モニタリングおよびトラブルシューティング

この章で説明する内容は、次のとおりです。

ログによるシステム アクティビティのモニター

この章で説明する内容は、次のとおりです。

- ログ ファイルのフィールドとタグ （57 ページ）
- ロギングのトラブルシューティング （75 ページ）

ロギングの概要

Secure Web Applianceでは、システムとトラフィックの管理アクティビティの記録がログファイル上に書き込まれます。管理者はこれらのログ ファイルを参照して、アプライアンスをモニターし、トラブルシューティングできます。

各種アクティビティはいくつかのロギング タイプごとに記録されるため、特定のアクティビティに関する情報の検索が容易です。多くのロギング タイプはデフォルトでイネーブルなりますが、いくつかは、必要に応じて手動でイネーブルにする必要があります。

ログ ファイルをイネーブルにして管理するには、ログ ファイル サブスクリプションを設定します。サブスクリプションにより、ログファイルの作成、カスタマイズ、および管理に関する設定を定義できます。

通常、管理者が主に使用するログ ファイルは、以下の 2 種類です。

- **アクセス ログ。**すべての Web プロキシ フィルタリングとスキャン アクティビティが記録されます。
- **トラフィック モニター ログ。**すべての L4 トラフィック モニター アクティビティが記録されます。

これらのログ タイプおよびその他のログ タイプを使用して、アプライアンスの現在と過去のアクティビティを確認できます。ログ ファイル エントリの内容を理解できるように、リファレンス テーブルが用意されています。

関連項目

- ロギングの共通タスク, on page 2
- ログ ファイルのタイプ, on page 4

ロギングの共通タスク

タスク	関連項目および手順へのリンク
ログ サブスクリプションを追加および編集する	ログ サブスクリプションの追加および編集, on page 12
ログ ファイルを表示する	ログ ファイルの表示, on page 22
ログ ファイルを解釈する	アクセス ログのスキャン判定エントリの解釈, on page 39
ログ ファイルをカスタマイズする	アクセス ログのカスタマイズ, on page 50

タスク	関連項目および手順へのリンク
別のサーバーにログ ファイルをプッシュする	別のサーバへのログ ファイルのプッシュ, on page 19
ログ ファイルをアーカイブする	ログ ファイルのアーカイブ, on page 20

ロギングのベスト プラクティス

- ログ サブスクリプションの数を最小限にすると、システム パフォーマンスが向上します。
- 記録する詳細を少なくすると、システム パフォーマンスが向上します。

ログによる Web プロキシのトラブルシューティング

Secure Web Applianceでは、デフォルトで、Web プロキシ ロギング メッセージ用の 1 つのログ サブスクリプションが作成されます（「デフォルト プロキシ ログ」と呼ばれます）このログには、すべての Web プロキシ モジュールに関する基本的な情報が記録されます。アプライアンスには、各 Web プロキシ モジュールのログ ファイル タイプも含まれているので、デフォルト プロキシ ログを画面いっぱいに散乱させることなく、各モジュールのより詳細なデバッグ情報を読み取ることができます。

使用可能な各種のログを使用して Web プロキシの問題をトラブルシューティングするには、以下の手順に従います。

Procedure

ステップ 1 デフォルト プロキシ ログを読みます。

ステップ 2 問題を解決するためにより詳細な情報が必要な場合は、その問題に関連する特定の Web プロキシ モジュールのログ サブスクリプションを作成します。以下の Web プロキシ モジュール ログ タイプのサブスクリプションを作成できます。

アクセス コントロール エンジン ログ	ロギング フレームワーク ログ
ADC エンジンフレームワークログ	McAfee 統合フレームワーク ログ
AVC エンジンフレームワークログ	メモリ マネージャ ログ
設定ログ	その他のプロキシ モジュール ログ
接続管理ログ	リクエスト デバッグ ログ
データ セキュリティ モジュール ログ	SNMP モジュール ログ
DCA エンジン フレームワーク ログ	Sophos 統合フレームワーク ログ
ディスク マネージャ ログ	WBRS フレームワーク ログ
FireAMP	WCCP モジュール ログ
FTP プロキシ ログ	Webcat 統合フレームワーク ログ
HTTPS ログ	Webroot 統合フレームワーク ログ
ライセンス モジュール ログ	

ステップ 3 問題を再現して、その問題に関する新しい Web プロキシ モジュール ログを確認します。

ステップ 4 必要に応じて、他の Web プロキシ モジュール ログを使用して繰り返します。

ステップ 5 不要になったサブスクリプションを削除します。

What to do next

関連項目

- ログ ファイルのタイプ, on page 4
- ログ サブスクリプションの追加および編集, on page 12

ログ ファイルのタイプ

Webプロキシコンポーネントに関するいくつかのログタイプはイネーブルになっていません。「デフォルト プロキシ ログ」と呼ばれるメインの Web プロキシ ログ タイプはデフォルトでイネーブルになっており、すべてのWebプロキシモジュールの基本的な情報が記録されます。各 Web プロキシ モジュールには、必要に応じてイネーブルにできる独自のログ タイプがあります。

以下の表は、 Secure Web Applianceのログ ファイル タイプを示しています。

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
アクセス コントロール エンジン ログ	Web プロキシ ACL（アクセス コントロール リスト）の評価エンジンに関連するメッセージを記録します。	非対応	非対応
AMP エンジンログ	ファイル レピュテーション スキャンとファイル分析に関する情報（Advanced Malware Protection）を記録します。 ログ ファイルも参照してください。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
監査ログ	認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、および Accounting）を記録します。アプリケーションおよびコマンドライン インターフェイスにおけるすべてのユーザ操作を記録し、変更内容を保存します。 監査ログの詳細の一部を次に示します。 • ユーザ - ログオン • ユーザ- ログオンに失敗しました、パスワードが正しくありません • ユーザ- ログオンに失敗しました、ユーザ名が不明です • ユーザ- ログオンに失敗しました、アカウントの有効期限が切れています • ユーザ - ログオフ • ユーザ - ロックアウト • ユーザ - アクティブ化済み • ユーザ - パスワードの変更 • ユーザ - パスワードのリセット • ユーザ -セキュリティ設定/プロファイルの変更 • ユーザ - 作成済み • ユーザ -削除済み/変更済み • グループ/ロール - 削除/変更済み • グループ/ロール - アクセス許可の変更	対応	対応
アクセス ログ	Web プロキシのクライアント履歴を記録します。	対応	対応
ADC エンジンフレームワークログ	Web プロキシと ADC エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
ADC エンジンログ	AVC エンジンからのデバッグメッセージを記録します。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
認証フレームワーク ログ	認証履歴とメッセージを記録します。	非対応	対応
AVC エンジン フレームワーク ログ	Web プロキシと AVC エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
AVC エンジン ログ	AVC エンジンからのデバッグ メッセージを記録します。	対応	対応
CLI 監査ログ	コマンドラインインターフェイス アクティビティの監査履歴を記録します。	対応	対応
設定ログ	Web プロキシ コンフィギュレーション管理システムに関連するメッセージを記録します。	非対応	非対応
接続管理ログ	Web プロキシ接続管理システムに関連するメッセージを記録します。	非対応	非対応
データ セキュリティ ログ	Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。	対応	対応
データ セキュリティ モジュール ログ	Cisco データ セキュリティ フィルタに関するメッセージを記録します。	非対応	非対応
DCA エンジン フレームワーク ログ（動的コンテンツ分析）	Web プロキシと Cisco Web 利用の制御動的コンテンツ分析エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
DCA エンジン ログ（動的コンテンツ分析）	Cisco Web 利用の制御動的コンテンツ分析エンジンに関連するメッセージを記録します。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
デフォルト プロキシ ログ	Web プロキシに関連するエラーを記録します。 これは、Web プロキシに関連するすべてのログの最も基本的なものです。Web プロキシに関連するより具体的な分野のトラブルシューティングを行うには、該当する Web プロキシ モジュールのログ サブスクリプションを作成します。	対応	対応
ディスク マネージャ ログ	ディスク上のキャッシュの書き込みに関連する Web プロキシ メッセージを記録します。	非対応	非対応
外部認証ログ	外部認証サーバによる通信の成功または失敗など、外部認証機能の使用に関連するメッセージを記録します。 外部認証がディセーブルされている場合でも、このログにはローカル ユーザのログインの成功または失敗に関するメッセージが記録されています。	非対応	対応
フィードバック ログ	誤って分類されたページをレポートする Web ユーザを記録します。	対応	対応
FTP プロキシ ログ	FTP プロキシに関連するエラーおよび警告メッセージを記録します。	非対応	非対応
FTP サーバ ログ	FTP を使用して、 Secure Web Appliance にアップロードされ、ダウンロードされるすべてのファイルを記録します。	対応	対応
GUI ログ （グラフィカル ユーザ インターフェイス）	Web インターフェイスのページ更新履歴を記録します。GUI ログには、SMTP トランザクションに関する情報（たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。	対応	対応
Haystack ログ	Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
HTTPS ログ	HTTPS プロキシ固有の Web プロキシ メッセージを記録します（HTTPS プロキシがイネーブルの場合）。	非対応	非対応
ISE サーバ ログ	ISE サーバの接続および動作情報を記録します。	対応	対応
ライセンス モジュール ログ	Web プロキシのライセンスおよび機能キー処理システムに関するメッセージを記録します。	非対応	非対応
ロギング フレームワーク ログ	Web プロキシのロギング システムに関するメッセージを記録します。	非対応	非対応
ロギング ログ	ログ管理に関連するエラーを記録します。	対応	対応
McAfee 統合フレームワーク ログ	Web プロキシと McAfee スキャン エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
McAfee ログ	McAfee スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	対応	対応
メモリ マネージャ ログ	Web プロキシ プロセスのメモリ内キャッシュを含むすべてのメモリの管理に関連する Web プロキシ メッセージを記録します。	非対応	非対応
その他のプロキシ モジュール ログ	主に開発者やカスタマー サポートによって使用される Web プロキシ メッセージを記録します。	非対応	非対応
AnyConnect セキュア モビリティ デーモン ログ	ステータスチェックなど、 Secure Web Appliance と AnyConnect クライアント間の相互作用を記録します。	対応	対応
NTP ログ（ネットワーク タイム プロトコル）	ネットワーク タイム プロトコルによって作成されたシステム時刻に変更します。	対応	対応
PAC ファイル ホスティング デーモン ログ	クライアントによるプロキシ自動設定（PAC）ファイルの使用状況を記録します。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
プロキシ バイパス ログ	Webプロキシをバイパスするトランザクションを記録します。	非対応	対応
レポーティング ログ	レポート生成履歴を記録します。	対応	対応
レポーティング クエリー ログ	レポート生成に関連するエラーを記録します。	対応	対応
リクエスト デバッグ ログ	すべての Web プロキシ モジュール ログ タイプから、特定の HTTP トランザクションに関する非常に詳細なデバッグ情報を記録します。他のすべてのプロキシ ログ サブスクリプションを作成することなく、特定のトランザクションによるプロキシ問題のトラブルシューティングを行うために、このログ サブスクリプションを作成する場合があります。 **注**：CLIでのみ、このログサブスクリプションを作成できます。	非対応	非対応
認証ログ	アクセス コントロール機能に関するメッセージを記録します。	対応	対応
SHD ログ （システム ヘルス デーモン）	システム サービスの動作状態の履歴および予期しないデーモンの再起動の履歴を記録します。	対応	対応
SNMP ログ	SNMP管理エンジンに関連するデバッグメッセージを記録します。	対応	対応
SNMP モジュール ログ	SNMP モニタリング システムとの対話に関連する Webプロキシ メッセージを記録します。	非対応	非対応
Sophos 統合フレームワーク ログ	Web プロキシと Sophos スキャン エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
Sophos ログ	Sophos スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	対応	対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
ステータス ログ	機能キーのダウンロードなど、システムに関連する情報を記録します。	対応	対応
システム ログ	DNS、エラー、およびコミット アクティビティを記録します。	対応	対応
トラフィック モニタリング エラー ログ	L4TM インターフェイスおよびキャプチャ エラーを記録します。	対応	対応
トラフィック モニタ ログ	L4TM ブロックおよび許可リストに追加されたサイトを記録します。	非対応	対応
UDS ログ （ユーザ検出サービス）	Web プロキシが実際の認証を行わずにユーザ名を検出する方法に関するデータを記録します。セキュア モビリティ用の Cisco 適応型セキュリティ アプライアンスとの対話、および透過的ユーザ ID 用の Novell eDirectory サーバとの統合に関する情報が含まれます。	対応	対応
アップデータ ログ	WBRS およびその他の更新の履歴を記録します。	対応	対応
W3C ログ	W3C 準拠の形式で Web プロキシ クライアント履歴を記録します。 詳細については、W3C 準拠のアクセス ログ ファイル, on page 48を参照してください。	対応	非対応
WBNP ログ （SensorBase ネットワーク参加）	SensorBase ネットワークへの Cisco SensorBase ネットワーク参加のアップロード履歴を記録します。	非対応	対応
WBRS フレームワーク ログ （Web レピュテーション スコア）	Web プロキシと Web レピュテーション フィルタ間の通信に関連するメッセージを記録します。	非対応	非対応
WCCP モジュール ログ	WCCP の実装に関連する Web プロキシ メッセージを記録します。	非対応	非対応

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
Webcat 統合フレームワーク ログ	Web プロキシと Cisco Web 利用の制御に関連付けられた URL フィルタリング エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
Webroot 統合フレームワーク ログ	Web プロキシと Webroot スキャン エンジン間の通信に関連するメッセージを記録します。	非対応	非対応
Webroot ログ	Webroot スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	対応	対応
ウェルカム ページ確認ログ	エンド ユーザの確認ページで [同意する（Accept）] ボタンをクリックする Web クライアントの履歴を記録します。	対応	対応

ログ サブスクリプションの追加および編集

ログ ファイルのタイプごとに複数のログ サブスクリプションを作成できます。サブスクリプションには、以下のようなアーカイブおよびストレージに関する設定の詳細が含まれています。

- ロールオーバー設定。ログ ファイルをアーカイブするタイミングを決定します。
- アーカイブ ログの圧縮設定。
- アーカイブ ログの取得の設定。ログをリモート サーバに保存するか、アプライアンスに保存するかを指定します。

Procedure

ステップ 1 [システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 ログ サブスクリプションを追加するには、[ログ設定を追加（Add Log Subscription）] をクリックします。あるいは、ログ サブスクリプションを編集するには、[ログ名（Log Name）] フィールドのログ ファイルの名前をクリックします。

ステップ 3 サブスクリプションを設定します。

オプション	説明
ログ タイプ（Log Type）	ユーザが登録できる使用可能なログ ファイル タイプのリスト。このページの他のオプションは、選択したログ ファイル タイプによって異なります。 **Note** [リクエスト デバッグ ログ（Request Debug Logs）] タイプは CLI を使用してのみ登録でき、このリストには表示されません。
ログ名（Log Name）	Secure Web Applianceでサブスクリプションの参照に使用される名前。この名前は、サブスクリプションのログ ファイルを保存するログ ディレクトリにも使用されます。ASCII 文字（[0-9]、[A-Z]、[a-z]、および _）のみを入力します。
ファイルサイズ別ロールオーバー（Rollover by File Size）	ログ ファイルの最大ファイル サイズ。このサイズを超えるとそのファイルがアーカイブされ、新しいログ ファイルが作成されます。100 キロバイトから 10 ギガバイトまでの数値を入力してください。
時刻によりロールオーバー（Rollover by Time）	ログファイルの最大記録時間。この時間を超えるとそのファイルがアーカイブされ、新しいファイルが作成されます。設定可能なオプションは、以下のとおりです。 • **[なし（None）]**。AsyncOS は、ログファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。 • **[カスタム時間間隔（Custom Time Interval）]**。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。末尾に d、h、m、s を追加して、ロールオーバー間の日数、時間、分、秒を指定します。 • **[日次ロールオーバー（Daily Rollover）]**。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。1 日に複数の時刻を設定するには、カンマを使用して区切ります。1 時間ごとにロールオーバーを実行するように指定するには、時間にアスタリスク（*）を使用します。また、1 分ごとにロールオーバーするためにアスタリスクを使用することもできます。 • **[週次ロールオーバー（Weekly Rollover）]**。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。
ログ スタイル（Log Style） （アクセス ログ）	使用するログ形式（[Squid]、[Apache]、または [Squid の詳細（Squid Details）] のいずれか）を選択します。

オプション	説明

カスタム フィールド（Custom Fields）
（アクセス ログ）
	各アクセス ログ エントリにカスタム情報を含めることができます。
	[カスタム フィールド（Custom Fields）] にフォーマット指定子を入力する構文は以下のとおりです。
	`<format_specifier_1> <format_specifier_2> ...`
	例：`%a %b %E`
	フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。次に例を示します。
	`client_IP %a body_bytes %b error_type %E`
	この場合、`client_IP`はログ フォーマット指定子`%a`の説明トークンです（以下同様）。

ファイル名（File Name）	ログ ファイルの名前。最新のログ ファイルには拡張子 `.c` が付き、ロール オーバー済みのログには、ファイル作成時のタイムスタンプと拡張子 `.s` が付きます。
ログ フィールド（Log Fields） （W3C アクセス ログ）	W3C アクセス ログに含めるフィールドを選択できます。 [使用可能フィールド（Available Fields）] リストでフィールドを選択するか、[カスタム フィールド（Custom Field）] ボックスにフィールドを入力し、[追加（Add）] をクリックします。 [選択されたログ フィールド（Selected Log Fields）] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド（Selected Log Fields）] リストでフィールドを選択し、[削除（Remove）] をクリックして、それを削除できます [カスタム フィールド（Custom Field）] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加（Add）] をクリックする前に、各エントリが改行（Enter キーを押します）で区切られている必要があります。 W3C ログ サブスクリプションに含まれるログ フィールドを変更すると、ログ サブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。 W3C ログでは、ログ フィールド *c-ip*、*cs-username*、または *cs-auth-group* を必要に応じて匿名化できます。*c-ip*、*cs-username*、および *cs-auth-group* フィールドを匿名化するには、[匿名化（Anonymization）]チェックボックスをオンにします。チェックボックスをオンにすると、フィールド名は、それぞれ *c-a-ip*、*cs-a-username*、および *cs-a-auth-group* に変更されます。 **Note** ログ ファイルのプッシュ先である外部サーバが匿名化機能の処理に対応していない場合、匿名化を有効にしないでください。 ログの作成後、必要に応じて匿名化したフィールドを非匿名化することができます。W3C ログ フィールドの非匿名化, on page 18を参照してください

オプション	説明
匿名化のためのパスフレーズ（Passphrase for Anonymization） （W3C アクセス ログ）	フィールドの値を暗号化するためのパスフレーズを作成することができます。このエリアは、ログ フィールド *c-ip*、*cs-username*、または *cs-auth-group* を匿名化することを選択している場合のみ有効化されます。 **Note** システムは、匿名化のためのパスフレーズの設定中に、パスフレーズのルールを適用します。 パスフレーズを自動的に生成するには、[パスフレーズの自動生成（Auto Generate Passphrase）] の横のチェックボックスをオンにし、[生成する（Generate）] をクリックします。 **Note** 複数のアプライアンスがある場合は、すべてのアプライアンスに同じパスフレーズを設定する必要があります。
ログの圧縮（Log Compression）	ロール オーバー ファイルを圧縮するかどうかを指定します。AsyncOS は gzip 圧縮形式を使用してログ ファイルを圧縮します。
ログ除外（Log Exclusions）（オプション） （アクセス ログ）	HTTP ステータス コード（4xx または 5xx のみ）を指定して、関連するトランザクションをアクセス ログまたは W3C アクセス ログから除外します。 たとえば、401 を入力すると、そのトランザクション番号を持つ、認証に失敗した要求が除外されます。

オプション	説明
ログ レベル（Log Level）	ログ エントリの詳細のレベルを設定します。次から選択します。 • [クリティカル（Critical）]。エラーだけが記録されます。これは、最小限の設定であり、syslog レベルの [アラート（Alert）] と同等です。 • [警告（Warning）]。エラーと警告が記録されます。このログ レベルは、syslog レベルの [警告（Warning）] と同等です。 • [情報（Information）]。エラー、警告、および他のシステム操作が記録されます。これはデフォルトの詳細レベルであり、syslog レベルの [情報（Information）] と同等です。 • [デバッグ（Debug）]。システム問題のデバッグに役立つデータが記録されます。エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。 • [トレース（Trace）]。これは、詳細レベルの最も高い設定です。このレベルには、システム操作とアクティビティの完全な記録が含まれます。Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。 **Note** 詳細レベルの設定を高くするほど、作成されるログ ファイルが大きくなり、システム パフォーマンスに大きな影響を及ぼします。
取得方法（Retrieval Method）	ロール オーバー ログ ファイルを保存する場所と、閲覧用に取得する方法を指定します。 利用可能な方法の説明については、下記を参照してください。
取得方法： アプライアンス上の FTP（FTP on Appliance）	[アプライアンス上の FTP（FTP on Appliance）] 方式（FTP ポーリングと同等）では、ログ ファイルを取得するために、管理者ユーザまたはオペレータ ユーザのユーザ名とパスフレーズを使用して、リモート FTP クライアントからアプライアンスにアクセスする必要があります。 この方法を選択した場合、アプライアンスに保存するログ ファイルの最大数を入力する必要があります。最大数に達すると、最も古いファイルが削除されます。 これは、デフォルトの取得方法です。

オプション	説明
取得方法： リモートサーバでの FTP（FTP on Remote Server）	[リモート サーバでの FTP（FTP on Remote Server）] 方式（FTP プッシュと同等）では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。 この方法を選択した場合、以下の情報を入力する必要があります。 • FTP サーバのホスト名 • ログ ファイルを保存する FTP サーバのディレクトリ • FTP サーバに接続する権限を持つユーザのユーザ名とパスフレーズ **Note** AsyncOS for Web は、リモート FTP サーバのパッシブ モードのみをサポートします。アクティブ モードの FTP サーバにログ ファイルをプッシュできません。
取得方法： リモートサーバでの SCP（SCP on Remote Server）	[リモート サーバでの SCP（SCP on Remote Server）] 方式（SCP プッシュと同等）では、セキュア コピー プロトコルを使用して、リモート SCP サーバに定期的にログ ファイルをプッシュします。この方法には、SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、ユーザ名、SSH キー、およびリモート コンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。 この方法を選択した場合、以下の情報を入力する必要があります。 • SCP サーバのホスト名 • ログ ファイルを保存する SCP サーバのディレクトリ • SCP サーバに接続する権限を持つユーザのユーザ名 **Note** 現在は、非 FIPS モードの SSH-RSA と SSH-DSS、および FIPS モードの SSH-RSA のみがサポートされています。

オプション	説明
取得方法： Syslog 送信（Syslog Push）	テキスト ベースのログの syslog のみを選択できます。 [Syslog 送信（Syslog Push）] 方式では、ポート 514 でリモート Syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。 この方法を選択した場合、以下の情報を入力する必要があります。 • Syslog サーバのホスト名 • 転送に使用するプロトコル（UDP または TCP） • 最大メッセージ サイズ（Maximum message size） UDP で有効な値は 1024 ～ 9216 です。 TCP で有効な値は 1024 ～ 65535 です。 最大メッセージ サイズは syslog サーバの設定に応じて異なります。 • ログで使用するファシリティ

ステップ 4 変更を送信し、保存します。

What to do next

取得方法として SCP を選択した場合は、アプライアンスによって SSH キーが表示されます。このキーを SCP サーバ ホストに追加します。別のサーバへのログ ファイルのプッシュ, on page 19 を参照してください。

関連項目

• ログ ファイルのタイプ, on page 4
• ログのファイル名とアプライアンスのディレクトリ構造, on page 21

W3C ログ フィールドの非匿名化

ログ サブスクリプションの際にフィールド値（*c-ip*、*cs-username*、および *cs-auth-group*）の匿名化機能をイネーブルにしていた場合、送信先のログ サーバは、これらのログ フィールドについて、実際の値ではなく匿名化された値（*c-a-ip*、*cs-a-username*、および *cs-a-auth-group*）を受信します。実際の値を表示したい場合は、ログ フィールドを非匿名化する必要があります。

W3C ログのサブスクリプションを追加する際に匿名化されたログ フィールド値 *c-a-ip*、*cs-a-username*、および *cs-a-auth-group* は、非匿名化できます。

手順

ステップ 1 [システム管理（System Administration）]>[ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 匿名化されたフィールドを非匿名化したいログの [非匿名化（Deanonymization）] 列で、[非匿名化（Deanonymization）] をクリックします。

ステップ 3 [方法（Method）] エリアで、暗号化されたテキストを非匿名化のために入力する方法として、次のいずれかを選択します。

- 暗号化されたテキストを貼り付ける：[匿名化されたテキスト（Anonymized Text）] フィールドに暗号化されたテキストのみを貼り付けます。このフィールドには、最大 500 エントリを入力できます。複数のエントリはカンマで区切る必要があります。
- ファイルをアップロードする：暗号化されたテキストを含むファイルを選択します。ファイルには、最大 1000 エントリを含めることができます。ファイル形式は、CSV にする必要があります。システムは、フィールド区切り文字として、スペース、改行、タブ、およびセミコロンをサポートしています。

（注）
パスフレーズを変更した場合、それ以前のデータを非匿名化するには、以前のパスフレーズを入力する必要があります。

ステップ 4 [非匿名化（Deanonymization）] をクリックすると、非匿名化されたログ フィールド値が [非匿名化結果（Deanonymization Result）] テーブルに表示されます。

別のサーバへのログ ファイルのプッシュ

Before you begin

必要なログ サブスクリプションを作成または編集し、取得方法として SCP を選択します。 ログ サブスクリプションの追加および編集, on page 12

Procedure

ステップ 1 リモート システムにキーを追加します。

a) CLI にアクセスします。
b) `logconfig -> hostkeyconfig` コマンドを入力します。
c) 以下のコマンドを使用してキーを表示します。

コマンド	説明
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに記入される値です。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに記入される値です。

d) これらのキーをリモート システムに追加します。

ステップ 2 CLI で、リモート サーバの SSH 公開ホスト キーをアプライアンスに追加します。

コマンド	説明
New	新しいキーを追加します。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。

ステップ 3 変更を保存します。

ログ ファイルのアーカイブ

AsyncOS は、最新のログ ファイルがユーザー指定の上限（最大ファイル サイズまたは最大時間）に達すると、ログ サブスクリプションをアーカイブ（ロール オーバー）します。

ログ サブスクリプションには以下のアーカイブ設定が含まれます。

- ファイル サイズ別ロールオーバー
- 時刻によりロールオーバー
- ログの圧縮
- 取得方法

また、ログ ファイルを手動でアーカイブ（ロールオーバー）することもできます。

Procedure

ステップ 1 [システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 アーカイブするログ サブスクリプションの [ロールオーバー（Rollover）] 列のチェックボックスをオンにするか、[すべて（All）] をオンにしてすべてのサブスクリプションを選択します。

ステップ 3 [今すぐロールオーバー（Rollover Now）] をクリックして、選択したログをアーカイブします。

What to do next

関連項目

- ログ サブスクリプションの追加および編集, on page 12
- ログのファイル名とアプライアンスのディレクトリ構造, on page 21

ログのファイル名とアプライアンスのディレクトリ構造

アプライアンスは、ログサブスクリプション名に基づいてログサブスクリプションごとにディレクトリを作成します。ディレクトリ内のログ ファイル名は、以下の情報で構成されます。

- ログ サブスクリプションで指定されたログ ファイル名
- ログ ファイルが開始された時点のタイムスタンプ
- .c（「current（現在）」を表す）、または .s（「saved（保存済み）」を表す）のいずれかを示す単一文字ステータス コード

ログのファイル名は、以下の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

Note 保存済みのステータスのログ ファイルのみを転送する必要があります。

ログ ファイルの閲覧と解釈

Secure Web Applianceをモニタしてトラブルシューティングする手段として、現在のログ ファイルのアクティビティを確認できます。これを行うには、アプライアンスのインターフェイスを使用します。

また、過去のアクティビティの記録についてアーカイブ ファイルを閲覧することもできます。アーカイブ ファイルがアプライアンスに保存されている場合は、アプライアンスのインターフェイスから閲覧できます。それ以外の場合は、適切な方法で外部ストレージの場所から読み取る必要があります。

ログ ファイルの各情報項目は、フィールド変数によって示されます。どのフィールドがどの情報項目を表しているのかを判別することにより、フィールドの機能を調べて、ログ ファイルの内容を解釈できます。W3C 準拠のアクセス ログの場合は、ファイル ヘッダーに、ログに表示される順でフィールド名がリストされます。しかし、標準のアクセス ログの場合は、このログ タイプに関するドキュメントを参照して、フィールドの順序について調べる必要があります。

関連項目

- ログ ファイルの表示, on page 22。
- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- W3C アクセス ログの解釈, on page 48。
- トラフィック モニタ ログの解釈, on page 56。

- ログ ファイルのフィールドとタグ, on page 57。

ログ ファイルの表示

Before you begin

ここでは、アプライアンス上に保存されているログ ファイルの表示方法について説明します。外部に格納されているファイルの表示方法については、このマニュアルでは説明しません。

Procedure

ステップ 1 [システム管理（System Administration）]>[ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 ログ サブスクリプション リストの [ログ ファイル（Log Files）] 列にあるログ サブスクリプション名をクリックします。

ステップ 3 プロンプトが表示されたら、アプライアンスにアクセスするための管理者のユーザ名とパスフレーズを入力します。

ステップ 4 ログインしたら、ログ ファイルのいずれかをクリックして、ブラウザで表示するか、またはディスクに保存します。

ステップ 5 最新の結果を表示するには、ブラウザの表示を更新します。

Note
ログ サブスクリプションが圧縮されている場合は、ダウンロードし、復元してから開きます。

What to do next

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- W3C アクセス ログの解釈, on page 48。
- トラフィック モニタ ログの解釈, on page 56。

アクセス ログ ファイル内の Web プロキシ情報

アクセス ログ ファイルには、すべての Web プロキシ フィルタリングとスキャン アクティビティに関する記述が含まれています。アクセス ログ ファイル エントリは、アプライアンスが各トランザクションを処理した方法を表示します。

アクセス ログには 2 つの形式（標準および W3C 準拠）があります。W3C 準拠のログ ファイルは、標準のアクセス ログよりも記録内容とレイアウトをさらにカスタマイズできます。

以下のテキストは、1 つのトランザクションに対するアクセス ログ ファイル エントリの例を示します。

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">
 -
```

フォーマット指定子	フィールド値	フィールドの説明
%t	1278096903.150	UNIX エポック以降のタイムスタンプ。
%e	97	経過時間（遅延）（ミリ秒単位）。
%a	172.xx.xx.xx	クライアント IP アドレス。 **注**：advancedproxyconfig > authentication CLI コマンドを使用して、アクセス ログの IP アドレスをマスクするように選択できます。
%w	TCP_MISS	トランザクション結果コード。 詳細については、W3C 準拠のアクセス ログ ファイル, on page 48を参照してください。
%h	200	HTTP 応答コード。
%s	8187	応答サイズ（ヘッダー + 本文）。
%1r %2r	GET http://my.site.com/	要求の先頭行。 注：要求の先頭行がネイティブ FTP トランザクション用の場合、ファイル名の一部の特殊文字はアクセス ログでは符号化された URL を表します。たとえば、「@」記号は、アクセス ログに「%40」として書き込まれます。 以下の文字が符号化された URL に使用されます。 & # % + , : ; = @ ^ { } [ ]

フォーマット指定子	フィールド値	フィールドの説明
%A	–	認証されたユーザ名。 **注**：`advancedproxyconfig > authentication` CLI コマンドを使用して、アクセスログのユーザ名をマスクするように選択できます。
%H	`DIRECT`	要求コンテンツを取得するために接続されたサーバを説明するコード。 最も一般的な値は以下のとおりです。 • **NONE**。Web プロキシにコンテンツが含まれていたので、コンテンツを取得するために他のサーバに接続されませんでした。 • **DIRECT**。Web プロキシは、コンテンツを取得するための要求で指定されたサーバに移行しました。 • **DEFAULT_PARENT**。Web プロキシは、コンテンツを取得するためにプライマリペアレントプロキシまたは外部DLPサーバに移行しました。
%d	`my.site.com`	データ ソースまたはサーバの IP アドレス。
%c	`text/plain`	応答本文の MIME タイプ。

フォーマット指定子	フィールド値	フィールドの説明
%D	`DEFAULT_CASE_11`	ACL デシジョン タグ。 **注**：ACL デシジョン タグの末尾に、Webプロキシが内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。 詳細については、ACLデシジョン タグ, on page 28を参照してください。
N/A（ACL デシジョン タグの一部）	`PolicyGroupName`	このトランザクションについて最終決定を行うポリシー グループの名前（アクセス ポリシー、復号ポリシー、またはデータ セキュリティ ポリシー）。トランザクションがグローバル ポリシーに一致する場合、この値は「DefaultGroup」になります。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`ID（Identity）`	ID ポリシー グループの名前。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`OutboundMalwareScanningPolicy`	発信マルウェア スキャン ポリシー グループの名前。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。

フォーマット指定子	フィールド値	フィールドの説明
N/A（ACL デシジョン タグの一部）	`DataSecurityPolicy`	Cisco データ セキュリティ ポリシー グループの名前。トランザクションがグローバルな Cisco データ セキュリティ ポリシーに一致する場合、この値は「DefaultGroup」になります。このポリシー グループ名は、Cisco データ セキュリティ フィルタが有効な場合にのみ表示されます。データ セキュリティ ポリシーに一致しなかった場合は、「NONE」と表示されます。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`ExternalDLPPolicy`	外部 DLP ポリシー グループの名前。トランザクションがグローバル外部 DLP ポリシーに一致する場合、この値は「DefaultGroup」になります。外部 DLP ポリシーに一致しなかった場合は、「NONE」と表示されます。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`RoutingPolicy`	ルーティング ポリシー グループ名は *ProxyGroupName/ProxyServerName*。 トランザクションがグローバル ルーティング ポリシーに一致する場合、この値は「DefaultRouting」になります。アップストリーム プロキシ サーバを使用しない場合、この値は「DIRECT」になります。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。

フォーマット指定子	フィールド値	フィールドの説明
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,-,""-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	スキャン判定情報。アクセス ログでは、山カッコ内にさまざまなスキャンエンジンの判定情報が含まれています。 **Note** AsyncOS バージョン 11.8 以降では、URL カテゴリ識別子が二重引用符で囲まれて表示されます。たとえば、“IW_comp” と表示されます。 山カッコ内の値の詳細については、アクセス ログのスキャン判定エントリの解釈, on page 39およびマルウェア スキャンの判定値, on page 73を参照してください。
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?% < User-Agent:%!%-%	–	不審なユーザ エージェント。

トランザクション結果コード

アクセス ログ ファイルのトランザクション結果コードは、アプライアンスがクライアント要求を解決する方法を示します。たとえば、オブジェクトの要求がキャッシュから解決可能な場合、結果コードは TCP_HIT です。ただし、オブジェクトがキャッシュに存在せず、アプライアンスが元のサーバからオブジェクトをプルする場合、結果コードは TCP_MISS です。以下の表に、トランザクション結果コードを示します。

結果コード	説明
TCP_HIT	要求されたオブジェクトがディスク キャッシュから取得されました。
TCP_IMS_HIT	クライアントがオブジェクトの IMS（If-Modified-Since）要求を送信し、オブジェクトがキャッシュ内で見つかりました。プロキシは 304 応答を返します。
TCP_MEM_HIT	要求されたオブジェクトがメモリ キャッシュから取得されました。

結果コード	説明
TCP_MISS	オブジェクトがキャッシュ内で見つからなかったため、元のサーバから取得されました。
TCP_REFRESH_HIT	オブジェクトはキャッシュ内にありましたが、期限切れでした。プロキシが元のサーバにIMS（If-Modified-Since）要求を送信し、サーバはオブジェクトが変更されていないことを確認しました。そのため、アプライアンスはディスクまたはメモリ キャッシュのいずれかからオブジェクトを取得しました。
TCP_CLIENT_REFRESH_MISS	クライアントが「Pragma: no-cache」ヘッダーを発行して、「don't fetch response from cache」要求を送信しました。クライアントから送信されたこのヘッダーにより、アプライアンスは元のサーバからオブジェクトを取得しました。
TCP_DENIED	クライアント要求がアクセスポリシーによって拒否されました。
UDP_MISS	オブジェクトは発信サーバから取得されました。
NONE	トランザクションでエラーが発生しました。DNS 障害やゲートウェイのタイムアウトなど。

ACL デシジョン タグ

ACL デシジョン タグは、Web プロキシがトランザクションを処理した方法を示すアクセス ログ エントリのフィールドです。Web レピュテーション フィルタ、URL カテゴリ、およびスキャン エンジンの情報が含まれます。

Note ACL デシジョン タグの末尾に、Web プロキシがパフォーマンスを高めるために内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。

以下の表は、ACL デシジョン タグの値を示しています。

ACL デシジョン タグ	説明
ALLOW_ADMIN_ERROR_PAGE	Web プロキシが、通知ページとそのページで使用される任意のロゴへのトランザクションを許可しました。
ALLOW_CUSTOMCAT	Web プロキシが、アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションを許可しました。
ALLOW_REFERER	Web プロキシが、埋め込み/参照コンテンツの免除に基づいてトランザクションを許可しました。

ACL デシジョン タグ	説明
ALLOW_WBRS	Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションを許可しました。
AMP_FILE_VERDICT	ファイルに対する AMP レピュテーションサーバーからの判定を表す値です。 • 1：不明 • 2：正常 • 3：悪意がある • 4：スキャン不可

ACL デシジョン タグ	説明
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	

ACL デシジョン タグ	説明
	アーカイブ スキャンの判定 ARCHIVESCAN_ALLCLEAR：検査したアーカイブ内にブロックされたファイル タイプはありません。 ARCHIVESCAN_BLOCKEDFILETYPE：検査したアーカイブ内にブロックされたファイル タイプがふくまれています。ログ エントリ（[Verdict Detail]）の次のフィールドに、ブロックされたファイルのタイプ、ブロックされたファイルの名前などの詳細が示されています。 ARCHIVESCAN_NESTEDTOODEEP：アーカイブに設定された最大値を超える数の「カプセル化」されたアーカイブまたはネストされたアーカイブが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドに「UnScanable Archive-Blocked」が含まれています。 ARCHIVESCAN_UNKNOWNFMT－アーカイブに不明な形式のファイル タイプが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。 ARCHIVESCAN_UNSCANABLE：アーカイブにスキャンできないファイルが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。 ARCHIVESCAN_FILETOOBIG：アーカイブのサイズが設定された最大値を超えているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。 **アーカイブ スキャン判定の詳細** ログ エントリの [Verdict] フィールドの次のフィールドには、ブロックされたファイルのタイプやブロックされたファイルの名前、ブロックされたファイル タイプがアーカイブに含まれていないことを示す「UnScanable Archive-Blocked」や「-」など、判定に関する追加情報が示されています。 たとえば、検査可能なアーカイブ ファイルが「アクセス ポリシー：カスタム オブジェクト ブロック」の設定に基づいてブロックされている場合（ARCHIVESCAN_BLOCKEDFILETYPE）、[Verdict Detail] エントリにはブロックされたファイルのタイプ、およびブロックされたファイルの名前が含まれています。 アーカイブ検査の詳細については、アクセス ポリシー：オブジェクトのブロッキングおよびアーカイブ検査の設定を

ACL デシジョン タグ	説明
	参照してください。
BLOCK_ADC	アクセス ポリシー グループの設定されたアプリケーション設定に基づいてトランザクションがブロックされました。
BLOCK_ADMIN	アクセス ポリシー グループのデフォルト設定に基づいてトランザクションがブロックされました。
BLOCK_ADMIN_CONNECT	アクセス ポリシー グループの HTTP CONNECT ポート設定で定義された宛先の TCP ポートに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_CUSTOM_USER_AGENT	アクセス ポリシー グループの [ブロックするユーザエージェント（Block Custom User Agents）] 設定で定義されたユーザエージェントに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_TUNNELING	Web プロキシは、アクセス ポリシー グループの HTTP ポート上の非 HTTP トラフィックのトンネリングに基づいてトランザクションをブロックしました。
BLOCK_ADMIN_HTTPS_NonLocalDestination	トランザクションがブロックされました。クライアントは、SSL ポートを明示的なプロキシとして使用して認証をバイパスしようとしました。これを防ぐために、SSL 接続が Secure Web Appliance 自体に向けられている場合、実際の Secure Web Appliance リダイレクトホスト名への要求だけが許可されます。
BLOCK_ADMIN_IDS	データセキュリティ ポリシー グループで定義された要求本文のコンテンツの MIME タイプに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_FILE_TYPE	アクセス ポリシー グループで定義されたファイル タイプに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_PROTOCOL	アクセス ポリシー グループの [ブロックするプロトコル（Block Protocols）] 設定で定義されたプロトコルに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_SIZE	アクセス ポリシー グループの [オブジェクト サイズ（Object Size）] 設定で定義された応答のサイズに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_SIZE_IDS	データセキュリティ ポリシー グループで定義された要求本文のコンテンツのサイズに基づいてトランザクションがブロックされました。

ACL デシジョン タグ	説明
BLOCK_AMP_RESP	Web プロキシが、アクセスポリシーグループの Advanced Malware Protection 設定に基づいて応答をブロックしました。
BLOCK_AMW_REQ	Web プロキシが、発信マルウェア スキャン ポリシー グループの Anti-Malware 設定に基づいて要求をブロックしました。要求の本文はポジティブなマルウェアの判定を生成しました。
BLOCK_AMW_RESP	Web プロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいて応答をブロックしました。
BLOCK_AMW_REQ_URL	Web プロキシが HTTP 要求の URL が安全ではないと疑い、アクセス ポリシー グループの Anti-Malware 設定に基づいて要求時にトランザクションをブロックしました。
BLOCK_AVC	アクセス ポリシー グループの設定されたアプリケーション設定に基づいてトランザクションがブロックされました。
BLOCK_CONTENT_UNSAFE	アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツをブロックするように設定されています。
BLOCK_CONTINUE_CONTENT_UNSAFE	アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。
BLOCK_CONTINUE_CUSTOMCAT	[警告（Warn）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。
BLOCK_CONTINUE_WEBCAT	[警告（Warn）] に設定されているアクセス ポリシー グループの定義済み URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。
BLOCK_CUSTOMCAT	アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。

ACL デシジョン タグ	説明
BLOCK_ICAP	Web プロキシが、外部 DLP ポリシー グループで定義された外部 DLP システムの判定に基づいて要求をブロックしました。
BLOCK_SEARCH_UNSAFE	クライアント要求には危険な検索クエリーが含まれており、アクセス ポリシーは安全検索を実行するように設定されているので、元のクライアント要求がブロックされました。
BLOCK_SUSPECT_USER_AGENT	アクセス ポリシー グループの [疑わしいユーザエージェント（Suspect User Agent）] 設定に基づいてトランザクションがブロックされました。
BLOCK_UNSUPPORTED_SEARCH_APP	アクセス ポリシー グループの安全検索設定に基づいてトランザクションがブロックされました。トランザクションはサポートされない検索エンジンに対するものであり、ポリシーはサポートされない検索エンジンをブロックするように設定されています。
BLOCK_WBRS	アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションがブロックされました。
BLOCK_WBRS_IDS	Web プロキシが、Data Security ポリシー グループの Web レピュテーション フィルタ設定に基づいてアップロード要求をブロックしました。
BLOCK_WEBCAT	アクセス ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。
BLOCK_WEBCAT_IDS	Web プロキシが、Data Security ポリシー グループの URL カテゴリ フィルタリング設定に基づいてアップロード要求をブロックしました。
BLOCK_YTCAT	Web プロキシが、アクセスポリシーグループに事前設定された YouTube カテゴリのフィルタ処理設定に基づいてトランザクションをブロックしました。
BLOCK_CONTINUE_YTCAT	Web プロキシが、[警告（Warn）] に設定されているアクセスポリシーグループの定義済み YouTube カテゴリに基づいてトランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。
DECRYPT_ADMIN	Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションを復号しました。

ACL デシジョン タグ	説明
DECRYPT_ADMIN_EXPIRED_CERT	サーバ証明書が失効していますが、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	EUN が有効な場合の復号ポリシーグループのドロップ接続として、デフォルト設定に基づき、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_EXPIRED_CERT	HTTPS プロキシ設定が、EUN が有効になっている期限切れの証明書をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	HTTPS プロキシ設定が、EUN が有効になっている無効の証明書をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	HTTPS プロキシ設定が、EUN が有効になっている不一致のホスト名をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	HTTPS プロキシ設定が、EUN が有効になっているその他のエラーをもつ OSCP をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	HTTPS プロキシ設定が、EUN が有効になっている OSCP が失効した証明書をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	HTTPS プロキシ設定が、認識できないルート権限または EUN が有効になっている発行者の証明書をドロップすると、Web プロキシがトランザクションを復号しました。
DECRYPT_EUN_CUSTOMCAT	Web プロキシが、復号ポリシーグループの URL カテゴリフィルタリング設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。
DECRYPT_EUN_WBRS	Web プロキシが、復号ポリシーグループの Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。
DECRYPT_EUN_WBRS_NO_SCORE	Web プロキシが、復号ポリシーグループのスコアなし URL の Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。

ACL デシジョン タグ	説明
DECRYPT_EUN_WEBCAT	Web プロキシが、復号ポリシーグループの URL カテゴリフィルタリング設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。
DECRYPT_WEBCAT	Web プロキシが、復号ポリシー グループの URL カテゴリフィルタリング設定に基づいてトランザクションを復号しました。
DECRYPT_WBRS	Web プロキシが、復号ポリシーグループの Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。
DEFAULT_CASE	AsyncOS サービスが Web レピュテーションやアンチマルウェア スキャンなど、トランザクションで処理を行わなかったため、Web プロキシがクライアントにサーバへのアクセスを許可しました。
DENY_ADMIN	Webプロキシがトランザクションを拒否しました。これは、HTTPS 要求に関して、認証が必要が場合に、HTTPS プロキシ設定で [認証のための復号（Decrypt for Authentication）] が無効になっていると発生します。
DROP_ADMIN	Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションをドロップました。
DROP_ADMIN_EXPIRED_CERT	サーバ証明書が失効しているため、Web プロキシがトランザクションをドロップしました。
DROP_WEBCAT	Web プロキシが、復号ポリシー グループの URL カテゴリフィルタリング設定に基づいてトランザクションをドロップしました。
DROP_WBRS	Web プロキシが、復号ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをドロップしました。
MONITOR_ADC	Web プロキシが、アクセス ポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。
MONITOR_ADMIN_EXPIRED_CERT	サーバ証明書が失効しているため、Web プロキシがサーバ応答をモニタしました。
MONITOR_AMP_RESP	Web プロキシが、アクセスポリシーグループの Advanced Malware Protection 設定に基づいてサーバー応答をモニタしました。

ACL デシジョン タグ	説明
MONITOR_AMW_RESP	Webプロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいてサーバ応答をモニタしました。
MONITOR_AMW_RESP_URL	Webプロキシが HTTP 要求の URL が安全ではないと疑っていますが、アクセス ポリシー グループの Anti-Malware 設定に基づいてトランザクションをモニタしました。
MONITOR_AVC	Web プロキシが、アクセス ポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。
MONITOR_CONTINUE_CONTENT_UNSAFE	任意で、Web プロキシが、アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_CUSTOMCAT	当初、Web プロキシは、[警告（Warn）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_WEBCAT	当初、Web プロキシは、[警告（Warn）] に設定されているアクセス ポリシー グループの定義済み URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_YTCAT	当初、Web プロキシが、[警告（Warn）] に設定されたアクセスポリシーグループの定義済み YouTube カテゴリに基づいてトランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャンエンジンは要求をブロックしませんでした。

ACL デシジョン タグ	説明
MONITOR_IDS	Web プロキシが、データ セキュリティ ポリシーまたは外部 DLP ポリシーのいずれかを使用してアップロード要求をスキャンしましたが、要求をブロックしませんでした。Web プロキシは、アクセス ポリシーに対して要求を評価しました。
MONITOR_SUSPECT_USER_AGENT	Web プロキシが、アクセス ポリシー グループの Suspect User Agent 設定に基づいてトランザクションをモニタしました。
MONITOR_WBRS	Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをモニタしました。
NO_AUTHORIZATION	ユーザが、ある認証レルムに対して認証済みであったが、アプリケーション認証ポリシーに設定されている認証レルムに対して未認証であったため、Web プロキシはアプリケーションへのユーザ アクセスを許可しませんでした。
NO_PASSWORD	ユーザが認証に失敗しました。
PASSTHRU_ADMIN	Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションをパススルーました。
PASSTHRU_ADMIN_EXPIRED_CERT	サーバ証明書が失効していますが、Web プロキシがトランザクションをパススルーしました。
PASSTHRU_WEBCAT	Web プロキシが、復号ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションをパススルーしました。
PASSTHRU_WBRS	Web プロキシが、復号ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをパススルーしました。
REDIRECT_CUSTOMCAT	Web プロキシが、[リダイレクト（Redirect）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションを別の URL にリダイレクトしました。
SAAS_AUTH	ユーザが、アプリケーション認証ポリシーに設定されている認証レルムに対して透過的に認証されていたため、Web プロキシはそのユーザがアプリケーションにアクセスすることを許可しました。

ACL デシジョン タグ	説明
OTHER	認可の失敗、サーバの切断、クライアントによる中止などのエラーにより、Web プロキシが要求を完了できませんでした。

アクセス ログのスキャン判定エントリの解釈

アクセス ログ ファイル エントリは、URL フィルタリング、Web レピュテーション フィルタリング、アンチマルウェア スキャンなど、さまざまなスキャン エンジンの結果を集約して表示します。アプライアンスは、各アクセス ログ エントリの末尾の山カッコ内にこの情報を表示します。

以下のテキストは、アクセス ログ ファイル エントリからのスキャン判定情報です。この例では、Webroot スキャン エンジンがマルウェアを検出しました。

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",
-,-,
IW_infr,-,"Trojan Phisher","-","-","Unknown","Unknown","-","-",489.73,0,

[Local],"-","-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

Note すべてのアクセス ログ ファイル エントリの例については、アクセス ログ ファイル内の Web プロキシ情報, on page 22を参照してください。

この例の各要素は、以下の表に示すログ ファイル フォーマット指定子に対応しています。

位置	フィールド値	フォーマット指定子	説明
1	IW_infr	%XC	トランザクションに割り当てられたカスタム URL カテゴリ（省略形）。カテゴリが割り当てられない場合、このフィールドには「nc」が表示されます。

位置	フィールド値	フォーマット指定子	説明
2	ns	%XW	Web レピュテーション フィルタ スコア。このフィールドには、スコアの数値、「ns」（スコアがない場合）、または「dns」（DNS ルックアップ エラーがある場合）が表示されます。
3	24	%Xv	Webroot が DVS エンジンに渡したマルウェア スキャンの判定。Webroot でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値, on page 73を参照してください。
4	“Trojan-Phisher-Gamec”	“%Xn”	オブジェクトに関連付けられているスパイウェアの名前。Webroot でのみ検出された応答に適用します。
5	0	%Xt	マルウェアが存在する可能性を判断する脅威リスク比（TRR）に関連付けられた Webroot 固有の値。Webroot でのみ検出された応答に適用します。
6	354385	%Xs	Webroot が脅威識別子として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。
7	12559	%Xi	Webroot がトレース識別子として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。
8	-	%Xd	McAfee が DVS エンジンに渡したマルウェア スキャンの判定。McAfee でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値, on page 73を参照してください。

位置	フィールド値	フォーマット指定子	説明
9	"-"	"%Xe"	McAfee がスキャンしたファイルの名前。McAfee でのみ検出された応答に適用します。
10	-	%Xf	McAfee がスキャン エラーとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
11	-	%Xg	McAfee が検出タイプとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
12	-	%Xh	McAfee がウイルス タイプとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
13	"-"	"%Xj"	McAfee がスキャンしたウイルスの名前。McAfee でのみ検出された応答に適用します。
18	-	%XY	Sophos が DVS エンジンに渡したマルウェア スキャンの判定。Sophos でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値, on page 73を参照してください。
15	-	%Xx	Sophos がスキャン戻りコードとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。

位置	フィールド値	フォーマット指定子	説明
16	"-"	"%Xy"	Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。
17	"-"	"%Xz"	Sophos が脅威名として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。
18	-	%Xl	Cisco データ セキュリティ ポリシーの [コンテンツ（Content）] 列のアクションに基づく、Ciscoデータ セキュリティのスキャン判定。以下のリストは、このフィールドで使用できる値を示します。 • **0.** 許可（Allow） • **1.** ブロック（Block） • **-（ハイフン）** Cisco データ セキュリティ フィルタによるスキャンが開始されませんでした。この値は、Cisco データ キュリティ フィルタがディセーブルの場合、またはURL カテゴリ アクションが [許可（Allow）] に設定されている場合に表示されます。

位置	フィールド値	フォーマット指定子	説明
19	-	%Xp	ICAP応答で指定された結果に基づく外部DLPスキャンの評価。以下のリストは、このフィールドで使用できる値を示します。 • **0.** 許可（Allow） • **1.** ブロック（Block） • **-（ハイフン）**外部 DLP サーバによるスキャンが開始されませんでした。この値は、外部DLPスキャンがディセーブルの場合、または[外部 DLP ポリシー（External DLP Policies）] > [接続先（Destinations）]ページに除外URLカテゴリがあるため、コンテンツがスキャンされなかった場合に表示されます。
20	`IW_infr`	%XQ	要求側のスキャン時に決定された定義済みURLカテゴリの判定（省略形）。URLフィルタリングがディセーブルの場合、このフィールドにはハイフン（-）が表示されます。 **Note** AsyncOS バージョン 11.8 以降では、URLカテゴリ識別子が二重引用符で囲まれて表示されます。たとえば、”IW_infr” などです。 URL カテゴリの省略形の一覧については、URL カテゴリについてを参照してください。

位置	フィールド値	フォーマット指定子	説明
21	-	%XA	応答側のスキャン中に動的コンテンツ分析エンジンによって判定されたURLカテゴリの評価（省略形）。Cisco Web利用の制御のURLフィルタリングエンジンにのみ適用されます。動的コンテンツ分析エンジンがイネーブルになっており、要求時にカテゴリが割り当てられなかった場合にのみ適用されます（値「nc」が要求側のスキャン判定に表示されます）。 URLカテゴリの省略形の一覧については、URLカテゴリについてを参照してください。
22	"Trojan Phisher"	"%XZ"	どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェアカテゴリを提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。
23	"-"	"%Xk"	カテゴリ名または脅威タイプは、Webレピュテーションフィルタによって返されます。Webレピュテーションが高い場合はカテゴリ名が返され、レピュテーションが低い場合は脅威タイプが返されます。
24	"-"	%X#10#	Google翻訳エンジンの中にカプセル化されたURL。カプセル化されたURLがない場合、フィールド値は「-」になります。
25	"Unknown"	"%XO"	AVCまたはADCエンジンによって返されたアプリケーションの名前（該当する場合）。AVCまたはADCエンジンが有効な場合にのみ適用されます。
26	"Unknown"	"%Xu"	AVCまたはADCエンジンによって返されたアプリケーションのタイプ（該当する場合）。AVCまたはADCエンジンが有効な場合にのみ適用されます。

位置	フィールド値	フォーマット指定子	説明
27	"-" or "Unknown"	"%Xb"	AVC または ADC エンジンによって返されたアプリケーションの動作（該当する場合）。AVC または ADC エンジンが有効な場合にのみ適用されます。 AVC の場合は「_」、ADC の場合は「Unknown」です。
28	"-"	"%XS"	安全なブラウジング スキャンの判定。この値は、セーフ サーチ機能またはサイト コンテンツ レーティング機能がトランザクションに適用されたかどうかを示します。 可能な値のリストについては、アダルト コンテンツ アクセスのロギングを参照してください。
29	489.73	%XB	要求に対応するために使用された平均帯域幅（KB/秒）。
30	0	%XT	帯域幅制限の制御設定によって要求が絞り込まれたかどうかを示す値。「1」は要求が絞り込まれたことを示し、「0」は絞り込まれなかったことを示します。
31	[Local]	%l	要求を行なっているユーザのタイプ（[ローカル（Local)] または [リモート（Remote)]）。AnyConnect Secure Mobility がイネーブルの場合にのみ適用されます。イネーブルでない場合、値はハイフン（-）です。
32	"-"	"%X3"	どのスキャン エンジンがイネーブルになっているかに依存しない、統合された要求側アンチマルウェア スキャンの判定。発信マルウェア スキャン ポリシーが適用されるときに、クライアント要求のスキャンによってブロックまたはモニタされるトランザクションに適用されます。

位置	フィールド値	フォーマット指定子	説明
33	"-"	"%X4"	該当する発信マルウェア スキャン ポリシーによってブロックまたはモニタされるクライアント要求に割り当てられた脅威の名前。 この脅威の名前は、どのアンチマルウェア スキャン エンジンがイネーブルになっているかには依存しません。
34	37	%X#1#	Advanced Malware Protection ファイル スキャンからの判定： • 0：悪意のないファイル • 1：ファイル タイプが原因で、ファイルがスキャンされなかった • 2：ファイル スキャンがタイムアウト • 3：スキャン エラー • 3 よりも大きい値：悪意のあるファイル
35	"W32.CiscoTestVector"	%X#2#	Advanced Malware Protection ファイル スキャンで判定された脅威の名前。「-」は脅威がないことを示します。
36	33	%X#3#	Advanced Malware Protection ファイル スキャンのレピュテーション スコア。このスコアは、クラウド レピュテーション サービスがファイルを正常と判定できない場合にのみ使用されます。 詳細については、ファイル レピュテーション フィルタリングとファイル分析の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。 。

位置	フィールド値	フォーマット指定子	説明
37	0	%X#4#	アップロードおよび分析要求のインジケータ： 「0」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されなかったことを示します。 「1」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されたことを示します。
38	"WSA-INFECTED-FILE.pdf"	%X#5#	ダウンロードして分析するファイルの名前。
39	"fd5ef49d4213e05f448 f11ed9c98253d85829614fba 368a421d14e64c426da5e"	%X#6#	このファイルの SHA-256 ID。
40	ARCHIVESCAN_BLOCKEDFILETYPE	%X#8#	アーカイブ スキャン判定。
41	EXT_ARCHIVESCAN_VERDICT	%Xo	アーカイブ スキャン判定の詳細。検査可能なアーカイブファイルがアクセス ポリシーのカスタム オブジェクト ブロック設定に基づいてブロックされている場合（ARCHIVESCAN_BLOCKEDFILETYPE）、この判定の詳細のエントリには、ブロックされたファイルのタイプおよびブロックされたファイルの名前が含まれます。
54	EXT_ARCHIVESCAN_THREATDETAIL	%Xm	アーカイブスキャナによるファイル判定。
43	EXT_WTT_BEHAVIOR	%XU	Web タップ動作。
44	EXT_YTCAT	%X#29#	トランザクションに割り当てられた YouTube URL カテゴリ（省略形）。カテゴリが割り当てられない場合、このフィールドには「nc」が表示されます。

各フォーマット指定子の機能については、ログ ファイルのフィールドとタグ, on page 57を参照してください。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22

- アクセス ログのカスタマイズ, on page 50
- W3C 準拠のアクセス ログ ファイル, on page 48
- ログ ファイルの表示, on page 22
- ログ ファイルのフィールドとタグ, on page 57

W3C 準拠のアクセス ログ ファイル

Secure Web Applianceには、Web プロキシ トランザクション情報を記録する 2 つの異なるログ タイプ（アクセス ログと W3C 形式のアクセス ログ）が用意されています。W3C アクセス ログは World Wide Web コンソーシアム（W3C）準拠であり、W3C 拡張ログ ファイル（ELF）形式でトランザクション履歴を記録します。

- W3C フィールド タイプ, on page 48
- W3C アクセス ログの解釈, on page 48

W3C フィールド タイプ

W3C アクセス ログ サブスクリプションを定義する場合は、ACL デシジョン タグまたはクライアント IP アドレスなど、含めるログ フィールドを選択します。以下のいずれかのログ フィールドのタイプを含めることができます。

- **定義済み。**Web インターフェイスには、選択できるフィールドのリストが含まれています。
- **ユーザ定義。**定義済みリストに含まれていないログ フィールドを入力できます。

W3C アクセス ログの解釈

W3C アクセス ログを解釈するときは、以下のルールとガイドラインを考慮してください。

- 各 W3C アクセス ログ サブスクリプションに記録されるデータは、管理者が指定します。したがって、W3C アクセス ログには設定済みのフィールド形式がありません。
- W3C ログは自己記述型です。ファイル形式（フィールドのリスト）は、各ログ ファイルの先頭のヘッダーで定義されます。
- W3C アクセス ログのフィールドは空白で区切ります。
- フィールドに特定のエントリのデータが含まれていない場合、ログ ファイルには代わりにハイフン（-）が表示されます。
- W3C アクセス ログ ファイルの各行は、1 つのトランザクションに対応し、各行は改行シーケンスで終了します。

- W3C ログ ファイルのヘッダー, on page 49
- W3C フィールドのプレフィックス, on page 49

W3C ログ ファイルのヘッダー

各 W3C ログ ファイルには、ファイルの先頭にヘッダー テキストが含まれています。各行は、# 文字で始まり、ログ ファイルを作成した Secure Web Applianceに関する情報を提供します。W3C ログ ファイルのヘッダーには、ログ ファイルを自己記述型にするファイル形式（フィールドのリスト）が含まれています。

以下の表は、各 W3C ログ ファイルの先頭に配置されているヘッダー フィールドの説明です。

ヘッダー フィールド	説明
バージョン（Version）	使用される W3C の ELF 形式バージョン
日付（Date）	ヘッダー（およびログ ファイル）が作成された日時。
システム（System）	ログ ファイルを生成した Secure Web Appliance（「Management_IP - Management_hostname」形式）。
ソフトウェア（Software）	これらのログを生成したソフトウェア
フィールド（Fields）	ログに記録されたフィールド

W3C ログ ファイルの例：

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

W3C フィールドのプレフィックス

ほとんどの W3C ログ フィールドの名前には、クライアントやサーバなど、値を取得したヘッダーを識別するプレフィックスが含まれています。プレフィックスのないログ フィールドは、トランザクションに関与するコンピュータに関係ない値を参照します。以下の表は、W3C ログ フィールドのプレフィックスの説明です。

プレフィックスのヘッダー	説明
c	クライアント
s	サーバ
cs	クライアントからサーバへ

プレフィックスのヘッダー	説明
sc	サーバからクライアントへ
x	アプリケーション固有の識別子。

たとえば、W3C ログ フィールド「cs-method」は、クライアントからサーバに送信された要求のメソッドを示し、「c-ip」はクライアントの IP アドレスを示しています。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- アクセス ログのカスタマイズ, on page 50。
- トラフィック モニタのログ ファイル, on page 56。
- ログ ファイルのフィールドとタグ, on page 57。
- ログ ファイルの表示, on page 22。

アクセス ログのカスタマイズ

標準アクセス ログや W3C アクセス ログをカスタマイズしてさまざまな定義済みフィールドやユーザ定義フィールドを追加して、ネットワーク内の Web トラフィックに関する包括的な情報を取得できます。

関連項目

- 定義済みフィールドの一覧については、ログ ファイルのフィールドとタグ, on page 57を参照してください。
- ユーザ定義フィールドの詳細については、アクセス ログのユーザ定義フィールド, on page 50を参照してください。

アクセス ログのユーザ定義フィールド

定義済みのフィールドだけではアクセス ログや W3C ログに記録できない HTTP/HTTPS トランザクションのヘッダー情報がある場合は、カスタム ログ フィールドを追加できます。これを行うには、アクセス ログや W3C ログのサブスクリプションを設定するときに、[カスタム フィールド（Custom Fields）] テキスト ボックスにユーザ定義のログ フィールドを入力します。

カスタム ログ フィールドは、クライアントまたはサーバから送信される任意のヘッダーから任意のデータをとることができます。ログ サブスクリプションに追加されるヘッダーが要求または応答に含まれていない場合、ログ ファイルはログ フィールド値としてハイフンを使用します。

以下の表は、アクセス ログおよび W3C ログにカスタム フィールドを追加するときの構文を示しています。

ヘッダー タイプ	アクセス ログ フォーマット指定子の構文	W3C ログ カスタム フィールドの構文
クライアント アプリケーションからヘッダー	%<*ClientHeaderName* :	cs(*ClientHeaderName*)
サーバからヘッダー	%<*ServerHeaderName* :	sc(*ServerHeaderName*)

たとえば、クライアント要求の If-Modified-Since ヘッダー値のログを記録する場合、W3C ログ サブスクリプションの [カスタム フィールド（Custom Field）] ボックスに以下のテキストを入力します。

```
cs(If-Modified-Since)
```

関連項目

- 標準アクセス ログのカスタマイズ, on page 51。
- W3C アクセス ログのカスタマイズ, on page 52。

標準アクセス ログのカスタマイズ

Procedure

ステップ 1 [システム管理（System Administration）]>[ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 アクセス ログ サブスクリプションを編集するには、アクセス ログ ファイル名をクリックします。

ステップ 3 [カスタム フィールド（Custom Fields）] に、必要なフォーマット指定子を入力します。

[カスタム フィールド（Custom Fields）] にフォーマット指定子を入力する構文は以下のとおりです。

```
<format_specifier_1> <format_specifier_2> ...
```

例：`%a %b %E`

フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。次に例を示します。

```
client_IP %a body_bytes %b error_type %E
```

この場合、`client_IP` はログ フォーマット指定子 `%a` の説明トークンです（以下同様）。

Note
クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

ステップ 4 変更を送信し、保存します。

What to do next

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- ログ ファイルのフィールドとタグ, on page 57。
- アクセス ログのユーザ定義フィールド, on page 50。

W3C アクセス ログのカスタマイズ

Procedure

ステップ 1 [システム管理（System Administration）]>[ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 W3C ログ サブスクリプションを編集するには、W3C ログ ファイル名をクリックします。

ステップ 3 [カスタム フィールド（Custom Fields）] ボックスにフィールドを入力し、[追加（Add）] をクリックします。

[選択されたログ フィールド（Selected Log Fields）] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド（Selected Log Fields）] リストでフィールドを選択し、[削除（Remove）] をクリックして、それを削除できます

[カスタム フィールド（Custom Field）] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加（Add）] をクリックする前に、各エントリが改行（Enter キーを押します）で区切られている必要があります。

W3C ログ サブスクリプションに含まれるログ フィールドを変更すると、ログ サブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。

Note
クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

ステップ 4 変更を送信し、保存します。

What to do next

関連項目

- W3C 準拠のアクセス ログ ファイル, on page 48。
- ログ ファイルのフィールドとタグ, on page 57。
- アクセス ログのユーザ定義フィールド, on page 50。
- Cisco CTA 固有のカスタム W3C ログの設定, on page 52
- Cisco Cloudlock に固有のカスタム W3C ログの設定, on page 54

Cisco CTA 固有のカスタム W3C ログの設定

アプライアンスを、Cognitive Threat Analytics（CTA）（分析とレポートのための Cisco Cloud Web Security サービス固有のカスタム W3C アクセス ログ）を「プッシュ」するよう設定する

ことができます。Cisco ScanCenter は Cloud Web Security（CWS）の管理ポータルです。https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.htmlを参照してください

始める前に

自動アップロードプロトコルとして SCP（Secure Copy Protocol）を選択して、アプライアンス用の Cisco ScanCenter にデバイスのアカウントを作成します。『Cisco ScanCenter Administrator』の「Proxy Device Uploads」のセクションを参照してください（https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html）。

SCP のホスト名とアプライアンス用の生成されたユーザ名に注意してください。ユーザ名は大文字と小文字が区別され、デバイスごとに異なります。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Cisco Cognitive Threat Analytics] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [ログフィールド（Log Fields）]エリアに、必要に応じて追加のログフィールドを追加します。ログ サブスクリプションの追加および編集 （12 ページ）を参照してください。

ステップ 4 [選択されたログフィールド（Selected Log Fields）] で、c-ip、cs-username または cs-auth-group の横のチェック ボックスを、個別にこれらのフィールドを匿名化する場合は、オンにします。

また、[匿名化（Anonymization）] チェック ボックスをオンにして、これらのフィールドを同時に匿名化することもできます。ログ サブスクリプションの追加および編集 （12 ページ）を参照してください。

ステップ 5 [検索方法（Retrieval Method）] 領域に、Cisco ScanCenter のデバイス用に生成されたユーザ名を入力します。デバイス ユーザ名は大文字と小文字が区別され、プロキシ デバイスごとに異なります。

ステップ 6 必要に応じて、[詳細オプション（Advanced Options）] の値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

アプライアンスは公開 SSH キーを生成し、[Cisco Cognitive Threat Analytics] ページにそれらが表示されます。

ステップ 8 公開 SSH キーのいずれかをクリップボードにコピーします。

ステップ 9 [Cisco Cognitive Threat Analyticsの表示（View Cisco Cognitive Threat Analytics）] ポータル リンクをクリックして、Cisco ScanCenter ポータルに切り替えて、適切なデバイス アカウントを選択してから、公開 SSH キーを [CTAデバイスプロビジョニング（CTA Device Provisioning）] ページに貼り付けます。（『Cisco ScanCenter Administrator Guide』の「Proxy Device Uploads」のセクションを参照してください）。

プロキシ デバイスからのログ ファイルは、プロキシ デバイスと CTA システム間の正常な認証での分析のため CTA システムにアップロードされます。

ステップ 10 アプライアンスに戻って、変更を確定します。

[システム管理（System Administration）] > [ログサブスクリプション（Log Subscription）] を使用して、CTA W3C ログを追加することもできます。W3C アクセス ログのカスタマイズ （52 ページ）の手順に従って、新しい W3C アクセス ログ サブスクリプションを次のオプションを指定して追加します。

- ログ タイプとして [W3C ログ（W3C Logs）]
- サブスクリプションとして [Cisco Cognitive Threat Analyticsサブスクリプション（Cisco Cognitive Threat Analytics Subscription）] を選択
- ファイル転送タイプとして [SCP] を選択

カスタム フィールドの詳細については、ログ サブスクリプションの追加および編集 （12 ページ）を参照してください。

（注）
CTA ログ サブスクリプションをすでに設定している場合には、アプライアンスの [Cisco Cognitive Threat Analytics] ページで、ログの名前を *cta_log* に変更する必要があります。

ログを作成した後、CTA ログを削除する場合は、[Cisco Cognitive Threat Analytics] ページで [無効化（Disable）] をクリックします。CTA ログは [ログサブスクリプション（Log Subscriptions）] ページからも削除できます（[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）]）。

匿名の CTA 固有 W3C ログ フィールドを非匿名化するには、[Cisco Cognitive Threat Analytics] ページで [非匿名化（Cisco Cognitive Threat Analytics）] をクリックします。W3C ログ フィールドの非匿名化 （18 ページ）を参照してください

また、[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] を使用して、匿名の CTA 固有 W3C ログ フィールドを非匿名化することもできます。「W3C ログ フィールドの非匿名化 （18 ページ）」を参照してください。

Cisco Cloudlock に固有のカスタム W3C ログの設定

Cisco Cloudlock は、クラウド ネイティブ CASB およびサイバー セキュリティ プラットフォームであり、Software-as-a-Service、Platform-as-a-Service、および Infrastructure-as-a-Service の全体にわたってユーザ、データ、およびアプリケーションを保護します。シスコの Cloudlock ポータルに W3C アクセス ログをプッシュするようお使いのアプライアンスを設定し、分析とレポーティングに役立てることができます。これらのカスタム W3C ログを使用すると、顧客の SaaS 利用状況がさらに把握しやすくなります。

始める前に

お使いのアプライアンスの Cloudlock ポータルにデバイス アカウントを作成し、自動アップロード プロトコルとして SCP を選択します。

Cloudlock ポータルにログオンしてオンライン ヘルプにアクセスし、Cloudlock ポータルにデバイス アカウントを作成するための手順に従ってください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [Cisco Cloudlock] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

（注）
ログのフィールドは、[ログ フィールド（Log Fields）] エリアでデフォルトで選択されています。デフォルトで選択されている以外のログ フィールドをさらに追加することはできません。[ログ フィールド（Log Fields）] エリアに表示されているログ フィールドの順番を変えることは推奨されません。

Cloudlock ログ ファイルのログ フィールド（*c-ip*、*cs-username*、または *cs-auth-group*）を匿名化することはできません。

ステップ 3 [取得方法（Retrieval Method）] エリアで、次の情報を入力します。

- Cloudlock サーバのホスト名とポート番号
- ログ ファイルを保存する Cloudlock サーバのディレクトリ
- Cloudlock サーバに接続する権限を持つユーザのユーザ名

ステップ 4 必要に応じ、[詳細オプション（Advanced Options）] の値を変更します。

ステップ 5 [送信（Submit）] をクリックします。

アプライアンスによって公開 SSH キーが生成され、Cisco Cloudlock ページに表示されます。

ステップ 6 公開 SSH キーのいずれかをクリップボードにコピーします。

ステップ 7 [Cloudlockポータルの表示（View Cloudlock Portal）] リンクをクリックして、Cisco Cloudlock ポータルに切り替えます。適切なデバイス アカウントを選択し、公開 SSH キーを [Cloudlock設定（Cloudlock Setting）] ページに貼り付けます。

お使いのプロキシ デバイスと Cloudlock システムの間で認証が成功すると、プロキシ デバイスからのログ ファイルが、分析のため、Cloudlock システムにアップロードされます。

ステップ 8 アプライアンスに戻って、変更を確定します。

Cloudlock W3C ログの追加は、[システム管理（System Administration）] > [ログサブスクリプション（Log Subscription）] を使用して行うこともできますW3C アクセス ログのカスタマイズ （52 ページ）の手順に従って、新しい W3C アクセス ログ サブスクリプションを次のオプションを指定して追加します。

- ログ タイプとして [W3C ログ（W3C Logs）]
- サブスクリプションとして [Cisco Cloudlock] を選択
- ファイル転送タイプとして [SCP] を選択

カスタム フィールドの詳細については、ログ サブスクリプションの追加および編集 （12 ページ）を参照してください。

（注）
Cloudlock ログ サブスクリプションがすでに設定済みの場合、ログ名を **cloudlock_log** に変更し、それを、アプライアンスの Cisco Cloudlock ページにリストする必要があります。

ログの作成後に Coudlock ログを削除する場合は、Cisco Cloudlock ページで [無効（Disable）] をクリックします。Cloudlock ログの削除は、[ログサブスクリプション（Log Subscription）] ページ（[システム管理（System Administration）] > [ログサブスクリプション（Log subscriptions）]）から行うこともできます。

トラフィック モニタのログ ファイル

レイヤ 4 トラフィック モニター ログ ファイルには、レイヤ 4 モニタリング アクティビティの詳細が記録されます。レイヤ4 トラフィック モニタ ログ ファイルのエントリを表示して、ファイアウォール ブロック リストやファイアウォール許可リストのアップデートを追跡できます。

トラフィック モニタ ログの解釈

下記の例では、トラフィック モニタ ログに記録されるさまざまなタイプのエントリの意味について説明します。

例 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

この例では、一致する場所がブロック リストのファイアウォール エントリとなります。レイヤ 4 トラフィック モニタにより、アプライアンスを通過した DNS 要求に基づいて、ブロック リストのドメイン名への IP アドレスが検出されました。その後で、その IP アドレスがファイアウォールのブロック リストに追加されました。

例 2

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow
list.
```

この例では、一致が許可リストのファイアウォール エントリとなります。レイヤ4 トラフィック モニタによりドメイン名エントリが照合され、一致がアプライアンスの許可リストに追加されました。その後で、その IP アドレスがファイアウォールの許可リストに追加されました。

例 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

この例では、レイヤ 4 トラフィック モニタにより内部 IP アドレスとブロック リストに記載されている外部 IP アドレス間で渡されたデータ レコードが記録されています。この場合、レイヤ 4 トラフィック モニタは、「ブロック」ではなく「モニタ」に設定されています。

関連項目

- ログ ファイルの表示, on page 22

ログ ファイルのフィールドとタグ

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

ログ ファイルでは、各ログ ファイル エントリを構成している情報項目を表すために変数が使用されます。これらの変数は、アクセス ログではフォーマット指定子、W3C ログではログ フィールドと呼ばれ、各フォーマット指定子には対応するログ フィールドがあります。

アクセス ログにこれらの値を表示するよう設定する方法については、アクセス ログのカスタマイズ, on page 50、および ログ サブスクリプションの追加および編集, on page 12 のカスタム フィールドに関する情報を参照してください。

以下の表は、これらの変数に関する説明です。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:<A	AclTime	アクセス制御リストトランザクションにかかった合計時間を出力します。
%{	x-id-shared	Umbrella と共有する ID のステータスを出力します。 IDがトランザクションで共有されている場合、対応するフォーマッタの値は「ID_SHARED」です。それ以外の場合は、アクセスログに「-」が表示されます。
%[	x-spoofed-ip	プロキシ IP スプーフィングで使用される送信元 IP アドレス。
%)	x-proxy-instance-id	ハイパフォーマンスモードが有効になっている場合のプロキシのインスタンスID。それ以外の場合は、ハイフンをログに記録します。
%(	cs-domain-map	ドメインマップを使用して解決された解決済みのドメイン名。
%X#11#	ext_auth_sgt	ISE統合で使用されるセキュリティ グループ タグのカスタム フィールド パラメーター。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%$	cipher information	トランザクションの両方のレッグの暗号情報（クライアントプロキシ暗号情報 ## プロキシサーバ暗号情報）。この情報は「<ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code>」のようなシーケンスで示されます。
%:<l	x-p2s-first-byte-time	Webプロキシがサーバへの接続を開始した時点から最初にサーバに書き込みが行えるようになるまでの時間。Webプロキシが複数のサーバに接続してトランザクションを完了する必要がある場合、これらの時間の合計になります。
%:<a	x-p2p-auth-wait-time	Webプロキシが要求を送信後、Webプロキシの認証プロセスからの応答を受信する待機時間。
%:<b	x-p2s-body-time	ヘッダーの後、要求本文をサーバに書き込むまでの待機時間。
%:<d	x-p2p-dns-wait-time	Web プロキシが Web プロキシ DNS プロセスに DNS 要求を送信するのにかかった時間。
%:<h	x-p2s-header-time	最初のバイトの後、要求ヘッダーをサーバに書き込むまでの待機時間。
%:<r	x-p2p-reputation- wait-time	Web プロキシが要求を送信後、Web レピュテーションフィルタからの応答を受信する待機時間。
%:<s	x-p2p-asw-req- wait-time	Webプロキシが要求を送信後、Webプロキシのアンチス パイウェア プロセスからの判定を受信する待機時間。
%:>l	x-s2p-first-byte-time	サーバからの最初の応答バイトの待機時間
%:>a	x-p2p-auth-svc-time	Webプロキシの認証プロセスからの応答を受信する待機時間（Webプロキシが要求を送信するのに必要な時間を含む）。
%:>b	x-s2p-body-time	受信したヘッダーの後の完全な応答本文の待機時間
%:>c	x-p2p-fetch-time	Webプロキシがディスク キャッシュからの応答を読み取るのに必要な時間。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:>d	x-p2p-dns-svc-time	Web プロキシ DNS プロセスが Web プロキシに DNS 結果を返送するのにかかった時間。
%:>h	x-s2p-header-time	最初の応答バイト後のサーバ ヘッダーの待機時間
%:>g		SSL サーバ ハンドシェイク遅延の情報。
%o	-	消費された時間クォータ。
% O	-	消費されたボリュームクォータ。
%X#41#	x-bw-info	適用される帯域幅クォータ制御レベル、リクエストにマッピングされた帯域幅パイプ番号、設定された帯域幅クォータ制限、および使用される帯域幅クォータプロファイル（level-pipe_no-quota_limit-quota_profile）。
%:>r	x-p2p-reputation-svc- time	Web レピュテーション フィルタからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:>s	x-p2p-asw-req-svc- time	Web プロキシのアンチス パイウェア プロセスからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:1<	x-c2p-first-byte-time	新しいクライアント接続からの最初の要求バイトを待機する時間。
%:1>	x-p2c-first-byte-time	最初のバイトがクライアントに書き込まれるまでの待機時間。
%:A<	x-p2p-avc-svc-time	AVC プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:A>	x-p2p-avc-wait-time	Web プロキシが要求を送信後、AVC プロセスからの応答を受信する待機時間。
%:b<	x-c2p-body-time	クライアント本文全体を待機する時間。
%:b>	x-p2c-body-time	本文全体がクライアントに書き込まれるまでの待機時間。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:C<	x-p2p-dca-resp- svc-time	動的コンテンツ分析からの判定を受信する待機時間（Webプロキシが要求を送信するのに必要な時間を含む）。
%:C>	x-p2p-dca-resp- wait-time	Webプロキシが要求を送信後、動的コンテンツ分析からの応答を受信する待機時間。
%:h<	x-c2p-header-time	最初のバイトの後の完全なクライアントヘッダーの待機時間
%:h>	x-p2c-header-time	クライアントに書き込まれる完全なヘッダーの待機時間
%:m<	x-p2p-mcafee-resp- svc-time	McAfee スキャン エンジンからの判定を受信する待機時間（Webプロキシが要求を送信するのに必要な時間を含む）。
%:m>	x-p2p-mcafee-resp- wait-time	Web プロキシが要求を送信後、McAfee スキャン エンジンからの応答を受信する待機時間。
%:p<	x-p2p-sophos-resp- svc-time	Sophos スキャン エンジンからの判定を受信する待機時間（Webプロキシが要求を送信するのに必要な時間を含む）。
%:p>	x-p2p-sophos-resp- wait-time	Web プロキシが要求を送信後、Sophos スキャン エンジンからの応答を受信する待機時間。
%:w<	x-p2p-webroot-resp -svc-time	Webroot スキャン エンジンからの判定を受信する待機時間（Webプロキシが要求を送信するのに必要な時間を含む）。
%:w>	x-p2p-webroot-resp-wait- time	Web プロキシが要求を送信後、Webroot スキャン エンジンからの応答を受信する待機時間。
%BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent%!%-%	x-suspect-user-agent	不審なユーザ エージェント（該当する場合）。ユーザ エージェントが疑わしい Web プロキシが判定した場合、このフィールドにそのユーザエージェントを記録します。それ以外の場合、ハイフンが表示されます。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%<Referer:	cs(Referer)	Referer ヘッダー
%>Server:	sc(Server)	応答の Server ヘッダー

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%a	c-ip	クライアント IP アドレス。
%A	cs-username	認証されたユーザ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%b	sc-body-size	本文のコンテンツ用に Web プロキシからクライアントに送信されたバイト数。
%B	bytes	使用された合計バイト数（要求サイズ+応答サイズ、つまり %q + %s）。
%c	cs-mime-type	応答本文の MIME タイプ。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%C	cs(Cookie)	Cookie ヘッダー。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%d	s-hostname	データ ソースまたはサーバの IP アドレス。
%]	x-http-rewrite-profile-name	HTTP ヘッダー書き換えプロファイル名。
%D	x-acltag	ACL デシジョン タグ。
%e	x-elapsed-time	ミリ秒単位の経過時間。 TCP トラフィックの場合、HTTP 接続の開始から完了までの経過時間です。 UDP トラフィックの場合、最初のデータグラムを送信してから、最後のデータグラムが許可される時間までの経過時間です。UDP トラフィックの経過時間が大きいと、タイムアウト値が大きくなる可能性があり、存続時間の長い UDP アソシエーションの許容データグラムが必要以上に長く許可される可能性があります。
%E	x-error-code	カスタマーサポートが失敗したトランザクションの原因をトラブルシューティングするのに役立つエラー コード番号。
%f	cs(X-Forwarded-For)	X-Forwarded-For ヘッダー
%F	c-port	クライアントの送信元ポート

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%g	cs-auth-group	承認されたグループ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドは、ユーザが適切なグループまたはポリシーに一致しているかどうかを判断する、認証問題のトラブルシューティングに使用されます。
%G		人間が読み取れる形式のタイムスタンプ。
%h	sc-http-status	HTTP 応答コード。
%H	s-hierarchy	階層の取得。
%i	x-icap-server	要求の処理中に接続した最後の ICAP サーバの IP アドレス。
%I	x-transaction-id	トランザクション ID。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%j	DCF	

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
		応答コードをキャッシュしません（DCF フラグ）。 応答コードの説明： • クライアント要求に基づく応答コード： • 1 = 要求に「no-cache」ヘッダーがあった。 • 2 = 要求に対してキャッシングが許可されていない。 • 4 = 要求に「Variant」ヘッダーがない。 • 8 = ユーザ要求にユーザ名またはパスフレーズが必要。 • 20 = 指定された HTTP メソッドへの応答。 • アプライアンスで受信された応答に基づく応答コード： • id="li_7443F05D141F4D9FB788FD416697DB65"> 40 =応答に「Cache-Control: private」ヘッダーが含まれている。 • 80 =応答に「Cache-Control: no-store」ヘッダーが含まれている。 • 100 = 応答は、要求がクエリーだったことを示している。 • 200 = 応答に含まれている「有効期限」の値が小さい（期限切れ間近）。 • 400 =応答に「Last Modified」ヘッダーがない。 • 1000 =応答がただちに期限切れになる。 • 2000 =応答ファイルが大きすぎてキャッシュできない。 • 20000 =ファイルの新しいコピーがある。 • 40000 = 応答の「Vary」ヘッダーに不正/無効な値がある。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
		• 80000 = 応答には Cookie の設定が必要。 • 100000 = キャッシュ不可の HTTP ステータス コード。 • 200000 = アプライアンスが受信したオブジェクトが不完全（サイズに基づく）。 • 800000 = 応答トレーラがキャッシュなしを示している。 • 1000000 = 応答のリライトが必要。
%k	s-ip	データ ソースの IP アドレス（サーバの IP アドレス） この値は、ネットワーク上の侵入検知デバイスによって IP アドレスがフラグ付けされたときに、要求元を決定するのに使用されます。これにより、フラグ付けされた IP アドレスを参照したクライアントの検索が可能になります。
%l	user-type	ユーザのタイプ（ローカルまたはリモート）。
%L	x-local_time	人間が読み取れる形式の要求のローカル時刻：DD/MMM/YYYY : hh:mm:ss +nnnn。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドを有効にすると、各ログ エントリのエポック タイムからローカル タイムを計算せずにログを問題に関連付けることができます。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%m	cs-auth-mechanism	認証問題をトラブルシューティングするのに使用されます。 トランザクションで使用する認証メカニズム。値は以下のとおりです。 • **BASIC**。ユーザ名が基本認証方式を使用して認証されました。 • **NTLMSSP**。ユーザ名が NTLMSSP 認証方式を使用して認証されました。 • **NEGOTIATE**。ユーザ名は Kerberos 認証方式を使用して認証されました。 • **SSO_TUI**。クライアント IP アドレスと透過的ユーザ ID を使用して認証されたユーザ名を照合することによって、ユーザ名が取得されました。 • **SSO_ISE**。ユーザは ISE サーバによって認証されました（ISE 認証のフォールバック メカニズムとして選択されている場合、ログには GUEST と表示されます）。 • **SSO_ASA**。ユーザがリモートユーザで、ユーザ名はセキュア モビリティを使用して Cisco ASA から取得されました。 • **FORM_AUTH**。アプリケーションへのアクセス時に、ユーザが Web ブラウザのフォームに認証クレデンシャルを入力しました。 • **GUEST**。ユーザが認証に失敗し、代わりにゲスト アクセスが許可されました。
%M	CMF	キャッシュ ミス フラグ（CMF フラグ）。
%N	s-computerName	サーバ名または宛先ホスト名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%p	s-port	宛先ポート番号。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%P	cs-version	使用されるプロトコル。値は以下のとおりです。 • 0 = プロトコルの使用なし • 1 = HTTP • 2 = HTTPS • 3 = FTP over HTTP • 4 = FTP • 5 = SOCKS • 6 = HTTP2
%q	cs-bytes	要求サイズ（ヘッダー + 本文）。
%r	x-req-first-line	要求の先頭行：要求方法（URI）。
%s	sc-bytes	応答サイズ（ヘッダー + 本文）。
%t	timestamp	UNIX エポックのタイムスタンプ **注**：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アクセスログを解析する場合は、timestamp フィールドを含める必要があります。ほとんどのログアナライザは、このフィールドで提供される形式の時間のみ認識します。
%u	cs(User-Agent)	ユーザエージェント。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドは、アプリケーションが認証に失敗しているかどうか、および/または別のアクセス権限が必要かどうかを判断するのに役立ちます。
%U	cs-uri	要求 URI。
%v	date	YYYY-MM-DD 形式の日付。
%V	時刻	HH:MM:SS 形式の時刻。
%w	sc-result-code	結果コード。例：TCP_MISS、TCP_HIT。
%W	sc-result-code-denial	結果コードの拒否。
%x	x-latency	待ち時間。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%X0	x-resp-dvs-scanverdict	どのスキャン エンジンがイネーブルになっているかに関係なく、マルウェア カテゴリ番号を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%X1	x-resp-dvs-threat-name	どのスキャン エンジンがイネーブルになっているかに関係なく、マルウェア脅威の名前を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%X2	x-req-dvs-scanverdict	要求側 DVS スキャンの判定
%X3	x-req-dvs-verdictname	要求側 DVS 判定の名前
%X4	x-req-dvs-threat-name	要求側 DVS 脅威の名前
%X6	x-as-malware-threat-name	マルウェア対策スキャン エンジンを起動することなく、適応型スキャンによってトランザクションがブロックされたかどうかを示します。設定可能な値は次のとおりです。 • **1.** トランザクションがブロックされました。 • **0.** トランザクションはブロックされませんでした。 この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。
%XA	x-webcat-resp-code- abbr	応答側のスキャン中に判定された URL カテゴリの評価（省略形）。Cisco Web 利用の制御の URL フィルタリング エンジンにのみ適用されます。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%Xb	x-avc-behavior	AVC または ADC エンジンによって識別される Web アプリケーションの動作。
%XB	x-avg-bw	帯域幅制限が AVC エンジンで定義されている場合、ユーザの平均帯域幅。
%XC	x-webcat-code-abbr	トランザクションに割り当てられたカスタムURL カテゴリの URL カテゴリの省略形。
%Xd	x-mcafee-scanverdict	McAfee 固有の ID：（スキャン判定）。
%Xe	x-mcafee-filename	McAfee固有のID：（判定を生成するファイル名）このフィールドは二重引用符付きでアクセス ログに書き込まれます。
%Xf	x-mcafee-av-scanerror	McAfee 固有の ID：（スキャン エラー）。
%XF	x-webcat-code-full	トランザクションに割り当てられた URL カテゴリの完全名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%Xg	x-mcafee-av-detecttype	McAfee 固有の ID：（検出タイプ）。
%XG	x-avc-reqhead-scanverdict	AVC 要求ヘッダーの判定。
%Xh	x-mcafee-av-virustype	McAfee 固有の ID：（ウイルス タイプ）。
%XH	x-avc-reqbody- scanverdict	AVC 要求本文の判定。
%Xi	x-webroot-trace-id	Webroot 固有のスキャン識別子：（トレース ID）
%Xj	x-mcafee-virus-name	McAfee 固有の ID：（ウイルス名）このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%Xk	x-wbrs-threat-type	Web レピュテーションの脅威タイプ。
%XK	x-wbrs-threat-reason	Web レピュテーションの脅威の理由。
%Xl	x-ids-verdict	Cisco データ セキュリティ ポリシーのスキャン判定。このフィールドが含まれている場合はIDS判定が表示されます。IDS がアクティブでドキュメントが「正常」とスキャン判定された場合は「0」、要求に対する IDS ポリシーがアクティブでない場合は「-」が表示されます。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%XL	x-webcat-resp-code- full	応答側のスキャン中に判定された URL カテゴリの評価（完全名）。Cisco Web 利用の制御の URL フィルタリング エンジンにのみ適用されます。
%XM	x-avc-resphead- scanverdict	AVC 応答ヘッダーの判定。
%Xn	x-webroot-threat-name	Webroot 固有の ID：（脅威の名前）このフィールドは二重引用符付きでアクセス ログに書き込まれます。
%XN	x-avc-reqbody-scanverdict	AVC 応答本文の判定。
%XO	xAPP	AVC または ADC エンジンによって識別される Web アプリケーションタイプ。
%Xp	x-icap-verdict	外部 DLP サーバのスキャン判定。
%XP	x-acl-added-headers	認識されないヘッダー。クライアント要求の追加ヘッダーのログを記録するには、このフィールドを使用します。クライアント要求を認証してリダイレクトする方法として要求にヘッダーを追加する、特殊なシステム（YouTube for Schools など）のトラブルシューティングをサポートします。
%XQ	x-webcat-req-code- abbr	要求側のスキャン時に決定された定義済み URL カテゴリの判定（省略形）。
%Xr	x-result-code	スキャン判定情報。
%XR	x-webcat-req-code-full	要求側のスキャン中に判定された URL カテゴリの評価（完全名）。
%Xs	x-webroot-spyid	Webroot 固有の ID：（スパイ ID）。
%XS	x-request-rewrite	安全なブラウジング スキャンの判定。 セーフ サーチ機能またはサイト コンテンツ レーティング機能がトランザクションに適用されたかどうかを示します。
%Xt	x-webroot-trr	Webroot 固有の ID：（脅威リスク比率（TRR））。
%XT	x-bw-throttled	帯域幅制限がトランザクションに適用されたかどうかを示すフラグ。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%Xu	xAPP タイプ	AVC または ADC エンジンによって識別される Web アプリケーション。
%Xv	x-webroot-scanverdict	Webroot からのマルウェア スキャンの判定。
%XV	x-request-source-ip	Web プロキシ設定で、[X-Forwarded-For を使用したクライアント IP アドレスの識別を有効にする（Enable Identification of Client IP Addresses using X-Forwarded-For）] チェックボックスをオンにした場合のダウンストリーム IP アドレス。
%XW	x-wbrs-score	復号された WBRS スコア <-10.0-10.0>。
%Xx	x-sophos-scanerror	Sophos 固有の ID：（スキャンの戻りコード）。
%Xy	x-sophos-file-name	Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。
%XY	x-sophos-scanverdict	Sophos 固有の ID：（スキャン判定）。
%Xz	x-sophos-virus-name	Sophos 固有の ID：（脅威の名前）。
%XZ	x-resp-dvs-verdictname	どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェア カテゴリを提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%X#1#	x-amp-verdict	Advanced Malware Protection ファイルスキャンからの判定： • 0：悪意のないファイル。 • 1：ファイル タイプが原因で、ファイルがスキャンされなかった。 • 2：ファイル スキャンがタイムアウト。 • 3：スキャン エラー。 • 3 よりも大きい値：悪意のあるファイル。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%X#2#	x-amp-malware-name	Advanced Malware Protection ファイルスキャンで判定された脅威の名前。「-」は脅威がないことを示します。
%X#3#	x-amp-score	Advanced Malware Protection ファイルスキャンのレピュテーションスコア。 このスコアは、クラウド レピュテーション サービスがファイルを正常と判定できない場合にのみ使用されます。 詳細については、ファイル レピュテーション フィルタリングとファイル分析の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。
%X#4#	x-amp-upload	アップロードおよび分析要求のインジケータ： 「0」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されなかったことを示します。 「1」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されたことを示します。
%X#5#	x-amp-filename	ダウンロードして分析するファイルの名前。
%X#6#	x-amp-sha	このファイルの SHA-256 ID。
%y	cs-method	方式。
%Y	cs-url	URL 全体。
%:>A	x-p2p-adc-svc-time	ADC プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:a>	x-p2p-adc-wait-time	Web プロキシが要求を送信後、ADC プロセスからの応答を受信する待機時間。
%:e<	x-p2p-amp-svc-time	AMP スキャンエンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:e>	x-p2p-amp-wait-time	Web プロキシが要求を送信後、 AMP スキャンエンジンからの応答を受信する待機時間。
該当なし	x-hierarchy-origin	要求コンテンツを取得するために接続したサーバを示すコード（DIRECT/www.example.com など）。
該当なし	x-resultcode-httpstatus	結果コードおよびHTTP 応答コード（間をスラッシュ（/）で区切ります）。
該当なし	x-archivescan-verdict	アーカイブ検査の判定を表示します。
該当なし	x-archivescan-verdict- reason	アーカイブ スキャンでブロックされるファイルの詳細。
%XU	該当なし	将来のために予約済み。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- W3C アクセス ログの解釈, on page 48。

マルウェア スキャンの判定値

マルウェア スキャンの判定は、マルウェアを含む可能性を判別する、URL 要求またはサーバ応答に割り当てられた値です。Webroot、McAfee、および Sophos のスキャン エンジンは、マルウェア スキャンの判定を DVS エンジンに返し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。特定のアクセス ポリシーに対するアンチマルウェア設定を編集した場合、各マルウェア スキャンの判定は、[アクセス ポリシー（Access Policies）] > [レピュテーションおよびマルウェア対策設定（Reputation and Anti-Malware Settings）] ページにリストされているマルウェア カテゴリに対応します。

以下のリストは、さまざまなマルウェア スキャンの判定値および対応するマルウェア カテゴリを示しています。

マルウェア スキャンの判定値	マルウェア カテゴリ
-	設定しない
0	不明
1	スキャンしない
2	タイムアウト

マルウェア スキャンの判定値	マルウェア カテゴリ
3	エラー
4	スキャン不可
10	一般的なスパイウェア
12	ブラウザ ヘルパー オブジェクト
13	アドウェア
14	システム モニタ
18	商用システム モニタ
19	ダイヤラ
20	ハイジャッカー
21	フィッシング URL
22	トロイのダウンローダ
23	トロイの木馬
24	トロイのフィッシャ
25	ワーム
26	暗号化ファイル
27	ウィルス
33	その他のマルウェア
34	PUA
35	中断
36	アウトブレイク ヒューリスティック
37	既知の悪意のある高リスク ファイル

関連項目

- アクセス ログ ファイル内の Web プロキシ情報, on page 22。
- W3C アクセス ログの解釈, on page 48。

ロギングのトラブルシューティング

トラブルシューティング

この章で説明する内容は、次のとおりです。

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, on page 57 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, on page 50 および ログ サブスクリプションの追加および編集, on page 12 を参照してください。

FIPS モードの問題

Secure Web Applianceを AsyncOS 10.5 にアップグレードして、FIPS モードおよび CSP 暗号化をイネーブルにした後に、暗号化と証明書に関する問題が発生した場合は、次の項目を確認してください。

CSP 暗号化

FIPS モードの CSP 暗号化がイネーブルになる前に動作していた機能が、暗号化がイネーブルになった後に動作しなくなった場合は、CSP 暗号化に問題があるかどうかを判別します。CSP 暗号化および FIPS モードをディセーブルにして、機能をテストします。動作する場合は、FIPS モードをイネーブルにして再びテストします。動作する場合は、CSP 暗号化をイネーブルにして再びテストします。「FIPS モードの有効化または無効化」を参照してください。

証明書の検証

AsyncOS 10.5 にアップグレードする前に Secure Web Applianceで受け入れられた証明書は、再アップロードしたときに、アップロード方法に関係なく拒否される可能性があります。（つまり、[HTTPS プロキシ（HTTPS Proxy）]、[証明書管理（Certificate Management）]、[SaaS のアイデンティティプロバイダ（Identity Provider for SaaS）]、ISE 設定、認証設定などの UI ページを使用した場合も、`certconfig` CLI コマンドを使用した場合も）拒否されることがあります。

証明書の署名者 CA が「カスタムの信頼できる証明機関」として [証明書の管理（Certificate Management）] ページ（[ネットワーク（Network）] > [証明書管理（Certificate Management）]）

ページで追加されていることを確認してください。証明書パス全体を信頼することができない場合は、証明書を Secure Web Applianceにアップロードできません。

また、古い設定をリロードすると、含まれている証明書が信頼されなくなって、リロードに失敗することがあります。保存された設定をロードする間に、これらの証明書を置き換えてください。

（注） すべての証明書検証エラーは、監査ログ（`/data/pub/audit_logs/audit_log.current`）に記録されます。

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

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、 Secure Web Appliance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、これらのユーザーエージェントの認証をバイパスします。「問題のあるユーザー エージェントの認証のバイパス」を参照してください。

LDAP に関する問題

NTLMSSP に起因する LDAP ユーザーの認証の失敗

LDAP サーバーは 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、ユーザーの認証に失敗します。

- ユーザーが 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。
- ユーザーが 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 サーバーを使用している。
- Active Directory サーバーが別の認証サーバーへの LDAP 参照を使用している。
- 参照された認証サーバが Secure Web Appliance 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 サーバー（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

関連する問題

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ーがクレデンシャルを要求される, on page 79

エラーによりユーザーがクレデンシャルを要求される

Secure Web Appliance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ー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、ユーザー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 Secure Web Appliance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）。

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, on page 79
• 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 のアップデートがブロックされる, on page 79

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 のアップデートがブロックされる

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 Secure Web Applianceを設定すると、Windows OneCare のアップデートがブロックされます。

ブラウザに関する問題

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 Secure Web Appliance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。

Procedure

ステップ 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。

ステップ 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 サーバー ポートとしてポート 80 を使用します。

ステップ 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。

ステップ 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 サーバー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。

フェールオーバーの問題

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、複数のプライマリアプライアンスをもたらしたり、その他のフェールオーバーの問題が発生したりす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。

例：

```
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: PRIMARY
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。

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。

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, on page 82
- 大規模 FTP 転送の切断, on page 82
- ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される, on page 82
- Chrome ブラウザが FTP-over-HTTP 要求でユーザー エージェントとして検出されない, on page 82
- 以下の項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, on page 104
  - HTTPS 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, on page 95

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 サーバー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ーである場合でも、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 サーバー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 サーバーにゼロ 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 サーバー上にゼロ バイト ファイルを作成します。

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

FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー 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

Secure Web Applianceは、数千ものクライアントとサーバーの接続を並行して処理するように設計されています。また、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、 Secure Web Appliance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 Secure Web Appliance を通じて 100 MB のファイルをダウンロードすると、サーバー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、Secure Web Appliance CLI コマンドを参照してください。

Caution 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。

自動送受信バッファは、networktuningによってデフォルトで有効になっていますが、他のネットワーク チューニング パラメータは変更できます。送信バッファと受信バッファに高い値を設定すると、高負荷シナリオで不安定になる可能性があることに注意してください。Cisco Secure Web Appliance は、アプライアンスの推奨 RPS の範囲内で、大きなファイルのダウンロードの最大 10% を処理できます。

メモリ負荷が原因で Cisco Secure Web Appliance が不安定になっていることに気付いた場合は、CLI から networktuning コマンドを使用して、自動送受信バッファを無効にできます。この調整により、低速のダウンロード速度で多数の並列ダウンロードがサポートされます。

networktuning コマンドの使用例を以下に示します。デフォルトの mbuf クラスタ値は、SWA モデルに基づいて設定されます。

```
networktuning
sendspace = 8192-2097152
recvspace = 8192-2097152
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 clusters = 252470-1000000
sendbuf-max = 2097152
recvbuf-max = 2097152
```

質問

これらのパラメータは何ですか。

Secure Web Appliance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）。

これらの例の値はどのように決定されましたか。

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。

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

重要x80 または x90 アプライアンスの電源を再投入する場合は、アプライアンスが起動するまで（すべての LED が緑色になるまで）少なくとも 20 分間待ってから、電源ボタンを押してください。

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/背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の説明については、『Cisco x90 Series Content Security Appliances *Installation and Maintenance Guide*』など、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html [英語] から入手可能なハードウェア 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ハードウェアでバッテリ再学習タイムアウト（RAIDイベント）（Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware）

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/証明書に関する問題

• HTTPS 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, on page 95

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ーとやり取りして、サーバー名とサーバーが属する 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、まだ宛先サーバー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。Web プロキシが URL カテゴリを認識していない場合、情報が不足しているために透過的 HTTPS 要求をユーザー定義のルーティングポリシーと一致させることはできません。

その結果、どのルーティングポリシーグループにも、どの識別プロファイルにもメンバーシップ基準がない場合は、透過的にリダイレクトされる HTTPS トランザクションのみがルーティングポリシーと一致します。ユーザー定義のルーティングポリシーまたは識別プロファイルが URL カテゴリ単位でメンバーシップを定義している場合は、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一致します。

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, on page 85
• 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, on page 85

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、またはユーザーを認証するために HTTPS 要求を復号します。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。「復号ポリシー」のトピックの「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 サイトの復号のバイパス

HTTPS サーバーへのトラフィックが、Web プロキシなどのプロキシ サーバーによって復号されると、一部のHTTPSサーバー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。

すべてのユーザー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、これらのサーバーへの HTTPS トラフィックの復号をバイパスします。

Procedure

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

ステップ 2 メンバーシップの一環としてステップ 1 で作成されたカスタム URL カテゴリを使用する復号ポリシーを作成し、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。

Note 時間範囲が設定されている場合、最も高い優先順位が割り当てられます。時間範囲クォータに達した場合、リファラは機能しません。

- 接続がトンネル化されていて HTTPS 復号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 に従って、ブラウザ クライアントにはオープンに/匿名で参照するためのトグル スイッチが用意されている場合があります。これによって、Refererおよび参照元情報の送信をそれぞれ有効/無効にすることができます。この機能は Referer ヘッダーのみに依存しており、それらの送信をオフにするとこの機能は使用できなくなります。
- 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。そのため、HTTPS ベースのサイトから HTTP ベースのサイトに対するすべての要求には Referer ヘッダーが含まれず、この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。ユーザーが 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ーに示されず、ユーザーは承認されない証明書を受け入れることができません。

Note **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

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 サーバー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/ISE-PIC サービスへの接続を参照）。
- ISE およびプロキシ ログ（以下を参照）。 ログによるシステム アクティビティのモニター, on page 1
- 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、Secure Web Appliance 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ー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、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, on page 97を参照してください。
- パケット キャプチャ, on page 105（サポートの使用 , on page 107 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 https://www.openssl.org/ から入手できます。

ISE サーバーの接続に関する問題

証明書の問題

Secure Web ApplianceとISE サーバー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、 Secure Web Applianceのクライアント証明書が自己署名の場合、該当するISEサーバー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、Web Appliance クライアント証明書が CA 署名付きの場合も、該当する ISE サーバーにその 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 サーバー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、Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要 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 Secure Web Applianceに存在していることを確認します。
  - Web Appliance クライアント証明書のルート CA 署名証明書が ISE サーバー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：
  - （ Secure Web Applianceで生成され、ダウンロードされた）Web Appliance クライアント証明書がISE サーバーにアップロードされていること、およびISE サーバー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 サーバーで生成され、ダウンロードされた）ISE 管理者証明書および pxGrid 証明書が Secure Web Applianceにアップロードされていること、およびこのアプライアンス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_se
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...
```

Secure Web Applianceのこれらのトレースレベルログエントリは、30 秒後に ISE サーバー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（ISE/ISE-PIC サービスへの接続）で [テスト開始（Start Test）] を実行中に ISE サーバーへの接続が失敗した場合、ポート 443 と 5222 に設定されている ISE サーバーへの接続を確認します。

ポート 5222 は公式のクライアント/サーバー Extensible Messaging and Presence Protocol（XMPP）ポートであり、ISE サーバー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 サーバーの接続に関するその他の問題

Secure Web Applianceが ISE サーバー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 サーバーのライセンスの期限が切れている。
- ISE サーバーの [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 Secure Web Applianceクライアント（特に「test_client」または「pxgrid_client」）が、ISE サーバー上に存在する。これらは削除する必要があります。ISE サーバーの [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、 Secure Web Applianceが ISE サーバーへの接続を試みている。

  ISE サーバーに対する一部の変更（証明書のアップデートなど）では、ISE サーバー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 サーバー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、 Secure Web Appliance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`

  Secure Web Applianceの ISE プロセスが 30 秒以内に ISE サーバー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`

  Web Appliance クライアント証明書とキーが Secure Web Appliance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`

  Secure Web Applianceの ISE プロセスが 120 秒以内に ISE サーバーに接続できず、終了しました。

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

  Secure Web Applianceの ISE プロセスが、アップデートのために ISE サーバー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 サーバー接続用に Secure Web Appliance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: ...`

  Secure Web Appliance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 ...`

  Secure Web Appliance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 ...`

  Secure Web Appliance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

カスタムおよび外部 URL カテゴリを作成および編集し、[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）] のいずれか）を提供する場合、[ファイルの取得（Get File）] ボタンをクリックして、指定した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。

.CSV ファイルの IIS サーバでの MIME タイプに関する問題

カスタムおよび外部 URL カテゴリの作成および編集中に [External Live Feed Category（外部ライブ フィード ファイル カテゴリ）] > [Cisco Feed Format（シスコ フィード形式）] オプションの .csv ファイルを提供すると、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にファイルを取得する際、[406 not acceptable（406 受け入れられません）] エラーが発生する場合があります。同様に、feedsd ログでは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 ペーストの後にフィード 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場合、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場合があります。

.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, on page 93
- HTTPS トランザクションのロギング, on page 93
- 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）, on page 93

• 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, on page 94

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、[モニター（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。 Secure Web Appliance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, on page 94
- オブジェクトのブロックに関する問題, on page 79
- 識別プロファイルがポリシーから削除される, on page 95
- ポリシーの照合に失敗, on page 95
- 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, on page 97
- 次のセクションも参照してください。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, on page 85

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, on page 79
- 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 のアップデートがブロックされる, on page 79

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 のアップデートがブロックされる

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 Secure Web Appliance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, on page 95
- HTTPS 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, on page 95
- HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致, on page 96
- ユーザーに誤ったアクセス ポリシーが割り当てられる , on page 96

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。

HTTPS 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。ユーザー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 を使用してユーザーを追跡すると、以下の動作が引き起こされます。

- **HTTPS**。Web プロキシは、復号ポリシーを割り当てる前にユーザー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）する必要がありますが、トランザクションを復号しない限り、Cookie を取得してユーザー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 サーバー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ー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ーがグローバル 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する場合、Web プロキシは、HTTP 要求を介した HTTPS および FTP の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ー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 プロキシはユーザー名を NULL に設定し、ユーザー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、[すべてのユーザー（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。

ユーザーに誤ったアクセス 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。
- Secure Web Appliance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。

ユーザー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。

Procedure

ステップ 1 `advancedproxyconfig > authentication` CLI コマンドを使用します。

ステップ 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。

ポリシーのパラメータを変更した後のポリシー トレースの不一致

[アクセス ポリシー（Access Policy）]、[識別プロファイルとユーザー（Identification Profiles and Users）]、[1 つ以上の識別プロファイルを選択（Select One or More Identification Profiles）]、[選択されたグループとユーザー（Selected Groups and Users）] など、ポリシーのパラメータを変更した場合、変更が有効になるまで数分かかります。

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

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。

Note 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。

Note 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

Note 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、指定したユーザー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、Secure Web Appliance CLI コマンド を参照してください。

Procedure

ステップ 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。

ステップ 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。

ステップ 3 （オプション）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。 **Note** 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。	[ユーザー名（User Name）] フィールドにユーザー名を入力し、[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。 **Note** 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ーに対して認証が機能するためには、ユーザーがあらかじめ Secure Web Applianceを介して正常に認証されている必要があります。

ステップ 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。

Note
[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（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。

Note
指定されたクライアントIPアドレスがルーティングできない場合、トレース結果に「接続トレース：発信サーバーへの接続：失敗（Connection Trace: Connection to Origin Server: Failed）」と表示されます。

What to do next

関連項目

• 詳細設定：要求の詳細, on page 99
• 詳細設定：レスポンスの詳細の上書き, on page 100

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。

Procedure

ステップ 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。

ステップ 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 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。
ユーザー エージェント（User Agent）	要求でシミュレートするユーザー 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。
アンチマルウェア 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。

ステップ 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。

Procedure

ステップ 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。

ステップ 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。
アプリケーション（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。 Web レピュテーションスコアを 100 にすると、「スコアなし」を意味します。
アンチマルウェア 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。

ステップ 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 レピュテーションと分析のトラブルシューティング」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

Note 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。

Procedure

ステップ 1 次の点をチェックします。

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

ステップ 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

Before you begin

- 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。

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」エラーが発生します。

Procedure

ステップ 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
```

S195、S395、および S695 モデルの場合は、次を使用します。

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password 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。

ステップ 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, on page 102
- POST 要求を使用してサイトにアクセスできない , on page 103
- 次のセクションも参照してください。特定 Web サイトの復号のバイパス, on page 86

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、 Secure Web Appliance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 のユーザー クラスを作成します。

関連項目

- 認証のバイパス

POST 要求を使用してサイトにアクセスできない

ユーザーの最初のクライアント要求が POST 要求で、ユーザー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 プロキシでユーザーを認証させます。
- 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。

Note 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。

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

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：

- Secure Web Appliance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 Secure Web Appliance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 サーバーでは「Proxy-Authorization」HTTP ヘッダーが必要であるため、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サーバーに直接接続するか、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、電源オフ、リセットの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。

解決方法

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、ウォッチドッグ問題、および高 CPU 使用率

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。

解決方法

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

Linux ホスト上で実行され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 展開で実行されている仮想アプライアンスに関する問題は、ホスト OS の設定の問題と関連している可能性があります。

解決方法

『*Virtualization Deployment and Administration Guide*』のトラブルシューティングに関するセクション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 [英語] 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, on page 105

最大ポート エントリ数

WCCP を使用している展開では、HTTP、HTTPS、および FTP の各ポートの合計 30 が最大ポート エントリ数になります。

パケット キャプチャ

• パケット キャプチャの開始, on page 106
• パケット キャプチャ ファイルの管理, on page 107

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。

Note 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。

Secure Web Appliance は、NIC ペアリングインターフェイスのパケットキャプチャをサポートしていません。パケットキャプチャは、アクティブなインターフェイスにのみ適用されます。たとえば、P1 と P2 の両方がペアになっている場合、P1 と P2 のどちらもユーザーインターフェイスまたは CLI で設定されません。

パケット キャプチャの開始

Procedure

ステップ 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。

ステップ 2 （オプション）[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。 **Note** 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（Interfaces）	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。

（オプション）パケット キャプチャの変更を送信して確定します。

Note

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。

ステップ 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, on page 107

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

Note 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。

Procedure

ステップ 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。

ステップ 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。

ステップ 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の情報収集 , on page 107
• テクニカル サポート要請の開始, on page 108
• 仮想アプライアンスのサポートの取得 , on page 108
• アプライアンスへのリモート アクセスのイネーブル化 , on page 109

効率的なサービス提供のための情報収集

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, on page 76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, on page 105」を参照してください。

テクニカル サポート要請の開始

Before you begin

- 自身の Cisco.com ユーザー 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一覧を参照するには、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 のユーザー ID がない場合は、登録して ID を取得してください。

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。

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

Procedure

ステップ 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。

ステップ 2 （オプション）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。

ステップ 3 自身の連絡先情報を入力します。

ステップ 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。

ステップ 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。

Procedure

ステップ 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。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 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。

オプション	説明
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ー 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。
送信元インターフェイス（Source Interface）	トンネルとリモートアクセス接続の確立に使用するインターフェイスを選択できます。
アプライアンスシリアル番号（Appliance Serial Number）	アプライアンスのシリアル番号。

ステップ 4 変更を送信し、保存します。

ステップ 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。

ステップ 6 シード文字列をサポート担当者に提出します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。