Clean Access Server の FAQ

目次

[概要](#)
[インストール](#)
[設定](#)
[二重および速度設定](#)
[サポートされている機能](#)
[ログ メッセージ](#)
[エラー メッセージ](#)
[その他](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Clean Access Server（旧名称 Perfigo SecureSmart Server）に関する FAQ について記述します。

製品名は変更されました。 この表は古い名前と新しい名前の両方をリストしています。

旧名称	新名称
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPI	Clean Access API

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

インストール

Q. Dell 1750 またはその他の LSI SCSI ドライバはどうすればインストールできますか。

A. 次の手順を実行します。

1. rawrite ファイルを C:\ および LSI ドライバに保存します。 ファイルを同じディレクトリで更新します。
2. コマンド プロンプトを開き、C:\rawrite と入力します。

3. ソース ファイルのフルネームと、2 つのフロッピー ディスクの宛先を入力します。
4. Clean Access Manager Machines (旧名称 CleanMachines) インストール CD を Cisco Clean Access Server または Cisco Clean Access Manager に挿入します。
5. boot> プロンプトで、「custom」と入力します。
6. 指示にしたがって アップデート ディスク、続いてドライバ ディスクを入力します。

設定

Q. Broadcom ドライバはどのように設定すればよいですか。

A. 次の手順を実行します。

1. ボックスにコンソール接続します。 `cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700`

   `insmod ./bcm5700.o`
2. ステップ 1 でエラーが出なければ、vi /etc/modules.conf コマンドを入力して次の 2 行を追加します。 `alias eth0 bcm5700`

   `alias eth1 bcm5700`

Q. Cisco Clean Access Server を NAT ゲートウェイの背後に設定するにはどうすればよいですか。

A. NAT ゲートウェイの背後に配備される各 Cisco Clean Access Server に対し、次の手順を行います。

1. SecureSmart サーバへの SSH またはシリアル コンソールを使用して、ルートとしてログインします。
2. /perfigo/access/bin/starttomcat ファイルを編集します。
3. アペンド**- CATALINA_OPTS** 変数行**への Djava.rmi.server .hostname - = < CAS_hostname - >**。
4. service perfigo restart を再始動します。
5. SmartManager への SSH またはシリアル コンソールを使用して、ルートとしてログインします。
6. /etc/hosts ファイルを編集して、次の行を追加します。 `<public_IP_address> <securesmart_hostname> <securesmart_hostname>`

二重および速度設定

Q. Cisco Clean Access Server ネットワーク インターフェイス カードのデュプレックスおよび速度はどのように設定すればよいですか。

A. /etc/modules.conf ファイルで適切なネットワーク インターフェイス カードを設定するには、次のことをガイドとして使用してください。

注: vi エディタで /etc/modules.conf ファイルを使用する場合は、最後にオプション パラメータを付けます。

- Broadcom 5700 カードを 100 Mbps 全二重に設定します。
  options bcm5700 line_speed=100,100 auto_speed=0,0 duplex=1,1
- Broadcom 5700 カードを 1000 Mbps 全二重に設定します。
  options bcm5700 line_speed=1000,1000 auto_speed=0,0 duplex=1,1
- e1000 カードを 100 Mbps 全二重に設定します。
  options e1000 Speed=100,100 Duplex=2,2
- e1000 カードを 1000 Mbps 全二重に設定します。
  options e1000 Speed=1000,1000 Duplex=2,2
- eepro100 カードを 100 Mbps 全二重に設定します。
  options eepro100 option="0x30,0x30"

Q. Cisco Clean Access インターフェイス "bnx2" の二重/速度を設定する方法

A. on Cisco Clean Access サーバ デバイスは（CAM で）、そこにプロパティおよびスピード/デュプレックス設定を記述する各ネットワーク インターフェイスのためのファイルです。

ステップはそれを手動で行う方法をここにあります:

1. **/etc/sysconfig/network-scripts** にディレクトリを変更して下さい。 各インターフェイスに関しては ifcfg-ethX、X が 2 0、1 である、場合もあるところで、先祖などと指名されるこのディレクトリにファイルがあります
2. どのインターフェイスの設定をハードコードしたいと思うこの行をのための追加して下さい：`ETHTOOL_OPTS="speed 100 duplex full autoneg off"`
3. ファイルを保存した後、「サービス ネットワーク 再始動」を行って下さい。
4. スイッチ設定が手動で行われることを確かめて下さい。 X がハードコードされる双方向設定を確認する 0 または 1 のどれである場合もあるシェルの eth **ツール ethX** コマンドの発行によって設定をチェックして下さい。 **注:** これはサービスを瞬間的に割り込みます。 ダウンタイムをスケジュールしなければならない場合考慮事項でこれを保存して下さい。

Q. Cisco Clean Access Server ネットワーク インターフェイス カード（NIC）のデュプレックスと速度はどうすれば確認できますか。

A. コマンド ラインから mii-tool ユーティリティを実行します。 このユーティリティはオンボード NIC では機能しますが、ファイバ NIC はサポートしません。

ファイバ NIC に関しては、/var/log/messages の**グレップ 'eth0** コマンドを使用して下さい。

また、/var/log/messages で tail -f コマンドを発行することもできます。 こうすると、NIC がアクティブまたは非アクティブになるたびにメッセージが表示されます。

サポートされている機能

Q. Cisco Clean Access Server 1 台あたりにサポートされる VPN 接続はいくつありますか。

A. IPsec に関しては、制限はありません。

PPTP および L2TP は、現在 1 サーバにつき 32 トンネルに設定されています。

Q. Cisco Clean Access Server の IP アドレスはどうすれば変更できますか。 Cisco Clean Access Server を一度削除してから、追加し直す必要がありますか。

A. Cisco Clean Access Server の IP アドレスは、Cisco Clean Access Manager の UI から変更することをお勧めします。 Cisco Clean Access サーバの IP アドレスがマネージャ UI から変更されるとき、Cisco Clean Access サーバをリブートして下さい。 リブート時に、Cisco Clean Access Server は自動的に Cisco Clean Access Manager に接続しようとします。 Cisco Clean Access Manager はデータベース内の Cisco Clean Access Server の IP アドレスを変更しますが、SSKEY は同じです。

注: Cisco Clean Access Server を削除してから追加し直すと、Cisco Clean Access Server のすべての構成設定が失われます。

Q. SSH アクセスを Cisco Clean Access Server に限定するにはどうすればよいですか。

A. /etc/ssh/sshd_config ファイルを変更するため、次の例のような行を追加します。

```
ListenAddress IP_address_of_where_you_want_ssh_to_allow_connections
```
次に、例を示します。

```
ListenAddress 192.168.151.60
```
SSHD プロセスを再起動するため、service sshd restart コマンドを発行します。

Q. Bandwidth Burst 設定はどうすれば機能しますか。

A. CleanMachines で [Windows All] のチェックをはずし、各 OS で個別に [Require Use of SmartEnforcer] を選択または選択をはずします。

Q. Clean Access サーバごとのサブネットの数推奨される最高値が 1000 であるページで 68 最近 Clean Access サーバインストールおよび管理 ガイド リリース 3.3BETA を読取ります。 以上 1000 作成する必要があります。 制限とは何か。

A. 1000 という制限は単なる警告です。 マシンに十分な（1G を超える）メモリがあれば、2500 までのサブネットを設定することができます。

Q. Clean Access Server によって管理される特定の VLAN 内のアクセス ポイントのバッチを管理するにはどうすればよいですか。 アクセス ポイントを Access Point Device Management に追加しています。

A. アクセス ポイント デバイス管理 セクションに対して**フィルタ >Devices** エリアへのアクセス ポイントの MAC アドレスを追加して下さい。

Q. 各 VLAN にセカンダリ（場合によっては複数のセカンダリ）サブネットがあります。 150 のサブネットはクライアント用であり、172 のサブネットはビル内のネットワーク機器管理用です。 Clean Access Server は 1 つの VLAN で複数のサブネットを取り扱えますか。

A. この問題の例を次に示します。

```
!
  interface Vlan 106
   ip address 150.135.47.1 255.255.255.0
   ip address 172.16.10.1 255.255.255.192 secondary
  !
```

Clean Access Server が仮想ゲートウェイ モードにある場合：

- この場合、Clean Access Server はサブネットの数やそれらに関連付けられている VLAN タグを確認しません。 VLAN の情報は、例外なくすべて通過します。

Clean Access Server がゲートウェイ（実際の IP または NAT）モードにある場合：

- この場合、Clean Access Server は DHCP リレーまたは DHCP サーバのどちらとしても機能します。 どちらの場合も、割り当てられる IP アドレスの範囲は VLAN タグやゲートウェイ アドレスによって異なり、ゲートウェイ アドレスも VLAN タグによって異なります。したがって、Clean Access Server は同じ VLAN にある 2 つのサブネットを（DHCP の観点から）区別できません。 1 つの制約として、同じ VLAN にある 2 つのサブネットのうち 1 つは、アドレスの割り当てに DHCP を使用すべきではありません。 代わりに、静的に IP アドレスを割り当てる必要があります。 ネットワーク内の 172 サブネットはネットワーク機器で構成されるため、これに当てはまると考えられます。

Q. Clean Access Manager（CAM）に Clean Access サーバを追加することができない理由

A. CAM に Clean Access サーバを追加することができない場合これはライセンスの問題です。 サーバライセンスがプライマリ CAM イーサネットに基づいて 0 MAC アドレス生成されることを確かめて下さい。 サーバライセンスの MAC アドレスは CAM の（プライマリ） MAC アドレスを一致する必要があります。

1. GUI > Administration > Clean Access Manager は CAM に > 行きま認可します。
2. 「取除きますすべてのライセンス」を行って下さい。
3. サーバライセンス ファイルを再度再インストールして下さい。

Q. Clean Access サーバの認証を更新するために新しい CSR を生成する必要がありますか。

A. いいえ。 Clean Access サーバの認証の更新に関しては、新しい CSR を生成しないで下さい。 ただし新しい CSR を生成すれば、そして Clean Access サーバのプライベートキーをアップロードしなければなりません。 プライベートキーをアップロードした後、Clean Access サーバをリブートして下さい。 これは再生過程を完了します。

Q. それは CCA を通してパススルー マルチキャストトラフィックに可能性のあるですか。

A. いいえインバンド実質ゲートウェイの下で、マルチキャスト サポートされません。 ただし、それはアウトオブバンドかバーチャル ゲートウェイのためにはたらきます。

Q. NAC は Windows 2008 64 ビット サーバをサポートしますか。

A. いいえ、だけどそれは 32ビット Windows 2008 サーバをサポートします。

Q. NAC は新規 ユーザ ロールにそれと関連付けられるユーザの役割およびポリシー/プロパティを重複させるために機能が含まれていますか。

A. いいえ。 これは GUI にそのようなプロビジョニングするがないのですることができません。

ログ メッセージ

Q. /var/log/messages または /var/log/ha-log messages にフェールオーバーのハートビート メッセージが複数あります。 原因と修正方法を教えてください。

A. 表示されるハートビート メッセージは次のようなものです。

```
heartbeat: 2004/09/15_11:23:27 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_14:19:17 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_18:59:53 info: Heartbeat restart on node ss1

heartbeat: 2004/09/15_19:36:18 info: Heartbeat restart on node ss1
```

これらのメッセージは、ピア サーバがリブート後アップになっているときに表示されます。 次の場合、プライマリ サーバのログにも表示されることがあります。

- **サービス perfigo 停止を**発行し、次にピアまたはスタンバイ マシンを **perfigo 始めを保守します**。または
- ピアまたはスタンバイ マシンをリブートする。

注: service perfigo restart コマンドを発行すると、このログはトリガーされません。

Q. Clean Access サーバを 2004-08-30 11:30:28 192.168.151.60 システム統計見ます: 負荷 率 0 （再度ブートする以来の最大値: 3） Mem: 261160960 237854720 23306240 212992 47259648 99737600 CPU 188552 イベントログの 153 の 91405324 の 194183 のメッセージ。 これはどういう意味ですか。

A. デフォルトとして、Clean Access Manager が管理する各 Clean Access Server のシステム統計は 1 時間ごとに作成されます。 レポートされる情報には、各サーバの負荷係数、リブート以降の最大負荷、メモリ、および CPU 使用状況が含まれます。

- **負荷 率**—負荷 率はパケットの数を説明する数ですサーバによって処理されるために待っている（たとえば、現在のロード Clean Access サーバによって処理される）。 負荷係数が高ければ、処理待ちのパケットがキューになっています。 負荷 率があらゆる一貫したある一定の時間の間 500 より大きければ（たとえば、5 分）、Clean Access サーバに入るパケット/トラフィックの安定した高負荷があること表しています。 数 500 にかより高いの達する場合かかわっている必要があります。
- **最大ので reboot** —どんな時点でもキューのパケットの最大数（たとえば、Clean Access サーバによって処理される最大負荷）。
- **Mem** —メモリ使用量統計情報。 6 つの数字があります（単位はバイト）。 これらの数字は合計メモリ、使用メモリ、空きメモリ、共有メモリ、バッファ メモリ、およびキャッシュ メモリを表します。
- **cpu** — ハードウェアのプロセッサ ロード。 CPU の使用状況を示す数字は 4 つあります（ほとんどのシステムで単位はjiffies、1 jiffy は時間単位で 10 ms）。 これらの数字は、ユーザ プ

ロセス、ナイス プロセス、システム プロセス、およびアイドル プロセスのシステム使用時間を示します。

例では、system % = 91405324*100/(188552+153+91405324+194183) = 99.58% です。 ほかの使用時間も同様に計算することができます。 ただし、Clean Access Server では通常システム時間が 90% を超えます。 これは健全なシステムを示します。

エラー メッセージ

Q. Clean Access Server 受け取る理由

A. 次のことを確認してください。

- Cisco Clean Access Server と Cisco Clean Access Manager の共有秘密が同じである。
- 証明書が正しい。
- Cisco Clean Access Server と Cisco Clean Access Manager の接続性、および RMI ポートをブロックするファイアウォール規則がない。

Q. なぜか CAS 受け取って下さい: Clean Access Clean Access Manager をトラブルシューティングするにはどうすればよいですか。

A. Clean Access Manager 認証が切れたり、信頼される場合がなかったりまたは達することができなければこのエラーを受け取るかもしれません。 エラーは CAS または CAM コミュニケーション問題が基本的に原因です。

この問題を解決するには、次の項目を確認してください：

- CAS および CAM が両方同じバージョンであることを確かめて下さい。
- 認証のために名前を使用する場合、名前が nslookup を使用して解決されますことを確かめて下さい。
- フェールオーバー 認証のためにサービス IP を利用して下さい。
- 認証をことを生成する前にそれらが同期される時間であることを確かめて下さい。
- make sure シークレット一致を共有しました。
- ファイアウォールは ACL ブロックあらゆる SSL 通信べきではないです。
- CAS に標準外ルートとして CAM 認証を追加して下さい。
- DNS 名前解決があるように確認して下さい。
- CAM と CAS 間の到達可能性のためのルーティングが正しいことを確かめて下さい。

Q. X509 …CAエラーメッセージ受け取る理由

A. 正しいルート証明を使用して下さい。 Microsoft Certificate Authority（CA）が使用される場合、Base64 の認証をよりもむしろディフォルトします符号化される保存して下さい。

Q. イベント ログに、Authentication 2004-11-01 15:53:40 Server 通信エラー、[00:0E:35:5F:F9:91 ## 172.19.168.42] bart および Authentication 2004-11-01 15:53:13 Server 通信エラー、[00:0E:35:5F:F9:91 ## 172.19.168.42] bart エラーが表示されます。 これはどのように解決すればよいですか。

A. 仮想ゲートウェイ モードでフェールオーバー Clean Access Server を実行している場合は、vi /etc/hosts ファイルを編集し、SS-1（Clean Access Server）のアドレスを Service IP（仮想アドレス）に変更します。 アクティブとスタンバイ、両方の Clean Access Server を変更する必要があります。

- 127.0.0.1 localhost localhost
- 192.168.1.2 SS-1 SS-1

Q. TCP/IPスタック シグニチャを得ます: 未知未知数 [65535:64:1:64:M1460,N,W2,N,N,T0,S,E:P] {}メッセージ。 どのようにこれを固定し、どのように iPhone のためのクライアントのインストールをディセーブルにすることができますか。

A. iPhone のためにエージェントを必要としないためにはたらく必要がある手順はここにあります:

1. **Clean Access > 一般的 な セットアップ > エージェント ログイン**の下でロールを選択して下さい。
2. iPhone または iPod touch のためのエージェント必要条件を設定するために **MAC_ALL を**選択して下さい。 チェックを外されたら、従って「すべて」からの共用設定を使用しなかったらバージョン別設定が規定 されない場合**使用** MAC OS ファミリーことを用の**すべての設定**確かめて下さい。 また必要とエージェント ダウンロード オプションがチェックを外される、従って Clean Access サーバがクライアント（iPhone/iPod touch）にエージェントをダウンロードするように頼まないことを、確かめて下さい。
3. MAC OS のためのエージェント必要条件を設定するために **MAC_OSX を**選択して下さい。 **すべての設定**オプションをチェックするか、またはこの仕様 OS を設定するためにチェックを外すことができます。 必要とエージェント ダウンロード オプションは規則的な MAC OS ユーザに MAC エージェントをダウンロードしてほしい場合チェックする必要があります。

Q. このエラーメッセージを受け取るかもしれません: `Error: CA` 。 これを解決するにはどうすればいいですか。

A. この問題を解決するには、次の手順を実行します。

1. CSR を生成して下さい。
2. プライベートキーを保存して下さい。
3. 保存されたプライベートキーが付いている新しい認証をアップロードして下さい。

Q. 次のエラー メッセージが表示されます： `NAC : _SYSTEM_ - 172.16.98.9 : XXX@YYY.com 2011 15-Jan-2010 11:41:44`。 このエラーを解決するにはどうすればよいのですか。

A. この問題は CSCsq86376（登録ユーザのみ）を煩わせるために releated、WLC からの RADIUSパケットで IP アドレスを使用していない場合現れます。

Q. CD の CAS をアップグレードしている間このエラー meaage を受け取りました: `I/O` 。 このエラーを解決するにはどうすればよいのですか。

A. この問題は通常 CD が破損していたりまたは高速で焼き付けられると発生します。 大きい ISO

を使うと CD は 10X か 8X 速度より多くで焼き付けられてはなりません。

Q. CAM に CAS を接続するときこのエラーメッセージを受け取るかもしれません: `Error: RMISocketFactory: RMI` 。 この問題はどうすれば解決しますか。

A. このエラーメッセージは CAM および CAS の組合わせを誤まられたバージョンが原因か組合わせを誤まられた認証か使用される共有秘密が原因で表示されるかもしれません。 認証問題を解決する方法に関する詳細については NAC （ CCA ）を参照して下さい: 4.1.6 にアップグレードの後で CAM/CAS の Certificate エラーを修正する方法。

Q. 次のエラー メッセージが表示されます： このエラーを解決するにはどうすればよいのですか。

A. CAS で使用される認証が自己**発行される**現れ、クライアントの証明書ストアで保存されませんのでこのメッセージが。 このエラーはクライアントマシンに既に知られている外部ベンダーから認証をロードすることによって解決することができます (Verisign、Entrust、等のような) 。 これはこれらのベンダーの 1 人からの認証を購入し、CAS でインストールすることを必要とします、またはあなた自身の認証局を使用できます (しかし、手動で各クライアントでこれから CA 認証をインストールする必要があります) 。

注: CAS の認証を再インストールすることはそれを取除き、CAM へ再追加することを必要とします。 これはネットワークに分裂的である場合もあります。 これは可能性のある 停止 ウィンドウがあるときだけ強く推奨されています。

その他

Q. Clean Access Server の DHCP サービスが再起動しなかったり、時々停止したりします。 どうすればよいですか。

A. DHCP 設定は Clean Access サーバで*コンパイルされます*。 コンパイルされた設定が破損することがあり、特に Clean Access Server ソフトウェアへアップグレードした後に起こります。 解決策としては、Clean Access Server でこの設定を強制的に再コンパイルします。 これをするために、変更を行ない、『Update』 をクリック して下さい。

症状：

DHCP サーバが Clean Access Server 上で起動しなかったり、時々障害が発生したりします。

手順：

1. サーバの DHCP デーモンが開始しない場合、マネージャに行き、その特定のサーバを開き、『Manage』 をクリック して下さい。
2. Network > DHCP > Subnet List の順に選択 し、サブネット リストの 1 つのために『Edit』をクリック して下さい。
3. サブネットへの変更を (たとえば、1 分までに Lease Time を高めて下さい) 行ない、『Update』 をクリック して下さい。
4. ステータス ページに戻り、DHCP サービスが起動しているか確認します。 この時点で DHCP 設定は再度コンパイルする必要があります。

注: DHCP サーバが起動しないもう 1 つのケースとして、サブネット設定がオーバーラップして

いる場合もあります。 これについても調べます。

Q. 一定の非アクティブ時間の後にデバイスをシステムからログオフさせるように、ハートビート タイマーを設定しました。 イベント ログには、デバイスへ ping できないことが示されているのに、デバイスはトラフィックの受け渡しを続けます。 これはどのように解決すればよいですか。

A. これはエラーの例です。

```
Authentication  2004-08-26 12:13:48
Unable to ping 149.151.206.251, going to logout user user1
```

デバイスに Cisco Clean Access Server からの ARP パケットをブロックするビルトインのファイアウォールがないか確認します。 Cisco Clean Access Server は ARP ping を行います。 これは ARP メッセージなのでブロックすべきでありません。

Q. 一定の非アクティブ時間の後にデバイスがシステムからログオフさせるように、ハートビート タイマーを設定しました。 イベント ログにはデバイスへ ping できないことが示されているのに、デバイスはトラフィックの受け渡しを続けます。 これはどのように解決すればよいですか。

A. シリアル ポートがフェールオーバー接続用に設定されていることを確認します。

Cisco Clean Access Server ソフトウェアが稼動するコンピュータに 2 つのシリアル ポートがある場合は、追加のポートをシリアル ケーブル接続に使用できます。 デフォルトでは、サーバで最初に検出されるシリアル コネクタがコンソール入出力用（インストールや他の管理上のアクセスを行うためのもの）として設定されます。 コンピュータに 1 つしかシリアルポート（ttyS0）がなく、それを管理上のアクセスに使用しない場合は、そのポートをフェールオーバー接続用に再設定できます。

ttyS0 をハートビート接続として再設定するには、次の手順を行います。

1. SSH クライアントから、ルート ユーザとして Cisco Clean Access Server にアクセスします。
2. /etc/lilo.conf を編集し、最後の行を削除またはコメント アウトします。 `append="console=ttyS0....."` この行は、コンソールの出力をシリアル ポートにリダイレクトさせます。 **注:** 行をコメント アウトするには、その行の先頭に # を付けます。 この文字で始まる行は無視されます。
3. /etc/inittab を編集し、最後の行を削除またはコメント アウトします。 `co:2345:respawn ...vt100`この行は、ログイン ターミナルをシリアル ポートで起動させます。
4. コマンド プロンプトで「lilo」と入力し、[Enter] キーを押します。 これにより、Linux ブート ローダである Lilo が起動します。
5. コンピュータを再起動するため、reboot コマンドを入力します。
6. フェールオーバー ピアの、Cisco Clean Access Server でこの手順を繰り返します。

Q. Cisco Clean Access サーバを時間を計るために Cisco Clean Access Manager（以前の SmartManager）がおよびどの位の時間を要するか **SecureSmart 2004-08-26 12:26:42** のために **192.168.1.1** ！表示するべきメッセージか。

A. Cisco Clean Access Manager が各 Cisco Clean Access Server をタイムアウトにし、「Not

Connected」ステータスを表示するまでには 3 分間かかります。

Q. Cisco Clean Access Server のネットワーク インターフェイス カード（NIC）を変更すると、どんな影響がありますか。

A. 非サイト ライセンスの場合、MAC アドレスの変更をシスコのテクニカルサポートへ連絡する必要はありません。 Clean Access Server の数が変更される場合にだけ、シスコのテクニカルサポートへの連絡が必要です。 サイト ライセンスをお持ちの場合は、シスコのテクニカルサポートへの連絡は必要ありません。

Q. Clean Access DHCP サーバから IP アドレスを取得できるのに、その後、外部アドレスへのブラウザを開こうとすると「Page Not Found」メッセージが表示されます。 Web のログイン ページへどうしてもリダイレクトされません。 なぜでしょうか。

A. 次の問題のどれかが起こっている可能性があります。

- Cisco Clean Access Server の DNS が、DNS サーバに設定されていません。Web ログイン ページの DNS名にリダイレクトされます。 DNS エントリで、securesmart.company.com を 192.168.0.1 に関連付けていないのかもしれません。
- 証明書が DNS 名を使用します。証明書は securesmart.company.com を使用しますが、DNS サーバがその名前に関連付けられていません。 証明書の検証は失敗します。
- 証明書が正しく作成されていないか、有効でありません。 /perfigo/access/apache/logs/error_log を確認します。 次のエラーがある場合は、SSL 証明書を作成し直します。`[root@securesmart logs]# cat error_log`

  `[Thu Sep 16 18:00:04 2004] [error] Unable to configure RSA server private key`

  `[Thu Sep 16 18:00:04 2004] [error] SSL Library Error: 185073780 error:0B080074:x509 certificate routines: X509_check_private_key:key values mismatch`**注:** どこに Clean Access Manager のログファイルがある参照して下さいか。 すべてのログファイルのため。
- httpd が起動していません。 http が **netstat** と **- Al** 開始するかどうか確認して下さい **| グレップ http** コマンド。 次のリストが表示されます。 表示されない場合、service perfigo restart コマンドを発行します。`tcp 0 0 *:http *:* LISTEN`

  `tcp 0 0 *:https *:* LISTEN`

Q. 障害のある Cisco Clean Access Server を交換した後、何か更新が必要ですか。

A. 場合によっては、ss_key が異なっていることがあります。 次の手順を実行します。

1. Cisco Clean Access Manager へ SSH して、ss_key を取得します。
2. psql -h 127.0.0.1 -U postgres controlsmartdb コマンドを発行します。
3. securesmart_info から * を選択します。 `ss_key | ss_group | ss_type | ss_ip | ss_loc`

   `00_40_33_60_43_D2_04_54_48_55_66_D5 | | standard_gateway | 10.0.0.1 |`
4. Cisco Clean Access Server へ SSH して、ss_key を取得し、更新します。
5. [root@securesmart etc]# cat /etc/.GUSSK コマンドを発行します。 `[root@securesmart etc]#`

```
cat /etc/.GUSSK

00_30_48_80_43_D6_00_30_48_80_43_D5
```

6. /etc/.GUSSK を編集し、Clean Access Manager の ss_key を使用してこれを更新します。
7. リブートを実行します。

Q. SSH 接続は CAS の perfigo サービスをサービス perfigo shutコマンドを使用してシャットダウンしている間失われます。 誰かがボックスに再接続、物理的になければそれを再起動できます。 問題を解決するには、どうすればよいですか

A. この問題は NAC バージョン 4.1 および それ 以降で**サービス perfigo メンテナンス** コマンドを使用することによって解決することができます。

Q. ある新しい CAS/CAM CD の NAC アプライアンスを起動することができません。 どうすればよいのですか。

A. これを解決するために次を確認して下さい:

- CAS/CAM のためにダウンロードされる ISO イメージのためのチェックサムを検証したようにして下さい。
- 最も遅い可能性のある焼き付けられた速度で ISO イメージを焼き付けて下さい。

関連情報

- Cisco Clean Access Agent FAQ
- Clean Access Manager FAQ
- Cisco Clean Access Manager FAQ 2
- テクニカルサポート - Cisco Systems