UCS Managerと連携するためのDuo Multi Factor Authenticationの設定

内容

概要

このドキュメントでは、UCS ManagerでCisco Duo Multi-Factor Authentication(MFA)を実装するための設定とベストプラクティスについて説明します。

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。

- UCS マネージャ
- Cisco Duo

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

背景説明

Cisco UCS Managerは、リモートユーザログインに2要素認証を使用します。二要素認証ログインでは、パスワードフィールドにユーザ名、トークン、パスワードの組み合わせが必要です。

2要素認証は、Remote Authentication Dial-In User Service(RADIUS)またはTerminal Access Controller Access Control System +(TACACS+)プロバイダーグループを、これらのドメインに対する二要素認証を備えた指定認証ドメインとともに使用する場合にサポートされます。2要素認証はInternetwork Performance Monitor(IPM)をサポートしておらず、認証レルムがLightweight Directory Access Protocol(LDAP)に設定されている場合はサポートされません(LDAP)、ローカル、またはなし。

Duoの実装では、Multi-Factor Authenticationは、RADIUSまたはLDAPを介してローカルデバイスおよびアプリケーションから認証要求を受信し、オプションでLDAPディレクトリまたはRADIUS認証サーバに対してプライマリ認証を実行し、Duoに連絡してセカンダリ認証をを実行します。ユーザが2要素要求を承認すると、Duo Mobileからプッシュ通知として受信されるか、電話などのコールとして受信されると、Duoプロキシは認証を要求したデバイスまたはアプリケーションにアクセス承認を返します。

設定

この設定は、LDAPおよびRadiusを使用したUCS ManagerによるDuoの実装を成功させるための要件をカバーしています。

> **注**：Duo認証プロキシの基本設定については、Duoプロキシのガイドラインを確認してください： Duo Proxy Document

LDAP統合

UCS マネージャ

[UCS Manager] > [Admin Section] > [User Management] > [LDAP]に移動し、LDAPプロバイダSSLを有効にします。これは、LDAPデータベースとの通信に暗号化が必要であることを意味します。LDAPはSTARTTLSを使用します。これにより、使用ポート389による暗号化通信が可能になります。Cisco UCSでは、ポート636でSSL用にTransport Layer Security(TLS)セッションがネゴシエートされますが、最初の接続はポート389で暗号化されずに開始されます。

```
Bind DN: Full DN path, it must be the same DN that is entered in the Duo Authentication Proxy
for exempt_ou_1= below
Base DN: Specify DN path
Port: 389 or whatever your preference is for STARTTLS traffic.
Timeout: 60 seconds
Vendor: MS AD
```

> **注**：STARTTLSは標準のLDAPポートで動作するため、LDAP統合とは異なり、

STARTTLS統合ではDuo認証プロキシの**port=フィールド**ではなく**ssl_port=フィールドを使用します。**

Duo認証プロキシ

```
[ldap_server_auto]
ikey=
skey_protected= ==
api_host=api.XXXXXX.duosecurity.com
client=ad_client1
failmode=secure
port=389 or the port of your LDAP or STARTTLS traffic.
ssl_port=636 or the port of your LDAPS traffic.
allow_unlimited_binds=true
exempt_primary_bind=false
ssl_key_path=YOURPRIVATE.key
ssl_cert_path=YOURCERT.pem
exempt_primary_bind=false
exempt_ou_1=full DN path
```

Radius統合

UCS マネージャ

[UCS Manager] > [**Admin] > [User Management] > [Radius]に移動し、[Radius Providers]をクリックします。**

Key and Authorization Port: Must match the Radius/ Authentication Proxy configuration.
Timeout: 60 seconds
Retries: 3

Duo認証プロキシ

```
[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=5.6.7.8
radius_secret_1=radiussecret1
client=ad_client
port=18121
failmode=safe
```

Duo認証プロキシのインストールと設定のベストプラクティス

ファイアウォールで保護された内部ネットワークに認証プロキシを導入し、次のことを行います。

- TCP/443で認証プロキシから一般インターネットへの発信通信を許可します。さらに制限が必要な場合は、DuoのList of IP ranges to Allowed Listを参照してください。
- Duo認証プロキシは、CONNECTプロトコルをサポートする設定済みのWebプロキシを介してDuoのサービスに到達するように設定することもできます。

- 適切なIDP（通常はTCP/636、TCP/389、またはUDP/1812）に接続可能
- 適切なRADIUS、LDAP、またはLDAPSポートでプロキシとの通信を許可します。これらのルールにより、アプライアンス/アプリケーションはプロキシに対してユーザを認証できます。
- 環境内にSSLインスペクションアプライアンスが存在する場合は、認証プロキシIPのリストSSLインスペクションを無効または許可します。
- 各[radius_server_METHOD(X)]セクションと[ldap_server_auto(X)]セクションを設定し、一意のポートでリッスンします。
  Duo認証プロキシを使用して複数のアプリケーションに電源を供給する方法の詳細については、DuoサイトのDuoプロキシで複数のアプリケーションを使用してください。
- 各アプライアンスに固有のRADIUSシークレットとパスワードを使用します。
- プロキシ設定ファイルで保護/暗号化されたパスワードを使用します。
- 認証プロキシは、多目的サーバ上で他のサービスと共存できますが、専用サーバを使用することをお勧めします。
- 正確な日付と時刻を保証するために、認証プロキシが信頼できるNTPサーバを指していることを確認します。
- 認証プロキシをアップグレードする前に、必ずコンフィギュレーションファイルのバックアップコピーを作成してください。
- Windowsベースの認証プロキシサーバの場合は、電源またはネットワークの障害の場合にいくつかの回復オプションを含むように、Duo Security Authentication Proxy Serviceを設定します。

  ステップ1：サーバ上のサービス内で、[Duo Security Authentication Proxy]サービスを右クリックし、[Preferences]をクリックします。
  ステップ2:[Recovery] をクリックし、障害発生後にサービスを再起動するオプションを設定します。
- Linuxベースの認証プロキシサーバの場合は、initスクリプトを作成するかどうかを確認するプロンプトがインストール上に表示され、[yes]をクリックします。次に、認証プロキシを起動する際に、sudo service duoauthproxy startなどのコマンドを使用します。これは、initスクリプトのコマンドが使用しているシステムによって異なる場合があるためです。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、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

- テクニカル サポートとドキュメント – Cisco Systems