Groupe de travail Réseau
Request for Comments : 5427
Catégorie : Sur la voie de la normalisation

G. Keeni, Cyber Solutions Inc.
mars 2009
Traduction Claude Brière de L'Isle

Conventions textuelles pour la gestion de Syslog

Résumé
Ce module de MIB définit les conventions textuelles pour représenter les informations de facilité et de sévérité couramment utilisées dans le messages syslog. L'intention est que ces conventions textuelles soient importées et utilisées dans les modules de MIB qui devraient autrement définir leurs propres représentations.

Table des matières

1. Cadre de gestion standard de l'Internet

Pour une description détaillée des documents qui spécifient le cadre actuel de gestion des normes de l'Internet, prière de se référer à la Section 7 de la [RFC3410].

Les objets gérés sont accédés via un magasin virtuel d'informations, appelée une base de données d'informations de gestion MIB, *Management Information Base)*. Les objets de MIB sont généralement accédés par le protocole simple de gestion de réseau (SMTP, *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 qui est conforme à SMIv2, qui est décrit dans le STD 58, [RFC2578], [RFC2579] et [RFC2580].

2. Fondements

Les systèmes d'exploitation, processus, et applications, appelés collectivement "facilités" dans ce qui suit, génèrent des messages qui indiquent leur propre état ou l'occurrence d'événements. Ces messages sont connus comme des messages syslog. Un message syslog va en général contenir entre autres choses un code représentant la facilité qui a généré le message et un code représentant la sévérité du message. Les codes de facilité et de sévérité sont couramment utilisés pour catégoriser et choisir les messages syslog reçus pour traitement et affichage. Les codes de facilité ont été utiles pour qualifier le générateur du contenu des messages mais dans certains cas, ils ne sont pas assez spécifiques pour identifier explicitement le générateur. Les mises en œuvre du protocole syslog [RFC5424] qui contiennent des éléments de données structurés (SDE, *structured data element*) devraient les utiliser pour préciser l'entité qui a généré le contenu du message.

Le présent document définit un ensemble de conventions textuelles (TC, *textual convention*) qui peuvent êtte utilisées pour représenter les codes de facilité et de sévérité utilisés couramment dans les messages syslog.

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

3. MIB de conventions textuelles Syslog

SYSLOG-TC-MIB DEFINITIONS ::= DÉBUT

IMPORTE
    MODULE-IDENTITY, mib-2
        FROM SNMPv2-SMI -- [RFC2578]
    TEXTUAL-CONVENTION
        FROM SNMPv2-TC; -- [RFC2579]

  syslogTCMIB MODULE-IDENTITY
    LAST-UPDATED "200903300000Z" -- 30 mars 2009
    ORGANIZATION "IETF Syslog Working Group"
    CONTACT-INFO
    " Glenn Mansfield Keeni
    Postal: Cyber Solutions Inc.
    6-6-3, Minami Yoshinari
    Aoba-ku, Sendai, Japan 989-3204.
    Tel: +81-22-303-4012
    Fax: +81-22-303-4015
    EMail: glenn@cysols.com

Adresse de messagerie du groupe de soutien : syslog@ietf.org
    "

DESCRIPTION : "Module de MIB contenant les conventions textuelles pour les messages syslog.

Ce logiciel est fourni par les détenteurs des droits de reproduction et les contributeurs "tel qu'il est" et toutes garanties expresses ou implicites, incluant, mais sans s'y limiter, les garanties implicites de commercialisabilité et de convenance à un objet particuler sont déclinées. En aucun cas le propriétaire des droits de reproduction ou les contributeurs ne seront responsables d'aucun dommage direct, indirect, incident, spécial, exemplaire, ou conséquent (incluant, mais sans s'y limiter, la fourniture de bien ou services de substitution, perte d'usage, de données, ou de profits, ou d'interruption d'affaires) cependant causés et de toute théorie de responsabilité, que ce soit par contrat, responsabilité stricte, ou tort (incluant la négligence ou autre) survenant de quelque manière de l'utilisation de ce logiciel, même si il est averti de la possibilité de tels dommages.

Cette version de ce module de MIB faii partie de la RFC 5427 ; voir dans la RFC elle-même les notices légales complètes."

REVISION "200903300000Z" -- 30 mars 2009
DESCRIPTION : "Version initiale, publiée comme RFC 5427."

::= { mib-2 173 }

-- ---
-- Conventions textuelles
-- ---

SyslogFacility ::= TEXTUAL-CONVENTION
STATUS : courant
DESCRIPTION : "Cette convention textuelle énumère les facilités qui génèrent des messages syslog.
Les facilités des messages syslog sont codées numériquement avec des valeurs décimales. Pour des raisons d'interopérabilité et de rétro compatibilité, le présent document spécifie une transposition normative entre une étiquette, qui représente une facilité, et la valeur numérique correspondante. Cette étiquette peut être utilisée, par exemple, dans les interfaces d'utilisateur de gestionnaire SNMP.

L'étiquette elle-même est souvent sans signification sémantique parce qu'il n'est pas pratique de tenter d'énumérer toutes les facilités possibles, et de nombreux automates et processus n'ont pas de code ou étiquette de facilité explicitement alloué. Par exemple, il n'y a pas d'étiquette de facilité correspondant à un service HTTP. Une mise en œuvre de service HTTP pourrait enregistrer des messages comme venant de, par exemple, "local7" ou "uucp". C'est une pratique courante normale, et les générateurs, relais, et collecteurs peuvent être configurés à traiter correctement cette situation. Pour une précision accrue, une application peut aussi inclure un élément de données structurées APP-NAME.

Noter que les mécanismes de système d 'exploitation pour configurer syslog, comme syslog.conf, n'ont pas encore été normalisés et pourraient utiliser des ensembles d'étiquettes de facilité et/ou transpositions entre étiquettes de facilité et codes de facilité différents de ceux de la MIB.

En particulier, les étiquettes qui correspondent aux codes de facilité 4, 10, 13, et 14, et le code correspondant à l'étiquette de facilité "cron" sont connues pour varier dans les différents systèmes d'exploitation. Pour distinguer entre les étiquettes qui correspondent aux codes de facilité 9 et 15, une étiquette de "cron2" est allouée au code de facilité 15. Cette liste n'est pas destinée à être exhaustive ; d'autres différences pourraient exister, et de nouvelles différences pourraient être introduites à l'avenir.

La transposition spécifiée ici DOIT être utilisée dans une MIB d'interface de gestion de réseau, même si une mise en œuvre syslog particulière pourrait utiliser une transposition différente dans une interface de gestion de réseau différente."

REFERENCE "Protocole Syslog (RFC5424) : Tableau 1"
SYNTAXE : ENTIER
{

kern (0), -- messages du noyau
user (1), -- messages de niveau utilisateur
mail (2), -- messages du système de messagerie
daemon (3), -- messages d'automates du système
auth (4), -- messages d'autorisation
syslog (5), -- messages générés en interne par syslogd
lpr (6), -- messages du sous système d'imprimante en ligne

```
news (7),           -- messages du sous système de nouvelles du réseau
uucp (8),           -- messages du sous système UUCP
cron  (9),          -- messages de l'automate d'horloge
authpriv (10),      -- messages de sécurité/autorisation
ftp  (11),          -- messages de l'automate ftp
ntp (12),           -- messages du sous système NTP
audit (13),         -- messages d'audit
console (14),       -- messages de la console
cron2  (15),        -- messages de l'automate d'horloge
local0 (16),
local1 (17),
local2 (18),
local3 (19),
local4 (20),
local5 (21),
local6 (22),
local7 (23)
}
```

SyslogSeverity ::= TEXTUAL-CONVENTION
STATUS : courant
DESCRIPTION : "Cette convention textuelle énumère les niveaux de sévérité des messages syslog.

Les niveaux de sévérité des messages syslog sont codés numériquement par des valeurs décimales. Pour des raisons d'interopérabilité er de rétro compatibilité, le présent document spécifie une transposition normative entre une étiquette, qui représente un niveau de sévérité, et la valeur numérique correspondante. Cette étiquette pourrait être utilisée, par exemple, par les interfaces d'utilisateur de gestionnaire SNMP.

L'étiquette elle-même est souvent sans signification sémantique parce qu'il n'est pas pratique de tenter de définir strictement les critères pour chaque niveau de sévérité, que les critères qui sont utilisés par les générateurs syslog sont, et ont été historiquement, dépendants de la mise en œuvre.

Noter que les mécanismes de système d'exploitation pour configurer syslog, comme syslog.conf, n'ont pas encore été normalisés et pourraient utiliser des ensembles d'étiquettes de sévérité et/ou de transposition entre les étiquettes de sévérité et les codes de sévérité différents de ceux de la MIB.

Par exemple, l'application foobar pourrait enregistrer des messages comme "crit" sur la base de critères subjectifs. Et l'opérateur peut configurer syslog à transmettre ces messages, même si les critères pour "crit" peuvent différer d'un générateur à l'autre. C'est la pratique courante normale, et les générateurs, relais, et collecteurs peuvent être configurés à traiter correctement cette situation."

REFERENCE : "Protocole Syslog (RFC5424) : Tableau 2"
SYNTAXE : ENTIER

```
{
emerg     (0),      -- Urgence : le système est inutilisable
alert     (1),      -- Alerte : une action doit être prise immédiatement
crit      (2),      -- Critique : conditions critiques
err       (3),      -- Erreur : conditions d'erreur
warning   (4),      -- Avertissement : conditions d'avertissement
notice    (5),      -- Remarque : condition normale mais significative
info      (6),      -- Information : messages d'information
debug     (7)       -- Débogage : messages de niveau débogage
}
FIN
```

4. Considérations sur la sécurité

Ce module ne définit aucun objet de gestion. Il définit plutôt une ensemble de conventions textuelles qui peuvent être utilisées dans d'autres modules de MIB pour définir des objets de gestion. Des considérations de sécurité significatives peuvent seulement être écrites dans les modules de MIB qui définissent des objets de gestion. Le présent document n'a

donc pas d'impact sur la sécurité de l'Internet. Comme les objets définis en utilisant les TC définies dans ce document peuvent introduire des problèmes de sécurité, les utilisateurs de ces TC devraient lire la section des considérations de sécurité de la [RFC5424].

5. Considérations relatives à l'IANA

Les modules de MIB de ce document utilisent les valeurs d'identifiant d'objet suivantes allouées par l'IANA enregistrées dans le registre des numéros de SMI :

Descripteur	**Valeur d'IDENTIFIANT D'OBJET**
syslogTCMIB	{ mib-2 173 }

6. Références

6.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

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

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

6.2 Références pour information

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

7. Remerciements

Ce document a été produit par le groupe de travail Syslog. L'auteur tient à remercier Chris Lonvick, David Harrington, Juergen Schoenwaelder, et Pasi Eronen de leurs commentaires et suggestions.

Adresse de l'auteur

Glenn Mansfield Keeni
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-3204
Japan

téléphone : +81-22-303-4012
mél : glenn@cysols.com