Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5674
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

S. Chisholm, Nortel
R. Gerhards, Adiscon GmbH
octobre 2009
Traduction Claude Brière de L'Isle

Alarmes dans Syslog

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.

Table des matières

1. Introduction

En plus d'envoyer en asynchrone des informations d'alarme via des protocoles comme le protocole simple de gestion de

réseau (SNMP, *Simple Network Management Protocol*) ou le protocole de configuration de réseau (Netconf, *Network Configuration Protocol*) de nombreuses mises en œuvre enregistrent aussi des alarmes via syslog. Le présent mémoire définit un ensemble de SD-PARAM pour prendre en charge l'enregistrement et définit une transposition de la sévérité syslog en la sévérité de l'alarme.

La MIB d'alarme [RFC3877] inclut des champs d'alarme obligatoires à partir de la Recommandation UIT-T X.733 [X.733] ainsi que des informations provenant de [X.736]. De plus, la MIB d'alarme introduit ses propres champs d'alarme. Le présent mémoire réutilise la terminologie et les champs de la MIB Alarme.

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].

La terminologie relative aux alarmes est définie dans la [RFC3877].

SD-ID, SD-PARAM, et les autres termes relatifs à syslog sont définis dans la [RFC5424].

2. Transposition de sévérité

La MIB Alarme [RFC3877] définit les sévérités perçues par l'UIT ; il est utile d'être capable de les mettre en relation avec les champs de message syslog, en particulier dans le cas où les alarmes sont enregistrées. Le présent mémoire décrit la représentation des sévérités perçues par l'UIT dans les champs syslog appropriés, qui sont décrits dans la [RFC5424]. Syslog offre à la fois un champ dit SEVERITY ainsi que STRUCTURED-DATA *(données structurées)*. Du fait des contraintes de syslog, il n'y a pas de transposition bijective possible pour SEVERITY. Un élément STRUCTURED-DATA est défini dans le présent document pour permettre l'inclusion de la sévérité perçue par l'UIT non modifiée.

Syslog prend en charge des valeurs de sévérité différentes des sévérités perçues par l'UIT. Elles sont définies au paragraphe 6.2.1 de la [RFC5424]. La transposition montrée au Tableau 1 ci-dessous DEVRAIT être utilisée pour transposer les sévérités perçues par l'UIT en sévérités syslog.

Sévérité perçue par l'UIT	**SEVERITY syslog (nom)**
Critique	1 (Alerte)
Majeure	2 (Critique
Mineure	3 (Erreur)
Avertissement	4 (Avertissement)
Indéterminée	5 (Remarque)
Supprimée	5 (Remarque)

Tableau 1 : Transposition de sévérité perçue par l'UIT en sévérité Syslog

3. Éléments d'alarme STRUCTURED-DATA

STRUCTURED-DATA permet l'inclusion de toutes informations structurées dans un message syslog. Ce qui suit est défini dans le présent document pour prendre en charge la structuration des informations d'alarme.

- Ressource sous alarme
- Cause probable
- Type d'événement
- Sévérité perçue
- Indication de tendance
- URI de ressource

La prise en charge du SD-ID "alarme" est facultative mais, une fois pris en charge, certains des SD-PARAMS sont obligatoires.

3.1 Resource

Si le SD-ID "alarme" est inclus, le SD-PARAM "resource" DOIT être inclus. Cet élément identifie de façon univoque la

ressource sous alarme dans la portée d'un élément de réseau.

3.2 probableCause

Si le SD-ID "alarme" est inclus, le SD-PARAM "probableCause" DOIT être inclus. Ce paramètre est le mnémonique associé à l'objet IANAItuProbableCause défini dans la [RFC3877] et toutes les extensions suivantes définies par l'IANA. Par exemple, IANAItuProbableCause définit une défaillance de transmission à une cause probable de "transmissionError (10)". La valeur du paramètre dans ce cas serait "transmissionError".

3.3 perceivedSeverity

Si le SD-ID "alarme" est inclus, le SD-PARAM "perceivedSeverity" DOIT être inclus. Comme pour la définition de la sévérité perçue dans [X.736] et la [RFC3877], cet objet peut prendre les valeurs suivantes :

- o cleared *(supprimé)*
- o indeterminate *(indéterminé)*
- o critical *(critique)*
- o major *(majeur)*
- o minor *(mineur)*
- o warning *(avertissement)*

Voir à la Section 2 la relation entre cette sévérité et la sévérité syslog.

3.4 eventType

Si le SD-ID "alarme" est inclus, le SD-PARAM "eventType" DEVRAIT être inclus. Ce paramètre est le mnémonique associé à l'objet IANAItuEventType défini dans la [RFC3877] et toutes les extensions suivantes définies par l'IANA. Par exemple, IANAItuEventType définit une alarme environnementale à un type d'événement de "environmentalAlarm (6)". La valeur du paramètre dans ce cas serait "environmentalAlarm".

3.5 trendIndication

Si le SD-ID "alarme" est inclus, le SD-PARAM "trendIndication" DEVRAIT être inclus. Comme pour la définition de la sévérité perçue dans [X.733] et la [RFC3877], cet objet peut prendre les valeurs suivantes :

- o moreSevere *(plus sévère)*
- o noChange *(pas de changement)*
- o lessSevere *(moins sévère)*

3.6 resourceURI

Si le SD-ID "alarme" est inclus, le SD-PARAM "resourceURI" DEVRAIT être inclus. Cet élément identifie de façon univoque la ressource sous alarme.

La valeur de ce champ DOIT se conformer à la définition d'URI dans la [RFC3986] et ses mises à jour. Dans le cas d'une ressource SNMP, la syntaxe de la [RFC4088] DOIT être utilisée et "resourceURI" doit pointer sur la même ressource que alarmActiveResourceId [RFC3877] pour cette alarme.

Les deux paramètres "resource" et "resourceURI" pointent sur la ressource qui subit l'alarme, mais le "resourceURI" a une contrainte syntaxique qui exige que ce soit un URI. Cela rend facile de corréler cette alarme syslog à toutes les alarmes qui sont reçues via d'autres protocoles, comme SNMP, ou d'utiliser SNMP ou d'autres protocoles pour obtenir des informations supplémentaires sur cette ressource.

4. Exemples

Exemple 1 - Informations d'alarme obligatoires

<165>1 2003-10-11T22:14:15.003Z mymachine.exemple.com

evntslog - ID47 [exampleSDID@32473 iut="3" eventSource=
"Application" eventID="1011"][alarm resource="su root"
probableCause="unauthorizedAccessAttempt"
perceivedSeverity="major"]
BOMUne entrée d'enregistrement d'événement d'application ...

Dans cet exemple, étendu de la [RFC5424], la VERSION est 1 et la Facilité a la valeur de 4. La sévérité est 2. Le message a été créé le 11 octobre 2003 à 22:14:15 UTC, 3 millisecondes dans la seconde suivante. Le message est généré d'un hôte qui s'identifie comme "mymachine.exemple.com". Le APP-NAME est "evntslog" et le PROCID est inconnu. Le MSGID est "ID47". On a inclus les données structurées de l'exemple original, un seul élément avec la valeur "[exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"]", et un nouvel élément avec les informations d'alarme définies dans le présent mémoire. Le SD-ID d'alarme contient le SD-PARAMS obligatoire de resource, probableCause, et perceivedSeverity. Le message lui-même est "Une entrée d'enregistrement d'événement d'application...". Le BOM au début du MSG indique le codage UTF-8.

Exemple 2 - Informations d'alarme supplémentaires

<165>1 2004-11-10T20:15:15.003Z mymachine.exemple.com
evntslog - ID48 [alarm resource="interface 42"
probableCause="unauthorizedAccessAttempt"
perceivedSeverity="major"
eventType="communicationsAlarm"
resourceURI="snmp://exemple.com//1.3.6.1.2.1.2.2.1.1.42"]

Dans cet exemple, on inclut deux champs d'alarme facultatifs : eventType et resourceURI.

5. Considérations sur la sécurité

En plus des considérations générales de syslog sur la sécurité discutées dans la [RFC5424], les informations contenues dans les alarmes peuvent fournir à des pirates des informations utiles sur des parties du système qui subissent actuellement une pression ainsi que des informations générales sur le système, comme des inventaires.

Les utilisateurs ne devraient pas avoir accès aux information d'alarmes que leurs permissions d'accès normales ne leur permettraient pas si l'accès aux informations se faisait d'une autre façon.

Il n'y a pas de modèle de contrôle d'accès normalisé pour syslog, et donc la capacité de filtrer les alarmes fondée sur une notion d'identité du receveur est, au mieux, spécifique de la mise en œuvre.

6. Considérations relatives à l'IANA

L'IANA a enregistré les valeurs d'identifiant de données structurées syslog et de PARAM-NAME montrées ci-dessous :

SD-ID	PARAM-NAME	
alarm		FACULTATIF
	resource	OBLIGATOIRE
	probableCause	OBLIGATOIRE
	perceivedSeverity	OBLIGATOIRE
	eventType	FACULTATIF
	trendIndication	FACULTATIF
	resourceURI	FACULTATIF

7. Remerciements

Merci aux membres des groupes de travail Syslog et OPSAWG qui ont contribué à cette spécification. Merci aussi à Juergen Schoenwaelder, Dave Harrington, Wes Hardaker, et Randy Presuhn de leur relecture.

8. Références

8.1 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)

[RFC3877] S. Chisholm, D. Romascanu, "Base de données d'informations de gestion d'alarmes", septembre 2004. *(P.S.)*

[RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiant de ressource uniforme (URI) : Syntaxe générique", DOI 10.17487/RFC3986, STD 66, janvier 2005. *(P.S. ; MàJ par* RFC8820)

[RFC4088] D. Black et autres, "Schéma d'identifiant de ressource uniforme (URI) pour le protocole simple de gestion de réseau (SNMP)", juin 2005.*(P.S.)*

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

8.2 Références pour information

[X.733] Recommandation UIT-T X.733, "Technologie de l'information - Interconnexion des systèmes ouverts - Gestion de système : Fonction de rapport d'alarme", <https://www.itu.int/rec/T-REC-X.733>. 1992.

[X.736] Recommandation UIT-T X.736, "Technologie de l'information - Interconnexion des systèmes ouverts - Gestion de système : Fonction de rapport d'alarme de sécurité", <https://www.itu.int/rec/T-REC-X.736>. 1992

Adresse des auteurs

Sharon Chisholm
Nortel
3500 Carling Ave
Nepean, Ontario K2H 8E9
Canada
mél : schishol@nortel.com

Rainer Gerhards
Adiscon GmbH
Mozartstrasse 21
Grossrinderfeld, BW 97950
Germany
mél : rgerhards@adiscon.com