DNP3 インスペクタ

DNP3 インスペクタの概要

タイプ	インスペクタ（サービス）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	`stream_tcp`、`stream_udp`
有効	`false`

Distributed Network Protocol（DNP3）は遠隔監視制御・情報取得（SCADA）プロトコルであり、当初は発電所間で一貫性のある通信を実現する目的で開発されました。DNP3 は水処理、廃棄物処理、輸送などの産業分野で幅広く使用されています。

`dnp3` インスペクタは、DNP3 トラフィックの異常を検出し、DNP3 プロトコルを分析します。`dnp3` 侵入ルールのオプションは、特定の DNP3 プロトコルフィールドにアクセスします。

DNP3 インスペクタのパラメータ

DNP3 TCP ポートの設定

`binder` インスペクタは、DNP3 TCP ポートの設定を定義します。詳細については、『バインダ インスペクタの概要』を参照してください。

例：

```
[
   {
       "when": {
           "role": "any",
           "service": "dnp3"
    },
       "use": {
           "type": "dnp3"
       }
    }
]
```

check_crc

DNP3 リンク層フレームに含まれているチェックサムを検証するかどうかを指定します。dnp3 インスペクタは、チェックサムが無効なフレームを無視します。侵入ルール 145:1 が有効になっている場合、Snort は無効なチェックサムに対してアラートを生成します。

型：ブール値

有効な値：true、false

デフォルト値：false

DNP3 インスペクタのルール

dnp3インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *1: DNP3* インスペクタのルール

GID:SID	ルール メッセージ
145:1	DNP3 リンク層フレームに不良 CRC が含まれている（DNP3 link-layer frame contains bad CRC）
145:2	DNP3 リンク層フレームがドロップされた（DNP3 link-layer frame was dropped）
145:3	DNP3 トランスポート層セグメントがリアセンブル中に削除された（DNP3 transport-layer segment was dropped during reassembly）
145:4	DNP3 リアセンブルバッファが、完全なメッセージをリアセンブルせずにクリアされた（DNP3 reassembly buffer was cleared without reassembling a complete message）
145:5	DNP3 リンク層フレームは予約済みアドレスを使用する（DNP3 link-layer frame uses a reserved address）
145:6	DNP3 アプリケーション層フラグメントは予約済み関数コードを使用する（DNP3 application-layer fragment uses a reserved function code）

DNP3 インスペクタの侵入ルールのオプション

dnp3_data

dnp3_data キーワードは、先行するルールのオプションに関係なく、アプリケーション層フラグメント内の DNP3 データの先頭に検出カーソルを配置します。このオプションを使用すると、データを分割して 16 バイトごとに CRC を追加することなく、フラグメント内のデータに基づいてルールを作成できます。

シンタックス：dnp3_data;

例：dnp3_data;

dnp3_func

このオプションは、DNP3 アプリケーション層の要求/応答のヘッダー内の関数コードと照合されます。コードは、以下のリストの 10 進数または文字列です。

型：文字列

シンタックス：dnp3_func: <DNP3_function>;

有効な値：*DNP3_function* は次のいずれかです。

- 0 ～ 255 の整数
- confirm（機能コード 0 に対応）
- read（機能コード 1 に対応）
- write（機能コード 2 に対応）
- select（機能コード 3 に対応）
- operate（機能コード 4 に対応）
- direct_operate（機能コード 5 に対応）
- direct_operat_nr（機能コード 6 に対応）
- immed_freeze（機能コード 7 に対応）
- immed_freeze_nr（機能コード 8 に対応）
- freeze_clear（機能コード 9 に対応）
- freeze_clear_nr（機能コード 10 に対応）
- freeze_at_time（機能コード 11 に対応）
- freeze_at_time_nr（機能コード 12 に対応）
- cold_restart（機能コード 13 に対応）

- warm_restart（機能コード 14 に対応）
- initialize_data（機能コード 15 に対応）
- initialize_appl（機能コード 16 に対応）
- initialize_appl（機能コード 17 に対応）
- initialize_appl（機能コード 18 に対応）
- save_config（機能コード 19 に対応）
- enable_unsolicited（機能コード 20 に対応）
- save_config（機能コード 21 に対応）
- assign_class（機能コード 22 に対応）
- assign_class（機能コード 23 に対応）
- record_current_time（機能コード 24 に対応）
- open_file（機能コード 25 に対応）
- close_file（機能コード 26 に対応）
- delete_file（機能コード 27 に対応）
- get_file_info（機能コード 28 に対応）
- authenticate_file（機能コード 29 に対応）
- abort_file（機能コード 30 に対応）
- activate_config（機能コード 31 に対応）
- authenticate_req（機能コード 32 に対応）
- authenticate_err（機能コード 33 に対応）
- response（機能コード 129 に対応）
- unsolicited_response（機能コード 130 に対応）
- authenticate_resp（機能コード 131 に対応）

例：

```
dnp3_func: 1;
dnp3_func: delete_file;
```

dnp3_ind

DNP3アプリケーション層の応答ヘッダーの内部インジケータフラグと照合する内部インジケータフラグのリストを表示します。1 つのオプションに複数のフラグを指定すると、いずれかの

フラグが設定されている場合にルールが起動します。複数のフラグにアラートを発行するには、複数のルールのオプションを使用します。

型：文字列

シンタックス：`dnp3_ind: "<flag> <flag>";`

有効な値：1 つ以上の DNP3 内部インジケータフラグ。ここで、`flag` は次のいずれかです。

- `all_stations`
- `class_1_events`
- `class_2_events`
- `class_3_events`
- `need_time`
- `local_control`
- `device_trouble`
- `device_restart`
- `no_func_code_support`
- `object_unknown`
- `parameter_error`
- `event_buffer_overflow`
- `already_executing`
- `config_corrupt`
- `reserved_2`
- `reserved_1`

例：

デバイスの再起動時または時刻同期の開始時のアラート：

```
dnp3_ind:"device_restart need_time";
```

class_1 イベントと class_2 AND class_3 イベントに関するアラート：

```
dnp3_ind:class_1_events; dnp3_ind:class_2_events; dnp3_ind:class_3_events;
```

dnp3_obj

DNP3 オブジェクト ヘッダー グループとバリエーションで照合します。

型：整数

構文： `dnp3_obj:<groupnum>,<varnum>;`

有効な値：DNP3 オブジェクトグループ ID とバリエーション ID。

- *`groupnum`* は DNP3 オブジェクトグループ指定する `0` 〜 `255` の整数です。

- *varnum* はオブジェクトグループ内のバリエーションを指定する 0 ～ 255 の整数です。

例：

DNP3 Date and Time オブジェクトのアラート：

```
dnp3_obj:50,1;
```

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。