目次

[概要](#)
[使用するコンポーネント](#)
[背景説明](#)
[通信を理解して下さい](#)
[ESA から SMA に配信を解決して下さい](#)
[SMA から ESA に配信を解決して下さい](#)
[TLS/Certificates](#)
[関連情報](#)
[Cisco サポート コミュニティ - 特集対話](#)

概要

中央集中型 policiy、ウイルスおよび発生 quarnatine が有効に なるときこの資料に配信および接続に関する問題を解決する方法を記述されています。

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。

- AsyncOS 8.1 またはそれ以降の E メール セキュリティ アプライアンス（ESA）
- AsyncOS 8.0 またはそれ以降のセキュリティ マネジメント アプライアンス（SMA）

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。

背景説明

中央集中型ポリシー、ウイルスおよび発生（PVO）検疫機能ありました導入されるで AsyncOS 8.0（ESA）/8.1（SMA）。 この機能に追加ネットワーク接続必要条件があり、トラブルシューティングのためのいくつかの新しいチャレンジを提起します。

通信を理解して下さい

- CPQ 通信は転送メタデータのためにいくつかの余分コマンドで SMTP を、使用します
- SMA は中央 集中型 サービスの下で定義されたインターフェイスおよびポートの接続を- > ポリシー、ウイルスおよび発生検疫聞き取ります。 デフォルトで、ポートは 7025 です、しかしこれは管理者ユーザによって変更されるかもしれません!
- ESA はセキュリティ サービスの下で定義されたインターフェイスおよびポートの接続を- > ポリシー、ウイルスおよび発生検疫聞き取ります。 再度、デフォルトで、ポートは 7025 です、しかしこれは管理者ユーザによって変更されるかもしれません!
- SMA はまた ESA から構成情報を得るのに SSH を（コマンド クライアントによって）使用

します。 特に、これは SMA が ESA にリリースされた電子メールを渡すとき使用されます。 SMA は SSH を ESA 設定を問い合わせ、リリースされた電子メールをにか渡すどのインターフェイス/ポート判別するのに使用します。

リスナー

- ESA におよび SMA に両方特定のポートで受信する「cpq_listener」と問い合わせられた非表示リスナーがあります。
- これらのリスナーはコンフィギュレーション ファイルで見られる場合があります。 次に、例を示します。

- これらのリスナーは管理者ユーザ使用「suspendlisteners すべて」か「一時停止する」中断されます。 ポートが接続を許可しない場合、システム状態が「オフ・ ライン」およびレジュームもし必要ならであるかどうか確認する必要があります。

ESA から SMA に配信を解決して下さい

- ESA が設定されたポートの SMA に接続し、インターフェイスできることを確認して下さい。 これは telnet を使用してすることができます。 通信が正常である場合 220 バナーを得る必要があります。
- ESA に SMA への配信のために並べられる間、メッセージが含まれている「the.cpq.host」と呼ばれたデスティネーションオブジェクトがあります。 「tophosts」を使用して- > 配信ステータスこれを表示するか、または監視できます。 それと「hoststatus」を使用できません「showrecipients」および「deleterecipients」を必要ならば使用できます。

SMA から ESA に配信を解決して下さい

- SMA が設定されたポートの ESA に接続し、インターフェイスできることを確認して下さい。 再度、telnet を使用でき、成功すればために 220 バナーを参照して下さい。
- クラスタを使用するとき、重要ことはクラスタ水平な下セキュリティ サービスで定義されるインターフェイス- > マシン レベルですべてのアプライアンスのために存在 する ポリシー、ウイルスおよび発生検疫です。 （チェック ネットワーク- > IP インターフェイス）。
- SMA wil に ESA への配信のために並べられる間、発表されたメッセージが含まれている「the.cpq.release.host」と呼ばれるデスティネーションオブジェクトがあります。 「tophosts」を使用するとこれを表示できます。 これは「hoststatus」か「showrecipients を」使用しないようではなくそれの「deleterecipients」をテストしませんでしたが、これはおそらくどちらかをはたらかせません。
- また SMA と ESA 間の SSH 通信に問題があるかもしれません。 これらの問題は必ずしもネットワーク ベース常にではないです、たとえば CSCus29647 で SMA の内蔵部品はオペレーションの出かけます。 これらのような問題はメール ログに一般的にのでアプリケーション エラー出て来、通常 SMA のリブートによって解決することができる。

TLS/Certificates

- どちらの方向でもすべての CPQ 接続は TLS に頼り、その結果暗号設定はロールを担うことができます。
- 成功する TLS 接続のために接続を開くデバイスは受信側デバイスが hiddent CPQ 認証を使用していることを確認できる必要があります。 アプライアンスが匿名暗号をネゴシエートする場合これが失敗することは可能性のあるです。 これはそのようなこととして口グに現われます:

- 「追加によって行われる発信配信暗号リストから匿名暗号を単に取除くことによってこれらの問題を解決できます： -暗号リストの端への aNULL」。 次に、例を示します。 ： ： - **aNULL**

ログファイル

- SMA にメール ログ サブスクリプション (デフォルトで) があれば、追加把握を収集するためにメール ログを見ることができます。
- イベントを受け取る CPQ は SMA に検疫される ESA に発表されたメッセージおよびメッセージ両方のためにこのようになります

- グレップを使用してこれらのイベントを例捜すことができます: `CPQ ICIDmail_logs`
- ESA から検疫する SMA からの検疫からの CPQ 配信イベント、両方およびリリースは、他のどの配信に類似したに検知 します、但し例外としてカスタム ポートはリストされて、少数の行は冗漫「中央集中型ポリシー検疫」が含まれています。 下記の例:

- seach にによって使用すること、例これらのイベントをポートのためにグレップを検索できます: `7025" mail_logs`

ディセーブルにされる ESA「イネーブル」ボタン

ESA の PVO を有効に するように試みるとき完了するすべての前提条件設定にもかかわらず、「イネーブル」ボタンが選択不可能になることが分るかもしれません。 ESA は PVO ページを表示するとき設定が有効に なって準備ができていることを確認するために、ポート 7025 上の SMA と通信します。 この通信が失敗した場合、「イネーブル」ボタンは無効です。 あらゆる ESA と同様に「ESA のポート 7025" のための grepping によってこれを- > SMA ポート 7025 通信解決できます。 詳細については関連情報にリストされている TechNote を参照して下さい。

関連情報

- ESA がクラスタ化される場合の PVO 移行 ウィザードのための必要条件
- ESA 中心になるポリシー、ウイルスおよび発生検疫 (PVO) は有効に することができません