Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1542

(09/2016)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange concernant les événements/les incidents/l'heuristique

Format d'échange de messages sur les informations de session

Recommandation UIT-T X.1542

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	**X.1540–X.1549**
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1542

Format d'échange de messages sur les informations de session

Résumé

Dans l'environnement actuel, les réseaux informatiques sont exposés à des menaces venant de l'intérieur mais aussi de l'extérieur d'une organisation. Les systèmes de pare-feu journalisent des informations de session sur des connexions TCP/IP (protocole de commande de transmission/protocole Internet) entrantes et sortantes sélectionnées.

Toutefois, les systèmes actuellement disponibles ne sont généralement pas interopérables car chacun a ses propres fonctionnalités, mécanismes de contrôle et formats de journal de session particuliers.

La plupart des administrateurs de sécurité ont aujourd'hui besoin de pouvoir maintenir un format d'échange de messages sur les informations de session compatible dans les différents systèmes de pare-feu et même dans des infrastructures différentes.

La Recommandation UIT-T X.1542 décrit un modèle d'information pour le format d'échange de messages sur les informations de session (SIMEF) et fournit un modèle de données associé, spécifié en langage de balisage extensible (XML). Le format SIMEF définit une représentation de modèle de données permettant de partager les informations sur les journaux de session de couche transport concernant la gestion centralisée de la sécurité du réseau et le système d'échange d'informations sur la sécurité. La spécification d'un protocole de transport ne relève pas de la présente Recommandation.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1542	07-09-2016	17	11.1002/1000/12852

Mots-clés

Modèle de données, échange de messages, sécurité de réseau, informations de session.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1542

Format d'échange de messages sur les informations de session

1 Domaine d'application

La présente Recommandation décrit le format d'échange de messages sur les informations de session (SIMEF), qui est un modèle de données permettant de représenter les informations de session exportées par les systèmes de sécurité comme les pare-feu, et explique les raisons motivant l'utilisation de ce modèle. On trouvera dans la présente Recommandation une mise en oeuvre de modèles de données en langage de balisage extensible (XML), une définition de type de document (DTD) XML et des exemples.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 analyseur: système de sécurité de réseau qui détecte les attaques en analysant les informations de session entrantes et sortantes. Il génère en outre un journal de session qu'il envoie aux systèmes de gestion de la sécurité.

3.1.1 informations de session [b-IETF RFC 2663]: informations concernant la session TCP/UDP (protocole de commande de transmission/protocole de datagramme utilisateur), le service d'application et les entités de session telles que les fournisseurs d'informations de session les voient. Une session est définie comme étant un ensemble de trafic qui est géré comme une unité pour la traduction. Les sessions TCP/UDP sont identifiées de façon unique par le nuplet (adresse IP source, port TCP/UDP source, adresse IP cible, port TCP/UDP cible).

NOTE – Cette définition est basée sur [b-IETF RFC 2663].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

BSD distribution de logiciels de Berkeley (*Berkeley software distribution*)

CGI interface de passerelle commune (*common gateway interface*)

DTD définition de type de document (*document type definition*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IP protocole Internet (*Internet protocol*)

LAN réseau local (*local area network*)

MAC commande d'accès au support (*media access control*)

NAT traduction d'adresse réseau (*network address translation*)

NTP protocole de temps réseau (*network time protocol*)

POSIX interface pour la portabilité des systèmes d'exploitation (*portable operating system interface*)

SIMEF format d'échange de messages sur les informations de session (*session information message exchange format*)

SNA architecture de réseau partagé (*shared network architecture*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

TCP protocole de commande de transmission (*transmission control protocol)*

UDP protocole de datagramme utilisateur (*user datagram protocol*)

UML langage de modélisation unifié (*unified modelling language*)

URL localisateur uniforme de ressources (*uniform resource locator*)

UTF format de transformation pour le jeu de caractères universel (*universal character set transformation format*)

VPN réseau privé virtuel (*virtual private network*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

UNIX ® est une marque de commerce déposée d'Open Group.

POSIX ® est une marque de commerce déposée de l'IEEE.

6 Aperçu

Dans l'environnement de réseau actuel, les réseaux informatiques sont exposés à des menaces venant de l'intérieur mais aussi de l'extérieur d'une organisation. Par conséquent, la plupart des recherches concernant la sécurité des réseaux portent sur l'élaboration de systèmes de gestion de la sécurité des réseaux et d'utilitaires de surveillance du réseau intégrés qui permettent à une organisation de récupérer des paquets TCP/IP qui passent par ses dispositifs de réseau et de visualiser les données ainsi récupérées sous la forme de séquences de conversations entre des clients et des services. Par exemple, les systèmes de pare-feu journalisent des informations de session concernant des connexions TCP/IP entrantes et sortantes sélectionnées.

La Figure 1 illustre le concept de format SIMEF. Les informations de session peuvent être collectées auprès des systèmes de pare-feu, des dispositifs de traduction d'adresse réseau (NAT), etc. Le format SIMEF spécifie le modèle de données qui couvre la connexion réseau client/serveur, le dispositif d'utilisateur final et le service d'application. Le format SIMEF définit un modèle de données et des classes de messages connexes permettant de partager les informations de session de couche transport qui présente un intérêt pour les systèmes de gestion de la sécurité et les systèmes de partage d'informations. Il peut être appliqué au système d'échange d'informations sur les intrusions.

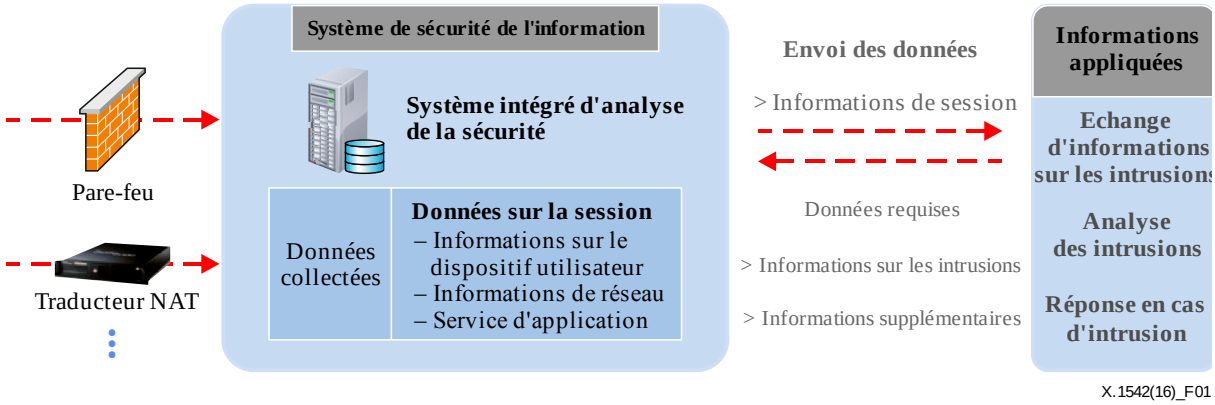

Figure 1 – Concept de format SIMEF

7 Représentation et définition

La présente Recommandation utilise trois notations: le langage de modélisation unifié (UML) pour décrire le modèle de données, le langage XML pour décrire le balisage utilisé dans les documents SIMEF et le balisage SIMEF pour représenter les documents.

7.1 Document SIMEF XML

La présente section décrit les règles de formatage des documents SIMEF XML. La plupart de ces règles sont "héritées" des règles de formatage des documents XML. Les paragraphes 7.1.1 et 7.1.2 décrivent le format du prologue d'un document SIMEF XML.

7.1.1 Déclaration XML

Les documents SIMEF échangés entre applications compatibles SIMEF doivent commencer par une déclaration XML et spécifier la version du langage XML utilisée. Il est recommandé de spécifier le codage utilisé.

Par conséquent, un message SIMEF devrait commencer comme suit:

```
   <?xml version="1.0" encoding="UTF-8"?>
   <simef: SIMEF-Message version="1.2"
xmlns:simef="http://iana.org/simef"/>
```

Les applications compatibles SIMEF peuvent choisir d'omettre la déclaration XML en interne afin de conserver de l'espace, en ajoutant cette déclaration uniquement lorsque le message est envoyé vers une autre destination (par exemple, un navigateur Internet). Cette pratique n'est pas recommandée, à moins qu'elle puisse être mise en oeuvre sans qu'aucune version et information de codage du message soit perdue.

Par conséquent, les responsables de la mise en oeuvre peuvent décider de prévoir que les analyseurs et les gestionnaires conviennent hors bande de la définition de type de document (DTD) qu'ils utiliseront pour échanger des messages (la définition type définie ici ou une version avec des extensions) puis omettre la définition DTD dans les messages SIMEF. La méthode à appliquer pour les négociations correspondantes ne relève pas de la présente Recommandation.

7.1.2 Traitements des données composées de caractères dans le format SIMEF

Pour des questions de portabilité, les applications compatibles SIMEF ne devraient pas utiliser de de formats de codage de caractères autres que les formats UTF-8 et UTF-16, de même que les messages SIMEF ne devraient pas être codés selon d'autres formats. Conformément à la norme XML, si aucun type de codage n'est spécifié pour un message SIMEF, on part du principe que le format UTF-8 est utilisé.

7.1.2.1 Références d'entités de caractères

Il est recommandé que les applications compatibles SIMEF utilisent la forme de références d'entités des caractères '&','<', '>', "" et ' (guillemets simples) lorsqu'elles utilisent ces caractères dans les données, afin d'éviter tout risque de mauvaise interprétation.

7.1.2.2 Traitement des espaces blancs

Tous les éléments SIMEF doivent prendre en charge l'attribut "xml:space".

7.1.2.3 Langages utilisés dans le format SIMEF

Les applications compatibles SIMEF doivent spécifier le langage utilisé pour le codage de leur contenu; en général, on peut pour ce faire définir l'attribut "xml:lang" pour l'élément de niveau supérieur et laisser tous les autres éléments "hériter" de cette définition.

7.2 Types de données SIMEF

Dans un message SIMEF XML, toutes les données doivent être exprimées sous la forme de texte, étant donné que le langage XML est un langage de formatage textuel. Les données fournissent des informations dactylographiques pour les attributs des classes du modèle de données. Chaque type de données du modèle a des exigences de formatage précises dans un message SIMEF XML; ces exigences sont présentées dans les paragraphes ci-après.

7.2.1 Entiers

Les attributs prenant la forme d'entiers sont représentés par le type de données INTEGER. Ces données doivent être codées en base 10 ou 16. Le codage d'entiers en base 10 utilise les chiffres '0' à '9' et un signe facultatif ('+' ou '-'). Par exemple, "123", "-456". Le codage d'entiers en base 16 utilise les chiffres '0' à '9' et les lettres 'a' à 'f' (ou leurs équivalents en caractères majuscules), précédés par les caractères "0x". Par exemple, "0x1a2b".

7.2.2 Nombres réels

Les attributs prenant la forme de nombres réels (virgule flottante) sont représentés par le type de données REAL. Ces données doivent être codées sur une base 10. Le codage des nombres réels est celui utilisé pour la fonction de bibliothèque "strtod" de l'interface pour la portabilité des systèmes d'exploitation (POSIX) définie dans 1003.1 [b-IEEE 1003.1], à savoir un signe facultatif ('+' ou '-') suivie d'une chaîne non vide de chiffres décimaux, pouvant contenir un caractère de base, puis une partie exposant facultative. Une partie exposant est composée d'un 'e'ou 'E', suivi d'un signe facultatif, suivi d'un ou plusieurs chiffres décimaux. Par exemple, "123.45e02", "-567, 89e-03". Les applications compatibles SIMEF doivent prendre en charge les deux caractères de base '.' et ','.

7.2.3 Caractères et chaînes

Les attributs à un seul caractère sont représentés par le type de données CHARACTER. Les attributs à plusieurs caractères d'une longueur connue sont représentés par le type de données STRING. Les données caractères et chaînes n'ont pas d'exigences particulières de formatage autres que la nécessité d'utiliser à certaines occasions des références de caractères pour présenter des caractères spéciaux.

7.2.3.1 Références d'entité de caractères

Dans les documents XML, certains caractères ont une signification particulière dans certains contextes. Afin que le caractère lui-même soit compris dans l'un de ces contextes, une séquence d'échappement particulière, appelée référence d'entité, doit être utilisée.

Les caractères pour lesquels un échappement est parfois nécessaire, ainsi que leurs références d'entité, sont les suivants:

Caractère	Référence d'entité
&	&amp;
<	&lt;
>	&gt;
“	&quot;
‘	&apos;

7.2.3.2 Références de codes de caractères

Tous les caractères définis dans les normes [b-ISO/CEI 10646] et Unicode peuvent figurer dans un document XML moyennant l'utilisation d'une référence de caractère. Une référence de caractère commence par les caractères '&' et '#' et finit par le caractère ';'. Entre ces caractères, on insère le code du caractère.

Si le code de caractère est précédé d'un 'x', il est interprété sur une base hexadécimale (base 16); si tel n'est pas le cas, il est interprété sur une base décimale (base 10). Par exemple, l'esperluette (&) est codée sous la forme & ou & et le signe inférieur à (<) est codé sous la forme < ou &#x003C. Tous les caractères à un, deux ou quatre octets spécifiés dans les normes ISO/CEI 10646 et Unicode peuvent être intégrés dans un document en utilisant cette technique.

7.2.4 Octets

Les données binaires sont représentées par le type de données BYTE (et BYTE[]). Les données binaires doivent être codées dans leur totalité sur une base 64.

7.2.5 Types énumérés

Les types énumérés sont représentés par le type de données ENUM et sont composés d'une suite ordonnée de valeurs acceptables.

7.2.6 Chaînes d'horodatage

Les chaînes d'horodatage sont représentées par le type de données DATETIME. Chaque chaîne d'horodatage identifie un instant précis dans le temps; les intervalles ne sont pas pris en charge. Les chaînes d'horodatage sont formatées selon un sous-ensemble défini dans [b-ISO 8601:2004], comme expliqué ci-après. Les numéros de section figurant entre parenthèses renvoient aux sections de [b-ISO 8601:2004].

7.2.7 Timbres horodateurs NTP

Les timbres horodateurs NTP (protocole de temps réseau) sont représentés par la type de données NTPSTAMP et sont décrits en détail dans [b-IETF RFC 1305] et [b-IETF RFC 5905]. Un timbre horodateur NTP est un nombre à virgule fixe non signé à 64 bits. La partie entière figure dans les 32 premiers bits et la partie décimale dans les 32 derniers. Dans les messages SIMEF, les timbres horodateurs NTP doivent être codés sous la forme de deux valeurs hexadécimales de 32 bits, séparées par un point ('.'). Par exemple, "0x12345678.0x87654321".

7.2.8 Listes de ports

Les listes de ports sont représentées par le type de données PORTLIST et sont composées d'une liste de nombres (entiers) et d'intervalles (N-M signifie ports N à M inclus) séparés par des virgules. Toutes les combinaisons de nombres et d'intervalles peuvent être utilisées dans une même liste. Par exemple,

"5-25,37,42,43,53,69-119,123-514".

7.2.9 Identificateurs uniques

Deux types d'identificateur unique sont utilisés dans la présente Recommandation. Tous deux sont représentés par le type de données STRING. Ces identificateurs sont mis en oeuvre en tant qu'attributs sur les éléments XML pertinents et doivent avoir des valeurs uniques comme suit:

1) L'attribut "deviceid" de classe Device (dispositif) (§ 8.2.3.2), s'il est spécifié, doit avoir une valeur unique pour tous les analyseurs dans l'environnement de détection des intrusions.

   La valeur par défaut est "0" et indique que l'analyseur ne peut pas générer d'identificateurs uniques.

2) L'attribut "ident" utilisé pour plusieurs classes, s'il est spécifié, doit avoir une value unique dans tous les messages envoyés par un même analyseur. La valeur de l'attribut "ident" doit être unique pour chaque combinaison de données identifiant un objet, non pour chaque objet. Les objets peuvent avoir plus d'une valeur "ident" qui leur est associée. Par exemple, l'identification d'un hôte par son nom aura une valeur, l'identification de ce même hôte par son adresse aura une autre valeur et l'identification de cet hôte toujours par son nom et son adresse aura encore une autre valeur.

La valeur par défaut est "0" et indique que l'analyseur ne peut pas générer d'identificateurs uniques.

La définition des méthodes permettant de créer les valeurs uniques contenues dans ces attributs ne relève pas de la présente Recommandation.

8 Modèle de données SIMEF

Les différents composants du modèle de données SIMEF sont présentés en détail dans les paragraphes ci-après. Des diagrammes UML sont fournis pour montrer les liens entre ces composants.

8.1 Structure générale du modèle de données

La Figure 2 montre les relations entre les principaux composants du modèle de données. La classe SIMEF-Message (message SIMEF) représente la classe de niveau supérieur; chaque type de message est une sous-classe de cette classe de niveau supérieur. Deux types de messages sont définis: les messages de connexion ("Connect") et les messages de pulsation ("Heartbeat"). Dans chaque message, des sous-classes de classe de message sont utilisées pour fournir les informations détaillées acheminées dans le message. La classe de messages de connexion comprend plusieurs sous-classes (dispositifs, politique, source, cible et données supplémentaires).

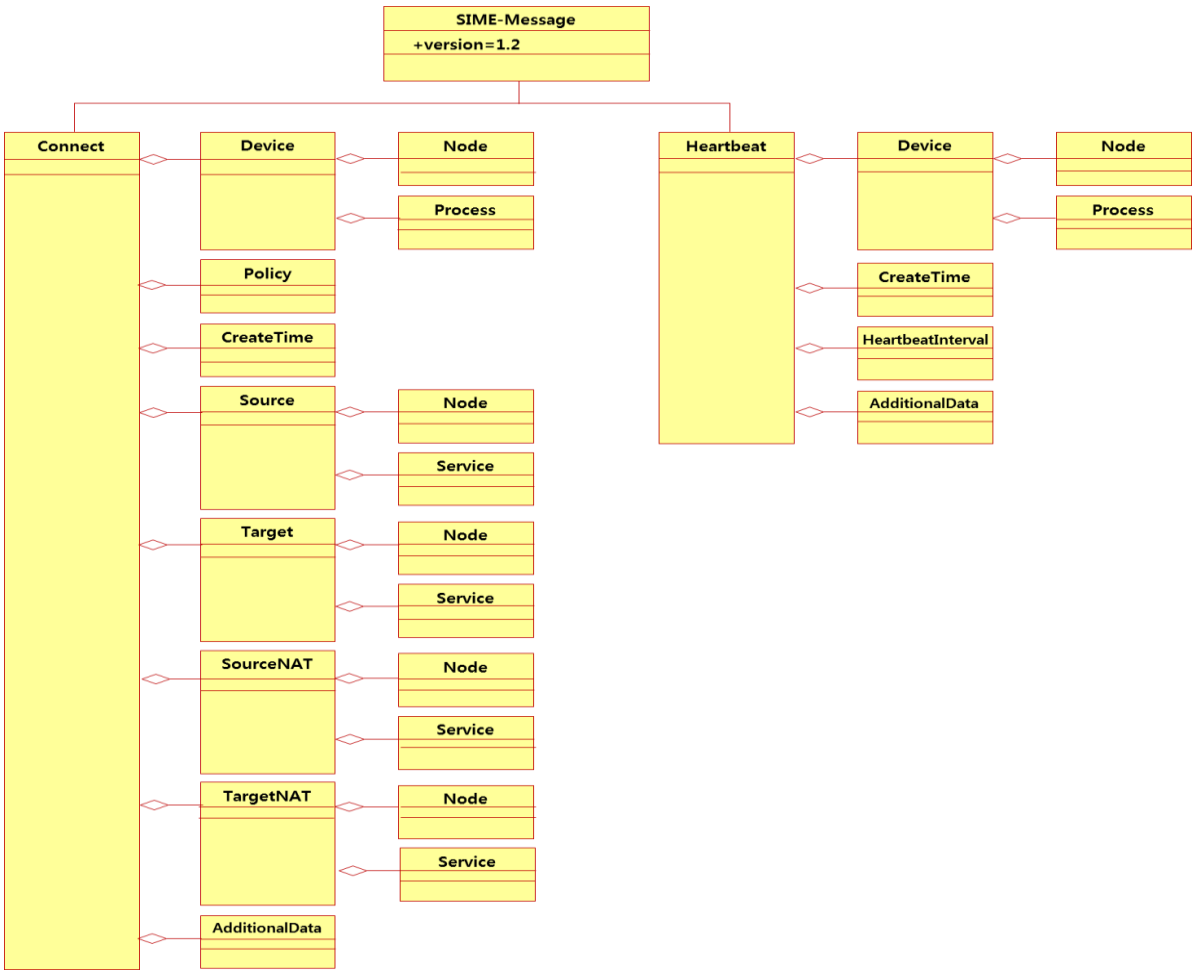

Figure 2 – Modèle de données SIMEF

8.1.1 Classes SIMEF

Tous les messages SIMEF sont des instances de la classe SIMEF-Message: Connect (connexion) et Heartbeat (pulsation). Les différentes classes sont décrites dans le présent paragraphe. Voir la Figure 3 et les Tableaux 1 et 2.

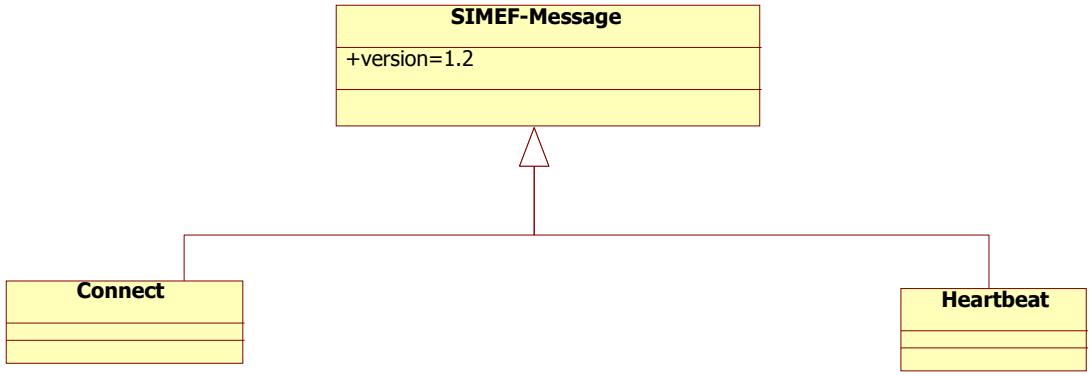

Figure 3 – Classe de niveau supérieur du modèle de données SIMEF

Tableau 1 – Attributs des classes SIMEF

Attribut	Utilisation	Type de données	Description
Version	Obligatoire	STRING	Information sur la version de format SIMEF Valeur par défaut: 1.2

Tableau 2 – Composants des classes SIMEF

Classes	Agrégation	Type de données	Description
Connect	Exactement un		Classe informations de sessions
Heartbeat	Zéro ou un		Classe informations sur l'état du système Fourniture facultative

8.2 Classes de message

Les différentes classes sont décrites aux paragraphes 8.2.1 à 8.2.4.

8.2.1 Classe Connect

La classe Connect (connexion) contient les informations de session. Elle exprime le type de journal généré par la connexion dans le pare-feu et montre en outre toutes les informations sur les tentatives de connexion vers l'intérieur mais aussi vers l'extérieur. Voir le Tableau 3. Les valeurs autorisées pour l'attribut "criticality" de la classe Connect sont données dans le Tableau 4. La classe Connect est composée de plusieurs classes d'agrégat, comme indiqué dans la Figure 4. Ces différentes classes d'agrégat sont décrites dans le Tableau 5.

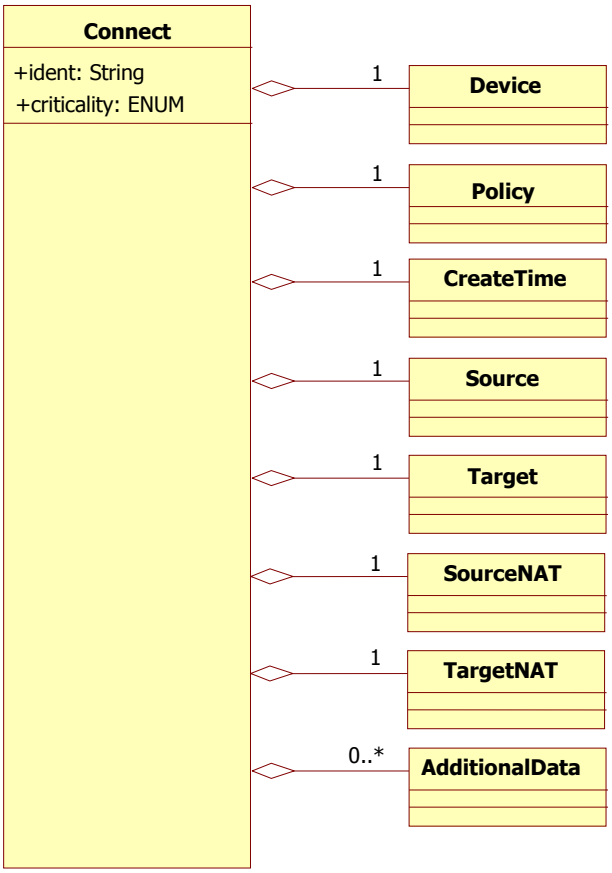

Figure 4 – Classes d'agrégat de la classe Connect

Tableau 3 – Attributs de la classe Connect

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique pour les informations relatives à l'accès
criticality	Facultative	ENUM	Classification selon l'évaluation de l'événement qui est générée par la connexion, Valeur par défaut: Unknown (inconnu)

Tableau 4 – Valeur de l'attribut "criticality"

Valeur	Mot clé	Définition
0	unknown (inconnu)	Lorsque l'effet de l'événement est inconnu ou ne peut pas être déterminé
1	normal (normal)	Si la connexion est normale
2	suspicious (suspect)	Si la connexion est suspecte
3	warning (avertissement)	Si la connexion peut être une alarme
4	critical (critique)	Si la connexion est sensible à l'action

Tableau 5 – Composants de la classe Connect

Classe	Agrégation	Type de données	Description
Device	Exactement un		Informations de l'analyseur générant un journal
Policy	Exactement un		Informations acheminées dans l'analyseur pour la connexion
CreateTime	Exactement un	DATETIME	Heure de création du journal
Source	Exactement un		Source de l'événement à l'origine de la connexion
Target	Exactement un		Informations sur la destination d'un événement à l'origine d'une connexion
SourceNAT	Exactement un		Informations sur la source NAT dans l'événement à l'origine de la connexion
TargetNAT	Exactement un		Informations de destination NAT d'un événement à l'origine d'une connexion
AdditionalData	Zéro ou plus		Informations supplémentaires générées par le détecteur qui ne sont pas dans les autres classes

8.2.1.1 Classe Policy

La classe Policy (politique) fournit les informations sur la suite à donner ("action") afin d'indiquer comment traiter une session dans l'analyseur. Voir la Figure 5.

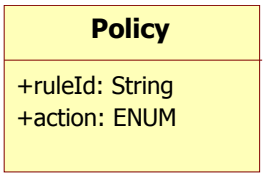

Figure 5 – Classe Policy

Les valeurs autorisées pour l'attribut "action" de la classe Policy (voir le Tableau 6) sont données dans le Tableau 7.

Tableau 6 – Attributs de la classe Policy

Attribut	Utilisation	Type de données	Description
ruleId	Facultative	STRING	Identificateur unique de la politique de pare-feu qui doit être généré par la connexion
action	Facultative	ENUM	Classification selon le pare-feu de l'opération causée par la connexion, Valeur par défaut: Unknown (inconnu)

Tableau 7 – Valeur de l'attribut "action"

Valeur	Mot clé	Définition
0	unknown (inconnu)	Si le comportement est inconnu
1	pass (laisser passer)	Si la connexion doit être autorisée
2	block (bloquer)	Si la connexion doit être refusée
3	protect (protéger)	Si le paquet transmis doit être chiffré ou si un code de vérification de l'intégrité doit être inséré [journal de réseau privé virtuel (VPN)].
4	reject (rejeter)	Si la connexion doit être rejetée. Toutefois, il faut fournir des messages d'erreur lorsque l'accès est refusé.

8.2.2 Classe Heartbeat

Les analyseurs utilisent des messages Heartbeat (pulsation) pour indiquer leur état actuel à leurs gestionnaires. Ces messages doivent être envoyés à intervalles réguliers, par exemple toutes les dix minutes ou toutes les heures. La réception d'un message Heartbeat envoyé par un analyseur indique au gestionnaire que l'analyseur fonctionne; l'absence de message Heartbeat (ou plus probablement, l'absence d'un certain nombre de messages Heartbeat consécutifs) indique une défaillance de l'analyseur ou de sa connexion réseau.

Tous les gestionnaires doivent prendre en charge la réception de message Heartbeat; toutefois, l'utilisation de ces messages par les analyseurs est facultative. Les développeurs de logiciels gestionnaires devraient prévoir la possibilité de configurer le logiciel en décidant, pour chaque analyseur, s'il utilise ou non les messages Heartbeat. Un message Heartbeat est composé de plusieurs classes d'agrégat, comme indiqué dans la Figure 6.

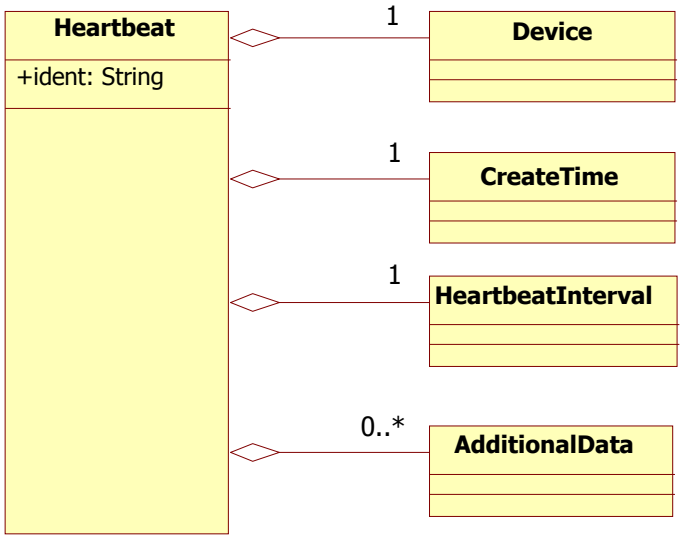

Figure 6 – Classes d'agrégat de la classe Heartbeat

Les informations concernant l'attribut et les composants de la classe Heartbeat sont présentées respectivement dans les Tableaux 8 et 9.

Tableau 8 – Attribut de la classe Heartbeat

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique pour la classe Heartbeat

Tableau 9 – Composants de la classe Heartbeat

Classes	Agrégation	Type de données	Description
Device	Exactement un		Informations d'identification de l'analyseur à l'origine du message Heartbeat
CreateTime	Exactement un	DATETIME	Heure de création du message Heartbeat
HeartbeatInterval	Exactement un	INTEGER	Intervalle en secondes auquel les messages de pulsations sont générés.
AdditionalData	Zéro ou un		Informations incluses par l'analyseur qui ne correspondent pas au modèle de données.

8.2.3 Classes essentielles

Les classes essentielles (Device, CreateTime, Source, Target, SourceNAT, TargetNAT et AdditionalData) sont les parties principales des classes Connect et Heartbeat, comme indiqué dans la Figure 7. Ces différentes classes sont décrites ci-après.

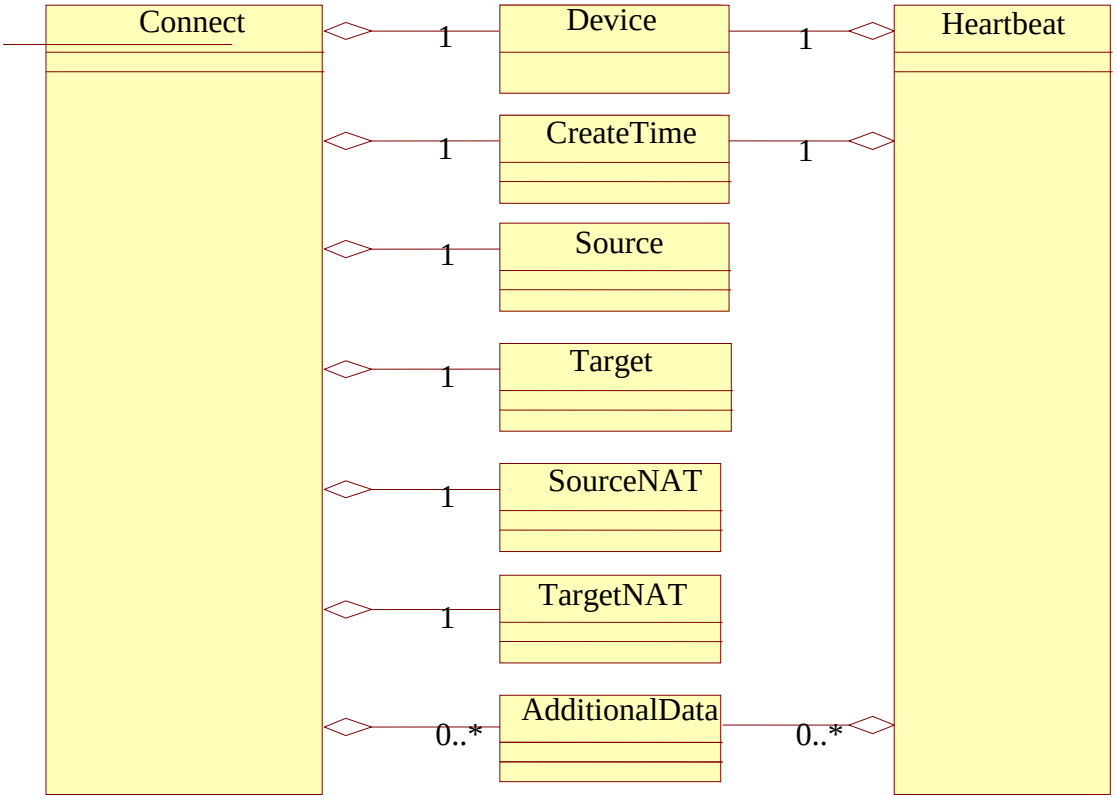

Figure 7 – Classes essentielles

8.2.3.1 Classe Device

La classe Device (dispositif) identifie l'analyseur à l'origine du message Connect ou Heartbeat. Un seul dispositif peut être codé pour chaque message Connect ou Heartbeat, qui sera le dispositif dont provient la connexion ou la pulsation.

La classe Device est composée de trois classes d'agrégat, comme indiqué dans la Figure 8.

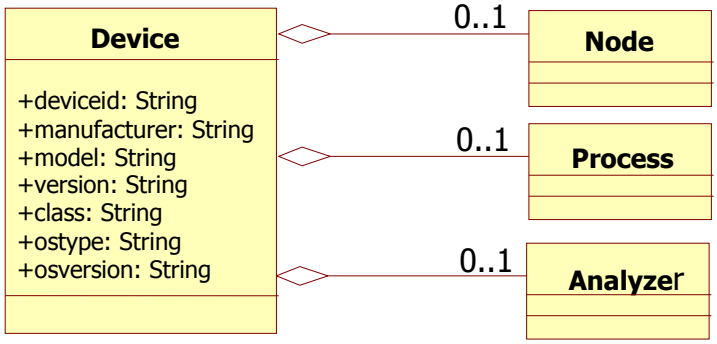

Figure 8 – Classes d'agrégat de la classe Device

La classe Device a sept attributs, comme indiqué dans le Tableau 10.

Tableau 10 – Attributs de la classe Device

Attribut	Utilisation	Type de données	Description
deviceid	Facultative	STRING	Identificateur unique du dispositif. Si le dispositif utilise l'attribut "ident" sur d'autres classes pour fournir des identificateurs uniques pour ces objets, il doit alors également fournir un attribut "deviceid" valide.
Manufacturer	Facultative	STRING	Fabricant du logiciel ou du matériel du dispositif.
Model	Facultative	STRING	Nom/numéro de modèle du logiciel/matériel du dispositif.
Version	Facultative	STRING	Numéro de version du logiciel/matériel du dispositif.
Class	Facultative	STRING	Classe du logiciel/matériel du dispositif.
Ostype	Facultative	STRING	Nom du système d'exploitation.
osversion	Facultative	STRING	Version du système d'exploitation.

Pour les systèmes compatibles POSIX 1003.1, la valeur de l'attribut "ostype" est celle renvoyée dans le champ utsname.sysname par l'appel système uname(), ou le résultat de la commande “uname –s”.

Pour les systèmes compatibles POSIX 1003.1, la valeur de l'attribut "osversion" est celle renvoyée dans le champ utsname.release par l'appel système uname(), ou le résultat de la commande “uname –r”.

Le contenu des attributs “manufacturer”, “model”, “version” et “class” dépend du fabricant, mais ces attributs peuvent être utilisés ensemble pour identifier différents types d'analyseurs.

Les classes d'agrégat qui composent une classe Device sont décrites dans le Tableau 11.

Tableau 11 – Composants de la classe Device

Classes	Agrégation	Type de données	Description
Node	Zéro ou un		Informations sur l'hôte ou le dispositif sur lequel l'analyseur est installé (adresse réseau, nom du réseau, etc.)
Process	Zéro ou un		Informations sur le processus dans le cadre duquel l'analyseur fonctionne.
Analyser	Zéro ou un		Informations sur l'analyseur par lequel le message est peut-être passé.

8.2.3.2 Classe CreateTime

La classe CreateTime (créer horodatage) est utilisée pour indiquer la date et l'heure sur le dispositif. Si cette différence devrait ensuite servir à ajuster les heures dans les éléments <CreateTime> et < NTP timestamps >, alors les timbres horodateurs NTP devraient eux aussi être ajustés.

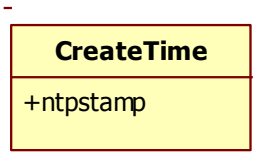

Figure 9 – Classe CreateTime

L'attribut de la classe CreateTime est décrit dans le Tableau 12.

Tableau 12 – Attribut de la classe CreateTime

Attribut	Utilisation	Type de données	Description
ntpstamp	Obligatoire	ntpstamp	Informations sur l'heure dans le dispositif.

8.2.3.3 Classe Source

La classe Source contient des informations sur la ou les sources possibles du ou des événements qui ont généré une session. Un événement peut avoir plus d'une source (par exemple, dans le cas d'une attaque de type déni de service réparti).

La classe Source est composée de trois classes d'agrégat, comme indiqué dans la Figure 10.

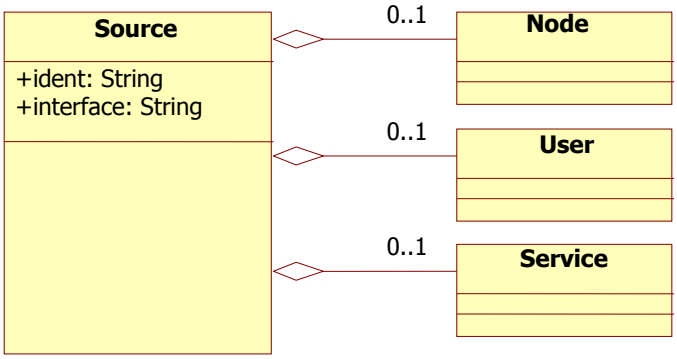

Figure 10 – Classes d'agrégat de la classe Source

La classe Source a deux attributs, comme indiqué dans le Tableau 13.

Tableau 13 – Attributs de la classe Source

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de cette source.
Interface	Facultative	STRING	Peut être utilisé par un dispositif réseau avec de multiples interfaces pour indiquer l'interface sur laquelle cette source a été vue.

Les classes d'agrégat qui composent la classe Source sont décrites dans le Tableau 14.

Tableau 14 – Composants de la classe Source

Classes	Agrégation	Type de données	Description
Node	Zéro ou un		Informations sur l'hôte ou le dispositif qui apparaît être la cause des événements (adresse réseau, nom du réseau, etc.).
User	Zéro ou un		Informations sur l'utilisateur qui apparaît être la cause du ou des événements.
Service	Zéro ou un		Informations sur le service de réseau concerné par le ou les événements.

8.2.3.4 Classe Target

La classe Target (cible) contient des informations sur la ou les cibles possibles du ou des événements qui ont généré une session. Un événement peut avoir plus d'une cible (par exemple, dans le cas d'un balayage des ports).

La classe Target class est composée de trois classes d'agrégat, comme indiqué dans la Figure 11.

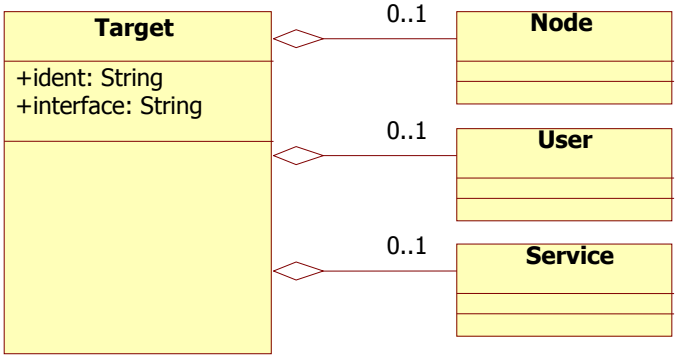

Figure 11 – Classes d'agrégat de la classe Target

La classe Target a deux attributs, comme indiqué dans le Tableau 15.

Tableau 15 – Attributs de la classe Target

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de cette cible.
Interface	Facultative	STRING	Peut être utilisé par un dispositif réseau avec de multiples interfaces pour indiquer l'interface sur laquelle cette cible a été vue.

Les classes d'agrégat qui composent la classe Target sont décrites dans le Tableau 16.

Tableau 16 – Composants de la classe Target

Classes	Agrégation	Type de données	Description
Node	Zéro ou un		Informations sur l'hôte ou le dispositif vers lequel le ou les événements (adresse réseau, nom du réseau, etc.) sont dirigés.
User	Zéro ou un		Informations sur l'utilisateur vers lequel le ou les événements sont dirigés.
Service	Zéro ou un		Informations sur le service de réseau concerné par le ou les événements.

8.2.3.5 Classe SourceNAT

La classe SourceNAT (traduction NAT de la source) contient des informations sur la ou les sources possibles du ou des événements NAT qui ont généré une session. Un événement peut avoir plus d'une source transformée par traduction NAT.

La classe SourceNAT est composée de trois classes d'agrégat, comme indiqué dans la Figure 12.

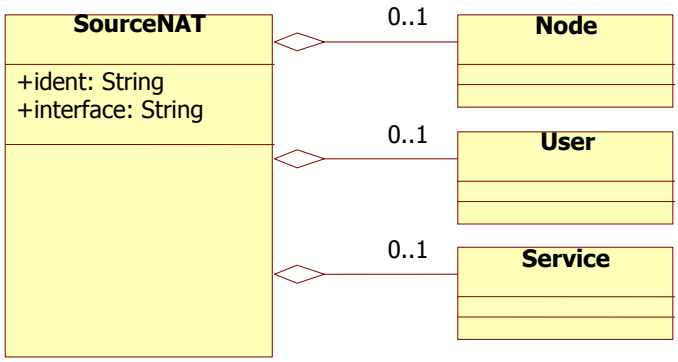

Figure 12 – Classes d'agrégat de la classe SourceNAT

La classe SourceNAT a deux attributs, comme indiqué dans le Tableau 17.

Tableau 17 – Attributs de la classe SourceNAT

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de cette source transformée par traduction NAT.
interface	Facultative	STRING	Peut être utilisé par un dispositif réseau avec de multiples interfaces pour indiquer l'interface sur laquelle cette source transformée par traduction NAT a été vue.

Les classes d'agrégat qui composent la classe SourceNAT class sont décrites dans le Tableau 18.

Tableau 18 – Composants de la classe SourceNAT

Classes	Agrégation	Type de données	Description
Node	Zéro ou un		Informations sur l'hôte ou le dispositif qui apparaît être la cause des événements (adresse réseau, nom du réseau, etc.).
User	Zéro ou un		Informations sur l'utilisateur qui apparaît être la cause du ou des événements.
Service	Zéro ou un		Informations sur le service de réseau concerné par le ou les événements.

8.2.3.6 Classe TargetNAT

La classe TargetNAT (traduction NAT de la cible) contient des informations sur la ou les cibles possibles du ou des événements NAT qui ont généré une session. Un événement peut avoir plus d'une cible transformée par traduction NAT.

La classe TargetNAT est composée de trois classes d'agrégat, comme indiqué dans la Figure 13.

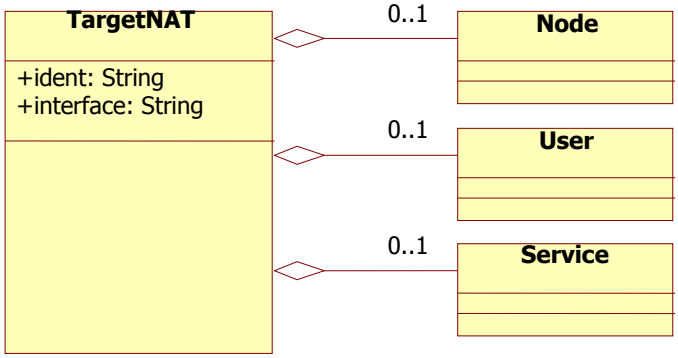

Figure 13 – Classes d'agrégat de la classe TargetNAT

La classe TargetNAT a deux attributs, comme indiqué dans le Tableau 19.

Tableau 19 – Attributs de la classe TargetNAT

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de cette cible transformée par traduction NAT.
interface	Facultative	STRING	Peut être utilisé par un dispositif réseau avec de multiples interfaces pour indiquer l'interface sur laquelle cette cible transformée par traduction NAT a été vue.

Les classes d'agrégat qui composent la classe Target sont décrites dans le Tableau 20.

Tableau 20 – Composants de la classe TargetNAT

Classes	Agrégation	Type de données	Description
Node	Zéro ou un		Informations sur l'hôte ou le dispositif vers lequel le ou les événements (adresse réseau, nom du réseau, etc.) sont dirigés.
User	Zéro ou un		Informations sur l'utilisateur vers lequel le ou les événements sont dirigés.
Service	Zéro ou un		Informations sur le service de réseau concerné par le ou les événements.

8.2.3.7 Classe AdditionalData

La classe AdditionalData (données supplémentaires) fournit des informations qui ne peuvent pas être représentées par le modèle de données SIMEF. Elle peut être utilisée pour fournir des données atomiques (entiers, chaînes, etc.) dans les cas où un petit volume d'informations supplémentaires seulement doit être envoyé; elle peut également être utilisée pour assurer une extension du modèle de données et de la définition DTD afin de prendre en charge la transmission de données complexes (par exemple, en-têtes de paquet).

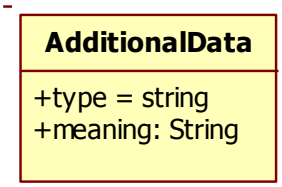

Figure 14 – Classe AdditionalData

La classe AdditionalData a deux attributs, comme indiqué dans le Tableau 21.

Tableau 21 – Attributs de la classe AdditionalData

Attribut	Utilisation	Type de données	Description
type	Obligatoire	ENUM	Type de données décrivant la signification du contenu d'un élément. Valeur par défaut: chaîne
meaning	Facultative	STRING	Chaîne décrivant la signification du contenu d'un élément.

On trouvera dans le Tableau 22 les types de classe AdditionalData et les valeurs autorisées pour cet attribut.

Tableau 22 – Valeur de l'attribut Type

Valeur	Mot clé	Définition
0	boolean (booléen)	L'élément contient une valeur booléenne, c'est-à-dire les chaînes "true" (vrai) ou "false" (faux).
1	byte (octet)	Le contenu de l'élément est un octet unique de 8 bits.
2	character (caractère)	Le contenu de l'élément est un caractère seul.
3	date-time (horodatage)	Le contenu de l'élément est une chaîne d'horodatage
4	integer (entier)	Le contenu de l'élément est un entier
5	ntpstamp (timbre ntp)	Le contenu de l'élément est un timbre horodateur NTP
6	portlist (liste de ports)	Le contenu de l'élément est une liste de ports
7	real (nombre réel)	Le contenu de l'élément est un nombre réel
8	string (chaîne)	Le contenu de l'élément est une chaîne
9	Byte-string (octet-chaîne)	Le contenu de l'élément est un byte[]
10	xml	Le contenu de l'élément est des données avec étiquette XML

Ces valeurs pour la classe AdditionalData dépendent du fabriquant/de la mise en oeuvre; la méthode permettant de faire en sorte que les gestionnaires comprennent les chaînes envoyées par les analyseurs ne relève pas de la présente Recommandation.

8.2.4 Les classes d'appui

Les classes d'appui constituent les parties principales des classes essentielles, qui les partagent.

8.2.4.1 Classe Node

La classe Node (noeud) est utilisée pour identifier les hôtes et les autres dispositifs de réseau (routeurs, commutateurs, etc.).

La classe Node est composée de trois classes d'agrégat, comme indiqué dans la Figure 15. On trouvera respectivement dans les Tableaux 23, 24 et 25 les attributs, les valeurs de l'attribut de type et les composants de la classe Node.

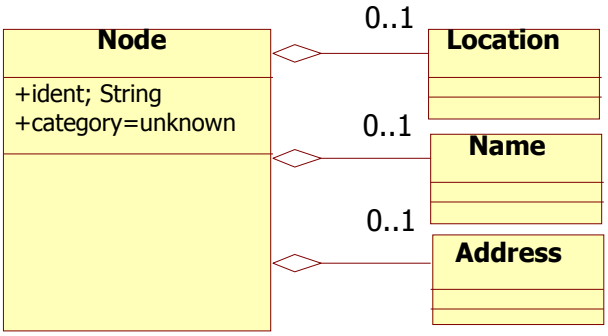

Figure 15 – Classes d'agrégat de la classe Node

Tableau 23 – Attributs de la classe Node

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique du noeud; voir § 7.2.9.
category	Facultative	ENUM	Le "domaine" auprès duquel l'information sur le nom a été obtenue. Valeur par défaut = unknown (inconnu)

Tableau 24 – Valeur de l'attribut Type

Valeur	Mot clé	Définition
0	Unknown (inconnu)	Domaine inconnu ou non applicable
1	ads	Service d'annuaire évolué Windows 2000
2	afs	Andrew File System (Transarc)
3	coda	Système de fichiers distribués Coda
4	dfs	Système de fichiers distribués (IBM)
5	dns	Système de noms de domaine
6	hosts	Fichier d'hôtes locaux
7	kerberos	Domaine Kerberos
8	nds	Services d'annuaire Novell
9	nis	Services d'information réseau (Sun)
10	nisplus	Services d'information réseau plus (Sun)
11	nt	Domaine Windows NT
12	wfw	Windows for Workgroups

Tableau 25 – Composants de la classe Node

Classes	Agrégation	Type de données	Description
Location	Zéro ou un	STRING	Emplacement de l'équipement
Name	Zéro ou un	STRING	Nom de l'équipement. Cette information doit être fournie si aucune information Address n'est fournie.
Address	Zéro ou un		Adresse réseau ou matérielle de l'équipement. A moins qu'un nom (voir ci-dessus) soit fourni, au moins une adresse doit être spécifiée.

8.2.4.2 Classe Address

La classe Address (adresse) est utilisée pour représenter les adresses réseau ou matérielles ou les adresses d'application.

La classe Address est composée de deux classes d'agrégat, comme indiqué dans la Figure 16.

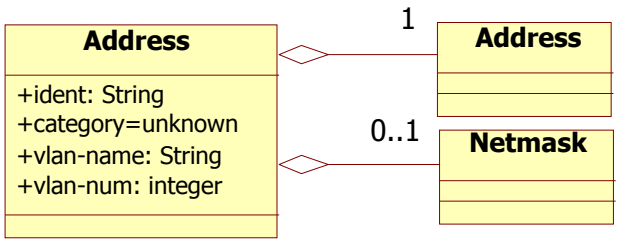

Figure 16 – Classes d'agrégat de la classe Address

On trouvera respectivement dans les Tableaux 26, 27 et 28 les attributs, les valeurs de l'attribut de type et les composants de la classe Address.

Tableau 26 – Attributs de la classe Address

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de l'adresse; voir le § 7.2.9.
category	Facultative	ENUM	Type d'adresse représenté. Les valeurs autorisées pour cet attribut sont présentées ci-après. Valeur par défaut: unknown (inconnu)
vlan-name	Facultative	STRING	Nom du réseau local (LAN) (LAN virtuel) auquel l'adresse appartient.
Vlan-num	Facultative	INTEGER	Numéro du réseau local (LAN virtuel) auquel l'adresse appartient.

Tableau 27 – Valeur de l'attribut Type

Valeur	Mot clé	Définition
0	unknown (inconnu)	Type d'adresse inconnu
1	atm	Adresse de réseau à mode de transfert asynchrone
2	e-mail	Adresse de courrier électronique ([b-IETF RFC 2822])
3	lotus-notes	Adresse de courrier électronique Lotus Notes
4	Mac	Adresse de commande d'accès au support (MAC)
5	Sna	Adresse d'architecture de réseau partagé (SNA) IBM
6	Vm	Adresse de courrier électronique IBM VM ("PROFS")
7	ipv4-addr	Adresse d'hôte IPv4 en notation décimale avec point (a.b.c.d)
8	ipv4-addr-hex	Adresse d'hôte IPv4 en notation hexadécimale
9	ipv4-net	Adresse réseau IPv4 en notation décimale avec point, barre oblique, bits significatifs (a.b.c.d/nn)
10	ipv4-net-mask	Adresse réseau IPv4 en notation décimale avec point, barre oblique, masque de réseau en notation décimale avec point (a.b.c.d./w.x.y.z)
11	ipv6-addr	Adresse d'hôte IPv6
12	ipv6-addr-hex	Adresse d'hôte IPv6 en notation hexadécimale
13	ipv6-net	Adresse réseau IPv6, barre oblique, bits significatifs
14	Ipv6-net-mask	Adresse réseau IPv6, barre oblique, masque de réseau

Tableau 28 – Composants de la classe Address

Classes	Agrégation	Type de données	Description
Address	Exactement un	STRING	Informations d'adresse. Le format de ces données dépend de l'attribut de catégorie.
Netmask	Zéro ou un	STRING	Masque de réseau pour l'adresse, le cas échéant.

8.2.4.3 Classe User

La classe User (utilisateur) est utilisée pour décrire les utilisateurs. Elle sert en premier lieu de classe de "conteneur" pour la classe d'agrégat "UserId" comme indiqué dans la Figure 17.

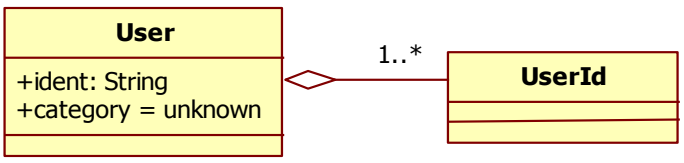

Figure 17 – Classes d'agrégat de la classe User

On trouvera respectivement dans les Tableaux 29, 30 et 31 les attributs, les valeurs de l'attribut de type et les composants de la classe User.

Tableau 29 – Attributs de la classe User

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique de l'utilisateur; voir le § 7.2.9.
category	Facultative	ENUM	Type d'utilisateur représenté. Les valeurs autorisées pour cet attribut sont présentées ci-après. Valeur par défaut = unknown (inconnu)

Tableau 30 – Valeur de l'attribut Type

Value	Mot clé	Définition
0	unknown (inconnu)	Type d'utilisateur inconnu
1	application	Application
2	os-device	Système d'exploitation ou dispositif

Tableau 31 – Composants de la classe User

Classes	Agrégation	Type de données	Description
UserId	Un ou plus		Identification d'un utilisateur, comme indiqué par son attribut Type

8.2.4.3.1 Classe UserId

La classe UserId (identificateur d'utilisateur) fournit des informations précises sur un utilisateur. Plusieurs identificateurs d'utilisateur peuvent être utilisés dans la classe User pour indiquer les tentatives de passage d'un utilisateur à un autre ou pour fournir des informations complètes sur les privilèges d'un utilisateur (ou d'un processus).

La classe UserId est composée de deux classes d'agrégat, comme indiqué dans la Figure 18.

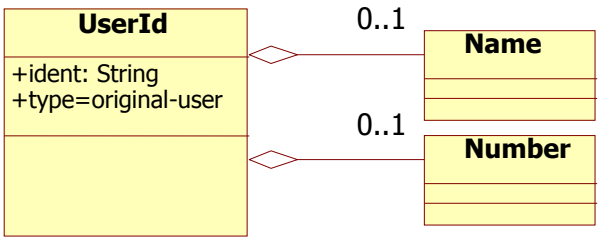

Figure 18 – Classes d'agrégat de la classe UserId

On trouvera respectivement dans les Tableaux 32 et 33 les attributs et les valeurs de l'attribut de type de la classe UserId.

Tableau 32 – Attributs de la classe UserId

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Type d'identificateur unique pour l'identificateur d'utilisateur; voir le § 7.2.9.
type	Facultative	ENUM	Type d'informations d'utilisateur représenté. Les valeurs autorisées pour cet attribut sont présentées ci-après. Valeur par défaut = original-user (utilisateur initial)

Tableau 33 – Valeur de l'attribut type

Valeur	Mot clé	Définition
0	current-user	Identificateur d'utilisateur actuellement utilisé par l'utilisateur ou le processus.
1	original-user	Identité effective de l'utilisateur ou du processus sur lequel porte le rapport. Sur les systèmes qui a) effectuent des opérations de vérification et b) prennent en charge l'extraction d'un identificateur d'utilisateur à partir du jeton "audit id", cette valeur devrait être utilisée. Sur les systèmes qui ne permettent pas cette prise en charge, et lorsque l'utilisateur s'est connecté au système, le jeton "login id" devrait être utilisé.
2	target-user	Identificateur d'utilisateur que l'utilisateur ou le processus essaie de devenir. S'applique, dans les systèmes Unix par exemple, lorsque l'utilisateur tente d'utiliser “su”, “rlogin”, “telnet”, etc.
3	user-privs	Autre identificateur d'utilisateur que l'utilisateur ou le processus a la capacité d'utiliser ou identificateur d'utilisateur associé à une permission d'accès aux fichiers. De multiples éléments UserId de ce type peuvent être utilisés pour spécifier une liste de privilèges.
4	current-group	Identificateur de groupe (le cas échéant) actuellement utilisé par l'utilisateur ou le processus.
5	group-privs	Un autre identificateur de groupe que le groupe ou le processus a la capacité d'utiliser ou identificateur de groupe associé à une permission d'accès aux fichiers. Par exemple, sur les systèmes Unix utilisant la distribution de logiciels de Berkeley (BSD), de multiples éléments UserId de ce type seront utilisés pour inclure tous les identificateurs de groupe dans la "liste de groupes".
6	other-privs	Non utilisé dans le contexte avec un utilisateur, un groupe ou un processus, uniquement utilisé dans le contexte avec un fichier. Permissions d'accès aux fichiers accordées aux utilisateurs qui ne correspondent pas aux permissions utilisateur ou de groupe associées au fichier.

Les classes d'agrégat qui composent la classe UserId sont décrites dans le Tableau 34.

Tableau 34 – Composants de la classe UserId

Classes	Agrégation	Type de données	Description
Name	Zéro ou un	STRING	Nom de l'utilisateur ou du groupe.
Num	Zéro ou un	INTERGER	Numéro de l'utilisateur ou du groupe.

8.2.4.4 Classe Process

La classe Process (processus) est utilisée pour décrire les processus en cours d'exécution sur les sources, les cibles et les analyseurs.

La classe Process est composée de cinq classes d'agrégat, comme indiqué dans la Figure 19.

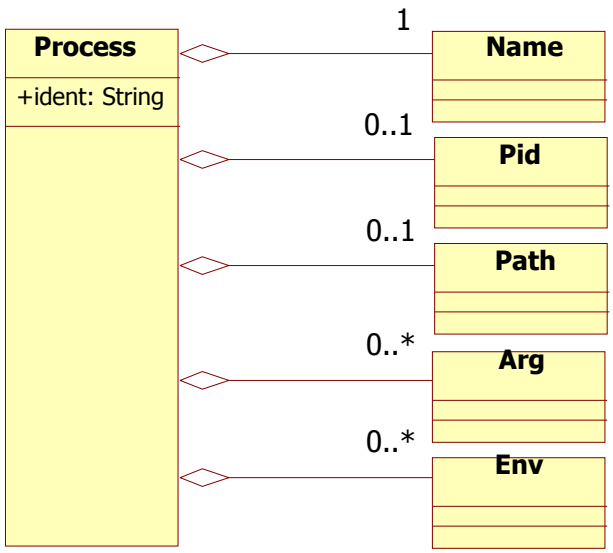

Figure 19 – Classes d'agrégat de la classe Process

La classe Process a un attribut (voir le Tableau 35).

Tableau 35 – Attribut de la classe Process

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique du processus; voir le § 7.2.9.

Les classes d'agrégat qui composent la classe Process sont décrites dans le Tableau 36.

Tableau 36 – Composants de la classe Process

Classes	Agrégation	Type de données	Description
Name	Exactement un	STRING	Nom du programme en cours d'exécution.
Pid	Zéro ou un	INTEGER	Identificateur du processus
Path	Zéro ou un	STRING	Chemin complet du programme en cours d'exécution.
Arg	Zéro ou plus	STRING	Argument de ligne de commande vers le programme.
Env	Zéro ou plus	STRING	Chaîne d'environnement associée au processus; généralement au format “VARIABLE=value”.

Dans la classe Process, la classe de nom est un nom abrégé et de multiples arguments peuvent être spécifiés avec de multiples utilisations de l'élément "arg". De multiples chaînes d'environnement peuvent être spécifiées avec de multiples utilisations de l'élément "env".

8.2.4.5 Classe Service

La classe Service décrit les services réseau sur les sources et les cibles. Elle peut identifier les services par leur nom, le port, la liste de ports et le protocole. Lorsque la classe Service est présente en tant que classe d'agrégat de la classe Source, il est entendu que le service est un service à l'origine de l'activité considérée et que ce service est "attaché" aux informations Node, Process et User également contenues dans la classe Source. De même, lorsque la classe Service est présente en tant que classe d'agrégat de la classe Target, il est entendu que le service est un service qui est visé par l'activité considérée et que ce service est "attaché" aux informations Node, Process et User également contenues dans la classe Target. Si la classe Service est présente à la fois dans la classe Source et dans la classe Target, alors les informations à ces deux endroits devraient être les mêmes. Si les informations sont les mêmes aux deux endroits et que les responsables de la mise en oeuvre souhaitent qu'elles soient acheminées à un seul endroit, ils devraient les spécifier en tant qu'agrégat de la classe Target.

La classe Service est composée de quatre classes d'agrégat, comme indiqué dans la Figure 20.

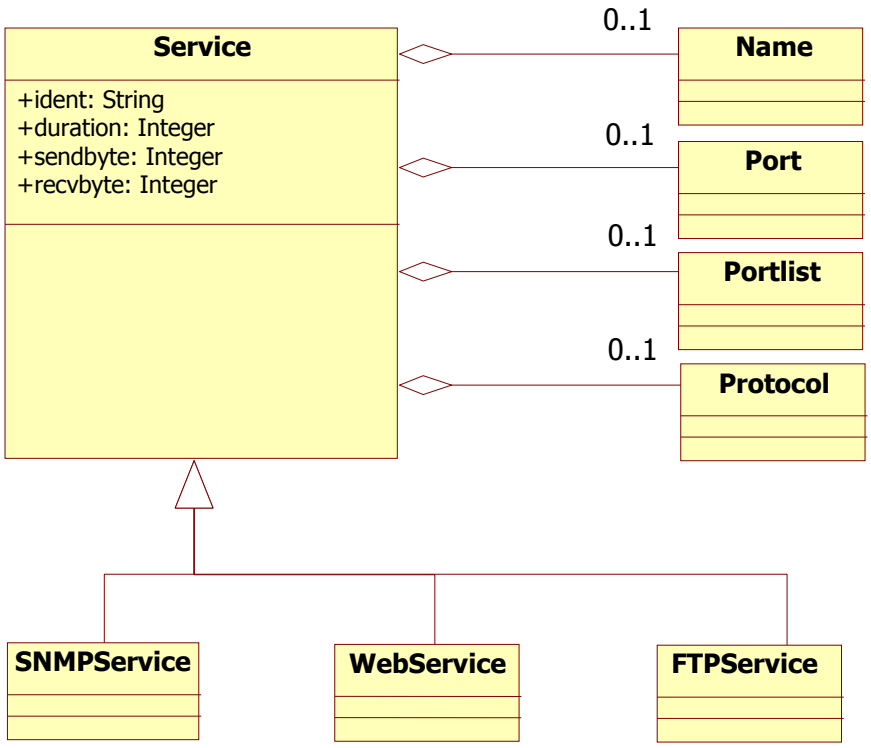

Figure 20 – Classes d'agrégat de la classe Service

La classe Service a quatre attributs, décrits dans le Tableau 37.

Tableau 37 – Attributs de la classe Service

Attribut	Utilisation	Type de données	Description
ident	Facultative	STRING	Identificateur unique du service; voir le § 7.2.9.
duration	Facultative	INTEGER	Durée de connexion
sendbyte	Facultative	INTEGER	Nombre d'octets lors de l'envoi après connexion
recvByte	Facultative	INTEGER	Nombre d'octets lors de la réception après connexion

Les classes d'agrégat qui composent la classe Service sont décrites dans le Tableau 38.

Tableau 38 – Composants de la classe Service

Classes	Agrégation	Type de données	Description
Name	Zéro ou un	STRING	Nom du service. A chaque fois que cela est possible, le nom figurant dans la liste de ports bien connus établie par l'Autorité de gestion des numéros Internet attribués (IANA) devrait être utilisé.
Port	Zéro ou un	INTEGER	Numéro du port utilisé.
Portlist	Zéro ou un	PORTLIST	Liste des numéros de port utilisés, voir le § 7.2.8 pour les règles de formatage.
Protocol	Zéro ou un	STRING	Informations supplémentaires sur le protocole utilisé.

8.2.4.5.1 Classe WebService

La classe WebService (service web) achemine les informations supplémentaires liées au trafic web.

La classe WebService est composée de quatre classes d'agrégat, comme indiqué dans la Figure 21.

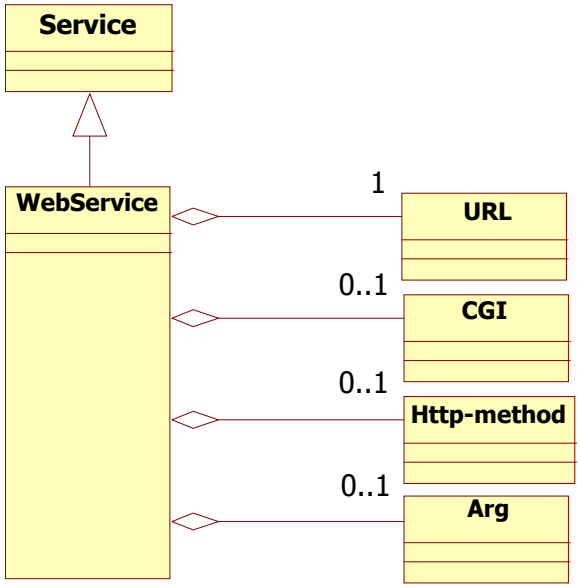

Figure 21 – Classes d'agrégat de la classe WebService

Les classes d'agrégat qui composent la classe WebService sont décrites dans le Tableau 39.

Tableau 39 – Composants de la classe WebService

Classes	Agrégation	Type de données	Description
URL	Exactement un	STRING	Localisateur uniforme de ressources (URL) figurant dans la demande.
CGI	Zéro ou un	STRING	Script d'interface de passerelle commune (CGI) figurant dans la demande, sans argument.
Http-method	Zéro ou un	STRING	Méthode de protocole de transfert hypertexte (HTTP) (PUT, GET) utilisée dans la demande.
Arg	Zéro ou un	STRING	Arguments du script CGI.

8.2.4.5.2 Classe SNMPService

La classe SNMPService (service SNMP) achemine des informations supplémentaires concernant le trafic de protocole simple de gestion de réseau (SNMP).

La classe SNMPService est composée de huit classes d'agrégat, comme indiqué dans la Figure 22.

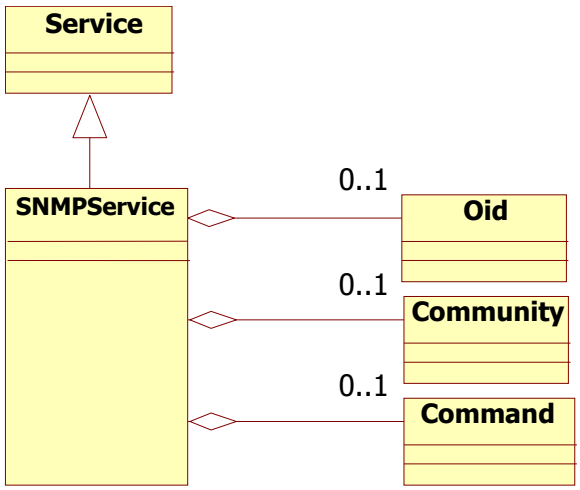

Figure 22 – Classes d'agrégat de la classe SNMPService

Les classes d'agrégat qui composent la classe SNMPService sont décrites dans le Tableau 40.

Tableau 40 – Composants de la classe SNMPService

Classes	Agrégation	Type de données	Description
Oid	Zéro ou un	STRING	Identificateur d'objet figurant dans la demande.
Community	Zéro ou un	STRING	Chaîne communautaire de l'objet
Command	Zéro ou un	STRING	Commande envoyée au serveur SNMP (GET, SET, etc.).

8.2.4.5.3 Classe FTPService

La classe FTPService (service FTP) achemine des informations supplémentaires concernant le trafic de protocole de transfert de fichier (FTP).

La classe FTPService est composée de deux classes d'agrégat, comme indiqué dans la Figure 23.

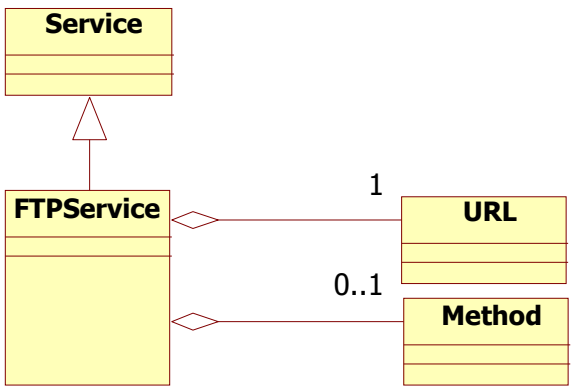

Figure 23 – Classes d'agrégat de la classe FTPService

Les classes d'agrégat qui composent la classe FTPService sont décrites dans le Tableau 41.

Tableau 41 – Composants de la classe FTPService

Classes	Agrégation	Type de données	Description
URL	Exactement un	STRING	URL figurant dans la demande.
Method	Zéro ou un	STRING	Méthode FTP (PUT, GET) utilisée dans la demande.

9 Considérations liées à la sécurité

On trouvera dans le présent paragraphe certaines considérations particulières dont les responsables de la mise en oeuvre du format SIMEF doivent tenir compte.

La présente Recommandation décrit le modèle d'information pour le format d'échange de messages sur les informations de session (SIMEF) et fournit un modèle de données associé, spécifié en langage XML. Le format SIMEF définit une représentation de modèle de données permettant de partager les informations sur les journaux de session de couche transport concernant la gestion centralisée de la sécurité du réseau et le système d'échange d'informations sur la sécurité.

Bien qu'aucune question de sécurité ne concerne directement le format de ces données, les données elles-mêmes peuvent contenir des informations sensibles pour la sécurité dont il peut être nécessaire de protéger la confidentialité, l'intégrité ou la disponibilité.

Selon la présente Recommandation, les systèmes utilisés pour recueillir, transmettre, traiter et stocker ces données devraient être protégés contre les utilisations non autorisées et les données elles-mêmes devraient être protégées contre les accès non autorisés. Les moyens permettant d'assurer cette protection n'entrent pas dans le cadre de la présente Recommandation.

Appendice I

Exemple et schéma SIMEF

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent Appendice donne un exemple de schéma XML pour le modèle SIMEF. On trouvera ci-après un exemple de schéma XML et un exemple de schéma SYSLOG permettant de coder les informations de session selon le modèle SIMEF.

I.1 Schéma SIMEF

I.1.1 Schéma XML

```
<?xml version="1.0" encoding="UTF-8"?>

<simef:SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef/">
     <Connect ident="1008380" criticality="normal">
        <Device Deviceid="TTA-FW" model="FW1000">
           <Node>
              <Address category="ipv4-addr">
                <address>1.1.1.1</address>
              </Address>
           </Node>
        </Device>
        <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                  2010-08-18T15:41:28+00:00
           </CreateTime>
        <Policy Ruleid="45" action="pass"></Policy>
           <Source>
           <Node>
              <Address category="ipv4-addr">
                <address>2.2.2.2</address>
              </Address>
           </Node>
           <Service duration="9" size="144">
              <port>38168</port>
              <protocol>17</protocol>
           </Service>
        </Source>
        <Target>
           <Node>
              <Address category="ipv4-addr">
                <address>3.3.3.3</address>
              </Address>
           </Node>
           <Service duration="9" size="0">
              <name>dns</name>
              <port>53</port>
              <protocol>17</protocol>
           </Service>
        </Target>
        <Classification origin="vendor-specific">
           <name>45</name>
        </Classification>
     </Connect>
</simef:SIMEF-Message>
```

I.1.2 Schéma SYSLOG

```
  2014-03-18  15:41:28  Local0.Notice  1.1.1.1  TTA:  TTA-FW  device_id=  TTA
[Root]system-notification-00257(traffic):    start_time="2014-03-18    15:41:19"
duration=9 policy_id=45 service=dns proto=17 src zone=Untrust dst zone=Trust
action=Permit sent=144 rcvd=0 src=2.2.2.2 dst=3.3.3.3 src_port=38168 dst_port=53
src-xlated ip=2.2.2.2 port=38168 dst-xlated ip=3.3.3.3 port=53 session_id=1008380
reason=Close - AGE OUT<000>
```

I.2 Exemples de modèle SIMEF

I.2.1 Permission de pare-feu

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008380" criticality="1">
              <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
                            </Address>
                     </Node>
              </Device>
              <Policy Ruleid="45" action="1"></Policy>
              <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                     2014-03-18T15:41:28+00:00
              </CreateTime>
              <Source>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>2.2.2.2</address>
                            </Address>
                     </Node>
                        <Service duration="9" size="144">
                            <port>38168</port>
                            <protocol>17</protocol>
                     </Service>
              </Source>
              <Target>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>3.3.3.3</address>
                            </Address>
                     </Node>
                     <Service duration="9" size="0">
                            <name>dns</name>
                            <port>53</port>
                            <protocol>17</protocol>
                     </Service>
              </Target>
              <Classification origin="2">
                     <name>45</name>
              </Classification>
       </Connect>
</SIMEF-Message>
```

I.2.2 Journal de VPN

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008057" criticality="1">
              <Device Deviceid="TTA-VPN" manufacturer="TTA" model="VPN1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
```

```
                        </Address>
                    </Node>
                </Device>
                <Policy ruleid="700" action="3"></Policy>
                <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                    2014-03-19T12:51:22+00:00
                </CreateTime>
                <Source>
                    <Node>
                        <Address category="ipv4-addr">
                            <address>2.2.2.2</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="16905">
                        <port>59078</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Source>
                <Target>
                    <Node>
                        <Address category="ipv4-addr">
                            <address>3.3.3.3</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="1448">
                        <name>junos-http</name>
                        <port>80</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Target>
                <Classification origin="2">
                    <name>700</name>
                </Classification>
        </Connect>
</SIMEF-Message>
```

I.2.3 Journal de NAT

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
        <Connect ident="1009632" criticality="1">
                <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                <Node>
                        <Address category="ipv4-addr">
                            <address>1.1.1.1</address>
                        </Address>
                    </Node>
                </Device>
                <Policy ruleid="57" action="1"></Policy>
                <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                    2014-03-19T16:21:12+00:02
                </CreateTime>
                <Source>
                    <Node>
                        <Address ident="" category="ipv4-addr”>
                            <address>2.2.2.2</address>
                        </Address>
                    </Node>
                    <Service duration="41" size="16905">
                        <port>59078</port>
                        <protocol>TCP</protocol>
                    </Service>
                </Source>
                <Target>
```

```
                <Node>
                        <Address ident="" category="ipv4-addr">
                                <address>3.3.3.3</address>
                        </Address>
                </Node>
                <Service duration="41" size="1448">
                        <name>junos-http</name>
                        <port>80</port>
                        <protocol>TCP</protocol>
                </Service>
        </Target>
        <SourceNat>
                <Node>
                        <name>trust</name>
                        <Address category="ipv4-addr">
                                <address>4.4.4.4</address>
                        </Address>
                </Node>
                <Service>
                        <port>59078</port>
                </Service>
        </SourceNat>
        <TargetNat>
                <Node>
                        <Address category="ipv4-addr">
                                <address>5.5.5.5</address>
                        </Address>
                </Node>
                <Service>
                        <port>80</port>
                </Service>
        </TargetNat>
    </Connect>
</SIMEF-Message>
```

Bibliographie

[b-ISO 8601:2004] ISO 8601:2004, *Eléments de données et formats d'échange – Echange d'information – Représentation de la date et de l'heure*.

[b-ISO/CEI 10646] ISO/CEI 10646:2012, *Technologies de l'information – Jeu universel de caractères codés (JUC)*.

[b-IEEE Std 1003.1] Norme IEEE 1003.1-2008, *IEEE Standard for Information Technology – Portable Operating System Interface (POSIX(R))*.

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network time protocol (version 3): Specification, implementation*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP network address translator (NAT): Terminology and considerations*.

[b-IETF RFC 2822]) IETF RFC 2822 (2001), *Internet message format*.

[b-IETF RFC 5905] IETF RFC 5905 (2010), *Network time protocol version 4: Protocol and algorithms specification*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changements climatiques, déchets d'équipements électriques et électroniques, efficacité énergétique, construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017