

Groupe de travail Réseau  
**Request for Comments: 5655**  
Catégorie : Sur la voie de la normalisation

B. Trammell, Hitachi Europe  
E. Boschi, Hitachi Europe  
L. Mark, Fraunhofer IFAM  
T. Zseby, Fraunhofer FOKUS  
A. Wagner, ETH Zurich  
octobre 2009

Traduction Claude Brière de L'Isle

# Spécification du format de fichier d'exportation d'informations de flux IP (IPFIX)

**Résumé**

Le présent document décrit un format de fichier pour la mémorisation des données de flux sur la base du protocole d'exportation d'informations de flux IP (IPFIX, *IP Flow Information Export*). Il propose un ensemble d'exigences pour les formats de fichier plat de données de flux binaire, puis spécifie le format de fichier IPFIX pour satisfaire ces exigences sur la base des messages IPFIX. Ce format de fichier IPFIX est conçu pour faciliter l'interopérabilité et la réutilisabilité parmi une grande variété de mémorisations de flux, de traitements et d'outils d'analyse.

*(La présente traduction incorpore les errata 3559, 6560, 1988, 4306, 2906, 2030, 1984 à 1987, 1990 à 1992)*

**Statut du présent mémoire**

Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

**Notice de droits de reproduction**

Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

## Table des matières

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 1. Introduction.....                                                | 2  |
| 1.1 Vue d'ensemble des documents IPFIX.....                         | 3  |
| 2. Terminologie.....                                                | 3  |
| 3. Vue d'ensemble du concept.....                                   | 3  |
| 4. Motivation.....                                                  | 4  |
| 5. Exigences.....                                                   | 6  |
| 5.1 Souplesse du format d'enregistrement.....                       | 6  |
| 5.2 Auto-description.....                                           | 6  |
| 5.3 Compression des données.....                                    | 6  |
| 5.4 Indexation et recherche.....                                    | 7  |
| 5.5 Récupération d'erreur.....                                      | 7  |
| 5.6 Authentification, confidentialité, et intégrité.....            | 7  |
| 5.7 Anonymisation et masquage.....                                  | 8  |
| 5.8 Examen et reproductibilité de session.....                      | 8  |
| 5.9 Caractéristiques de performances.....                           | 8  |
| 6. Applicabilité.....                                               | 8  |
| 6.1 Mémorisation des données de flux collectées par IPFIX.....      | 9  |
| 6.2 Mémorisation des données de flux collectées par NetFlow-V9..... | 9  |
| 6.3 Essai des processus de collecte IPFIX.....                      | 9  |
| 6.4 Diagnostics des appareils IPFIX.....                            | 9  |
| 7. Spécification détaillée du format de fichier.....                | 9  |
| 7.1 Spécification du lecteur de fichier.....                        | 10 |
| 7.2 Spécification du rédacteur de fichier.....                      | 10 |
| 7.3 Cas d'utilisation spécifiques du rédacteur de fichier.....      | 11 |

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| 7.4 Type de support des fichiers IPFIX.....                                             | 14 |
| 8. Spécification des métadonnées de format de fichier.....                              | 14 |
| 8.1 Gabarits d'options recommandés pour les fichiers IPFIX.....                         | 14 |
| 8.2 Éléments d'information recommandés pour les fichiers IPFIX.....                     | 16 |
| 9. Signature et chiffrement des fichiers IPFIX.....                                     | 20 |
| 9.1 Signatures détachées de CMS.....                                                    | 20 |
| 9.2 Résilience à l'erreur de chiffrement.....                                           | 22 |
| 10. Compression des fichiers IPFIX.....                                                 | 23 |
| 10.1 Formats de compression pris en charge.....                                         | 23 |
| 10.2 Reconnaissance de la compression chez le lecteur de fichier.....                   | 23 |
| 10.3 Résilience à l'erreur de compression.....                                          | 23 |
| 11. Stratégies recommandées d'intégration de fichier.....                               | 24 |
| 11.1 Encapsulation de données non IPFIX dans les fichiers IPFIX.....                    | 24 |
| 11.2 Encapsulation de fichiers IPFIX dans d'autres formats de fichier.....              | 24 |
| 12. Considérations sur la sécurité.....                                                 | 24 |
| 12.1 Relations entre fichier IPFIX et chiffrement de transport.....                     | 25 |
| 12.2 Assertions de bout en bout pour les fichiers IPFIX.....                            | 25 |
| 12.3 Recommandations sur la force cryptographique pour les fichiers IPFIX.....          | 25 |
| 13. Considérations relatives à l'IANA.....                                              | 25 |
| 14. Remerciements.....                                                                  | 26 |
| 15. Références.....                                                                     | 27 |
| 15.1 Références normatives.....                                                         | 27 |
| 15.2 Références pour information.....                                                   | 27 |
| Appendice A. Exemple de fichier IPFIX.....                                              | 28 |
| A.1 Exemple de gabarits d'options.....                                                  | 29 |
| A.2 Exemple supplémentaire de données d'options.....                                    | 30 |
| A.3 Exemple de somme de contrôle de message.....                                        | 31 |
| A.4 Exemple de fichier Data Set.....                                                    | 31 |
| A.5 Exemple de fichier complet.....                                                     | 32 |
| Appendice B. Applicabilité des fichiers IPFIX à la mémorisation de flux NetFlow V9..... | 32 |
| B.1 Comparaison de NetFlow V9 avec IPFIX.....                                           | 32 |
| B.2 Methode pour transformer les messages NetFlow V9 en IPFIX.....                      | 34 |
| B.3 Exemple de transformation de NetFlow V9.....                                        | 35 |
| Adresse des auteurs.....                                                                | 36 |

## 1. Introduction

Le présent document spécifie un format de fichier fondé sur IPFIX, conçu pour faciliter l'interopérabilité et la réutilisation d'une large variété d'outils de mémorisation, de traitement, et d'analyse de flux. Il commence par un survol du format de fichier IPFIX, et un bref résumé de la façon dont les fichiers IPFIX fonctionnent (Section 3). La spécification détaillée du format de fichier IPFIX apparaît à la Section 7 ; cette section inclut des spécifications générales pour les lecteurs de fichiers IPFIX et les rédacteurs de fichiers IPFIX et des recommandations spécifiques pour les situations courantes dans lesquelles ils sont utilisés. Le format utilise le mécanisme des options IPFIX pour des métadonnées de fichier supplémentaires, afin d'éviter d'exiger des extensions au protocole, et minimiser les efforts exigés pour adapter les mises en œuvre de IPFIX pour utiliser le format de fichier ; une définition détaillée des gabarits d'options utilisés pour la mémorisation des métadonnées apparaît à la Section 8. L'Appendice A contient un exemple détaillé de fichier IPFIX.

Un avantage de la mémorisation fondée sur le fichier est que les fichiers peuvent être directement encapsulés les uns dans les autres et dans d'autres formats de mémorisation et transmission de données. Le format de fichier IPFIX s'appuie sur cela pour fournir le chiffrement, décrit à la Section 9 et la compression, décrite à la Section 10. La Section 11 fournit des recommandations spécifiques pour l'intégration des données de fichier IPFIX avec d'autres formats.

Le format de fichier IPFIX a été conçu pour être applicable à une large variété de situations de mémorisation de flux ; le motif derrière sa création est décrit à la Section 4. Le document souligne à la Section 5 l'ensemble des exigences que le format est conçu pour satisfaire, et explore à la Section 6 l'applicabilité d'un tel format à diverses zones d'application spécifiques. Ces sections sont destinées à donner les fondements du développement des fichiers IPFIX.

## 1.1 Vue d'ensemble des documents IPFIX

"Spécification du protocole d'exportation d'informations de flux IP (IPFIX) pour l'échange d'informations de flux de trafic IP" [RFC5101] et ses documents associés définit le protocole IPFIX, qui fournit aux ingénieurs et administrateurs de réseau l'accès aux informations de flux de trafic IP.

"Architecture pour l'exportation d'informations de flux IP" [RFC5470] définit l'architecture pour l'exportation d'informations de flux IP mesurés à partir d'un processus d'exportation IPFIX à un processus de collecte IPFIX, et la terminologie de base utilisée pour décrire les éléments de cette architecture, selon les exigences définies dans les "Exigences pour l'exportation d'informations de flux IP" [RFC3917]. La [RFC5101] couvre aussi les détails de la méthode de transport des enregistrements et gabarits de données IPFIX via un protocole de transport tenant compte de l'encombrement d'un processus d'exportation IPFIX à un processus de collecte IPFIX.

"Modèle d'information pour l'exportation d'informations de flux IP" [RFC5102] décrit les éléments d'information utilisés par IPFIX, y compris les détails de dénomination des éléments d'information, de numérotation, et le codage du type de données.

"Applicabilité de l'exportation d'informations de flux IP (IPFIX)" [RFC5472] décrit les diverses applications du protocole IPFIX et leur utilisation des informations exportées via IPFIX, et il rapproche l'architecture IPFIX des autres architectures et cadres de mesures.

De plus, "Exportation des informations de type pour les éléments d'information Exportation d'information de flux IP (IPFIX)" [RFC5610] spécifie une méthode de codage des propriétés du modèle d'information au sein d'un flux de messages IPFIX.

Le présent document fait référence aux [RFC5101] et [RFC5470] pour la terminologie, définit le rédacteur de fichier IPFIX et le lecteur de fichier IPFIX dans les termes des définitions de processus d'exportation IPFIX et de processus de collecte IPFIX d'après la [RFC5101], et étend le modèle d'informations IPFIX défini dans la [RFC5102] pour fournir de nouveaux éléments d'information pour les métadonnées de fichier IPFIX. Il utilise la méthode décrite dans la [RFC5610] pour prendre en charge l'auto description de fichiers IPFIX contenant des éléments d'information spécifiques d'entreprise.

## 2. Terminologie

Cette section définit la terminologie relative au format de fichier IPFIX. De plus, les termes utilisés dans le présent document qui sont définis dans la section "Terminologie" de la [RFC5101] sont à interpréter comme défini ici.

**Fichier IPFIX** : un fichier IPFIX est un flux de messages IPFIX en série ; ce flux peut être mémorisé sur un système de fichiers ou transporté en utilisant toute technique utilisée couramment pour les fichiers. Tout flux de messages IPFIX qui serait considéré valide quand il est transporté sur un ou plusieurs des transports IPFIX spécifiés (protocole de transmission de contrôle de flux (SCTP) TCP, ou UDP) comme défini dans la [RFC5101] est considéré comme un fichier IPFIX. Cependant, le présent document étend cette définition avec des recommandations sur la construction de fichiers IPFIX qui satisfont les exigences identifiées à la Section 5.

**Lecteur de fichier IPFIX** : un lecteur de fichiers IPFIX est un processus qui lit les fichiers IPFIX à partir d'un système de fichiers. Un lecteur de fichiers IPFIX opère comme un processus de collecte IPFIX spécifié dans la [RFC5101], sauf comme modifié par le présent document.

**Rédacteur de fichier IPFIX** : c'est un processus qui écrit des fichiers IPFIX dans un système de fichiers. Un rédacteur de fichier IPFIX opère comme un processus d'exportation IPFIX spécifié dans la [RFC5101], sauf comme modifié par le présent document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

## 3. Vue d'ensemble du concept

Un fichier IPFIX est simplement un flux de données contenant un ou plusieurs messages IPFIX mis en série dans un système de fichiers. Bien que tout ensemble de messages IPFIX valides puisse être mis en série dans un fichier IPFIX, la

spécification inclut des lignes directrices conçues pour faciliter la mémorisation et la restitution des données de flux en utilisant le format de fichier IPFIX.

Les fichiers IPFIX contiennent seulement des messages IPFIX ; toutes les métadonnées de fichier comme des sommes de contrôle ou détails de session d'exportation sont mémorisées en utilisant des options au sein du message IPFIX. Cette conception est complètement compatible avec le protocole IPFIX sur le réseau. Un schéma de fichier IPFIX typique est montré ci-dessous :

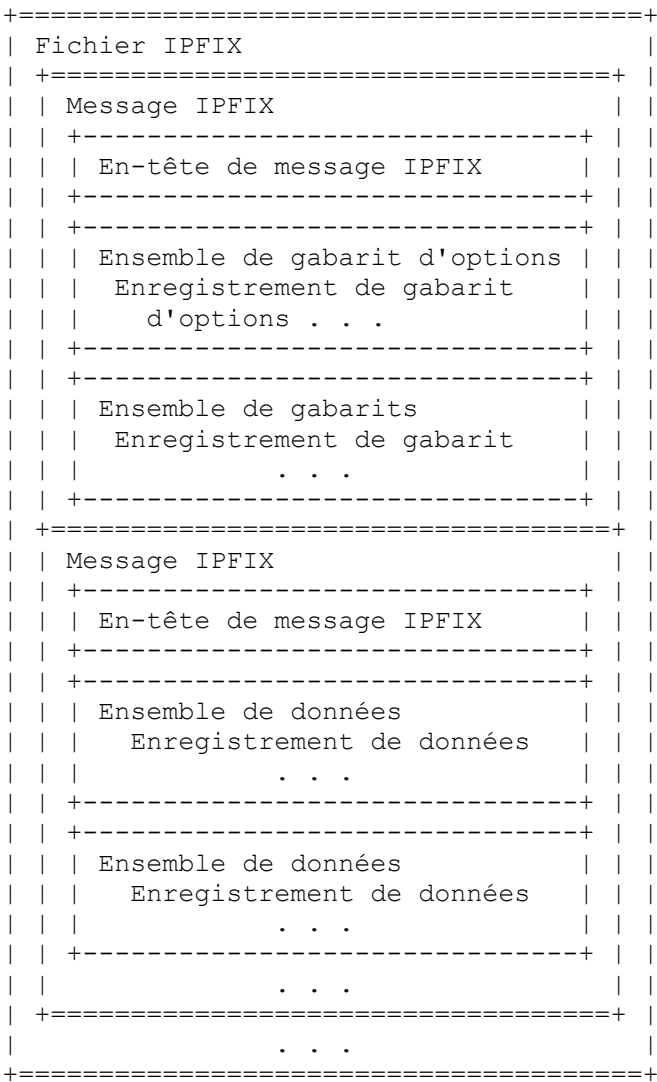


Figure 1 : Structure typique de fichier

4. Motivation

Il y a une grande variété d'applications pour la mémorisation de données de flux IP fondées sur le fichier, à travers un continuum d'échelles de temps. Les outils utilisés dans l'analyse des données de flux et la création des produits d'analyse utilisent souvent des fichiers comme unité pratique de travail, avec une durée de vie éphémère. Un ensemble de flux pertinent pour une investigation de sécurité peut être mémorisé dans un fichier pour la durée de cette investigation, et ensuite échangé entre les traitements incidents via la messagerie ou au sein d'une application externe de traitement de flux de travail incidente. Les ensembles de données de flux pertinentes pour une recherche de mesures Internet peuvent être publiés comme des fichiers, un peu comme le sont le fichiers de trace de paquet libpcap [pcap], pour fournir des ensembles de données communs pour la répétabilité des efforts de recherche ; ces fichiers vont avoir des durées de vie mesurées en mois ou années. Les systèmes opérationnels de mesure de flux ont aussi un besoin de mémorisation à long terme d'archives de données de flux, soit comme répertoire principal de données de flux, soit comme sauvegarde pour la mémorisation en

ligne dans un système de gestion de base de données relationnelles (RDBMS, *relational database management system*).

La variété des applications de données de flux, et la variété des approches de mémorisation présentement déployées, indiquent le besoin d'une approche standard de la mémorisation de flux avec applicabilité à travers le continuum des échelles de temps sur lesquelles les données de flux sont mémorisées. Un format de mémorisation fondé sur des fichiers plats conviendrait mieux à la diversité des exigences de mémorisation. Bien que beaucoup de travail ait été fait sur la mémorisation structurée via RDBMS, les systèmes de base de données relationnelles ne sont pas une bonne base pour la normalisation de format du fait que leurs structures de données internes sont généralement privées sur une seule mise en œuvre et sujettes à des changements pour des raisons internes. Aussi, il y a une grande variété d'opérations disponibles sur les fichiers plats, et des outils et normes externes peuvent servir d'appui pour satisfaire les exigences de mémorisation de flux fondées sur le fichier. De plus, les données de flux ne sont souvent pas très compliquées sémantiquement, et sont gérées en très gros volume ; donc, un système de mémorisation de flux fondé sur RDBMS ne bénéficierait pas beaucoup des avantages de la technologie de la base de données relationnelles.

La façon la plus simple de créer un nouveau format de fichier est simplement de mettre en série un modèle de données internes sur un disque, avec une représentation textuelle ou binaire des éléments de données, et une stratégie de tramage pour délimiter les champs et les enregistrements. Des formats de fichier "ad hoc" comme ceux-là ont plusieurs inconvénients importants. Ils imposent la sémantique du modèle des données d'où ils sont dérivés au format de fichier, et à ce titre, sont difficiles à étendre, décrire, et normaliser.

Bien sûr, une norme de fait pour la mémorisation des données de flux est un de ces formats ad hoc. Une méthode courante pour mémoriser les données collectées via NetFlow de Cisco est de mettre en série un flux de datagrammes NetFlow bruts dans les fichiers. Ces fichiers de PDU NetFlow consistent en une collection de blocs préfixés d'un en-tête (correspondant aux datagrammes reçus sur le réseau) contenant des enregistrements de flux binaires de longueur fixe. Les données NetFlow V5, V7, et V8 peuvent être mélangées au sein d'un fichier donné, car l'en-tête de chaque datagramme définit la version NetFlow de l'enregistrement qui suit. Bien que ce format de fichier de PDU NetFlow ait tous les inconvénients d'un format ad hoc, et ne soit pas extensible aux modèles de données autres que ceux définis par le NetFlow de Cisco, il est au moins raisonnablement bien compris du fait de son ubiquité.

Dans la décennie passée, XML a émergé comme nouveau format de représentation "universel" pour les données structurées. Il est destiné à être lisible par l'homme ; bien sûr, c'est une des raisons de son adoption rapide. Cependant, XML a une utilité limitée pour représenter des données de flux du réseau. Les données de flux du réseau ont une structure simple, répétitive, non hiérarchique qui ne profite pas beaucoup de XML. Une représentation XML de données de flux serait essentiellement une liste plate des attributs et de leurs valeurs pour chaque enregistrement de flux.

L'approche XML du codage des données est très lourde comparée au codage de flux binaire. L'utilisation par XML d'étiquettes de début et de fin, et le codage du texte des valeurs réelles, conduit à une inefficacité significative de la taille du codage. Les ensembles de données normaux du trafic du réseau peuvent contenir des millions ou de milliards de flux par heure de trafic représenté. Toute augmentation de taille de mémorisation par enregistrement peut avoir un impact sévère sur la mémorisation des données de flux et les tailles de transfert. Alors que les algorithmes de compression de données peuvent partiellement supprimer la redondance introduite par le codage XML, ils introduisent d'eux-mêmes des frais généraux supplémentaires.

Un autre problème est que les outils de traitement XML exigent un analyseur XML complet. Les analyseurs XML sont pleinement généraux et donc complexes, gourmands en ressources, et relativement lents, introduisant un temps de traitement significatif pour les grands ensembles de données de flux de réseau. À l'opposé, les analyseurs pour les codages de données de flux binaires normaux sont simplement structurés, car ils ont seulement besoin d'analyser un très petit en-tête et ont alors une connaissance complète de tous les champs suivants pour le flux particulier. Ils peuvent alors être lus très efficacement de façon linéaire.

Cela nous conduit à proposer le format de message IPFIX comme base d'un nouveau format de fichier de données de flux. Le groupe de travail IPFIX, en définissant le protocole IPFIX, a déjà défini un modèle d'information et des règles de formatage des données pour la représentation des données de flux. En particulier à de plus courtes échelles de temps, quand un fichier est une unité d'échange de données, le système de fichiers peut être vu comme simplement un autre transport de message IPFIX entre processus. Ce format est particulièrement bien adapté pour représenter des données de flux, car il a été conçu spécifiquement pour l'exportation des données de flux ; il est facilement extensible, à la différence de la mise en série ad hoc, et compact, à la différence de XML. De plus, IPFIX est un protocole sur la voie de la normalisation de l'IETF pour l'exportation et la collecte des données de flux ; utiliser un format commun pour la mémorisation et l'analyse du côté de la collecte permet aux mises en œuvre d'utiliser essentiellement le même modèle d'information et la même mise en œuvre de formatage des données pour le transport et la mémorisation.

## 5. Exigences

Dans cette section, on souligne un ensemble proposé d'exigences [SAINT2007] pour tout format persistant de mémorisation pour les données de flux. D'abord et avant tout, un format de fichier de données de flux devrait prendre en charge la mémorisation à travers le continuum d'échelles de temps importantes pour les applications de mémorisation de flux. Chacune des exigences énumérées dans les paragraphes qui suivent est largement applicable aux applications de mémorisation de flux, bien que chacune puisse être plus importante à certaines échelles de temps. Pour chacune, on identifie d'abord l'exigence, puis on explique comment le format de message IPFIX la traite, ou on mentionne brièvement les changements qui doivent être faits pour qu'un format de fichier fondé sur IPFIX satisfasse l'exigence.

### 5.1 Souplesse du format d'enregistrement

Du fait de la grande diversité d'attributs de flux collectés par les différents systèmes de mesure d'attribut de flux de réseau, le format idéal de mémorisation de flux ne va pas imposer un seul modèle de données ou un type spécifique d'enregistrement aux flux qu'il mémorise. Le format de fichier doit être souple et extensible ; c'est-à-dire, il doit prendre en charge la définition de plusieurs types d'enregistrement au sein du fichier lui-même, et doit être capable de prendre facilement en charge de nouveaux types de champs pour les données au sein des enregistrements.

IPFIX fournit la souplesse du format d'enregistrement par l'utilisation de gabarits pour décrire chaque enregistrement de données, par l'utilisation d'un registre de l'IANA pour définir ses éléments d'information, et par l'utilisation d'éléments d'information spécifiques d'entreprise.

### 5.2 Auto-description

Les données archivées peuvent être lues à un moment futur où toute référence externe à la signification des données peut être perdue. Le format idéal de mémorisation de flux devrait être auto descriptif ; c'est-à-dire, un processus de lecture des données de flux à partir de la mémorisation devrait être capable d'interpréter correctement les flux mémorisés sans référence à quelque chose d'autre que des sources standard (par exemple, les document standard qui décrivent le format de fichier) et les données de flux mémorisé elles-mêmes.

Le format du message IPFIX est partiellement auto descriptif ; c'est-à-dire, les gabarits IPFIX qui contiennent seulement des éléments d'information alloués par l'IANA peuvent être complètement interprétés en accord avec le modèle d'informations IPFIX sans données externes supplémentaires.

Cependant, les gabarits qui contiennent des éléments d'information privés manquent d'informations détaillées de type et de sémantique ; un processus de collecte qui reçoit des enregistrements de données décrites par un gabarit contenant des éléments d'information spécifiques d'entreprise qu'il ne comprend pas peut seulement traiter les données contenues dans ces éléments d'information comme un dispositif d'octets.

Pour être complètement auto descriptifs, des éléments d'information spécifiques d'entreprise doivent être de plus décrits via des options IPFIX en accord avec le gabarit d'options de type d'élément d'information défini dans la [RFC5610].

### 5.3 Compression des données

Sans considération du format de représentation, les données de flux qui décrivent le trafic sur les réseaux réels tendent à être très compressibles. La compression tend à améliorer l'adaptabilité des systèmes de collecte de flux, en réduisant la mémorisation sur le disque et l'exigence de bande passante d'entrée/sortie pour une charge de travail donnée. Le format idéal de mémorisation de flux devrait supporter des applications qui souhaitent s'appuyer sur ce fait en prenant en charge la compression des données mémorisées.

Le format de message IPFIX ne prend pas en charge la compression des données, car le protocole IPFIX a été conçu pour la rapidité et la simplicité de l'exportation. Bien sûr, tout fichier plat est directement compressible en utilisant une large variété d'outils, formats, et algorithmes de compression de données externes ; donc, cette exigence peut être satisfaite via l'encapsulation dans un de ces formats. La Section 10 spécifie une encapsulation fondée sur bzip2 ou gzip, pour maximiser l'interopérabilité.

Quelques optimisations simples peuvent être faites par des rédacteurs de fichiers pour augmenter l'intégrité et l'utilisabilité des données compressées IPFIX ; elles sont mentionnées au paragraphe 10.3.

## 5.4 Indexation et recherche

Les formats de fichier binaires, en mode enregistrement de flux prennent d'origine seulement en charge une forme de recherche : l'examen séquentiel dans l'ordre de fichier. En choisissant avec soin l'ordre des enregistrements dans un fichier (par exemple, par l'heure de fin de flux) un fichier peut être indexé par une seule clé.

Au delà de cela, l'indexation d'adressage approprié est un problème spécifique de l'application, car il implique naturellement des compromis entre complexité de mémorisation et vitesse de restitution, et les exigences varient largement selon les échelles de temps et les types d'interrogations utilisés d'un site à l'autre. Cependant, un format générique standard de mémorisation de flux peut fournir une prise en charge limitée directe pour l'indexation et la recherche.

Le format idéal de mémorisation de flux va prendre en charge une facilité limitée de tableau de contenus en notant que les enregistrements dans un fichier contiennent des données se rapportant seulement à certaines clés ou valeurs de clés, afin d'empêcher que des mises en œuvre de recherche multi-fichiers aient à examiner un fichier pour des données qu'il ne contient pas.

Le format de message IPFIX n'a pas de soutien direct de l'indexation. Cependant, la technique décrite dans la [RFC5473] "Réduction de redondance dans les rapports d'exportation d'informations de flux IP (IPFIX) et d'échantillonnage de paquet (PSAMP)" peut être utilisée pour décrire le contenu d'un fichier d'une façon limitée. De plus, comme les données de flux sont souvent triées et divisées par le temps, les heures de début et de fin des flux dans un fichier peuvent être déclarées en utilisant le gabarit Options de fenêtre temporelle de fichier défini au paragraphe 8.1.2.

## 5.5 Récupération d'erreur

Quand on mémorise des données de flux à des fins d'archivage, il est important de s'assurer que des fautes de matériel ou de logiciel n'introduisent pas d'erreurs dans les données au fil du temps. Le format idéal de mémorisation de flux va prendre en charge la détection et la correction des erreurs au niveau du codage dans les données.

Noter qu'une correction d'erreur plus évoluée est mieux traitée à une couche en dessous de celle visée par le présent document. La correction d'erreur est en général un sujet bien traité par l'industrie de la mémorisation (par exemple, par les matrices redondantes de disques indépendants (RAID, *Redundant Array of Independent Disks*) et autres technologies). En spécifiant un format de mémorisation de flux fondé sur les fichiers, on peut développer ces caractéristiques pour satisfaire cette exigence.

Cependant, le format idéal de mémorisation de flux va être résilient aux erreurs, fournissant une facilité interne pour la détection des erreurs et la capacité d'isoler les erreurs sur aussi peu d'enregistrements de données que possible.

Noter que cette exigence interagit avec le choix de la compression de données ou de l'algorithme de chiffrement. Par exemple, l'utilisation d'algorithmes de compression de blocs peut servir à isoler des erreurs sur un seul bloc de compression, à la différence des compresseurs de flux, qui peuvent échouer à se resynchroniser après une seule erreur de bit, invalidant le flux de message entier.

Le format de message IPFIX ne prend pas en charge l'assurance d'intégrité des données. On suppose qu'une correction d'erreur évoluée va être fournie en externe. La compression et le chiffrement, si ils sont utilisés, fournissent des tolérances pour la détection, sinon la correction, des erreurs. Pour la simple prise en charge de la détection d'erreur en l'absence de compression ou chiffrement, des sommes de contrôle peuvent être attachées aux messages via les options IPFIX conformément au gabarit d'options de somme de contrôle de message défini au paragraphe 8.1.1.

## 5.6 Authentification, confidentialité, et intégrité

La mémorisation d'archive de données de flux peut aussi exiger l'assurance qu'aucune entité non autorisée ne peut lire ou modifier les données mémorisées. Le chiffrement peut être appliqué à ce problème pour assurer l'intégrité et la confidentialité par la signature et le chiffrement.

Comme avec la correction d'erreur, ce problème a été bien traité à une couche inférieure à celle qui est visée par le présent document. On peut s'appuyer sur le fait que les technologies de chiffrement existantes fonctionnent assez bien sur les données mémorisées dans des fichiers pour satisfaire cette exigence.

Au delà de la prise en charge de l'utilisation de la sécurité de la couche transport (TLS, *Transport Layer Security*) pour le transport sur TCP ou la sécurité de la couche de transport de datagrammes (DTLS, *Datagram Transport Layer Security*) pour les transport sur SCTP ou UDP, qui tous deux fournissent une authentification et confidentialité transitoires, le protocole IPFIX ne prend pas en charge directement cette exigence. L'IETF a spécifié la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*) [RFC5652] pour créer des signatures détachées pour l'intégrité et l'authentification ; la Section 9 spécifie une méthode fondée sur la CMS pour signer les fichiers IPFIX. La protection de la confidentialité est supposée satisfaite par des méthodes externes à la présente spécification, s'appuyant sur une des nombreuses technologies de chiffrement des fichiers pour satisfaire des exigences spécifiques d'application et processus ; cependant, des notes sur l'amélioration de l'intégrité d'archivage des fichiers IPFIX chiffrés sont données au paragraphe 9.2.

## 5.7 Anonymisation et masquage

Pour assurer la confidentialité des individus et organisations aux points d'extrémité de communication représentés par les enregistrements de flux, il est souvent nécessaire de masquer ou d'anonymiser les données de flux mémorisées et exportées. Le format idéal de mémorisation de flux va fournir une notation qu'un élément d'information donné sur un type d'enregistrement donné représente des données anonymisées, plutôt que réelles.

Le protocole IPFIX n'a présentement pas de notation prise en charge pour l'anonymisation. On devrait noter que l'anonymisation est une des exigences données pour IPFIX dans la [RFC3917]. La décision de qualifier cette exigence avec "PEUT" et non "DOIT" dans le document des exigences, et son manque de spécification ultérieur dans la version actuelle du protocole IPFIX, est due au fait que les algorithmes d'anonymisation sont encore un domaine de recherche ouvert, et qu'il n'existe actuellement pas de méthode normalisée pour l'anonymisation.

Aucun soutien n'est présentement défini dans la [RFC5101] ou le format de fichier fondé sur IPFIX pour l'anonymisation, car la notation de l'anonymisation est un sujet de recherches pour le groupe de travail IPFIX.

## 5.8 Examen et reproductibilité de session

Certains cas d'utilisation de la mémorisation de flux pour archivage exigent la mémorisation de détails d'infrastructure de collection avec les données elles-mêmes. Ces détails incluent des informations sur comment et quand les données ont été reçues, et d'où elles ont été reçues. Ils sont utiles pour l'audit ainsi que pour la réexécution de données reçues pour des besoins d'essai.

Le protocole IPFIX ne contient pas de prise en charge directe d'audit ni de répétition, bien que le modèle d'informations IPFIX définisse bien divers éléments d'information exigés pour représenter les détails de l'infrastructure de collecte. Ces détails peuvent être mémorisés dans les fichiers IPFIX en utilisant le gabarit d'options Détails de session d'exportation défini au paragraphe 8.1.3, et le gabarit d'options Détails de message au paragraphe 8.1.4.

## 5.9 Caractéristiques de performances

Le format idéal de mémorisation de flux standard n'aura pas d'impact négatif significatif sur les performances de l'application générant ou traitant les données de flux mémorisées dans le format. C'est une exigence non fonctionnelle, mais il est important de noter qu'un standard qui implique une pénalité de performances significative a peu de chances d'être largement mis en œuvre et adopté.

Un examen du protocole IPFIX semblerait suggérer que ses mises en œuvre ne sont pas particulièrement enclines à la lenteur ; bien sûr, une représentation de données fondée sur un gabarit est plus facilement sujette à optimisation pour les cas courants que les représentations qui incorporent des informations structurelles directement dans le flux de données (par exemple, XML). Cependant, une analyse complète de l'impact de l'utilisation des messages IPFIX comme base de la mémorisation de données de flux sur les performances de lecture/écriture va exiger plus d'expérience et de mesures de performances des mises en œuvre.

## 6. Applicabilité

Cette Section décrit l'applicabilité spécifique des fichiers IPFIX aux divers cas d'utilisation. Les fichiers IPFIX sont particulièrement utiles dans une infrastructure de collecte et traitement de flux en utilisant IPFIX pour l'exportation de flux. On explore l'applicabilité et on fournit des lignes directrices pour l'utilisation des fichiers IPFIX pour la mémorisation des

données de flux collectées par IPFIX des processus de collecte et des collecteurs NetFlow V9, l'essai des processus de collecte IPFIX, et les diagnostics d'appareils IPFIX.

### 6.1 Mémorisation des données de flux collectées par IPFIX

Les fichiers IPFIX peuvent naturellement être utilisés pour mémoriser les données de flux collectées par un processus de collecte IPFIX ; bien sûr, c'était une des principales motivations initiales du format de fichier décrit dans ce document. L'utilisation de fichiers IPFIX fournit un seul codage, standard, bien compris à utiliser pour les données de flux sur disque et dans le réseau, et permet aux mises en œuvre IPFIX d'utiliser substantiellement le même code pour l'exportation et la mémorisation de flux. De plus, la mémorisation d'une seule session de transport dans les fichiers IPFIX est particulièrement importante pour la recherche de mesures du réseau, permettant de répéter des expériences en fournissant un format pour la mémorisation et l'échange de données de traçage de flux IPFIX un peu comme le format libpcap [pcap] qui est utilisé pour les expériences sur les données de traçage de paquet.

### 6.2 Mémorisation des données de flux collectées par NetFlow-V9

Bien que le protocole IPFIX soit fondé sur le protocole des services NetFlow de Cisco, version 9 (NetFlow V9) [RFC3954], les deux ont divergé depuis que le travail a commencé sur IPFIX. Cependant, comme le modèle d'information de NetFlow V9 est un sous ensemble compatible du modèle d'informations IPFIX, il est possible d'utiliser les fichiers IPFIX pour mémoriser les données de flux NetFlow V9 collectées. Cette approche peut être particulièrement utile dans des infrastructures de collecte multi-fabricants, multi-protocoles en utilisant à la fois NetFlow V9 et IPFIX pour exporter les données de flux.

L'applicabilité des fichiers IPFIX à ce cas d'utilisation est soulignée dans l'Appendice B.

### 6.3 Essai des processus de collecte IPFIX

Les fichiers IPFIX peuvent être utilisés pour mémoriser des messages IPFIX pour l'essai des processus de collecte IPFIX. Divers cas d'essai peuvent être mémorisés dans les fichiers IPFIX. D'abord, les données IPFIX collectées dans des environnements de réseau réels et mémorisées dans un fichier IPFIX peuvent être utilisées en entrée pour vérifier le comportement de mises en œuvre nouvelles ou étendues de collecteurs IPFIX. De plus, les fichiers IPFIX peuvent être utilisés pour valider le fonctionnement d'un processus de collecte IPFIX donné dans un nouvel environnement, c'est-à-dire, pour essayer avec des données IPFIX enregistrées à partir du réseau cible avant d'installer le processus de collecte dans le réseau.

Le format de fichier IPFIX peut aussi être utilisé pour mémoriser des messages artificiels de référence non conformes pour les cas d'essai spécifiques du processus de collecte. Des exemples de tels cas d'essai sont des ensembles d'enregistrements IPFIX avec des éléments d'information indéfinis, des enregistrements de données décrits par des gabarits manquants, ou des messages ou ensembles de données incorrectement tramés. Des cas d'essai représentatifs des traitements d'erreur sont définis dans la [RFC5471].

De plus, la répétition rapide de messages IPFIX mémorisés dans un fichier peut être utilisée pour des essais de tension/charge (par exemple, haut débit d'enregistrements de données entrants, grands gabarits avec comptes d'éléments d'information importants) comme décrit dans la [RFC5471]. Le provisionnement et l'utilisation de fichiers d'ensembles de référence pour des essais simplifie les performances des essais et augmente la comparabilité des résultats d'essais.

### 6.4 Diagnostics des appareils IPFIX

Comme un fichier IPFIX peut être utilisé pour mémoriser toute collection de flux, le format peut aussi être utilisé pour entasser et mémoriser divers types de données de flux pour des diagnostics d'appareils IPFIX (par exemple, l'antémémoire ouverte de flux d'un processus de mesure ou l'arriéré de flux d'un processus d'exportation ou de collecte au moment d'une réinitialisation ou défaillance d'un processus). La mémorisation fondée sur le fichier est préférable à la transmission à distance dans de telles situations de récupération d'erreurs.

## 7. Spécification détaillée du format de fichier

Tout flux valide de messages IPFIX en série DOIT être accepté par un lecteur de fichier comme un fichier IPFIX valide. De

cette façon, le système de fichiers est simplement traité comme un autre transport IPFIX à côté de SCTP, TCP, et UDP, bien que transport à latence potentiellement élevée, parce que le lecteur de fichier et le rédacteur de fichier ne fonctionnent pas nécessairement au même moment.

Cette section spécifie le détail des actions des lecteurs et rédacteurs de fichiers dans le traitement des fichiers IPFIX, et spécifie de plus les actions des rédacteurs de fichiers dans des cas d'utilisation spécifiques. Sauf mention contraire, les rédacteurs de fichier IPFIX DOIVENT se comporter comme des processus d'exportation IPFIX, et les lecteurs de fichier IPFIX DOIVENT se comporter comme des processus de collecte IPFIX, lorsque approprié.

## 7.1 Spécification du lecteur de fichier

Un lecteur de fichier IPFIX DOIT agir comme un processus de collecte IPFIX comme spécifié dans la [RFC5101], sauf comme modifié par le présent document.

Un lecteur de fichier IPFIX DOIT accepter comme valide tout flux de message IPFIX en série qui serait considéré comme valide par une ou plusieurs des autres couches de transport définies par IPFIX. Pratiquement, cela signifie que l'union des caractéristiques de gestion de gabarit IPFIX prises en charge par SCTP, TCP, et UDP DOIT être prise en charge dans les fichiers IPFIX. Les lecteurs de fichier DOIVENT :

- o accepter les messages IPFIX qui contiennent des ensembles de gabarits, des ensembles de gabarits d'options, et des ensembles de données au sein du même message, comme avec IPFIX sur TCP ou UDP ;
- o accepter des ensembles de gabarits qui définissent des gabarits déjà définis au sein du fichier, comme cela peut se produire avec la retransmission de gabarits quand on utilise IPFIX sur UDP comme décrit au paragraphe 10.3.6 de la [RFC5101] ;
- o résoudre tout conflit entre une définition renvoyée et une précédente définition en supposant que le nouveau gabarit remplace l'ancien, en cohérence avec l'expiration de gabarit et la réutilisation d'identifiant quand on utilise UDP comme protocole de transport IPFIX ; et
- o accepter les retraits de gabarit comme décrit à la Section 8 de la [RFC5101], pourvu que le gabarit à retirer soit défini, comme c'est le cas avec IPFIX sur TCP et SCTP.

Du point de vue du système de fichiers comme transport, en général, un fichier IPFIX DEVRAIT être traité comme contenant une seule session de transport comme défini par la [RFC5101]. Cependant, certaines applications peuvent bénéficier de la capacité de traiter une collection de fichiers IPFIX comme une seule session de transport ; voir en particulier le paragraphe 7.3.3. Un lecteur de fichier PEUT être configurable à traiter une collection de fichiers comme une seule session de transport. Cependant, un lecteur de fichier NE DOIT PAS traiter un seul fichier IPFIX comme contenant plusieurs sessions de transport.

Si un fichier IPFIX utilise la technique décrite dans la [RFC5473] ET si tous les gabarits non d'options dans le fichier contiennent l'élément d'information `commonPropertiesId`, un lecteur de fichier PEUT supposer que l'ensemble de définitions de `commonPropertiesId` fournit un tableau complet de contenus du fichier pour les besoins de recherches.

## 7.2 Spécification du rédacteur de fichier

Un rédacteur de fichier IPFIX DOIT agir comme un processus d'exportation IPFIX comme spécifié dans la [RFC5101], sauf comme modifié par le présent document. Ce paragraphe contient les spécifications pour les rédacteurs de fichier IPFIX dans toutes les situations ; les spécifications et recommandations de rédacteur de fichier pour les cas d'utilisation spécifiques se trouvent au paragraphe 7.3.

Les rédacteurs de fichier DEVRAIENT mémoriser les gabarits et options exigés pour décoder les données au sein du fichier lui-même, sauf si ils sont modifiés par les exigences d'un cas d'utilisation spécifique au paragraphe 7.3. De cette façon, un seul fichier IPFIX contient généralement une seule notion de session de transport comme défini par la [RFC5101].

Les rédacteurs de fichier DEVRAIENT émettre chaque ensemble de gabarits ou ensemble de gabarit d'options comme apparaissant dans le fichier avant tout ensemble de données décrit par les gabarits au sein de cet ensemble, pour s'assurer que le lecteur de fichier peut décoder tout ensemble de données sans attendre de traiter les gabarits ou gabarits d'options

suivants.

Les rédacteurs de fichier DEVRAIENT émettre les enregistrements de données décrits par les gabarits d'options pour apparaître dans le fichier avant tous les enregistrements de données qui dépendent des portées définies par ces options.

Les rédacteurs de fichier DEVRAIENT utiliser les retraits de gabarit pour supprimer des gabarits si des identifiants de gabarits doivent être réutilisés. Les retraits de gabarit NE DEVRAIENT PAS être utilisés si il n'est pas nécessaire de réutiliser les identifiants de gabarit.

Les rédacteurs de fichier DEVRAIENT écrire les messages IPFIX au sein d'un fichier IPFIX en ordre ascendant d'heure d'exportation.

Les rédacteurs de fichier PEUVENT écrire des enregistrements de données sur un fichier IPFIX dans tout ordre. Cependant, les rédacteurs de fichier qui écrivent des enregistrements de flux dans un fichier IPFIX dans l'ordre de flowStartTime ou de flowEndTime DEVRAIENT être cohérents avec cet ordre au sein de chaque fichier.

### 7.3 Cas d'utilisation spécifiques du rédacteur de fichier

Les spécifications de ce paragraphe s'appliquent à des situations spécifiques. Chaque sous paragraphe ci-dessous étend ou modifie la spécification de base du rédacteur de fichier du paragraphe 7.2. Les considérations sur la co-localisation d'un rédacteur de fichier avec les processus de collecte et processus de mesure IPFIX sont données, ainsi que les lignes directrices pour utiliser les fichiers IPFIX pour la mémorisation d'archivage, ou comme documents. Est aussi couverte l'utilisation de fichiers IPFIX dans l'essai et les diagnostics d'appareils IPFIX.

#### 7.3.1 Co-localisation d'un rédacteur de fichier avec un processus de collecte

Quand on co-localise un rédacteur de fichier avec un processus de collecte IPFIX pour la mémorisation d'archivage de données collectées dans les fichiers IPFIX comme décrit au paragraphe 6.1, les recommandations suivantes peuvent améliorer l'utilité des données mémorisées.

La façon la plus simple pour un rédacteur de fichier de mémoriser les données collectées dans une seule session de transport est de simplement écrire les messages IPFIX entrants dans un fichier IPFIX quand ils sont collectés. Cette approche a plusieurs inconvénients. D'abord, si le processus d'exportation original ne se conforme pas aux recommandations du paragraphe 7.2 à l'égard de l'ordre du gabarit et de l'enregistrement de données, le fichier écrit peut être difficile à utiliser ultérieurement ; dans ce cas, les rédacteurs de fichier PEUVENT réordonner les enregistrements reçus afin de s'assurer que les gabarits apparaissent avant les enregistrements de données qu'ils décrivent.

Un rédacteur de fichier co-localisé avec un processus de collecte qui commence à écrire des données à partir d'une session de transport en fonctionnement DEVRAIT écrire tous les gabarits actuellement actifs au sein de cette session de transport avant d'écrire aucun enregistrement de données qu'ils décrivent.

Aussi, les fichiers IPFIX résultants qui manquent des informations sur la session de transport IPFIX utilisée pour les exporter, comme les adresses réseau des processus d'exportation et de collecte et les protocoles utilisés pour les transporter. Dans ce cas, si les informations sur la session de transport sont exigées, le rédacteur de fichier DEVRAIT mémoriser une seule session de transport IPFIX dans un fichier IPFIX et DEVRAIT enregistrer les informations sur la session de transport en utilisant le gabarit d'options Détails de session d'exportation décrit au paragraphe 8.1.3.

Des informations supplémentaires par message PEUVENT être enregistrées par le rédacteur de fichier en utilisant le gabarit d'options Détails de message décrit au paragraphe 8.1.4. Les informations par message incluent l'heure à laquelle chaque message IPFIX a été reçu au processus de collecte, et peuvent être utilisées pour envoyer à nouveau les messages IPFIX tout en conservant le profil de trafic de plan de mesure original.

Quand on co-localise un rédacteur de fichier avec un processus de collecte, l'heure d'exportation de chaque message DEVRAIT être l'heure d'exportation du message reçu par le processus de collecte contenant le premier enregistrement de données dans le message. Noter que les rédacteurs de fichier qui mémorisent les données IPFIX collectées d'un processus de collecte IPFIX en utilisant SCTP comme protocole de transport DEVRAIENT entrelacer les messages provenant de plusieurs flux afin de préserver l'ordre de temps d'exportation, et DEVRAIENT réordonner les messages écrits comme nécessaire pour assurer que chaque ensemble de gabarits ou ensemble de gabarits d'options apparaît dans le fichier avant tout ensemble de données décrit par les gabarits au sein de cet ensemble. La remise en ordre de gabarits DOIT préserver la

séquence des ensembles de gabarits avec les retraits de gabarit afin d'assurer la cohérence des gabarits.

Noter que quand on ajoute des informations aux messages IPFIX reçus des processus de collecte (par exemple, Options somme de contrôle de message, Options détails de message) le rédacteur de fichier DEVRAIT étendre la longueur du message des données supplémentaires, si possible ; autrement, le message DEVRAIT être partagé en deux messages de taille approximativement égale alignés sur une frontière d'ensemble de données ou d'ensemble de gabarits dans le message original si possible ; autrement, le message DEVRAIT être partagé en deux messages de taille approximativement égale alignés sur une frontière d'enregistrement de données. Noter que, comme la taille maximum de segment (MSS, *Maximum Segment Size*) ou la MTU de la plupart des liaisons de réseau (1500 à 9000 pour les Ethernets courants) est plus petite que la taille maximum de message IPFIX (65 536) au sein d'un fichier IPFIX, on s'attend à ce que l'extension de longueur de message suffise dans la plupart des circonstances.

Un rédacteur de fichier co-localisé avec un processus de collecte NE DEVRAIT PAS signer un fichier comme spécifié au paragraphe 9.1 sauf si la session de transport sur laquelle les données ont été exportées était protégée via TLS ou DTLS, et si le processus de collecte était positivement identifié au processus d'exportation par son certificat. Voir le paragraphe 12.2 pour plus d'informations sur cette question.

### 7.3.2 Co-localisation d'un rédacteur de fichier avec un processus de mesure

Noter que les rédacteurs de fichier peuvent aussi être co-localisés directement avec les processus de mesure IPFIX, pour écrire directement les informations mesurées sur un disque sans processus IPFIX intermédiaire de collecte ou d'exportation. Cet arrangement peut être particulièrement utile quand on fournit des données à un environnement d'analyse avec un flux de travail fondé sur le fichier IPFIX, quand on fait des essais sur un processus de mesure en développement, ou quand l'authentification d'un processus de mesure est importante.

Quand on co-localise un rédacteur de fichier avec un processus de mesure, on notera que les éléments d'information associés aux processus d'exportation ou de collecte n'ont pas de signification, et NE DEVRAIT PAS apparaître dans le gabarit d'options Détails de session d'exportation décrit au paragraphe 8.1.3 ou le gabarit d'options Détails de message décrit au paragraphe 8.1.4.

Quand on co-localise un rédacteur de fichier avec un processus de mesure, l'heure d'exportation de chaque message DEVRAIT être l'heure à laquelle le premier enregistrement de données dans le message a été reçu du processus de mesure.

Noter que co-localiser un rédacteur de fichier avec un processus de mesure est la seule façon de fournir une authentification positive d'un processus de mesure par des signatures comme au paragraphe 9.1. Voir le paragraphe 12.2 pour plus d'informations sur cette question.

### 7.3.3 Utilisation de fichiers IPFIX pour la mémorisation d'archivage

Alors que dans le cas général, les rédacteurs de fichier devraient mémoriser une session de transport par fichier IPFIX, certaines applications qui mémorisent de grandes collections de données sur de longues périodes peuvent bénéficier de la capacité de traiter une collection de fichiers IPFIX comme une seule session de transport. Un rédacteur de fichier PEUT être configurable à écrire des données provenant d'une seule session de transport en plusieurs fichiers IPFIX ; cependant, les rédacteurs de fichier qui prennent en charge une telle option de configuration DOIVENT fournir une option de configuration pour prendre en charge le comportement de un fichier par session pour les besoins d'interopérabilité.

Les rédacteurs de fichier qui utilisent les fichiers IPFIX pour une mémorisation d'archivage DEVRAIENT prendre en charge la compression décrite à la Section 10.

### 7.3.4 Utilisation des fichiers IPFIX comme documents

Quand les fichiers IPFIX sont utilisés comme des documents, pour mémoriser un ensemble de flux pertinents pour l'interrogation, l'investigation, ou autres contextes courants, ou pour la publication d'ensembles de données de trafic pertinents pour des recherches sur le réseau, chaque fichier DOIT être lisible comme une seule session de transport, auto-contenue à côté de toute signature détachée comme décrit au paragraphe 9.1, et ne faisant aucune référence à des métadonnées mémorisées dans des fichiers séparés, afin d'assurer l'interopérabilité.

Quand on écrit des fichiers à utiliser comme des documents, les rédacteurs de fichier PEUVENT émettre des enregistrements de données spéciaux décrits par des gabarits d'options avant tous autres enregistrements de données dans le

fichier dans l'ordre suivant pour faciliter l'inspection et l'utilisation des documents par les lecteurs de fichier :

- o les enregistrements de fenêtre horaire décrits par le gabarit Options de fenêtre horaire de fichier comme défini au paragraphe 8.1.2 ; suivi par :
- o les enregistrements de type d'élément d'information comme décrit dans la [RFC5610] ; suivi par :
- o les définitions de `commonPropertiesId` comme décrites dans la [RFC5473] ; suivies par :
- o les enregistrements de détails de session d'exportation décrits par le gabarit d'options Détails de session d'exportation défini au paragraphe 8.1.3.

L'heure d'exportation de chaque message au sein d'un fichier utilisé comme document DEVRAIT être l'heure à laquelle le message a été écrit par le rédacteur de fichier.

Si un fichier IPFIX utilisé comme document utilise la technique décrite dans la [RFC5473] ET tous les gabarits non d'options dans le fichier contiennent l'élément d'information `commonPropertiesId`, un lecteur de fichier PEUT supposer que l'ensemble de définitions de `commonPropertiesId` fournit un tableau complet des contenus pour le fichier à des fins de recherches.

### 7.3.5 Utilisation des fichiers IPFIX pour des essais

Les fichiers IPFIX peuvent être utilisés pour essayer des processus de collecte IPFIX de deux façons. D'abord, les fichiers IPFIX peuvent être utilisés pour mémoriser des données de flux spécifique pour des essais de régression et de tension sur les collecteurs ; il n'y a pas de considérations particulières pour les fichiers IPFIX utilisés de cette façon.

Ensuite, les fichiers IPFIX sont utiles pour mémoriser des messages de référence qui ne se conforment pas au protocole IPFIX afin de vérifier le traitement d'erreur et le comportement de récupération des collecteurs. Bien sûr, les fichiers IPFIX destinés à être utilisés dans cette application PEUVENT nécessairement violer toutes les spécifications du présent document ou de la [RFC5101], et de tels fichiers NE DOIVENT PAS être transmis à des processus de collecte ou donnés en entrée aux lecteurs de fichier qui ne sont pas en essai.

Noter qu'un processus d'exportation IPFIX extrêmement simple peut être construit pour des essais simplement en lisant un fichier IPFIX et en le transmettant directement à un processus de collecte. De même, un processus de collecte extrêmement simple peut être construit pour des essais en acceptant simplement des connexions et/ou des messages IPFIX provenant de processus d'exportation et en écrivant un flux de messages de la session dans un fichier IPFIX.

### 7.3.6 Rédaction de fichiers IPFIX pour des diagnostics d'appareil

Les fichiers IPFIX peuvent être utilisés au débogage d'appareils qui utilisent des données de flux comme état interne, comme un format commun pour la représentation de tableaux de flux. Dans ces situations, l'élément d'information `opaqueOctets` peut être utilisé pour mémoriser des informations supplémentaires non codées IPFIX qui ne sont pas de flux (par exemple, des traces de pile, un état de processus, etc.) au sein du fichier IPFIX comme au paragraphe 11.1 ; les informations de tableau de flux IPFIX pourraient aussi être incorporées dans un plus large format de diagnostic propriétaire en utilisant des délimiteurs comme au paragraphe 11.2.

### 7.3.7 Manipulation de fichiers IPFIX

Pour de nombreuses applications, il peut se révéler utile que les mises en œuvre fournissent une fonction de manipulation des fichiers IPFIX ; par exemple, pour choisir des données dans un fichier, pour changer les gabarits utilisés au sein d'un fichier, ou pour partager ou joindre des données dans les fichiers. Un tel utilitaire devrait prendre un soin particulier pour s'assurer que son résultat reste un fichier IPFIX valide, en particulier par rapport aux gabarits et options, qui ont une portée de sessions de transport.

Toute opération qui partage un fichier en plusieurs fichiers DEVRAIT écrire tous les gabarits et options nécessaires dans chaque fichier résultant, et s'assurer que les options écrites sont valides pour chaque fichier résultant (par exemple, le gabarit Options de fenêtre temporelle au paragraphe 8.1.2). Toute opération qui joint plusieurs fichiers en un seul fichier devrait faire de même, en s'assurant de plus que les identifiants de gabarit n'entrent pas en collision, par l'utilisation d'identifiants de domaine d'observation différents ou en réécrivant l'identifiant de gabarit. La combinaison d'opérations peut aussi vouloir assurer que l'ordre désiré des enregistrements de flux est conservé.

7.4 Type de support des fichiers IPFIX

Le type de support pour les fichiers IPFIX est application/ipfix. Les informations d'enregistrement [RFC4288] pour ce type de support sont données dans la section des considérations relatives à l'IANA.

8. Spécification des métadonnées de format de fichier

Cette section définit les gabarits d'options utilisés pour les métadonnées de fichier IPFIX, et les éléments d'information qu'ils exigent.

8.1 Gabarits d'options recommandés pour les fichiers IPFIX

Les gabarits d'options suivants permettent aux flux de messages IPFIX de satisfaire les exigences mentionnées ci-dessus sans extension du format ou protocole de message. Ils sont définis dans les termes des éléments d'information existants définis dans la [RFC5102], des éléments d'information définis dans la [RFC5610], ainsi que des éléments d'information définis au paragraphe 8.2. Les rédacteurs et lecteurs de fichier IPFIX DEVRAIENT prendre en charge ces gabarits d'options comme défini ci-dessous.

De plus, les rédacteurs et lecteurs de fichier IPFIX DEVRAIENT prendre en charge les gabarits d'options définis dans la [RFC5610] afin de supporter l'auto-description d'éléments d'information spécifiques d'entreprise.

8.1.1 Gabarit d'options Somme de contrôle de message

Le gabarit d'options Somme de contrôle de message spécifie la structure d'un enregistrement de données pour attacher une somme de contrôle de message MD5 à un message IPFIX. Une somme de contrôle de message MD5 comme décrite PEUT être utilisée si l'intégrité des données est importante pour l'application mais la signature de fichier n'est pas disponible ou désirée. L'enregistrement de données décrit DOIT apparaître seulement une fois par message IPFIX, mais PEUT apparaître n'importe où au sein du message.

Ce gabarit d'options DEVRAIT contenir les éléments d'information (IE) suivants :

| IE                    | Description                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| messageScope [portée] | Marqueur notant que cette option s'applique à tout le message IPFIX ; le contenu est ignoré. Cet élément d'information DOIT être défini comme un champ Scope. |
| messageMD5Checksum    | Somme de contrôle MD5 du message IPFIX contenant.                                                                                                             |

8.1.2 Gabarit d'options de fenêtre temporelle de fichier

Le gabarit Options de fenêtre temporelle de fichier spécifie la structure d'un enregistrement de données pour attacher une fenêtre temporelle à un fichier IPFIX ; cet enregistrement de données est appelé un enregistrement de fenêtre temporelle. Un enregistrement de fenêtre temporelle définit l'heure de début du flux et l'heure de fin de flux des enregistrements de flux au sein d'un fichier. Un et seulement un enregistrement de fenêtre temporelle PEUT apparaître au sein d'un fichier IPFIX si les informations de fenêtre temporelle sont disponibles ; un rédacteur de fichier NE DOIT PAS écrire plus d'un enregistrement de fenêtre temporelle dans un fichier IPFIX. Un rédacteur de fichier qui écrit un enregistrement de fenêtre temporelle dans un fichier NE DOIT PAS écrire de flux avec une heure de début précédant le début de la fenêtre ou une heure de fin après la fin de la fenêtre dans ce fichier.

Ce gabarit d'options DEVRAIT contenir les éléments d'information (IE) suivants :

| IE                    | Description                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sessionScope [portée] | Marqueur notant que cette option s'applique à toute la session de transport IPFIX (c'est-à-dire, le fichier IPFIX dans le cas courant) ; le contenu est ignoré. Cet élément d'information DOIT être défini comme un champ Scope.                                                                               |
| minFlowStart*         | Exactement une de minFlowStartSeconds, minFlowStartMilliseconds, minFlowStartMicroseconds, ou minFlowStartNanoseconds DEVRAIT correspondre à la précision de l'élément d'information maxFlowEnd* accompagnant. C'est l'heure de début du premier flux dans la session de transport (c'est-à-dire, le fichier). |
| maxFlowEnd*           | Exactement une de maxFlowEndSeconds, maxFlowEndMilliseconds, maxFlowEndMicroseconds,                                                                                                                                                                                                                           |

ou maxFlowEndNanoseconds DEVRAIT correspondre à la précision de l'élément d'information minFlowStart\* accompagnant. C'est l'heure de fin du dernier flux dans la session de transport (c'est-à-dire, le fichier).

### 8.1.3 Gabarit d'options de détails d'exportation de session

Le gabarit d'options Détails de session d'exportation spécifie la structure d'un enregistrement de données pour enregistrer les détails d'une session de transport IPFIX dans un fichier IPFIX. Il est destiné à être utilisé à mémoriser une seule session de transport IPFIX complète dans un seul fichier IPFIX. L'enregistrement de données décrit DEVRAIT apparaître seulement une fois dans un fichier IPFIX donné.

Ce gabarit d'options DEVRAIT contenir au moins les éléments d'information suivants, sous réserve de leur applicabilité comme noté dans chaque élément d'information :

| IE                         | Description                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sessionScope [portée]      | Marqueur notant que cette option s'applique à toute la session de transport IPFIX (c'est-à-dire, généralement le fichier IPFIX) ; le contenu est ignoré. Cet élément d'information DOIT être défini comme champ Portée.                                                                                                                      |
| exporterIPv4Address        | Adresse IPv4 du processus d'exportation IPFIX d'où les messages dans cette session de transport ont été reçus. Présent seulement pour les processus d'exportation avec une interface IPv4. Pour des associations SCTP multi-rattachements, cela DEVRAIT être l'adresse principale de point d'extrémité de chemin du processus d'exportation. |
| exporterIPv6Address        | Adresse IPv6 du processus d'exportation IPFIX d'où les messages dans cette session de transport ont été reçus. Présent seulement pour les processus d'exportation avec une interface IPv6. Pour des associations SCTP multi-rattachements, cela DEVRAIT être l'adresse principale de point d'extrémité de chemin du processus d'exportation. |
| exporterTransportPort      | Accès de source d'où les messages de cette session de transport ont été reçus.                                                                                                                                                                                                                                                               |
| exporterCertificate        | Certificat utilisé par le processus d'exportation IPFIX d'où ont été reçus les messages de cette session de transport. Présent seulement pour les sessions de transport protégées par TLS ou DTLS.                                                                                                                                           |
| collectorIPv4Address       | Adresse IPv4 du processus de collecte IPFIX qui a reçu les messages dans cette session de transport. Présent seulement pour des processus de collecte avec une interface IPv4. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte.                 |
| collectorIPv6Address       | Adresse IPv6 du processus de collecte IPFIX qui a reçu les messages dans cette session de transport. Présent seulement pour des processus de collecte avec une interface IPv6. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte.                 |
| collectorTransportPort     | Accès de destination sur lequel ont été reçus les messages dans cette session de transport.                                                                                                                                                                                                                                                  |
| collectorTransportProtocol | Identifiant de protocole IP du protocole de transport utilisé pour transporter les messages au sein de cette session de transport.                                                                                                                                                                                                           |
| collectorProtocolVersion   | Version du protocole d'exportation utilisé pour transporter les messages au sein de cette session de transport. Applicable seulement dans des environnements de collecte mixte NetFlow V9-IPFIX quand on mémorise les données NetFlow V9 dans les messages IPFIX (Appendice B).                                                              |
| collectorCertificate       | Certificat utilisé par le processus de collecte IPFIX qui a reçu les messages dans cette session de transport. Présent seulement pour les sessions de transport protégées par TLS ou DTLS.                                                                                                                                                   |
| minExportSeconds           | Heure d'exportation du premier message de la session de transport.                                                                                                                                                                                                                                                                           |
| maxExportSeconds           | Heure d'exportation du dernier message de la session de transport.                                                                                                                                                                                                                                                                           |

### 8.1.4 Gabarit d'options de détails de message

Le gabarit d'options Détails de message spécifie la structure d'un enregistrement de données pour attacher des détails d'exportation supplémentaires à un message IPFIX. Ces détails incluent l'heure de réception du message et des informations sur l'infrastructure d'exportation et de collecte utilisée pour transporter le message. Ce gabarit d'options permet aussi la mémorisation des métadonnées d'exportation fournies par le gabarit d'options Détails de session d'exportation, pour mémoriser les informations provenant de plusieurs sessions de transport dans le même fichier IPFIX.

Ce gabarit d'options DEVRAIT contenir au moins les éléments d'information suivants, sous réserve de leur applicabilité comme notée pour chaque élément d'information. Noter que quand il est utilisé conjointement avec le gabarit d'options

Détails de session d'exportation, quand on mémorise une seule session de transport IPFIX complète dans un fichier IPFIX, ce gabarit d'options DEVRAIT contenir seulement les éléments d'information `collectionTimeMilliseconds` et `messageScope`, et l'élément d'information `exportSctpStreamId` pour les messages transportés via SCTP.

| IE                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>messageScope [portée]</code>      | Marqueur notant que cette option s'applique à tout le message IPFIX ; le contenu est ignoré. Cet élément d'information DOIT être défini comme un champ Portée.                                                                                                                                                                                                                                             |
| <code>collectionTimeMilliseconds</code> | Temps absolu auquel ce message a été reçu par le processus de collecte IPFIX.                                                                                                                                                                                                                                                                                                                              |
| <code>exporterIPv4Address</code>        | Adresse IPv4 du processus d'exportation IPFIX d'où a été reçu ce message. Présent seulement pour un processus d'exportation avec une interface IPv4, et si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte. |
| <code>exporterIPv6Address</code>        | Adresse IPv6 du processus d'exportation IPFIX d'où a été reçu ce message. Présent seulement pour un processus d'exportation avec une interface IPv6, et si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte. |
| <code>exporterTransportPort</code>      | Accès de source d'où ce message a été reçu. Présent seulement si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation.                                                                                                                                                                                                                                         |
| <code>exporterCertificate</code>        | Certificat utilisé par le processus d'exportation IPFIX d'où a été reçu ce message. Présent seulement pour les sessions de transport protégées par TLS ou DTLS.                                                                                                                                                                                                                                            |
| <code>collectorIPv4Address</code>       | Adresse IPv4 du processus de collecte IPFIX qui a reçu ce message. Présent seulement pour des processus de collecte avec une interface IPv4, et si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte.         |
| <code>collectorIPv6Address</code>       | Adresse IPv6 du processus de collecte IPFIX qui a reçu ce message. Présent seulement pour des processus de collecte avec une interface IPv6, et si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation. Pour les associations SCTP multi-rattachements, ce DEVRAIT être l'adresse principale du point d'extrémité de chemin du processus de collecte.         |
| <code>collectorTransportPort</code>     | Accès de destination sur lequel ce message a été reçu. Présent seulement si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation.                                                                                                                                                                                                                              |
| <code>collectorTransportProtocol</code> | Identifiant de protocole IP du protocole de transport utilisé pour transporter ce message. Présent seulement si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation.                                                                                                                                                                                          |
| <code>collectorProtocolVersion</code>   | Version du protocole d'exportation utilisé pour transporter ce message. Présent seulement si nécessaire et si cette information n'est pas disponible via le gabarit d'options Détails de session d'exportation.                                                                                                                                                                                            |
| <code>collectorCertificate</code>       | Certificat utilisé par le processus de collecte IPFIX qui a reçu ce message. Présent seulement pour les sessions de transport protégées par TLS ou DTLS.                                                                                                                                                                                                                                                   |
| <code>exportSctpStreamId</code>         | Flux SCTP utilisé pour transporter ce message. Présent seulement si le message était transporté via SCTP.                                                                                                                                                                                                                                                                                                  |

## 8.2 Éléments d'information recommandés pour les fichiers IPFIX

Les éléments d'information suivants sont utilisés par les gabarits d'options du paragraphe 8.1 pour permettre que les flux de messages IPFIX satisfassent les exigences mentionnées ci-dessus sans extension du protocole. Les rédacteurs et lecteurs de fichier IPFIX DEVRAIENT prendre en charge ces éléments d'information comme défini ci-dessous.

De plus, les rédacteurs et lecteurs de fichier IPFIX DEVRAIENT prendre en charge les éléments d'information définis dans la [RFC5610] afin de supporter l'auto-description des éléments d'information.

### 8.2.1 `collectionTimeMilliseconds`

Description : horodatage absolu auquel les données au sein de la portée contenant cet élément d'information ont été reçues par un processus de collecte. Cet élément d'information DEVRAIT être lié à son message IPFIX contenant via des options IPFIX et l'élément d'information `messageScope`, comme défini ci-dessous.

Type de données abstrait : dateTimeMilliseconds  
ElementId : 258  
Statut : courant  
Unités : millisecondes

### 8.2.2 collectorCertificate

Description : certificat X.509 complet, codé en format DER ASN.1, utilisé par le collecteur quand les messages IPFIX ont été transmis en utilisant TLS ou DTLS. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via un enregistrement d'options et l'élément d'information sessionScope, ou à son message IPFIX contenant via un enregistrement d'options et l'élément d'information messageScope.

Type de données abstrait : octetArray  
ElementId : 274  
Statut : courant

### 8.2.3 exporterCertificate

Description : certificat X.509 complet, codé en format DER ASN.1, utilisé par le collecteur quand les messages IPFIX ont été transmis en utilisant TLS ou DTLS. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via un enregistrement d'options et l'élément d'information sessionScope, ou à son message IPFIX contenant via un enregistrement d'options et l'élément d'information messageScope.

Type de données abstrait : octetArray  
ElementId : 275  
Statut : courant

### 8.2.4 exportSctpStreamId

Description : valeur de l'identifiant de flux SCTP utilisé par le processus d'exportation pour exporter les données de message IPFIX. Elle est portée dans le champ Identifiant de flux de l'en-tête du tronçon SCTP DATA qui contient le ou les messages IPFIX.

Type de données abstrait : unsigned16  
Signification du type de données : identifiant  
ElementId : 259  
Statut : courant

### 8.2.5 maxExportSeconds

Description : temps absolu d'exportation du dernier message IPFIX au sein de la portée contenant cet élément d'information. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via les options IPFIX et l'élément d'information sessionScope.

Type de données abstrait : dateTimeSeconds  
ElementId : 260  
Statut : courant  
Unités : secondes

### 8.2.6 maxFlowEndMicroseconds

Description : dernier horodatage absolu du dernier paquet au sein de tout flux dans la portée qui contient cet élément d'information, arrondi à la microseconde supérieure si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via les options IPFIX et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport contenant des enregistrements de flux avec des éléments d'information d'horodatage d'une précision à la microseconde (ou meilleure).

Type de données abstrait : dateTimeMicroseconds

ElementId : 268  
Statut : courant  
Unités : microsecondes

### 8.2.7 maxFlowEndMilliseconds

Description : dernier horodatage absolu du dernier paquet au sein de tout flux dans la portée de cet élément d'information, arrondi à la milliseconde si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via les options IPFIX et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport qui contiennent des enregistrements de flux d'éléments d'information d'horodatage d'une précision de milliseconde (ou meilleure).

Type de données abstrait : dateTimeMilliseconds  
ElementId : 269  
Statut : courant  
Unités : millisecondes

### 8.2.8 maxFlowEndNanoseconds

Description : dernier horodatage absolu du dernier paquet au sein de tout flux dans la portée de cet élément d'information. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via les options IPFIX et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport qui contiennent des enregistrements de flux d'éléments d'information d'horodatage d'une précision de nanoseconde.

Type de données abstrait : dateTimeNanoseconds  
ElementId : 270  
Statut : courant  
Unités : nanosecondes

### 8.2.9 maxFlowEndSeconds

Description : dernier horodatage absolu du dernier paquet au sein de tout flux dans la portée de cet élément d'information, arrondi à la seconde si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via les options IPFIX et l'élément d'information sessionScope.

Type de données abstrait : dateTimeSeconds  
ElementId : 261  
Statut : courant  
Unités : secondes

### 8.2.10 messageMD5Checksum

Description : somme de contrôle MD5 du message IPFIX contenant cet enregistrement. Cet élément d'information DEVRAIT être lié à son message IPFIX contenant via un enregistrement d'options et l'élément d'information messageScope, comme défini ci-dessous, et DEVRAIT apparaître seulement une fois dans un message IPFIX donné. Pour calculer la valeur de cet élément d'information, on met d'abord en antémémoire le message IPFIX contenant, et on règle la valeur de cet élément d'information tout à zéro. On calcule ensuite la somme de contrôle MD5 de la mémoire tampon résultante comme défini dans la [RFC1321], on place la valeur résultante dans cet élément d'information, et on exporte le message en mémoire tampon. Cet élément d'information est entendu seulement comme une simple somme de contrôle ; donc la résistance à la collision et l'agilité d'algorithme ne sont pas exigées, et MD5 est un résumé de message approprié.

Type de données abstrait : octetArray (16 octets)  
ElementId : 262  
Statut : courant  
Référence : Algorithme MD5 de résumé de message [RFC1321]

### 8.2.11 messageScope

Description : la présence de cet élément d'information comme portée dans un gabarit d'options signifie que les options décrites par le gabarit s'appliquent à tout le message IPFIX qui les contient. Il est défini pour un message général de portée des options, et proposé spécifiquement pour permettre le rattachement de la somme de contrôle et des informations de collecte à un message via les options IPFIX. La valeur de cet élément d'information DOIT être écrite à 0 par le rédacteur de fichier ou processus d'exportation. La valeur de cet élément d'information DOIT être ignorée par le lecteur de fichier ou le processus de collecte.

Type de données abstrait : unsigned8

ElementId : 263

Statut : courant

Gamme : la gamme valide est 0-0

### 8.2.12 minExportSeconds

Description : heure absolue d'exportation du premier message IPFIX dans la portée contenant cet élément d'information. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenante via un enregistrement d'options et l'élément d'information sessionScope.

Type de données abstrait : dateTimeSeconds

ElementId : 264

Statut : courant

Unités : secondes

### 8.2.13 minFlowStartMicroseconds

Description : premier horodatage absolu du premier paquet au sein de tout flux dans la portée contenant cet élément d'information, arrondi à la microseconde inférieure si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenante via un enregistrement d'options et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport contenant des enregistrements de flux d'éléments d'information d'horodatage à la précision de la microseconde (ou meilleure).

Type de données abstrait : dateTimeMicroseconds

ElementId : 271

Statut : courant

Unités : microsecondes

### 8.2.14 minFlowStartMilliseconds

Description : premier horodatage absolu du premier paquet au sein de tout flux dans la portée contenant cet élément d'information, arrondi à la milliseconde inférieure si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenante via un enregistrement d'options et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport contenant des enregistrements de flux d'éléments d'information d'horodatage à la précision de la milliseconde (ou meilleure).

Type de données abstrait : dateTimeMilliseconds

ElementId : 272

Statut : courant

Unités : millisecondes

### 8.2.15 minFlowStartNanoseconds

Description : premier horodatage absolu du premier paquet au sein de tout flux dans la portée contenant cet élément d'information. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenante via un enregistrement d'options et l'élément d'information sessionScope. Cet élément d'information DEVRAIT être utilisé seulement dans les sessions de transport contenant des enregistrements de flux d'éléments d'information d'horodatage à la précision de la nanoseconde.

Type de données abstrait : dateTimeNanoseconds

ElementId : 273  
Statut : courant  
Unités : nanosecondes

### 8.2.16 minFlowStartSeconds

Description : premier horodatage absolu du premier paquet au sein de tout flux dans la portée contenant cet élément d'information, arrondi à la seconde inférieure si nécessaire. Cet élément d'information DEVRAIT être lié à sa session de transport IPFIX contenant via un enregistrement d'options et l'élément d'information sessionScope.

Type de données abstrait : dateTimeSeconds  
ElementId : 265  
Statut : courant  
Unités : secondes

### 8.2.17 opaqueOctets

Description : cet élément d'information est utilisé pour encapsuler des données non IPFIX dans un flux de messages IPFIX, afin de permettre à un processeur de données non IPFIX de mémoriser en ligne un flux de données au sein d'un fichier IPFIX. Un processus de collecte ou rédacteur de fichier NE DOIT PAS essayer d'interpréter ces données binaires. Cet élément d'information diffère des octets de bourrage car son contenu est significatif dans certains contextes non IPFIX, alors que le contenu des paddingOctets DOIT être 0x00 et est destiné seulement à l'alignement des éléments d'information.

Type de données abstrait : octetArray  
ElementId : 266  
Statut : courant

### 8.2.18 sessionScope

Description : la présence de cet élément d'information comme portée dans un gabarit d'options signifie que les options décrites par le gabarit s'appliquent à la session de transport IPFIX qui les contient. Noter que comme toutes les options ont implicitement pour portée la session de transport et le domaine d'observation, cet élément d'information est équivalent à une portée "nulle". Il est défini pour une portée d'options de session d'objet général, et proposé spécifiquement pour permettre le rattachement d'une fenêtre temporelle et des informations de collecte à un fichier IPFIX via les options IPFIX. La valeur de cet élément d'information DOIT être écrite comme 0 par le rédacteur de fichier ou le processus d'exportation. La valeur de cet élément d'information DOIT être ignorée par le lecteur de fichier ou le processus de collecte.

Type de données abstrait : unsigned8  
ElementId : 267  
Statut : courant  
Gamme : la gamme valide est 0-0

## 9. Signature et chiffrement des fichiers IPFIX

Afin d'assurer l'intégrité des fichiers IPFIX et l'identité des rédacteurs de fichier IPFIX, les rédacteurs de fichier et les lecteurs de fichier DEVRAIENT fournir une méthode interoperable et facilement mise en œuvre pour signer les fichiers IPFIX, et vérifier ces signatures. Cette section spécifie une de ces méthodes via des signatures détachées de CMS.

Noter que bien que la CMS spécifie un format d'encapsulation qui peut être utilisé pour le chiffrement ainsi que la signature, aucune méthode n'est spécifiée pour l'encapsulation pour la protection de la confidentialité. On suppose que les exigences spécifiques d'application ou de processus outrepassent le besoin d'interopérabilité pour les fichiers chiffrés.

### 9.1 Signatures détachées de CMS

La syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*) [RFC5652] définit une syntaxe

d'encapsulation pour la protection des données, utilisée pour signer numériquement, authentifier, ou chiffrer un contenu de message arbitraire. La CMS peut aussi être utilisée pour créer des signatures détachées, dans lesquelles la signature est mémorisée dans un fichier séparé. Cet arrangement maximise l'interopérabilité, car les lecteurs de fichier qui ne connaissent pas les signatures détachées de CMS et n'ont pas d'exigence pour elles peuvent simplement les ignorer ; le contenu du fichier IPFIX lui-même est inchangé par la signature.

Le fichier de signature détaché pour un fichier IPFIX DEVRAIT être mémorisé, transporté, ou autrement rendu disponible (par exemple, par FTP ou HTTP) avec le fichier IPFIX signé, avec le même nom de fichier que le fichier IPFIX, sauf que l'extension de fichier ".p7s" est ajoutée à la fin, conformément à la convention de dénomination de la [RFC3851].

Dans la signature détachée, le type de CMS ContentInfo DOIT toujours être présent, et il DOIT encapsuler le type de contenu de CMS SignedData, qui à son tour NE DOIT PAS encapsuler le contenu signé du fichier IPFIX. La signature détachée de CMS est résumée comme suit :

```
ContentInfo {
  contentType  id-signedData,                -- (1.2.840.113549.1.7.2)
  content      SignedData
}

SignedData {
  version      CMSVersion,                  -- toujours réglé à 3
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo EncapsulatedContentInfo,
  certificates  CertificateSet,              -- certificats du rédacteur de fichier
  crls          CertificateRevocationLists,  -- facultatif
  signerInfos   SET OF SignerInfo           -- un seul signataire
}

SignerInfo {
  version      CMSVersion,                  -- toujours réglé à 3
  sid          SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttrs  SignedAttributes,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature     SignatureValue,
  unsignedAttrs UnsignedAttributes
}

EncapsulatedContentInfo {
  eContentType  id-data,                    -- (1.2.840.113549.1.7.1)
  eContent      OCTET STRING                -- toujours absent
}
```

Les détails du contenu de chaque encapsulation de CMS sont précisés dans les paragraphes suivants.

### 9.1.1 ContentInfo

La [RFC5652] exige que l'encapsulation la plus externe soit ContentInfo ; les champs de ContentInfo sont comme suit :

**contentType** : type du contenu associé. Pour le fichier de signature détachée, le type encapsulé est toujours SignedData, de sorte que l'identifiant d'objet id-signedData (1.2.840.113549.1.7.2) DOIT être présent dans ce champ.

**content** : un contenu SignedData, détaillé au paragraphe 9.1.2.

### 9.1.2 SignedData

Le type de contenu SignedData contient la signature du fichier IPFIX et des informations pour aider à la validation ; les champs de SignedData sont comme suit :

version : DOIT être 3.

digestAlgorithms : collection d'identifiants de fonctions de hachage unidirectionnelles. Elle DOIT contenir l'identifiant utilisé par le rédacteur de fichier pour générer la signature numérique.

encapContentInfo : contenu signé, incluant un identifiant de type de contenu. Comme une signature détachée est créée, il n'encapsule pas le fichier IPFIX. EncapsulatedContentInfo est détaillé au paragraphe 9.1.4.

certificates : collection de certificats. Il DEVRAIT inclure le certificat X.509 nécessaire pour valider le fichier de la signature numérique. Les certificats d'autorité de certification (CA) et de rédacteur de fichier DOIVENT se conformer au profil de certificat spécifié dans la [RFC5280].

crls : collection facultative de listes de révocation de certificats (CRL). Elle NE DEVRAIT PAS contenir de CRL ; toute CRL présente DOIT se conformer au profil de certificat spécifié dans la [RFC5280].

signerInfos : collection d'informations par signataire ; cela identifie le rédacteur de fichier. Plus d'un SignerInfo PEUT apparaître pour faciliter les transitions entre clés ou algorithmes. Le type SignerInfo est détaillé au paragraphe 9.1.3.

### 9.1.3 SignerInfo

Le type SignerInfo identifie le rédacteur de fichier ; les champs de SignerInfo sont comme suit :

version : DOIT être 3.

sid : identifie la clé publique du rédacteur de fichier. Cet identifiant DOIT correspondre à la valeur incluse dans l'extension de certificat subjectKeyIdentifier sur le certificat X.509 du rédacteur de fichier.

digestAlgorithm : identifie la fonction de hachage unidirectionnelle et les paramètres associés utilisés pour générer la signature.

signedAttrs : ensemble facultatif d'attributs qui sont signés avec le contenu.

signatureAlgorithm : identifie l'algorithme de signature numérique et les paramètres associés utilisés pour générer la signature.

signature : signature numérique du fichier associé.

unsignedAttrs : ensemble facultatif d'attributs qui ne sont pas signés.

### 9.1.4 EncapsulatedContentInfo

La structure EncapsulatedContentInfo contient un identifiant de type de contenu. Comme une signature détachée est créée, elle n'encapsule pas le fichier IPFIX. Les champs de EncapsulatedContentInfo sont comme suit :

eContentType : identifiant d'objet qui spécifie de façon univoque le type de contenu. Le type de contenu associé au fichier IPFIX DOIT être id-data (1.2.840.113549.1.7.1).

eContent : champ facultatif contenant le contenu signé. Comme c'est une signature détachée, eContent DOIT être absent.

## 9.2 Résilience à l'erreur de chiffrement

Noter que des erreurs d'un seul bit dans le flux de données chiffrées peuvent résulter en de plus grosses erreurs dans le flux de données déchiffrées, selon le schéma de chiffrement utilisé.

Dans les applications (par exemple, mémorisation d'archivage) dans lesquelles la résilience à l'erreur est très importante, les rédacteurs de fichier DEVRAIENT utiliser un schéma de chiffrement qui puisse se resynchroniser après des erreurs de bits. Un exemple courant est un chiffrement de bloc en mode chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*). Dans ce cas, les rédacteurs de fichier PEUVENT aussi utiliser le gabarit d'options Somme de contrôle de message pour attacher une somme de contrôle à chaque message IPFIX dans le fichier IPFIX, afin de prendre en charge la reconnaissance

des erreurs dans les données déchiffrées.

## 10. Compression des fichiers IPFIX

Les données de mesure de trafic du réseau sont généralement très compressibles. Les gabarits IPFIX tendent à accroître le contenu d'information par enregistrement en n'exigeant pas l'exportation des champs non pertinents ou non présents dans les enregistrements, et la technique décrite dans la [RFC5473] réduit aussi l'exportation d'informations redondantes. Cependant, même avec ces techniques, la compression généralisée peut diminuer significativement les exigences de mémorisation ; donc, les rédacteurs de fichier IPFIX et les lecteurs de fichier DEVRAIENT prendre en charge la compression comme décrite dans cette section.

### 10.1 Formats de compression pris en charge

Les fichiers IPFIX prennent en charge deux formats de compression d'encapsulation : bzip2 [bzip2] et gzip [RFC1952]. bzip2 fournit une meilleure compression que gzip et, comme algorithme de compression de bloc, de meilleures caractéristiques de récupération d'erreur, au prix d'une compression plus lente. gzip est potentiellement un meilleur choix quand le temps de compression est un problème. Ces deux algorithmes et formats d'encapsulation ont été choisis pour leur large diffusion et leur facilité de mise en œuvre.

Les rédacteurs et lecteurs de fichier IPFIX qui prennent en charge la compression DOIVENT prendre en charge bzip2, et DEVRAIT prendre en charge gzip.

### 10.2 Reconnaissance de la compression chez le lecteur de fichier

bzip2, gzip, et les fichiers IPFIX non compressés ont des numéros magiques distincts. Les lecteurs de fichier IPFIX DEVRAIENT utiliser ces numéros magiques pour déterminer quelle compression, si il en est, est utilisée pour un fichier IPFIX, et invoquer la décompression appropriée. Les fichiers bzip2 sont identifiés par la chaîne initiale de trois octets 0x42, 0x5A, 0x68 ("BZh"). Les fichiers gzip sont identifiés par la chaîne initiale de deux octets 0x1F, 0x8B. Les fichiers IPFIX sont identifiés par la chaîne initiale de deux octets 0x00, 0x0A ; ce sont les octets de version de l'en-tête du premier message IPFIX dans le fichier.

### 10.3 Résilience à l'erreur de compression

La compression au niveau du fichier, comme le chiffrement, n'est pas particulièrement résiliente aux erreurs ; dans le pire des cas, une erreur d'un seul bit dans un fichier de flux compressé pourrait résulter en la perte du fichier entier.

Comme les algorithmes de compression de bloc qui prennent en charge l'identification et l'isolement de blocs contenant des erreurs limitent l'impact des erreurs sur la possibilité de récupérer les données compressées, l'utilisation de bzip2 dans les applications où la résilience à l'erreur est importante est RECOMMANDÉE.

Comme la limite de bloc d'un fichier IPFIX à blocs compressés peut tomber au milieu d'un message IPFIX, la resynchronisation d'un flux de messages IPFIX par un lecteur de fichier après une erreur de compression exige une certaine attention. Le début d'un message IPFIX peut être identifié par sa signature d'en-tête (le champ Version de l'en-tête de message, 0x00 0x0A, suivi par une longueur de message de 16 bits) mais chercher simplement la première occurrence du champ Version est insuffisant, car ces deux octets peuvent survenir dans un gabarit ou ensemble de données IPFIX valide.

Donc, on spécifie l'algorithme suivant pour que les lecteurs de fichier resynchronisent un flux de messages IPFIX après avoir sauté un bloc compressé contenant des erreurs :

1. Chercher après l'erreur la première occurrence de la chaîne d'octets 0x00, 0x0A (le champ Version de l'en-tête du message IPFIX).
2. Traiter ce champ comme le début d'un message IPFIX candidat. Lire les deux octets suivant le champ Version comme la longueur de message, et chercher ce décalage à partir du début du message IPFIX candidat.
3. Si les deux premiers octets après le message IPFIX candidat sont 0x00, 0x0A (c'est-à-dire, le champ Version de l'en-tête du message IPFIX du prochain message dans le flux) ou si la fin de fichier est atteinte précisément à la fin du message IPFIX candidat, on supposera que le message IPFIX candidat est valide, et on commence à lire le fichier

IPFIX à partir du début du message IPFIX candidat.

4. Sinon, ou si la recherche atteint la fin de fichier ou un autre bloc contenant des erreurs avant de trouver la fin du message candidat, revenir à l'étape 1, en commençant la recherche des deux octets à partir du début du message IPFIX candidat.

L'algorithme ci-dessus va improprement identifier un non message comme un message dans approximativement 1 fois sur  $2^{32}$ , en supposant des données IPFIX aléatoires. Il peut être étendu à considérer plusieurs messages IPFIX candidats afin d'augmenter la fiabilité.

Dans des applications (par exemple, mémorisation d'archivage) dans lesquelles la résilience à l'erreur est très importante, les rédacteurs de fichier DEVRAIENT utiliser des algorithmes de compression de bloc, et PEUVENT tenter d'aligner les messages IPFIX au sein de blocs de compression pour faciliter la resynchronisation après des erreurs. Les lecteurs de fichier DEVRAIENT utiliser l'algorithme de resynchronisation ci-dessus pour minimiser les pertes de données dues à des erreurs de compression.

## 11. Stratégies recommandées d'intégration de fichier

Cette section décrit les méthodes pour intégrer les données de fichier IPFIX avec d'autres formats de fichier.

### 11.1 Encapsulation de données non IPFIX dans les fichiers IPFIX

Parfois, il peut être utile d'exporter ou mémoriser des données non IPFIX en ligne dans un fichier IPFIX ou un flux de messages. Pour faire cela proprement, ces données doivent être encapsulées dans des messages IPFIX afin qu'un lecteur de fichier IPFIX ou un processus de collecte puisse les traiter sans qu'il soit besoin de les interpréter. En même temps, ces données ne doivent pas être changées durant la transmission ou la mémorisation. L'élément d'information opaqueOctets, défini au paragraphe 8.2.17, est fourni pour cette encapsulation.

Le traitement des données non IPFIX encapsulées est laissé à des mécanismes de traitement séparés qui peuvent identifier les données non IPFIX encapsulées dans un flux de messages IPFIX, mais n'ont pas besoin d'avoir d'autres capacités de traitement IPFIX, sauf la capacité de sauter tous les messages IPFIX qui n'encapsulent pas de données non IPFIX.

Le gabarit d'options Somme de contrôle de message, décrit au paragraphe 8.1.1, peut être utilisé comme mécanisme uniforme pour identifier des erreurs au sein de données encapsulées.

Noter que ce mécanisme peut seulement encapsuler des objets de données jusqu'à 65 515 octets de long. Si l'espace disponible dans un message IPFIX n'est pas suffisant pour la quantité de données à encapsuler, alors les données doivent être coupées en plus petits segments qui sont encapsulés dans des messages IPFIX consécutifs. Toute structuration ou sémantique supplémentaire des données brutes sort du domaine d'application de IPFIX et doit être mise en œuvre au sein des données binaires elles-mêmes encapsulées. De plus, le lecteur de fichier IPFIX ne peut pas supposer que les données brutes encapsulées ont un format spécifique.

### 11.2 Encapsulation de fichiers IPFIX dans d'autres formats de fichier

Par conséquent, il peut aussi être utile d'inverser l'encapsulation, c'est-à-dire, d'exporter ou mémoriser les données IPFIX en ligne au sein d'un fichier ou flux de données non IPFIX. Cela a un sens quand les autres formats de fichier ne sont pas compatibles avec l'encapsulation décrite au paragraphe 11.1. Généralement parlant, cette encapsulation va être spécifique du format du fichier contenant. Par exemple, les fichiers IPFIX peuvent être incorporée dans des éléments XML en utilisant un codage hexadécimal ou Base64, ou dans des fichiers binaires bruts en utilisant des délimiteurs de début et de fin ou une forme de codage de longueur courante. Comme il y a ici autant d'encapsulations potentielles qu'il y a de formats de fichier potentiels, les spécificités de chacune sortent du domaine d'application de cette spécification.

## 12. Considérations sur la sécurité

La section des considérations sur la sécurité de la [RFC5101], sur laquelle le format de fichier IPFIX est fondé, est largement concernée par la bonne application de TLS et DTLS pour assurer la confidentialité et l'intégrité quand on exporte

des messages IPFIX. Par analogie, le présent document spécifie l'utilisation des signatures détachées de CMS [RFC5652] pour fournir une protection équivalente de l'intégrité à TLS et DTLS au paragraphe 9.1. Cependant, à côté de simplement appliquer la CMS pour les signatures, il y a plusieurs questions de sécurité qui doivent être considérées dans certaines circonstances ; elles sont couvertes dans les paragraphes qui suivent.

## 12.1 Relations entre fichier IPFIX et chiffrement de transport

Le protocole sous-jacent utilisé pour échanger les informations qui vont être mémorisées en utilisant le format proposé dans ce document doit aussi appliquer les procédures appropriées pour garantir l'intégrité et la confidentialité des informations exportées. Des telles questions sont traitées dans la [RFC5101]. Spécifiquement, les fichiers IPFIX qui mémorisent des données tirées d'un processus de collecte IPFIX en utilisant TLS ou DTLS pour la sécurité du transport DEVRAIENT être signés comme au paragraphe 9.1 et DEVRAIENT être chiffrés hors bande ; la mémorisation de telles données de flux sans chiffrement peut soulever une potentielle rupture de confidentialité. À l'inverse, les données de flux considérés comme assez sensibles pour exiger le chiffrement dans la mémorisation qui est ensuite transmise en utilisant IPFIX DEVRAIENT être transmises en utilisant TLS ou DTLS pour la sécurité du transport.

## 12.2 Assertions de bout en bout pour les fichiers IPFIX

Noter qu'alors que TLS et la CMS fournissent toutes deux la capacité de signer une session de transport IPFIX ou un fichier IPFIX, il n'existe pas de méthode pour protéger l'intégrité des données de bout en bout dans le cas où un processus de collecte est co-localisé avec un rédacteur de fichier. Le canal du processus d'exportation au processus de collecte en utilisant IPFIX est signé par la clé de processus d'exportation et protégé via TLS et DTLS, tandis que le fichier est signé par la clé du rédacteur de fichier et protégé via la CMS. L'identité du processus d'exportation n'est pas affirmée dans le fichier, et les enregistrements peuvent être modifiés entre le processus de collecte et le rédacteur de fichier.

Il y a potentiellement deux façons de traiter ce problème. La première est le consentement, et n'est appropriée que quand l'application permet que le canal du processus de collecte au rédacteur de fichier soit de confiance. Dans ce cas, la signature du rédacteur de fichier est une assertion implicite que le canal au processus d'exportation était protégé, que la signature du processus d'exportation a été vérifiée, et que les données n'ont pas été changées après la collecte. Pour que cela fonctionne, un rédacteur de fichier co-localisé avec un processus de collecte NE DEVRAIT PAS signer un fichier comme spécifié au paragraphe 9.1 sauf si la session de transport sur laquelle les données ont été exportées était protégée via TLS ou DTLS, et si le processus de collecte a identifié positivement le processus d'exportation par son certificat. Le rédacteur de fichier DEVRAIT inclure les certificats de processus d'exportation et de processus de collecte au sein du fichier en utilisant le gabarit d'options Détails de session d'exportation du paragraphe 8.1.3 ou le gabarit d'options Détails de message du paragraphe 8.1.4 pour permettre une vérification ultérieure.

Dans des situations où le processus de collecte et/ou le rédacteur de fichier ne peuvent pas être de confiance, l'intégrité de bout en bout peut alors être approximée en colocalisant le rédacteur de fichier avec le processus de mesure, et en supprimant complètement le protocole IPFIX de la chaîne. Dans ce cas, la signature du rédacteur de fichier est une assertion implicite que le processus de mesure est identifié et n'altère pas les informations telles qu'observées dans le réseau.

La vérification de ces relations de confiance sort du domaine d'application de ce document, et devrait être examinée sur la base de la mise en œuvre.

## 12.3 Recommandations sur la force cryptographique pour les fichiers IPFIX

Noter que quand on chiffre les fichiers pour une mémorisation d'archivage, la force du chiffrement dépend de la durée pendant laquelle les données sont supposées être archivées. Une mémorisation à long terme peut exiger une ré-application périodique de la protection cryptographique en re-signant et en re-chiffrant les fichiers avec des clés plus fortes. Dans ce cas, il est recommandé que les données signées et/ou chiffrées existantes soient encapsulées au sein d'une nouvelle protection plus forte. Voir la [RFC4810] pour une discussion de cette question.

## 13. Considérations relatives à l'IANA

Le présent document spécifie la création de plusieurs nouveaux éléments d'information IPFIX dans le registre IPFIX des éléments d'information situé à <http://www.iana.org>, comme défini au paragraphe 8.2. L'IANA a alloué les numéros

d'élément d'information suivants :

258 : élément d'information collectionTimeMilliseconds  
 259 : élément d'information exportSctpStreamId  
 260 : élément d'information maxExportSeconds  
 261 : élément d'information maxFlowEndSeconds  
 262 : élément d'information messageMD5Checksum  
 263 : élément d'information messageScope  
 264 : élément d'information minExportSeconds  
 265 : élément d'information minFlowStartSeconds  
 266 : élément d'information opaqueOctets  
 267 : élément d'information sessionScope  
 268 : élément d'information maxFlowEndMicroseconds  
 269 : élément d'information maxFlowEndMilliseconds  
 270 : élément d'information maxFlowEndNanoseconds  
 271 : élément d'information minFlowStartMicroseconds  
 272 : élément d'information minFlowStartMilliseconds  
 273 : élément d'information minFlowStartNanoseconds  
 274 : élément d'information collectorCertificate  
 275 : élément d'information exporterCertificate

L'IANA a créé le type de support application/ipfix pour les données IPFIX, comme décrit par les informations d'enregistrement suivantes :

Nom de type : application

Nom de sous type : ipfix

Paramètres exigés : aucun

Paramètres facultatifs : aucun

Considérations de codage : les fichiers IPFIX sont binaires, et donc doivent être codés dans les contextes non binaires.

Considérations de sécurité : voir les considérations sur la sécurité (Section 12) de la RFC 5655, et les considérations sur la sécurité de la [RFC5101].

Considérations d'interopérabilité : voir la "Spécification détaillée" (Section 7) de la RFC 5655. Le format est conçu pour être largement interopérable, car tout flux valide de messages IPFIX sur tout transport spécifié dans la [RFC5101] DOIT être reconnaissable comme fichier IPFIX valide.

Spécification publiée : RFC 5655, en particulier la Section 7, et [RFC5101].

Applications qui utilisent ce type de support : diverses mises en œuvre IPFIX (voir la [RFC5153]) prennent en charge la construction de lecteurs et rédacteurs de fichiers IPFIX.

Information supplémentaires :

Numéros magiques : aucun, bien que les deux premiers octets de tout fichier IPFIX soient les deux premiers octets d'un en-tête de message, le champ Version, conformément à la [RFC5101] est toujours 10 dans l'ordre des octets du réseau : 0x00, 0x0A.

Extension de fichier : .ipfix

Code de type de fichier Macintosh : aucun

Personne & adresse de messagerie à contacter pour plus d'informations : Brian Trammell <brian.trammell@hitachi-eu.com> pour les auteurs de la RFC 5655 ; Nevil Brownlee <n.brownlee@auckland.ac.nz> pour le groupe de travail IPFIX.

Usage prévu : USAGE LIMITÉ

Restrictions d'usage : aucune

Contrôleur des changements : Brian Trammell <brian.trammell@hitachi-eu.com> pour les auteurs de la RFC 5655 ; Nevil Brownlee <n.brownlee@auckland.ac.nz> pour le groupe de travail IPFIX.

## 14. Remerciements

Merci à Maurizio Molina, Tom Kosnar, et Andreas Kind pour leur assistance technique sur les exigences pour un format standard de mémorisation de flux. Merci à Benoit Claise, Paul Aitken, Andrew Johnson, Gerhard Muenz, et Nevil Brownlee pour leur relecture et leur retours. Merci à Pasi Eronen pour avoir attiré notre attention sur la [RFC5485], et à Russ Housley pour l'avoir écrite ; il spécifie un format de signature détaché d'où est largement tiré le paragraphe 9.1. Merci au projet PRISM pour son soutien au présent travail.

## 15. Références

### 15.1 Références normatives

- [bzip2] Seward, J., "bzip2 (<http://www.bzip.org/>)", mars 2008.
- [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992, DOI 10.17487/RFC1321, (*Information*)
- [RFC1952] P. Deutsch, "Spécification du format de fichier GZIP version 4.3", DOI 10.17487/RFC1952, mai 1996. (*Info*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, (*MàJ par [RFC8174](#)*)
- [RFC4810] C. Wallace et autres, "Exigences pour un service d'archive à long terme", mars 2007. (*Information*)
- [RFC5101] B. Claise, éd., "Spécification du [protocole d'exportation d'informations](#) de flux IP (IPFIX) pour l'échange d'informations de flux de trafic IP", janvier 2008. (*P.S.*) (*Obsolète, voir [RFC7011](#), STD77*)
- [RFC5102] J. Quittek et autres, "[Modèle d'informations](#) pour l'exportation d'informations de flux IP", janvier 2008. (*P.S.*) (*Remplacée par [RFC7012](#)*)
- [RFC5280] D. Cooper et autres, "[Profil de certificat d'infrastructure](#) de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", mai 2008. (*Remplace les [RFC3280](#), [RFC4325](#), [RFC4630](#)*) (*P.S.* ; *MàJ par [RFC8398](#), [8399](#)*)
- [RFC5610] E. Boschi, B. Trammell, L. Mark, T. Zseby, "[Exportation des informations de type](#) pour les éléments d'information Exportation d'information de flux IP (IPFIX)", juillet 2009. (*P. S.*)
- [RFC5652] R. Housley, "[Syntaxe de message cryptographique](#) (CMS)", STD70, septembre 2009. (*Remplace [RFC3852](#)*)

### 15.2 Références pour information

- [pcap] "libpcap (<http://www.tcpdump.org/>)", octobre 2008.
- [RFC3851] B. Ramsdell, "[Spécification du message d'extensions](#) de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. (*Obsolète, voir [RFC5751](#)*)
- [RFC3917] J. Quittek, T. Zseby, B. Claise, S. Zander, "Exigences pour l'exportation d'informations de flux IP (IPFIX)", octobre 2004. (*Information*)
- [RFC3954] B. Claise, éd., "Format d'exportation de données pour la version 9 des services NetFlow de Cisco Systems", octobre 2004. (*Information*)
- [RFC4288] N. Freed et J. Klensin, "Spécifications du [type de support et procédures d'enregistrement](#)", [BCP 13](#), décembre 2005.
- [RFC5153] E. Boschi et autres, "Lignes directrices pour la mise en œuvre de IPFIX", avril 2008. (*Information*)
- [RFC5470] G. Sadasivan et autres, "[Architecture pour l'exportation d'informations](#) de flux IP", mars 2009. (*Information*)
- [RFC5471] C. Schmoll, P. Aitken et B. Claise, "Lignes directrices pour l'essai d'exportation d'informations de flux IP (IPFIX)", mars 2009. (*Information*)
- [RFC5472] T. Zseby et autres, "Applicabilité de l'exportation d'information de flux IP (IPFIX)", mars 2009. (*Information*)

- [RFC5473] E. Boschi et autres, "Réduction de redondance dans les rapports d'exportation d'informations de flux IP (IPFIX) et d'échantillonnage de paquet (PSAMP)", mars 2009. (*Information*)
- [RFC5485] R. Housley, "Signatures numériques sur les documents de projet Internet", mars 2009. (*Info. ; MàJ par RFC8358*)
- [SAINT2007] Trammell, B., Boschi, E., Mark, L., and T. Zseby, "Requirements for a standardized flow storage solution", in Proceedings of the SAINT 2007 workshop on Internet Measurement Technology, Hiroshima, Japan, janvier 2007.

## Appendice A. Exemple de fichier IPFIX

Dans cette section, on explore un exemple de fichier IPFIX qui montre les diverses caractéristiques du format de fichier IPFIX. Ce fichier contient des enregistrements de flux décrits par un seul gabarit. Ce fichier contient aussi un enregistrement Fenêtre temporelle de fichier pour noter l'heure de début et de fin des données, et un enregistrement Détails de session d'exportation pour l'enregistrement des informations d'infrastructure de collecte. Chaque message au sein de ce fichier contient aussi un enregistrement Somme de contrôle de message, car ce fichier peut être chiffré en externe et/ou mémorisé comme archive. La structure de ce fichier est montrée à la Figure 2.

```

+=====+
| message IPFIX                               seq. 0 |
| +-----+ |
| | Ensemble de gabarits (ID 2)                1 rec | |
| |   Gabarit de données ID 256                | |
| | +-----+ |
| | ensemble de gabarits d'options (ID 3) 3 recs | |
| |   fichier Time Window Opt. Tmpl. ID 257      | |
| |   Message Checksum Opt. Tmpl. ID 259         | |
| |   Export Session Details Opt. Tmpl. ID 258    | |
| | +-----+ |
| | Data Set (ID 259) [Message Checksum] 1 rec   | |
| | +-----+ |
+=====+
| message IPFIX                               seq. 1 |
| +-----+ |
| | Data Set (ID 257) [fichier Time Window] 1 r. | |
| | +-----+ |
| | Data Set (ID 258) [Export Session] 1 rec    | |
| | +-----+ |
| | Data Set (ID 259) [Message Checksum] 1 rec   | |
| | +-----+ |
+=====+
| message IPFIX                               seq. 4 |
| +-----+ |
| | Data Set (ID 256)                          50 recs | |
| |   contient données de flux                  | |
| | +-----+ |
| | Data Set (ID 259) [Message Checksum] 1 rec   | |
| | +-----+ |
+=====+
| message IPFIX                               seq. 55 |
| . . . |

```

**Figure 2 : Exemple de structure de fichier**

Le gabarit qui décrit les enregistrements de données contient un horodatage de début de flux, un quintuplet IPv4, et des comptes de totaux de paquets et d'octets. L'ensemble de gabarits qui définit cela est montré à la Figure 3:

**Figure 3 : Exemple de fichier de gabarit de données**

Ceci est suivi par un ensemble de gabarits d'options contenant les gabarits d'options exigés pour lire le fichier : le gabarit d'options Fenêtre temporelle de fichier (défini au paragraphe 8.1.2) le gabarit d'options Détails de session d'exportation (défini au paragraphe 8.1.3) et le gabarit d'options Somme de contrôle de message (défini au paragraphe 8.1.1). Cet ensemble de gabarits d'options est montré aux figures 4 et 5 ci-dessous :

**Figure 4 : Exemple de fichier Gabarits d'options (fenêtre de temps et somme de contrôle)**

page - 29 -

|                   |            |                                |                       |       |
|-------------------|------------|--------------------------------|-----------------------|-------|
| Compte de champ   | Portée = 1 | 0                              | sessionScope          | = 267 |
| Longueur de champ | = 1        | 0                              | exporterIPv4Address   | = 130 |
| Longueur de champ | = 4        | 0                              | collectorIPv4Address  | = 211 |
| Longueur de champ | = 4        | 0                              | exporterTransportPort | = 217 |
| Longueur de champ | = 2        | 0                              | col.TransportPort     | = 216 |
| Longueur de champ | = 2        | 0                              | col.TransportProtocol | = 215 |
| Longueur de champ | = 1        | 0                              | col.ProtocolVersion   | = 214 |
| Longueur de champ | = 1        | 0                              | minExportSeconds      | = 264 |
| Longueur de champ | = 4        | 0                              | maxExportSeconds      | = 260 |
| Longueur de champ | = 4        | Bourrage d'ensemble (2 octets) |                       |       |

**Figure 5 : Exemple de fichier Gabarits d'options, suite (détails de session)**

## A.2 Exemple supplémentaire de données d'options

Suite aux gabarits exigés pour décoder le fichier sont les informations supplémentaires d'options IPFIX utilisées pour décrire le contenu et les informations de type du fichier. D'abord vient l'enregistrement fenêtre temporelle du fichier ; il note que le fichier contient des données du 9 octobre 2007 entre 00:01:13 et 23:56:27 UTC, et apparaît comme montré à la Figure 6 :

| 1                            |   |   |   |   |   |   |   |   |   | 2                       |   |   |   |   |   |   |   |   |   | 3     |   |   |   |   |   |   |   |   |   |   |   |
|------------------------------|---|---|---|---|---|---|---|---|---|-------------------------|---|---|---|---|---|---|---|---|---|-------|---|---|---|---|---|---|---|---|---|---|---|
| 0                            | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0                       | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0     | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |
| Identifiant d'ensemble = 257 |   |   |   |   |   |   |   |   |   | Longueur = 13           |   |   |   |   |   |   |   |   |   |       |   |   |   |   |   |   |   |   |   |   |   |
| sessionScope                 |   |   |   |   |   |   |   |   |   | minFlowStartSeconds     |   |   |   |   |   |   |   |   |   |       |   |   |   |   |   |   |   |   |   |   |   |
| 0                            |   |   |   |   |   |   |   |   |   | 2007-10-09 00:01:13 UTC |   |   |   |   |   |   |   |   |   | . . . |   |   |   |   |   |   |   |   |   |   |   |
|                              |   |   |   |   |   |   |   |   |   | maxFlowEndSeconds       |   |   |   |   |   |   |   |   |   |       |   |   |   |   |   |   |   |   |   |   |   |
| . . .                        |   |   |   |   |   |   |   |   |   | 2007-10-09 23:56:27 UTC |   |   |   |   |   |   |   |   |   | . . . |   |   |   |   |   |   |   |   |   |   |   |
|                              |   |   |   |   |   |   |   |   |   |                         |   |   |   |   |   |   |   |   |   |       |   |   |   |   |   |   |   |   |   |   |   |
| . . .                        |   |   |   |   |   |   |   |   |   |                         |   |   |   |   |   |   |   |   |   |       |   |   |   |   |   |   |   |   |   |   |   |

**Figure 6 : Exemple de fichier Fenêtre temporelle**

Ceci est suivi par des informations sur la façon dont les données du fichier ont été collectées, dans l'enregistrement Détails de session d'exportation. Cet enregistrement note que la session mémorisée dans ce fichier a été envoyée via SCTP d'un exportateur à 192.0.2.30 accès 32769 à un collecteur à 192.0.2.40 accès 4739, et contient des messages exportés entre 00:01:57 et 23:57:12 UTC le 9 octobre 2007 ; il est représenté dans son ensemble de données (Data Set) à la Figure 7 :

| 1                            |   |   |   |   |   |   |   |   |   | 2                                     |   |   |   |   |   |   |   |   |   | 3 |   |   |   |   |   |   |   |   |   |   |   |
|------------------------------|---|---|---|---|---|---|---|---|---|---------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0                            | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0                                     | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |
| Identifiant d'ensemble = 258 |   |   |   |   |   |   |   |   |   | Longueur = 27                         |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| sessionScope 0               |   |   |   |   |   |   |   |   |   | exporterIPv4Address 192.0.2.30 . . .  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| . . .                        |   |   |   |   |   |   |   |   |   | collectorIPv4Address 192.0.2.31 . . . |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |



```

| sourceTransportPort 32770 | destinationTransportPort 80 |
+-----+-----+-----+-----+
| protocolId 6 | totalOctetCount 18000 . . . |
+-----+-----+-----+-----+
. . . | totalPacketCount 65 . . . |
+-----+-----+-----+-----+
. . . | (49 enregistrements de plus) . . . |
+-----+-----+-----+-----+

```

Figure 9 : Exemple de fichier Ensemble de données

### A.5 Exemple de fichier complet

En mettant ensemble les exemples ci-dessus et en ajoutant les en-têtes de message appropriés, un cliché hexadécimal des 285 premiers octets de l'exemple de fichier construit ci-dessus apparaîtrait comme noté dans la Figure 10.

```

0:|00 0A 00 A0 47 0A B6 E5 00 00 00 00 00 00 00 01
  [^ en-tête premier message (long. 160 octets) -->
16:|00 02 00 28 01 00 00 08 00 96 00 04 00 08 00 04
  [^ ensemble de gabarit de données -->
32: 00 0C 00 04 00 07 00 02 00 0B 00 02 00 04 00 01
48: 00 55 00 04 00 56 00 04|00 03 00 50 01 01 00 03
  [^ ensemble de gabarit d'options -->
64: 00 01 01 0B 00 01 01 09 00 04 01 05 00 04 01 03
80: 00 02 00 01 01 07 00 01 01 06 00 10 01 02 00 09
96: 00 01 01 0B 00 01 00 82 00 04 00 D3 00 04 00 D9
112: 00 02 00 D8 00 02 00 D7 00 01 00 D0 00 01 01 08
128: 00 04 01 04 00 04 00 00|01 03 00 18 00 73 F1 12
  [^ enregistrement de somme de contrôle -->
144: D6 C7 58 BE 44 E6 60 06 4E 78 74 AE 7D 00 00 00
160:|00 0A 00 50 47 0A B6 E5 00 00 00 01 00 00 00 01
  [^ en-tête second message (longueur 80 octets) -->
176:|01 01 00 0E 00 47 0A B6 B9 47 0C 07 1B 00|01 02
  [^ enreg. fenêtre temp -> [détails session ^ -->
198: 00 1C 00 C0 00 02 1E 0C 00 02 1F 80 01 12 83 84
208: 0A 47 0A B6 E5 47 0C 07 48 00|01 03 00 16 00 3E
[ enregistrement somme de contrôle ^ -->
224: 2B 37 08 CE B2 0E 30 11 32 12 4A 5F E3 AD DB 00
240:|00 0A 05 10 47 0A B6 E5 00 00 00 06 00 00 00 01
  [^ en-tête troisième message (longueur 1296 octets) -->
253:|01 00 04 E6|47 0A B6 B9 C0 00 02 02 C0 00 02 03
  [^ set hdr ][^ enreg. premières données -->
272: 80 02 00 50 06 00 00 46 50 00 00 00 00 41

```

Figure 10 : Exemple de fichier Hex Dump

## Appendice B. Applicabilité des fichiers IPFIX à la mémorisation de flux NetFlow V9

Comme le format de message IPFIX est presque un sur ensemble du format de paquet NetFlow V9, les fichiers IPFIX peuvent être utilisés pour mémoriser relativement facilement des données NetFlow V9. Cette section décrit une méthode pour le faire. Les différences entre les deux protocoles sont décrites à l'Appendice B.1. Une méthode de traduction simple, légère, message par message, pour transformer les paquets V9 en messages IPFIX pour la mémorisation au sein de fichiers IPFIX, est décrite à l'Appendix B.2. Un exemple de cette méthode de traduction est donnée à l'Appendice B.3.

### B.1 Comparaison de NetFlow V9 avec IPFIX

Avec quelques différences, le protocole IPFIX est un sur ensemble du protocole NetFlow V9, qui a évolué à partir de lui largement par un processus d'ajout de caractéristiques pour le mettre en conformité avec les exigences de IPFIX et les

besoins des participants au groupe de travail IPFIX. Ce appendice mentionne les différences entre les deux protocoles. Il est seulement pour information, et est présenté comme une exploration des deux protocoles pour motiver l'usage de fichiers IPFIX pour mémoriser les données de flux collectées par V9.

B.1.1   Format d'en-tête de message

NetFlow V9 et IPFIX utilisent tous deux des flux de messages préfixés par un en-tête de message, bien que l'en-tête de message diffère significativement entre les deux. Noter que dans la terminologie NetFlow V9, ces messages sont appelés des paquets, et les messages doivent être délimités par les limites de datagrammes. IPFIX n'a pas cette contrainte. Les formats d'en-tête sont détaillés ci-dessous :

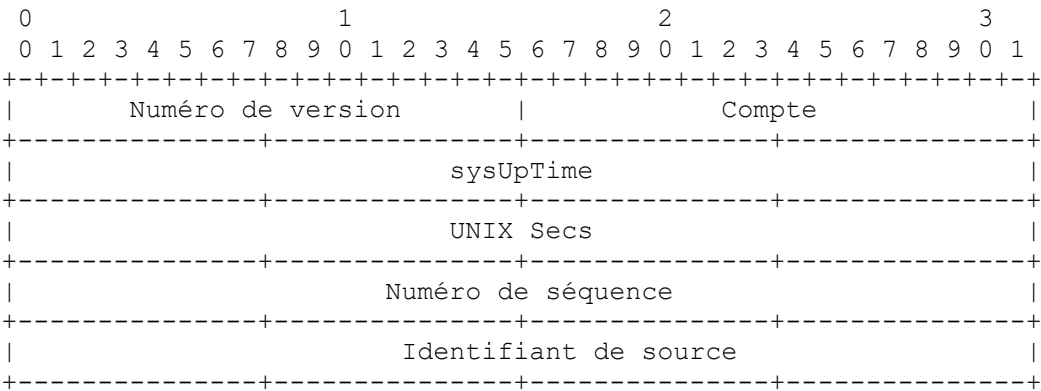


Figure 11 : Format d'en-tête de paquet NetFlow V9

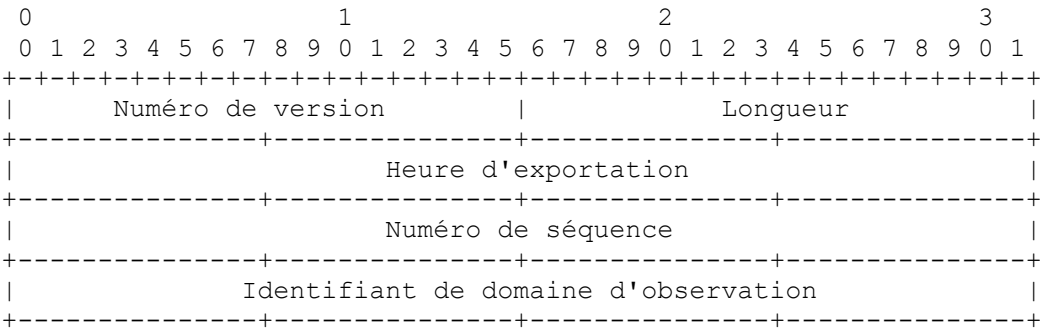


Figure 12 : Format d'en-tête de message IPFIX

- Numéro de version : le numéro de version IPFIX DOIT être 10, tandis que le numéro de version NetFlow V9 DOIT être 9.
- Longueur ou Compte : le champ Compte dans l'en-tête de paquet NetFlow V9 compte les enregistrements dans le message (y compris les enregistrements de données et de gabarits) tandis que le champ Longueur dans l'en-tête de message IPFIX compte les octets dans le message. Noter que cela implique que les collecteurs NetFlow V9 doivent s'appuyer sur les limites de datagrammes ou autres délimiteurs externes ; autrement, ils doivent consommer complètement un message avant de trouver sa fin.
- Heure d'activation du système (sysUpTime) : cette valeur en millisecondes est exportée dans l'en-tête de paquet NetFlow V9. Ce champ n'est pas présent dans l'en-tête de message IPFIX, et doit être exporté en utilisant une option IPFIX si il est exigé.
- Heure d'exportation : à part d'être appelée UNIX Secs dans l'en-tête de paquet NetFlow V9, l'heure d'exportation en secondes depuis le 1er janvier 1970 à 0000 UTC apparaît dans les deux en-têtes de message NetFlow V9 et IPFIX.
- Numéro de séquence : le numéro de séquence NetFlow V9 compte des paquets, tandis que le numéro de séquence IPFIX compte les enregistrements en ensembles de données (*Data Set*). Leur portée à tous deux est le domaine d'observation.
- Identifiant de domaine d'observation : de même, l'identifiant de source NetFlow V9 est devenu l'identifiant de domaine

d'observation IPFIX.

### B.1.2 Format d'en-tête d'ensemble

Les en-têtes d'ensemble sont identiques dans NetFlow V9 et IPFIX ; c'est-à-dire, chaque ensemble (ensemble de flux (*FlowSet*) dans la terminologie de NetFlow V9) est préfixé d'un en-tête d'ensemble de 4 octets contenant l'identifiant d'ensemble et la longueur de l'ensemble en octets.

Noter que les identifiants d'ensemble spéciaux sont différents entre IPFIX et NetFlow V9. Les ensembles de gabarits IPFIX sont identifiés par l'identifiant d'ensemble 2, tandis que les FlowSets de gabarit NetFlow V9 sont identifiés par l'identifiant d'ensemble 0. De même, les ensembles de gabarit d'options IPFIX sont identifiés par l'identifiant d'ensemble 3, tandis que les FlowSets de gabarit d'options NetFlow V9 sont identifiés par l'identifiant d'ensemble 1.

Les deux protocoles réservent les identifiants d'ensemble 0 à -255, et utilisent les identifiants d'ensemble de 256 à 65535 pour les ensembles de données (ou FlowSets, dans la terminologie NetFlow V9).

### B.1.3 Format de gabarit

Le gabarit FlowSets dans NetFlow V9 prend en charge un sous ensemble des fonctions de IPFIX. Précisément, NetFlow V9 n'a pas de prise en charge des éléments d'information spécifiques du fabricant comme l'a IPFIX, de sorte qu'il n'y a pas de bit ou facilité d'entreprise pour associer un numéro d'entreprise privée avec un élément d'information. NetFlow V9 ne prend pas non plus en charge les champs de longueur variable.

Les gabarits d'options FlowSets dans NetFlow V9 sont similaires aux ensembles de gabarit d'options dans IPFIX sous réserve des mêmes avertissements.

### B.1.4 Modèle d'information

Les définitions de type de champ NetFlow V9 sont un sous ensemble compatible, et ont évolué de concert avec le modèle d'informations IPFIX. Les identifiants d'élément d'information IPFIX dans la gamme de 1 à 127 sont définis par le modèle d'informations IPFIX [RFC5102] comme étant compatibles avec les types de champ NetFlow V9 correspondants.

### B.1.5 Gestion de gabarit

NetFlow V9 n'a pas de concept de session de transport comme dans IPFIX, car NetFlow V9 a été conçu en pensant à un transport sans connexion. Les identifiants de gabarit ont donc une portée de la durée de vie d'un processus d'exportation (c'est-à-dire, une instance de processus d'exportation entre les redémarrages). Il n'y a pas de facilité dans NetFlow V9 comme dans IPFIX pour le retrait ou la réutilisation d'identifiant de gabarit. La retransmission de gabarit chez l'exportateur fonctionne comme dans les processus d'exportation IPFIX fondés sur UDP.

### B.1.6 Transport

En pratique, bien que NetFlow V9 soit conçu pour être indépendant du transport, il est transporté seulement sur UDP. Il n'y a pas de facilité comme dans IPFIX pour un transport en mode connexion sans limites de datagramme, du fait de l'utilisation d'un champ de compte d'enregistrements par opposition au champ de longueur de message dans l'en-tête de paquet. Il n'y a pas dans NetFlow V9 de prise en charge de la sécurité de la couche transport via TLS ou DTLS.

## B.2 Methode pour transformer les messages NetFlow V9 en IPFIX

Cet appendice décrit une méthode pour transformer les paquets NetFlow V9 en messages IPFIX, qui peut être utilisée pour mémoriser les données NetFlow V9 dans des fichiers IPFIX. Un processus de transformation des paquets NetFlow V9 en messages IPFIX doit traiter le fait que les paquets NetFlow V9 et les messages IPFIX sont tramés différemment, que les numéros de séquence fonctionnent différemment, et que les définitions de type de champ NetFlow V9 sont seulement compatibles avec le modèle d'informations IPFIX en dessous de l'identifiant d'élément d'information 128.

Pour chaque paquet NetFlow V9 entrant, le processus de transformation doit :

1. Vérifier que le champ Version de l'en-tête de paquet est 9.
2. Vérifier que le champ Numéro de séquence de l'en-tête de paquet est valide.



|   |                              |        |                          |        |
|---|------------------------------|--------|--------------------------|--------|
|   | Identifiant d'ensemble = 256 |        | Longueur d'ensemble = 16 |        |
| + | -----+                       | -----+ | -----+                   | -----+ |
|   | IPV4_SRC_ADDR                |        | 192.0.2.2                |        |
| + | -----+                       | -----+ | -----+                   | -----+ |
|   | IPV4_DST_ADDR                |        | 192.0.2.3                |        |
| + | -----+                       | -----+ | -----+                   | -----+ |
|   | IN_BYTES                     |        | 60303                    |        |
| + | -----+                       | -----+ | -----+                   | -----+ |

Figure 13 : Exemple de paquet NetFlow V9

| 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |   |   |   |   |   |   |   |   |   | 2 |   |   |   |   |   |   |   |   |   | 3 |   |   |   |   |   |   |   |   |   |   |   |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|
| 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |  |
| +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----- |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |

Figure 14 : Exemple correspondant de message IPFIX

Adresse des auteurs

|                                                                                                                                                                                                                          |                                                                                                                                                                                          |                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Brian Trammell<br>Hitachi Europe<br>c/o ETH Zurich<br>Gloriastrasse 35<br>8092 Zurich<br>Switzerland<br>mél : <a href="mailto:brian.trammell@hitachi-eu.com">brian.trammell@hitachi-eu.com</a>                           | Elisa Boschi<br>Hitachi Europe<br>c/o ETH Zurich<br>Gloriastrasse 35<br>8092 Zurich<br>Switzerland<br>mél : <a href="mailto:elisa.boschi@hitachi-eu.com">elisa.boschi@hitachi-eu.com</a> | Lutz Mark<br>Fraunhofer IFAM<br>Wiener Str. 12<br>28359 Bremen<br>Germany<br>mél : <a href="mailto:lutz.mark@ifam.fraunhofer.de">lutz.mark@ifam.fraunhofer.de</a> |
| Tanja Zseby<br>Fraunhofer Institute for Open Communication Systems<br>Kaiserin-Augusta-Allee 31<br>10589 Berlin<br>Germany<br>mél : <a href="mailto:tanja.zseby@fokus.fraunhofer.de">tanja.zseby@fokus.fraunhofer.de</a> | Arno Wagner<br>ETH Zurich<br>Gloriastrasse 35<br>8092 Zurich<br>Switzerland<br>mél : <a href="mailto:arno@wagner.name">arno@wagner.name</a>                                              |                                                                                                                                                                   |