA(config)# debug ldap 255

[142] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[142] supportedLDAPVersion: value = 3
[142] supportedLDAPVersion: value = 2
[142] Binding as Administrator
[142] Performing Simple authentication for Administrator to 10.48.66.128
[142] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=Administrator]
       Scope   = [SUBTREE]
[142] Request for Administrator returned code (-1) Can't contact LDAP server
```

ASA バージョン 9.1.3 では同じ設定で正しく機能します。 2 つの LDAP セッションがあります。最初のセッションはコード 773（Password expired）のエラーを返し、2 番目のセッションはパスワードの変更で使用されます。

```
[53] Session Start
[53] New request Session, context 0xadebe3d4, reqType = Modify Password
[53] Fiber started
[53] Creating LDAP context with uri=ldaps://10.48.66.128:636
[53] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.48.66.128
[53] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[53] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[53] Talking to Active Directory server 10.48.66.128
[53] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[53] Read bad password count 0
[53] Change Password for cisco-test successfully converted old password to
unicode
[53] Change Password for cisco-test successfully converted new password to
unicode
[53] Password for cisco-test successfully changed
[53] Retrieved User Attributes:

<....most attributes details ommitted for clarity>
accountExpires: value = 130256568000000000 <----- 100ns intervals since
January 1, 1601 (UTC)
```

パスワードの変更を検証するには、パケットを参照してください。 LDAP サーバの秘密キーは、SSL トラフィックを復号化するために Wireshark で使用できます。

ASA でのインターネット キー エクスチェンジ（IKE）/認証、許可、アカウンティング（AAA）デバッグは、RADIUS 認証シナリオで使用されるものとよく似ています。

有効期限が切れる前の LDAP と警告

LDAP では、パスワードの有効期限が切れる前に警告を送信する機能を使用できます。 この設定を使用して、ASA はパスワードの有効期限が切れる 90 日前にユーザに警告します。

```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

パスワードの有効期限が切れる 42 日前にユーザがログインを試行する場合の例は次のとおりです。

```
ASA# debug ldap 255
<some outputs removed for clarity>

[84] Binding as test-cisco
[84] Performing Simple authentication for test-cisco to 10.48.66.128
[84] Processing LDAP response for user test-cisco
[84] Message (test-cisco):
[84] Checking password policy
[84] Authentication successful for test-cisco to 10.48.66.128
[84] now: Fri, 04 Oct 2013 09:41:55 GMT, lastset: Fri, 04 Oct 2013 09:07:23
GMT, delta=2072, maxage=1244139139 secs
[84] expire in: 3708780 secs, 42 days
[84] Password expires Sat, 16 Nov 2013 07:54:55 GMT
[84] Password expiring in 42 day(s),threshold 90 days
```

ASA は警告を送信し、パスワードを変更するオプションを提示します。

ユーザがパスワードを変更した場合、新しいパスワードの入力を求めるプロンプトが表示され、通常のパスワード変更手順が開始されます。

ASA と L2TP

前の例では、IKE バージョン 1（IKEv1）と IPSec VPN を示しました。

Layer 2 Tunneling Protocol（L2TP）と IPSec、PPP は認証用のトランスポートとして使用されます。 パスワードの変更を機能させるためには、PAP ではなく MSCHAPv2 が必要です。

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

PPP セッション内の L2TP の拡張認証では、MSCHAPv2 がネゴシエートされます。

ユーザのパスワードの有効期限が切れると、コード 648 のエラーが返されます。

パスワードを変更する必要があります。 残りのプロセスは、MSCHAPv2 を使用した RADIUS のシナリオとよく似ています。

L2TP の設定方法に関する詳細については、事前共有キーを使用した Windows 2000/XP PC と PIX/ASA 7.2 の間の L2TP Over IPSec 設定例を参照してください。

ASA SSL VPN クライアント

前の例では、サポート終了（EOL）の IKEv1 と Cisco VPN Client を参照しました。

リモート アクセス VPN で推奨されるソリューションは、IKE バージョン 2（IKEv2）および SSL プロトコルを使用する Cisco AnyConnect セキュア モビリティです。 パスワードの変更とパスワードの有効期限機能は、Cisco VPN Client で実行される Cisco AnyConnect とまったく同様に動作します。

IKEv1 では、パスワードの変更とパスワードの有効期限データは、フェーズ 1.5 において ASA と VPN クライアントの間で交換されました（Xauth/モード設定）。

IKEv2 でも同様に、 コンフィギュレーション モードで CFG_REQUEST/CFG_REPLY パケットを使用します。

SSL の場合、データは制御 Datagram Transport Layer Security（DTLS）セッションで保存されます。

設定は ASA と同じです。

この設定例は、SSL 経由の LDAP サーバで Cisco AnyConnect と SSL プロトコルを使用しています。

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

正しいパスワード（期限切れのパスワード）を指定すると、Cisco AnyConnect は接続を試み、新しいパスワードを要求します。

このログはユーザの資格情報が 2 回入力されたことを示しています。

より詳細なログは、Diagnostic AnyConnect Reporting Tool（DART）から入手できます。

ASA SSL Web ポータル

同じログイン プロセスが Web ポータルでも行われます。

同じパスワードの期限切れとパスワードの変更プロセスが行われます。

ACS ユーザのパスワード変更

VPN 経由でパスワードは変更できませんが、ACS User Change Password（UCP）専用の Web サービスを使用できます。 詳細については、『Cisco Secure Access Control System 5.4 ソフトウェア開発者ガイド』の「 UCP Web サービスの使用」を参照してください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- CLI を使用した Cisco ASA 5500 シリーズ設定ガイド、8.4 および 8.6： セキュリティ アプライアンスのユーザ承認用の外部サーバの設定
- テクニカルサポートとドキュメント - Cisco Systems