

Groupe de travail Réseau
Request for Comments : 4088
 Catégorie : Sur la voie de la normalisation
 Traduction Claude Brière de L'Isle

D. Black, EMC Corporation
 K. McCloghrie, Cisco Systems
 J. Schoenwaelder, International University Bremen
 juin 2005

Schéma d'identifiant de ressource universel (URI) pour le protocole simple de gestion de réseau (SNMP)

Statut de ce 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 (2005).

Résumé

Le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) et le cadre de gestion standard de l'Internet sont largement utilisés pour la gestion des appareils de communication, créant le besoin de spécifier l'accès SNMP (incluant l'accès aux instances d'objet de MIB SNMP) à partir d'environnements de gestion non SNMP. Par exemple, lorsque la gestion IP hors bande est utilisée via une interface de gestion séparée (par exemple, pour un appareil qui ne prend pas en charge l'accès IP dans la bande) une façon uniforme d'indiquer comment contacter l'appareil pour la gestion est nécessaire. Les identifiants de ressource universels (URI, *Uniform Resource Identifier*) satisfont bien à ce besoin, car ils permettent qu'une seule chaîne de texte indique un point d'extrémité de communication d'accès de gestion pour une grande variété de protocoles fondés sur IP.

Le présent document définit un schéma d'URI afin que SNMP puisse être désigné comme le protocole utilisé pour la gestion. Le schéma permet aussi à un URI de désigner une ou plusieurs instances d'objets de MIB.

Table des Matières

1. Introduction.....	1
2. Usage.....	2
3. Syntaxe d'URI SNMP.....	3
3.1 Considérations de références relatives.....	4
4. Sémantique et fonctionnement.....	4
4.1 URI de service SNMP.....	4
4.2 URI d'objet SNMP.....	4
4.3 Groupes d'OID dans les URI SNMP.....	6
4.4 Considérations d'interopérabilité.....	6
5. Exemples.....	7
6. Considérations sur la sécurité.....	7
6.1 Considérations de sécurité d'URI SNMP à passerelle SNMP.....	8
7. Considérations relatives à l'IANA.....	8
8. Références normatives.....	8
9. Références pour information.....	9
10. Remerciements.....	9
Appendice A. Gabarit d'enregistrement.....	9
Adresse des auteurs.....	10
Déclaration complète de droits de reproduction.....	10

1. Introduction

SNMP et le cadre de gestion standard de l'Internet ont été conçus à l'origine pour gérer les appareils IP via des moyens dans la bande, dans lesquels l'accès de gestion est principalement via la ou les mêmes interfaces qu'utilisées pour envoyer et recevoir le trafic IP. La large adoption de SNMP a résulté en son utilisation pour gérer des appareils de communication qui ne prennent pas en charge l'accès IP dans la bande (par exemple, les appareils de canal fibre) ; une interface IP hors bande

séparée est souvent utilisée pour la gestion. Les URI fournissent un moyen commode pour localiser cette interface et spécifier le protocole à utiliser pour la gestion ; un scénario possible est qu'une interrogation dans la bande retourne un URI qui indique comment l'appareil est géré. Le présent document spécifie un schéma d'URI pour permettre à SNMP (incluant un contexte SNMP spécifique) d'être désigné comme protocole de gestion par un tel URI. Ce schéma permet aussi à un URI de se référer à des instances d'objet spécifiques au sein d'une MIB SNMP.

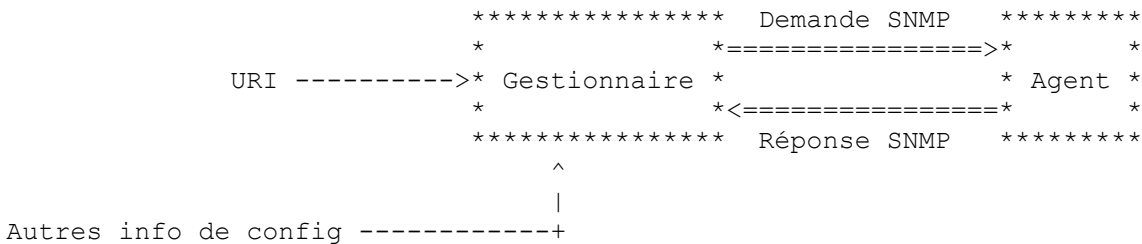
Pour une vue détaillée des documents qui décrivent le cadre actuel de gestion standard de l'Internet, prière de se référer à la Section 7 de la [RFC3410].

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].

2. Usage

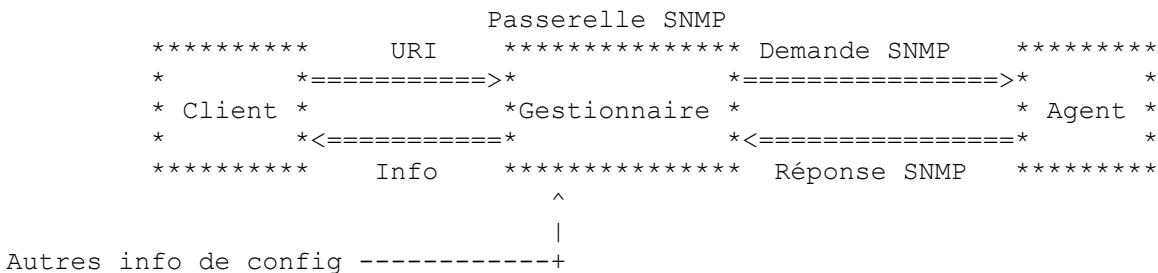
Il y a deux classes majeures d'usage d'URI SNMP : la configuration et les passerelles entre SNMP et les autres protocoles qui utilisent les URI SNMP.

Un URI SNMP utilisé pour la configuration indique la localisation des informations de gestion au titre de la configuration d'une application contenant un gestionnaire SNMP. L'URI peut être obtenu d'un fichier de configuration ou peut être fourni par un appareil géré (voir un exemple à la Section 1). Les informations de gestion sont échangées entre le gestionnaire SNMP et un agent, mais elles ne s'écoulent pas au delà du gestionnaire, comme le montre le diagramme suivant :



Des informations de configuration supplémentaires (par exemple, un secret ou clé de sécurité) peuvent être fournies via une interface autre que celle utilisée pour l'URI. Par exemple, quand un appareil géré fournit un URI SNMP d'une façon non protégée, cet appareil ne devrait pas fournir un secret ou une clé requise pour utiliser l'URI. Le secret ou la clé devrait plutôt être pré configuré dans le gestionnaire ou pré autorisé à celui-ci ; voir la Section 6.

Pour l'usage de passerelle, les clients emploient des URI SNMP pour demander des informations de gestion via un URI SNMP à la passerelle SNMP (aussi appelée une passerelle SNMP dans le présent document). Le gestionnaire SNMP au sein de la passerelle SNMP accède aux informations de gestion et les retourne au client demandeur, comme le montre le diagramme suivant :



Des informations de configuration supplémentaires (par exemple, des secrets ou clés de sécurité) peuvent être fournies via une interface autre que celle utilisée pour l'URI. Par exemple, certains types d'informations de sécurité, incluant des secrets et des clés, devraient être pré configurés dans le gestionnaire ou pré autorisés à celui-ci plutôt que d'être fournis par le client ; voir la Section 6.

3. Syntaxe d'URI SNMP

Un URI SNMP a la syntaxe ABNF [RFC2234] suivante, sur la base des règles de syntaxe ABNF pour userinfo, host, port, et segment (de chemin) de la [RFC3986] la règle de syntaxe ABNF pour HEXDIG dans la [RFC2234] :

```

snmp-uri = "snmp://" snmp-authority [ context [ oids ] ]

snmp-authority = [ securityName "@" ] host [ ":" port ]
securityName   = userinfo           ; securityName SNMP

context = "/" contextName [ ";" contextEngineID ]
contextName = segment              ; contextName SNMP
contextEngineID = 1*(HEXDIG HEXDIG) ; contextEngineID SNMP

oids = "/" ( oid / oid-group ) [ suffix ]
oid-group = "(" oid *(", " oid ) ")"
oid = < comme spécifié par la [RFC 3061] >
suffix = "+" / ".*"

```

Les règles ABNF userinfo et segment (de chemin) ne sont réutilisées que pour la syntaxe. À l'opposé, host et port ont tous deux leur syntaxe et leur sémantique spécifiées dans la [RFC3986]. Voir dans la [RFC3411] la sémantique de securityName, contextEngineID, et contextName.

La syntaxe de snmp-authority correspond à la syntaxe de URI d'autorité au paragraphe 3.2 de la [RFC3986], avec la restriction supplémentaire que le composant userinfo d'une autorité (lorsque présente) DOIT être un securityName SNMP. Si le securityName est vide ou n'est pas donné, l'entité qui fait usage d'un URI SNMP est supposée savoir quel securityName SNMP utiliser si il en est exigé un. L'inclusion d'informations d'authentification (par exemple, des mots de passe) dans les URI a été déconseillée (voir au paragraphe 3.2.1 de la [RFC3986]) de sorte que tout secret ou clé exigé pour l'accès à SNMP doit être fourni via d'autres moyens qui peuvent être hors bande par rapport à la communication de l'URI. Si l'accès est vide ou n'est pas donné, l'accès 161 est supposé.

Si le contextName (nom de contexte) est vide ou n'est pas donné, la chaîne de longueur zéro ("") est supposée, car c'est le contexte SNMP par défaut. Un contextEngineID (*identifiant de moteur de contexte*) SNMP est un élément binaire de format variable qui est généralement découvert par un gestionnaire SNMP. Un URI SNMP code un contextEngineID comme les chiffres hexadécimaux qui correspondent à une séquence d'octets. Si le contextEngineID est vide ou n'est pas donné, le moteur de contexte est à découvrir en interrogeant l'agent SNMP à l'hôte et accès spécifiés ; voir au paragraphe 4.1. Le composant contextEngineID de l'URI DEVRAIT être présent si plus d'un moteur de contexte prend en charge le contexte désigné à l'hôte et accès désignés.

Un URI SNMP qui désigne le contexte SNMP par défaut ("") PEUT se terminer par le caractère "/" qui introduit le composant contextName (*nom de contexte*). Un URI SNMP NE DOIT PAS se terminer par le caractère "/" qui introduit un composant oid ou oid-group, car la chaîne vide n'est pas un OID valide pour SNMP.

Les règles de codage spécifiées dans la [RFC3986] DOIVENT être utilisées pour les URI SNMP, y compris l'utilisation du codage en pourcentage ("%") suivi par deux chiffres hexadécimaux) comme nécessaire pour représenter les caractères définis comme réservés dans la [RFC3986] et tous caractères interdits dans un URI. SNMP permet tous les caractères UTF-8 dans un securityName ou contextName ; tous les caractères UTF-8 multi octets dans un URI SNMP DOIVENT être codés en pourcentage comme spécifié aux paragraphes 2.1 et 2.5 de la [RFC3986]. Ces exigences sont une conséquence de la réutilisation des règles de syntaxe ABNF pour userinfo et segment de la [RFC3986].

Les URI SNMP vont généralement être assez courts pour éviter les limites de longueur de chaîne des mises en œuvre (par exemple, celle qui peut se produire à 255 caractères). De telles limites peuvent être un problème pour les grands groupes d'OID ; des références relative aux URI (voir au paragraphe 4.2 de la [RFC3986]) peuvent fournir une solution de remplacement dans certaines circonstances.

L'utilisation d'adresses IP dans les URI SNMP est acceptable dans des situations où la dépendance à la disponibilité du service du DNS n'est pas souhaitable ou doit être évitée ; autrement, les adresses IP ne devraient pas être utilisées (voir plus d'explications dans la [RFC1900]).

3.1 Considérations de références relatives

L'utilisation du contexte SNMP par défaut (chaîne de longueur zéro) au sein d'un URI SNMP peut résulter en une seconde instance de "/" dans l'URI, comme dans : `snmp://<hôte>//<oid>`

Ceci est permis par la syntaxe de la [RFC3986] ; si un analyseur d'URI ne traite pas correctement le second "/", l'analyseur a un problème et doit être réparé. Cet exemple est important parce que il est prévu que l'utilisation du contexte SNMP par défaut dans les URI SNMP soit courante.

D'un autre côté, la seconde occurrence de "/" dans un URI absolu SNMP affecte l'usage des références relatives à cet URI (voir le paragraphe 4.2 de la [RFC3986]) parce que un "/" au début d'une référence relative introduit toujours un composant d'autorité d'URI (hôte plus userinfo et/ou accès facultatifs ; voir la [RFC3986]). Précisément, une référence relative de la forme `//<oid2>` ne va pas fonctionner, parce que le "/" va être cause que `<oid2>` sera analysé comme une autorité d'URI, résultant en une erreur de syntaxe lorsque l'analyseur ne trouve pas d'hôte dans `<oid2>`. Pour éviter ce problème, les références relatives qui commencent par "/" mais ne contiennent pas de composant d'autorité d'URI NE DOIVENT PAS être utilisées. Une fonctionnalité équivalente à cette référence relative interdite peut être obtenue en ajoutant en préfixe "." ou ".." à la référence relative interdite (par exemple, `../<oid2>`). Le préfixe à utiliser dépend de l'URI de base.

4. Sémantique et fonctionnement

Un URI SNMP qui n'inclut pas d'OID est appelé un URI de service SNMP parce qu'il désigne un point d'extrémité de communication pour l'accès à un service de gestion SNMP. Un URI SNMP qui inclut un ou plusieurs OID est appelé un URI d'objet SNMP parce qu'il désigne une ou plusieurs instances d'objets dans une MIB SNMP. Les moyens attendus de l'utilisation d'un URI SNMP sont d'employer un gestionnaire SNMP pour accéder au contexte SNMP désigné par l'URI via l'agent SNMP à l'hôte et accès désignés par l'URI.

4.1 URI de service SNMP

Un URI de service SNMP ne désigne pas un objet de données, mais plutôt un contexte SNMP auquel on accède par un service ; le schéma d'URI telnet [RFC1738] est un autre exemple d'URI qui désigne un accès de service. Si le `contextName` dans l'URI est vide ou n'est pas donné, "" (la chaîne de longueur zéro) est supposée, car c'est le contexte SNMP par défaut.

Si un `contextEngineID` est donné dans un URI de service SNMP, le moteur de contexte qu'il désigne doit être utilisé. Si le `contextEngineID` est vide ou n'est pas donné dans l'URI, le moteur de contexte est à découvrir ; le moteur de contexte à utiliser est celui qui prend en charge le contexte désigné par l'URI. Le composant `contextEngineID` de l'URI DEVRAIT être présent si plus d'un moteur de contexte prend en charge le contexte désigné à l'hôte et l'accès désignés.

De nombreuses utilisations courantes des URI SNMP vont probablement omettre (c'est-à-dire inclure la valeur par défaut) le `contextEngineID` parce qu'elles n'impliquent pas d'agents mandataires SNMP, qui sont la raison la plus courante de l'existence de plusieurs moteurs de contexte SNMP à un seul hôte et accès. Précisément, lorsque un agent SNMP est local pour l'interface réseau qu'il gère, l'agent va généralement avoir seulement un moteur de contexte, et dans ce cas il est sûr d'omettre le composant `contextEngineID` d'un URI SNMP. De plus, de nombreux agents SNMP qui sont locaux pour une interface réseau ne prennent en charge le contexte SNMP par défaut (chaîne de longueur zéro).

4.2 URI d'objet SNMP

Un URI d'objet SNMP contient un ou plusieurs OID. L'URI est utilisé en séparant d'abord l'OID ou groupe d'OID (incluant sa barre oblique précédente plus toutes parenthèses et suffixes) et en traitant ensuite l'URI de service SNMP résultant comme spécifié au paragraphe 4.1 pour déterminer le contexte SNMP auquel accéder. L'OID ou groupe d'OID est alors utilisé pour générer les opérations SNMP dirigées sur ce contexte SNMP.

La sémantique d'un URI d'objet SNMP dépend de si l'OID ou groupe d'OID a un suffixe et de ce qu'est ce suffixe. Il y a trois formats possibles ; dans chaque cas, les instances d'objets de MIB sont désignés dans le contexte SNMP spécifié par la portion URI de service de l'URI d'objet SNMP. La sémantique d'un URI d'objet SNMP qui contient un seul OID est la suivante :

- (1) un OID sans suffixe désigne l'instance d'objet de MIB nommée par l'OID ;
- (2) un OID avec un suffixe "+" désigne la prochaine instance lexicale d'objet de MIB suivant l'OID ;

- (3) un OID avec un suffixe ".*" désigne l'ensemble d'instances d'objets de MIB pour lequel l'OID est un strict préfixe lexical ; cela n'inclut pas l'instance d'objet de MIB nommée par l'OID.

Un groupe d'OID dans un URI SNMP consiste en un ensemble d'OID entre parenthèses. Dans chaque cas, la sémantique du groupe d'OID est l'extension de la seule sémantique d'OID de chaque OID dans le groupe (par exemple, un URI avec un suffixe "+" désigne l'ensemble des instances d'objet de MIB consistant en l'instance lexicalement suivante pour chaque OID dans le groupe d'OID).

Lorsque il y a un choix à faire entre les formats d'URI pour désigner la ou les mêmes instances d'objet de MIB, la liste ci dessus est en ordre de préférence (aucun suffixe n'est plus préférable) car elle va du plus précis au moins précis. C'est parce que un OID sans suffixe désigne précisément une instance d'objet, tandis qu'un suffixe "+" désigne la prochaine instance d'objet, qui peut changer, et le suffixe ".*" pourrait désigner plusieurs instances d'objet. Plusieurs URI SNMP syntaxiquement distincts NE DEVRAIENT PAS être utilisés pour désigner la même instance ou ensemble d'instances d'objet de MIB, car cela peut causer des résultats inattendus dans les systèmes fondés sur les URI qui utilisent la comparaison de chaîne pour vérifier l'égalité des URI.

Les URI d'objet SNMP désignent les données auxquels accéder, par opposition aux opérations SNMP spécifiques à utiliser pour l'accès ; le paragraphe 4.2.1 donne des exemples de comment les opérations SNMP peuvent être utilisées pour accéder aux données pour les URI d'objet SNMP. Néanmoins, toute opération SNMP applicable, incluant GetBulk, PEUT être utilisée pour les données d'accès pour tout ou partie d'un ou plusieurs URI d'objet SNMP (par exemple, via l'utilisation de plusieurs liens de variables dans une seule opération) ; il n'est pas nécessaire d'utiliser les opérations spécifiques décrites au paragraphe 4.2.1 tant que le résultat (les liens de variable retournés ou une erreur) pourrait avoir été obtenu en suivant les descriptions du paragraphe 4.2.1. L'utilisation de références relatives qui ne changent pas le contextName (c'est-à-dire, ./<oid>) devrait être vue comme une indication que l'optimisation de l'accès SNMP à travers plusieurs URI SNMP est possible.

Un URI d'objet SNMP PEUT aussi être utilisé pour spécifier une instance d'objet de MIB ou des instances à écrire ; ceci cause la génération d'une opération SNMP Set au lieu d'un Get. Les suffixes "+" et ".*" NE DOIVENT PAS être utilisés dans ce cas ; toute tentative de le faire est une erreur qui NE DOIT PAS générer d'opération SNMP Set. Les valeurs à écrire dans cette ou ces instances d'objet de MIB ne sont pas spécifiées dans un URI d'objet SNMP.

Les URI d'objet SNMP désignent des données dans les MIB SNMP et donc ne fournissent pas de moyen pour générer toutes les opérations possibles du protocole SNMP. Par exemple, l'accès aux données pour un URI d'objet SNMP ne peut pas directement générer de notification Snmpv2-Trap ou InformRequest, bien qu'un effet collatéral de l'accès aux données pourrait causer de telles notifications (selon la MIB). De plus, si et comment GetBulk est utilisé pour un URI d'objet SNMP avec un suffixe ".*" est spécifique de la mise en œuvre.

4.2.1 Accès aux données d'URI d'objet SNMP

L'accès aux données sur la base d'un URI d'objet SNMP retourne un lien de variable SNMP pour chaque instance d'objet de MIB désigné par l'URI, ou une erreur SNMP si l'opération échoue. Un lien de variable SNMP lie un nom de variable (OID) à une valeur ou une exception SNMP (voir la [RFC3416]). La ou les opérations SNMP nécessaires pour accéder aux données désignées par un URI d'objet SNMP dépendent du suffixe de l'OID ou du groupe d'OID, ou de son absence. Les descriptions qui suivent ne sont pas la seule méthode pour effectuer l'accès aux données pour un URI d'objet SNMP ; toute opération SNMP convenable peut être utilisée pour autant que les résultats (les liens de variable retournés ou l'erreur) soient fonctionnellement équivalents.

- (1) Pour un OID ou groupe d'OID sans suffixe, une opération SNMP Get est générée en utilisant chaque OID comme un nom de lien de variable. Si une erreur SNMP se produit, cette erreur est le résultat d'un accès aux données d'URI ; autrement, le ou les liens de variable retournés sont le résultat d'un accès aux données d'URI. Noter que tout lien de variable retourné peut contenir une exception SNMP "noSuchObject" ou "noSuchInstance".
- (2) Pour un OID ou groupe d'OID avec un suffixe "+", une opération SNMP GetNext est générée en utilisant chaque OID comme un nom de lien de variable. Si une erreur SNMP se produit, cette erreur est le résultat d'un accès aux données d'URI ; autrement, le ou les liens de variable retournés sont le résultat d'un accès aux données d'URI. Noter que tout lien de variable retourné peut contenir une exception SNMP "endOfMibView".
- (3) Pour un OID ou groupe d'OID avec un suffixe ".*", une opération SNMP GetNext est initialement générée en utilisant chaque OID comme un nom de lien de variable. Si le résultat est une erreur SNMP, cette erreur est le résultat d'un accès aux données d'URI. Si tous les liens de variable retournés contiennent soit a) un OID pour lequel l'OID d'URI correspondant n'est pas un préfixe lexical, soit b) une exception SNMP "endOfMibView", alors le lien de variable

retourné est le résultat d'un accès aux données d'URI.

Autrement, les résultats de l'opération GetNext sont sauvegardés, et une autre opération SNMP GetNext est générée en utilisant les OID nouvellement retournés comme noms de liens de variables. Ceci est répété (en sauvegardant les résultats et en générant un GetNext avec les nouveaux OID retournés comme noms de lien de variable) jusqu'à ce que tous les liens de variable retournés d'un GetNext contiennent soit a) un OID pour lequel l'OID d'URI correspondant n'est pas un préfixe lexical, soit b) une exception SNMP "endOfMibView". Les résultats de toutes les opérations GetNext sont combinés pour devenir le résultat global d'accès aux données d'URI ; cela peut inclure des liens de variable dont l'OID n'est pas une extension lexicale de l'OID d'URI correspondant. Si les sous arborescences d'OID (ensembles d'OID pour lesquels un OID d'URI spécifique est un préfixe lexical) ne sont pas de la même taille pour tous les OID dans le groupe d'OID, la plus grande sous arborescence détermine quand cette itération cesse. Les opérations SNMP GetBulk PEUVENT être utilisées pour optimiser cette itération d'accès.

Chaque fois qu'un lien de variable retourné contient un OID pour lequel l'OID d'URI correspondant n'est pas un préfixe lexical ou une exception SNMP "endOfMibView", l'itération de cet élément du groupe d'OID PEUT cesser, réduisant le nombre de liens de variables utilisés dans les opérations GetNext suivantes. Dans ce cas, le résultat de l'accès aux données d'URI pour l'URI SNMP ne va pas consister entièrement d'ensembles de liens de variables qui auraient des tailles de groupe d'OID. Même si cela ne se produit pas, le dernier lien de variable retourné pour chaque membre du groupe d'OID va généralement contenir une exception SNMP "endOfMibView" ou un OID pour lequel l'OID d'URI correspondant n'est pas un préfixe lexical.

4.3 Groupes d'OID dans les URI SNMP

Les groupes d'OID entre parenthèses dans les URI SNMP sont destinés à prendre en charge les instances d'objet de MIB pour lesquels l'accès via une seule opération SNMP est exigé pour assurer des résultats cohérents. Donc, les OID au sein d'un groupe d'OID dans un URI SNMP DEVRAIENT être accédés par une seule opération SNMP contenant un lien de variable correspondant à chaque OID du groupe. Un exemple spécifique implique les conventions textuelles InetAddress et InetAddressType définies dans la [RFC4001], pour lesquelles le format d'une instance InetAddress est spécifié par une instance InetAddressType associée. Si deux de ces instances associées sont lues via des opérations SNMP séparées, les valeurs résultantes pourraient être incohérentes (par exemple, dues à un Set intercalé) causant une interprétation incorrecte de la valeur de InetAddress.

Cette exigence ("DEVRAIT") d'une seule opération s'applique aussi à chaque groupe d'OID résultant de l'itération d'accès pour un URI SNMP avec un suffixe ".*". Lorsque les membres d'un groupe d'OID d'URI SNMP diffèrent par le nombre d'OID pour lequel chacun est un préfixe lexical, cette itération peut être invasive en retournant de nombreux liens de variable pour lesquels l'OID correspondant dans le groupe d'OID n'est pas un préfixe lexical. Une telle invasion peut être évitée en utilisant des références relatives au sein du même contexte (c'est-à-dire, ./<oid>.*) lorsque il n'est pas important d'accéder à plusieurs instances d'objet de MIB dans une seule opération SNMP.

4.4 Considérations d'interopérabilité

Le présent document définit un schéma "snmp" indépendant du transport qui est destiné à s'accommoder de transports SNMP autres que UDP. UDP est le transport par défaut pour l'accès aux informations spécifiées par un URI SNMP pour la rétro compatibilité avec les usages existants, mais d'autres transports PEUVENT être utilisés. Si plus d'un transport peut être utilisé (par exemple, SNMP sur TCP [RFC3430] en plus de SNMP sur UDP) les informations ou l'accès au service SNMP désignées par un URI SNMP NE DEVRAIENT PAS dépendre du transport utilisé (pour SNMP sur TCP, c'est impliqué par la Section 2 de la [RFC3430]).

Un URI SNMP désigne l'utilisation de SNMPv3 comme spécifié par les [RFC3416], [RFC3417], et les documents en rapport, mais d'anciennes versions de SNMP PEUVENT être utilisées conformément à la [RFC3584] quand l'usage de telles versions plus anciennes est inévitable. Pour SNMPv1 et SNMPv2c, les éléments securityName, contextName, et contextEngineID d'un URI SNMP sont transposés de/en le nom de communauté, comme décrit dans la [RFC3584]. Quand le nom de communauté est gardé secret comme forme faible d'authentification, cette transposition devrait être configurée de telle sorte que ces trois éléments ne révèlent pas d'information sur le nom de communauté. Si ce n'est pas fait, tout composant d'URI SNMP qui divulguerait des informations significatives sur un nom de communauté secret DEVRAIT alors être omis. Noter que certains noms de communauté contiennent des caractères réservés (par exemple, "@") qui exigent un codage en pourcentage lorsque ils sont utilisés dans un URI SNMP. Des versions de SNMP (par exemple, v3) ont été omises du schéma d'URI SNMP pour permettre l'utilisation des plus anciennes versions de SNMP, ainsi que de tous possibles futurs successeurs de SNMPv3.

5. Exemples

`snmp://exemple.com`

Cet exemple désigne le contexte SNMP par défaut à l'agent SNMP à l'accès 161 de l'hôte `exemple.com`.

`snmp://tester5@exemple.com:8161`

Cet exemple désigne le contexte SNMP par défaut à l'agent SNMP à l'accès 8161 de l'hôte `exemple.com` et indique que le nom de sécurité SNMP "tester5" doit être utilisé pour accéder à cet agent. Une raison possible d'utiliser un accès non standard est de vérifier une nouvelle version du code d'agent SNMP.

`snmp://exemple.com/bridge1`

Cet exemple désigne le contexte SNMP "bridge1" à `exemple.com`. Parce que le composant `contextEngineID` de l'URI est omis, il DEVRAIT au plus y avoir un moteur de contexte SNMP à `exemple.com` qui prend en charge le contexte "bridge1".

`snmp://exemple.com/bridge1;800002b804616263`

Cet exemple désigne le contexte "bridge1" à `snmp.exemple.com` via le moteur de contexte SNMP 800002b804616263 (représentation de chaîne d'une valeur hexadécimale). Cela évite les ambiguïtés si d'autres moteurs de contexte prennent en charge un contexte "bridge1". Les deux exemples ci-dessus se fondent sur la figure du paragraphe 3.3 de la [RFC3411].

`snmp://exemple.com//1.3.6.1.2.1.1.3.0`

`snmp://exemple.com//1.3.6.1.2.1.1.3+`

`snmp://exemple.com//1.3.6.1.2.1.1.3.*`

Ces trois exemples désignent tous l'instance d'objet `sysUpTime.0` dans la MIB SNMPv2 ou la MIB RFC1213 pour le contexte SNMP par défaut ("") à `exemple.com` car `sysUpTime.0` est :

- a) désigné directement par l'OID 1.3.6.1.2.1.1.3.0,
- b) la prochaine instance lexicale d'objet de MIB après l'OID 1.3.6.1.2.1.1.3, et
- c) la seule instance d'objet de MIB dont l'OID a 1.3.6.1.2.1.1.3 comme préfixe lexical.

Ces trois exemples sont fournis seulement comme illustration, car plusieurs URI syntaxiquement distincts NE DEVRAIENT PAS être utilisés pour désigner la même instance d'objet de MIB, afin d'éviter des résultats inattendus dans les systèmes fondés sur les URI qui utilisent la comparaison de chaîne pour vérifier l'égalité des URI.

`snmp://exemple.com/bridge1/1.3.6.1.2.1.2.2.1.8.*`

Cet exemple désigne la colonne `ifOperStatus` de la MIB IF dans le contexte `bridge1` SNMP à `exemple.com`.

`snmp://exemple.com//(1.3.6.1.2.1.2.2.1.7,1.3.6.1.2.1.2.2.1.8).*`

Cet exemple désigne toutes les paires (`ifAdminStatus`, `ifOperStatus`) dans la MIB IF dans le contexte SNMP par défaut à `exemple.com`.

6. Considérations sur la sécurité

Une utilisation prévue pour ce schéma d'URI est la désignation de la localisation de l'accès de gestion aux appareils de communication. Des telles informations de localisation peuvent être considérées comme sensibles dans certains environnements, rendant important le contrôle de l'accès à ces informations et éventuellement même de les chiffrer lorsque elles sont envoyées sur le réseau. Toutes les utilisations de ce schéma d'URI devraient fournir des mécanismes de sécurité appropriés aux environnements dans lesquels de telles utilisations ont des chances d'être déployées.

L'architecture SNMP inclut le contrôle de l'accès aux informations de gestion (voir le paragraphe 4.3 de la [RFC3411]). Un URI SNMP ne contient pas d'informations de sécurité suffisantes pour obtenir l'accès dans toutes les situations, car la syntaxe d'URI SNMP est incapable de coder les modèles de sécurité SNMP, les niveaux de sécurité SNMP, et les accreditifs ou les informations de chiffrement pour les noms de sécurité SNMP. D'autres moyens sont nécessaires pour fournir de telles informations ; une possibilité est la pré configuration hors bande du gestionnaire SNMP, comme le montrent les diagrammes de la Section 2.

Par elle-même, la présence d'un nom de sécurité (*securityName*) dans un URI SNMP n'autorise pas l'utilisation de ce nom de sécurité pour accéder aux informations de gestion. Le gestionnaire SNMP DEVRAIT plutôt confronter le nom de sécurité dans l'URI à un nom de sécurité SNMP et aux informations de sécurité associées qui ont été pré configurées pour l'usage du gestionnaire. Si un URI SNMP contient un nom de sécurité que le gestionnaire SNMP n'est pas provisionné à utiliser, les opérations SNMP pour cet URI NE DEVRAIENT PAS être générées.

Les versions SNMP antérieures à SNMPv3 n'incluaient pas de sécurité adéquate. Même si le réseau lui-même est sûr (par

exemple, via l'utilisation de IPsec) il n'y a pas de contrôle sur qui sur le réseau sûr est autorisé à accéder et effectuer GET/SET (lire/changer/crée/supprimer) sur les objets dans les modules de MIB. Il est RECOMMANDÉ que les mises en œuvre considèrent les caractéristiques de sécurité fournies par le cadre SNMPv3 (voir une vue d'ensemble à la section 8 de la [RFC3410]) incluant la pleine prise en charge des mécanismes de chiffrement pour SNMPv3 (pour l'authentification et la protection de la confidentialité). Ceci est d'une importance encore plus grande pour les éléments de MIB considérés comme sensibles ou vulnérables à cause des effets collatéraux des GET.

De plus, le déploiement de versions SNMP antérieures à SNMPv3 N'EST PAS RECOMMANDÉ. Il est plutôt 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 module de MIB est correctement configurée pour donner accès aux objets seulement aux principaux (utilisateurs) qui ont des droits légitimes à opérer les GET ou SET (lire/changer/créer/supprimer) sur eux.

6.1 Considérations de sécurité d'URI SNMP à passerelle SNMP

Des considérations de sécurité supplémentaires s'appliquent aux passerelles SNMP qui génèrent des opérations SNMP pour les URI SNMP et retournent les résultats aux clients (voir à la Section 2) parce que les informations de gestion sont communiquées au delà du cadre SNMP. En général, une passerelle SNMP devrait avoir connaissance de la structure et la fonction des informations de gestion auxquelles elle accède via SNMP. Entre autres avantages, cela permet à une passerelle SNMP d'éviter les défaillances du contrôle d'accès SNMP parce que la passerelle peut rejeter un URI SNMP qui va causer de telles défaillances avant de générer une opération SNMP.

Les passerelles SNMP DEVRAIENT imposer des vérifications d'autorisation ou de contrôle d'accès sur tous les clients. Si une passerelle SNMP n'impose pas d'autorisation ou de contrôle d'accès, elle NE DOIT PAS obtenir ou utiliser automatiquement le matériel d'authentification SNMP pour des noms de sécurité arbitraires car le faire déjouerait les contrôles d'accès de SNMP. Toutes les passerelles SNMP DEVRAIENT plutôt authentifier chaque client et vérifier son autorisation d'utiliser un nom de sécurité dans un URI SNMP avant d'utiliser le nom de sécurité au nom de ce client.

Une passerelle SNMP est aussi chargée de s'assurer que toutes ses communications sont sécurisées de façon appropriée. Précisément, une passerelle SNMP DEVRAIT s'assurer que la communication des informations de gestion avec tout client est protégée au moins au niveau de sécurité SNMP utilisé pour l'accès SNMP correspondant (voir plus d'informations sur le niveau de sécurité au paragraphe 3.4.3 de la [RFC3411]). Si le client fournit des informations de sécurité SNMP, la passerelle SNMP DEVRAIT authentifier le client et DEVRAIT s'assurer qu'une vérification d'intégrité cryptographique authentifiée est utilisée pour cette communication afin d'empêcher la modification des informations de sécurité. De plus, si un client fournit une clé ou un secret, la passerelle SNMP DEVRAIT s'assurer qu'un chiffrement est utilisé en plus de la vérification d'intégrité pour cette communication pour empêcher la divulgation des clés ou secrets.

Il y a des objets de gestion définis dans les MIB SNMP dont le MAX-ACCESS est lecture-écriture et/ou lecture-crétion. De tels objets peuvent être considérés comme sensibles ou vulnérables dans certains environnements de réseau. Une passerelle SNMP qui prend en charge les opérations SNMP SET dans un environnement non sûr sans protection appropriée peut avoir un effet négatif sur le fonctionnement du réseau. Les spécifications de modules de MIB individuels, et en particulier leurs considérations sur la sécurité, devraient être consultées pour plus d'informations

Certains objets lisibles dans certains modules de MIB (c'est-à-dire, des objets avec un MAX-ACCESS autre que "not-accessible") peuvent être considérés comme sensibles ou vulnérables dans certains environnements de réseau. Il est donc important de contrôler même l'accès GET à ces objets via une passerelle SNMP et éventuellement même de chiffrer les valeurs de ces objets lorsque ils sont envoyés sur le réseau. Les spécifications de modules de MIB individuels, et en particulier leurs considérations sur la sécurité, devraient être consultées pour plus d'informations. Cette considération s'applique aussi aux objets pour lesquels les opérations de lecture ont des effets collatéraux.

7. Considérations relatives à l'IANA

L'IANA a enregistré le gabarit d'enregistrement d'URL qui se trouve en Appendice A conformément à la [RFC2717].

8. 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](#))

- [RFC2234] D. Crocker et P. Overell, "[BNF augmenté](#) pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir RFC5234*)
- [RFC3061] M. Mealling, "Espace de noms d'URN d'identifiant d'objet", février 2001. (*Information*)
- [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*)
- [RFC3416] R. Presuhn, éd., "[Version 2 des opérations de protocole](#) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (*STD0062*)
- [RFC3417] R. Presuhn, éd., "[Transpositions de transport](#) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par RFC4789*) (*STD0062*)
- [RFC3584] R. Frye et autres, "Coexistence entre les version 1, version 2, et version 3 du cadre de gestion de réseau standard de l'Internet", août 2003. (*BCP0074*)
- [RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD 66, janvier 2005.

9. Références pour information

- [RFC1738] T. Berners-Lee et autres, "[Localisateurs uniformes de ressource](#) (URL)", décembre 1994. (*P.S., Obsolète, voir les RFC4248 et 4266 ; MàJ par RFC8089*)
- [RFC1900] B. Carpenter, Y. Rekhter, "[Un dénumérotage représente du travail](#)", février 1996. (*Information*)
- [RFC2717] R. Petke, I. King, "Procédures d'enregistrement des noms de schéma d'URL", novembre 1999. (*Obsolète, voir RFC4395*) (*BCP0035*)
- [RFC3410] J. Case et autres, "[Introduction et déclarations d'applicabilité](#) pour le cadre de gestion standard de l'Internet", décembre 2002. (*Information*)
- [RFC3430] J. Schoenwaelder, "Transposition de transport du protocole simple de gestion de réseau sur le protocole de contrôle de transmission", décembre 2002. (*Expérimentale*)
- [RFC3617] E. Lear, "Schéma d'identifiants de ressource uniformes (URI) et déclaration d'applicabilité pour le protocole trivial de transfert de fichier (TFTP)", octobre 2003. (*Information*)
- [RFC4001] M. Daniele et autres, "[Conventions textuelles pour les adresses réseau](#) Internet", février 2005. (*P.S.*)

10. Remerciements

Des portions du présent document sont adaptées de la spécification de schéma d'URI TFTP de Eliot Lear [RFC3617]. Des portions des considérations sur la sécurité ont été adaptées des considérations sur la sécurité "passe-partout" largement utilisées pour les modules des MIB. Des commentaires de Ted Hardie, Michael Mealing, Larry Masinter, Frank Strauss, Bert Wijnen, Steve Bellovin, des listes de diffusion mreview@ops.ietf.org et uri@w3c.org mailing sur des versions antérieures du présent document ont résulté en améliorations significatives et ils en sont chaleureusement remerciés.

Appendice A. Gabarit d'enregistrement

Nom de schéma d'URL : snmp

Syntaxe de schéma d'URL : Section 3

Considérations de codage de caractère : Section 3

Utilisation prévue : Sections 1 et 2

Applications et/ou protocoles qui utilisent ce schéma : SNMP, toutes versions, voir les [RFC3410] et [RFC3584]. Aussi SNMP sur TCP, voir la [RFC3430].

Considérations d'interopérabilité : paragraphe 4.4

Considérations sur la sécurité : Section 6

Publications pertinentes : voir la liste dans la [RFC3410]. Aussi [RFC3430] et [RFC3584].

Contact : David L. Black, voir ci-dessous

Auteur/Contrôleur des changements : IESG

Adresse des auteurs

David L. Black
EMC Corporation
176 South Street
Hopkinton, MA 01748
USA
téléphone : +1 (508) 293-7953
mél : black_david@emc.com

Keith McCloghrie
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA USA 95134
USA
téléphone : +1 (408) 526-5260
mél : kzm@cisco.com

Juergen Schoenwaelder
International University Bremen
P.O. Box 750 561
28725 Bremen
Germany
téléphone : +49 421 200 3587
mél : j.schoenwaelder@iu-bremen.de

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.