2024年10月に動作するようにDNS Umbrella証明書を更新

内容

はじめに

このドキュメントでは、SD-WANルータが新しい証明書の代わりに期限切れの証明書を使用する場合のDNS Umbrellaの問題を解決する方法について説明します。

背景説明

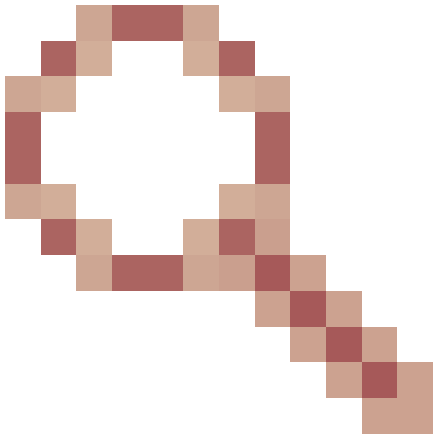
Cisco Catalyst SD-WANルータがCisco Umbrella DNSにAPIキー/シークレット認証方式を使用して登録するために使用するデジタル証明書は、2024年9月30日に期限切れになりました。証明書の有効期限が切れた Cisco SD-WAN ルータは、Cisco Umbrella DNS サービスへの登録に失敗します。この問題は、Umbrella DNS登録用のトークンベース認証には該当しません。

詳細については、2024年9月30日に期限切れになるCisco Umbrella DNS証明書をField Notice FN74166 で参照してください。

期限切れの包括ルートCA証明書を持つ該当SD-WANデバイスは、デバイス登録用のCisco Umbrella DNSとのセキュアな接続を確立できません。 デバイスがUmbrella DNSサービスに登録されていないため、エンドユーザのDNS要求は、DNSセキュリティポリシーを適用するために

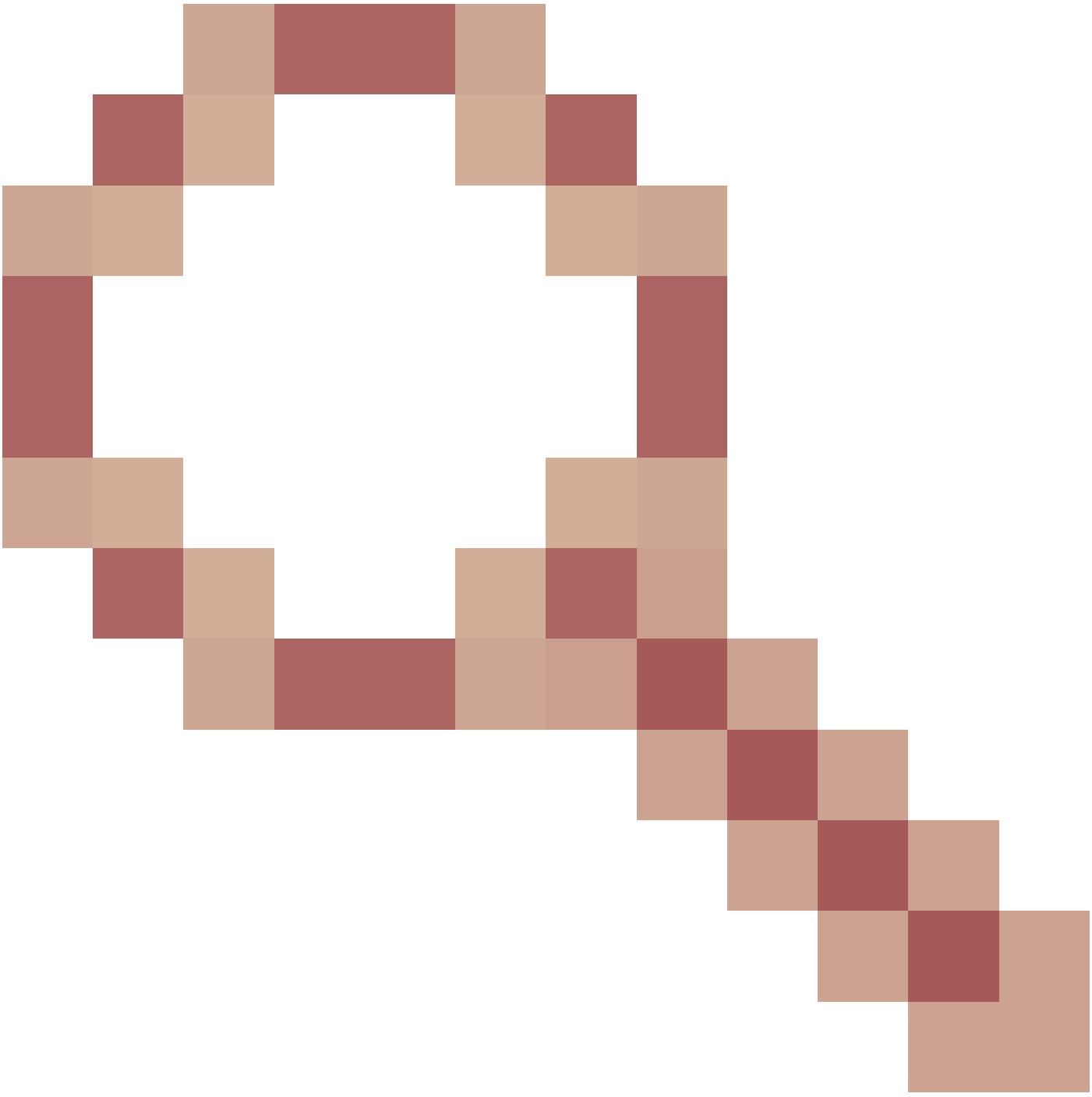
SD-WANエッジによってUmbrellaドメインサーバにリダイレクトされません。SD-WANエッジの背後にあるエンドユーザからのDNS要求はドロップされず、エンドユーザデバイスで設定されたDNSドメインサーバによって処理されます。

障害情報



証明書は、Cisco Bug ID CSCwi43360の一部として更新されました
: UmbrellaクラウドへのDNSセキュリティ登録の証明書が2024年9月に期限切れになります。（17.9.6、17.12.4、17.15.1aで修正）

証明書が更新されても、SSLハンドシェイクの確立に失敗します。これは、Cisco Bug ID CSCwm73365



: umbrella_root_ca.caと最新の証明書がデバイスに存在するにもかかわらず、SSLハンドシェイクが失敗します。（17.6.8aで修正）

修正済みリリース

CCOリリース

Release	17.6.8a

修復マトリックス

リリース	シスコが推奨する修復手順
17.3.x/17.4.x/17.5.x	セクション1の手順に従います。コントローラモードでCisco IOS XEソフトウェアリリース17.5.x以前を実行しているシスコデバイス
17.6.1 ~ 17.6.7、17.7.x、17.8.x	セクション2の手順に従います。コントローラモードでCisco IOS XEソフトウェアリリース17.6.x ~ 17.8.xを実行しているシスコデバイス
17.6.8a	Umbrella DNS証明書の期限切れの問題は、このリリースで修正されています。
17.9.1 ~ 17.9.4、17.10.x、17.11.x、17.12.1 ~ 17.12.2、17.13.x、17.14.x、17.15.1a	Umbrella DNS証明書スクリプトを使用して、エッジデバイスに証明書を自動的にコピーします。スクリプトの実行に使用する手順については、GITのreadmeファイルを参照してください。
17.9.5a	セクション3の手順に従います
17.9.6	セクション4の手順に従います
17.12.3a	セクション5の手順に従います
17.12.4	セクション6の手順に従います

1. コントローラモードでCisco IOS XEソフトウェアリリース17.5.x以前を実行しているシスコデバイス

修復オプションを使用して、新しいUmbrellaルートCA証明書をインストールします。

自動化

1. SD-WAN Manager 20.9.1以降では、vManageからエッジデバイスへの証明書の自動コピーにUmbrella DNS証明書スクリプトを使用します。
2. Umbrela DNS証明書スクリプト
3. スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。
4. RootCA証明書がデバイスにコピーされたら、ルータをリロードしてインストールプロセス

を完了します。

手動

1. New Umbrella Certificate Webサイトから新しい期限切れではない証明書をダウンロードし、SD-WANオーバーレイの該当ルータにアクセスできるデバイスに配置します。
2. Linux scp コマンドまたは同様のメカニズムを入力して、ダウンロードデバイスから影響を受ける各ルータに安全なファイルコピーを実行します。

   例：

   scp ./isrgrootx1.pem <ユーザー名>@<EdgeIP>:trustidrootx3_ca.ca

   <Username>をadminユーザ、<EdgeIP>を該当ルータのIPアドレスに置き換えます。

3. RootCA証明書がデバイスにコピーされたら、ルータをリロードしてインストールプロセスを完了します。

2. コントローラモードでCisco IOS XEソフトウェアリリース17.6.x ~ 17.8.xを実行しているシスコデバイス

修復オプションを使用して、新しいUmbrellaルートCA証明書をインストールします。

自動化

1. SD-WAN Manager 20.9.1以降では、vManageからエッジデバイスへの証明書の自動コピーにUmbrella DNS証明書スクリプトを使用します。
2. Umbrella DNS証明書スクリプト
3. スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。
4. RootCA証明書がデバイスにコピーされたら、ルータをリロードしてインストールプロセスを完了します。

手動

1. New Umbrella Certificate Webサイトから新しい期限切れではない証明書をダウンロードし、SD-WANオーバーレイの該当ルータにアクセスできるデバイスに配置します。
2. Linux scp コマンドまたは同様のメカニズムを入力して、ダウンロードデバイスから影響を受ける各ルータに安全なファイルコピーを実行します。

   例：

   scp ./isrgrootx1.pem admin@<エッジIP>:trustidrootx3_ca_092024.ca

   <EdgeIP> を影響を受けるルータの IP アドレスに置き換えます。

3. RootCA証明書がデバイスにコピーされたら、ルータをリロードしてインストールプロセスを完了します

3. コントローラモードでCisco IOS XEソフトウェアリリース17.9.5aを実行しているシスコデバイス

このセクションで説明されているように、修復オプションを使用して新しいUmbrellaルートCA証明書をインストールします。ほとんどのプラットフォームでは、修正で使用できるホットSMUがあります。新しいUmbrellaルートCA証明書をインストールするために記載されているスクリプトを実行するオプションもあります。

1. HOT SMUは次のプラットフォームに適用されます：「無中断/推奨SMU、SSLハンドシェイクが失敗し、デバイスに最新の証明書が存在するumbrella_root_ca.caが失敗する」

   4431サービス統合型ルータ
   4451-Xサービス統合型ルータ

   ASR 1001-Xルータ
   仮想ルータ
   4331サービス統合型ルータ
   4221サービス統合型ルータ
   4351サービス統合型ルータ
   Catalyst 8500Lエッジプラットフォーム
   ASR 1001-HXルータ
   4321サービス統合型ルータ

   Catalyst 8500エッジプラットフォーム

   4461サービス統合型ルータ

2. SMUの代わりに、スクリプトUmbrella DNS Cert Scriptを実行します。スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。

スクリプトのみのオプション：
ASR1002-Xルータ

Catalyst 8300エッジプラットフォーム

Cisco IOS XE SD-WANを実行するISR 1000シリーズ

4. コントローラモードでCisco IOS XEソフトウェアリリース17.9.6を実行しているシスコデバイス

1. HOT SMUは次のプラットフォームに適用されます。「無中断/推奨SMU、SSLハンドシェイクが失敗し、umbrella_root_ca.caと最新の証明書がデバイスに存在します」：

   4221サービス統合型ルータ
   4321サービス統合型ルータ
   4451-Xサービス統合型ルータ
   Catalyst 8500エッジプラットフォーム
   4431サービス統合型ルータ

仮想ルータ
4461サービス統合型ルータ
4331サービス統合型ルータ
4351サービス統合型ルータ
ASR 1001-HXルータ
ASR 1001-Xルータ
Catalyst 8500Lエッジプラットフォーム

3. SMUの代わりに、スクリプトUmbrella DNS Cert Scriptを実行します。スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。

スクリプトのみのオプション：

ASR1002-Xルータ

Catalyst 8300エッジプラットフォーム

Cisco IOS XE SD-WANを実行するISR 1000シリーズ

5. コントローラモードのCisco IOS XEソフトウェアリリース17.12.3aであるシスコデバイス

1. HOT SMUは次のプラットフォームに適用されます。「無中断/推奨SMU、SSLハンドシェイクが失敗し、umbrella_root_ca.caと最新の証明書がデバイスに存在します」：

4221サービス統合型ルータ
Catalyst 8300エッジプラットフォーム
4331サービス統合型ルータ
4461サービス統合型ルータ
1100サービス統合型ルータ
4351サービス統合型ルータ
4321サービス統合型ルータ
4431サービス統合型ルータ
仮想ルータ
4451-Xサービス統合型ルータ

Catalyst 8500Lエッジプラットフォーム
Catalyst 8500エッジプラットフォーム
ASR 1001-HXルータ

2. SMUの代わりに、スクリプトUmbrella DNS Cert Scriptを実行します。

スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。

6. コントローラモードでCisco IOS XEソフトウェアリリース17.12.4を実行しているシスコデバイス

1. HOT SMUは次のプラットフォームに適用されます。「無中断/推奨SMU、SSLハンドシェイクが失敗し、umbrella_root_ca.caと最新の証明書がデバイスに存在します」:

Catalyst 8500エッジプラットフォーム
ASR 1001-HXルータ
4331サービス統合型ルータ
4321サービス統合型ルータ
4221サービス統合型ルータ
仮想ルータ
4351サービス統合型ルータ
4451-Xサービス統合型ルータ
4461サービス統合型ルータ
Catalyst 8300エッジプラットフォーム
ASR 1002-HXルータ
4431サービス統合型ルータ

1100サービス統合型ルータ

Catalyst 8500Lエッジプラットフォーム

2. SMUの代替はスクリプトUmbrella DNS Cert Scriptを実行することです。スクリプトの詳細な使用手順については、GITのreadmeファイルを参照してください。

⚠ 注意：デバイスのリブートや新しい登録がない限り、デバイスからの包括DNS登録は機能し続けます。

⚠ 注意:umbrella設定が削除されて再適用されると、umbrella DNSの再登録がトリガーされます。このプロセスに従わない限り、Umbrella DNSは正常に機能します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。