トラブルシューティング

- 一般的なトラブルシューティングとベスト プラクティス
- 認証に関する問題
- オブジェクトのブロックに関する問題
- ブラウザに関する問題
- DNS に関する問題
- フェールオーバーに関する問題
- 機能 キーの期限切れ
- FTP に関する問題
- アップロード/ダウンロード速度の問題（A-7 ページ）
- ハードウェアに関する問題
- HTTPS/復号化/証明書に関する問題
- Identity Services Engine に関する問題
- カスタム URL カテゴリおよび外部 URL カテゴリに関する問題
- ロギングに関する問題
- ポリシーに関する問題
- ファイル レピュテーションとファイル分析に関する問題
- リブートの問題
- サイトへのアクセスに関する問題
- アップストリーム プロキシに関する問題
- 仮想アプライアンス
- WCCP に関する問題
- パケット キャプチャ
- サポートの使用

一般的なトラブルシューティングとベスト プラクティス

以下のカスタム フィールドを含むようにアクセス ログを設定します。

%u、%g、%m、%k、%L（これらの値は大文字と小文字が区別されます）。

これらのフィールドの説明については、アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド（21-37 ページ）を参照してください。

設定の手順については、アクセス ログのカスタマイズ（21-32 ページ）およびログ サブスクリプションの追加と編集（21-8 ページ）を参照してください。

認証に関する問題

- 認証の問題のトラブルシューティング ツール
- 認証の失敗による通常動作への影響
- LDAP に関する問題
- 基本認証に関する問題
- シングル サインオンに関する問題
- 以下の項も参照してください。
  - 一般的なトラブルシューティングとベスト プラクティス
  - HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する
  - 認証をサポートしていない URL にアクセスできない
  - クライアント要求がアップストリーム プロキシで失敗する

認証の問題のトラブルシューティング ツール

Kerberos チケットのキャッシュを表示および消去するための KerbTray または klist（どちらも Windows Server Resource Kit に付属）。Active Directory を表示および編集するための Active Directory Explorer。Wireshark は、ネットワークのトラブルシューティングに使用できるパケット アナライザです。

認証の失敗による通常動作への影響

一部のユーザ エージェントまたはアプリケーションは、認証に失敗してアクセスを拒否されると、Web セキュリティ アプライアンスへの要求の送信を繰り返します。その結果、マシン クレデンシャルを使用して、Active Directory サーバへの要求の送信が繰り返されるので、運用に悪影響を及ぼすことがあります。

最適な結果を得るには、これらのユーザ エージェントの認証をバイパスします。問題のあるユーザ エージェントの認証のバイパス（5-30 ページ）を参照してください。

LDAP に関する問題

- NTLMSSP に起因する LDAP ユーザの認証の失敗
- LDAP 参照に起因する LDAP 認証の失敗

NTLMSSP に起因する LDAP ユーザの認証の失敗

LDAP サーバは NTLMSSP をサポートしていません。一部のクライアント アプリケーション（Internet Explorer など）は、NTLMSSP と Basic の選択肢が与えられたときに、常に NTLMSSP を選択します。以下の条件がすべて該当する場合は、ユーザの認証に失敗します。

- ユーザが LDAP レルムにのみ存在する。
- 識別プロファイルで LDAP レルムと NTLM レルムの両方を含むシーケンスを使用している。
- 識別プロファイルで「基本または NTLMSSP」認証方式を使用している。
- ユーザが Basic を介して NTLMSSP を選択するアプリケーションから要求を送信する。

上記の条件の少なくとも 1 つが該当する場合は、認証プロファイル、認証レルム、またはアプリケーションを再設定してください。

LDAP 参照に起因する LDAP 認証の失敗

以下の条件がすべて該当する場合は、LDAP 認証に失敗します。

- LDAP 認証レルムで Active Directory サーバを使用している。
- Active Directory サーバが別の認証サーバへの LDAP 参照を使用している。
- 参照された認証サーバが Web セキュリティ アプライアンスで使用できない。

回避策：

- アプライアンスで LDAP 認証レルムを設定するときに、Active Directory フォレストにグローバル カタログ サーバ（デフォルト ポートは 3268）を指定します。
- `advancedproxyconfig > authentication` CLI コマンドを使用して、LDAP 参照をディセーブルにします。デフォルトでは、LDAP 参照はディセーブルになります。

基本認証に関する問題

- 基本認証の失敗

関連する問題

- アップストリーム プロキシが基本クレデンシャルを受け取らない

基本認証の失敗

基本認証方式を使用する場合、AsyncOS for Web では 7 ビット ASCII 文字のパスフレーズのみがサポートされます。パスフレーズに 7 ビット ASCII 以外の文字が含まれていると、基本認証は失敗します。

シングル サインオンに関する問題

- エラーによりユーザがクレデンシャルを要求される

エラーによりユーザがクレデンシャルを要求される

Web セキュリティ アプライアンスが WCCP v2 対応デバイスに接続されている場合、NTLM 認証が機能しないことがあります。透過 NTLM 認証を適切に実行しない、厳格にロックダウンされた Internet Explorer バージョンを使ってユーザが要求を行っており、アプライアンスが WCCP v2 対応デバイスに接続されている場合、ブラウザはデフォルトで基本認証を使用します。その結果、認証クレデンシャルが不要な場合でも、ユーザはクレデンシャルの入力を要求されます。

回避策

Internet Explorer で、[ローカル イントラネット] ゾーンの [信頼済みサイト] リストに Web セキュリティ アプライアンスのリダイレクト ホスト名を追加します([ツール] > [インターネット オプション] > [セキュリティ] タブ)。

ブラウザに関する問題

- Firefox で WPAD を使用できない

Firefox で WPAD を使用できない

Firefox ブラウザが WPAD による DHCP ルックアップをサポートしていない可能性があります。最新の情報については、`https://bugzilla.mozilla.org/show_bug.cgi?id=356831` を参照してください。

PAC ファイルが Web セキュリティ アプライアンスにホストされている場合に、Firefox(または、DHCP をサポートしていない他のブラウザ)で WPAD を使用するには、ポート 80 を介して PAC ファイルを使用するようにアプライアンスを設定します。

手順 1　[セキュリティサービス(Security Services)] > [Web プロキシ(Web Proxy)] を選択し、[プロキシを設定する HTTP ポート(HTTP Ports to Proxy)] フィールドからポート 80 を削除します。

手順 2　アプライアンスにファイルをアップロードする場合、PAC サーバ ポートとしてポート 80 を使用します。

手順 3　ポート 80 の Web プロキシを指し示すようにブラウザが手動設定されている場合は、[プロキシを設定するHTTP ポート(HTTP Ports to Proxy)] フィールドで、別のポートを指し示すようにブラウザを再設定します。

手順 4　PAC ファイルのポート 80 への参照を変更します。

DNS に関する問題

- アラート:DNS キャッシュのブートに失敗(Failed to bootstrap the DNS cache)

アラート:DNS キャッシュのブートに失敗(Failed to bootstrap the DNS cache)

アプライアンスのリブート時に、「DNS キャッシュのブートに失敗(Failed to bootstrap the DNS cache)」というメッセージを含むアラートが生成された場合は、システムがプライマリ DNS サーバに接続できなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

機能 キーの期限切れ

(Web インターフェイスから)アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコの担当者またはサポート組織までご連絡ください。

フェールオーバーに関する問題

- フェールオーバーの誤った設定
- 仮想アプライアンスでのフェールオーバーに関する問題

フェールオーバーの誤った設定

フェールオーバー グループを誤って設定すると、複数のマスター アプライアンスが生じたり、その他のフェールオーバー問題が引き起こされる可能性があります。`failoverconfig` CLI コマンドの `testfailovergroup` サブコマンドを使用して、フェールオーバーの問題を診断します。

次に例を示します。

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: MASTER
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

仮想アプライアンスでのフェールオーバーに関する問題

仮想アプライアンス上に展開している場合は、ハイパーバイザのインターフェイス/仮想スイッチが無差別モードを使用するように設定されていることを確認してください。

FTP に関する問題

- URL カテゴリが一部の FTP サイトをブロックしない
- 大規模 FTP 転送の切断
- ファイルのアップロード後に FTP サーバにゼロ バイト ファイルが表示される
- Chrome ブラウザが FTP-over-HTTP 要求でユーザ エージェントとして検出されない（A-6 ページ）
- 以下のセクションも参照してください。
  - アップストリーム プロキシ経由で FTP 要求をルーティングできない
  - HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

URL カテゴリが一部の FTP サイトをブロックしない

ネイティブ FTP 要求が FTP プロキシに透過的にリダイレクトされる場合、FTP サーバに対するホスト名情報は含まれず、IP アドレス情報だけが含まれます。そのため、要求の宛先がそれらのサーバである場合でも、ホスト名情報しか持っていない一部の定義済み URL カテゴリと Web レピュテーション フィルタが、ネイティブ FTP 要求と一致しなくなります。それらのサイトへのアクセスをブロックする場合は、サイトの IP アドレスを使用してサイト用のカスタム URL カテゴリを作成する必要があります。

大規模 FTP 転送の切断

FTP プロキシと FTP サーバとの接続が遅い場合、特に、Cisco データ セキュリティ フィルタがイネーブルのときに、大きなファイルのアップロードに時間がかかることがあります。そのため、FTP プロキシがファイル全体をアップロードする前に FTP クライアントがタイムアウトしてしまい、トランザクション失敗の通知を受け取る場合があります。しかし、トランザクションは失敗しておらず、バックグラウンドで続行され、FTP プロキシによって完了されます。

FTP クライアントのアイドル タイムアウト値を適切に増加することにより、この問題を回避できます。

ファイルのアップロード後に FTP サーバにゼロ バイト ファイルが表示される

発信マルウェア対策スキャンによって FTP プロキシがアップロードをブロックすると、FTP クライアントは FTP サーバ上にゼロ バイト ファイルを作成します。

Chrome ブラウザが FTP-over-HTTP 要求でユーザ エージェントとして検出されない

FTP-over-HTTP 要求では、Chrome ブラウザはユーザ エージェント文字列を含まないためユーザ エージェントとして検出されません。

アップロード/ダウンロード速度の問題

WSA は、数千ものクライアントとサーバの接続を並行して処理するように設計されており、送信/受信バッファのサイズは安定性を犠牲にすることなく、最適なパフォーマンスを実現するように設定されています。通常、実際の用途は、多数の一時的な接続で構成されたブラウザ トラフィックです。これには受信パケットステアリング（RPS）データと受信フローステアリング（RFS）データが含まれ、WSA が最適化されています。

ただし、プロキシ経由で大容量ファイルを転送する場合などは、アップロードまたはダウンロード速度が著しく低下することがあります。たとえば、10 Mbps の回線で WSA を通じて 100 MB のファイルをダウンロードすると、サーバからファイルを直接ダウンロードするよりも約 7 ～ 8 倍の時間がかかる可能性があります。

大容量ファイル転送が多数行われる特異な環境では、この問題を改善するために networktuning コマンドを使用して送信/受信バッファのサイズを増やすことができますが、そうするとネットワーク メモリが枯渇してシステムの安定性に影響が生じる可能性もあります。networktuning コマンドの詳細については、Web セキュリティ アプライアンスの CLI コマンド（B-6 ページ）を参照してください。

注意　TCP 受信/送信バッファ制御ポイントとその他の TCP バッファ パラメータを変更する場合は、注意が必要です。副次的な影響を理解している場合にのみ、networktuning コマンドを使用してください。

networktuning コマンドの使用例を以下に示します。

S380 の場合

```
networktuning
    sendspace = 131072
    recvspace = 131072
    send_auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
    recv_auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
    mbuf_cluster_count = 98304 * (X/Y) where is X is RAM in GBs on the system and Y is 4GB.
    sendbuf_max = 1048576
    recvbuf_max = 1048576
```

Q.　これらのパラメータは何ですか。

A.　WSA には、固有のニーズに合わせて変更できる複数のバッファと最適化アルゴリズムがあります。バッファ サイズは、「最も一般的な」導入シナリオに合わせて初めから最適化されています。ただし、より高速の接続ごとのパフォーマンスが必要な場合に大きいバッファ サイズを使用できますが、全体的なメモリ使用量が増加します。そのため、バッファ サイズの増加は、システムで使用可能なメモリの範囲内にする必要があります。送信/受信スペース変数は、ソケット経由の通信用にデータを保存するために使用できるバッファ サイズを制御します。自動送信/受信オプションを使用して、送信/受信 TCP ウィンドウ サイズの動的スケーリングを有効および無効にします（これらのパラメータは、FreeBSD カーネルに適用されます）。

Q.　これらの例の値はどのように決定されましたか。

A.　この「問題」が発生したお客様のネットワークでさまざまな値のセットをテストして、これらの値に絞りました。その後、シスコのラボで安定性の変化とパフォーマンスの向上についてさらにテストしました。自己責任で、これら以外の値を自由に使用できます。

Q. なぜ、これらの値はデフォルトではないのですか。

A. 前述のとおり、デフォルトで WSA は最も一般的な導入向けに最適化されており、また、非常に多くの場所で動作する際に接続ごとのパフォーマンスに不満がないように最適化されています。ここで説明した変更を行うと、RPS 数は増加せず、実際には低下する可能性があります。

ハードウェアに関する問題

- アプライアンスの電源の再投入（A-8 ページ）
- アプライアンスの状態およびステータス インジケータ（A-8 ページ）
- アラート：380 または 680 ハードウェアでの [バッテリ再学習タイムアウト（Battery Relearn Timed Out）]（RAID イベント）（A-8 ページ）

アプライアンスの電源の再投入

重要 x80 アプライアンスの電源を再投入する場合は、電源ボタンを押す前に、アプライアンスが回復する（すべての LED がグリーンになる）まで、少なくとも 20 分間お待ちください。

アプライアンスの状態およびステータス インジケータ

ハードウェア アプライアンスの前面パネルおよび/または後面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータについては、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から使用できるハードウェア ガイドを参照してください。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。

アラート：380 または 680 ハードウェアでの [バッテリ再学習タイムアウト（Battery Relearn Timed Out）]（RAID イベント）

このアラートは、問題を示している場合と示していない場合があります。バッテリ再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間、他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID タイプのアラートが示されない場合は、この警告を無視してかまいません。

HTTPS/復号化/証明書に関する問題

- URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス
- HTTPS 要求の失敗
- 特定 Web サイトの復号化のバイパス
- 埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項

- アラート:セキュリティ証明書に関する問題(Problem with Security Certificate)
- 以下の項も参照してください。
  - HTTPS トランザクションのロギング
  - HTTPS に対してアクセス ポリシーを設定できない
  - HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス

透過的にリダイレクトされた HTTPS 要求の場合、Web プロキシは宛先サーバとやり取りして、サーバ名とサーバが属する URL カテゴリを判別する必要があります。したがって、Web プロキシがルーティング ポリシー グループのメンバーシップを評価する時点では、まだ宛先サーバとやり取りしていないので、HTTPS 要求の URL カテゴリが不明です。URL カテゴリが不明だと、Web プロキシは透過的 HTTPS 要求を、メンバーシップ基準として URL カテゴリを使用しているルーティング ポリシーと照合できません。

その結果、透過的にリダイレクトされた HTTPS トランザクションは、ルーティング ポリシー グループのメンバーシップ基準を URL カテゴリによって定義していないルーティング ポリシーとのみ照合されます。すべてのユーザ定義のルーティング ポリシーがメンバーシップを URL カテゴリによって定義している場合、透過的 HTTPS トランザクションはデフォルトのルーティング ポリシー グループと照合されます。

HTTPS 要求の失敗

- IP ベースのサロゲートと透過的要求を含む HTTPS
- カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作

IP ベースのサロゲートと透過的要求を含む HTTPS

HTTPS 要求が、以前の HTTP 要求の認証情報を利用できないクライアントから発信された場合、AsyncOS は、HTTPS プロキシの設定に応じて、HTTPS 要求に失敗するか、またはユーザを認証するために HTTPS 要求を復号化します。この動作を定義するには、[セキュリティ サービス(Security Services)] > [HTTPS プロキシ(HTTPS Proxy)] ページで [HTTPS 透過的要求(HTTPS Transparent Request)] 設定を使用します。「復号化ポリシー」の章の「HTTPS プロキシの有効化」に関する項を参照してください。

カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作

パケット キャプチャをスキャンすると、カスタム カテゴリおよびデフォルト(Web)カテゴリの HTTPS 復号化パススルー ポリシーに対して別々の時間で「Client Hello」ハンドシェイクが送信されます。

デフォルト カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信する前に Client Hello が送信され、接続が失敗します。カスタム URL カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信した後に Client Hello が送信され、接続が成功します。

対応策として、SSL 3.0 のみと互換性がある Web ページのパススルー アクションを使用して、カスタム URL カテゴリを作成することができます。

特定 Web サイトの復号化のバイパス

HTTPS サーバへのトラフィックが、Web プロキシなどのプロキシ サーバによって復号化されると、一部の HTTPS サーバは期待どおりに機能しなくなります。たとえば、セキュリティの高い銀行のサイトなど、一部の Web サイトとそれらに関連する Web アプリケーションおよびアプレットは、オペレーティング システムの証明書ストアを使用するのではなく、信頼できる証明書のハードコードされたリストを維持します。

すべてのユーザがこれらのタイプのサイトにアクセスできるようにするには、これらのサーバへの HTTPS トラフィックの復号化をバイパスします。

手順 1　拡張プロパティを設定して、影響を受ける HTTPS サーバを含むカスタム URL カテゴリを作成します。

手順 2　メンバーシップの一環として手順 1 で作成されたカスタム URL カテゴリを使用する復号化ポリシーを作成し、カスタム URL カテゴリに対するアクションを [通過（Pass Through）] に設定します。

埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項

Referer ベースの例外は、アクセス ポリシーでのみサポートされます。HTTPS トラフィックでこの機能を使用するには、アクセス ポリシーで例外を定義する前に、例外用に選択する URL カテゴリの HTTPS 復号化を設定する必要があります。ただし、この機能は特定の条件下では機能しません。

- 接続がトンネル化されていて HTTPS 復号化が有効になっていない場合、この機能は HTTPS サイトに発行される要求に対して機能しません。
- RFC 2616 によると、ブラウザでは公開ブラウジングまたは匿名ブラウジングを選択できます。選択に応じて、HTTP ヘッダーの Referer の情報 および From の情報の組み込みが有効/無効になります。WSA の例外機能は、Referer ヘッダーの存在に完全に依存しているため、このヘッダーを無効にすると動作しなくなります。
- RFC 2616 に従って、参照元ページがセキュアなプロトコルで転送された場合、クライアントには（セキュアでない）HTTP 要求の Referer ヘッダー フィールドは含まれません。つまり、HTTPS ベースのサイトから HTTP ベースのサイトに送られる要求に Referer ヘッダーが含まれていないと、例外機能は期待どおりに動作しません。
- 復号ポリシーが設定されている場合（カスタム カテゴリが復号ポリシーと一致する場合やアクションがドロップに設定されている場合など）、そのカテゴリのすべての着信要求はドロップされ、バイパスは実行されません。

アラート:セキュリティ証明書に関する問題(Problem with Security Certificate)

通常、アプライアンスで生成またはアップロードされるルート証明書情報は、信頼できるルート認証局としてクライアント アプリケーションで認識されません。ユーザが HTTPS 要求を送信すると、大部分の Web ブラウザでは、デフォルトで、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアント アプリケーションによって表示されます。通常、エラー メッセージには、Web サイトのセキュリティ証明書が信頼できる認証局によって発行されていないこと、または Web サイトが未知の認証局によって認証されていることが表示されます。クライアント アプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

(注)　**Mozilla Firefox ブラウザ:**Mozilla Firefox ブラウザで使用するには、アップロードする証明書に「basicConstraints=CA:True」を含める必要があります。この制約により、Firefox は、信頼されたルート認証局としてルート証明書を認識できるようになります。

Identity Services Engine に関する問題

- ISE 問題のトラブルシューティング ツール
- ISE サーバの接続に関する問題
- ISE 関連の重要なログ メッセージ

ISE 問題のトラブルシューティング ツール

以下のツールは、ISE 関連の問題をトラブルシューティングする際に役立ちます。

- ISE テスト ユーティリティ。ISE サーバへの接続のテストに使用され、貴重な接続関連情報を提供します。これは、[Identity Services Engine] ページの [テスト開始(Start Test)] オプションです(ISE サービスへの接続を参照)。
- ISE およびプロキシ ログ。ログによるシステム アクティビティのモニタを参照してください。
- ISE 関連の CLI コマンド `iseconfig`および`isedata`。特に `isedata`は、セキュリティ グループ タグ(SGT)のダウンロードを確認するために使用します。詳細については、Web セキュリティ アプライアンスの CLI コマンドを参照してください。
- Web トラッキング機能およびポリシー トレース機能。これらを使用してポリシーの一致に関する問題をデバッグできます。たとえば、許可されるべきユーザがブロックされた場合(または、その逆の場合)などに使用できます。詳細については、[Web トラッキング(Web Tracking)] ページおよびポリシーのトラブルシューティング ツール:ポリシー トレースを参照してください。
- パケット キャプチャ(サポートの使用する場合)
- 認証ステータスを確認する場合は、`openssl` Online Certificate Status Protocol(`ocsp`)ユーティリティを使用できます。これは www.openssl.org から入手できます。

ISE サーバの接続に関する問題

証明書の問題

WSA と ISE サーバは 証明書を使用して正常な接続を相互認証します。したがって、一方のエンティティによって指定された各証明書を、もう一方が認識できなければなりません。たとえば、WSA のクライアント証明書が自己署名の場合、該当する ISE サーバの信頼できる証明書リストに同じ証明書が含まれている必要があります。同様に、WSA クライアント証明書が CA 署名付きの場合も、該当する ISE サーバにその CA ルート証明書が存在している必要があります。同様の要件は、ISE サーバ関連の管理証明書および pxGrid 証明書にも該当します。

証明書の要件およびインストールについては、Cisco Identity Services Engine の統合で説明されています。証明書関連の問題が発生した場合は、以下を確認してください。

- CA 署名付き証明書を使用する場合:
  - 管理証明書および pxGrid 証明書のルート CA 署名証明書が WSA に存在していることを確認します。
  - WSA クライアント証明書のルート CA 署名証明書が ISE サーバの信頼できる証明書リストに含まれていることを確認します。
- 自己署名証明書を使用する場合:
  - (WSA で生成され、ダウンロードされた)WSA クライアント証明書が、ISE サーバにアップロードされており、ISE サーバの信頼できる証明書リストに含まれていることを確認します。
  - (ISE サーバで生成され、ダウンロードされた)ISE 管理者証明書および pxGrid 証明書が、WSA にアップロードされており、WSA の証明書リストに含まれていることを確認します。
- 期限切れの証明書:
  - アップロード時に有効だった証明書が、期限切れでないことを確認します。

証明書の問題を示すログ出力

以下の ISE サービス ログの抜粋は、証明書の欠落または無効な証明書による接続タイムアウトを示しています。

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

WSA のこれらのトレース レベル ログ エントリは、30 秒後に ISE サーバへの接続の試行が終了されることを示しています。

ネットワークの問題

- [Identity Services Engine] ページで [テスト開始(Start Test)] を実行中に ISE サーバへの接続が失敗した場合(ISE サービスへの接続)は、ポート 443 と 5222 に設定されている ISE サーバへの接続を確認します。

  ポート 5222 は公式のクライアント/サーバ Extensible Messaging and Presence Protocol (XMPP) ポートであり、ISE サーバへの接続に使用されます。また、Jabber や Google Talk などのアプリケーションでも使用されます。ただし、一部のファイアウォールはポート 5222 をブロックするように設定されています。

  接続の確認に使用できるツールには、`tcpdump` などがあります。

ISE サーバの接続に関するその他の問題

WSA が ISE サーバへの接続を試みたときに、以下の問題によって失敗することがあります。

- ISE サーバのライセンスの期限が切れている。
- ISE サーバの [管理(Administration)] > [pxGrid サービス(pxGrid Services)] ページで、pxGrid ノードのステータスが [未接続(not connected)] になっている。このページで [自動登録の有効化(Enable Auto-Registration)] がオンになっていることを確認してください。
- 失効した WSA クライアント(特に「test_client」または「pxgrid_client」)が、ISE サーバ上に存在する。これらは削除する必要があります。ISE サーバの [管理(Administration)] > [pxGrid サービス(pxGrid Services)] > [クライアント(Clients)] を参照してください。
- すべてのサービスが起動して実行される前に、WSA が ISE サーバへの接続を試みている。

  ISE サーバに対する一部の変更(証明書のアップデートなど)では、ISE サーバまたはそこで実行されているサービスの再起動が必要です。この間に ISE サーバへの接続を試みると失敗しますが、最終的に接続に成功します。

ISE 関連の重要なログ メッセージ

ここでは、WSA における ISE 関連の重要なログ メッセージについて説明します。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  WSA の ISE プロセスが 30 秒以内に ISE サーバに接続できませんでした。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing.Please check ISE config`

  WSA クライアント証明書とキーが WSA の [Identity Service Engine] 設定ページでアップロードされなかったか、生成されませんでした。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  WSA の ISE プロセスが 120 秒以内に ISE サーバに接続できず、終了しました。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed …`

  WSA の ISE プロセスが、アップデートのために ISE サーバに登録できませんでした。

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: …`

  ISE サーバ接続用の WSA の ISE クライアントを作成するときに、内部エラーが発生しました。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: …`

  この内部エラーは、接続または再接続時に SGT の一括ダウンロードに失敗したことを示しています。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service.Error:…`

  WSA の ISE サービスの起動に失敗しました。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal …`

  WSA の ISE サービスが `heimdall` に Ready 信号を送信できませんでした。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal …`

  WSA の ISE サービスが `heimdall` に再起動信号を送信できませんでした。

カスタム URL カテゴリおよび外部 URL カテゴリに関する問題

- 外部ライブフィード ファイルのダウンロードに関する問題（A-14 ページ）
- IIS サーバでの .CSV ファイルの MIME タイプに関する問題（A-15 ページ）
- コピー アンド ペースト後にフィード ファイルの形式が不正になる（A-15 ページ）

外部ライブフィード ファイルのダウンロードに関する問題

カスタムおよび外部 URL カテゴリの作成と編集（9-16 ページ）において、[外部ライブフィード（External Live Feed）] ファイル（[シスコ フィード形式（Cisco Feed Format）] または [Office 365 フィード形式（Office 365 Feed Format）]）を指定する場合は、[ファイルの取得（Get File）] ボタンをクリックして指定サーバとの接続を開始し、ファイルをダウンロードして解析する必要があります。このプロセスの進行状況と結果が表示されます。エラーが発生した場合は、進行状況と結果が説明されます。問題を修正し、もう一度ファイルのダウンロードを試します。

次の 4 種類のエラーが発生する可能性があります。

- 接続の例外

  `Failed to resolve server hostname`：フィード ファイルの場所として指定した URL は無効です。この問題を解決するには、正しい URL を指定します。
- プロトコル エラー

  `Authentication failed due to invalid credentials`：サーバ認証が失敗しました。サーバ接続に適切なユーザ名とパスフレーズを指定します。

  `The requested file is not found on the server`：フィード ファイルに指定した URL が無効なリソースを示しています。指定したサーバで正しいファイルが使用できることを確認します。
- コンテンツ検証エラー

  `Failed to validate the content of the field`：フィード ファイルのコンテンツが無効です。
- 解析エラー

- シスコ フィード形式 .csv ファイルは、1 つ以上のエントリを含む必要があります。各エントリはサイトのアドレスまたは有効な正規表現文字列で、カンマ、アドレスタイプ（site または regex のいずれか）が続きます。フィード ファイルのエントリに対してこの表記規則に従わない場合、解析エラーがスローされます。

  また、http:// または https:// を site エントリの一部としてファイルに含めないでください。エラーが発生します。つまり、www.example.com は正しく解析されますが、http://www.example.com ではエラーが発生します。

- Microsoft サーバから取得した XML ファイルは、標準の XML パーサーによって解析されます。XML タギングの矛盾にも、解析エラーとしてフラグが付きます。

解析エラーの行番号はログに含まれます。次に例を示します。

Line 8: 'www.anyurl.com' - Line is missing address or address-type field.フィード ファイルの 8 行目には、有効なアドレスまたは正規表現のパターン、またはアドレスタイプは含まれていません。

Line 12: 'www.test.com' - Unknown address type.12 行目に無効なアドレスタイプがあります。アドレスタイプは site または regex のいずれかになります。

IIS サーバでの .CSV ファイルの MIME タイプに関する問題

カスタムおよび外部 URL カテゴリの作成と編集において、[外部ライブフィード カテゴリ（External Live Feed Category）] > [シスコ フィード形式（Cisco Feed Format）] オプションで .csv ファイルを指定すると、シスコ フィード形式サーバがインターネット インフォメーション サービス（IIS）のバージョン 7 または 8 ソフトウェアを実行している場合、ファイルの取得時に「406 受諾不可（406 not acceptable）」というエラー メッセージが表示されることがあります。同様に、feedsd ログで次のような内容が報告されます。31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'。

これは、IIS 上の .csv ファイルのデフォルトの MIME タイプが text/csv ではなく application/csv であるためです。この問題は、IIS サーバにログインし、.csv ファイルの MIME タイプのエントリを text/csv に編集することで解決できます。

コピー アンド ペースト後にフィード ファイルの形式が不正になる

UNIX または OS X システムから Windows システムに .csv（テキスト）フィード ファイルのコンテンツをコピーアンドペーストすると、余分な改行（\r）が自動的に追加され、フィード ファイルの形式が不正になることがあります。

.csv ファイルを手動で作成する場合や、SCP、FTP、または POST を使用して UNIX または OS X から Windows システムにファイルを転送する場合は、問題はありません。

ロギングに関する問題

- アクセス ログ エントリにカスタム URL カテゴリが表示されない
- HTTPS トランザクションのロギング
- アラート：生成データのレートを維持できない（Unable to Maintain the Rate of Data Being Generated）
- W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題

アクセス ログ エントリにカスタム URL カテゴリが表示されない

Web アクセス ポリシー グループに、[モニタ（Monito）] に設定されたカスタム URL カテゴリ セットとその他のコンポーネント（Web レピュテーション フィルタ、DVS エンジンなど）がある場合に、カスタム URL カテゴリ内の URL に対する要求を許可するかブロックするかについて最終決定が行われると、要求のアクセス ログ エントリには、カスタム URL カテゴリの代わりに、定義済みの URL カテゴリが表示されます。

HTTPS トランザクションのロギング

アクセス ログでの HTTPS トランザクションの表示は、HTTP トランザクションと似ていますが、特性は少し異なります。記録される内容は、トランザクションが HTTPS プロキシに明示的に送信されるか、または透過的にリダイレクトされるかどうかによって異なります。

- **TUNNEL。**これは、HTTPS 要求が HTTPS プロキシに透過的にリダイレクトされたときにアクセス ログに記録されます。
- **CONNECT。**これは、HTTPS 要求が HTTPS プロキシに明示的に送信されたときにアクセス ログに記録されます。

HTTPS トラフィックが復号化されたときは、アクセス ログにトランザクションに対して、以下の 2 つのエントリが含まれます。

- TUNNEL または CONNECT が、処理された要求のタイプに応じて記録されます。
- HTTP 方式および復号化された URL。例：「GET https://ftp.example.com」。

完全な URL は、HTTPS プロキシがトラフィックを復号化するときだけ表示されます。

アラート：生成データのレートを維持できない（Unable to Maintain the Rate of Data Being Generated）

内部ロギング プロセスがフル バッファにより Web トランザクション イベントをドロップする場合、AsyncOS for Web が設定されたアラート受信者にクリティカルな電子メール メッセージを送信します。

デフォルトでは、Web プロキシが非常に高い負荷を受けたときに、内部ロギング プロセスは Web プロキシの負荷を減らす際にそれらを記録するイベントをバッファします。ロギング バッファ ファイルが完全に満杯になったときに、Web プロキシはトラフィックの処理を続行しますが、ロギング プロセスはイベントの一部をアクセス ログまたは Web トラッキング レポートに記録しません。これは、Web トラフィックのスパイク時に発生する可能性があります。

ただし、アプライアンスが持続的に過剰容量になっている場合にも、ロギング バッファが満杯になることがあります。AsyncOS for Web は、ロギング プロセスがデータをドロップしなくなるまで、数分ごとにクリティカルな電子メール メッセージを送信し続けます。

クリティカルなメッセージは以下のようなテキストが含まれます。

```
Reporting Client: The reporting system is unable to maintain the rate of data being
generated. Any new data generated will be lost.
```

AsyncOS for Web が、このクリティカルなメッセージを継続的または頻繁に送信する場合、アプライアンスは過剰容量になっている可能性があります。Web セキュリティ アプライアンスの容量を追加する必要があるかどうかを確認するには、シスコ カスタマー サポートにお問い合わせください。

W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題

サードパーティ製のログ アナライザ ツールを使用して、W3C アクセス ログを閲覧したり解析する場合は、状況に応じて [タイムスタンプ(timestamp)] フィールドを含める必要があります。W3C の [タイムスタンプ(timestamp)] フィールドには、UNIX エポック以降の時間が表示され、ほとんどのログ アナライザはこの形式の時間のみ認識します。

ポリシーに関する問題

- HTTPS に対してアクセス ポリシーを設定できない
- オブジェクトのブロックに関する問題
- 識別プロファイルがポリシーから削除される
- ポリシーの照合に失敗
- ポリシーのトラブルシューティング ツール:ポリシー トレース
- URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセスも参照してください。

HTTPS に対してアクセス ポリシーを設定できない

HTTPS プロキシをイネーブルにすると、すべての HTTPS ポリシー決定が復号化ポリシーによって処理されます。また、アクセスおよびルーティング ポリシー グループ メンバーシップを HTTPS で定義することも、HTTPS トランザクションをブロックするようにアクセス ポリシーを設定することもできなくなります。

アクセスおよびルーティング ポリシー グループの一部のメンバーシップが HTTPS によって定義されており、一部のアクセス ポリシーが HTTPS をブロックする場合は、HTTPS プロキシをイネーブルにすると、それらのアクセスおよびルーティング ポリシー グループがディセーブルになります。ポリシーは、いつでもイネーブルにすることができますが、そうすると、HTTPS 関連の設定がすべて削除されます。

オブジェクトのブロックに関する問題

- 一部の Microsoft Office ファイルがブロックされない
- DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare の更新がブロックされる

一部の Microsoft Office ファイルがブロックされない

[ブロックするオブジェクト タイプ(Block Object Type)] セクションで Microsoft Office ファイルをブロックすると、一部の Microsoft Office ファイルがブロックされない可能性があります。

すべての Microsoft Office ファイルをブロックする必要がある場合は、[ブロックする MIME タイプ(Block Custom MIME Types)] フィールドに `application/x-ole` を追加します。ただし、このカスタム MIME タイプをブロックすると、Visio ファイルや一部のサード パーティ アプリケーションなど、すべての Microsoft 複合オブジェクト フォーマット タイプがブロックされます。

DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare の更新がブロックされる

DOS の実行可能オブジェクト タイプをブロックするように Web セキュリティ アプライアンスを設定すると、Windows OneCare のアップデートがブロックされます。

識別プロファイルがポリシーから削除される

識別プロファイルをディセーブルにすると、その識別プロファイルは関連するポリシーから削除されます。識別プロファイルがイネーブルになっていることを確認し、再びポリシーに追加します。

ポリシーの照合に失敗

- ポリシーが適用されない
- HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する
- HTTPS 要求および FTP over HTTP 要求の場合にユーザがグローバル ポリシーに一致
- ユーザに誤ったアクセス ポリシーが割り当てられる

ポリシーが適用されない

複数の識別プロファイルの基準が同じである場合、AsyncOS は一致する最初の識別プロファイルにトランザクションを割り当てます。したがって、トランザクションはその他の同じ基準の識別プロファイルとは照合されず、以降の同じ基準の識別プロファイルに適用されるポリシーは照合も適用もされません。

HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

クレデンシャルの暗号化がイネーブルの場合は、サロゲートとして IP アドレスを使用するようにアプライアンスを設定する必要があります。

クレデンシャルの暗号化がイネーブルになっており、サロゲート タイプとして Cookie を使用するように設定されている場合、認証は HTTPS 要求や FTP over HTTP 要求で機能しません。クレデンシャルの暗号化がイネーブルの場合、Web プロキシは HTTPS 接続を使用して、クライアントを認証のために Web プロキシ自体にリダイレクトするからです。認証が成功した後、Web プロキシは元の Web サイトにクライアントをリダイレクトします。ユーザの識別を続行するために、Web プロキシはサロゲート（IP またはクッキー）を使用する必要があります。ただし、要求が HTTP または FTP over HTTP を使用している場合、Cookie を使用してユーザを追跡すると、以下の動作が引き起こされます。

- **HTTPS。**Web プロキシは、復号化ポリシーを割り当てる前にユーザのアイデンティティを解決（したがって、トランザクションを復号化）する必要がありますが、トランザクションを復号化しない限り、Cookie を取得してユーザを識別することはできません。

- **FTP over HTTP。**FTP over HTTP を使用して FTP サーバにアクセスする場合のジレンマは、HTTPS サイトにアクセスする場合と同様です。Web プロキシは、アクセス ポリシーを割り当てる前にユーザのアイデンティティを解決する必要がありますが、FTP トランザクションから Cookie を設定できません。

したがって、HTTP 要求と FTP over HTTP 要求は、認証を必要としないアクセス ポリシーとのみ一致します。通常、これらの要求は、認証を必要としないグローバル アクセス ポリシーに一致します。

HTTPS 要求および FTP over HTTP 要求の場合にユーザがグローバル ポリシーに一致

アプライアンスがクッキー ベースの認証を使用している場合、Web プロキシは、HTTPS 要求および FTP over HTTP 要求に対してクライアントからクッキー情報を取得しません。このため、クッキーからユーザ名を取得できません。

HTTPS 要求や FTP over HTTP 要求は、他のメンバーシップ基準に従って識別プロファイルと照合されますが、識別プロファイルで認証が必要な場合でも、Web プロキシはクライアントに認証を要求しません。代わりに、Web プロキシはユーザ名を NULL に設定し、ユーザを未認証と見なします。

その後、ポリシーと照合して評価される際に、未認証の要求は [すべての ID（All Identities）] を指定しているポリシーとのみ一致し、[すべてのユーザ（All Users）] が適用されます。通常、これはグローバル アクセス ポリシーなどのグローバル ポリシーです。

ユーザに誤ったアクセス ポリシーが割り当てられる

- ネットワーク上のクライアントが、ネットワーク接続状態インジケータ（NCSI）を使用している。
- Web セキュリティ アプライアンスが NTLMSSP 認証を使用している。
- 識別プロファイルが IP ベースのサロゲートを使用している。

ユーザは自分のクレデンシャルではなく、マシン クレデンシャルを使用して識別され、その結果、誤ったアクセス ポリシーが割り当てられる場合があります。

回避策：

- マシン クレデンシャルのサロゲート タイムアウト値を小さくします。

手順 1　advancedproxyconfig > authentication CLI コマンドを使用します。

手順 2　マシン クレデンシャルのサロゲート タイムアウトを入力します。

ポリシーのトラブルシューティング ツール：ポリシー トレース

- ポリシー トレース ツールについて
- クライアント要求のトレース
- 詳細設定：要求の詳細
- 詳細設定：レスポンスの詳細の上書き

ポリシー トレース ツールについて

ポリシー トレース ツールはクライアント要求をエミュレートし、Web プロキシによる要求の処理方法を詳しく示します。Web プロキシの問題をトラブルシューティングするときに、このツールを使用し、クライアント要求を追跡してポリシー処理をデバッグできます。基本トレースを実行したり、詳細なトレース設定を行ってオプションをオーバーライドしたりできます。

(注)　ポリシー トレース ツールを使用する場合、Web プロキシはアクセス ログまたはレポート データベース内の要求を記録しません。

ポリシー トレース ツールは、要求を Web プロキシだけで使用されるポリシーと照合して評価します。これらのポリシーには、アクセス、暗号化 HTTPS 管理、ルーティング、セキュリティ、発信マルウェア スキャンがあげられます。

(注)　SOCKS および外部 DLP ポリシーは、ポリシー トレース ツールによって評価されません。

クライアント要求のトレース

(注)　CLI コマンド `maxhttpheadersize` を使用して、プロキシ要求の最大 HTTP ヘッダー サイズを変更できます。この値を大きくすると、指定したユーザが多数の認証グループに属しているか、または応答ヘッダーが現在の最大ヘッダー サイズよりも大きい場合に発生する可能性のあるポリシー トレースの失敗を軽減できます。このコマンドの詳細については、Web セキュリティ アプライアンスの CLI コマンド(B-6 ページ)を参照してください。

手順 1　[システム管理(System Administration)] > [ポリシー トレース(Policy Trace)] を選択します。

手順 2　[送信先 URL(Destination URL)] フィールドに、トレースする URL を入力します。

手順 3　(任意)追加のエミュレーション パラメータを入力します。

エミュレート対象	入力
要求を行う際に使用されるクライアントの送信元 IP アドレス。	[クライアント IP アドレス(Client IP Address)] フィールドに IP アドレス。 (注)　IP アドレスを指定しない場合、AsyncOS は localhost を使用します。また、SGT(セキュリティ グループ タグ)は取得できず、SGT に基づくポリシーは照合されません。
要求を行う際に使用される認証/識別クレデンシャル。	[ユーザ名(User Name)] フィールドにユーザ名を入力し、[認証/識別(Authentication/Identification)] ドロップダウン リストから [Identity Services Engine] または認証レルムを選択します。 (注)　イネーブルになっているオプションのみを使用できます。つまり、認証オプションと ISE オプションは、両方がイネーブルになっている場合にのみを使用できます。 ここで入力するユーザの認証については、そのユーザが Web セキュリティ アプライアンスを介して認証済みである必要があります。

手順 4　[一致するポリシーの検索(Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果(Results)] ペインに表示されます。

(注)　[HTTPS を通過(Pass Through HTTPS)] トランザクションでは、ポリシー トレース ツールはさらにスキャンをバイパスし、トランザクションにアクセス ポリシーは関連付けられません。同様に、[HTTPS を復号化(Decrypt HTTPS)] トランザクションでは、ツールは実際にはトランザクションを復号化できず、適用されるアクセス ポリシーを決定することができません。いずれの場合も、[ドロップ(Drop)] トランザクションの場合と同様、トレースの結果には「アクセス ポリシー:適用なし(Access policy: Not Applicable)」が表示されます。

関連項目

- 詳細設定:要求の詳細(A-21 ページ)
- 詳細設定:レスポンスの詳細の上書き(A-22 ページ)

詳細設定:要求の詳細

[ポリシー トレース(Policy Trace)] ページの [詳細設定(Advanced)] セクションで、[要求の詳細(Request Details)] ペインの設定項目を使用し、このポリシー トレース用に発信マルウェア スキャン要求を調整できます。

手順 1　[ポリシー トレース(Policy Trace)] ページの [詳細設定(Advanced)] セクションを展開します。

手順 2　[要求の詳細(Request Details)] ペインのフィールドを必要に応じて設定します。

設定	説明
プロキシ ポート(Proxy Port)	プロキシ ポートに基づいてポリシー グループ メンバーシップをテストするトレース要求に対して、使用する特定のプロキシ ポートを選択します。
ユーザ エージェント(User Agent)	要求でシミュレートするユーザ エージェントを指定します。
要求の時間帯(Time of Request)	要求でシミュレートする日付と時間帯を指定します。
ファイルのアップロード(Upload File)	要求でアップロードをシミュレートするローカル ファイルを選択します。 ここでアップロードするファイルを指定する場合、Web プロキシは、GET 要求ではなく HTTP POST 要求をシミュレートします。
オブジェクトのサイズ(Object Size)	要求オブジェクトのサイズ(バイト単位)を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。
MIME タイプ(MIME Type)	MIME タイプを入力します。
マルウェア対策スキャンの判定(Anti-malware Scanning Verdicts)	Webroot、McAfee、Sophos スキャンの判定をオーバーライドするには、オーバーライドする特定タイプの判定を選択します。

手順 3　[一致するポリシーの検索(Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果(Results)] ペインに表示されます。

詳細設定: レスポンスの詳細の上書き

[ポリシー トレース(Policy Trace)] ページの [詳細設定(Advanced)] セクションで、[レスポンスの詳細の上書き(Response Detail Overrides)] ペインの設定項目を使用し、このポリシー トレース用に Web アクセス ポリシー レスポンスのアスペクトを「調整」できます。

手順 1　[ポリシー トレース(Policy Trace)] ページの [詳細設定(Advanced)] セクションを展開します。

手順 2　[レスポンスの詳細の上書き(Response Detail Overrides)] ペインのフィールドを必要に応じて設定します。

設定	説明
URL カテゴリ(URL Category)	トレース応答の URL トランザクション カテゴリをオーバーライドするには、この設定を使用します。応答結果の URL カテゴリと置き換えるカテゴリを選択します。
Application	同様に、トレース応答のアプリケーション カテゴリをオーバーライドするには、この設定を使用します。応答結果のアプリケーション カテゴリと置き換えるカテゴリを選択します。
オブジェクトのサイズ(Object Size)	応答オブジェクトのサイズ(バイト単位)を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。
MIME タイプ(MIME Type)	MIME タイプを入力します。
Web レピュテーション スコア(Web Reputation Score)	Web レピュテーション スコア(-10.0 ～ 10.0)を入力します。
マルウェア対策スキャンの判定(Anti-malware Scanning Verdicts)	これらのオプションを使用して、トレース応答で提供される特定のマルウェア対策スキャンの判定をオーバーライドします。応答結果の Webroot、McAfee、または Sophos のスキャン判定と置き換える判定を選択します。

手順 3　[一致するポリシーの検索(Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果(Results)] ペインに表示されます。

ファイル レピュテーションとファイル分析に関する問題

ファイル レピュテーションおよび分析のトラブルシューティング(14-20 ページ)を参照してください。

リブートの問題

- KVM で動作する仮想アプライアンスがリブート時にハングアップ
- ハードウェア アプライアンス:アプライアンスの電源のリモート リセット

KVM で動作する仮想アプライアンスがリブート時にハングアップ

(注)　これは KVM の問題であり、状況によって異なる場合があります。

詳細については、https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html および https://bugs.launchpad.net/qemu/+bug/1329956 を参照してください。

手順 1　以下の点をチェックします。

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

手順 2　上記の値が Y に設定されている場合:

a. 仮想アプライアンスを停止し、KVM カーネル モジュールを再インストールします。

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b. 仮想アプライアンスを再起動します。

ハードウェア アプライアンス:アプライアンスの電源のリモート リセット

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management (IPMI) ツールを使用してアプライアンス シャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。詳細については、リモート電源再投入の有効化 (22-5 ページ) を参照してください。
- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。詳細は、リモート電源再投入の有効化 (22-5 ページ) を参照してください。
- 以下の IPMI コマンドだけがサポートされます:status、on、off、cycle、reset、diag、soft。サポートされていないコマンドを発行すると、「権限不足」エラーが生じます。

はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

手順 1　IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

ここで 192.0.2.1 は、リモート電源管理ポートに割り当てられた IP アドレスであり、remoteresetuser および passphrase は、この機能を有効にしたときに入力したクレデンシャルです。

手順 2　アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。

サイトへのアクセスに関する問題

- 認証をサポートしていない URL にアクセスできない
- POST 要求を使用してサイトにアクセスできない
- 特定 Web サイトの復号化のバイパスも参照してください。

認証をサポートしていない URL にアクセスできない

以下は、認証をサポートしていないため、Web セキュリティ アプライアンスが透過モードで展開されている場合に使用できないアプリケーションのリストの一部です。

- Mozilla Thunderbird
- Adobe Acrobat アップデート
- HttpBridge
- CollabNet の Subversion
- Microsoft Windows アップデート
- Microsoft Visual Studio

回避策：認証を必要としない URL のユーザ クラスを作成します。

関連項目

- 認証のバイパス（5-32 ページ）

POST 要求を使用してサイトにアクセスできない

ユーザの最初のクライアント要求が POST 要求で、ユーザの認証が必要な場合、POST 本文のコンテンツは失われます。この問題は、アクセス コントロールのシングル サインオン機能を使用しているアプリケーションに対して POST 要求を行った場合に発生することがあります。

回避策：

- 最初の要求として POST を使用する URL に接続する前に、ブラウザから別の URL を要求して、最初に Web プロキシでユーザを認証させます。
- 最初の要求として POST を使用する URL の認証をバイパスします。

（注）　アクセス コントロールを使用すると、アプリケーション認証ポリシーで設定された Assertion Consumer Service（ACS）URL の認証をバイパスできます。

関連項目

- 認証のバイパス (5-32 ページ)

アップストリーム プロキシに関する問題

- アップストリーム プロキシが基本クレデンシャルを受け取らない
- クライアント要求がアップストリーム プロキシで失敗する

アップストリーム プロキシが基本クレデンシャルを受け取らない

アプライアンスとアップストリーム プロキシの両方が NTLMSPP による認証を使用している場合、設定によっては、アプライアンスとアップストリーム プロキシで、認証クレデンシャルを要求する無限ループが発生する可能性があります。たとえば、アップストリーム プロキシでは基本認証が必要だが、アプライアンスでは NTLMSPP 認証が必要な場合、アプライアンスはアップストリーム プロキシに正常に基本認証クレデンシャルを渡すことができません。これは、認証プロトコルの制限によるものです。

クライアント要求がアップストリーム プロキシで失敗する

設定:

- Web セキュリティ アプライアンスとアップストリーム プロキシ サーバが基本認証を使用している。
- ダウンストリームの Web セキュリティ アプライアンスでクレデンシャルの暗号化がイネーブルになっている。

Web プロキシはクライアントから「Authorization」HTTP ヘッダーを受信しますが、アップストリーム プロキシ サーバは「Proxy-Authorization」HTTP ヘッダーを要求するため、クライアント要求はアップストリーム プロキシで失敗します。

アップストリーム プロキシ経由で FTP 要求をルーティングできない

ネットワークに FTP 接続をサポートしていないアップストリーム プロキシが含まれる場合は、すべての ID に適用され、かつ FTP 要求にのみ適用されるルーティング ポリシーを作成する必要があります。ルーティング ポリシーを設定して、FTP サーバに直接接続するか、プロキシのすべてが FTP 接続をサポートしているプロキシ グループに接続します。

仮想アプライアンス

- AsyncOS の起動中に [強制リセット (Reset)]、[電源オフ (Power Off)]、または [リセット (Reset)] オプションを使用しないでください
- KVM 展開でネットワーク接続が最初は機能するが、その後失敗する
- KVM 展開におけるパフォーマンスの低下、ウォッチドッグの問題、および CPU の使用率が高い
- Linux ホストで実行している仮想アプライアンスの一般的なトラブルシューティング

AsyncOS の起動中に [強制リセット（Reset）]、[電源オフ（Power Off）]、または [リセット（Reset）] オプションを使用しないでください

仮想ホストにおける以下の操作は、ハードウェア アプライアンスのプラグを抜くことと同等であり、特に AsyncOS の起動中ではサポートされていません。

- KVM の強制リセットオプション。
- VMware の電源オフとリセット オプション。（これらのオプションは、アプライアンスが完全に起動してから安全に使用できます）。

KVM 展開でネットワーク接続が最初は機能するが、その後失敗する

問題　前回の作業後にネットワーク接続が失われる。

解決策　これは KVM の問題です。OpenStack ドキュメントの「KVM: Network connectivity works initially, then fails」の項を参照してください。このドキュメントは、http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html にあります。

KVM 展開におけるパフォーマンスの低下、ウォッチドッグの問題、および CPU の使用率が高い

問題　Ubuntu 仮想マシン上で実行しているときに、アプライアンスのパフォーマンスが低下して、ウォッチドッグの問題が発生し、アプライアンスが異常に高い CPU 使用率を示す。

解決策　Ubuntu から Host OS アップデートをインストールしてください。

Linux ホストで実行している仮想アプライアンスの一般的なトラブルシューティング

問題　KVM 展開で動作している仮想アプライアンスに関する問題は、ホスト OS の設定の問題に関連している可能性があります。

解決策　『*Virtualization Deployment and Administration Guide*』のトラブルシューティンに関する項およびその他の情報を参照してください。このドキュメントは、https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf から入手できます。

WCCP に関する問題

- 最大ポート エントリ数

最大ポート エントリ数

WCCP を使用している展開では、HTTP、HTTPS、FTP ポートを合計した最大ポート エントリ数は 30 になります。

パケット キャプチャ

- パケット キャプチャの開始
- パケット キャプチャ ファイルの管理

アプライアンスでは、アプライアンスが接続されているネットワークで送受信される TCP/IP と他のパケットをキャプチャして表示できます。

(注)　パケット キャプチャ機能は UNIX の tcpdump コマンドに似ています。

パケット キャプチャの開始

手順 1　[ヘルプとサポート(Help and Support)] > [パケットキャプチャ(Packet Capture)] を選択します。

手順 2　(任意)[設定の編集(Edit Settings)] をクリックし、パケット キャプチャの設定を変更します。

オプション	説明
キャプチャ ファイル サイズ制限(Capture File Size Limit)	キャプチャ ファイルを拡大できる最大サイズを指定します。[キャプチャ期間(Capture Duration)] が [ファイルサイズの上限に達するまでキャプチャを実行(Run Capture Until File Size Limit Reached)] に設定されていない場合は、上限に達すると、データが破棄されて新しいファイルが開始されます。
キャプチャ期間(Capture Duration)	キャプチャを自動的に停止するとき(および場合)のオプション。次から選択します。 • [ファイルサイズの上限に達するまでキャプチャを実行(Run Capture Until File Size Limit Reached)]。キャプチャはファイル サイズの上限に達するまで実行されます。 • [制限時間に達するまでキャプチャを実行(Run Capture Until Time Elapsed Reaches)]。キャプチャは指定された期間だけ実行されます。単位を指定せずに時間の長さを入力すると、AsyncOS は、デフォルトで秒を使用します。 • [制限なしでキャプチャを実行(Run Capture Indefinitely)]。パケット キャプチャは、手動で停止するまで実行されます。 (注)　キャプチャは手動でいつでも終了できます。
インターフェイス	トラフィックがキャプチャされるインターフェイス。
フィルタ(Filters)	パケットをキャプチャするときに適用するフィルタリング オプション。フィルタリングを使用すると、必要なパケットだけをキャプチャできます。次から選択します。 • [フィルタなし(No Filters)]。すべてのパケットがキャプチャされます。 • [事前定義されたフィルタ(Predefined Filters)]。定義済みのフィルタを使用して、ポートや IP アドレスによりフィルタリングできます。何も指定しなかった場合は、すべてのトラフィックがキャプチャされます。 • [カスタムフィルタ(Custom Filter)]。必要なパケット キャプチャ オプションの正確な構文がわかっている場合は、このオプションを使用します。標準の tcpdump 構文を使用します。

（任意）パケット キャプチャの変更を送信して確定します。

（注）　変更内容をコミットせずにパケット キャプチャ設定を変更し、パケット キャプチャを開始する場合、AsyncOS は新しい設定を使用します。これにより、今後のパケット キャプチャの実行に対する設定を適用せずに現在のセッションで新しい設定を使用することができます。この設定は、クリアするまで有効なままになります。

手順 3　[キャプチャを開始（Start Capture）] をクリックします。実行中のキャプチャを手動で停止するには、[キャプチャを停止（Stop Capture）] をクリックします。

パケット キャプチャ ファイルの管理

アプライアンスは、取り込んだパケット アクティビティをファイルに保存し、そのファイルをローカルに格納します。デバッグやトラブルシューティングのために、FTP を使用してパケット キャプチャ ファイルをシスコ カスタマー サポートに送信できます。

- パケット キャプチャ ファイルのダウンロードまたは削除

パケット キャプチャ ファイルのダウンロードまたは削除

（注）　また、FTP を使用してアプライアンスに接続し、captures ディレクトリからパケット キャプチャ ファイルを取り出すこともできます。

手順 1　[ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。

手順 2　[パケットキャプチャファイルの管理（Manage Packet Capture Files）] ペインから、使用するパケット キャプチャ ファイルを選択します。このペインが表示されない場合は、アプライアンスにパケット キャプチャ ファイルが保存されていません。

手順 3　必要に応じて、[ファイルのダウンロード（Download File）] または [選択ファイルの削除（Delete Selected File）] をクリックします。

サポートの使用

- 効率的なサービス提供のため情報収集（A-29 ページ）
- テクニカル サポート要請の開始（A-29 ページ）
- 仮想アプライアンスのサポートの取得（A-29 ページ）
- アプライアンスへのリモート アクセスのイネーブル化（A-30 ページ）

効率的なサービス提供のため情報収集

サポートに問い合わせる前に以下の手順を実行してください。

- 一般的なトラブルシューティングとベスト プラクティス（A-2 ページ）の説明に従い、カスタム ログのフィールドを有効にします。
- パケット キャプチャを実行することを検討してください。パケット キャプチャ（A-27 ページ）を参照してください。

テクニカル サポート要請の開始

緊急ではない場合は、アプライアンスを使用してサポート要請をシスコ カスタマー サポートに送信できます。アプライアンスは要請を送信する際に、アプライアンスの設定も送信します。サポート要求を送信するには、アプライアンスがインターネットに電子メールを送信できる必要があります。

(注)　緊急の問題がある場合は、Cisco Worldwide Support Center に連絡してください。

はじめる前に

- 自身の Cisco.com ユーザ ID がこのアプライアンスのサービス契約に関連付けられていることを確認します。Cisco.com プロファイルに現在関連付けられているサービス契約のリストを閲覧するには、Cisco.com Profile Manager（https://sso.cisco.com/autho/forms/CDClogin.html）にアクセスしてください。Cisco.com ユーザ ID をお持ちでない場合は、登録して ID を取得してください。

手順 1　[ヘルプとサポート（Help and Support）] > [テクニカルサポートに問い合わせる（Contact Technical Support）] を選択します。

手順 2　（任意）要請のその他の受信者を選択します。デフォルトでは、サポート要請とコンフィギュレーション ファイルがシスコ カスタマー サポートに送信されます。

手順 3　自身の連絡先情報を入力します。

手順 4　問題の詳細を入力します。

- この問題に関するカスタマー サポート チケットをすでに持っている場合は、それを入力してください。

手順 5　[送信（Send）] をクリックします。トラブル チケットがシスコで作成されます。

仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、仮想ライセンス番号（VLN）、契約番号、および製品 ID コード（PID）を提供する必要があります。

発注書を参照するか以下の表を使用すると、仮想アプライアンスで動作中のソフトウェア ライセンスに基づく PID を特定できます。

機能	PID	説明
Web Security Essentials	WSA-WSE-LIC=	内容: • Web Usage Controls • Web レピュテーション
Web Security Premium	WSA-WSP-LIC=	内容: • Web Usage Controls • Web レピュテーション • Sophos および Webroot Anti-Malware シグネチャ
Web Security Anti-Malware	WSA-WSM-LIC=	Sophos および Webroot Anti-Malware シグネチャが含まれます。
McAfee Anti-Malware	WSA-AMM-LIC=	—
Advanced Malware Protection	WSA-AMP-LIC=	—

アプライアンスへのリモート アクセスのイネーブル化

[リモートアクセス(Remote Access)] オプションを使用すると、シスコ カスタマー サポートがサポートのためにリモート アプライアンスにアクセスできるようになります。

手順 1　[ヘルプとサポート(Help and Support)] > [リモートアクセス(Remote Access)] を選択します。

手順 2　[有効(Enable)] をクリックします。

手順 3　[カスタマーサポートのリモートアクセス(Customer Support Remote Access)] オプションを設定します。

オプション	説明
シード文字列(Seed String)	文字列を入力する場合は、その文字列が既存または将来のパスフレーズと一致しないようにしてください。 [送信(Submit)] をクリックすると、文字列がページの上部に表示されます。 この文字列をサポート担当者に提出します。
セキュア トンネル(Secure Tunnel)(推奨)	リモート アクセス接続にセキュア トンネルを使用するかどうかを指定します。 このオプションがイネーブルの場合、アプライアンスは、指定されたポートからサーバ upgrades.ironport.com への SSH トンネルを作成します(デフォルトでは、ポート 443)。接続が確立されると、シスコ カスタマー サポートは SSH トンネルを使用してアプライアンスにアクセスできるようになります。 techsupport トンネルがイネーブルになると、`upgrades.ironport.com` に 7 日間接続されたままになります。7 日が経過すると、techsupport トンネルを使用して新しい接続を作成できなくなりますが、既存の接続は存続し、機能します。 リモート アクセス アカウントは、明確に非アクティブ化されるまでアクティブな状態を維持します。

手順 4　変更を送信し、保存します。

手順 5　ページ上部近くに表示される成功メッセージでシード文字列を検索し、書き留めます。

セキュリティ上の理由から、この文字列はアプライアンスに保存されず、後から文字列を確認する方法はありません。

安全な場所にこのシード文字列を保存します。

手順 6　シード文字列をサポート担当者に提出します。