Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5676
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

J. Schoenwaelder, Jacobs University Bremen
A. Clemm, Cisco Systems
A. Karmakar, Cisco Systems India Pvt Ltd
octobre 2009
Traduction Claude Brière de L'Isle

Définitions des objets gérés pour la transposition des messages SYSLOG en notifications du protocole simple de gestion de réseau (SNMP)

Résumé
Le présent document décrit comment envoyer des informations d'alarme dans syslog. Il inclut la transposition des sévérités perçues de l'UIT en champs de messages syslog. Il inclut aussi un certain nombre de définitions SD-PARAM spécifiques d'alarme provenant de la Recommandation UIT-T X.733 et de la MIB Alarm de l'IETF.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5676

Table des matières

1. Introduction

SNMP ([RFC3410], [RFC3411]) et SYSLOG [RFC5424] sont deux protocoles largement utilisés pour communiquer des

notifications d'événement. Bien que la coexistence de plusieurs protocoles de gestion dans un environnement de fonctionnement soit possible, certains environnements exigent que toutes les notifications d'événement soient collectées par un seul automate de système, comme un collecteur SYSLOG ou un receveur de notifications SNMP, via un seul protocole de gestion. Dans de tels environnements, il est nécessaire de traduire les notifications d'événement entre les protocoles de gestion.

Le présent document définit un module de MIB SNMP pour représenter les messages SYSLOG et pour envoyer des messages SYSLOG comme notifications SNMP aux receveurs de notifications SNMP.

2. Cadre de gestion standard de l'Internet

Pour une vue détaillée des documents qui décrivent le cadre actuel de gestion de l'Internet, voir la Section 7 de la [RFC3410].

L'accès aux objets est fait via un magasin virtuel d'informations, appelé la base de données d'informations de gestion (MIB, *Management Information Base*). L'accès aux objets de MIB se fait généralement par le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*). Les objets dans la MIB sont définis en utilisant les mécanismes définis dans la structure des informations de gestion (SMI, *Structure of Management Information*). Le présent mémoire spécifie un module de MIB conforme à SMIv2, décrit dans le STD 58, [RFC2578], [RFC2579] et [RFC2580].

3. Conventions

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].

4. Vue d'ensemble

Les messages SYSLOG sont traduits en SNMP par un traducteur de SYSLOG en SNMP. Un tel traducteur agit comme un collecteur SYSLOG [RFC5424] et met en œuvre un module de MIB conformément à l'architecture SNMP [RFC3411]. Le traducteur peut être étroitement couplé à un agent SNMP ou peut s'interfacer avec un agent SNMP via un protocole de sous agent.

Après l'initialisation, le traducteur de SYSLOG en SNMP va écouter les messages SYSLOG. À réception d'un message, le message va être analysé pour extraire les informations comme décrit dans le module de MIB. Un tableau conceptuel est rempli avec les informations extraites du message SYSLOG, et finalement une notification peut être générée.

Le module de MIB est organisé en un groupe de scalaires et deux tableaux. Le groupe syslogMsgControl contient deux scalaires qui contrôlent le nombre maximum de messages SYSLOG enregistrés dans les tableaux et contrôlent aussi si des notifications SNMP sont générées pour des messages SYSLOG.

```
--syslogMsgObjects(1)
  |
  +--syslogMsgControl(1)
     |
     +-- Unsigned32 syslogMsgTableMaxSize(1)
     +-- TruthValue syslogMsgEnableNotifications(2)
```

Le syslogMsgTable contient une entrée pour chaque message SYSLOG enregistré. Les champs de base des messages SYSLOG ainsi que les propriétés des messages sont représentés dans les différentes colonnes du tableau conceptuel.

```
--syslogMsgObjects(1)
  |
  +--syslogMsgTable(2)
     |
```

```
   +--syslogMsgEntry(1) [syslogMsgIndex]
      |
      +-- Unsigned32        syslogMsgIndex(1)
      +-- SyslogFacility    syslogMsgFacility(2)
      +-- SyslogSeverity    syslogMsgSeverity(3)
      +-- Unsigned32        syslogMsgVersion(4)
      +-- SyslogTimeStamp syslogMsgTimeStamp(5)
      +-- DisplayString     syslogMsgHostName(6)
      +-- DisplayString     syslogMsgAppName(7)
      +-- DisplayString     syslogMsgProcID(8)
      +-- DisplayString     syslogMsgMsgID(9)
      +-- Unsigned32        syslogMsgSDParams(10)
      +-- OctetString       syslogMsgMsg(11)
```

Le syslogMsgSDTable contient une entrée pour chaque paramètre d'élément de données structuré contenu dans un message SYSLOG. Comme les éléments de données structurés sont facultatifs, la relation entre le syslogMsgTable et le syslogMsgSDTable va de un à zéro à un à plusieurs.

```
  --syslogMsgObjects(1)
    |
    +--syslogMsgSDTable(3)
       |
       +--syslogMsgSDEntry(1)      [syslogMsgIndex,
          |                         syslogMsgSDParamIndex,
          |                         syslogMsgSDID,
          |                         syslogMsgSDParamName]
          |
          +-- Unsigned32              syslogMsgSDParamIndex(1)
          +-- DisplayString           syslogMsgSDID(2)
          +-- DisplayString           syslogMsgSDParamName(3)
          +-- SyslogParamValueString  syslogMsgSDParamValue(4)
```

5. Relations avec les autres modules de MIB

La NOTIFICATION-LOG-MIB [RFC3014] fournit un mécanisme générique pour enregistrer les notifications SNMP afin de traiter les notifications SNMP perdues, par exemple, à cause de problèmes temporaires de communication. Les applications peuvent interroger le registre des notifications pour vérifier qu'elles n'ont pas manqué d'importantes notifications SNMP.

Le module de MIB défini dans le présent mémoire donne un mécanisme pour enregistrer les notifications SYSLOG. Cet enregistrement supplémentaire de notifications SYSLOG est fourni parce que (a) les messages SYSLOG pourraient ne pas conduire à une notification SNMP (ceci est configurable) et (b) les notifications SNMP pourraient ne pas porter toutes les informations associées à une notification SYSLOG.

Le module de MIB IMPORTE des objets de SNMPv2-SMI [RFC2578], SNMPv2-TC [RFC2579], SNMPv2-CONF [RFC2580], SNMP-FRAMEWORK-MIB [RFC3411], et SYSLOG-TC-MIB [RFC5427].

La convention textuelle SyslogParamValueString utilise le format de transformation UTF-8 du jeu de caractères de la norme internationale ISO/CEI 10646-1 défini dans la [RFC3629].

6. Relations de la notification SNMP à la transposition SYSLOG

Un document d'accompagnement [RFC5675] définit une transposition de notifications SNMP en messages SYSLOG. Cette section discute les possibilités d'utiliser une combinaison des deux spécifications.

Un collecteur SYSLOG qui met en œuvre le module de MIB SYSLOG-MSG et la transposition des notifications SNMP en messages SYSLOG peut être configuré à traduire les messages SYSLOG reçus qui contiennent des notifications SNMP en

la notification SNMP originale. Dans ce cas, les tableaux pertinents de la SYSLOG-MSG-MIB ne vont pas être remplis pour les messages SYSLOG portant des notifications SNMP. Cette configuration permet aux opérateurs de construire une chaîne de transmission où les notifications SNMP sont "tunnelées" à travers les messages SYSLOG. Du fait des restrictions de taille des transports SYSLOG et du codage textuel plus verbeux utilisé par SYSLOG, il est possible que le contenu de la notification SNMP soit tronqué quand il est tunnelé à travers SYSLOG, et donc la notification SNMP résultante peut être incomplète.

Une application de gestion SNMP qui prend en charge la SYSLOG-MSG-MIB et la transposition de notifications SNMP en messages SYSLOG peut traiter les informations provenant de la SYSLOG-MSG-MIB afin d'émettre un message SYSLOG représentant le message SYSLOG enregistré dans le module SYSLOG-MSG-MIB. Cette configuration permet aux opérateurs de construire une chaîne de transmission où les messages SYSLOG sont "tunnelés" à travers les messages SNMP. Un receveur de notification peut déterminer si une syslogMsgNotification contenait tous les paramètres d'élément de données structuré d'un message SYSLOG. En cas de paramètres manquants, une application de transmission DOIT restituer les paramètres manquants à partir de la SYSLOG-MSG-MIB. L'interrogation régulière de la SYSLOG-MSG-MIB peut être utilisée pour s'occuper de toute notification SNMP perdue.

7. Définitions

DÉFINITIONS DE SYSLOG-MSG-MIB ::= DÉBUT

```
 IMPORTE
    MODULE-IDENTITY, TYPE D'OBJET, NOTIFICATION-TYPE, Unsigned32, mib-2
       DE SNMPv2-SMI
    TEXTUAL-CONVENTION, DisplayString, TruthValue
       DE SNMPv2-TC
    OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
       DE SNMPv2-CONF
    SyslogFacility, SyslogSeverity
       DE SYSLOG-TC-MIB;

IDENTITÉ DE MODULE syslogMsgMib
    DERNIERE MISE A JOUR "200908130800Z"
    ORGANISATION "Groupe de travail OPSAWG de l'IETF"
    INFORMATIONS DE CONTACT
       "Juergen Schoenwaelder
        <j.schoenwaelder@jacobs-university.de>
        Jacobs University Bremen
        Campus Ring 1
        28757 Bremen
        Germany

        Alexander Clemm
        <alex@cisco.com>
        Cisco Systems
        170 West Tasman Drive
        San Jose, CA 95134-1706
        USA

        Anirban Karmakar
        <akarmaka@cisco.com>
        Cisco Systems India Pvt Ltd
        SEZ Unit, Cessna Business Park,
        Sarjapur Marathahalli ORR,
        Bangalore, Karnataka 560103
        India"

DESCRIPTION : "Ce module de MIB représente les messages SYSLOG comme des objets SNMP.
Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du code. Tous droits réservés.
La redistribution et l'utilisation en formes source et binaire, avec ou sans modification, est permise et est soumise aux
```

termes de licence contenus dans la licence BSD simplifiée établie dans la Section 4.c des dispositions légales de l'IETF Trust relatives aux documents de l'IETF (http://trustee.ietf.org/license-info).

Cette version de module de MIB fait partie de la RFC 5676 ; voir la RFC elle-même pour les notices légales complètes."

RÉVISION "200908130800Z"
DESCRIPTION ;: "Version initiale produite au titre de la RFC 5676."
::= { mib-2 192 }

-- définitions des conventions textuelles

SyslogTimeStamp ::= TEXTUAL-CONVENTION
DISPLAY-HINT "2d-1d-1d,1d:1d:1d.3d,1a1d:1d"
STATUT courant
DESCRIPTION : "Spécification de date et heure. Ce type est similaire au type DateAndTime défini dans le SNMPv2-TC, excepté que la granulation de sous seconde est la microseconde au lieu du dixième de seconde et qu'une chaîne de longueur zéro peut être utilisée pour indiquer une valeur manquante.

Champ	**Octets**	**Contenus**	**Gamme**	
1	1-2	année*	0..65536	
2	3	mois	1..12	
3	4	jour	1..31	
4	5	heure	0..23	
5	6	minutes	0..59	
6	7	secondes	0..60	(utilisation de 60 pour la seconde sautée)
7	8-10	microsecondes*	0..999999	
8	11	direction de l'UTC	'+' / '-'	
9	12	heures de l'UTC*	0..13	
10	13	minutes de l'UTC	0..59	

* Notes :
- la valeur de l'année est dans l'ordre des octets du réseau
- la valeur de microsecondes est dans l'ordre des octets du réseau
- l'horaire d'été en Nouvelle Zélande est +13

Par exemple, Mardi 26 mai 1992 à 1:30:15 de l'après midi EDT serait affiché : 1992-5-26,13:30:15.0,-4:0

Noter que si seulement l'heure locale est connue, les informations de zone horaire (champs 11-13) ne sont pas présentes."

SYNTAXE CHAINE D'OCTETS (TAILLE (0 | 10 | 13))

SyslogParamValueString ::= TEXTUAL-CONVENTION
DISPLAY-HINT "65535t"
STATUT courant
DESCRIPTION : "La valeur d'un SYSLOG SD-PARAM est représentée en utilisant le jeu de caractères de la norme internationale ISO/CEI 10646-1, codée comme une chaîne d'octets en utilisant le format de transformation UTF-8 décrit dans la RFC 3629. Comme des codets supplémentaires sont ajoutés de temps en temps par des amendements à la norme 10646, les mises en œuvre doivent être prêtes à rencontrer tout codet de 0x00000000 à 0x7fffffff. Les séquences d'octets qui ne correspondent pas au codage UTF-8 valide d'un codet ou qui sortent de cette gamme sont interdites. De même, les séquences UTF-8 trop longues sont interdites. UTF-8 peut exiger plusieurs octets pour représenter un seul caractère/codet ; donc, la longueur de cet objet en octets peut être différente du nombre de caractères codés. De même, les contraintes de taille se réfèrent au nombre d'octets codés, non au nombre de caractères représentés par un codage."
RÉFÉRENCE : "RFC 3629 : UTF-8, un format de transformation de ISO 10646"
SYNTAXE CHAINE D'OCTETS

-- définitions d'objets

IDENTIFIANT D'OBJET syslogMsgNotifications ::= { syslogMsgMib 0 }
IDENTIFIANT D'OBJET syslogMsgObjects ::= { syslogMsgMib 1 }
IDENTIFIANT D'OBJET syslogMsgConformance ::= { syslogMsgMib 2 }

IDENTIFIANT D'OBJET syslogMsgControl ::= { syslogMsgObjects 1 }

TYPE D'OBJET syslogMsgTableMaxSize
SYNTAXE Unsigned32
MAX-ACCESS lecture-écriture
STATUT courant
DESCRIPTION : "Nombre maximum de messages SYSLOG qui peuvent être détenus dans un syslogMsgTable. Un réglage particulier ne garantit pas qu'une mémoire suffisante est disponible pour le nombre maximum d'entrées de tableau indiqué par cet objet. Une valeur de 0 signifie qu'il n'y a pas de limite fixée. Si une application réduit la limite alors qu'il y a des messages SYSLOG dans le syslogMsgTable, les messages SYSLOG qui sont dans le syslogMsgTable depuis le plus longtemps DOIVENT être éliminés pour ramener le tableau à la nouvelle limite. La valeur de cet objet devrait être conservée dans une mémoire non volatile."
DEFVAL { 0 }
::= { syslogMsgControl 1 }

TYPE D'OBJET syslogMsgEnableNotifications
SYNTAXE TruthValue
MAX-ACCESS lecture-écriture
STATUT courant
DESCRIPTION : "Indique si des notifications syslogMsgNotification sont générées. La valeur de cet objet devrait être conservée dans une mémoire non volatile."
DEFVAL { faux }
::= { syslogMsgControl 2 }

TYPE D'OBJET syslogMsgTable
SYNTAXE SEQUENCE DE SyslogMsgEntry
MAX-ACCESS non-accessible
STATUT courant
DESCRIPTION : "Tableau contenant les messages SYSLOG récents. La taille du tableau est contrôlée par l'objet syslogMsgTableMaxSize."
::= { syslogMsgObjects 2 }

TYPE D'OBJET syslogMsgEntry
SYNTAXE SyslogMsgEntry
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Entrée de syslogMsgTable."
INDEX { syslogMsgIndex }
::= { syslogMsgTable 1 }

```
SyslogMsgEntry ::= SEQUENCE {
    syslogMsgIndex      Unsigned32,
    syslogMsgFacility   SyslogFacility,
    syslogMsgSeverity   SyslogSeverity,
    syslogMsgVersion    Unsigned32,
    syslogMsgTimeStamp  SyslogTimeStamp,
    syslogMsgHostName   DisplayString,
    syslogMsgAppName    DisplayString,
    syslogMsgProcID     DisplayString,
    syslogMsgMsgID      DisplayString,
    syslogMsgSDParams   Unsigned32,
    syslogMsgMsg        CHAINE D'OCTETS
 }
```

TYPE D'OBJET syslogMsgIndex
SYNTAXE Unsigned32 (1..4294967295)
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Nombre d'accroissement monotone utilisé pour identifier les entrées dans le syslogMsgTable. Quand syslogMsgIndex atteint la valeur maximum (4 294 967 295) elle revient à 1. Les applications qui interrogent périodiquement le syslogMsgTable sur les nouvelles entrées devraient tenir compte de ce qu'un retour à zéro complet de

syslogMsgIndex va se produire si plus de 4 294 967 294 messages sont reçus durant un intervalle entre deux interrogations."
::= { syslogMsgEntry 1 }

TYPE D'OBJET syslogMsgFacility
SYNTAXE SyslogFacility
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "La facilité de message SYSLOG."
RÉFÉRENCE "RFC 5424 : Protocole Syslog (paragraphe 6.2.1) ; RFC 5427 : Conventions textuelles pour la gestion Syslog"
::= { syslogMsgEntry 2 }

TYPE D'OBJET syslogMsgSeverity
SYNTAXE SyslogSeverity
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Sévérité du message SYSLOG"
RÉFÉRENCE "RFC 5424 : Protocole Syslog (paragraphe 6.2.1) ; RFC 5427 : Conventions textuelles pour la gestion Syslog"
::= { syslogMsgEntry 3 }

TYPE D'OBJET syslogMsgVersion
SYNTAXE Unsigned32 (0..999)
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Version du message SYSLOG. Une valeur de 0 indique que la version est inconnue."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.2)"
::= { syslogMsgEntry 4 }

TYPE D'OBJET syslogMsgTimeStamp
SYNTAXE SyslogTimeStamp
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Horodatage du message SYSLOG. Une chaîne de longueur zéro est retournée si l'horodatage est inconnu."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.3)"
::= { syslogMsgEntry 5 }

TYPE D'OBJET syslogMsgHostName
SYNTAXE DisplayString (TAILLE (0..255))
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Le nom d'hôte et le nom de domaine (facultatif) du message SYSLOG. Une chaîne de longueur zéro indique un nom d'hôte inconnu. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.4)"
::= { syslogMsgEntry 6 }

TYPE D'OBJET syslogMsgAppName
SYNTAXE DisplayString (TAILLE (0..48))
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Le nom de l'application du message SYSLOG. Une chaîne de longueur zéro indique un nom d'application inconnu. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.5)"
::= { syslogMsgEntry 7 }

TYPE D'OBJET syslogMsgProcID
SYNTAXE DisplayString (TAILLE (0..128))
MAX-ACCESS lecture seule

STATUT courant
DESCRIPTION : "Identifiant de processus du message SYSLOG. Une chaîne de longueur zéro indique un identifiant de processus inconnu. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.6)"
::= { syslogMsgEntry 8 }

TYPE D'OBJET syslogMsgMsgID
SYNTAXE DisplayString (TAILLE (0..32))
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Identifiant de message du message SYSLOG. Une chaîne de longueur zéro indique un identifiant de message inconnu. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.2.7)"
::= { syslogMsgEntry 9 }

TYPE D'OBJET syslogMsgSDParams
SYNTAXE Unsigned32
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Nombre total de paramètres d'élément de données structuré portés dans le message SYSLOG. Ce nombre indique effectivement le nombre d'entrées dans le syslogMsgSDTable. Il peut être utilisé, par exemple, par un receveur de notification pour déterminer si une notification porte tous les paramètres d'élément de données structuré d'un message SYSLOG."
::= { syslogMsgEntry 10 }

TYPE D'OBJET syslogMsgMsg
SYNTAXE CHAINE D'OCTETS
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Partie message du message SYSLOG. La syntaxe n'impose pas de restriction de taille. Les mises en œuvre de ce module de MIB peuvent tronquer la partie message du message SYSLOG de façon à ce qu'il tienne dans les contraintes de taille imposées par l'environnement de mise en œuvre. Une telle troncature peut aussi arriver ailleurs dans la chaîne de transmission SYSLOG. Si les premiers octets contiennent la valeur 'EFBBBF'h, alors le reste du message est une chaîne UTF-8. Comme les messages SYSLOG peuvent être tronqués à des limites d'octet arbitraires durant la transmission, le message peut contenir des codages UTF-8 invalides à la fin."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphes 6.1 et 6.4)"
::= { syslogMsgEntry 11 }

TYPE D'OBJET syslogMsgSDTable
SYNTAXE SEQUENCE DE SyslogMsgSDEntry
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Tableau contenant des éléments de données structurés de messages SYSLOG."
::= { syslogMsgObjects 3 }

TYPE D'OBJET syslogMsgSDEntry
SYNTAXE SyslogMsgSDEntry
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Entrée du tableau syslogMsgSDTable."
INDEX { syslogMsgIndex, syslogMsgSDParamIndex, syslogMsgSDID, syslogMsgSDParamName }
::= { syslogMsgSDTable 1 }

```
SyslogMsgSDEntry ::= SEQUENCE {
    syslogMsgSDParamIndex   Unsigned32,
    syslogMsgSDID           DisplayString,
    syslogMsgSDParamName    DisplayString,
    syslogMsgSDParamValue   SyslogParamValueString
 }
```

TYPE D'OBJET syslogMsgSDParamIndex

SYNTAXE Unsigned32 (1..4294967295)
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Cet objet indexe les paramètres d'élément de données structuré contenus dans un message SYSLOG. Le premier paramètre d'élément de données structuré a la valeur d'indice 1, et les paramètres suivants sont indexés en incrémentant l'indice du paramètre précédent. L'indice s'augmente à travers les frontières d'élément de données structuré de sorte que la valeur reflète la position d'un paramètre d'élément de données structuré dans un message SYSLOG."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.3.3)".
::= { syslogMsgSDEntry 1 }

TYPE D'OBJET syslogMsgSDID
SYNTAXE DisplayString (TAILLE (1..32))
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Le nom (SD-ID) d'un élément de données structuré. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.3.2)".
::= { syslogMsgSDEntry 2 }

TYPE D'OBJET syslogMsgSDParamName
SYNTAXE DisplayString (TAILLE (1..32))
MAX-ACCESS non accessible
STATUT courant
DESCRIPTION : "Nom d'un paramètre de l'élément de données structuré. La spécification du protocole SYSLOG restreint cette chaîne aux codets US-ASCII imprimables."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.3.3)"
::= { syslogMsgSDEntry 3 }

TYPE D'OBJET syslogMsgSDParamValue
SYNTAXE SyslogParamValueString
MAX-ACCESS lecture seule
STATUT courant
DESCRIPTION : "Valeur du paramètre d'un message SYSLOG identifié par l'indice de ce tableau. La valeur est mémorisée dans le format non échappé."
RÉFÉRENCE : "RFC 5424 : Protocole Syslog (paragraphe 6.3.3)"
::= { syslogMsgSDEntry 4 }

-- définitions de notification
TYPE DE NOTIFICATION syslogMsgNotification
OBJETS { syslogMsgFacility, syslogMsgSeverity, syslogMsgVersion, syslogMsgTimeStamp, syslogMsgHostName, syslogMsgAppName, syslogMsgProcID, syslogMsgMsgID, syslogMsgSDParams, syslogMsgMsg }
STATUT courant
DESCRIPTION : "La notification syslogMsgNotification est générée quand un nouveau message SYSLOG est reçu et que la valeur de syslogMsgGenerateNotifications est VRAI. Les mises en œuvre peuvent ajouter des objets syslogMsgSDParamValue tant que la notification résultante tient dans les contraintes de taille imposées par l'environnement de mise en œuvre et les contrainte de taille de message de notification imposées par maxMessageSize [RFC3412] et les transpositions de transport SNMP."
::= { syslogMsgNotifications 1 }

-- déclarations de conformité
IDENTIFIANT D'OBJET syslogMsgGroups ::= { syslogMsgConformance 1 }
IDENTIFIANT D'OBJET syslogMsgCompliances ::= { syslogMsgConformance 2 }

CONFORMITÉ DE MODULE syslogMsgFullCompliance
STATUT courant
DESCRIPTION : "Déclaration de conformité pour les mises en œuvre de la SYSLOG-MSG-MIB."
MODULE -- ce module
GROUPES OBLIGATOIRES {
syslogMsgGroup,
syslogMsgSDGroup,
syslogMsgControlGroup,

```
        syslogMsgNotificationGroup
    }
    ::= { syslogMsgCompliances 1 }

    CONFORMITÉ DE MODULE syslogMsgReadOnlyCompliance
    STATUT      courant
    DESCRIPTION : "Déclaration de conformité pour les mises en œuvre de la SYSLOG-MSG-MIB qui ne prennent pas en
    charge l'accès en lecture-écriture."
    MODULE      -- ce module
    GROUPES OBLIGATOIRES {
            syslogMsgGroup,
            syslogMsgSDGroup,
            syslogMsgControlGroup,
            syslogMsgNotificationGroup
        }

    OBJET syslogMsgTableMaxSize
    MIN-ACCESS  lecture seule
    DESCRIPTION : "L'accès en écriture n'est pas exigé."

    OBJET syslogMsgEnableNotifications
    MIN-ACCESS  lecture seule
    DESCRIPTION : "L'accès en écriture n'est pas exigé ."
    ::= { syslogMsgCompliances 2 }

    CONFORMITÉ DE MODULE syslogMsgNotificationCompliance
    STATUT      courant
    DESCRIPTION : "Déclaration de conformité pour les mises en œuvre de la SYSLOG-MSG-MIB qui génèrent seulement
    des notifications et ne fournissent pas un tableau pour permettre l'accès en lecture aux détails du message SYSLOG."
    MODULE      -- ce module
    GROUPES OBLIGATOIRES {
            syslogMsgGroup,
            syslogMsgSDGroup,
            syslogMsgNotificationGroup
        }
    OBJET syslogMsgFacility
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET  syslogMsgSeverity
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé "
    OBJET syslogMsgVersion
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgTimeStamp
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgHostName
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgAppName
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgProcID
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgMsgID
    MIN-ACCESS  accessible pour notification
    DESCRIPTION : "L'accès en lecture n'est pas exigé."
    OBJET syslogMsgSDParams
    MIN-ACCESS  accessible pour notification
```

DESCRIPTION : "L'accès en lecture n'est pas exigé."
OBJET syslogMsgMsg
MIN-ACCESS accessible pour notification
DESCRIPTION : "L'accès en lecture n'est pas exigé."
OBJET syslogMsgSDParamValue
MIN-ACCESS accessible pour notification
DESCRIPTION : "L'accès en lecture n'est pas exigé."
::= { syslogMsgCompliances 3 }

GROUPE DE NOTIFICATION syslogMsgNotificationGroup
NOTIFICATIONS { syslogMsgNotification }
STATUT courant
DESCRIPTION : "Notifications émises par ce module de MIB."
::= { syslogMsgGroups 1 }

GROUPE D'OBJETS syslogMsgGroup
OBJETS {
-- syslogMsgIndex,
syslogMsgFacility,
syslogMsgSeverity,
syslogMsgVersion,
syslogMsgTimeStamp,
syslogMsgHostName,
syslogMsgAppName,
syslogMsgProcID,
syslogMsgMsgID,
syslogMsgSDParams,
syslogMsgMsg
}
STATUT courant
DESCRIPTION : "Collection d'objets représentant un message SYSLOG, à l'exclusion des éléments de données structurés."
::= { syslogMsgGroups 2 }

GROUPE D'OBJETS syslogMsgSDGroup
OBJETS {
-- syslogMsgSDParamIndex,
-- syslogMsgSDID,
-- syslogMsgSDParamName,
-- syslogMsgSDParamValue
}
STATUT courant
DESCRIPTION : "Collection d'objets représentant les éléments de données structurés d'un message SYSLOG."
::= { syslogMsgGroups 3 }

GROUPE D'OBJETS syslogMsgControlGroup
OBJETS {
syslogMsgTableMaxSize,
syslogMsgEnableNotifications
}
STATUT courant
DESCRIPTION : "Collection d'objets de contrôle pour contrôler la taille du syslogMsgTable et pour activer/désactiver les notifications."
::= { syslogMsgGroups 4 }

FIN

8. Exemple d'utilisation

L'exemple suivant montre un message SYSLOG valide incluant des données structurées. La marque d'ordre des octets (BOM, *byte order mark*) Unicode autrement non imprimable est représentée comme "BOM" dans l'exemple.

```
<165>1 2003-10-11T22:14:15.003Z mymachine.exemple.com
evntslog - ID47 [exampleSDID@32473 iut="3" eventSource="Application"
eventID="1011"] BOMUne entrée d'enregistrement d'événement d'application ...
```

Ce message SYSLOG conduit aux entrées suivantes dans le syslogMsgTable et le syslogMsgSDTable (noter que les indices de chaînes sont écrits comme des chaînes pour des raisons de lisibilité) :

```
syslogMsgIndex.1 = 1
syslogMsgFacility.1 = 20
syslogMsgSeverity.1 = 5
syslogMsgVersion.1 = 1
syslogMsgTimeStamp.1 = 2003-10-11,22:14:15.003,+0:0
syslogMsgHostName.1 = "mymachine.exemple.com"
syslogMsgAppName.1 = "evntslog"
syslogMsgProcID.1 = "-"
syslogMsgMsgID.1 = "ID47"
syslogMsgMsg.1 = "BOMUne entrée d'enregistrement d'événement d'application ..."
syslogMsgSDParamValue.1.1."exampleSDID@32473"."iut" = "3"
syslogMsgSDParamValue.1.2."exampleSDID@32473"."eventSource" = "Application"
syslogMsgSDParamValue.1.3."exampleSDID@32473"."eventID" = "1011"
```

9. Considérations relatives à l'IANA

L'IANA a alloué la valeur "192" dans la sous arborescence "mib-2" et enregistré l'allocation dans le registre des numéros de SMI.

10. Considérations sur la sécurité

Un certain nombre d'objets de gestion définis dans ce module de MIB avec une clause MAX-ACCESS de lecture-écriture et/ou lecture-création. De tels objets peuvent être considérés comme sensibles ou vulnérables dans certains environnements de réseau. La prise en charge des opérations SET dans un environnement non sûr sans la protection appropriée peut avoir un effet négatif sur le fonctionnement du réseau. Voici ces tableaux et objets et leur sensibilité/vulnérabilité :

- syslogMsgTableMaxSize : cet objet contrôle le nombre d'entrées qui sont conservées dans le syslogMsgTable. Des modifications non autorisées peuvent causer un accroissement de la consommation de mémoire (en réglant cet objet à une valeur élevée) ou couper la capacité de restituer les notifications en utilisant les opérations de classe GET (en réglant cet objet à zéro). Cela pourrait être utilisé pour cacher les traces d'une attaque.

- syslogMsgEnableNotifications : cet objet permet les notifications. Des modifications non autorisées pour désactiver la génération de notifications peuvent être utilisées pour cacher une attaque en empêchant les applications de gestion qui utilisent SNMP de recevoir des notifications en temps réel sur les événements portés dans les messages SYSLOG. Des modifications non autorisées pour permettre la génération de notifications peuvent être utilisées au titre d'une attaque de déni de service contre un système de gestion de réseau si, par exemple, le traducteur de SYSLOG en SNMP accepte les messages SYSLOG non autorisés.

Certains des objets lisibles dans ce module de MIB (c'est-à-dire, les objets avec un MAX-ACCESS autre que non accessible) peuvent être considérés comme sensibles ou vulnérables dans certains environnements de réseau. Il est donc important de contrôler même l'accès GET et/ou NOTIFY à ces objets et éventuellement même de chiffrer les valeurs de ces objets lors de leur envoi sur le réseau via SNMP. Voici ces tableaux et objets et leur sensibilité/vulnérabilité :

- syslogMsgTableMaxSize, syslogMsgEnableNotifications : ces objets fournissent des informations sur si les messages

SYSLOG sont transmis comme des notifications SNMP et combien de messages vont être conservés dans le syslogMsgTable. Ces informations pourraient être exploitées par un attaquant afin de planifier des actions dans le but de cacher les activités d'attaque.

- o syslogMsgFacility, syslogMsgSeverity, syslogMsgVersion, syslogMsgTimeStamp, syslogMsgHostName, syslogMsgAppName, syslogMsgProcID, syslogMsgMsgID, syslogMsgSDParams, syslogMsgMsg, syslogMsgSDParamValue : ces objets portent le contenu des messages SYSLOG et les considérations sur la sécurité de SYSLOG en mode message de la [RFC5424] s'appliquent. En particulier, un attaquant qui obtient l'accès aux messages SYSLOG via SNMP peut utiliser les connaissances tirées des messages SYSLOG pour compromettre une machine ou faire d'autres dommages. Il est donc désirable de configurer les règles de contrôle d'accès SNMP, en appliquant une politique de sécurité cohérente pour les messages SYSLOG.

Les versions de SNMP antérieures à SNMPv3 n'incluaient pas de sécurité adéquate. Même si le réseau lui-même est sûr (par exemple en utilisant IPsec) il n'y a pas de contrôle sur à qui il est permis d'accéder au réseau sûr et faire des GET/SET (lire/changer/créer/dsupprimer) sur les objets dans ce module de MIB.

Il est RECOMMANDÉ que les mises en œuvre considèrent les caractéristiques de sécurité fournies par le cadre SNMPv3 (voir la Section 8 de la [RFC3410]) incluant la prise en charge complète des mécanismes de chiffrement de SNMPv3 (pour l'authentification et la confidentialité).

De plus, le déploiement de versions SNMP antérieures à SNMPv3 est NON RECOMMANDÉ. À la place, il est RECOMMANDÉ de déployer SNMPv3 et d'activer la sécurité cryptographique. Il est alors de la responsabilité du consommateur/opérateur de s'assurer que l'entité SNMP qui donne accès à une instance de ce module de MIB est configurée de façon appropriée pour donner seulement l'accès aux objets à ces principaux (utilisateurs) qui ont des droits légitimes pour effectuer sur eux des GET ou SET (changer/créer/supprimer).

Utiliser les caractéristiques de sécurité du cadre SNMPv3 sécurise le transport des données SYSLOG via SNMP seulement. Il est donc RECOMMANDÉ que les déploiements utilisent les mécanismes de sécurité de SYSLOG afin d'empêcher des attaquants d'ajouter des données SYSLOG malveillantes aux tableaux de MIB.

11. Remerciements

Les éditeurs souhaitent remercier les personnes suivantes de leurs utiles commentaires sur les diverses versions de ce document : Martin Bjorklund, Washam Fan, Rainer Gerhards, Wes Hardacker, David Harrington, Tom Petch, Juergen Quittek, Dan Romascanu, et Bert Wijnen.

12. Références

12.1 Références normatives

[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)

[RFC2578] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Structure des informations de gestion, version 2 (SMIv2)", avril 1999, DOI 10.17487/RFC2578. (STD0058)

[RFC2579] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Conventions textuelles pour SMIv2", avril 1999. (STD0058)

[RFC2580] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Déclarations de conformité pour SMIv2", avril 1999. (STD0058)

[RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* RFC5343) (STD0062)

[RFC3412] J. Case et autres, "Traitement et distribution de message pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003, DOI 10.17487/RFC3629.

[RFC5424] R. Gerhards, "Le protocole Syslog", mars 2009. (*Remplace la* RFC3164, *P. S.*)

[RFC5427] G. Keeni, "Conventions textuelles pour gestion Syslog", mars 2009. *(P. S.)*

[RFC5675] V. Marinov, J. Schoenwaelder, "Transposition des notifications du protocole simple de gestion de réseau (SNMP) en messages SYSLOG", **o**ctobre 2009. *(P. S.)*

12.2 Références pour information

[RFC3014] R. Kavasseri, "MIB d'enregistrement de notification", novembre 2000. *(P.S.)*

[RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. *(Information)*

Adresse des auteurs

Juergen Schoenwaelder
Jacobs University Bremen
Campus Ring 1
28725 Bremen
Germany
mél : j.schoenwaelder@jacobs-university.de

Alexander Clemm
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706
USA
mél : alex@cisco.com

Anirban Karmakar
Cisco Systems India Pvt Ltd
SEZ Unit, Cessna Business Park,
Sarjapur Marathahalli ORR,
Bangalore, Karnataka 560103
India
mél : akarmaka@cisco.com