CHAPTER 21

クライアントレス SSL VPN のトラブルシューティング

2014 年 4 月 14 日

hosts ファイル エラーを回避するための Application Access の終了

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終えたら、Application Access ウィンドウを必ず閉じるようにします。ウィンドウを閉じるには、[Close] アイコンをクリックします。

Application Access 使用時の hosts ファイル エラーからの回復

Application Access ウィンドウを正しく閉じないと、次のエラーが発生する可能性があります。

- 次に Application Access を起動しようとしたときに、Application Access がオフに切り替わっている可能性があり、「`Backup HOSTS File Found`」エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がオフに切り替わっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次に例を示します。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

- hosts ファイルの概要
- 不正な Application Access の終了
- クライアントレス SSL VPN による hosts ファイルの自動再設定
- 手動による hosts ファイルの再設定

hosts ファイルの概要

ローカル システム上の hosts ファイルは、IP アドレスをホスト名にマッピングしています。Application Access を起動すると、クライアントレス SSL VPN は hosts ファイルを修正し、クライアントレス SSL VPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	• クライアントレス SSL VPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。 • 次に、クライアントレス SSL VPN は hosts ファイルを編集し、クライアントレス SSL VPN 固有の情報を挿入します。
Application Access の終了時	• クライアントレス SSL VPN はバックアップ ファイルを `hosts` ファイルにコピーして、hosts ファイルを元の状態に戻します。 • クライアントレス SSL VPN は、hosts.webvpn を削除します。
Application Access の終了後	hosts ファイルは元の状態です。

（注）　Microsoft 社のアンチスパイウェア ソフトウェアは、ポート転送 Java アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、www.microsoft.com を参照してください。

不正な Application Access の終了

Application Access が正しく終了しなかった場合は、`hosts` ファイルは、クライアントレス SSL VPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、クライアントレス SSL VPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、「`Backup HOSTS File Found`」というエラー メッセージが表示され、Application Access が一時的にオフに切り替わります。

Application Access を正しくシャットダウンしないと、リモート アクセス クライアント/サーバ アプリケーションが不安定な状態のままになります。クライアントレス SSL VPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

クライアントレス SSL VPN による hosts ファイルの自動再設定

リモート アクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

手順の詳細

ステップ 1　クライアントレス SSL VPN を起動してログインします。ホームページが開きます。

ステップ 2　**[Applications Access]** リンクをクリックします。`Backup HOSTS File Found` メッセージが表示されます。

ステップ 3　次のいずれかのオプションを選択します。

- **[Restore from backup]**：クライアントレス SSL VPN は強制的に正しくシャットダウンされます。クライアントレス SSL VPN は hosts.webvpn backup ファイルを `hosts` ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- **[Do nothing]**：Application Access は起動しません。リモート アクセスのホームページが再び表示されます。
- **[Delete backup]**：クライアントレス SSL VPN は hosts.webvpn ファイルを削除し、hosts ファイルをクライアントレス SSL VPN 用にカスタマイズされた状態にしておきます。元の `hosts` ファイル設定は失われます。Application Access は、クライアントレス SSL VPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します （「手動による hosts ファイルの再設定」を参照）。

手動による hosts ファイルの再設定

現在の場所からリモート アクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

手順の詳細

ステップ 1　hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\system32\drivers\etc\hosts です。

ステップ 2　`# added by WebVpnPortForward` という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルはクライアントレス SSL VPN 用にカスタマイズされています。hosts ファイルがクライアントレス SSL VPN 用にカスタマイズされている場合、次の例のようになっています。

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward
```

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

ステップ 3　`# added by WebVpnPortForward` という文字列が含まれている行を削除します。

ステップ 4　ファイルを保存して、閉じます。

ステップ 5　クライアントレス SSL VPN を起動してログインします。

ホームページが表示されます。

ステップ 6　**[Application Access]** リンクをクリックします。

[Application Access] ウィンドウが表示されます。これで Application Access がイネーブルになります。

データのキャプチャ

CLI **capture** コマンドを使用すると、クライアントレス SSL VPN セッションでは正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の項では、クライアントレス SSL VPN セッション データのキャプチャおよび表示方法について説明します。

- 「キャプチャ ファイルの作成」（P.21-5）
- 「キャプチャ データを表示するためのブラウザの使用」（P.21-6）

前提条件

- クライアントレス SSL VPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順の詳細

	コマンド	目的
ステップ 1	**capture *capture_name* type webvpn user *webvpn_username*** 例： hostname# **capture hr type webvpn user user2** WebVPN capture started. capture name hr user name user2 hostname# **no capture hr**	クライアントレス SSL VPN のキャプチャ ユーティリティを開始します。 • *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。 • *webvpn_user* は、キャプチャの対象となるユーザ名です。 hr という名前のキャプチャを作成します。これは、user2 へのトラフィックをファイルにキャプチャします。
ステップ 2	（オプション） **no capture capture_name**	ユーザがログインし、クライアントレス SSL VPN セッションを開始した後に、キャプチャ ユーティリティでのパケットの取得を停止します。キャプチャ ユーティリティは *capture_name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。
ステップ 3	.zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。	
ステップ 4	パスワード *koleso* を使用してファイルの内容を解凍します。	

キャプチャ データを表示するためのブラウザの使用

手順の詳細

	コマンド	目的
ステップ 1	**capture *capture_name* type webvpn user *webvpn_username***	クライアントレス SSL VPN のキャプチャ ユーティリティを開始します。 • *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。 • *webvpn_user* は、キャプチャの対象となるユーザ名です。
ステップ 2	（オプション） **no capture capture_name**	ユーザがログインし、クライアントレス SSL VPN セッションを開始した後に、キャプチャ ユーティリティでのパケットの取得を停止します。
ステップ 3	ブラウザを開き、次のように入力します。 **https://***asdm_enabled_interface_of_the_security_appliance*:*port*/**admin/capture/***capture_name*/pcap **例：** **https://192.0.2.1:60000/admin/capture/hr/pcap**	hr という名前のキャプチャを sniffer 形式で表示します。
ステップ 4	ステップ 2 を繰り返します。	