SYNESIS version 4.5 release 3
リリースノート
2019/06/17

SYNESIS version 4.5 release 3 における変更点

- GTP Inner 解析で、特定のパケットが解析できずキャプチャドロップを引き起こす不具合を修正しました。 (Ref #9773)
- MFA で、送信元と送信先のポート番号が同じ場合に、異なる 2 つのフローとして検出される不具合を修正しました。 (Ref #9806)
- VoIP フィルタで、SIP と RTP のポート番号範囲が重複している場合に RTP がフィルタされない不具合を修正しました。 (Ref #9838)
- 長時間のキャプチャレコードからのトレース保存が遅くなる不具合を修正しました。 (Ref #9841)
- Version 3.0 以前の SYNESIS からバージョンアップした場合にログの取得が失敗する不具合を修正しました。 (Ref #9882)
- VoIP フィルタを適用したトレース保存では、チャネルごとにフィルタを適用する方式から、全チャネルのパケットをタイムスタンプ順に並べてからフィルタする方式に変更しました。 (Ref #9946)
- VoIP フィルタでは RFC3261 に従い、SIP メッセージ内の特定のヘッダを大文字・小文字を問わずに解釈するよう変更しました。 (Ref #9958)

SYNESIS version 4.5 release 2 における変更点

- ダッシュボードまたはレポートの TopN 棒グラフおよび表において、global ではなく Others を表示するよう変更しました。 (Ref #9424)
- ダッシュボードまたはレポートの TopN 円グラフで、Others に該当するパケットが存在しない場合にグラフが描画されない不具合を修正しました。 (Ref #9424)

SYNESIS version 4.5
リリースノート
2019/05/10

本文書は、大容量パケットキャプチャ/解析システム「SYNESIS」のリリースノートです。

1. SYNESIS version 4.5 のコンセプト

- これまで、1G/10G インタフェースの SYNESIS と 100G インタフェースの SYNESIS ではバージョンが異なり、機能差がありました。SYNESIS 4.5 ではこれらのバージョンを統一して機能差をなくしました。
- ただしパケットリプレイヤー機能については SYNESIS 5.0 で統合の予定です。

2. 本文書におけるパケットリプレイヤーの区別について

- 本文書中で「統合版のパケットリプレイヤー」と表記した場合は、SYNESIS の Web アプリケーションにログインし、画面左下の下記アイコンから実行する機能を指します。

- 本文書中で「別製品のパケットリプレイヤー」と表記した場合は、SYNESIS の OS またはリモートデスクトップでログイン後に下記アイコンから実行するプログラムの機能、あるいはそのプログラムをコマンドラインで実行する機能を指します。

3. SYNESIS version 4.5 の新機能

3.1. VoIP 保存フィルタ

- 電話番号条件に一致する SIP, RTP の UDP パケットがフィルタ可能になりました。

3.2. キャプチャ時のタイムスタンプ分解能

- 本バージョンでリリースする全てのモデルで、タイムスタンプ分解能が 1ns になりました。

3.3. RESTful API

- トレースファイルの保存時に、分割ファイルサイズが指定できるようになりました。

3.4. SYNESIS のシステム情報

- 構成メニュー内に、SYNESIS のバージョン情報、製品名、構成部品名を表示するメニューを追加しました。

4. バージョン 4.0 からの変更点

4.1. V4.5 での重要な制限事項

- パケットリプレイヤー（統合版・別製品とも）では、FCS をそのままで送信することができません。
- SYNESIS 統合版のパケットリプレイヤーでは、パケット編集時に L3, L4 のチェックサムが再計算されません。別製品のパケットリプレイヤーでは再計算されます。
- V4.5 で新規製造された SYNESIS の 1G モデルでは、10M のリンクができません。

4.2. V4.0→V4.5 で修正された制限事項・不具合

- 新規製造時にレポート機能が正しくインストールされず、レポート機能が全く使用できない不具合は、修正されました。
- 特定のトレースで MFA の時刻同期が実行できない不具合は、修正されました。
- リアルタイムデコードを 1 回でも実行すると、その後通常のデコードが実行できなくなる不具合は、修正されました。
- 間欠的にリアルタイムデコードの結果が取得できない不具合は、修正されました。
- GTP ヘッダにシーケンス番号のフィールドが存在する場合に、保存フィルタ適用時や解析時に当パケットの Inner ヘッダが正しくされない認識されない不具合は、修正されました。
- Top N グラフにおいて、常に Global Site が表示される挙動は、修正されました。
- Wireshark でキャプチャを行い pcapng 形式で保存したトレースファイルが MFA でマージできない不具合は、修正されました。

4.3. V4.0→V4.5 で変更された機能

- キャプチャレコードのバックアップ、および外部データソース機能は、誤操作を防ぐため非サポートとなりました。

5. バージョン 4.1 からの変更点

5.1. V4.1→V4.5 で追加される機能

- SYNESIS バージョン 3.5 および 4.0 で提供された機能のうち、統合版のパケットリプレイヤーを除く機能が追加されました。詳しくは過去の SYNESIS リリースノートを参照ください。

5.2. V4.1→V4.5 へのバージョンアップ時の注意点

- バージョンアップ時に下記の設定が引き継がれません。現状の設定を控えていただき、バージョンアップ後に再設定が必要になります。詳しくはバージョンアップ手順書を参照ください。
  - キャプチャフィルタ(フロー)および保存フィルタ(フロー)のポート番号
  - アラートの有効(ON)/無効(OFF)設定
  - マイクロバーストの設定
  - NTP 設定
- Web アプリケーションおよび RESTful API の URL が、http から https に変更されます。
  - これに伴い、SYNESIS の Web アプリケーションで使用するポートが 8080 から 443 に変更されます。
- [キャプチャ中の自動解析]オプションを指定する場所を、構成(解析)画面からキャプチャオプション(共通)画面に変更しました。

5.3. V4.1→V4.5 で修正された制限事項・不具合

- SNMP トラップトリガによるロック機能で、入力したコミュニティ以外のトラップによってもロックが追加される不具合は、修正されました。 (Ref #1721)
- ディスクの空き容量が十分にある場合でも、ディスク容量不足の警告が表示される場合がある不具合は、修正されました。 (Ref #1725)
- デコード画面でフローフィルタを使用し IPv6 のアドレスを “::” で省略した場合、フィルタが正しく適用されない不具合は、修正されました。 (Ref #2178)
- デコード画面の保存フィルタを使ってトレース保存した場合でもトレースファイルタブの保存フィルタの一覧に表示されない不具合は、修正されました。 (Ref #2620)
- デコードタブを開いたままデコード対象のトレースを削除した場合、タブが残り続ける不具合は、修正されました。 (Ref #2637)
- 不正形式のフレームが大量に含まれているレコードをデコードさせると、GUI が停止することがある不具合は、修正されました。 (Ref #2645)
- Email の通知機能と DLC アラート機能が同時に有効の場合、DLC グラフの描画が不安定になる不具合は、修正されました。 (Ref #2653)
- キャプチャ中のレコードの統計情報が、エージェント・ワークスペースのレコードタブからエクスポートできない不具合は、修正されました。 (Ref #2665)
- トレースファイルのサイズが 256 MB より大きい場合、デコード機能へのリンクが表示されない制限は、撤廃されました。(Ref #2756)

- デコード画面では、最大 500,000 個のパケットまでしか表示できない制限は、撤廃されました。 (Ref #2756)
- Wireshark の SSL デコード機能を使用する際に、キーファイルの削除・追加の操作を行うと Wireshark が強制終了することがある不具合は、修正されました。 (Ref #3450)
- リモートデスクトップから LibreOffice スイートを使用する場合、メニューのショートカット表示が "???" のように文字化けする不具合は、修正されました。
- エージェント画面の総バイト数と NPM 解析後の総バイト数が一致しない不具合は、修正されました。 (Ref #4931)
- バージョン 4.1 以前では、SYNESIS のストレージ情報に表示されるパケットストアの容量が本来よりも小さく表示される不具合があり、「GiB」で計算された値に「GB」の単位が付加されて表示されていました。本バージョンで修正され、「GB」で計算された数値が表示されるようになりました。
- トレースファイルのサイズが実際よりも 1 だけ小さく表示される不具合を修正しました。
- キャプチャオプションの自動保存で保存フィルタを選択しても、キャプチャ開始時にフィルタが適用できない不具合を修正しました。 (Ref #4833)
- V4.1 では、保存フィルタの「エラー」は未サポートでしたが、V4.5 ではサポートされました。
- 別製品のパケットリプレイヤーで、パケット編集時に大量のログが出力される挙動は、修正されました。

5.4. V4.1→V4.5 で変更された機能

- キャプチャレコードのバックアップ、および外部データソース機能は、誤操作を防ぐため非表示となりました。

6. 既知の不具合

6.1. バージョン 4.0 以前からの不具合

- キャプチャ中のレコードの名称を変更しても、キャプチャ終了時に変更前の名称に戻ります。 (Ref #1114)
- アラート画面から各アラートのトレースファイルを作成しようとした場合、ソフトウェアフィルタが自動では適用されません。デフォルト設定では該当の期間の全パケットが保存されます。(Ref #1649)
- 保存フィルタの入力画面で新規フィルタを作成する画面を開いた際、前回入力した値がそのまま表示されます。 (Ref #1754)
- 直近のデータの解析結果は、キャプチャの停止を行う、または次のパケットがキャプチャされるまで、ダッシュボード、APM/NPM 画面で閲覧できません。 (Ref #2865)
- デコード画面からトレース保存を行う場合、ファイル名を指定できません。 (Ref #4017)
- インストール後はじめて L2/L3 プロトコル統計を有効にして自動解析を ON にした場合、キャプチャ開始直後の 1 秒間、およびキャプチャ終了直前の 1 秒間のカウントが実数より少なくなる場合があります。 (Ref #4169)
- ダッシュボード画面のトレンドグラフで、表示期間を 30 分以上にした場合、右端のプロットが 0 になる場合があります。 (Ref #4212)
- 最大ファイル数を 2 以上としてトレースの保存を開始し、保存先の容量が一杯になった場合は、作成済のファイルもダウンロードできません。 (Ref #4358)
- 解析の進捗度は、解析が完了するまでは 0%と表示されます。実際の進捗度は表示されません。 (Ref #4580)
- レポート機能の周期レポートおよび単発レポートで、集計間隔が 1 ヶ月のグラフは、正しく描画されない場合があります。 (Ref #4741)
- 統計のエクスポート機能で、ユニキャストパケットの総和が実際と合わない場合があります。この現象はブロードキャストパケットおよびマルチキャストパケットのみキャプチャされ、ユニキャストパケットがキャプチャされない場合に発生します。 (Ref #4771)
- SYS-2G-EP/SYS-2G-ER モデルでキャプチャ後にマイクロバースト解析を行うと、複数チャネルでバーストが発生している場合に正しく検知できない場合があります。キャプチャ中の自動解析であれば正しく検知できます。 (Ref #4774)
- ディスクフル時の動作を停止にしてキャプチャを開始した場合、ディスクがフルになった後もキャプチャステータスが更新されません。画面をリフレッシュするとステータスが停止になります。 (Ref #4781)
- SYNESIS の初期化機能を出荷後はじめて実行した場合に失敗することがありますが、もう 1 度初期化を実行すれば正常に完了できます。 (Ref #T62515)
- 自動保存を有効にして、かつ時刻トリガによるロックを有効にしてキャプチャを行うと、ロックが設定時刻より遅れて作成される場合があります。 (Ref #7819)
- RADIUS による外部認証が有効な状態であっても、RESTful API はローカルユーザで認証されます。 (Ref #7858)

- MFA およびデコード機能で、エキスパート情報の表示領域を縮めることができません。そのためご使用のモニタサイズによっては、パケット一覧およびパケット詳細情報の表示領域が十分に確保できない場合があります。 (Ref #8150)

6.2. 本バージョンで追加した既知の不具合

本バージョンで追加した既知の不具合はありません。

7. 制限事項

7.1. バージョン 4.0 以前からの制限事項

- APM/NPM 画面において、新たに登録したサイト、サーバーグループはウェブページをリフレッシュするまで反映されません。 (Ref #130)
- 各チャネルのリンク状況を確認できるモデルで、キャプチャ開始直後の統計情報のステータスが "unknown"と表示されることがあります。 (Ref #3671)
- 検出したマイクロバーストのアラームは最大 500 個までしかテーブルに表示できません。
- キャプチャ期間が 5 分未満のレコードでは、APM 解析の結果が検出できないことがあります。APM 解析を行う場合には 5 分以上キャプチャしたレコードに対して行ってください。
- キャプチャ開始後 2 秒間はパケット数などの統計情報がカウントされません。
- マイクロバースト解析はチャネル A～D に対してのみ実行できます。5 ポート以上存在するモデルでは、チャネル E 以降のデータはマイクロバースト解析できません。
- 自動保存機能の保存先としてネットワークマウントを行っているディレクトリを指定する場合には、マウント時に適切にタイムアウトを設定する必要があります。
- 自動保存機能は、キャプチャ停止の直前 10 秒間のパケットは保存されません。
- SYS-2G-ER で自動保存機能を使用すると、キャプチャ性能に影響が出る場合があります。
- パケットリプレイヤー（統合版・別製品とも）では、複数ポートから再生する場合はフルレートの性能が出せません。1 ポートからの再生時のみフルレートでの再生が可能です。
- 周期レポート機能でトレンドグラフを生成すると、時間範囲の最終時刻を X 軸の値としてプロットします。例えば集計間隔 1 日のグラフで、1/1 0:00 から 1/2 0:00 のデータ点は、横軸が 1/2 の位置にプロットされます。
- 設定のバックアップ・リストア機能では、異なるモデルの SYNESIS に設定をリストアする場合、別途ファイルを編集する必要があります。
- 統合版のパケットリプレイヤーでリプレイを行い、同時にキャプチャフィルタを有効にしてキャプチャを行うと、フィルタが正しく適用されない場合があります。 (Ref #5531)
- 統合版のパケットリプレイヤーでキャプチャレコードをリプレイする場合に、そのレコードの開始直後、あるいは終了直前の 1 秒間の統計データと、実際にリプレイされるパケットに差異が生じる場合があります。 (Ref #6591)

- 統合版のパケットリプレイヤーで使用率が数%またはそれ以下のキャプチャレコードは、ワイヤーレートでリプレイしても、安定して 100%のワイヤーレートにならない場合があります。 (Ref #7695)
- 統合版のパケットリプレイヤーでは 64 バイト未満の malformed packet がリプレイできません。
  (Ref #7924)

7.2. バージョン 4.1 以前からの制限事項

- APM/NPM での解析結果として表示されたデータをソートした場合、全データからソートは行われません。「構成->解析->上位のフロー」で設定された数のデータがあらかじめ取得され、その中でのみソートが行われます。(Ref #4940)
- 「ディスクフル時の動作」を「停止」に設定した場合、自動でキャプチャが停止する直前の数秒間ドロップカウントが上昇します。これは、ディスクがフルになった後に届いたパケットがカウントされているもので、SYNESIS がパケットのキャプチャに失敗したことを示すものではありません。

7.3. 本バージョンで追加した制限事項

- パケットリプレイヤー（統合版・別製品とも）では、FCS をそのままで送信することができません。
- 統合版のパケットリプレイヤーでは、パケット編集時に L3, L4 のチェックサムが再計算されません。別製品のパケットリプレイヤーでは再計算されます。
- V4.5 で新規製造された SYNESIS の 1G モデルでは、10M のリンクができません。
- フローフィルタおよび IP フローフィルタのトンネルオプションに「すべてのヘッダ」を選択した場合、以下のパケットに対してフィルタが適用されません。
  - アウターヘッダとインナーヘッダの L3 プロトコルがともに IPv4 で、アウターヘッダにフィルタ条件がマッチするパケット
  - アウターヘッダとインナーヘッダの L3 プロトコルがともに IPv6 で、アウターヘッダにフィルタ条件がマッチするパケット
- ハードウェアフィルタの IP フローフィルタおよびフローフィルタにおいて、一方のアドレス＋ポートの範囲が他方を包含する指定をした場合、そのフィルタを保存できない場合があります。
  また設定を保存できたとしても、キャプチャに適用した際に意図通りにフィルタリングできない場合があります。
  - IP フローフィルタの設定不可例(IP アドレス 1 が IP アドレス 2 を包含する)：
    IP アドレス 1 - 10.1.0.0/16
    IP アドレス 2 - 10.1.1.0/24
  - フローフィルタの設定不可例(IP アドレス 1+ポート 1 が IP アドレス 2+ポート 2 を包含する)：
    IP アドレス 1 - 10.1.0.0/16, ポート 1 - なし(Any)
    IP アドレス 2 - 10.1.1.0/24, ポート 2 - 100

以上