

Groupe de travail Réseau
Request for Comments : 2872
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

Y. Bernet
R. Pabbati
Microsoft
juin 2000

Élément de politique d'identité d'application et de sous-application à utiliser avec RSVP

Statut du présent mémoire

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

Notice de Copyright

Copyright (C) The Internet Society (2000). Tous droits réservés.

Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

Résumé

Les messages de signalisation RSVP [RFC2205] comportent normalement des objets de données de politique, qui à leur tour contiennent des éléments de politique. Les éléments de politique peuvent décrire des informations d'utilisateur et/ou d'application, qui peuvent être utilisées par les éléments de réseau à capacité RSVP pour appliquer les décisions de politique appropriées à un flux de trafic. Le présent mémoire détaille l'usage des éléments de politique qui fournissent les informations d'application.

1. Généralités

Les éléments de réseau à capacité RSVP peuvent agir comme des points de mise en application de politique (PEP, *policy enforcement point*). Ils travaillent ensemble avec les points de décision de politique (PDP, *policy decision point*) pour mettre en application la politique de qualité de service. En bref, les PEP extraient les informations de politique des demandes de signalisation RSVP et comparent ces informations à celles mémorisées par un PDP dans une base de données ou répertoire de politique (éventuellement distant). Une décision de politique est prise sur la base des résultats de la comparaison.

Un type d'information de politique décrit l'application au nom de laquelle est générée une demande de signalisation RSVP. Lorsque les informations de politique d'application sont disponibles, les administrateurs de réseau sont capables de gérer la QS sur la base du type d'application. Ainsi, par exemple, un administrateur de réseau peut établir une politique qui donne la priorité sur des jeux à des applications dont la mission critique est connue.

Le présent mémoire décrit une structure pour un élément de politique qui peut être utilisée pour identifier des flux de trafic d'applications. L'élément de politique comporte un certain nombre d'attributs, dont l'un est un localisateur de politique. Ce localisateur de politique comporte les sous-éléments ordonnés hiérarchiquement suivants (en niveaux de hiérarchie décroissants) :

1. identifiant qui identifie de façon univoque le fabricant de l'application
2. identifiant de l'application
3. numéro de version de l'application
4. identifiant de sous application

Un nombre arbitraire d'identifiants de sous-application peut être inclus dans le localisateur de politique. Un exemple d'un tel identifiant est "imprimer la transaction".

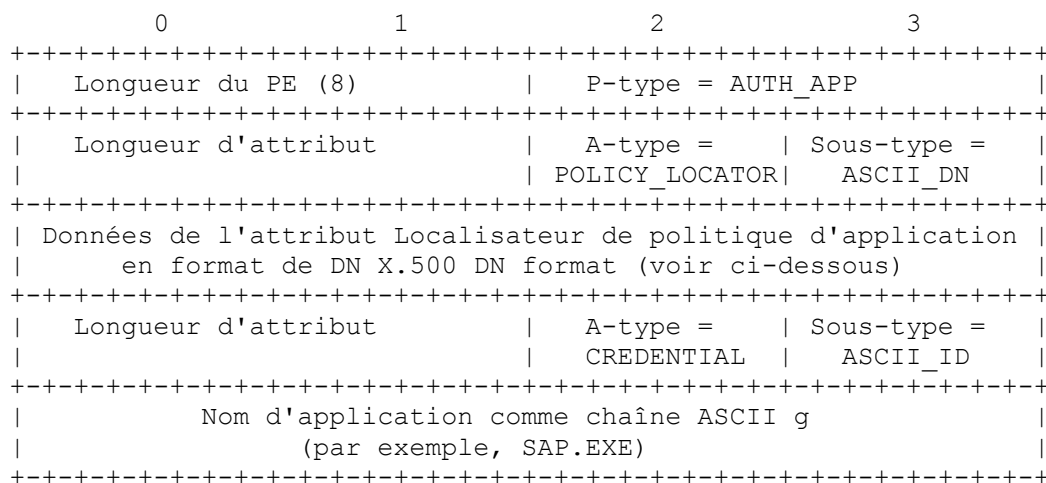
Le présent mémoire spécifie la structure de l'élément de politique d'application et propose des mots clés pour les sous-éléments à chaque niveau de la hiérarchie. Il n'énumère pas les valeurs spécifiques des sous-éléments : une telle énumération sort du domaine d'application du présent mémoire.

2. Structure simple d'élément de politique d'identité d'application

Les éléments généraux de politique d'identité d'application sont définis dans la [RFC2752]. Ce sont des éléments de politique avec un P-type de AUTH_APP. Une liste d'attributs d'authentification suit l'en-tête de l'élément de politique.

Le premier attribut d'authentification est du A-type POLICY_LOCATOR. Le sous-type de l'attribut POLICY_LOCATOR est du type ASCII_DN [RFC1779] ou UNICODE_DN. Les données d'attribut réelles sont formatées comme un nom distinctif X.500 (DN), représentant, dans une structure hiérarchique, un identifiant unique au monde, l'application, le numéro de version et la sous-application. L'attribut POLICY_LOCATOR contient des mots clés comme décrit à la section 2. Pour plus de détails sur le format de l'attribut POLICY_LOCATOR, voir la [RFC2752].

Le second attribut d'authentification est du A-type CREDENTIAL. Le sous-type de l'attribut CREDENTIAL est du type ASCII_ID ou UNICODE_ID. Les données d'attribut réelles sont une chaîne ASCII ou Unicode représentant le nom de l'application. Cette structure est illustrée dans le diagramme suivant :



Les mots clés suivants sont RECOMMANDÉS, mais d'autres PEUVENT être utilisés :

Clé	Attribut
GUID	Identifiant unique au monde (facultatif)
APP	Nom d'application
VER	Numéro de version d'application
SAPP	Sous application (facultatif)

Ci-après figurent des exemples de localisateurs de politique conformes :

```
"APP=SAP, VER=1.1, SAPP=Print"
```

```
"GUID=http://www.microsoft.com/apps, APP=MyApplication, VER=1.2.3"
```

Les attributs APP, VER et SAPP DEVRAIENT décrire l'application à un lecteur humain d'une façon aussi univoque et non ambiguë que possible. L'attribut GUID PEUT être utilisé lorsque l'unicité absolue de l'identification de l'application est nécessaire et son contenu DOIT être un identifiant venant d'une source unique au monde (par exemple, des noms de domaine tels qu'alloués par les autorités d'enregistrement correspondantes). Noter que la publication des identifiants choisis dans un format convenable est vivement encouragée.

3. Considérations pour la sécurité

L'élément de politique simple proposé ne garantit pas que cet élément soit bien associé à l'application à laquelle il prétend être associé. Afin de fournir de telles garanties, il est nécessaire de signer les applications. Les éléments de politique d'application signés pourront être proposés à l'avenir. Noter que, normalement, l'élément de politique d'application sera inclus dans un message RSVP avec un élément de politique chiffré et authentifié. Un niveau de sécurité supplémentaire est fourni en ne faisant confiance à l'élément de politique d'application que si l'élément de politique d'utilisateur est de confiance.

Toutes les considérations sur l'intégrité dans RSVP s'appliquent au message qui contient l'élément de politique d'application.

4. Références

- [ASCII] "Coded Character Set -- 7-Bit American Standard Code for Information Interchange", ANSI X3.4-1986.
- [RFC1779] S. Kille, "Représentation de chaîne des noms distinctifs", mars 1995. (*Obsolète, voir [RFC2253](#), [RFC3494](#)*) (*Historique*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "[Protocole de réservation de ressource](#) (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par [RFC2750](#), [RFC3936](#), [RFC4495](#)*) (*P.S.*)
- [RFC2752] S. Yadav et autres, "[Représentation d'identité](#) pour RSVP", janvier 2000. (*Obsolète, voir [RFC3182](#)*) (*P.S.*)
- [UNICODE] The Unicode Consortium, "The Unicode Standard, Version 2.0", Addison-Wesley, Reading, MA, 1996.

5. Remerciements

Merci pour leurs apports à Tim Moore, Shai Mohaban, Andrew Smith, Ulrich Homann et aux autres contributeurs au groupe de travail RAP de l'IETF.

6. Adresse des auteurs

Yoram Bernet
One Microsoft Way
Redmond, WA 98052
téléphone : (425) 936-9568
mél : yoramb@microsoft.com

Ramesh Pabbati
One Microsoft Way
Redmond, WA 98052
USA
mél : rameshpa@microsoft.com

7. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2000). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de droits de reproduction ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.